A Term of Commutative Algebra

By Allen ALTMAN
and Steven KLEIMAN

$$
\begin{tikzcd}
& & R/\mathfrak{a} \arrow[dl, "\psi"] \arrow[dd, "1"] \\
R \arrow[urr, "\kappa"] \arrow[r, "\varphi"] \arrow[drr, "\kappa"'] & R' \arrow[dr, "\psi'"] & \\
& & R/\mathfrak{a}
\end{tikzcd}
$$

Worldwide Center of Mathematics

A Term of
Commutative Algebra

By Allen B. ALTMAN
and Steven L. KLEIMAN

Version of March 11, 2018: `tca.tex`

v. edition number for publishing purposes
ISBN 978-0-9885572-1-5

Contents

Preface

There is no shortage of books on Commutative Algebra, but the present book is different. Most books are monographs, with extensive coverage. But there is one notable exception: Atiyah and Macdonald's 1969 classic [4]. It is a clear, concise, and efficient textbook, aimed at beginners, with a good selection of topics. So it has remained popular. However, its age and flaws do show. So there is need for an updated and improved version, which the present book aims to be.

Atiyah and Macdonald explain their philosophy in their introduction. They say their book "has the modest aim of providing a rapid introduction to the subject. It is designed to be read by students who have had a first elementary course in general algebra. On the other hand, it is not intended as a substitute for the more voluminous tracts on Commutative Algebra. . . . The lecture-note origin of this book accounts for the rather terse style, with little general padding, and for the condensed account of many proofs." They "resisted the temptation to expand it in the hope that the brevity of [the] presentation will make clearer the mathematical structure of what is by now an elegant and attractive theory." They endeavor "to build up to the main theorems in a succession of simple steps and to omit routine verifications."

Atiyah and Macdonald's successful philosophy is wholeheartedly embraced below (it is a feature, not a flaw!), and also refined a bit. The present book also "grew out of a course of lectures." That course was based primarily on their book, but has been offered a number of times, and has evolved over the years, influenced by other publications, especially [16], and the reactions of the students. That course had as prerequisite a "first elementary course in general algebra" based on [3]. Below, to further clarify and streamline the "mathematical structure" of the theory, the theory is usually developed in its natural generality, where the settings are just what is appropriate for the arguments.

Atiyah and Macdonald's book comprises eleven chapters, split into forty-two sections. The present book comprises twenty-six chapters; each chapter represents a single lecture, and is self-contained. Lecturers are encouraged to emphasize the meaning of statements and the ideas of proofs, especially those in the longer and richer chapters, "waving their hands" and leaving the details for students to read on their own and to discuss with others.

Atiyah and Macdonald "provided . . . exercises at the end of each chapter," as well as some exercises within the text. They "provided hints, and sometimes complete solutions, to the hard" exercises. Furthermore, they developed a significant amount of new material in the exercises. By contrast, in the present book, the exercises are more closely tied in to the text, and complete solutions are given in the second part of the book. Doing so lengthened the book considerably. The solutions fill nearly as much space as the text. Moreover, seven chapters have appendices; they elaborate on important issues, most stemming from Atiyah and Macdonald's exercises.

There are 594 exercises below, including all of Atiyah and Macdonald's. The disposition of the latter is indicated in a special index. The 594 also include many exercises that come from other publications and many that originate here. Here the exercises are tailored to provide a means for students to check, to solidify, and to expand their understanding. Nearly all the 594 are intentionally not difficult, tricky, or involved. Rarely do they introduce new techniques, although some introduce new concepts, and many are used later. All the exercises within the text are used right away. Another special index indicates all the exercises that are used, and where.

Students are encouraged to try to solve lots of exercises, without first reading the solutions. If they become stuck on an exercise, then they should review the relevant material; if they remain stuck, then they should change tack by studying the solution, possibly discussing it with others, but always making sure they can, eventually, solve the whole exercise entirely on their own. In any event, students should always read the given solutions, just to make sure they haven't missed any details; also, some solutions provide enlightening alternative arguments.

As to prioritizing the exercises, here is one reasonable order: first, those that appear within the text; second, those that are used more often, as indicated in the index, "Use of the Exercises . . . "; third, those whose solutions are less involved, as indicated by their length; fourth, those whose statements sound interesting; fifth, those stemming from the exercises in Atiyah and Macdonald's book, as indicated in the index, "Disposition . . . ." Of course, no one should exhaust all the exercises of one level of priority before considering exercises of lower level; rather, if there's no other good reason to choose one exercise over another, then the order of priorities could serve as the deciding factor.

Instructors are encouraged to assign six exercises with short solutions, say a paragraph or two long, per lecture, and to ask students to write up solutions in their own words. Instructors are encouraged to examine students, possibly orally at a blackboard, possibly via written tests, on a small, randomly chosen subset of the assigned exercises. For use during each exam, instructors are urged to provide each student with a copy of the book that omits the solutions. A reasonable way to grade is to count the exerecises as 30%, a midterm as 30%, and a final as 40%.

Atiyah and Macdonald explain that "a proper treatment of Homological Algebra is impossible within the confines of a small book; on the other hand, it is hardly sensible to ignore it completely." So they "use elementary homological methods — exact sequence, diagrams, etc. — but . . . stop short of any results requiring a deep study of homology." Again, their philosophy is embraced and refined in the present book. Notably, below, elementary methods are used, not Tor's as they do, to prove the Ideal Criterion for flatness, and to prove that, over local rings, flat modules are free. Also, projective modules are treated below, but not in their book.

In the present book, Category Theory is a basic tool; in Atiyah and Macdonald's, it seems like a foreign language. Thus they discuss the universal (mapping) property (UMP) of localization of a ring, but provide an ad hoc characterization. They also prove the UMP of tensor product of modules, but do not name it this time. Below, the UMP is fundamental: there are many standard constructions; each has a UMP, which serves to characterize the resulting object up to unique isomorphism owing to one general observation of Category Theory. For example, the Left Exactness of Hom is viewed simply as expressing in other words that the kernel and the cokernel of a map are characterized by their UMPs; by contrast, Atiyah and Macdonald prove the Left Exactness via a tedious elementary argument.

Atiyah and Macdonald prove the Adjoint-Associativity Formula. They note it says that Tensor Product is the left adjoint of Hom. From it and the Left Exactness of Hom, they deduce the Right Exactness of Tensor Product. They note that this derivation shows that any "left adjoint is right exact." More generally, as explained below, this derivation shows that any left adjoint preserves arbitrary direct limits, ones indexed by any small category. Atiyah and Macdonald consider only direct limits indexed by a directed set, and sketch an ad hoc argument showing that tensor product preserves direct limit. Also, arbitrary direct sums are direct limits indexed by a discrete category (it is not a directed set); hence, the general result yields that Tensor Product and other left adjoints preserve arbitrary Direct Sum.

Below, left adjoints are proved unique up to unique isomorphism. Therefore, the functor of localization of a module is canonically isomorphic to the functor of tensor product with the localized base ring, as both are left adjoints of the same functor, Restriction of Scalars from the localized ring to the base ring. There is an alternative argument: since Localization is a left adjoint, it preserves Direct Sum and Cokernel; whence, it is isomorphic to that tensor-product functor by Watts Theorem, which characterizes all tensor-product functors as those linear functors that preserve Direct Sum and Cokernel. Atiyah and Macdonald's treatment is ad hoc. However, they do use the proof of Watts Theorem directly to show that, under the appropriate conditions, Completion of a module is Tensor Product with the completed base ring.

Below, Direct Limit is also considered as a functor, defined on the appropriate category of functors. As such, Direct Limit is a left adjoint. Hence, direct limits preserve other direct limits. Here the theory briefly climbs to a higher level of abstraction. The discussion is completely elementary, but by far the most abstract in the book. The extra abstraction can be difficult, especially for beginners.

Below, filtered direct limits are treated too. They are closer to the kind of limits treated by Atiyah and Macdonald. In particular, filtered direct limits preserve exactness and flatness. Further, they appear in the following lovely form of Lazard's Theorem: in a canonical way, every module is the direct limit of free modules of finite rank; moreover, the module is flat if and only if that direct limit is filtered.

Atiyah and Macdonald treat primary decomposition in a somewhat dated way. First, they study primary decompositions of ideals. Then, in the exercises, they indicate how to translate the theory to modules. Associated primes play a secondary role: they are defined as the radicals of the primary components, then characterized as the primes that are the radicals of annihilators of elements. Finally, when the rings and modules are Noetherian, primary decompositions are proved to exist, and associated primes to be annihilators themselves.

Below, as is standard nowadays, associated primes of modules are studied right from the start; they are defined as the primes that are annihilators of elements. Submodules are called primary if the quotient modules have only one associated prime. Below, Atiyah and Macdonald's primary submodules are called old-primary submodules, and they are studied too, mostly in an appendix. In the Noetherian case, the two notions agree; so the two studies provide alternative proofs.

Below, general dimension theory is developed for Noetherian modules; whereas, Atiyah and Macdonald treat only Noetherian rings. Moreover, the modules below are often assumed to be semilocal — that is, their annihilator lies in only finitely many maximal ideals — correspondingly, Atiyah and Macdonald's rings are local.

There are several other significant differences between Atiyah and Macdonald's treatment and the one below. First, the Noether Normalization Lemma is proved below in a stronger form for nested sequences of ideals; consequently, for algebras that are finitely generated over a field, dimension theory can be developed directly and more extensively, without treating Noetherian local rings first (see **(21.25)** for the latter approach). Second, in a number of results below, the modules are assumed to be finitely presented over an arbitrary ring, rather than finitely generated over a Noetherian ring. Third, there is an elementary treatment of regular sequences below and a proof of Serre's Criterion for Normality; this important topic is developed further in an appendix. Fourth, below, the Adjoint-Associativity Formula is proved over a pair of base rings; hence, it yields both a left and a right adjoint to the functor of restriction of scalars.

Many people have contributed to the quality of the present book. Pavel Etingof and Bjorn Poonen lectured from an earlier edition, and Dan Grayson, Antoni Rangachev, and Amnon Yekutieli read parts of it; all five have made a number of good comments and suggestions, which were incorporated. Many people have pointed out typos, which were corrected. For this service to the community, the authors are grateful, and they welcome any future such remarks from anyone.

It is rarely easy to learn anything new of substance, value, and beauty, like Commutative Algebra, but it is always satisfying, enjoyable, and worthwhile to do so. The authors bid their readers much success in learning Commutative Algebra.

Allen B. Altman and Steven L. Kleiman
11 March 2018

A Term of Commutative Algebra

Subject Matter

By Allen ALTMAN
and Steven KLEIMAN

$$
\begin{tikzcd}
 & & R/\mathfrak{a} \arrow[dl, "\psi"] \arrow[dd, "1"] \\
R \arrow[urr, "\kappa"] \arrow[r, "\varphi"] \arrow[drr, "\kappa"'] & R' \arrow[dr, "\psi'"] & \\
 & & R/\mathfrak{a}
\end{tikzcd}
$$

Worldwide Center of Mathematics

Part I
Subject Matter

1. Rings and Ideals

We begin by reviewing and developing basic notions and conventions to set the stage. Throughout this book, we emphasize universal mapping properties (UMPs); they are used to characterize notions and to make constructions. So, although polynomial rings and residue rings should already be familiar in other ways, we present their UMPs immediately, and use them extensively. We also discuss Boolean rings, idempotents, and the Chinese Remainder Theorem.

A. Text

(1.1) (Rings). — Recall that a **ring** R is an abelian group, written additively, with an associative multiplication that is distributive over the addition.

Throughout this book, every ring has a multiplicative identity, denoted by 1. Further, every ring is commutative (that is, $xy = yx$ in it), with an occasional exception, which is always marked (normally, it's a ring of matrices).

As usual, the additive identity is denoted by 0. Note that, for any x in R,

$$x \cdot 0 = 0;$$

indeed, $x \cdot 0 = x(0+0) = x \cdot 0 + x \cdot 0$, and $x \cdot 0$ can be canceled by adding $-(x \cdot 0)$.

We allow $1 = 0$. *If* $1 = 0$*, then* $R = 0$; indeed, $x = x \cdot 1 = x \cdot 0 = 0$ for any x.

A **unit** is an element u with a **reciprocal** $1/u$ such that $u \cdot 1/u = 1$. Alternatively, $1/u$ is denoted u^{-1} and is called the **multiplicative inverse** of u. The units form a multiplicative group, denoted $R^\times$.

For example, the ordinary integers form a ring $\mathbb{Z}$, and its units are 1 and -1.

A ring **homomorphism**, or simply a **ring map**, $\varphi\colon R \to R'$ is a map preserving sums, products, and 1. Clearly, $\varphi(R^\times) \subset R'^\times$. We call φ an **isomorphism** if it is bijective, and then we write $\varphi : R \xrightarrow{\sim} R'$. We call φ an **endomorphism** if $R' = R$. We call φ an **automorphism** if it is bijective and if $R' = R$.

If there is an unnamed isomorphism between rings R and R', then we write $R = R'$ when it is **canonical**; that is, it does not depend on any artificial choices, so that for all practical purposes, R and R' are the same — they are just copies of each other. For example, the polynomial rings $R[X]$ and $R[Y]$ in variables X and Y are canonically isomorphic when X and Y are identified. (Recognizing that an isomorphism is canonical can provide insight and obviate verifications. The notion is psychological, and depends on the context.) Otherwise, we write $R \simeq R'$.

A subset $R'' \subset R$ is a **subring** if R'' is a ring and the inclusion $R'' \hookrightarrow R$ a ring map. In this case, we call R a **extension (ring)** of R', and the inclusion $R'' \hookrightarrow R$ an **extension (of rings)** or a **(ring) extension**. For example, given a ring map $\varphi\colon R \to R'$, its image $\mathrm{Im}(\varphi) := \varphi(R)$ is a subring of R'. We call $\varphi\colon R \to R'$ an **extension** of $\varphi''\colon R'' \to R'$, and we say that φ'' **extends** to φ if $\varphi|R'' = \varphi''$.

An R**-algebra** is a ring R' that comes equipped with a ring map $\varphi\colon R \to R'$, called the **structure map**. To indicate that R' is an R-algebra without referring to φ, we write R'/R. For example, every ring is canonically a $\mathbb{Z}$-algebra. An R-**algebra homomorphism**, or R**-map**, $R' \to R''$ is a ring map between R-algebras compatible with their structure maps.

A group G is said to **act** on R if there is a homomorphism given from G into the group of automorphisms of R. Normally, we identify each $g \in G$ with its associated automorphism. The **ring of invariants** R^G is the subring defined by

$$R^G := \{x \in R \mid gx = g \text{ for all } g \in G\}.$$

Similarly, a group G is said to **act** on R'/R if G acts on R' and each $g \in G$ is an R-map. Note that R'^G is an R-subalgebra.

(1.2) (Boolean rings). — The simplest nonzero ring has two elements, 0 and 1. It is unique, and denoted $\mathbb{F}_2$.

Given any ring R and any set X, let R^X denote the set of functions $f\colon X \to R$. Then R^X is, clearly, a ring under valuewise addition and multiplication.

For example, take $R := \mathbb{F}_2$. Given $f\colon X \to R$, put $S := f^{-1}\{1\}$. Then $f(x) = 1$ if $x \in S$, and $f(x) = 0$ if $x \notin S$; in other words, f is the **characteristic function** χ_S. Thus *the characteristic functions form a ring, namely,* $\mathbb{F}_2^X$*.*

Given $T \subset X$, clearly $\chi_S \cdot \chi_T = \chi_{S\cap T}$. Further, $\chi_S + \chi_T = \chi_{S\triangle T}$, where $S\triangle T$ is the **symmetric difference**:

$$S\triangle T := (S \cup T) - (S \cap T) = (S - T) \cup (T - S);$$

here $S - T$ denotes, as usual, the set of elements of S not in T. Thus *the subsets of X form a ring: sum is symmetric difference, and product is intersection. This ring is canonically isomorphic to* $\mathbb{F}_2^X$*.*

A ring B is called **Boolean** if $f^2 = f$ for all $f \in B$. If so, then $2f = 0$ as $2f = (f + f)^2 = f^2 + 2f + f^2 = 4f$. For example, $\mathbb{F}_2^X$ is, plainly, Boolean.

Suppose X is a topological space, and give $\mathbb{F}_2$ the **discrete** topology; that is, every subset is both open and closed. Consider the continuous functions $f\colon X \to \mathbb{F}_2$. Clearly, they are just the χ_S where S is both open and closed. Clearly, they form a Boolean subring of $\mathbb{F}_2^X$. Conversely, Stone's Theorem (**13.44**) asserts that *every Boolean ring is canonically isomorphic to the ring of continuous functions from a compact Hausdorff topological space X to $\mathbb{F}_2$, or equivalently, isomorphic to the ring of open and closed subsets of X.*

(1.3) (Polynomial rings). — Let R be a ring, $P := R[X_1, \ldots, X_n]$ the polynomial ring in n variables (see [**3**, pp. 352–3] or [**11**, p. 268]). Recall that P has this **Universal Mapping Property** (UMP): *given a ring map $\varphi\colon R \to R'$ and given an element x_i of R' for each i, there is a unique ring map $\pi\colon P \to R'$ with $\pi|R = \varphi$ and $\pi(X_i) = x_i$.* In fact, since π is a ring map, necessarily π is given by the formula:

$$\pi\Big(\sum a_{(i_1,\ldots,i_n)} X_1^{i_1} \cdots X_n^{i_n}\Big) = \sum \varphi(a_{(i_1,\ldots,i_n)}) x_1^{i_1} \cdots x_n^{i_n}. \qquad \textbf{(1.3.1)}$$

In other words, P is universal among R-algebras equipped with a list of n elements: P is one, and P maps uniquely to any other with the lists are respected.

Similarly, let $\mathcal{X} := \{X_\lambda\}_{\lambda\in\Lambda}$ be any set of variables. Set $P' := R[\mathcal{X}]$; the elements of P' are the polynomials in any finitely many of the X_λ; sum and product are defined as in P. Thus P' contains as a subring the polynomial ring in any finitely many X_λ, and P' is the union of these subrings. Clearly, P' has essentially the same UMP as P: *given $\varphi\colon R \to R'$ and given $x_\lambda \in R'$ for each λ, there is a unique $\pi\colon P' \to R'$ with $\pi|R = \varphi$ and $\pi(X_\lambda) = x_\lambda$.*

(1.4) (Ideals). — Let R be a ring. Recall that a subset $\mathfrak{a}$ is called an **ideal** if

(1) $0 \in \mathfrak{a}$,

(2) whenever $a, b \in \mathfrak{a}$, also $a + b \in \mathfrak{a}$, and

(3) whenever $x \in R$ and $a \in \mathfrak{a}$, also $xa \in \mathfrak{a}$.

Given a subset $\mathfrak{a} \subset R$, by the ideal $\langle \mathfrak{a} \rangle$ that $\mathfrak{a}$ **generates**, we mean the smallest ideal containing $\mathfrak{a}$. Given elements $a_\lambda \in R$ for $\lambda \in \Lambda$, by the ideal they **generate**, we mean the ideal generated by the set $\{a_\lambda\}$. If $\Lambda = \emptyset$, then this ideal consists just of 0. If $\Lambda = \{1, \ldots, n\}$, then the ideal is usually denoted by $\langle a_1, \ldots, a_n \rangle$.

Any ideal containing all the a_λ contains any (finite) **linear combination** $\sum x_\lambda a_\lambda$ with $x_\lambda \in R$ and almost all 0. Form the set $\mathfrak{a}$, or $\sum Ra_\lambda$, of all such linear combinations. Plainly, $\mathfrak{a}$ is an ideal containing all a_λ, so is the ideal they generate.

Given an ideal $\mathfrak{a}$ and elements a_λ that generate it, we call the a_λ **generators**.

Given a single element a, we say that the ideal $\langle a \rangle$ is **principal**. By the preceding observation, $\langle a \rangle$ is equal to the set of all multiples xa with $x \in R$.

Given a number of ideals $\mathfrak{a}_\lambda$, by their **sum** $\sum \mathfrak{a}_\lambda$, we mean the set of all finite linear combinations $\sum x_\lambda a_\lambda$ with $x_\lambda \in R$ and $a_\lambda \in \mathfrak{a}_\lambda$. Plainly, $\sum \mathfrak{a}_\lambda$ is equal to the ideal the $\mathfrak{a}_\lambda$ **generate**, namely, the smallest ideal that contains all $\mathfrak{a}_\lambda$.

By the intersection $\bigcap \mathfrak{a}_\lambda$, we mean the intersection as sets. It is plainly an ideal.

If the $\mathfrak{a}_\lambda$ are finite in number, by their **product** $\prod \mathfrak{a}_\lambda$, we mean the ideal generated by all products $\prod a_\lambda$ with $a_\lambda \in \mathfrak{a}_\lambda$.

Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, by the **transporter** of $\mathfrak{b}$ into $\mathfrak{a}$, we mean the set

$$(\mathfrak{a} : \mathfrak{b}) := \{x \in R \mid x\mathfrak{b} \subset \mathfrak{a}\}.$$

Plainly, $(\mathfrak{a} : \mathfrak{b})$ is an ideal. Plainly,

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}, \quad \mathfrak{a}, \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}, \quad \text{and} \quad \mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b}).$$

Further, for any ideal $\mathfrak{c}$, the distributive law holds: $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}$.

Given an ideal $\mathfrak{a}$, notice $\mathfrak{a} = R$ *if and only if* $1 \in \mathfrak{a}$. Indeed, if $1 \in \mathfrak{a}$, then $x = x \cdot 1 \in \mathfrak{a}$ for every $x \in R$. It follows that $\mathfrak{a} = R$ *if and only if* $\mathfrak{a}$ *contains a unit.* Further, if $\langle x \rangle = R$, then x is a unit, since then there is an element y such that $xy = 1$. If $\mathfrak{a} \neq R$, then $\mathfrak{a}$ is said to be **proper**.

Given a ring map $\varphi\colon R \to R'$, denote by $\mathfrak{a}R'$ or $\mathfrak{a}^e$ the ideal of R' generated by the set $\varphi(\mathfrak{a})$. We call it the **extension** of $\mathfrak{a}$.

Given an ideal $\mathfrak{a}'$ of R', its preimage $\varphi^{-1}(\mathfrak{a}')$ is, plainly, an ideal of R. We call $\varphi^{-1}(\mathfrak{a}')$ the **contraction** of $\mathfrak{a}'$ and sometimes denote it by $\mathfrak{a}'^c$.

(1.5) (Residue rings). — Let $\varphi\colon R \to R'$ be a ring map. Recall its **kernel** $\mathrm{Ker}(\varphi)$ is defined to be the ideal $\varphi^{-1}(0)$ of R. Recall $\mathrm{Ker}(\varphi) = 0$ if and only if φ is injective.

Conversely, let $\mathfrak{a}$ be an ideal of R. Form the set of cosets of $\mathfrak{a}$:

$$R/\mathfrak{a} := \{x + \mathfrak{a} \mid x \in R\}.$$

Recall that $R/\mathfrak{a}$ inherits a ring structure, and is called the **residue ring** or **quotient ring** or **factor ring** of R **modulo** $\mathfrak{a}$. Form the **quotient map**

$$\kappa\colon R \to R/\mathfrak{a} \quad \text{by} \quad \kappa x := x + \mathfrak{a}.$$

The element $\kappa x \in R/\mathfrak{a}$ is called the **residue** of x. Clearly, κ is surjective, κ is a ring map, and κ has kernel $\mathfrak{a}$. Thus every ideal is a kernel!

Note that $\mathrm{Ker}(\varphi) \supset \mathfrak{a}$ if and only if $\varphi\mathfrak{a} = 0$.

Recall that, *if* $\mathrm{Ker}(\varphi) \supset \mathfrak{a}$*, then there is a ring map* $\psi\colon R/\mathfrak{a} \to R'$ *with* $\psi\kappa = \varphi$;

that is, the following diagram is **commutative**:

$$\begin{tikzcd} R \arrow[r, "\kappa"] \arrow[dr, "\varphi"'] & R/\mathfrak{a} \arrow[d, "\psi"] \\ & R' \end{tikzcd}$$

Conversely, *if ψ exists, then* $\operatorname{Ker}(\varphi) \supset \mathfrak{a}$, *or* $\varphi\mathfrak{a} = 0$, or $\mathfrak{a}R' = 0$, since $\kappa\mathfrak{a} = 0$.

Further, *if ψ exists, then ψ is unique* as κ is surjective.

Finally, as κ is surjective, *if ψ exists, then ψ is surjective if and only if φ is so.* In addition, then ψ *is injective if and only if* $\mathfrak{a} = \operatorname{Ker}(\varphi)$. Hence then ψ *is an isomorphism if and only if φ is surjective and* $\mathfrak{a} = \operatorname{Ker}(\varphi)$. Therefore, always

$$R/\operatorname{Ker}(\varphi) \xrightarrow{\sim} \operatorname{Im}(\varphi). \tag{1.5.1}$$

In practice, it is usually more productive to view $R/\mathfrak{a}$ not as a set of cosets, but simply as another ring R' that comes equipped with a surjective ring map $\varphi\colon R \to R'$ whose kernel is the given ideal $\mathfrak{a}$.

Finally, $R/\mathfrak{a}$ has, as we saw, this UMP: $\kappa(\mathfrak{a}) = 0$*, and given $\varphi\colon R \to R'$ such that $\varphi(\mathfrak{a}) = 0$, there is a unique ring map $\psi\colon R/\mathfrak{a} \to R'$ such that $\psi\kappa = \varphi$.* In other words, $R/\mathfrak{a}$ is universal among R-algebras R' such that $\mathfrak{a}R' = 0$.

Above, if $\mathfrak{a}$ is the ideal generated by elements a_λ, then the UMP can be usefully rephrased as follows: $\kappa(a_\lambda) = 0$ *for all λ, and given $\varphi\colon R \to R'$ such that $\varphi(a_\lambda) = 0$ for all λ, there is a unique ring map $\psi\colon R/\mathfrak{a} \to R'$ such that $\psi\kappa = \varphi$.*

The UMP serves to determine $R/\mathfrak{a}$ up to unique isomorphism. Indeed, say R', equipped with $\varphi\colon R \to R'$, has the UMP too. Then $\varphi(\mathfrak{a}) = 0$; so there is a unique $\psi\colon R/\mathfrak{a} \to R'$ with $\psi\kappa = \varphi$. And $\kappa(\mathfrak{a}) = 0$; so there is a unique $\psi'\colon R' \to R/\mathfrak{a}$ with $\psi'\varphi = \kappa$. Then, as shown, $(\psi'\psi)\kappa = \kappa$, but $1 \circ \kappa = \kappa$ where 1

$$\begin{tikzcd} & & R/\mathfrak{a} \arrow[dl, "\psi"] \arrow[dd, "1"] \\ R \arrow[urr, "\kappa"] \arrow[r, "\varphi"] \arrow[drr, "\kappa"'] & R' \arrow[dr, "\psi'"] & \\ & & R/\mathfrak{a} \end{tikzcd}$$

is the identity map of $R/\mathfrak{a}$; hence, $\psi'\psi = 1$ by uniqueness. Similarly, $\psi\psi' = 1$ where 1 now stands for the identity map of R'. Thus ψ and ψ' are inverse isomorphisms.

The preceding proof is completely formal, and so works widely. There are many more constructions to come, and each one has an associated UMP, which therefore serves to determine the construction up to unique isomorphism.

Proposition (1.6). — *Let R be a ring, $P := R[X]$ the polynomial ring in one variable, $a \in R$, and $\pi\colon P \to R$ the R-algebra map defined by $\pi(X) := a$. Then*

(1) $\operatorname{Ker}(\pi) = \{F(X) \in P \mid F(a) = 0\} = \langle X - a\rangle$ *and* (2) $P/\langle X - a\rangle \xrightarrow{\sim} R$.

Proof: Set $G := X - a$. Given $F \in P$, let's show $F = GH + r$ with $H \in P$ and $r \in R$. By linearity, we may assume $F := X^n$. If $n \geq 1$, then $F = (G + a)X^{n-1}$, so $F = GH + aX^{n-1}$ with $H := X^{n-1}$. If $n - 1 \geq 1$, repeat with $F := X^{n-1}$. Etc.

Then $\pi(F) = \pi(G)\pi(H) + \pi(r) = r$. Hence $F \in \operatorname{Ker}(\pi)$ if and only if $F = GH$. But $\pi(F) = F(a)$ by **(1.3.1)**. Thus (1) holds. So **(1.5.1)** yields (2). □

(1.7) (Degree of a polynomial). — Let R be a ring, P the polynomial ring in any number of variables. Given a nonzero $F \in P$, recall that its (total) **degree**, $\deg(F)$, is defined as follows: if F is a monomial $\mathbf{M}$, then its degree $\deg(\mathbf{M})$ is the sum of its exponents; in general, $\deg(F)$ is the largest $\deg(\mathbf{M})$ of all monomials $\mathbf{M}$ in F.

Given any $G \in P$ with FG nonzero, notice that

$$\deg(FG) \le \deg(F) + \deg(G). \tag{1.7.1}$$

Indeed, any monomial in FG is the product $\mathbf{MN}$ of a monomial $\mathbf{M}$ in F and a monomial $\mathbf{N}$ in G. Further, $\deg(\mathbf{MN}) = \deg(\mathbf{M}) + \deg(\mathbf{N}) \le \deg(F) + \deg(G)$.

However, equality need not hold. For example, suppose that there is only one variable X, that $F = aX^m + \cdots$ and $G = bX^n + \cdots$ with $m = \deg(F)$ and $n = \deg(G)$, and that $ab = 0$. Then $\deg(FG) < mn$.

Note also that, if $a \ne b$, then the polynomial $X^2 - (a+b)X$ has degree 2, but at least three distinct zeros: 0, a, b.

(1.8) (Order of a polynomial). — Let R be a ring, P the polynomial ring in variables X_λ for $\lambda \in \Lambda$, and $(x_\lambda) \in R^\Lambda$ a vector. Let $\varphi_{(x_\lambda)}\colon P \to P$ denote the R-algebra map defined by $\varphi_{(x_\lambda)} X_\mu := X_\mu + x_\mu$ for all $\mu \in \Lambda$. Plainly $\varphi_{(x_\lambda)}$ is an automorphism with inverse $\varphi_{(-x_\lambda)}$. Fix a nonzero $F \in P$.

The **order** of F at the zero vector (0), denoted $\operatorname{ord}_{(0)} F$, is defined as the smallest $\deg(\mathbf{M})$ of all the monomials $\mathbf{M}$ in F. In general, the **order** of F at the vector (x_λ), denoted $\operatorname{ord}_{(x_\lambda)} F$, is defined by the formula: $\operatorname{ord}_{(x_\lambda)} F := \operatorname{ord}_{(0)}(\varphi_{(x_\lambda)} F)$.

Notice that $\operatorname{ord}_{(x_\lambda)} F = 0$ *if and only if* $F(x_\lambda) \ne 0$. Indeed, the equivalence is obvious if $(x_\lambda) = (0)$. Thus it always holds, as $(\varphi_{(x_\lambda)} F)(0) = F(x_\lambda)$.

Given μ and $x \in R$, form $F_{\mu,x}$ by substituting x for X_μ in F. If $F_{\mu,x_\mu} \ne 0$, then

$$\operatorname{ord}_{(x_\lambda)} F \le \operatorname{ord}_{(x_\lambda)} F_{\mu,x_\mu}. \tag{1.8.1}$$

Indeed, if $x_\mu = 0$, then F_{μ,x_μ} is the sum of the terms without X_μ in F. Hence, if $(x_\lambda) = (0)$, then **(1.8.1)** holds. But substituting 0 for X_μ in $\varphi_{(x_\lambda)} F$ is the same as substituting x_μ for X_μ in F and then applying $\varphi_{(x_\lambda)}$ to the result; that is, $(\varphi_{(x_\lambda)} F)_{\mu,0} = \varphi_{(x_\lambda)} F_{\mu,x_\mu}$. Thus (1.8.1) always holds.

Of course, $F_{\mu,x}$ lies in the polynomial subring in the variables X_λ for all $\lambda \ne \mu$. Let $(\check{x}_\mu)$ be the vector of x_λ for all $\lambda \ne \mu$. If $F_{\mu,x_\mu} \ne 0$, then

$$\operatorname{ord}_{(x_\lambda)} F_{\mu,x_\mu} = \operatorname{ord}_{(\check{x}_\mu)} F_{\mu,x_\mu}. \tag{1.8.2}$$

Plainly, **(1.8.2)** holds if $(x_\lambda) = (0)$. So it always holds, as $\varphi_{(x_\lambda)} F_{\mu,x_\mu} = \varphi_{(\check{x}_\mu)} F_{\mu,x_\mu}$.

Given any $G \in P$ with FG nonzero, notice that

$$\operatorname{ord}_{(x_\lambda)} FG \ge \operatorname{ord}_{(x_\lambda)} F + \operatorname{ord}_{(x_\lambda)} G, \tag{1.8.3}$$

Indeed, if $(x_\lambda) = (0)$, then the proof of **(1.8.3)** is similar to that of **(1.7.1)**. But $\varphi_{(x_\lambda)} FG = \varphi_{(x_\lambda)} F \, \varphi_{(x_\lambda)} G$. Thus **(1.8.3)** always holds.

(1.9) (Nested ideals). — Let R be a ring, $\mathfrak{a}$ an ideal, and $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Given an ideal $\mathfrak{b} \supset \mathfrak{a}$, form the corresponding set of cosets of $\mathfrak{a}$:

$$\mathfrak{b}/\mathfrak{a} := \{b + \mathfrak{a} \mid b \in \mathfrak{b}\} = \kappa(\mathfrak{b}).$$

Clearly, $\mathfrak{b}/\mathfrak{a}$ is an ideal of $R/\mathfrak{a}$. Also $\mathfrak{b}/\mathfrak{a} = \mathfrak{b}(R/\mathfrak{a})$.

Clearly, *the operations $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ and $\mathfrak{b}' \mapsto \kappa^{-1}(\mathfrak{b}')$ are inverse to each other, and establish a bijective correspondence between the set of ideals $\mathfrak{b}$ of R containing $\mathfrak{a}$ and the set of all ideals $\mathfrak{b}'$ of $R/\mathfrak{a}$. Moreover, this correspondence preserves inclusions.*

Given an ideal $\mathfrak{b} \supset \mathfrak{a}$, form the composition of the quotient maps

$$\varphi\colon R \to R/\mathfrak{a} \to (R/\mathfrak{a})\big/(\mathfrak{b}/\mathfrak{a}).$$

Clearly, φ is surjective, and $\mathrm{Ker}(\varphi) = \mathfrak{b}$. Hence, owing to (**1.5**), φ factors through the canonical isomorphism ψ in this commutative diagram:

$$\begin{tikzcd} R \arrow[r] \arrow[d] & R/\mathfrak{b} \arrow[d, "\psi"', "\simeq"] \\ R/\mathfrak{a} \arrow[r] & (R/\mathfrak{a})\big/(\mathfrak{b}/\mathfrak{a}) \end{tikzcd}$$

(1.10) (Idempotents). — Let R be a ring. Let $e \in R$ be an **idempotent**; that is, $e^2 = e$. Then Re is a ring with e as 1, because $(xe)e = xe$. But Re is not a subring of R unless $e = 1$, although Re is an ideal.

Set $e' := 1 - e$. Then e' is idempotent and $e \cdot e' = 0$. We call e and e' **complementary idempotents**. Conversely, if two elements $e_1, e_2 \in R$ satisfy $e_1 + e_2 = 1$ and $e_1 e_2 = 0$, then they are complementary idempotents, as for each i,

$$e_i = e_i \cdot 1 = e_i(e_1 + e_2) = e_i^2.$$

We denote the set of all idempotents by $\mathrm{Idem}(R)$. Let $\varphi\colon R \to R'$ be a ring map. Then $\varphi(e)$ is idempotent. So the restriction of φ to $\mathrm{Idem}(R)$ is a map

$$\mathrm{Idem}(\varphi)\colon\ \mathrm{Idem}(R) \to \mathrm{Idem}(R').$$

Example (1.11). — Let $R := R' \times R''$ be a **product** of two rings: its operations are performed componentwise. The additive identity is $(0, 0)$; the multiplicative identity is $(1, 1)$. Set $e' := (1, 0)$ and $e'' := (0, 1)$. Then e' and e'' are complementary idempotents. The next proposition shows this example is the only one possible.

Proposition (1.12). — *Let R be a ring, and e', e'' complementary idempotents. Set $R' := Re'$ and $R'' := Re''$. Define $\varphi\colon R \to R' \times R''$ by $\varphi(x) := (xe', xe'')$. Then φ is a ring isomorphism. Moreover, $R' = R/Re''$ and $R'' = R/Re'$.*

Proof: Define a surjection $\varphi'\colon R \to R'$ by $\varphi'(x) := xe'$. Then φ' is a ring map, since $xye' = xye'^2 = (xe')(ye')$. Moreover, $\mathrm{Ker}(\varphi') = Re''$, since if $xe' = 0$, then $x = x \cdot 1 = xe + xe'' = xe''$. Thus (**1.5.1**) yields $R' = R/Re''$.

Similarly, define a surjection $\varphi''\colon R \to R''$ by $\varphi''(x) := xe''$. Then φ'' is a ring map, and $\mathrm{Ker}(\varphi'') = Re'$. Thus $R'' = R/Re'$.

So φ is a ring map. It's surjective, since $(xe', x'e'') = \varphi(xe' + x'e'')$. It's injective, since if $xe' = 0$ and $xe'' = 0$, then $x = xe' + xe'' = 0$. Thus φ is an isomorphism. □

B. Exercises

Exercise (1.13) . — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$, $\mathfrak{a}_1$, $\mathfrak{a}_2$ ideals of R, and $\mathfrak{b}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$ ideals of R'. Prove the following statements:

(1a) $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$.	(1b) $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supset \mathfrak{b}_1^c + \mathfrak{b}_2^c$.
(2a) $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subset \mathfrak{a}^e \cap \mathfrak{a}_2^e$.	(2b) $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.
(3a) $(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$.	(3b) $(\mathfrak{b}_1\mathfrak{b}_2)^c \supset \mathfrak{b}_1^c\mathfrak{b}_2^c$.
(4a) $(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subset (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$.	(4b) $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subset (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$.

Exercise (1.14) . — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Prove the following statements:

(1) Then $\mathfrak{a}^{ec} \supset \mathfrak{a}$ and $\mathfrak{b}^{ce} \subset \mathfrak{b}$. (2) Then $\mathfrak{a}^{ece} = \mathfrak{a}^{e}$ and $\mathfrak{b}^{cec} = \mathfrak{b}^{c}$.

(3) If $\mathfrak{b}$ is an extension, then $\mathfrak{b}^c$ is the largest ideal of R with extension $\mathfrak{b}$.

(4) If two extensions have the same contraction, then they are equal.

Exercise (1.15) . — Let R be a ring, $\mathfrak{a}$ an ideal, $\mathcal{X}$ a set of variables. Prove:

(1) The extension $\mathfrak{a}\big(R[\mathcal{X}]\big)$ is the set $\mathfrak{a}[\mathcal{X}]$ of polynomials with coefficients in $\mathfrak{a}$.

(2) $\mathfrak{a}\big(R[\mathcal{X}]\big) \cap R = \mathfrak{a}$.

Exercise (1.16) . — Let R be a ring, $\mathfrak{a}$ an ideal, and $\mathcal{X}$ a set of variables. Set $P := R[\mathcal{X}]$. Prove $P/\mathfrak{a}P = (R/\mathfrak{a})[\mathcal{X}]$.

Exercise (1.17) . — Let R be a ring, $P := R[\{X_\lambda\}]$ the polynomial ring in variables X_λ for $\lambda \in \Lambda$, and $(x_\lambda) \in R^\Lambda$ a vector. Let $\pi_{(x_\lambda)}\colon P \to R$ denote the R-algebra map defined by $\pi_{(x_\lambda)}X_\mu := x_\mu$ for all $\mu \in \Lambda$. Show:

(1) Any $F \in P$ has the form $F = \sum a_{(i_1,\ldots,i_n)}(X_{\lambda_1} - x_{\lambda_1})^{i_1} \cdots (X_{\lambda_n} - x_{\lambda_n})^{i_n}$ for unique $a_{(i_1,\ldots,i_n)} \in R$..

(2) Then $\operatorname{Ker}(\pi_{(x_\lambda)}) = \{F \in P \mid F\big((x_\lambda)\big) = 0\} = \langle\{X_\lambda - x_\lambda\}\rangle$.

(3) Then π induces an isomorphism $P/\langle\{X_\lambda - x_\lambda\}\rangle \xrightarrow{\sim} R$.

(4) Given $F \in P$, its residue in $P/\langle\{X_\lambda - x_\lambda\}\rangle$ is equal to $F\big((x_\lambda)\big)$.

(5) Let $\mathcal{Y}$ be a second set of variables. Then $P[\mathcal{Y}]/\langle\{X_\lambda - x_\lambda\}\rangle \xrightarrow{\sim} R[\mathcal{Y}]$.

Exercise (1.18) . — Let R be a ring, $P := R[X_1, \ldots, X_n]$ the polynomial ring in variables X_i. Given $F = \sum a_{(i_1,\ldots,i_n)}X_1^{i_1} \cdots X_n^{i_n} \in P$, formally set

$$\partial F/\partial X_j := \sum i_j a_{(i_1,\ldots,i_n)}X_1^{i_1} \cdots X_n^{i_n}/X_j \in P \quad \text{for } j = 1, \ldots, n. \qquad \textbf{(1.18.1)}$$

Given $(x_1, \ldots, x_n) \in R^n$, set $\mathbf{x} := (x_1, \ldots, x_n)$, set $a_j := (\partial F/\partial X_j)(\mathbf{x})$, and set $\mathfrak{M} := \langle X_1 - x_1, \ldots, X_n - x_n\rangle$. Show $F = F(\mathbf{x}) + \sum a_j(X_j - x_j) + G$ with $G \in \mathfrak{M}^2$. First show that, if $F = (X_1 - x_1)^{i_1} \cdots (X_n - x_n)^{i_n}$, then $\partial F/\partial X_j = i_jF/(X_j - x_j)$.

Exercise (1.19) . — Let R be a ring, X a variable, $F \in P := R[X]$, and $a \in R$. Set $F' := \partial F/\partial X$; see **(1.18.1)**. We call a a **root** of F if $F(a) = 0$, a **simple root** if also $F'(a) \neq 0$, and a **supersimple root** if also $F'(a)$ is a unit.

Show that a is a root of F if and only if $F = (X - a)G$ for some $G \in P$, and if so, then G is unique: that a is a simple root if and only if also $G(a) \neq 0$; and that a is a supersimple root if and only if also $G(a)$ is a unit.

Exercise (1.20) . — Let R be a ring, $P := R[X_1, \ldots, X_n]$ the polynomial ring, $F \in P$ of degree d, and $F_i := X_i^{d_i} + a_1X_i^{d_i-1} + \cdots$ a monic polynomial in X_i alone for all i. Find $G, G_i \in P$ such that $F = \sum_{i=1}^n F_iG_i + G$ where $G_i = 0$ or $\deg(G_i) \leq d - d_i$ and where the highest power of X_i in G is less than d_i.

Exercise (1.21) (*Chinese Remainder Theorem*) . — Let R be a ring.

(1) Let $\mathfrak{a}$ and $\mathfrak{b}$ be **comaximal** ideals; that is, $\mathfrak{a} + \mathfrak{b} = R$. Show

$$\text{(a) } \mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} \quad \text{and} \quad \text{(b) } R/\mathfrak{a}\mathfrak{b} = (R/\mathfrak{a}) \times (R/\mathfrak{b}).$$

(2) Let $\mathfrak{a}$ be comaximal to both $\mathfrak{b}$ and $\mathfrak{b}'$. Show $\mathfrak{a}$ is also comaximal to $\mathfrak{b}\mathfrak{b}'$.

(3) Given $m, n \geq 1$, show $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal if and only if $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are.

(4) Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ be pairwise comaximal. Show:

(a) $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ are comaximal;
(b) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$;
(c) $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\sim} \prod(R/\mathfrak{a}_i)$.

(5) Find an example where $\mathfrak{a}$ and $\mathfrak{b}$ satisfy (1)(a), but aren't comaximal.

Exercise (1.22) . — First, given a prime number p and a $k \geq 1$, find the idempotents in $\mathbb{Z}/\langle p^k \rangle$. Second, find the idempotents in $\mathbb{Z}/\langle 12 \rangle$. Third, find the number of idempotents in $\mathbb{Z}/\langle n \rangle$ where $n = \prod_{i=1}^{N} p_i^{n_i}$ with p_i distinct prime numbers.

Exercise (1.23) . — Let $R := R' \times R''$ be a product of rings, $\mathfrak{a} \subset R$ an ideal. Show $\mathfrak{a} = \mathfrak{a}' \times \mathfrak{a}''$ with $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ ideals. Show $R/\mathfrak{a} = (R'/\mathfrak{a}') \times (R''/\mathfrak{a}'')$.

Exercise (1.24) . — Let R be a ring; e, e' idempotents (see **(10.23)** also). Show:

(1) Set $\mathfrak{a} := \langle e \rangle$. Then $\mathfrak{a}$ is **idempotent**; that is, $\mathfrak{a}^2 = \mathfrak{a}$.
(2) Let $\mathfrak{a}$ be a principal idempotent ideal. Then $\mathfrak{a} = \langle f \rangle$ with f idempotent.
(3) Set $e'' := e + e' - ee'$. Then $\langle e, e' \rangle = \langle e'' \rangle$, and e'' is idempotent.
(4) Let $e_1, \ldots, e_r$ be idempotents. Then $\langle e_1, \ldots, e_r \rangle = \langle f \rangle$ with f idempotent.
(5) Assume R is Boolean. Then every finitely generated ideal is principal.

Exercise (1.25) . — Let L be a **lattice**, that is, a partially ordered set in which every pair $x, y \in L$ has a sup $x \vee y$ and an inf $x \wedge y$. Assume L is **Boolean**; that is:

(1) L has a least element 0 and a greatest element 1.
(2) The operations $\wedge$ and $\vee$ **distribute** over each other; that is,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \text{and} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

(3) Each $x \in L$ has a unique **complement** x'; that is, $x \wedge x' = 0$ and $x \vee x' = 1$.

Show that the following six laws are obeyed:

$$x \wedge x = x \quad \text{and} \quad x \vee x = x. \qquad \textbf{(idempotent)}$$
$$x \wedge 0 = 0,\ x \wedge 1 = x \quad \text{and} \quad x \vee 1 = 1,\ x \vee 0 = x. \qquad \textbf{(unitary)}$$
$$x \wedge y = y \wedge x \quad \text{and} \quad x \vee y = y \vee x. \qquad \textbf{(commutative)}$$
$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \quad \text{and} \quad x \vee (y \vee z) = (x \vee y) \vee z. \qquad \textbf{(associative)}$$
$$x'' = x \quad \text{and} \quad 0' = 1,\ 1' = 0. \qquad \textbf{(involutory)}$$
$$(x \wedge y)' = x' \vee y' \quad \text{and} \quad (x \vee y)' = x' \wedge y'. \qquad \textbf{(De Morgan's)}$$

Moreover, show that $x \leq y$ if and only if $x = x \wedge y$.

Exercise (1.26) . — Let L be a Boolean lattice; see **(1.25)**. For all $x, y \in L$, set

$$x + y := (x \wedge y') \vee (x' \wedge y) \quad \text{and} \quad xy := x \wedge y.$$

Show: (1) $x + y = (x \vee y)(x' \vee y')$ and (2) $(x + y)' = (x'y') \vee (xy)$. Furthermore, show L is a Boolean ring.

Exercise (1.27) . — Given a Boolean ring R, order R by $x \leq y$ if $x = xy$. Show R is thus a Boolean lattice. Viewing this construction as a map ρ from the set of Boolean-ring structures on the set R to the set of Boolean-lattice structures on R, show ρ is bijective with inverse the map λ associated to the construction in **(1.26)**.

Exercise (1.28) . — Let X be a set, and L the set of all subsets of X, partially ordered by inclusion. Show that L is a Boolean lattice and that the ring structure on L constructed in (**1.2**) coincides with that constructed in (**1.26**).

Assume X is a topological space, and let M be the set of all its open and closed subsets. Show that M is a sublattice of L, and that the subring structure on M of (**1.2**) coincides with the ring structure of (**1.26**) with M for L.

Exercise (1.29) . — Let R be a ring, $P := R[X_1, \dots, X_m]$ the polynomial ring in variables X_i, and $V \subset R^m$ the set of common zeros of a set of polynomials $F_\lambda \in P$.

(1) Let $I(V)$ be the ideal of all $F \in P$ vanishing on V, and $P(V)$ the R-algebra of all functions $\gamma\colon V \to R$ given by evaluating some $G \in P$. Show $I(V)$ is the largest set of polynomials with V as set of common zeros. Show $P/I(V) = P(V)$. And show $1 \in I(V)$ (or $P(V) = 0$) if and only if $V = \emptyset$.

(2) Let $W \subset R^n$ be like V, and $\rho\colon V \to W$ any map. Call ρ **regular** if there are $G_i \in P$ with $\rho(v) = (G_1(v), \dots, G_n(v))$ for all $v \in V$. If ρ is regular, define $\rho^*\colon P(W) \to P(V)$ by $\rho^*(\delta) := \delta \circ \rho$, and show ρ^* is a well-defined algebra map.

(3) Let $Q := R[Y_1, \dots, Y_n]$ be the polynomial ring, and $\zeta_i \in P(W)$ the function given by evaluating the variable Y_i. Let $\varphi\colon P(W) \to P(V)$ be an algebra map. Define $\varphi^*\colon V \to W$ by $\varphi^*(v) := (w_1, \dots, w_n)$ where $w_i := (\varphi\zeta_i)(v)$, and show φ^* is a well-defined regular map.

(4) Show $\rho \mapsto \rho^*$ and $\varphi \mapsto \varphi^*$ define inverse bijective correspondences between the regular maps $\rho\colon V \to W$ and the algebra maps $\varphi\colon P(W) \to P(V)$.

2. Prime Ideals

Prime ideals are the key to the structure of commutative rings. So we review the basic theory. Specifically, we define prime ideals, and show their residue rings are domains. We show maximal ideals are prime, and discuss examples. Finally, we use Zorn's Lemma to prove the existence of maximal ideals in every nonzero ring.

A. Text

(2.1) (Zerodivisors). — Let R be a ring. An element x is called a **zerodivisor** if there is a nonzero y with $xy = 0$; otherwise, x is called a **nonzerodivisor**. Denote the set of zerodivisors by $\operatorname{z.div}(R)$ and the set of nonzerodivisors by S_0.

(2.2) (Multiplicative subsets, prime ideals). — Let R be a ring. A subset S is called **multiplicative** if $1 \in S$ and if $x, y \in S$ implies $xy \in S$.

For example, the subset of nonzerodivisors S_0 is multiplicative.

An ideal $\mathfrak{p}$ is called **prime** if its complement $R - \mathfrak{p}$ is multiplicative, or equivalently, if $1 \notin \mathfrak{p}$ and if $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

(2.3) (Fields, domains). — A ring is called a **field** if $1 \neq 0$ and if every nonzero element is a unit. Standard examples include the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, and the finite field $\mathbb{F}_q$ with q elements.

A ring is called an **integral domain**, or simply a **domain**, if $\langle 0 \rangle$ is prime, or equivalently, if R is nonzero and has no nonzero zerodivisors.

Every domain R is a subring of its **fraction field** $\operatorname{Frac}(R)$, which consists of the fractions x/y with $x, y \in R$ and $y \neq 0$. Conversely, any subring R of a field K, including K itself, is a domain; indeed, any nonzero $x \in R$ cannot be a zerodivisor, because, if $xy = 0$, then $(1/x)(xy) = 0$, so $y = 0$. Further, $\operatorname{Frac}(R)$ has this UMP: the inclusion of R into any field L extends uniquely to an inclusion of $\operatorname{Frac}(R)$ into L. For example, the ring of integers $\mathbb{Z}$ is a domain, and $\operatorname{Frac}(\mathbb{Z}) = \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

(2.4) (Polynomials over a domain). — Let R be a domain, $\mathcal{X} := \{X_\lambda\}_{\lambda \in \Lambda}$ a set of variables. Set $P := R[\mathcal{X}]$. Then P is a domain too. In fact, given nonzero $F, G \in P$, not only is their product FG nonzero, but also, as explained next, given a well ordering of the variables, the grlex leading term of FG is the product of the grlex leading terms of F and G, and

$$\deg(FG) = \deg(F) + \deg(G). \tag{2.4.1}$$

Using the given ordering of the variables, well order all the monomials $\mathbf{M}$ of the same degree via the lexicographic order on exponents. Among the $\mathbf{M}$ in F with $\deg(\mathbf{M}) = \deg(F)$, the largest is called the **grlex leading monomial** of F. Its **grlex leading term** is the product $a\mathbf{M}$ where $a \in R$ is the coefficient of $\mathbf{M}$ in F, and a is called the **grlex leading coefficient**.

The grlex leading term of FG is the product of those $a\mathbf{M}$ and $b\mathbf{N}$ of F and G, and (2.4.1) holds, for the following reasons. First, $ab \neq 0$ as R is a domain. Second,

$$\deg(\mathbf{MN}) = \deg(\mathbf{M}) + \deg(\mathbf{N}) = \deg(F) + \deg(G).$$

Third, $\deg(\mathbf{MN}) \geq \deg(\mathbf{M}'\mathbf{N}')$ for every pair of monomials $\mathbf{M}'$ and $\mathbf{N}'$ in F and G. Equality holds if and only if $\deg(\mathbf{M}') = \deg(F)$ and $\deg(\mathbf{N}') = \deg(G)$. If so and if either $\mathbf{M}' \neq \mathbf{M}$ or $\mathbf{N}' \neq \mathbf{N}$, then $\mathbf{M}'\mathbf{N}'$ is strictly smaller than $\mathbf{MN}$. Thus $ab\mathbf{MN}$ is the grlex leading term of FG, and **(2.4.1)** holds.

Similarly, as explained next, *the grlex hind term of FG is the product of the grlex hind terms of F and G.* Further, given a vector $(x_\lambda) \in R^\Lambda$, then

$$\mathrm{ord}_{(x_\lambda)} FG = \mathrm{ord}_{(x_\lambda)} F + \mathrm{ord}_{(x_\lambda)} G, \tag{2.4.2}$$

Among the monomials $\mathbf{M}$ in F with $\mathrm{ord}(\mathbf{M}) = \mathrm{ord}(F)$, the smallest is called the **grlex hind monomial** of F. The **grlex hind term** of F is the product $a\mathbf{M}$ where $a \in R$ is the coefficient of $\mathbf{M}$ in F.

It is easy to prove that *the grlex hind term of FG is the product of the grlex hind terms of F and G* by adapting the reasoning with grlex leading terms given above. Hence, if $(x_\lambda) = (0)$, then **(2.4.2)** holds. Thus it holds in general, because $\varphi_{(x_\lambda)} FG = \varphi_{(x_\lambda)} F\, \varphi_{(x_\lambda)} G$; see **(1.8)**.

If $FG = 1$, note $F, G \in R$ owing to **(2.4.1)**. This observation can fail if R is not a domain. For example, if $a^2 = 0$ in R, then $(1 + aX)(1 - aX) = 1$ in $R[X]$.

The fraction field $\mathrm{Frac}(P)$ is called the field of **rational functions,** and is also denoted by $K(\mathcal{X})$ where $K := \mathrm{Frac}(R)$.

(2.5) (Unique factorization). — Let R be a domain, p a nonzero nonunit. We call p **prime** if, whenever $p \mid xy$ (that is, there exists $z \in R$ such that $pz = xy$), either $p \mid x$ or $p \mid y$. Clearly, *p is prime if and only if the ideal $\langle p \rangle$ is prime.*

Given $x, y \in R$, we call any $d \in R$ their **greatest common divisor** and write $d = \gcd(x, y)$ if $d \mid x$ and $d \mid y$ and if $c \mid x$ and $c \mid y$ implies $c \mid d$. As R is a domain, it's easy to see that $\gcd(x, y)$ is unique up to unit factor.

We call p **irreducible** if, whenever $p = yz$, either y or z is a unit. We call R a **Unique Factorization Domain** (UFD) if (1) every nonzero nonunit factors into a product of irreducibles and (2) the factorization is unique up to order and units.

Recall that (1) holds if and only if every ascending chain of principal ideals $\langle x_1 \rangle \subset \langle x_2 \rangle \subset \cdots$ stabilizes; see [**3**, (2.3), p. 393]. Moreover, if (1) holds, then (2) holds if and only if every irreducible is prime; see [**3**, (2.8), p. 395]. Conversely, primes are, plainly, always irreducible.

Plainly, if R is a UFD, then $\gcd(x, y)$ always exists.

Standard examples of UFDs include any field, the integers $\mathbb{Z}$, and a polynomial ring in n variables over a UFD; see [**3**, p. 398, p. 401], [**11**, Cor. 18.23, p. 297].

Lemma (2.6). — *Let $\varphi\colon R \to R'$ be a ring map, and $T \subset R'$ a subset. If T is multiplicative, then $\varphi^{-1}T$ is multiplicative; the converse holds if φ is surjective.*

Proof: Set $S := \varphi^{-1}T$. If T is multiplicative, then $1 \in S$ as $\varphi(1) = 1 \in T$, and $x, y \in S$ implies $xy \in S$ as $\varphi(xy) = \varphi(x)\varphi(y) \in T$; thus S is multiplicative.

If S is multiplicative, then $1 \in T$ as $1 \in S$ and $\varphi(1) = 1$; further, $x, y \in S$ implies $\varphi(x)$, $\varphi(y)$, $\varphi(xy) \in T$. If φ is surjective, then every $x' \in T$ is of the form $x' = \varphi(x)$ for some $x \in S$. Thus if φ is surjective, then T is multiplicative if $\varphi^{-1}T$ is. □

Proposition (2.7). — *Let $\varphi\colon R \to R'$ be a ring map, and $\mathfrak{q} \subset R'$ an ideal. Set $\mathfrak{p} := \varphi^{-1}\mathfrak{q}$. If $\mathfrak{q}$ is prime, then $\mathfrak{p}$ is prime; the converse holds if φ is surjective.*

Proof: By **(2.6)**, $R - \mathfrak{p}$ is multiplicative if and only if $R' - \mathfrak{q}$ is. So the assertion results from the definition **(2.2)**. □

Corollary (2.8). — *Let R be a ring, $\mathfrak{p}$ an ideal. Then $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is a domain.*

Proof: By (**2.7**), $\mathfrak{p}$ is prime if and only if $\langle 0\rangle \subset R/\mathfrak{p}$ is. So the assertion results from the definition of domain in (**2.3**). □

Exercise (2.9) . — Let R be a ring, $P := R[\mathcal{X}, \mathcal{Y}]$ the polynomial ring in two sets of variables $\mathcal{X}$ and $\mathcal{Y}$. Set $\mathfrak{p} := \langle \mathcal{X}\rangle$. Show $\mathfrak{p}$ is prime if and only if R is a domain.

Definition (2.10). — Let R be a ring. An ideal $\mathfrak{m}$ is said to be **maximal** if $\mathfrak{m}$ is proper and if there is no proper ideal $\mathfrak{a}$ with $\mathfrak{m} \subsetneqq \mathfrak{a}$.

Example (2.11). — Let R be a domain, $R[X, Y]$ the polynomial ring. Then $\langle X\rangle$ is prime by (**2.9**). However, $\langle X\rangle$ is not maximal since $\langle X\rangle \subsetneqq \langle X, Y\rangle$. Moreover, $\langle X, Y\rangle$ is maximal if and only if R is a field by (**1.17**)(3) and by (**2.14**) below.

Proposition (2.12). — *A ring R is a field if and only if $\langle 0\rangle$ is a maximal ideal.*

Proof: Suppose R is a field. Let $\mathfrak{a}$ be a nonzero ideal, and a a nonzero element of $\mathfrak{a}$. Since R is a field, $a \in R^\times$. So (**1.4**) yields $\mathfrak{a} = R$.

Conversely, suppose $\langle 0\rangle$ is maximal. Take $x \neq 0$. Then $\langle x\rangle \neq \langle 0\rangle$. So $\langle x\rangle = R$. So x is a unit by (**1.4**). Thus R is a field. □

Corollary (2.13). — *Let R be a ring, $\mathfrak{m}$ an ideal. Then $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.*

Proof: Clearly, $\mathfrak{m}$ is maximal in R if and only if $\langle 0\rangle$ is maximal in $R/\mathfrak{m}$ by (**1.9**). Thus (**2.12**) yields the assertion. □

Example (2.14). — Let R be a ring, P the polynomial ring in variables X_λ, and $x_\lambda \in R$ for all λ. Set $\mathfrak{m} := \langle \{X_\lambda - x_\lambda\}\rangle$. Then $P/\mathfrak{m} = R$ by (**1.17**)(3). Thus $\mathfrak{m}$ is maximal if and only if R is a field by (**2.13**).

Corollary (2.15). — *In a ring, every maximal ideal is prime.*

Proof: A field is a domain by (**2.3**). So (**2.8**) and (**2.13**) yield the result. □

(2.16) (Coprime elements). — Let R be a ring, and $x, y \in R$. We say x and y are **(strictly) coprime** if their ideals $\langle x\rangle$ and $\langle y\rangle$ are comaximal.

Plainly, x and y are coprime if and only if there are $a, b \in R$ such that $ax+by = 1$, if and only if, given any $z \in R$, there are $a, b \in R$ such that $ax + by = z$.

Plainly, x and y are coprime if and only if there is $b \in R$ with $by \equiv 1 \pmod{\langle x\rangle}$, if and only if the residue of y is a unit in $R/\langle x\rangle$.

Fix $m, n \geq 1$. By (**1.21**)(3), x and y are coprime if and only if x^m and y^n are.

If x and y are coprime, then their images in any algebra R' are too.

(2.17) (PIDs). — A domain R is called a **Principal Ideal Domain** (PID) if every ideal is principal. Examples include a field k, the polynomial ring $k[X]$ in one variable, and the ring $\mathbb{Z}$ of integers. A PID is a UFD; see [**3**, (2.12), p. 396], [**11**, Thm. 18.11, p. 291].

Let R be a PID, $\mathfrak{p}$ a nonzero prime ideal. Say $\mathfrak{p} = \langle p\rangle$. Then p is prime by (**2.5**), so irreducible. Now, let $q \in R$ be irreducible. Then $\langle q\rangle$ is maximal for this reason: if $\langle q\rangle \subsetneqq \langle x\rangle$, then $q = xy$ for some nonunit y; so x must be a unit as q is irreducible. So $R/\langle q\rangle$ is a field by (**2.13**). Also $\langle q\rangle$ is prime by (**2.15**); so q is prime by (**2.5**). Thus every irreducible element is prime, and every nonzero prime ideal is maximal.

Exercise (2.18) . — Show that, in a PID, nonzero elements x and y are **relatively prime** (share no prime factor) if and only if they're coprime.

Example (2.19). — Let R be a PID, and $p \in R$ a prime. Set $k := R/\langle p\rangle$. Let X be a variable, and set $P := R[X]$. Take $G \in P$; let G' be its image in $k[X]$; assume G' is irreducible. Set $\mathfrak{m} := \langle p, G\rangle$. Then $P/\mathfrak{m} \xrightarrow{\sim} k[X]/\langle G'\rangle$ by (**1.16**) and (**1.9**), and $k[X]/\langle G'\rangle$ is a field by (**2.17**); hence, $\mathfrak{m}$ is maximal by (**2.13**).

Theorem (2.20). — *Let R be a PID. Let $P := R[X]$ be the polynomial ring in one variable X, and $\mathfrak{p}$ a nonzero prime ideal of P.*

(1) *Then $\mathfrak{p} = \langle F\rangle$ with F prime, or $\mathfrak{p}$ is maximal.*

(2) *Assume $\mathfrak{p}$ is maximal. Then either $\mathfrak{p} = \langle F\rangle$ with F prime, or $\mathfrak{p} = \langle p, G\rangle$ with $p \in R$ prime, $pR = \mathfrak{p} \cap R$, and $G \in P$ prime with image $G' \in (R/pR)[X]$ prime.*

Proof: Recall that R is a UFD, and so P is one too; see (**2.17**) and (**2.5**).

If $\mathfrak{p} = \langle F\rangle$ for some $F \in P$, then F is prime as $\mathfrak{p}$ is. So assume $\mathfrak{p}$ isn't principal.

Take a nonzero $F_1 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, $\mathfrak{p}$ contains a prime factor F_1' of F_1. Replace F_1 by F_1'. As $\mathfrak{p}$ isn't principal, $\mathfrak{p} \neq \langle F_1\rangle$. So there is a prime $F_2 \in \mathfrak{p} - \langle F_1\rangle$. Set $K := \mathrm{Frac}(R)$. Gauss's Lemma implies that F_1 and F_2 are also prime in $K[X]$; see [**3**, p. 401], [**11**, Thm. 18.15, p. 295]. So F_1 and F_2 are relatively prime in $K[X]$. So (**2.17**) and (**2.18**) yield $G_1, G_2 \in P$ and $c \in R$ with $(G_1/c)F_1 + (G_2/c)F_2 = 1$. So $c = G_1F_1 + G_2F_2 \in R \cap \mathfrak{p}$. Hence $R \cap \mathfrak{p} \neq 0$. But $R \cap \mathfrak{p}$ is prime, and R is a PID; so $R \cap \mathfrak{p} = pR$ where p is prime. Also pR is maximal by (**2.17**).

Set $k := R/pR$. Then k is a field by (**2.13**). Set $\mathfrak{q} := \mathfrak{p}/pR \subset k[X]$. Then $k[X]/\mathfrak{q} = P/\mathfrak{p}$ by (**1.16**) and (**1.9**). But $\mathfrak{p}$ is prime; so $P/\mathfrak{p}$ is a domain by (**2.8**). So $k[X]/\mathfrak{q}$ is a domain too. So $\mathfrak{q}$ is prime also by (**2.8**). So $\mathfrak{q}$ is maximal by (**2.17**). So $\mathfrak{p}$ is maximal by (**1.9**). In particular, (1) holds.

Since $k[X]$ is a PID and $\mathfrak{q}$ is prime, $\mathfrak{q} = \langle G'\rangle$ where G' is prime in $k[X]$. Take $G \in \mathfrak{p}$ with image G'. Then $\mathfrak{p} = \langle p, G\rangle$ as $\mathfrak{p}/\langle p\rangle = \langle G'\rangle$. Say $G = \prod G_i$ with $G_i \in P$ prime. So $G' = \prod G_i'$ with G_i' the image of G_i in $k[X]$. But G' is prime. So $\langle G'\rangle = \langle G_j'\rangle$ for some j. So replace G' by G_j' and G by G_j. Then G is prime.

Finally, $\mathfrak{p} = \langle F\rangle$ and $\mathfrak{p} = \langle p, G\rangle$ can't both hold. Else, $F \mid p$. So $\deg(F) = 0$ by (**2.4.1**). So $\langle F\rangle = \langle p\rangle$. So $\mathfrak{p} = \langle p\rangle$. So $G' = 0$, a contradiction. Thus (2) holds. □

Theorem (2.21). — *Every proper ideal $\mathfrak{a}$ is contained in some maximal ideal.*

Proof: Set $\mathcal{S} := \{\text{ideals } \mathfrak{b} \mid \mathfrak{b} \supset \mathfrak{a} \text{ and } \mathfrak{b} \not\ni 1\}$. Then $\mathfrak{a} \in \mathcal{S}$, and $\mathcal{S}$ is partially ordered by inclusion. Given a totally ordered subset $\{\mathfrak{b}_\lambda\}$ of $\mathcal{S}$, set $\mathfrak{b} := \bigcup \mathfrak{b}_\lambda$. Then $\mathfrak{b}$ is clearly an ideal, and $1 \notin \mathfrak{b}$; so $\mathfrak{b}$ is an upper bound of $\{\mathfrak{b}_\lambda\}$ in $\mathcal{S}$. Hence by Zorn's Lemma [**16**, pp. 25, 26], [**14**, p. 880, p. 884], $\mathcal{S}$ has a maximal element, and it is the desired maximal ideal. □

Corollary (2.22). — *Let R be a ring, $x \in R$. Then x is a unit if and only if x belongs to no maximal ideal.*

Proof: By (**1.4**), x is a unit if and only if $\langle x\rangle$ is not proper. Apply (**2.21**). □

B. Exercises

Exercise (2.23) . — Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals, and $\mathfrak{p}$ a prime ideal. Prove that these conditions are equivalent: (1) $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$; and (2) $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p}$; and (3) $\mathfrak{ab} \subset \mathfrak{p}$.

Exercise (2.24) . — Let R be a ring, $\mathfrak{p}$ a prime ideal, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ maximal ideals. Assume $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Show $\mathfrak{p} = \mathfrak{m}_i$ for some i.

Exercise (2.25) . — Let R be a ring, and $\mathfrak{p}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals with $\mathfrak{p}$ prime.
(1) Assume $\mathfrak{p} \supset \bigcap_{i=1}^{n} \mathfrak{a}_i$. Show $\mathfrak{p} \supset \mathfrak{a}_j$ for some j,
(2) Assume $\mathfrak{p} = \bigcap_{i=1}^{n} \mathfrak{a}_i$. Show $\mathfrak{p} = \mathfrak{a}_j$ for some j,

Exercise (2.26) . — Let R be a ring, $\mathcal{S}$ the set of all ideals that consist entirely of zerodivisors. Show that $\mathcal{S}$ has maximal elements and they're prime. Conclude that $\mathrm{z.div}(R)$ is a union of primes.

Exercise (2.27) . — Given a prime number p and an integer $n \geq 2$, prove that the residue ring $\mathbb{Z}/\langle p^n \rangle$ does not contain a domain as a subring.

Exercise (2.28) . — Let $R := R' \times R''$ be a product of two rings. Show that R is a domain if and only if either R' or R'' is a domain and the other is 0.

Exercise (2.29) . — Let $R := R' \times R''$ be a product of rings, $\mathfrak{p} \subset R$ an ideal. Prove $\mathfrak{p}$ is prime if and only if either $\mathfrak{p} = \mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $\mathfrak{p} = R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime. What if *prime* is replaced by *maximal*?

Exercise (2.30) . — Let R be a domain, and $x, y \in R$. Assume $\langle x \rangle = \langle y \rangle$. Show $x = uy$ for some unit u.

Exercise (2.31) . — Let k be a field, R a nonzero ring, $\varphi\colon k \to R$ a ring map. Prove φ is injective.

Exercise (2.32) . — Let R be a ring, $\mathfrak{p}$ a prime, $\mathcal{X}$ a set of variables. Let $\mathfrak{p}[\mathcal{X}]$ denote the set of polynomials with coefficients in $\mathfrak{p}$. Prove these statements:

(1) $\mathfrak{p}R[\mathcal{X}]$ and $\mathfrak{p}[\mathcal{X}]$ and $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$ are primes of $R[\mathcal{X}]$, which contract to $\mathfrak{p}$.
(2) Assume $\mathfrak{p}$ is maximal. Then $\mathfrak{p}R[\mathcal{X}] + \langle \mathcal{X} \rangle$ is maximal.

Exercise (2.33) . — Let R be a ring, X a variable, $H \in P := R[X]$, and $a \in R$. Given $n \geq 1$, show $(X-a)^n$ and H are coprime if and only if $H(a)$ is a unit.

Exercise (2.34) . — Let R be a ring, X a variable, $F \in P := R[X]$, and $a \in R$. Set $F' := \partial F / \partial X$; see **(1.18.1)**. Show the following statements are equivalent:

(1) a is a supersimple root of F.
(2) a is a root of F, and $X - a$ and F' are coprime.
(3) $F = (X-a)G$ for some G in P coprime to $X - a$.

Show that, if (3) holds, then G is unique.

Exercise (2.35) . — Let R be a ring, X a variable, $F(X)$ a polynomial of degree d. Show: (1) Assume R is a domain. Then F has at most d (distict) zeros in R.
(2) Take $R := \mathbb{Z}/\langle 6 \rangle$ and $F := X^2 + X$. Then F has more than d zeros in R.

Exercise (2.36) . — Let R be a ring, $\mathfrak{p}$ a prime; $\mathcal{X}$ a set of variables; $F, G \in R[\mathcal{X}]$. Let $c(F)$, $c(G)$, $c(FG)$ be the ideals of R generated by the coefficients of F, G, FG.
(1) Assume $\mathfrak{p}$ doesn't contain either $c(F)$ or $c(G)$. Show $\mathfrak{p}$ doesn't contain $c(FG)$.
(2) Assume $c(F) = R$ and $c(G) = R$. Show $c(FG) = R$.

Exercise (2.37) . — Let B be a Boolean ring. Show that every prime $\mathfrak{p}$ is maximal, and that $B/\mathfrak{p} = \mathbb{F}_2$.

Exercise (2.38) . — Let R be a ring. Assume that, given any $x \in R$, there is an $n \geq 2$ with $x^n = x$. Show that every prime $\mathfrak{p}$ is maximal.

Exercise (2.39) . — Prove the following statements or give a counterexample.

(1) The complement of a multiplicative subset is a prime ideal.
(2) Given two prime ideals, their intersection is prime.
(3) Given two prime ideals, their sum is prime.
(4) Given a ring map $\varphi\colon R \to R'$, the operation φ^{-1} carries maximal ideals of R' to maximal ideals of R.
(5) In (1.9), an ideal $\mathfrak{n}' \subset R/\mathfrak{a}$ is maximal if and only if $\kappa^{-1}\mathfrak{n}' \subset R$ is maximal.

Exercise (2.40) . — Preserve the setup of (2.20). Let $F := a_0X^n + \cdots + a_n$ be a polynomial of positive degree n. Assume that R has infinitely many prime elements p, or simply that there is a p such that $p \nmid a_0$. Show that $\langle F\rangle$ is not maximal.

Exercise (2.41) . — Preserve the setup of (2.20). Let $\langle 0\rangle \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ be a chain of primes in P. Show $n \leq 2$, with equality if the chain is **maximal** — or, not a proper subchain of a longer chain — and if R has infinitely many primes.

Exercise (2.42) (*Schwartz–Zippel Theorem with multiplicities*) . — Let R be a domain, $T \subset R$ a subset of q elements, $P := R[X_1, \dots, X_n]$ the polynomial ring in n variables, and $F \in P$ a nonzero polynomial of degree d.

(1) Show by induction on n that $\sum_{x_i \in T} \operatorname{ord}_{(x_1,\dots,x_n)} F \leq dq^{n-1}$.
(2) Show that at most dq^{n-1} points $(x_1, \dots, x_n) \in T^n$ satisfy $F(x_1, \dots, x_n) = 0$.
(3) Assume $d < q$. Show that $F(x_1, \dots, x_n) \neq 0$ for some $x_i \in T_i$.

Exercise (2.43) . — Let R be a domain, $P := R[X_1, \dots, X_n]$ the polynomial ring, $F \in P$ nonzero, and $T_i \subset R$ subsets with t_i elements for $i = 1, \dots, n$. For all i, assume that the highest power of X_i in F is at most $t_i - 1$. Show by induction on n that $F(x_1, \dots, x_n) \neq 0$ for some $x_i \in T_i$.

Exercise (2.44) (*Alon's Combinatorial Nullstellensatz* [1]) . — Let R be a domain, $P := R[X_1, \dots, X_n]$ the polynomial ring, $F \in P$ nonzero of degree d, and $T_i \subset R$ a subset with t_i elements for $i = 1, \dots, n$. Let $\mathbf{M} := \prod_{i=1}^n X_i^{m_i}$ be a monomial with $m_i < t_i$ for all i. Assume F vanishes on $T_1 \times \cdots \times T_n$. Set $F_i(X_i) := \prod_{x \in T_i}(X_i - x)$.

(1) Find $G_i \in P$ with $\deg(G_i) \leq d - t_i$ such that $F = \sum_{i=1}^n F_iG_i$.
(2) Assume $\mathbf{M}$ appears in F. Show $\deg(\mathbf{M}) < d$.
(3) Assume R is a field K. Set $\mathfrak{a} := \langle F_1, \dots, F_n\rangle$ and $t := \prod_{i=1}^n t_i$. Define the evaluation map $\mathrm{ev}\colon P \to K^t$ by $\mathrm{ev}(G) := \big(G(x_1, \dots, x_n)\big)$ where $(x_1, \dots, x_n)$ runs over $T_1 \times \cdots \times T_n$. Show that ev induces a K-algebra isomorphism $\varphi\colon P/\mathfrak{a} \xrightarrow{\sim} K^t$.

Exercise (2.45) (*Cauchy–Davenport Theorem*) . — Let $A, B \subset \mathbb{F}_p$ be nonempty subsets. Set $C := \{a + b \mid a \in A \text{ and } b \in B\}$. Say A, B, C have α, β, γ elements.

(1) Assume $C \subsetneqq \mathbb{F}_p$. Use $F(X, Y) := \prod_{c \in C}(X + Y - c)$ to show $\gamma \geq \alpha + \beta - 1$.
(2) Show $\gamma \geq \min\{\alpha + \beta - 1,\ p\}$.

Exercise (2.46) (*Chevalley–Warning Theorem*) . — Let $P := \mathbb{F}_q[X_1, \dots, X_n]$ be the polynomial ring, $F_1, \dots, F_m \in P$, and $(c_1, \dots, c_n) \in \mathbb{F}_q^n$ a common zero of the

F_j. Assume $n > \sum_{i=1}^{m} \deg(F_i)$. Set

$$G_1 := \prod_{i=1}^{m}(1 - F_i^{q-1}), \quad G_2 := \delta \prod_{j=1}^{n} \prod_{c \in \mathbb{F}_q,\, c \neq c_j} (X_j - c), \quad \text{and} \quad F := G_1 - G_2,$$

and choose δ so that $F(c_1, \ldots, c_n) = 0$.

(1) Show that $X_1^{q-1} \cdots X_n^{q-1}$ has coefficient $-\delta$ in F and $\delta \neq 0$.

(2) Use F and **(2.44)**(4) to show that the F_j have another common zero.

3. Radicals

Two radicals of a ring are commonly used in Commutative Algebra: the Jacobson radical, which is the intersection of all maximal ideals, and the nilradical, which is the set of all nilpotent elements. Closely related to the nilradical is the radical of a subset. We define these three radicals, and discuss examples. In particular, we study local rings; a local ring has only one maximal ideal, which is then its Jacobson radical. We prove two important general results: *Prime Avoidance*, which states that, if an ideal lies in a finite union of primes, then it lies in one of them, and the *Scheinnullstellensatz*, which states that the nilradical of an ideal is equal to the intersection of all the prime ideals containing it.

A. Text

Definition (3.1). — Let R be a ring. Its (Jacobson) **radical** $\operatorname{rad}(R)$ is defined to be the intersection of all its maximal ideals.

Proposition (3.2). — *Let R be a ring, $\mathfrak{a}$ an ideal, $x \in R$, and $u \in R^\times$. Then $x \in \operatorname{rad}(R)$ if and only if $u - xy \in R^\times$ for all $y \in R$. In particular, the sum of an element of $\operatorname{rad}(R)$ and a unit is a unit, and $\mathfrak{a} \subset \operatorname{rad}(R)$ if $1 - \mathfrak{a} \in R^\times$.*

Proof: Assume $x \in \operatorname{rad}(R)$. Given a maximal ideal $\mathfrak{m}$, suppose $u - xy \in \mathfrak{m}$. Since $x \in \mathfrak{m}$ too, also $u \in \mathfrak{m}$, a contradiction. Thus $u - xy$ is a unit by (**2.22**). In particular, taking $y := -1$ yields $u + x \in R^\times$.

Conversely, assume $x \notin \operatorname{rad}(R)$. Then there is a maximal ideal $\mathfrak{m}$ with $x \notin \mathfrak{m}$. So $\langle x \rangle + \mathfrak{m} = R$. Hence there exist $y \in R$ and $m \in \mathfrak{m}$ such that $xy + m = u$. Then $u - xy = m \in \mathfrak{m}$. So $u - xy$ is not a unit by (**2.22**), or directly by (**1.4**).

In particular, given $y \in R$, set $a := u^{-1}xy$. Then $u - xy = u(1 - a) \in R^\times$ if $1 - a \in R^\times$. Also $a \in \mathfrak{a}$ if $x \in \mathfrak{a}$. Thus the first assertion implies the last. $\square$

Corollary (3.3). — *Let R be a ring, $\mathfrak{a}$ an ideal, $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Assume $\mathfrak{a} \subset \operatorname{rad}(R)$. Then $\operatorname{Idem}(\kappa)$ is injective.*

Proof: Given $e, e' \in \operatorname{Idem}(R)$ with $\kappa(e) = \kappa(e')$, set $x := e - e'$. Then

$$x^3 = e^3 - 3e^2e' + 3ee'^2 - e'^3 = e - e' = x.$$

Hence $x(1 - x^2) = 0$. But $\kappa(x) = 0$; so $x \in \mathfrak{a}$. But $\mathfrak{a} \subset \operatorname{rad}(R)$. Hence $1 - x^2$ is a unit by (**3.2**). Thus $x = 0$. Thus $\operatorname{Idem}(\kappa)$ is injective. $\square$

Definition (3.4). — A ring is called **local** if it has exactly one maximal ideal, and **semilocal** if it has at least one and at most finitely many.

By the **residue field** of a local ring A, we mean the field $A/\mathfrak{m}$ where $\mathfrak{m}$ is the (unique) maximal ideal of A.

Lemma (3.5) (Nonunit Criterion)**. —** *Let A be a ring, $\mathfrak{n}$ the set of nonunits. Then A is local if and only if $\mathfrak{n}$ is an ideal; if so, then $\mathfrak{n}$ is the maximal ideal.*

Proof: Every proper ideal $\mathfrak{a}$ lies in $\mathfrak{n}$ as $\mathfrak{a}$ contains no unit. So, if $\mathfrak{n}$ is an ideal, then it is a maximal ideal, and the only one. Thus A is local.

Conversely, assume A is local with maximal ideal $\mathfrak{m}$. Then $A - \mathfrak{n} = A - \mathfrak{m}$ by (**2.22**). So $\mathfrak{n} = \mathfrak{m}$. Thus $\mathfrak{n}$ is an ideal. $\square$

Example (3.6). — The product ring $R' \times R''$ is not local by (**3.5**) if both R' and R'' are nonzero. Indeed, $(1,0)$ and $(0,1)$ are nonunits, but their sum is a unit.

Example (3.7). — Let R be a ring. A **formal power series** in the n variables $X_1, \ldots, X_n$ is a formal infinite sum of the form $\sum a_{(i)} X_1^{i_1} \cdots X_n^{i_n}$ where $a_{(i)} \in R$ and where $(i) := (i_1, \ldots, i_n)$ with each $i_j \geq 0$. The term $a_{(0)}$ where $(0) := (0, \ldots, 0)$ is called the **constant term**. Addition and multiplication are performed as for polynomials; with these operations, these series form a ring $R[[X_1, \ldots, X_n]]$.

Set $P := R[[X_1, \ldots, X_n]]$ and $\mathfrak{a} := \langle X_1, \ldots, X_n \rangle$. Then $\sum a_{(i)} X_1^{i_1} \cdots X_n^{i_n} \mapsto a_{(0)}$ is a canonical surjective ring map $P \to R$ with kernel $\mathfrak{a}$; hence, $P/\mathfrak{a} = R$.

Given an ideal $\mathfrak{m} \subset R$, set $\mathfrak{n} := \mathfrak{a} + \mathfrak{m}P$. Then (**1.9**) yields $P/\mathfrak{n} = R/\mathfrak{m}$.

A power series F is a unit if and only if its constant term $a_{(0)}$ is a unit. Indeed, if $FF' = 1$, then $a_{(0)} a'_{(0)} = 1$ where $a'_{(0)}$ is the constant term of F'. Conversely, if $a_{(0)}$ is a unit, then $F = a_{(0)}(1 - G)$ with $G \in \mathfrak{a}$. Set $F' := a_{(0)}^{-1}(1 + G + G^2 + \cdots)$; this sum makes sense as the component of degree d involves only the first $d + 1$ summands. Clearly $F \cdot F' = 1$.

Suppose R is a local ring with maximal ideal $\mathfrak{m}$. Given a power series $F \notin \mathfrak{n}$, its constant term lies outside $\mathfrak{m}$, so is a unit by (**2.22**). So F itself is a unit. Hence the nonunits constitute $\mathfrak{n}$. Thus (**3.5**) implies P *is local with maximal ideal* $\mathfrak{n}$.

Example (3.8). — Let k be a ring, and $A := k[[X]]$ the formal power series ring in one variable. A **formal Laurent series** is a formal sum of the form $\sum_{i=-m}^{\infty} a_i X^i$ with $a_i \in k$ and $m \in \mathbb{Z}$. Plainly, these series form a ring $k\{\{X\}\}$. Set $K := k\{\{X\}\}$.

Set $F := \sum_{i=-m}^{\infty} a_i X^i$. If $a_{-m} \in k^{\times}$, then $F \in K^{\times}$; indeed, $F = a_{-m} X^{-m}(1 - G)$ where $G \in A$, and $F \cdot a_{-m}^{-1} X^m (1 + G + G^2 + \cdots) = 1$.

Assume k is a field. If $F \neq 0$, then $F = X^{-m} H$ with $H := a_{-m}(1 - G) \in A^{\times}$. Let $\mathfrak{a} \subset A$ be a nonzero ideal. Suppose $F \in \mathfrak{a}$. Then $X^{-m} \in \mathfrak{a}$. Let n be the smallest integer such that $X^n \in \mathfrak{a}$. Then $-m \geq n$. Set $E := X^{-m-n} H$. Then $E \in A$ and $F = X^n E$. Hence $\mathfrak{a} = \langle X^n \rangle$. Thus A *is a* PID.

Further, K is a field. In fact, $K = \mathrm{Frac}(A)$ because any nonzero $F \in K$ is of the form $F = H/X^m$ where $H,\, X^m \in A$.

Let $A[Y]$ be the polynomial ring in one variable, and $\iota\colon A \hookrightarrow K$ the inclusion. Define $\varphi\colon A[Y] \to K$ by $\varphi|A = \iota$ and $\varphi(Y) := X^{-1}$. Then φ is surjective. Set $\mathfrak{m} := \mathrm{Ker}(\varphi)$. Then $\mathfrak{m}$ is maximal by (**2.13**) and (**1.5**). So by (**2.20**), $\mathfrak{m}$ has the form $\langle F \rangle$ with F irreducible, or the form $\langle p, G \rangle$ with $p \in A$ irreducible and $G \in A[Y]$. But $\mathfrak{m} \cap A = \langle 0 \rangle$ as ι is injective. So $\mathfrak{m} = \langle F \rangle$. But $XY - 1$ belongs to $\mathfrak{m}$, and is clearly irreducible; hence, $XY - 1 = FH$ with H a unit. Thus $\langle XY - 1 \rangle$ is maximal.

In addition, $\langle X, Y \rangle$ is maximal. Indeed, $A[Y]/\langle Y \rangle = A$ by (**1.6**)(2), and so (**3.7**) yields $A[Y]/\langle X, Y \rangle = A/\langle X \rangle = k$. However, $\langle X, Y \rangle$ is not principal, as no nonunit of $A[Y]$ divides both X and Y. Thus $A[Y]$ *has both principal and nonprincipal maximal ideals, the two types allowed by* (**2.20**).

Proposition (3.9). — *Let R be a ring, S a multiplicative subset, and $\mathfrak{a}$ an ideal with $\mathfrak{a} \cap S = \emptyset$. Set $\mathcal{S} := \{$ideals $\mathfrak{b} \mid \mathfrak{b} \supset \mathfrak{a}$ and $\mathfrak{b} \cap S = \emptyset\}$. Then $\mathcal{S}$ has a maximal element $\mathfrak{p}$, and every such $\mathfrak{p}$ is prime.*

Proof: Clearly, $\mathfrak{a} \in \mathcal{S}$, and $\mathcal{S}$ is partially ordered by inclusion. Given a totally ordered subset $\{\mathfrak{b}_\lambda\}$ of $\mathcal{S}$, set $\mathfrak{b} := \bigcup \mathfrak{b}_\lambda$. Then $\mathfrak{b}$ is an upper bound for $\{\mathfrak{b}_\lambda\}$ in $\mathcal{S}$. So by Zorn's Lemma, $\mathcal{S}$ has a maximal element $\mathfrak{p}$. Let's show $\mathfrak{p}$ is prime.

Take $x, y \in R - \mathfrak{p}$. Then $\mathfrak{p} + \langle x\rangle$ and $\mathfrak{p} + \langle y\rangle$ are strictly larger than $\mathfrak{p}$. So there are $p, q \in \mathfrak{p}$ and $a, b \in R$ with $p + ax \in S$ and $q + by \in S$. Since S is multiplicative, $pq + pby + qax + abxy \in S$. But $pq + pby + qax \in \mathfrak{p}$, so $xy \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is prime. □

Exercise (3.10) . — Let $\varphi\colon R \to R'$ be a ring map, $\mathfrak{p}$ an ideal of R. Show:

(1) there is an ideal $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ if and only if $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$.
(2) if $\mathfrak{p}$ is prime with $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$, then there's a prime $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

(3.11) (Saturated multiplicative subsets). — Let R be a ring, and S a multiplicative subset. We say S is **saturated** if, given $x, y \in R$ with $xy \in S$, necessarily $x, y \in S$.

For example, the following statements are easy to check. *The group of units $R^\times$ and the subset of nonzerodivisors S_0 are saturated multiplicative subsets. Further, let $\varphi\colon R \to R'$ be a ring map, $T \subset R'$ a subset. If T is saturated multiplicative, then so is $\varphi^{-1}T$. The converse holds if φ is surjective.*

Lemma (3.12) (Prime Avoidance). — *Let R be a ring, $\mathfrak{a}$ a subset of R that is stable under addition and multiplication, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideals such that $\mathfrak{p}_3, \ldots, \mathfrak{p}_n$ are prime. If $\mathfrak{a} \not\subset \mathfrak{p}_j$ for all j, then there is an $x \in \mathfrak{a}$ such that $x \notin \mathfrak{p}_j$ for all j; or equivalently, if $\mathfrak{a} \subset \bigcup_{i=1}^n \mathfrak{p}_i$, then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.*

Proof: Proceed by induction on n. If $n = 1$, the assertion is trivial. Assume that $n \ge 2$ and by induction that, for every i, there is an $x_i \in \mathfrak{a}$ such that $x_i \notin \mathfrak{p}_j$ for all $j \ne i$. We may assume $x_i \in \mathfrak{p}_i$ for every i, else we're done. If $n = 2$, then clearly $x_1 + x_2 \notin \mathfrak{p}_j$ for $j = 1, 2$. If $n \ge 3$, then $(x_1 \cdots x_{n-1}) + x_n \notin \mathfrak{p}_j$ for all j as, if $j = n$, then $x_n \in \mathfrak{p}_n$ and $\mathfrak{p}_n$ is prime, and if $j < n$, then $x_n \notin \mathfrak{p}_j$ and $x_j \in \mathfrak{p}_j$. □

(3.13) (Other radicals). — Let R be a ring, $\mathfrak{a}$ a subset. Its **radical** $\sqrt{\mathfrak{a}}$ is the set

$$\sqrt{\mathfrak{a}} := \{x \in R \mid x^n \in \mathfrak{a} \text{ for some } n = n(x) \ge 1\}.$$

Notice $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$ and $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$. Given a subset $\mathfrak{b} \subset \mathfrak{a}$, notice $\sqrt{\mathfrak{b}} \subset \sqrt{\mathfrak{a}}$.

If $\mathfrak{a}$ is an ideal and $\mathfrak{a} = \sqrt{\mathfrak{a}}$, then $\mathfrak{a}$ is said to be **radical**. For example, suppose $\mathfrak{a} = \bigcap \mathfrak{p}_\lambda$ with all $\mathfrak{p}_\lambda$ prime. If $x^n \in \mathfrak{a}$ for some $n \ge 1$, then $x \in \mathfrak{p}_\lambda$ for all λ. So $\sqrt{\mathfrak{a}} \subset \mathfrak{a}$. Thus $\mathfrak{a}$ is radical. This example is the only one by **(3.14)** below.

We call $\sqrt{\langle 0\rangle}$ the **nilradical**, and sometimes denote it by $\operatorname{nil}(R)$. We call an element $x \in R$ **nilpotent** if x belongs to $\sqrt{\langle 0\rangle}$, that is, if $x^n = 0$ for some $n \ge 1$. We call an ideal $\mathfrak{a}$ **nilpotent** if $\mathfrak{a}^n = 0$ for some $n \ge 1$.

Recall that every maximal ideal is prime by **(2.15)** and that $\operatorname{rad}(R)$ is defined to be the intersection of all the maximal ideals. Thus $\sqrt{\operatorname{rad}(R)} = \operatorname{rad}(R)$.

However, $\langle 0\rangle \subset \operatorname{rad}(R)$. So $\sqrt{\langle 0\rangle} \subset \sqrt{\operatorname{rad}(R)}$. Thus

$$\operatorname{nil}(R) \subset \operatorname{rad}(R) \qquad \textbf{(3.13.1)}$$

We call R **reduced** if $\operatorname{nil}(R) = \langle 0\rangle$, that is, if R has no nonzero nilpotents.

Theorem (3.14) (Scheinnullstellensatz). — *Let R be a ring, $\mathfrak{a}$ an ideal. Then*

$$\sqrt{\mathfrak{a}} = \bigcap\nolimits_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$$

where $\mathfrak{p}$ runs through all the prime ideals containing $\mathfrak{a}$. (By convention, the empty intersection is equal to R.)

Proof: Take $x \notin \sqrt{\mathfrak{a}}$. Set $S := \{1, x, x^2, \dots\}$. Then S is multiplicative, and $\mathfrak{a} \cap S = \emptyset$. By (**3.9**), there is a $\mathfrak{p} \supset \mathfrak{a}$, but $x \notin \mathfrak{p}$. So $x \notin \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. Thus $\sqrt{\mathfrak{a}} \supset \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$.

Conversely, take $x \in \sqrt{\mathfrak{a}}$. Say $x^n \in \mathfrak{a} \subset \mathfrak{p}$. Then $x \in \mathfrak{p}$. Thus $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. □

Proposition (3.15). — *Let R be a ring, $\mathfrak{a}$ an ideal. Then $\sqrt{\mathfrak{a}}$ is an ideal.*

Proof: Take $x, y \in \sqrt{\mathfrak{a}}$; say $x^n \in \mathfrak{a}$ and $y^m \in \mathfrak{a}$. Then

$$(x+y)^{n+m-1} = \sum_{i+j=m+n-1} \binom{n+m-1}{j} x^i y^j. \qquad \textbf{(3.15.1)}$$

This sum belongs to $\mathfrak{a}$ as, in each summand, either x^i or y^j does, since, if $i \le n-1$ and $j \le m-1$, then $i+j \le m+n-2$. Thus $x+y \in \sqrt{\mathfrak{a}}$. So clearly $\sqrt{\mathfrak{a}}$ is an ideal.

Alternatively, given any collection of ideals $\mathfrak{a}_\lambda$, note that $\bigcap \mathfrak{a}_\lambda$ is also an ideal. So $\sqrt{\mathfrak{a}}$ is an ideal owing to (**3.14**). □

Exercise (3.16) . — Use Zorn's lemma to prove that any prime ideal $\mathfrak{p}$ contains a prime ideal $\mathfrak{q}$ that is minimal containing any given subset $\mathfrak{s} \subset \mathfrak{p}$.

(3.17) (Minimal primes). — Let R be a ring, $\mathfrak{a}$ an ideal, $\mathfrak{p}$ a prime. We call $\mathfrak{p}$ a **minimal prime** of $\mathfrak{a}$, or over $\mathfrak{a}$, if $\mathfrak{p}$ is minimal in the set of primes containing $\mathfrak{a}$. We call $\mathfrak{p}$ a **minimal prime** of R if $\mathfrak{p}$ is a minimal prime of $\langle 0 \rangle$.

Owing to (**3.16**), every prime of R containing $\mathfrak{a}$ contains a minimal prime of $\mathfrak{a}$. So owing to the Scheinnullstellensatz (**3.14**), the radical $\sqrt{\mathfrak{a}}$ is the intersection of all the minimal primes of $\mathfrak{a}$. In particular, every prime of R contains a minimal prime of R, and $\operatorname{nil}(R)$ is the intersection of all the minimal primes of R.

Proposition (3.18). — *A ring R is reduced and has only one minimal prime if and only if R is a domain.*

Proof: Suppose R is reduced, or $\langle 0 \rangle = \sqrt{\langle 0 \rangle}$, and has only one minimal prime $\mathfrak{q}$. Then (**3.17**) implies $\langle 0 \rangle = \mathfrak{q}$. Thus R is a domain. The converse is obvious. □

Exercise (3.19) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $R[[X]]$ the formal power series ring, $\mathfrak{M} \subset R[[X]]$ an ideal, $F := \sum a_n X^n \in R[[X]]$. Set $\mathfrak{m} := \mathfrak{M} \cap R$ and $\mathfrak{A} := \left\{ \sum b_n X^n \mid b_n \in \mathfrak{a} \right\}$. Prove the following statements:

(1) If F is nilpotent, then a_n is nilpotent for all n. The converse is false.
(2) Then $F \in \operatorname{rad}(R[[X]])$ if and only if $a_0 \in \operatorname{rad}(R)$.
(3) Assume $X \in \mathfrak{M}$. Then X and $\mathfrak{m}$ generate $\mathfrak{M}$.
(4) Assume $\mathfrak{M}$ is maximal. Then $X \in \mathfrak{M}$ and $\mathfrak{m}$ is maximal.
(5) If $\mathfrak{a}$ is finitely generated, then $\mathfrak{a}R[[X]] = \mathfrak{A}$. However, there's an example of an R with a prime ideal $\mathfrak{a}$ such that $\mathfrak{a}R[[X]] \ne \mathfrak{A}$.

Example (3.20). — Let R be a ring, $R[[X]]$ the formal power series ring. Then every prime $\mathfrak{p}$ of R is the contraction of a prime of $R[[X]]$. Indeed, $\mathfrak{p}R[[X]] \cap R = \mathfrak{p}$. So by (**3.10**)(2), there's a prime $\mathfrak{q}$ of $R[[X]]$ with $\mathfrak{q} \cap R = \mathfrak{p}$. In fact, a specific choice for $\mathfrak{q}$ is the set of series $\sum a_n X^n$ with $a_n \in \mathfrak{p}$. Indeed, the canonical map $R \to R/\mathfrak{p}$ induces a surjection $R[[X]] \to (R/\mathfrak{p})[[X]]$ with kernel $\mathfrak{q}$; so $R[[X]]/\mathfrak{q} = (R/\mathfrak{p})[[X]]$. Plainly $(R/\mathfrak{p})[[X]]$ is a domain. But (**3.19**)(5) shows $\mathfrak{q}$ may not be equal to $\mathfrak{p}R[[X]]$.

B. Exercises

Exercise (3.21) . — Let R be a ring, $\mathfrak{a} \subset \operatorname{rad}(R)$ an ideal, $w \in R$, and $w' \in R/\mathfrak{a}$ its residue. Prove that $w \in R^\times$ if and only if $w' \in (R/\mathfrak{a})^\times$. What if $\mathfrak{a} \not\subset \operatorname{rad}(R)$?

Exercise (3.22) . — Let A be a local ring, e an idempotent. Show $e = 1$ or $e = 0$.

Exercise (3.23) . — Let A be a ring, $\mathfrak{m}$ a maximal ideal such that $1 + m$ is a unit for every $m \in \mathfrak{m}$. Prove A is local. Is this assertion still true if $\mathfrak{m}$ is not maximal?

Exercise (3.24) . — Let R be a ring, S a subset. Show that S is saturated multiplicative if and only if $R - S$ is a union of primes.

Exercise (3.25) . — Let R be a ring, and S a multiplicative subset. Define its **saturation** to be the subset

$$\overline{S} := \{\, x \in R \mid \text{there is } y \in R \text{ with } xy \in S \,\}.$$

(1) Show (a) that $\overline{S} \supset S$, and (b) that $\overline{S}$ is saturated multiplicative, and (c) that any saturated multiplicative subset T containing S also contains $\overline{S}$.

(2) Set $U := \bigcup_{\mathfrak{p} \cap S = \emptyset} \mathfrak{p}$. Show that $R - \overline{S} = U$.

(3) Let $\mathfrak{a}$ be an ideal; assume $S = 1 + \mathfrak{a}$; set $W := \bigcup_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$. Show $R - \overline{S} = W$.

(4) Given $f, g \in R$, show that $\overline{S_f} \subset \overline{S_g}$ if and only if $\sqrt{\langle f \rangle} \supset \sqrt{\langle g \rangle}$.

Exercise (3.26) . — Let R be a nonzero ring, S a subset. Show S is maximal in the set $\mathfrak{S}$ of multiplicative subsets T of R with $0 \notin T$ if and only if $R - S$ is a minimal prime of R.

Exercise (3.27) . — Let k be a field, X_λ for $\lambda \in \Lambda$ variables, and Λ_π for $\pi \in \Pi$ disjoint subsets of Λ. Set $P := k[\{X_\lambda\}_{\lambda \in \Lambda}]$ and $\mathfrak{p}_\pi := \langle \{X_\lambda\}_{\lambda \in \Lambda_\pi} \rangle$ for all $\pi \in \Pi$. Let $F, G \in P$ be nonzero, and $\mathfrak{a} \subset P$ a nonzero ideal. Set $U := \bigcup_{\pi \in \Pi} \mathfrak{p}_\pi$. Show:

(1) Assume $F \in \mathfrak{p}_\pi$ for some $\pi \in \Pi$, Then every monomial of F is in $\mathfrak{p}_\pi$.

(2) Assume there are $\pi, \rho \in \Pi$ such that $F + G \in \mathfrak{p}_\pi$ and $G \in \mathfrak{p}_\rho$ but $\mathfrak{p}_\rho$ contains no monomial of F. Then $\mathfrak{p}_\pi$ contains every monomial of F and of G.

(3) Assume $\mathfrak{a} \subset U$. Then $\mathfrak{a} \subset \mathfrak{p}_\pi$ for some $\pi \in \Pi$.

Exercise (3.28) . — Let k be a field, $\mathcal{S} \subset k$ a subset of cardinality d at least 2.

(1) Let $P := k[X_1, \ldots, X_n]$ be the polynomial ring, $F \in P$ nonzero. Assume the highest power of any X_i in F is less than d. Proceeding by induction on n, show that there are $a_1, \ldots, a_n \in \mathcal{S}$ with $F(a_1, \ldots, a_n) \neq 0$.

(2) Let V be a k-vector space, and $W_1, \ldots, W_r$ proper subspaces. Assume $r < d$. Show $\bigcup_i W_i \neq V$.

(3) In (2), let $W \subset \bigcup_i W_i$ be a subspace. Show $W \subset W_i$ for some i.

(4) Let R a k-algebra, $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ideals with $\mathfrak{a} \subset \bigcup_i \mathfrak{a}_i$. Show $\mathfrak{a} \subset \mathfrak{a}_i$ for some i.

Exercise (3.29) . — Let k be a field, $R := k[X, Y]$ the polynomial ring in two variables, $\mathfrak{m} := \langle X, Y \rangle$. Show $\mathfrak{m}$ is a union of strictly smaller primes.

Exercise (3.30) . — Find the nilpotents in $\mathbb{Z}/\langle n \rangle$. In particular, take $n = 12$.

Exercise (3.31) (*Nakayama's Lemma for nilpotent ideals*) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Assume $\mathfrak{a}M = M$ and $\mathfrak{a}$ is nilpotent. Show $M = 0$.

Exercise (3.32) . — Let R be a ring; $\mathfrak{a}$, $\mathfrak{b}$ ideals; $\mathfrak{p}$ a prime. Prove the following:

(1) $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. (2) $\sqrt{\mathfrak{a}} = R$ if and only if $\mathfrak{a} = R$.
(3) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$. (4) $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n > 0$.

Exercise (3.33) . — Let R be a ring. Prove these statements: (1) Assume every ideal not contained in $\operatorname{nil}(R)$ contains a nonzero idempotent. Then $\operatorname{nil}(R) = \operatorname{rad}(R)$.
(2) Assume R is Boolean. Then $\operatorname{nil}(R) = \operatorname{rad}(R) = \langle 0 \rangle$.

Exercise (3.34) . — Let $e, e' \in \operatorname{Idem}(R)$. Assume $\sqrt{\langle e \rangle} = \sqrt{\langle e' \rangle}$. Show $e = e'$.

Exercise (3.35) . — Let R be a ring, $\mathfrak{a}_1$, $\mathfrak{a}_2$ comaximal ideals with $\mathfrak{a}_1\mathfrak{a}_2 \subset \operatorname{nil}(R)$. Show there are complementary idempotents e_1 and e_2 with $e_i \in \mathfrak{a}_i$.

Exercise (3.36) . — Let R be a ring, $\mathfrak{a}$ an ideal, $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Assume $\mathfrak{a} \subset \operatorname{nil}(R)$. Show $\operatorname{Idem}(\kappa)$ is bijective.

Exercise (3.37) . — Let R be a ring. Prove the following statements equivalent:
(1) R has exactly one prime $\mathfrak{p}$;
(2) every element of R is either nilpotent or a unit;
(3) $R/\operatorname{nil}(R)$ is a field.

Exercise (3.38) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Assume that $\mathfrak{b}$ is finitely generated modulo $\mathfrak{a}$ and that $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$. Show there's $n \geq 1$ with $\mathfrak{b}^n \subset \mathfrak{a}$.

Exercise (3.39) . — Let $\varphi\colon R \to R'$ be a ring map, $\mathfrak{a} \subset R$ and $\mathfrak{b} \subset R'$ subsets. Prove these two relations: (1) $(\varphi\sqrt{\mathfrak{a}})R' \subset \sqrt{(\varphi\mathfrak{a})R'}$ and (2) $\varphi^{-1}\sqrt{\mathfrak{b}} = \sqrt{\varphi^{-1}\mathfrak{b}}$.

Exercise (3.40) . — Let R be a ring, $\mathfrak{q}$ an ideal, $\mathfrak{p}$ a prime. Assume $\mathfrak{p}$ is finitely generated modulo $\mathfrak{q}$. Show $\mathfrak{p} = \sqrt{\mathfrak{q}}$ if and only if there's $n \geq 1$ with $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$.

Exercise (3.41) . — Let R be a ring. Assume R is reduced and has finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Prove $\varphi\colon R \to \prod(R/\mathfrak{p}_i)$ is injective, and for each i, there is some $(x_1, \ldots, x_n) \in \operatorname{Im}(\varphi)$ with $x_i \neq 0$ but $x_j = 0$ for $j \neq i$.

Exercise (3.42) . — Let R be a ring, X a variable, $F := a_0 + a_1X + \cdots + a_nX^n$.
(1) Prove F is nilpotent if and only if $a_0, \ldots, a_n$ are nilpotent.
(2) Prove F is a unit if and only if a_0 is a unit and $a_1, \ldots, a_n$ are nilpotent.

Exercise (3.43) . — Generalize (3.42) to the polynomial ring $P := R[X_1, \ldots, X_r]$.

Exercise (3.44) . — Let R be a ring, R' an algebra, X a variable. Show:

(1) $\operatorname{nil}(R)R' \subset \operatorname{nil}(R')$ and (2) $\operatorname{rad}(R[X]) = \operatorname{nil}(R[X]) = \operatorname{nil}(R)R[X]$.

4. Modules

In Commutative Algebra, it has proven advantageous to expand the study of rings to include modules. Thus we obtain a richer theory, which is more flexible and more useful. We begin the expansion here by discussing residue modules, kernels, and images. In particular, we identify the UMP of the residue module, and use it to construct the Noether isomorphisms. We also construct free modules, direct sums, and direct products, and we describe their UMPs.

A. Text

(4.1) (Modules). — Let R be a ring. Recall that an **R-module** M is an abelian group, written additively, with a **scalar multiplication**, $R \times M \to M$, written $(x, m) \mapsto xm$, which is

(1) **distributive**, $x(m+n) = xm + xn$ and $(x+y)m = xm + ym$,
(2) **associative**, $x(ym) = (xy)m$, and
(3) **unitary**, $1 \cdot m = m$.

For example, if R is a field, then an R-module is a vector space. Moreover, a $\mathbb{Z}$-module is just an abelian group; multiplication is repeated addition.

As in **(1.1)**, for any $x \in R$ and $m \in M$, we have $x \cdot 0 = 0$ and $0 \cdot m = 0$.

A **submodule** N of M is a subgroup that is **closed under** multiplication; that is, $xn \in N$ for all $x \in R$ and $n \in N$. For example, the ring R is itself an R-module, and the submodules are just the ideals. Given an ideal $\mathfrak{a}$, let $\mathfrak{a}N$ denote the smallest submodule containing all products an with $a \in \mathfrak{a}$ and $n \in N$. Similar to **(1.4)**, clearly $\mathfrak{a}N$ is equal to the set of finite sums $\sum a_i n_i$ with $a_i \in \mathfrak{a}$ and $n_i \in N$.

Given $m \in M$, define its annihilator, denoted $\operatorname{Ann}(m)$ or $\operatorname{Ann}_R(m)$, by

$$\operatorname{Ann}(m) := \{x \in R \mid xm = 0\}.$$

Furthermore, define the **annihilator** of M, denoted $\operatorname{Ann}(M)$ or $\operatorname{Ann}_R(M)$, by

$$\operatorname{Ann}(M) := \{x \in R \mid xm = 0 \text{ for all } m \in M\}.$$

Plainly, $\operatorname{Ann}(m)$ and $\operatorname{Ann}(M)$ are ideals.

We call the intersection of all maximal ideals containing $\operatorname{Ann}(M)$ the **radical** of M, and denote it by $\operatorname{rad}(M)$ or $\operatorname{rad}_R(M)$. Note that, owing to **(1.9)**, reduction sets up a bijective correspondence between the maximal ideals containing $\operatorname{Ann}(M)$ and the maximal ideals of $R/\operatorname{Ann}(M)$; hence,

$$\operatorname{rad}(R/\operatorname{Ann}(M)) = \operatorname{rad}(M)/\operatorname{Ann}(M). \qquad \textbf{(4.1.1)}$$

If R is local with maximal ideal $\mathfrak{m}$ and if $M \neq 0$, notice $\mathfrak{m} = \operatorname{rad}(M)$.

Given a submodule N of M, note $\operatorname{Ann}(M) \subset \operatorname{Ann}(N)$. Thus $\operatorname{rad}(M) \subset \operatorname{rad}(N)$. Similarly, $\operatorname{Ann}(M) \subset \operatorname{Ann}(M/N)$. Thus $\operatorname{rad}(M) \subset \operatorname{rad}(M/N)$.

We call M **semilocal** if there are only finitely many maximal ideals containing $\operatorname{Ann}(M)$. Trivially, if R is semilocal, then so is M. Moreover, owing to the bijective correspondence between maximal ideals noted above, *M is semilocal if and only if $R/\operatorname{Ann}(M)$ is a semilocal ring.*

Given a set $\mathcal{X} := \{X_\lambda\}_{\lambda \in \Lambda}$ of variables, form the set of "polynomials":

$$M[\mathcal{X}] := \left\{ \textstyle\sum_{i=0}^{n} m_i \mathbf{M}_i \mid m_i \in M \text{ and the } \mathbf{M}_i \text{ monomials in the } X_\lambda \right\}$$

Canonically, $M[\mathfrak{X}]$ is an $R[\mathfrak{X}]$-module.

(4.2) (Homomorphisms). — Let R be a ring, M and N modules. Recall that a **homomorphism**, or R**-linear map**, or simply R**-map**, is a map $\alpha\colon M \to N$ with

$$\alpha(xm + yn) = x(\alpha m) + y(\alpha n).$$

Associated to a homomorphism $\alpha\colon M \to N$ are its **kernel** and its **image**

$$\mathrm{Ker}(\alpha) := \alpha^{-1}(0) \subset M \quad \text{and} \quad \mathrm{Im}(\alpha) := \alpha(M) \subset N.$$

They are defined as subsets, but are obviously submodules.

Let $\iota\colon \mathrm{Ker}(\alpha) \to M$ be the inclusion. Then $\mathrm{Ker}(\alpha)$ has this UMP: $\alpha\iota = 0$, and given a homomorphism $\beta\colon K \to M$ with $\alpha\beta = 0$, there is a unique homomorphism $\gamma\colon K \to \mathrm{Ker}(\alpha)$ with $\iota\gamma = \beta$ as shown below

$$\begin{tikzcd}
\mathrm{Ker}(\alpha) \arrow[r, "\iota"] & M \arrow[r, "\alpha"] & N \\
 & K \arrow[ul, "\gamma"] \arrow[u, "\beta"] \arrow[ur, "0"'] &
\end{tikzcd}$$

A homomorphism α is called an **isomorphism** if it is bijective. If so, then we write $\alpha\colon M \xrightarrow{\sim} N$. Then the set-theoretic inverse $\alpha^{-1}\colon N \to M$ is a homomorphism too. So α *is an isomorphism if and only if there is a set map* $\beta\colon N \to M$ *such that* $\beta\alpha = 1_M$ *and* $\alpha\beta = 1_N$, where 1_M and 1_N are the identity maps, *and then* $\beta = \alpha^{-1}$. If there is an unnamed isomorphism between M and N, then we write $M = N$ when it is **canonical** (that is, it does not depend on any artificial choices), and we write $M \simeq N$ otherwise.

The set of homomorphisms α is denoted by $\mathrm{Hom}_R(M, N)$ or simply $\mathrm{Hom}(M, N)$. It is an R-module with addition and scalar multiplication defined by

$$(\alpha + \beta)m := \alpha m + \beta m \quad \text{and} \quad (x\alpha)m := x(\alpha m) = \alpha(xm).$$

Homomorphisms $\alpha\colon L \to M$ and $\beta\colon N \to P$ induce, via composition, a map

$$\mathrm{Hom}(\alpha, \beta)\colon\ \mathrm{Hom}(M, N) \to \mathrm{Hom}(L, P),$$

which is obviously a homomorphism. When α is the identity map 1_M, we write $\mathrm{Hom}(M, \beta)$ for $\mathrm{Hom}(1_M, \beta)$; similarly, we write $\mathrm{Hom}(\alpha, N)$ for $\mathrm{Hom}(\alpha, 1_N)$.

Exercise (4.3) . — Let R be a ring, M a module. Consider the set map

$$\rho\colon\ \mathrm{Hom}(R, M) \to M \quad \text{defined by} \quad \rho(\theta) := \theta(1).$$

Show that ρ is an isomorphism, and describe its inverse.

(4.4) (Endomorphisms). — Let R be a ring, M a module. An **endomorphism** of M is a homomorphism $\alpha\colon M \to M$. The module of endomorphisms $\mathrm{Hom}(M, M)$ is also denoted $\mathrm{End}_R(M)$. It is a ring, usually noncommutative, with multiplication given by composition. Further, $\mathrm{End}_R(M)$ is a subring of $\mathrm{End}_{\mathbb{Z}}(M)$.

Given $x \in R$, let $\mu_x\colon M \to M$ denote the map of *multiplication by* x, defined by $\mu_x(m) := xm$. It is an endomorphism. Further, $x \mapsto \mu_x$ is a ring map

$$\mu_R\colon R \to \mathrm{End}_R(M) \subset \mathrm{End}_{\mathbb{Z}}(M).$$

(Thus we may view μ_R as representing R as a ring of operators on the abelian group M.) Note that $\mathrm{Ker}(\mu_R) = \mathrm{Ann}(M)$.

Conversely, given an abelian group N and a ring map

$$\nu\colon R \to \mathrm{End}_{\mathbb{Z}}(N),$$

we obtain a module structure on N by setting $xn := (\nu x)(n)$. Then $\mu_R = \nu$.

We call M **faithful** if $\mu_R\colon R \to \mathrm{End}_R(M)$ is injective, or $\mathrm{Ann}(M) = 0$. For example, R is a faithful R-module, as $x \cdot 1 = 0$ implies $x = 0$.

(4.5) (Algebras). — Fix two rings R and R'.

Suppose R' is an R-algebra with structure map φ. Let M' be an R'-module. Then M' is also an R-module by **restriction of scalars**: $xm := \varphi(x)m$. In other words, the R-module structure on M' corresponds to the composition

$$R \xrightarrow{\varphi} R' \xrightarrow{\mu_{R'}} \mathrm{End}_{\mathbb{Z}}(M').$$

In particular, R' is an R'-module, so R' *is an R-module; further,*

$$(xy)z = x(yz) \quad \textit{for all } x \in R \textit{ and } y, z \in R'. \tag{4.5.1}$$

Indeed, R' is an R'-module, so an R-module by restriction of scalars; further, $(xy)z = x(yz)$ since $(\varphi(x)y)z = \varphi(x)(yz)$ by associativity in R'.

Conversely, suppose R' is an R-module satisfying **(4.5.1)**. Then R' has an R-algebra structure that is compatible with the given R-module structure. Indeed, define $\varphi\colon R \to R'$ by $\varphi(x) := x \cdot 1$. Then $\varphi(x)z = xz$ as $(x \cdot 1)z = x(1 \cdot z)$. So the composition $\mu_{R'}\varphi\colon R \to R' \to \mathrm{End}_{\mathbb{Z}}(R')$ is equal to μ_R. Hence φ is a ring map, because μ_R is one and $\mu_{R'}$ is injective by **(4.4)**. Thus R' is an R-algebra, and restriction of scalars recovers its given R-module structure.

Suppose that $R' = R/\mathfrak{a}$ for some ideal $\mathfrak{a}$. Then an R-module M has a compatible R'-module structure if and only if $\mathfrak{a}M = 0$; if so, then the R'-structure is unique. Indeed, the ring map $\mu_R\colon R \to \mathrm{End}_{\mathbb{Z}}(M)$ factors through R' if and only if $\mu_R(\mathfrak{a}) = 0$ by **(1.5)**, so if and only if $\mathfrak{a}M = 0$; as $\mathrm{End}_{\mathbb{Z}}(M)$ may be noncommutative, we must apply **(1.5)** to $\mu_R(R)$, which is commutative.

For a second example, suppose R' is the polynomial ring in one variable $R[X]$. Fix an R-module M. Then to give a compatible $R[X]$-module structure is the same as to give an endomorphism $\chi\colon M \to M$, because to give a factorization $\mu_R\colon R \to R[X] \to \mathrm{End}_R(M)$ is the same as to give an $\chi \in \mathrm{End}_R(M)$.

Again suppose R' is an arbitrary R-algebra with structure map φ. A **subalgebra** R'' of R' is a subring such that φ maps into R''. The subalgebra **generated** by $x_\lambda \in R'$ for $\lambda \in \Lambda$ is the smallest R-subalgebra that contains all x_λ. We denote it by $R[\{x_\lambda\}]$, or simply by $R[x_1, \dots, x_n]$ if $\Lambda = \{1, \dots, n\}$, and call the x_λ algebra **generators**. This subalgebra plainly contains all polynomial combinations of the x_λ with coefficients in R. In fact, the set R'' of these polynomial combinations is itself, plainly, an R-subalgebra; hence, $R'' = R[\{x_\lambda\}]$.

We say R' is a **finitely generated R-algebra** or is **algebra finite over** R if there exist $x_1, \dots, x_n \in R'$ such that $R' = R[x_1, \dots, x_n]$.

(4.6) (Residue modules). — Let R be a ring, M a module, $M' \subset M$ a submodule. Form the set of cosets, or set of residues,

$$M/M' := \{m + M' \mid m \in M\}.$$

Recall that M/M' inherits a module structure, and is called the **residue module**, or **quotient**, of M **modulo** M'. Form the **quotient map**

$$\kappa\colon M \to M/M' \quad \text{by} \quad \kappa(m) := m + M'.$$

Clearly κ is surjective, κ is linear, and κ has kernel M'.

Let $\alpha\colon M \to N$ be linear. Note that $\mathrm{Ker}(\alpha) \supset M'$ *if and only if* $\alpha(M') = 0$.

Recall that, *if* $\mathrm{Ker}(\alpha) \supset M'$*, then there exists a homomorphism* $\beta\colon M/M' \to N$ such that $\beta\kappa = \alpha$; that is, the following diagram is commutative:

$$\begin{tikzcd} M \arrow[r, "\kappa"] \arrow[dr, "\alpha"'] & M/M' \arrow[d, "\beta"'] \\ & N \end{tikzcd}$$

Conversely, *if* β *exists, then* $\mathrm{Ker}(\alpha) \supset M'$*, or* $\alpha(M') = 0$*, as* $\kappa(M') = 0$.

Further, *if* β *exists, then* β *is unique* as κ is surjective.

Thus, as κ is surjective, *if* β *exists, then* β *is surjective if and only if* α *is so. In addition, then* β *is injective if and only if* $M' = \mathrm{Ker}(\alpha)$*. Therefore,* β *is an isomorphism if and only if* α *is surjective and* $M' = \mathrm{Ker}(\alpha)$*. In particular, always*

$$M/\mathrm{Ker}(\alpha) \xrightarrow{\sim} \mathrm{Im}(\alpha). \tag{4.6.1}$$

In practice, it is usually more productive to view M/M' not as a set of cosets, but simply another module M'' that comes equipped with a surjective homomorphism $\alpha\colon M \to M''$ whose kernel is the given submodule M'.

Finally, as we have seen, M/M' has the following UMP: $\kappa(M') = 0$, *and given* $\alpha\colon M \to N$ *such that* $\alpha(M') = 0$*, there is a unique homomorphism* $\beta\colon M/M' \to N$ *such that* $\beta\kappa = \alpha$. Formally, the UMP determines M/M' up to unique isomorphism.

(4.7) (Cyclic modules). — Let R be a ring. A module M is said to be **cyclic** if there exists $m \in M$ such that $M = Rm$. If so, form $\alpha\colon R \to M$ by $x \mapsto xm$; then α induces an isomorphism $R/\mathrm{Ann}(m) \xrightarrow{\sim} M$ as $\mathrm{Ker}(\alpha) = \mathrm{Ann}(m)$; see (**4.6.1**). Note that $\mathrm{Ann}(m) = \mathrm{Ann}(M)$. Conversely, given any ideal $\mathfrak{a}$, the R-module $R/\mathfrak{a}$ is cyclic, generated by the coset of 1, and $\mathrm{Ann}(R/\mathfrak{a}) = \mathfrak{a}$.

(4.8) (Noether Isomorphisms). — Let R be a ring, N a module, and L and M submodules.

First, assume $L \subset M$. Form the following composition of quotient maps:

$$\alpha\colon N \to N/L \to (N/L)\big/(M/L).$$

Clearly α is surjective, and $\mathrm{Ker}(\alpha) = M$. Hence owing to (**4.6**), α *factors through the isomorphism* β in this commutative diagram:

$$\begin{tikzcd} N \arrow[r] \arrow[d] & N/M \arrow[d, "\beta"', "\simeq"] \\ N/L \arrow[r] & (N/L)\big/(M/L) \end{tikzcd} \tag{4.8.1}$$

Second, no longer assuming $L \subset M$, set

$$L + M := \{\, \ell + m \mid \ell \in L,\ m \in M \,\} \subset N.$$

Plainly $L + M$ is a submodule. It is called the **sum** of L and M.

Form the composition α' of the inclusion map $L \to L + M$ and the quotient map $L + M \to (L + M)/M$. Clearly α' is surjective and $\mathrm{Ker}(\alpha') = L \cap M$. Hence owing to (**4.6**), α' *factors through the isomorphism* β' in this commutative diagram:

$$\begin{tikzcd} L \arrow[r] \arrow[d] & L/(L \cap M) \arrow[d, "\beta'"', "\simeq"] \\ L + M \arrow[r] & (L + M)/M \end{tikzcd} \tag{4.8.2}$$

The isomorphisms of (**4.6.1**) and (**4.8.1**) and (**4.8.2**) are called **Noether's First, Second, and Third Isomorphisms.**

(4.9) (Cokernels, coimages). — Let R be a ring, $\alpha\colon M \to N$ a linear map. Associated to α are its **cokernel** and its **coimage**,

$$\operatorname{Coker}(\alpha) := N/\operatorname{Im}(\alpha) \quad \text{and} \quad \operatorname{Coim}(\alpha) := M/\operatorname{Ker}(\alpha);$$

they are quotient modules, and their quotient maps are both denoted by κ.

Note (**4.6**) yields the UMP of the cokernel: $\kappa\alpha = 0$, *and given a map* $\beta\colon N \to P$ *with* $\beta\alpha = 0$, *there is a unique map* $\gamma\colon \operatorname{Coker}(\alpha) \to P$ *with* $\gamma\kappa = \beta$ as shown below

$$\begin{tikzcd} M \arrow[r, "\alpha"] \arrow[dr, "0"'] & N \arrow[r, "\kappa"] \arrow[d, "\beta"] & \operatorname{Coker}(\alpha) \arrow[dl, "\gamma"] \\ & P & \end{tikzcd}$$

Further, (**4.6.1**) becomes $\operatorname{Coim}(\alpha) \xrightarrow{\sim} \operatorname{Im}(\alpha)$. Moreover, $\operatorname{Im}(\alpha) = \operatorname{Ker}(\kappa)$.

(4.10) (Generators, free modules). — Let R be a ring, M a module. Given a subset $N \subset M$, by the submodule $\langle N\rangle$ that N **generates**, we mean the smallest submodule containing N.

Given elements $m_\lambda \in M$ for $\lambda \in \Lambda$, by the submodule they **generate**, we mean the submodule generated by the set $\{\mathfrak{m}_\lambda\}$. If $\Lambda = \emptyset$, then this submodule consists just of 0. If $\Lambda = \{1, \ldots, n\}$, then the submodule is usually denoted by $\langle m_1, \ldots, m_n\rangle$.

Any submodule containing all the m_λ contains any (finite) **linear combination** $\sum x_\lambda m_\lambda$ with $x_\lambda \in R$ and almost all 0. Form the set N, or $\sum Rm_\lambda$, of all such linear combinations. Plainly, N is a submodule containing all m_λ, so is the submodule they generate.

Given a submodule N and elements $m_\lambda \in N$ that generate N, we refer to the m_λ as **generators** of N.

Given a number of submodules N_λ, by their **sum** $\sum N_\lambda$, we mean the set of all finite linear combinations $\sum x_\lambda m_\lambda$ with $x_\lambda \in R$ and $m_\lambda \in N_\lambda$. Plainly, $\sum N_\lambda$ is equal to the submodule the N_λ **generate**, namely, the smallest submodule that contains all N_λ.

By the intersection $\bigcap N_\lambda$, we mean the intersection as sets. It is, plainly, a submodule.

Elements $m_\lambda \in M$ are said to be **free** or **linearly independent** if, whenever $\sum x_\lambda m_\lambda = 0$, also $x_\lambda = 0$ for all λ. The m_λ are said to form a **(free) basis** of M if they are free and generate M; if so, then we say M is **free** on the m_λ.

We say M is **finitely generated** if it has a finite set of generators.

We say M is **free** if it has a free basis. If so, then by either (**5.32**)(2) or (**10.5**) below, any two free bases have the same number ℓ of elements, and we say M is **free of rank** ℓ, and we set $\operatorname{rank}(M) := \ell$.

For example, form the set of **restricted vectors**

$$R^{\oplus\Lambda} := \{(x_\lambda) \mid x_\lambda \in R \text{ with } x_\lambda = 0 \text{ for almost all } \lambda\}.$$

It is a module under componentwise addition and scalar multiplication. It has a **standard basis**, which consists of the vectors e_μ whose λth component is the value of the **Kronecker delta function**; that is,

$$e_\mu := (\delta_{\mu\lambda}) \quad \text{where} \quad \delta_{\mu\lambda} := \begin{cases} 1, & \text{if } \lambda = \mu; \\ 0, & \text{if } \lambda \neq \mu. \end{cases}$$

Clearly the standard basis is free. If Λ has a finite number ℓ of elements, then $R^{\oplus\Lambda}$ is often written R^ℓ and called the *direct sum of ℓ copies of R.*

For instance, $\mathbb{Z}^{\oplus\Lambda}$ is just the free Abelian group on Λ.

The free module $R^{\oplus\Lambda}$ has the following UMP: *given a module M and elements $m_\lambda \in M$ for $\lambda \in \Lambda$, there is a unique R-map*

$$\alpha\colon R^{\oplus\Lambda} \to M \text{ with } \alpha(e_\lambda) = m_\lambda \text{ for each } \lambda \in \Lambda;$$

namely, $\alpha\big((x_\lambda)\big) = \alpha\big(\sum x_\lambda e_\lambda\big) = \sum x_\lambda m_\lambda$. Note the following obvious statements:

(1) *α is surjective if and only if the m_λ generate M.*
(2) *α is injective if and only if the m_λ are linearly independent.*
(3) *α is an isomorphism if and only if the m_λ form a free basis.*

Thus *M is free of rank ℓ if and only if $M \simeq R^\ell$.*

Example (4.11). — Take $R := \mathbb{Z}$ and $M := \mathbb{Q}$. Then any two x, y in M are not free; indeed, if $x = a/b$ and $y = -c/d$, then $bcx + ady = 0$. So M is not free.

Also M is not finitely generated. Indeed, given any $m_1/n_1, \ldots, m_r/n_r \in M$, let d be a common multiple of $n_1, \ldots, n_r$. Then $(1/d)\mathbb{Z}$ contains every linear combination $x_1(m_1/n_1) + \cdots + x_\ell(m_\ell/n_\ell)$, but $(1/d)\mathbb{Z} \neq M$.

Moreover, $\mathbb{Q}$ is not algebra finite over $\mathbb{Z}$. Indeed, let $p \in \mathbb{Z}$ be any prime not dividing $n_1 \cdots n_r$. Then $1/p \notin \mathbb{Z}[m_1/n_1, \ldots, m_r/n_r]$.

Theorem (4.12). — *Let R be a* PID*, E a free module, $\{e_\lambda\}_{\lambda\in\Lambda}$ a (free) basis, and F a submodule. Then F is free, and has a basis indexed by a subset of Λ.*

Proof: Well order Λ. For all λ, let $\pi_\lambda\colon E \to R$ be the λth projection. For all μ, set $E_\mu := \bigoplus_{\lambda\le\mu} Re_\lambda$ and $F_\mu := F \cap E_\mu$. Then $\pi_\mu(F_\mu) = \langle a_\mu\rangle$ for some $a_\mu \in R$ as R is a PID. Choose $f_\mu \in F_\mu$ with $\pi_\mu(f_\mu) = a_\mu$. Set $\Lambda_0 := \{\mu \in \Lambda \mid a_\mu \neq 0\}$.

Say $\sum_{\mu\in\Lambda_0} c_\mu f_\mu = 0$ for some $c_\mu \in R$. Set $\Lambda_1 := \{\mu \in \Lambda_0 \mid c_\mu \neq 0\}$. Suppose $\Lambda_1 \neq \emptyset$. Note Λ_1 is finite. Let μ_1 be the greatest element of Λ_1. Then $\pi_{\mu_1}(f_\mu) = 0$ for $\mu < \mu_1$ as $f_\mu \in E_\mu$. So $\pi_{\mu_1}(\sum c_\mu f_\mu) = c_{\mu_1} a_{\mu_1}$. So $c_{\mu_1} a_{\mu_1} = 0$. But $c_{\mu_1} \neq 0$ and $a_{\mu_1} \neq 0$, a contradiction. Thus $\{f_\mu\}_{\mu\in\Lambda_0}$ is linearly independent.

Note $F = \bigcup_{\lambda\in\Lambda_0} F_\lambda$. Given $\lambda \in \Lambda_0$, set $\Lambda_\lambda := \{\mu \in \Lambda_0 \mid \mu \le \lambda\}$. Suppose λ is least such that $\{f_\mu\}_{\mu\in\Lambda_\lambda}$ does not generate F_λ. Given $f \in F_\lambda$, say $f = \sum_{\mu\le\lambda} c_\mu e_\mu$ with $c_\mu \in R$. Then $\pi_\lambda(f) = c_\lambda$. But $\pi_\lambda(F_\lambda) = \langle a_\lambda\rangle$. So $c_\lambda = b_\lambda a_\lambda$ for some $b_\lambda \in R$. Set $g := f - b_\lambda f_\lambda$. Then $g \in F_\lambda$, and $\pi_\lambda(g) = 0$. So $g \in F_\nu$ for some $\nu \in \Lambda_0$ with $\nu < \lambda$. Hence $g = \sum_{\mu\in\Lambda_\nu} b_\mu f_\mu$ for some $b_\mu \in R$. So $f = \sum_{\mu\in\Lambda_\lambda} b_\mu f_\mu$, a contradiction. Hence $\{f_\mu\}_{\mu\in\Lambda_\lambda}$ generates F_λ. Thus $\{f_\mu\}_{\mu\in\Lambda_0}$ is a basis of F. □

(4.13) (Direct Products, Direct Sums). — Let R be a ring, Λ a set, M_λ a module for $\lambda \in \Lambda$. The **direct product** of the M_λ is the set of arbitrary vectors:

$$\prod M_\lambda := \{(m_\lambda) \mid m_\lambda \in M_\lambda\}.$$

Clearly, $\prod M_\lambda$ is a module under componentwise addition and scalar multiplication.

The **direct sum** of the M_λ is the subset of **restricted vectors**:

$$\bigoplus M_\lambda := \{(m_\lambda) \mid m_\lambda = 0 \text{ for almost all } \lambda\} \subset \prod M_\lambda.$$

Clearly, $\bigoplus M_\lambda$ is a submodule of $\prod M_\lambda$. Clearly, $\bigoplus M_\lambda = \prod M_\lambda$ if Λ is finite. If $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$, then $\bigoplus M_\lambda$ is also denoted by $M_{\lambda_1} \oplus \cdots \oplus M_{\lambda_n}$. Further, if $M_\lambda = M$ for all λ, then $\bigoplus M_\lambda$ is also denoted by M^Λ, or by M^n if Λ has just n elements.

The direct product comes equipped with projections

$$\pi_\kappa\colon \prod M_\lambda \to M_\kappa \quad \text{given by} \quad \pi_\kappa\big((m_\lambda)\big) := m_\kappa.$$

It is easy to see that $\prod M_\lambda$ has this UMP: *given R-maps $\alpha_\kappa\colon L \to M_\kappa$, there's a unique R-map $\alpha\colon L \to \prod M_\lambda$ with $\pi_\kappa\alpha = \alpha_\kappa$* for all $\kappa \in \Lambda$; namely, $\alpha(n) = \big(\alpha_\lambda(n)\big)$. Often, α is denoted (α_λ). In other words, the π_λ induce a bijection of sets,

$$\operatorname{Hom}\big(L, \prod M_\lambda\big) \xrightarrow{\sim} \prod \operatorname{Hom}(L, M_\lambda). \tag{4.13.1}$$

Clearly, this bijection is an isomorphism of modules.

Similarly, the direct sum comes equipped with injections

$$\iota_\kappa\colon M_\kappa \to \bigoplus M_\lambda \quad \text{given by} \quad \iota_\kappa(m) := (m_\lambda) \text{ where } m_\lambda := \begin{cases} m, & \text{if } \lambda = \kappa; \\ 0, & \text{if } \lambda \neq \kappa. \end{cases}$$

It's easy to see it has this UMP: *given R-maps $\beta_\kappa\colon M_\kappa \to N$, there's a unique R-map $\beta\colon \bigoplus M_\lambda \to N$ with $\beta\iota_\kappa = \beta_\kappa$* for all $\kappa \in \Lambda$; namely, $\beta\big((m_\lambda)\big) = \sum \beta_\lambda(m_\lambda)$. Often, β is denoted $\sum \beta_\lambda$; often, (β_λ). In other words, the ι_κ induce this bijection:

$$\operatorname{Hom}\big(\bigoplus M_\lambda, N\big) \xrightarrow{\sim} \prod \operatorname{Hom}(M_\lambda, N). \tag{4.13.2}$$

Clearly, this bijection of sets is an isomorphism of modules.

For example, if $M_\lambda = R$ for all λ, then $\bigoplus M_\lambda = R^{\oplus\Lambda}$ by construction. Further, if $N_\lambda := N$ for all λ, then $\operatorname{Hom}(R^{\oplus\Lambda}, N) = \prod N_\lambda$ by (**4.13.2**) and (**4.3**).

Given maps $\alpha_\lambda\colon M_\lambda \to N_\lambda$, form the maps $\alpha_\mu\pi_\mu\colon \prod M_\lambda \to N_\mu$. The UMP yields a unique map $\prod \alpha_\lambda\colon \prod M_\lambda \to \prod N_\lambda$ satisfying $\pi_\mu(\prod \alpha_\lambda) = \alpha_\mu\pi_\mu$ for all $\mu \in \Lambda$. Note $(\prod \alpha_\lambda)((m_\lambda)) = (\alpha_\lambda(m_\lambda))$.

Similarly, the maps $\iota_\kappa\alpha_\kappa\colon M_\kappa \to \bigoplus N_\lambda$ induce a map $\bigoplus \alpha_\lambda\colon \bigoplus M_\lambda \to \bigoplus N_\lambda$, unique with $(\bigoplus \alpha_\lambda)\iota_\kappa = \iota_\kappa\alpha_\kappa$ for all κ. Again note $(\bigoplus \alpha_\lambda)((m_\lambda)) = (\alpha_\lambda(m_\lambda))$.

B. Exercises

Exercise (4.14) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, M and N modules. Set

$$\Gamma_{\mathfrak{a}}(M) := \Big\{ m \in M \;\Big|\; \mathfrak{a} \subset \sqrt{\operatorname{Ann}(m)} \Big\}.$$

Show: (1) Assume $\mathfrak{a} \supset \mathfrak{b}$. Then $\Gamma_{\mathfrak{a}}(M) \subset \Gamma_{\mathfrak{b}}(M)$.

(2) Assume $M \subset N$. Then $\Gamma_{\mathfrak{a}}(M) = \Gamma_{\mathfrak{a}}(N) \cap M$.

(3) Then $\Gamma_{\mathfrak{a}}(\Gamma_{\mathfrak{b}}(M)) = \Gamma_{a+\mathfrak{b}}(M) = \Gamma_{\mathfrak{a}}(M) \cap \Gamma_{\mathfrak{b}}(M)$.

(4) Then $\Gamma_{\mathfrak{a}}(M) = \Gamma_{\sqrt{\mathfrak{a}}}(M)$.

(5) Assume $\mathfrak{a}$ is finitely generated. Then $\Gamma_{\mathfrak{a}}(M) = \bigcup_{n\ge1}\{ m \in M \mid \mathfrak{a}^n m = 0 \}$.

Exercise (4.15) . — Let R be a ring, M a module, $x \in \operatorname{rad}(M)$, and $m \in M$. Assume $(1+x)m = 0$. Show $m = 0$.

Exercise (4.16) . — Let R be a ring, M a module, N and N_λ submodules for $\lambda \in \Lambda$, and $\mathfrak{a}$, $\mathfrak{a}_\lambda$, $\mathfrak{b}$ ideals for $\lambda \in \Lambda$. Set $(N : \mathfrak{a}) := \{m \in M \mid \mathfrak{a}m \subset N\}$. Show:

(1) $(N : \mathfrak{a})$ is a submodule. (2) $N \subset (N : \mathfrak{a})$.

(3) $(N : \mathfrak{a})\mathfrak{a} \subset N$. (4) $((N : \mathfrak{a}) : \mathfrak{b}) = (N : \mathfrak{a}\mathfrak{b}) = ((N : \mathfrak{b}) : \mathfrak{a})$.

(5) $\big(\bigcap N_\lambda : \mathfrak{a}\big) = \bigcap (N_\lambda : \mathfrak{a})$. (6) $\big(N : \sum \mathfrak{a}_\lambda\big) = \bigcap (N : \mathfrak{a}_\lambda)$.

Exercise (4.17) . — Let R be a ring, M a module, N, N_λ, L, L_λ submodules for $\lambda \in \Lambda$. Set $(N : L) := \{x \in R \mid xL \subset N\}$. Show:

(1) $(N : L)$ is an ideal. (2) $(N : L) = \mathrm{Ann}((L + N)/N)$.
(3) $(0 : L) = \mathrm{Ann}(L)$. (4) $(N : L) = R$ if $L \subset N$
(5) $(\bigcap N_\lambda : L) = \bigcap (N_\lambda : L)$. (6) $\big(N : \sum L_\lambda\big) = \bigcap (N : L_\lambda)$.

Exercise (4.18) . — Let R be a ring, $\mathcal{X} := \{X_\lambda\}$ a set of variables, M a module, N a submodule. Set $P := R[\mathcal{X}]$. Prove these statements:

(1) $M[\mathcal{X}]$ is universal among P-modules Q with a given R-map $\alpha\colon M \to Q$; namely, there's a unique P-map $\beta\colon M[\mathcal{X}] \to Q$ with $\beta|M = \alpha$.

(2) $M[\mathcal{X}]$ has this UMP: given a P-module Q and R-maps $\alpha\colon M \to Q$ and $\chi_\lambda\colon Q \to Q$ for all λ, there's a unique R-map $\beta\colon M[\mathcal{X}] \to Q$ with $\beta|M = \alpha$ and $\beta\mu_{X_\lambda} = \chi_\lambda\beta$ for all λ.

(3) $M[\mathcal{X}]/N[\mathcal{X}] = (M/N)[\mathcal{X}]$.

Exercise (4.19) . — Let R be a ring, $\mathcal{X}$ a set of variables, M a module, and $N_1, \ldots, N_r$ submodules. Set $N = \bigcap N_i$. Prove the following equations:

$$(1)\ \ \mathrm{Ann}\big(M[\mathcal{X}]\big) = \mathrm{Ann}(M)[\mathcal{X}]. \quad (2)\ \ N[\mathcal{X}] = \bigcap N_i[\mathcal{X}].$$

Exercise (4.20) . — Let R be a ring, M a module, X a variable, $F \in R[X]$. Assume there's a nonzero $G \in M[X]$ with $FG = 0$. Show there's a nonzero $m \in M$ with $Fm = 0$. Proceed as follows. Say $G = m_0 + m_1X + \cdots + m_sX^s$ with $m_s \neq 0$. Assume s is minimal among all possible G. Show $Fm_s = 0$ (so $s = 0$).

Exercise (4.21) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module. Set $N := M/\mathfrak{a}M$. Show that $M/(\mathfrak{a} + \mathfrak{b})M \xrightarrow{\sim} N/\mathfrak{b}N$.

Exercise (4.22) . — Show that a finitely generated free module F has finite rank.

Exercise (4.23) . — Let R be a domain, and $x \in R$ nonzero. Let M be the submodule of $\mathrm{Frac}(R)$ generated by $1,\ x^{-1},\ x^{-2}, \ldots.$ Suppose that M is finitely generated. Prove that $x^{-1} \in R$, and conclude that $M = R$.

Exercise (4.24) . — Let Λ be an infinite set, R_λ a nonzero ring for $\lambda \in \Lambda$. Endow $\prod R_\lambda$ and $\bigoplus R_\lambda$ with componentwise addition and multiplication. Show that $\prod R_\lambda$ has a multiplicative identity (so is a ring), but that $\bigoplus R_\lambda$ does not (so is not a ring).

Exercise (4.25) . — Let R be a ring, M a module, and M', M'' submodules. Show that $M = M' \oplus M''$ if and only if $M = M' + M''$ and $M' \cap M'' = 0$.

Exercise (4.26) . — Let L, M, and N be modules. Consider a diagram

$$L \underset{\rho}{\overset{\alpha}{\rightleftarrows}} M \underset{\sigma}{\overset{\beta}{\rightleftarrows}} N$$

where α, β, ρ, and σ are homomorphisms. Prove that

$$M = L \oplus N \quad \text{and} \quad \alpha = \iota_L,\ \beta = \pi_N,\ \sigma = \iota_N,\ \rho = \pi_L$$

if and only if the following relations hold:

$$\beta\alpha = 0,\ \beta\sigma = 1,\ \rho\sigma = 0,\ \rho\alpha 1,\ \text{and}\ \alpha\rho + \sigma\beta = 1.$$

Exercise (4.27) . — Let L be a module, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove that the injections $\iota_\kappa\colon M_\kappa \to \bigoplus M_\lambda$ induce an injection

$$\bigoplus \mathrm{Hom}(L,\ M_\lambda) \hookrightarrow \mathrm{Hom}(L,\ \bigoplus M_\lambda),$$

and that it is an isomorphism if L is finitely generated.

Exercise (4.28) . — Let $\mathfrak{a}$ be an ideal, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove $\mathfrak{a}\big(\bigoplus M_\lambda\big) = \bigoplus \mathfrak{a} M_\lambda$. Prove $\mathfrak{a}(\prod M_\lambda) = \prod \mathfrak{a} M_\lambda$ if $\mathfrak{a}$ is finitely generated.

Exercise (4.29) . — Let R be a ring, Λ a set, M_λ a module for $\lambda \in \Lambda$, and $N_\lambda \subset M_\lambda$ a submodule. Set $M := \bigoplus M_\lambda$ and $N := \bigoplus N_\lambda$ and $Q := \bigoplus M_\lambda / N_\lambda$. Show $M/N = Q$.

5. Exact Sequences

In the study of modules, the exact sequence plays a central role. We relate it to the kernel and image, the direct sum and direct product. We introduce diagram chasing, and prove the Snake Lemma, which is a fundamental result in homological algebra. We define projective modules, and characterize them in four ways. Finally, we prove Schanuel's Lemma, which relates two arbitrary presentations of a module.

In an appendix, we use determinants to study Fitting ideals and free modules. In particular, we prove that the rank of a free module is invariant under isomorphism; more proofs are given in **(8.25)**(2) and **(10.5)**(2). We also prove the Elementary Divisors Theorem for a nested pair $N \subset M$ of free modules with N of rank n over a PID; it asserts that M has a (free) basis containing elements $x_1, \ldots, x_n$ with unique multiples $d_1x_1, \ldots, d_nx_n$ that form a basis of N; also, $d_i \mid d_{i+1}$ for $i < n$.

A. Text

Definition (5.1). — A (finite or infinite) sequence of module homomorphisms

$$\cdots \to M_{i-1} \xrightarrow{\alpha_{i-1}} M_i \xrightarrow{\alpha_i} M_{i+1} \to \cdots$$

is said to be **exact at** M_i if $\mathrm{Ker}(\alpha_i) = \mathrm{Im}(\alpha_{i-1})$. The sequence is said to be **exact** if it is exact at every M_i, except an initial source or final target.

Example (5.2). — (1) A sequence $0 \to L \xrightarrow{\alpha} M$ is exact if and only if α is injective. If so, then we often identify L with its image $\alpha(L)$.

Dually — that is, in the analogous situation with all arrows reversed — a sequence $M \xrightarrow{\beta} N \to 0$ is exact if and only if β is surjective.

(2) A sequence $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is exact if and only if $L = \mathrm{Ker}(\beta)$, where '$=$' means "canonically isomorphic." Dually, a sequence $L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is exact if and only if $N = \mathrm{Coker}(\alpha)$ owing to (1) and **(4.6.1)**.

(5.3) (Short exact sequences). — A sequence $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ is exact if and only if α is injective and $N = \mathrm{Coker}(\alpha)$, or dually, if and only if β is surjective and $L = \mathrm{Ker}(\beta)$. If so, then the sequence is called **short exact**, and often we regard L as a submodule of M, and N as the quotient M/L.

For example, the following sequence is clearly short exact:

$$0 \to L \xrightarrow{\iota_L} L \oplus N \xrightarrow{\pi_N} N \to 0 \quad \text{where}$$
$$\iota_L(l) := (l, 0) \quad \text{and} \quad \pi_N(l, n) := n.$$

Proposition (5.4). — *For $\lambda \in \Lambda$, let $M'_\lambda \to M_\lambda \to M''_\lambda$ be a sequence of module homomorphisms. If every sequence is exact, then so are the two induced sequences*

$$\bigoplus M'_\lambda \to \bigoplus M_\lambda \to \bigoplus M''_\lambda \quad \textit{and} \quad \prod M'_\lambda \to \prod M_\lambda \to \prod M''_\lambda.$$

Conversely, if either induced sequence is exact then so is every original one.

Proof: The assertions are immediate from (**5.1**) and (**4.13**). □

Exercise (5.5) . — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Prove that, if M' and M'' are finitely generated, then so is M.

Proposition (5.6). — *Let $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ be a short exact sequence, and $N \subset M$ a submodule. Set $N' := \alpha^{-1}(N)$ and $N'' := \beta(N)$. Then the induced sequence $0 \to N' \to N \to N'' \to 0$ is short exact.*

Proof: It is simple and straightforward to verify the asserted exactness. □

(5.7) (Retraction, section, splits). — We call a linear map $\rho\colon M \to M'$ a **retraction** of another $\alpha\colon M' \to M$ if $\rho\alpha = 1_{M'}$. Then α is injective and ρ is surjective.

Dually, we call a linear map $\sigma\colon M'' \to M$ a **section** of another $\beta\colon M \to M''$ if $\beta\sigma = 1_{M''}$. Then β is surjective and σ is injective..

We say that a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ **splits** if there is an isomorphism $\varphi\colon M \xrightarrow{\sim} M' \oplus M''$ with $\varphi\alpha = \iota_{M'}$ and $\beta = \pi_{M''}\varphi$.

Proposition (5.8). — *Let $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ be a 3-term exact sequence. Then the following conditions are equivalent:*

(1) *The sequence splits.*
(2) *There exists a retraction $\rho\colon M \to M'$ of α, and β is surjective.*
(3) *There exists a section $\sigma\colon M'' \to M$ of β, and α is injective.*

Proof: Assume (1). Then there exists $\varphi\colon M \xrightarrow{\sim} M' \oplus M''$ such that $\varphi\alpha = \iota_{M'}$ and $\beta = \pi_{M''}\varphi$. Set $\rho := \pi_{M'}\varphi$ and $\sigma := \varphi^{-1}\iota_{M''}$. Then plainly (2) and (3) hold.

Assume (2). Set $\sigma' := 1_M - \alpha\rho$. Then $\sigma'\alpha = \alpha - \alpha\rho\alpha$. But $\rho\alpha = 1_{M'}$ as ρ is a retraction. So $\sigma'\alpha = 0$. Hence there exists $\sigma\colon M'' \to M$ with $\sigma\beta = \sigma'$ by (**5.2**)(2) and the UMP of (**4.9**). Thus $1_M = \alpha\rho + \sigma\beta$.

Hence $\beta = \beta\alpha\rho + \beta\sigma\beta$. But $\beta\alpha = 0$ as the sequence is exact. So $\beta = \beta\sigma\beta$. But β is surjective. Thus $1_{M''} = \beta\sigma$; that is, (3) holds.

Similarly, $\sigma = \alpha\rho\sigma + \sigma\beta\sigma$. But $\beta\sigma = 1_{M''}$ as (3) holds. So $0 = \alpha\rho\sigma$. But α is injective, as ρ is a retraction of it. Thus $\rho\sigma = 0$. Thus (**4.26**) yields (1).

Assume (3). Then similarly (1) and (2) hold. □

Example (5.9). — Let R be a ring, R' an R-algebra, and M an R'-module. Set $H := \mathrm{Hom}_R(R', M)$. Define $\alpha\colon M \to H$ by $\alpha(m)(x) := xm$, and $\rho\colon H \to M$ by $\rho(\theta) := \theta(1)$. Then ρ is a retraction of α, as $\rho(\alpha(m)) = 1\cdot m$. Let $\beta\colon H \to \mathrm{Coker}(\alpha)$ be the quotient map. Then (**5.8**) implies that M is a direct summand of H with $\alpha = \iota_M$ and $\rho = \pi_M$.

Lemma (5.10) (Snake). — *Consider this commutative diagram with exact rows:*

$$\begin{array}{ccccccc}
 & & M' & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & M'' & \to 0\\
 & & {\scriptstyle\gamma'}\big\downarrow & & {\scriptstyle\gamma}\big\downarrow & & {\scriptstyle\gamma''}\big\downarrow & \\
0 & \to & N' & \xrightarrow{\alpha'} & N & \xrightarrow{\beta'} & N'' &
\end{array}$$

It yields the following exact sequence:

$$\mathrm{Ker}(\gamma') \xrightarrow{\varphi} \mathrm{Ker}(\gamma) \xrightarrow{\psi} \mathrm{Ker}(\gamma'') \xrightarrow{\partial} \mathrm{Coker}(\gamma') \xrightarrow{\varphi'} \mathrm{Coker}(\gamma) \xrightarrow{\psi'} \mathrm{Coker}(\gamma''). \qquad \textbf{(5.10.1)}$$

Moreover, if α is injective, then so is φ; dually, if β' is surjective, then so is ψ'.

Proof: Clearly α restricts to a map φ, because $\alpha\big(\mathrm{Ker}(\gamma')\big) \subset \mathrm{Ker}(\gamma)$ since $\alpha'\gamma'\big(\mathrm{Ker}(\gamma')\big) = 0$. By the UMP discussed in (**4.9**), α' factors through a unique map φ' because M' goes to 0 in $\mathrm{Coker}(\gamma)$. Similarly, β and β' induce corresponding maps ψ and ψ'. Thus all the maps in (**5.10.1**) are defined except for ∂.

To define ∂, **chase** an $m'' \in \mathrm{Ker}(\gamma'')$ through the diagram. Since β is surjective, there is $m \in M$ such that $\beta(m) = m''$. By commutativity, $\gamma''\beta(m) = \beta'\gamma(m)$. So

$\beta'\gamma(m) = 0$. By exactness of the bottom row, there is a unique $n' \in N'$ such that $\alpha'(n') = \gamma(m)$. Define $\partial(m'')$ to be the image of n' in $\mathrm{Coker}(\gamma')$.

To see ∂ is well defined, choose another $m_1 \in M$ with $\beta(m_1) = m''$. Let $n'_1 \in N'$ be the unique element with $\alpha'(n'_1) = \gamma(m_1)$ as above. Since $\beta(m - m_1) = 0$, there is an $m' \in M'$ with $\alpha(m') = m - m_1$. But $\alpha'\gamma' = \gamma\alpha$. So $\alpha'\gamma'(m') = \alpha'(n' - n'_1)$. Hence $\gamma'(m') = n' - n'_1$ since α' is injective. So n' and n'_1 have the same image in $\mathrm{Coker}(\gamma')$. Thus ∂ is well defined.

Let's show that **(5.10.1)** is exact at $\mathrm{Ker}(\gamma'')$. Take $m'' \in \mathrm{Ker}(\gamma'')$. As in the construction of ∂, take $m \in M$ such that $\beta(m) = m''$ and take $n' \in N'$ such that $\alpha'(n') = \gamma(m)$. Suppose $m'' \in \mathrm{Ker}(\partial)$. Then the image of n' in $\mathrm{Coker}(\gamma')$ is equal to 0; so there is $m' \in M'$ such that $\gamma'(m') = n'$. Clearly $\gamma\alpha(m') = \alpha'\gamma'(m')$. So $\gamma\alpha(m') = \alpha'(n') = \gamma(m)$. Hence $m - \alpha(m') \in \mathrm{Ker}(\gamma)$. Since $\beta\big(m - \alpha(m')\big) = m''$, clearly $m'' = \psi(m - \alpha(m'))$; so $m'' \in \mathrm{Im}(\psi)$. Hence $\mathrm{Ker}(\partial) \subset \mathrm{Im}(\psi)$.

Conversely, suppose $m'' \in \mathrm{Im}(\psi)$. We may assume $m \in \mathrm{Ker}(\gamma)$. So $\gamma(m) = 0$ and $\alpha'(n') = 0$. Since α' is injective, $n' = 0$. Thus $\partial(m'') = 0$, and so $\mathrm{Im}(\psi) \subset \mathrm{Ker}(\partial)$. Thus $\mathrm{Ker}(\partial)$ is equal to $\mathrm{Im}(\psi)$; that is, **(5.10.1)** is exact at $\mathrm{Ker}(\gamma'')$.

The other verifications of exactness are similar or easier.

The last two assertions are clearly true. □

Theorem (5.11) (Left exactness of Hom). — (1) *Let $M' \to M \to M'' \to 0$ be a sequence of linear maps. Then it is exact if and only if, for all modules N, the following induced sequence is exact:*

$$0 \to \mathrm{Hom}(M'', N) \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N). \tag{5.11.1}$$

(2) *Let $0 \to N' \to N \to N''$ be a sequence of linear maps. Then it is exact if and only if, for all modules M, the following induced sequence is exact:*

$$0 \to \mathrm{Hom}(M, N') \to \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'').$$

Proof: By **(5.2)**(2), the exactness of $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ means simply that $M'' = \mathrm{Coker}(\alpha)$. On the other hand, the exactness of **(5.11.1)** means that a $\varphi \in \mathrm{Hom}(M, N)$ maps to 0, or equivalently $\varphi\alpha = 0$, if and only if there is a unique $\gamma\colon M'' \to N$ such that $\gamma\beta = \varphi$. So **(5.11.1)** is exact if and only if M'' has the UMP of $\mathrm{Coker}(\alpha)$, discussed in **(4.9)**; that is, $M'' = \mathrm{Coker}(\alpha)$. Thus (1) holds.

The proof of (2) is similar — in fact, dual. □

Definition (5.12). — A (free) **presentation** of a module M is an exact sequence

$$G \to F \to M \to 0$$

with G and F free. If G and F are free of finite rank, then the presentation is called **finite**. If M has a finite presentation, then M is said to be **finitely presented**.

Proposition (5.13). — *Let R be a ring, M a module, m_λ for $\lambda \in \Lambda$ generators. Then there is an exact sequence $0 \to K \to R^{\oplus\Lambda} \xrightarrow{\alpha} M \to 0$ with $\alpha(e_\lambda) = m_\lambda$, where $\{e_\lambda\}$ is the standard basis, and there is a presentation $R^{\oplus\Sigma} \to R^{\oplus\Lambda} \xrightarrow{\alpha} M \to 0$.*

Proof: By **(4.10)**(1), there is a surjection $\alpha\colon R^{\oplus\Lambda} \twoheadrightarrow M$ with $\alpha(e_\lambda) = m_\lambda$. Set $K := \mathrm{Ker}(\alpha)$. Then $0 \to K \to R^{\oplus\Lambda} \to M \to 0$ is exact by **(5.3)**. Take a set of generators $\{k_\sigma\}_{\sigma\in\Sigma}$ of K, and repeat the process to obtain a surjection $R^{\oplus\Sigma} \twoheadrightarrow K$. Then $R^{\oplus\Sigma} \to R^{\oplus\Lambda} \to M \to 0$ is a presentation. □

Definition (5.14). — A module P is called **projective** if, given any surjective linear map $\beta\colon M \twoheadrightarrow N$, every linear map $\alpha\colon P \to N$ **lifts** to one $\gamma\colon P \to M$; namely, $\alpha = \beta\gamma$.

Exercise (5.15) . — Show that a free module $R^{\oplus\Lambda}$ is projective.

Theorem (5.16). — *The following conditions on an R-module P are equivalent:*

(1) *The module P is projective.*
(2) *Every short exact sequence $0 \to K \to M \to P \to 0$ splits.*
(3) *There is a module K such that $K \oplus P$ is free.*
(4) *Every exact sequence $N' \to N \to N''$ induces an exact sequence*

$$\operatorname{Hom}(P,\, N') \to \operatorname{Hom}(P,\, N) \to \operatorname{Hom}(P,\, N''). \tag{5.16.1}$$

(5) *Every surjective homomorphism $\beta\colon M \twoheadrightarrow N$ induces a surjection*

$$\operatorname{Hom}(P, \beta)\colon\ \operatorname{Hom}(P,\, M) \to \operatorname{Hom}(P,\, N).$$

Proof: Assume (1). In (2), the surjection $M \twoheadrightarrow P$ and the identity $P \to P$ yield a section $P \to M$. So the sequence splits by **(5.8)**. Thus (2) holds.

Assume (2). By **(5.13)**, there is an exact sequence $0 \to K \to R^{\oplus\Lambda} \to P \to 0$. Then (2) implies $K \oplus P \simeq R^{\oplus\Lambda}$. Thus (3) holds.

Assume (3); say $K \oplus P \simeq R^{\oplus\Lambda}$. For each $\lambda \in \Lambda$, take a copy $N'_\lambda \to N_\lambda \to N'_\lambda$ of the exact sequence $N' \to N \to N''$ of (4). Then the induced sequence

$$\prod N'_\lambda \to \prod N_\lambda \to \prod N''_\lambda.$$

is exact by **(5.4)**. But by the end of **(4.13)**, that sequence is equal to this one:

$$\operatorname{Hom}(R^{\oplus\Lambda},\, N') \to \operatorname{Hom}(R^{\oplus\Lambda},\, N) \to \operatorname{Hom}(R^{\oplus\Lambda},\, N'').$$

But $K \oplus P \simeq R^{\oplus\Lambda}$. So owing to **(4.13.2)**, the latter sequence is also equal to

$$\operatorname{Hom}(K, N') \oplus \operatorname{Hom}(P, N') \to \operatorname{Hom}(K, N) \oplus \operatorname{Hom}(P, N) \to \operatorname{Hom}(K, N'') \oplus \operatorname{Hom}(P, N'').$$

Hence **(5.16.1)** is exact by **(5.4)**. Thus (4) holds.

Assume (4). Then every exact sequence $M \xrightarrow{\beta} N \to 0$ induces an exact sequence

$$\operatorname{Hom}(P,\, M) \xrightarrow{\operatorname{Hom}(P,\beta)} \operatorname{Hom}(P,\, N) \to 0.$$

In other words, (5) holds.

Assume (5). Then every $\alpha \in \operatorname{Hom}(P,\, N)$ is the image under $\operatorname{Hom}(P, \beta)$ of some $\gamma \in \operatorname{Hom}(P,\, M)$. But, by definition, $\operatorname{Hom}(P, \beta)(\gamma) = \beta\gamma$. Thus (1) holds. □

Lemma (5.17) (Schanuel's)**. —** *Any two short exact sequences*

$$0 \to L \xrightarrow{i} P \xrightarrow{\alpha} M \to 0 \quad \textit{and} \quad 0 \to L' \xrightarrow{i'} P' \xrightarrow{\alpha'} M \to 0$$

with P and P' projective are essentially isomorphic; namely, there's a commutative diagram with vertical isomorphisms:

$$\begin{tikzcd}
0 \arrow[r] & L \oplus P' \arrow[r, "i\oplus 1_{P'}"] \arrow[d, "\beta", "\simeq"'] & P \oplus P' \arrow[r, "(\alpha\ 0)"] \arrow[d, "\gamma", "\simeq"'] & M \arrow[r] \arrow[d, "1_M", "="'] & 0 \\
0 \arrow[r] & P \oplus L' \arrow[r, "1_P\oplus i'"] & P \oplus P' \arrow[r, "(0\ \alpha')"] & M \arrow[r] & 0
\end{tikzcd}$$

Proof: First, let's construct an intermediate isomorphism of exact sequences:

$$\begin{array}{ccccccccc} 0 & \to & L\oplus P' & \xrightarrow{i\oplus 1_{P'}} & P\oplus P' & \xrightarrow{(\alpha\ 0)} & M & \to & 0\\ & & \simeq\big\uparrow\lambda & & \simeq\big\uparrow\theta & & =\big\uparrow 1_M & & \\ 0 & \longrightarrow & K & \longrightarrow & P\oplus P' & \xrightarrow{(\alpha\ \alpha')} & M & \to & 0 \end{array}$$

Take $K := \operatorname{Ker}(\alpha\,\alpha')$. To form θ, recall that P' is projective and α is surjective. So there is a map $\pi\colon P' \to P$ such that $\alpha' = \alpha\pi$. Take $\theta := \left(\begin{smallmatrix}1 & \pi\\ 0 & 1\end{smallmatrix}\right)$.

Then θ has $\left(\begin{smallmatrix}1 & -\pi\\ 0 & 1\end{smallmatrix}\right)$ as inverse. Further, the right-hand square is commutative:

$$(\alpha\ 0)\theta = (\alpha\ 0)\left(\begin{smallmatrix}1 & \pi\\ 0 & 1\end{smallmatrix}\right) = (\alpha\ \alpha\pi) = (\alpha\ \alpha').$$

So θ induces the desired isomorphism $\lambda\colon K \xrightarrow{\sim} L\oplus P'$.

Symmetrically, form an isomorphism $\theta'\colon P\oplus P' \xrightarrow{\sim} P\oplus P$, which induces an isomorphism $\lambda'\colon K \xrightarrow{\sim} P\oplus L'$. Finally, take $\gamma := \theta'\theta^{-1}$ and $\beta := \lambda'\lambda^{-1}$. $\square$

Exercise (5.18) . — Let R be a ring, and $0 \to L \to R^n \to M \to 0$ an exact sequence. Prove M is finitely presented if and only if L is finitely generated.

Proposition (5.19). — *Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with L finitely generated and M finitely presented. Then N is finitely presented.*

Proof: Let R be the ground ring, $\mu\colon R^m \to M$ any surjection. Set $\nu := \beta\mu$, set $K := \operatorname{Ker}\nu$, and set $\lambda := \mu|K$. Then the following diagram is commutative:

$$\begin{array}{ccccccccc} 0 & \to & K & \to & R^m & \xrightarrow{\nu} & N & \to & 0\\ & & \lambda\big\downarrow & & \mu\big\downarrow & & 1_N\big\downarrow & & \\ 0 & \to & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \to & 0 \end{array}$$

The Snake Lemma (5.10) yields an isomorphism $\operatorname{Ker}\lambda \xrightarrow{\sim} \operatorname{Ker}\mu$. But $\operatorname{Ker}\mu$ is finitely generated by (5.18). So $\operatorname{Ker}\lambda$ is finitely generated. Also, the Snake Lemma implies $\operatorname{Coker}\lambda = 0$ as $\operatorname{Coker}\mu = 0$; so $0 \to \operatorname{Ker}\lambda \to K \xrightarrow{\lambda} L \to 0$ is exact. Hence K is finitely generated by (5.5). Thus N is finitely presented by (5.18). $\square$

Proposition (5.20). — *Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with L and N finitely presented. Then M is finitely presented too.*

Proof: Let R be the ground ring, $\lambda\colon R^\ell \to L$ and $\nu\colon R^n \twoheadrightarrow N$ any surjections. Define $\gamma\colon R^\ell \to M$ by $\gamma := \alpha\lambda$. Note R^n is projective by (5.15), and define $\delta\colon R^n \to M$ by lifting ν along β. Define $\mu\colon R^\ell\oplus R^n \to M$ by $\mu := \gamma+\delta$. Then the following diagram is, plainly, commutative, where $\iota := \iota_{R^\ell}$ and $\pi := \pi_{R^n}$:

$$\begin{array}{ccccccccc} 0 & \to & R^\ell & \xrightarrow{\iota} & R^\ell\oplus R^n & \xrightarrow{\pi} & R^n & \to & 0\\ & & \lambda\big\downarrow & & \mu\big\downarrow & & \nu\big\downarrow & & \\ 0 & \longrightarrow & L & \xrightarrow{\alpha} & M & \xrightarrow{\beta} & N & \to & 0 \end{array}$$

Since λ and ν are surjective, the Snake Lemma (5.10) yields an exact sequence

$$0 \to \operatorname{Ker}\lambda \to \operatorname{Ker}\mu \to \operatorname{Ker}\nu \to 0,$$

and implies $\operatorname{Coker}\mu = 0$. Also, $\operatorname{Ker}\lambda$ and $\operatorname{Ker}\nu$ are finitely generated by (5.18). So $\operatorname{Ker}\mu$ is finitely generated by (5.5). Thus M is finitely presented by (5.18). $\square$

B. Exercises

Exercise (5.21) . — Let M' and M'' be modules, $N \subset M'$ a submodule. Set $M := M' \oplus M''$. Using (5.2)(1) and (5.3) and (5.4), prove $M/N = M'/N \oplus M''$.

Exercise (5.22) . — Let M', M'' be modules, and set $M := M' \oplus M''$. Let N be a submodule of M containing M', and set $N'' := N \cap M''$. Prove $N = M' \oplus N''$.

Exercise (5.23) (*Five Lemma*) . — Consider this commutative diagram:

$$\begin{array}{ccccccccc}
M_4 & \xrightarrow{\alpha_4} & M_3 & \xrightarrow{\alpha_3} & M_2 & \xrightarrow{\alpha_2} & M_1 & \xrightarrow{\alpha_1} & M_0 \\
\gamma_4\downarrow & & \gamma_3\downarrow & & \gamma_2\downarrow & & \gamma_1\downarrow & & \gamma_0\downarrow \\
N_4 & \xrightarrow{\beta_4} & N_3 & \xrightarrow{\beta_3} & N_2 & \xrightarrow{\beta_2} & N_1 & \xrightarrow{\beta_1} & N_0
\end{array}$$

Assume it has exact rows. Via a chase, prove these two statements:

(1) If γ_3 and γ_1 are surjective and if γ_0 is injective, then γ_2 is surjective.
(2) If γ_3 and γ_1 are injective and if γ_4 is surjective, then γ_2 is injective.

Exercise (5.24) (*Nine Lemma*) . — Consider this commutative diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & L' & \to & L & \to & L'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & M' & \to & M & \to & M'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & N' & \to & N & \to & N'' & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array} \qquad (5.24.1)$$

Assume all the columns are exact and the middle row is exact. Applying the Snake Lemma (5.10), show that the first row is exact if and only if the third is.

Exercise (5.25) . — Referring to (4.8), give an alternative proof that β is an isomorphism by applying the Snake Lemma (5.10) to the diagram

$$\begin{array}{ccccccccc}
0 & \to & M & \to & N & \to & N/M & \to & 0 \\
 & & \downarrow & & \kappa\downarrow & & \beta\downarrow & & \\
0 & \to & M/L & \to & N/L & \xrightarrow{\lambda} & (N/L)\big/(M/L) & \to & 0
\end{array}$$

Exercise (5.26) . — Consider this commutative diagram with exact rows:

$$\begin{array}{ccccc}
M' & \xrightarrow{\beta} & M & \xrightarrow{\gamma} & M'' \\
\alpha'\downarrow & & \alpha\downarrow & & \alpha''\downarrow \\
N' & \xrightarrow{\beta'} & N & \xrightarrow{\gamma'} & N''
\end{array}$$

Assume α' and γ are surjective. Given $n \in N$ and $m'' \in M''$ with $\alpha''(m'') = \gamma'(n)$, show that there is $m \in M$ such that $\alpha(m) = n$ and $\gamma(m) = m''$.

Exercise (5.27) . — Let R be a ring. Show that a module P is finitely generated and projective if and only if it's a direct summand of a free module of finite rank.

Exercise (5.28) . — Let R be a ring, P and N finitely generated modules with P projective. Prove $\mathrm{Hom}(P, N)$ is finitely generated, and is finitely presented if N is.

Exercise (5.29) . — Let R be a ring, $X_1, X_2, \dots$ infinitely many variables. Set $P := R[X_1, X_2, \dots]$ and $M := P/\langle X_1, X_2, \dots\rangle$. Is M finitely presented? Explain.

Exercise (5.30) . — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with M finitely generated and N finitely presented. Prove L is finitely generated.

C. Appendix: Fitting Ideals

(5.31) (The Ideals of Minors). — Let R be a ring, $\mathbf{A} := (a_{ij})$ an $m \times n$ matrix with $a_{ij} \in R$. Given $r \in \mathbb{Z}$, let $I_r(\mathbf{A})$ denote the ideal generated by the $r \times r$ minors of $\mathbf{A}$; by convention, we have

$$I_r(\mathbf{A}) = \begin{cases} \langle 0\rangle, & \text{if } r > \min\{m, n\}; \\ R, & \text{if } r \le 0. \end{cases} \tag{5.31.1}$$

Let $\mathbf{B} := (b_{ij})$ be an $r \times r$ submatrix of $\mathbf{A}$. Let $\mathbf{B}_{ij}$ be the $(r-1) \times (r-1)$ submatrix obtained from $\mathbf{B}$ by deleting the ith row and the jth column. For any i, expansion yields $\det(\mathbf{B}) = \sum_{j=1}^{r} (-1)^{i+j} b_{ij} \det(\mathbf{B}_{ij})$. So $I_r(\mathbf{A}) \subset I_{r-1}(\mathbf{A})$. Thus

$$R = I_0(\mathbf{A}) \supset I_1(\mathbf{A}) \supset \cdots . \tag{5.31.2}$$

Let $\mathbf{U}$ be an invertible $m \times m$ matrix. Then $\det(\mathbf{U})$ is a unit, as $UV = I$ yields $\det(U)\det(V) = 1$. So $I_m(\mathbf{U}) = R$. Thus $I_r(\mathbf{U}) = R$ for all $r \le m$.

Proposition (5.32). — *Let R be a nonzero ring, and $\alpha\colon R^n \to R^m$ a linear map.* (1) *If α is injective, then $n \le m$.* (2) *If α is an isomorphism, then $n = m$.*

Proof: For (1), assume $n > m$, and let's show α is not injective.

Let $\mathbf{A}$ be the matrix of α. Note **(5.31.1)** yields $I_p(\mathbf{A}) = \langle 0\rangle$ for $p > m$ and $I_0(\mathbf{A}) = R$. Let r be the largest integer with $\mathrm{Ann}(I_r(\mathbf{A})) = \langle 0\rangle$. Then $0 \le r \le m$.

Take any nonzero $x \in \mathrm{Ann}(I_{r+1}(\mathbf{A}))$. If $r = 0$, set $z := (x, 0, \dots, 0)$. Then $z \ne 0$ and $\alpha(z) = 0$; so α is not injective. So assume $r > 0$.

As $x \ne 0$, also $x \notin \mathrm{Ann}(I_r(\mathbf{A}))$. So there's an $r \times r$ submatrix $\mathbf{B}$ of $\mathbf{A}$ with $x \det(\mathbf{B}) \ne 0$. By renumbering, we may assume that $\mathbf{B}$ is the upper left $r \times r$ submatrix of $\mathbf{A}$. Let $\mathbf{C}$ be the upper left $(r+1) \times (r+1)$ submatrix if $r \le m$; if $r = m$, let $\mathbf{C}$ be the left $r \times (r+1)$ submatrix augmented at the bottom by a row of $r+1$ zeros.

Let c_i be the cofactor of $a_{(r+1)i}$ in $\det(\mathbf{C})$; so $\det(\mathbf{C}) = \sum_{i=1}^{r+1} a_{(r+1)i} c_i$. Then $c_{r+1} = \det(\mathbf{B})$. So $x c_{r+1} \ne 0$. Set $z := x(c_1, \dots, c_{r+1}, 0, \dots, 0)$. Then $z \ne 0$.

Let's show $\alpha(z) = 0$. Given $1 \le k \le m$, denote by $\mathbf{A}_k$ the kth row of $\mathbf{A}$, by $\mathbf{D}$ the matrix obtained by replacing the $(r+1)$st row of $\mathbf{C}$ with the first $(r+1)$ entries of $\mathbf{A}_k$, and by $z \cdot \mathbf{A}_k$ the dot product. Then $z \cdot \mathbf{A}_k = x \det(\mathbf{D})$. If $k \le r$, then $\mathbf{D}$ has two equal rows; so $z \cdot \mathbf{A}_k = 0$. If $k \ge r+1$, then $\mathbf{D}$ is an $(r+1) \times (r+1)$ submatrix of $\mathbf{A}$; so $z \cdot \mathbf{A}_k = 0$ as $x I_{r+1}(\mathbf{A}) = 0$. Thus $\alpha(z) = 0$. Thus α is not injective. Thus (1) holds.

For (2), apply (1) to α^{-1} too; thus also $m \le n$. Thus (2) holds. □

Lemma (5.33). — *Let R be a ring, $\mathbf{A}$ an $m \times n$ matrix, $\mathbf{B}$ an $n \times p$ matrix, $\mathbf{U}$ be an invertible $m \times m$ matrix, and $\mathbf{V}$ an invertible $n \times n$ matrix. Then for all r,*

$$(1)\ \ I_r(\mathbf{AB}) \subset I_r(\mathbf{A}) I_r(\mathbf{B}) \quad \textit{and} \quad (2)\ \ I_r(\mathbf{UAV}) = I_r(\mathbf{A}).$$

Proof: As a matter of notation, given a $p \times q$ matrix $\mathbf{X} := (x_{ij})$, denote its jth column by $\mathbf{X}^j$. Given sequences $I := (i_1, \ldots, i_r)$ with $1 \le i_1 < \cdots < i_r \le p$ and $J := (j_1, \ldots, j_r)$ with $1 \le j_1 < \cdots < j_r \le q$, set

$$\mathbf{X}_{IJ} := \begin{pmatrix} x_{i_1 j_1} & \ldots & x_{i_1 j_r} \\ \vdots & & \vdots \\ x_{i_r j_1} & \ldots & x_{i_r j_r} \end{pmatrix} \quad \text{and} \quad \mathbf{X}_I := \begin{pmatrix} x_{i_1 1} & \ldots & x_{i_1 n} \\ \vdots & & \vdots \\ x_{i_r 1} & \ldots & x_{i_r n} \end{pmatrix}.$$

For (1), say $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{ij})$. Set $\mathbf{C} := \mathbf{AB}$. Given $I := (i_1, \ldots, i_r)$ with $1 \le i_1 < \cdots < i_r \le m$ and $K := (k_1, \ldots, k_r)$ with $1 \le k_1 < \cdots < k_r \le p$, note

$$\begin{aligned} \det(\mathbf{C}_{IK}) &= \det\bigl(C^1_{IK}, \ldots, C^r_{IK}\bigr) \\ &= \det\Bigl(\sum_{j_1=1}^{n} \mathbf{A}_I^{j_1} b_{j_1 k_1}, \ldots, \sum_{j_r=1}^{n} \mathbf{A}_I^{j_r} b_{j_r k_r}\Bigr) \\ &= \sum_{j_1, \ldots, j_r = 1}^{n} \det\bigl(\mathbf{A}_I^{j_1}, \ldots, \mathbf{A}_I^{j_r}\bigr) \cdot b_{j_1 k_1} \cdots b_{j_r k_r}. \end{aligned}$$

In the last sum, each term corresponds to a sequence $J := (j_1, \ldots, j_r)$ with $1 \le j_i \le n$. If two j_i are equal, then $\det\bigl(\mathbf{A}_I^{j_1}, \ldots, \mathbf{A}_I^{j_r}\bigr) = 0$ as two columns are equal. Suppose no two j_i are equal. Then J is a permutation σ of $H := (h_1, \ldots, h_r)$ with $1 \le h_1 < \cdots < h_r \le q$; so $j_i = \sigma(h_i)$. Denote the sign of σ by $(-1)^\sigma$. Then

$$\det\bigl(\mathbf{A}_I^{j_1}, \ldots, \mathbf{A}_I^{j_r}\bigr) = (-1)^\sigma \det(\mathbf{A}_{IH}).$$

But $\det(\mathbf{B}_{HK}) = \sum_\sigma (-1)^\sigma b_{\sigma(h_1)k_1} \cdots b_{\sigma(h_r)k_r}$. Hence

$$\det(\mathbf{C}_{IK}) = \textstyle\sum_H \det(\mathbf{A}_{IH}) \det(\mathbf{B}_{HK}).$$

Thus (1) holds.

For (2), note $I_r(W) = R$ for $W = U, U^{-1}, V, V^{-1}$ and $r \le \min\{m, n\}$ by **(5.31)**. So (1) implies

$$I_r(\mathbf{A}) = I_r(\mathbf{U}^{-1}\mathbf{UAVV}^{-1}) \subset I_r(\mathbf{UAV}) \subset I_r(\mathbf{A}).$$

Thus (2) holds. □

Lemma (5.34) (Fitting). — *Let R be a ring, M a module, r an integer, and*

$$R^n \xrightarrow{\alpha} R^m \xrightarrow{\mu} M \to 0 \quad \text{and} \quad R^q \xrightarrow{\beta} R^p \xrightarrow{\pi} M \to 0$$

presentations. Represent α, β by matrices $\mathbf{A}$, $\mathbf{B}$. Then $I_{m-r}(\mathbf{A}) = I_{p-r}(\mathbf{B})$.

Proof: First, assume $m = p$ and $\mu = \pi$. Set $K := \mathrm{Ker}(\mu)$. Then $\mathrm{Im}(\alpha) = K$ and $\mathrm{Im}(\beta) = K$ by exactness; so $\mathrm{Im}(\alpha) = \mathrm{Im}(\beta)$. But $\mathrm{Im}(\alpha)$ is generated by the columns of $\mathbf{A}$. Hence each column of $\mathbf{B}$ is a linear combination of the columns of $\mathbf{A}$. So there's a matrix $\mathbf{C}$ with $\mathbf{AC} = \mathbf{B}$. Set $s := m - r$. Then **(5.33)**(1) yields

$$I_s(\mathbf{B}) = I_s(\mathbf{AC}) \subset I_s(\mathbf{A}) I_s(\mathbf{C}) \subset I_s(\mathbf{A}).$$

Symmetrically, $I_s(\mathbf{A}) \subset I_s(\mathbf{B})$. Thus $I_s(\mathbf{A}) = I_s(\mathbf{B})$, as desired.

Second, assume $m = p$ and that there's an isomorphism $\gamma \colon R^m \to R^p$ with $\pi\gamma = \mu$. Represent γ by a matrix $\mathbf{G}$. Then $R^n \xrightarrow{\gamma\alpha} R^p \xrightarrow{\pi} M \to 0$ is a presentation, and $\mathbf{GA}$ represents $\gamma\alpha$. So, by the first paragraph, $I_s(\mathbf{B}) = I_s(\mathbf{GA})$. But $\mathbf{G}$ is invertible. So $I_s(\mathbf{GA}) = I_s(\mathbf{A})$ by **(5.33)**(2). Thus $I_s(\mathbf{A}) = I_s(\mathbf{B})$, as desired.

Third, assume that $q = n + t$ and $p = m + t$ for some $t \ge 1$ and that $\beta = \alpha \oplus 1_{R^t}$

and $\pi = \mu + 0$. Then $\mathbf{B} = \left(\begin{smallmatrix} \mathbf{A} & \mathbf{0}_{mt} \\ \mathbf{0}_{tn} & \mathbf{I}_t \end{smallmatrix}\right)$.

Given an $s \times s$ submatrix $\mathbf{C}$ of $\mathbf{A}$, set $\mathbf{D} := \left(\begin{smallmatrix} \mathbf{C} & \mathbf{0}_{st} \\ \mathbf{0}_{ts} & \mathbf{I}_t \end{smallmatrix}\right)$. Then $\mathbf{D}$ is an $(s+t) \times (s+t)$ submatrix of $\mathbf{B}$, and $\det(\mathbf{D}) = \det(\mathbf{C})$. Thus $I_s(\mathbf{A}) \subset I_{s+t}(\mathbf{B})$.

For the opposite inclusion, given an $(s+t) \times (s+t)$ submatrix $\mathbf{D}$ of $\mathbf{B}$, assume $\det(\mathbf{D}) \neq 0$. If $\mathbf{D}$ includes part of the $(m+i)$th row of $\mathbf{B}$, then $\mathbf{D}$ must also include part of the $(n+i)$th column, or $\mathbf{D}$ would have an all zero row. Similarly, if $\mathbf{D}$ includes part of the $(n+i)$th column, then $\mathbf{D}$ must include part of the $(m+i)$th row. So $\mathbf{D}\left(\begin{smallmatrix} \mathbf{C} & \mathbf{0}_{hk} \\ \mathbf{0}_{k\,h} & \mathbf{I}_k \end{smallmatrix}\right)$ where $h := s + t - k$ for some $k \leq t$ and for some $h \times h$ submatrix $\mathbf{C}$ of $\mathbf{A}$. But $\det(\mathbf{D}) = \det(\mathbf{C})$. So $\det(\mathbf{D}) \in I_h(\mathbf{A})$. But $I_h(\mathbf{A}) \subset I_s(\mathbf{A})$ by **(5.31.2)**. So $\det(\mathbf{D}) \in I_s(\mathbf{A})$. Thus $I_{s+t}(\mathbf{B}) \subset I_s(\mathbf{A})$. Thus $I_{s+t}(\mathbf{B}) = I_s(\mathbf{A})$, or $I_{m-r}(\mathbf{A}) = I_{p-r}(\mathbf{B})$, as desired.

Finally, in general, Schanuel's Lemma **(5.17)** yields the commutative diagram

$$\begin{tikzcd}
R^n \oplus R^p \arrow[r, "\alpha\oplus 1_{R^p}"] & R^m \oplus R^p \arrow[r, "\mu+0"] \arrow[d, "\gamma", "\simeq"'] & M \arrow[r] \arrow[d, "1_M", "="'] & 0 \\
R^m \oplus R^q \arrow[r, "1_{R^m}\oplus\beta"] & R^m \oplus R^p \arrow[r, "0+\pi"] & M \arrow[r] & 0
\end{tikzcd}$$

Thus, by the last two paragraphs, $I_{m-r}(\mathbf{A}) = I_{p-r}(\mathbf{B})$, as desired. □

(5.35) (Fitting Ideals). — Let R be a ring, M a finitely presented module, r an integer. Take any presentation $R^n \xrightarrow{\alpha} R^m \to M \to 0$, let $\mathbf{A}$ be the matrix of α, and define the rth **Fitting ideal** of M by

$$F_r(M) := I_{m-r}(\mathbf{A}).$$

It is independent of the choice of presentation by **(5.34)**.

By definition, $F_r(M)$ is finitely generated. Also, **(5.31.2)** and **(5.31.1)** yield

$$\langle 0 \rangle = F_{-1}(M) \subset F_0(M) \subset \cdots \subset F_m(M) = R. \tag{5.35.1}$$

Exercise (5.36) . — Let R be a ring, and $a_1, \ldots, a_m \in R$ with $\langle a_1 \rangle \supset \cdots \supset \langle a_m \rangle$. Set $M := R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_m \rangle$. Show that $F_r(M) = \langle a_1 \cdots a_{m-r} \rangle$.

Exercise (5.37) . — In the setup of **(5.36)**, assume a_1 is a nonunit. Show:

(1) Then m is the smallest integer such that $F_m(M) = R$.

(2) Let n be the largest integer with $F_n(M) = \langle 0 \rangle$; set $k := m - n$. Assume R is a domain. Then (a) $a_i \neq 0$ for $i < k$ and $a_i = 0$ for $i \geq k$, and (b) each a_i is unique up to unit multiple.

Theorem (5.38) (Elementary Divisors). — *Let R be a* PID*, M a free module, N a free submodule of rank $n < \infty$. Then there's a decomposition $M = M' \oplus M''$, a basis $x_1, \ldots, x_n$ of M', and $d_1, \ldots, d_n \in R$, unique up to unit multiple, with*

$$M' = Rx_1 \oplus \cdots \oplus Rx_n, \quad N = Rd_1x_1 \oplus \cdots \oplus Rd_nx_n, \quad d_1 \mid \cdots \mid d_n \neq 0.$$

Moreover, set $Q := \{m \in M \mid xm \in N \text{ for some nonzero } x \in R\}$. Then $M' = Q$.

Proof: Let's prove existence by induction on n. For $n = 0$, take $M' := 0$; no d_i or x_i are needed. So $M'' = M$, and the displayed conditions are trivially satisfied.

Let $\{e_\lambda\}$ be a basis of M, and $\pi_\lambda \colon M \to R$ the λth projection.

Assume $n > 0$. Given any nonzero $z \in N$, write $z = \sum c_\lambda e_\lambda$ for some $c_\lambda \in R$. Then some $c_{\lambda_0} \neq 0$. But $c_{\lambda_0} = \pi_{\lambda_0}(z)$. Thus $\pi_{\lambda_0}(N) \neq 0$.

Consider the set $\mathcal{S}$ of nonzero ideals of the form $\alpha(N)$ where $\alpha \colon M \to R$ is a linear map. Partially order $\mathcal{S}$ by inclusion. Given a totally ordered subset $\{\alpha_\nu(N)\}$, set

$\mathfrak{b} := \bigcup \alpha_\nu(N)$. Then $\mathfrak{b}$ is an ideal. So $\mathfrak{b} = \langle b\rangle$ for some $b \in R$ as R is a PID. Then $b \in \alpha_\nu(N)$ for some ν. So $\alpha_\nu(N) = \mathfrak{b}$. By Zorn's Lemma, $\mathcal{S}$ has a maximal element, say $\alpha_1(N)$. Fix $d_1 \in R$ with $\alpha_1(N) = \langle d_1\rangle$, and fix $y_1 \in N$ with $\alpha_1(y_1) = d_1$.

Given any linear map $\beta\colon M \to R$, set $b := \beta(y_1)$. Then $\langle d_1\rangle + \langle b\rangle = \langle c\rangle$ for some $c \in R$, as R is a PID. Write $c = dd_1 + eb$ for $d, e \in R$, and set $\gamma := d\alpha_1 + e\beta$. Then $\gamma(N) \supset \langle \gamma(y_1)\rangle$. But $\gamma(y_1) = c$. So $\langle c\rangle \subset \gamma(N)$. But $\langle d_1\rangle \subset \langle c\rangle$. Hence, by maximality, $\langle d_1\rangle = \gamma(N)$. But $\langle b\rangle \subset \langle c\rangle$. Thus $\beta(y_1) = b \in \langle d_1\rangle$.

Write $y_1 = \sum c_\lambda e_\lambda$ for some $c_\lambda \in R$. Then $\pi_\lambda(y_1) = c_\lambda$. But $c_\lambda = d_1 d_\lambda$ for some $d_\lambda \in R$ by the above paragraph with $\beta := \pi_\lambda$. Set $x_1 := \sum d_\lambda e_\lambda$. Then $y_1 = d_1 x_1$.

So $\alpha_1(y_1) = d_1\alpha_1(x_1)$. But $\alpha_1(y_1) = d_1$. So $d_1\alpha_1(x_1) = d_1$. But R is a domain and $d_1 \neq 0$. Thus $\alpha_1(x_1) = 1$.

Set $M_1 := \mathrm{Ker}(\alpha_1)$. As $\alpha_1(x_1) = 1$, clearly $Rx_1 \cap M_1 = 0$. Also, given $x \in M$, write $x = \alpha_1(x)x_1 + (x - \alpha_1(x)x_1)$; thus $x \in Rx_1 + M_1$. Hence **(4.25)** implies $M = Rx_1 \oplus M_1$. Further, Rx_1 and M_1 are free by **(4.12)**. Set $N_1 := M_1 \cap N$.

Recall $d_1x_1 = y_1 \in N$. So $N \supset Rd_1x_1 \oplus N_1$. Conversely, given $y \in N$, write $y = bx_1 + m_1$ with $b \in R$ and $m_1 \in M_1$. Then $\alpha_1(y) = b$, so $b \in \langle d_1\rangle$. Hence $y \in Rd_1x_1 + N_1$. Thus $N = Rd_1x_1 \oplus N_1$.

Define $\varphi\colon R \to Rd_1x_1$ by $\varphi(a) = ad_1x_1$. If $\varphi(a) = 0$, then $ad_1 = 0$ as $\alpha_1(x_1) = 1$, and so $a = 0$ as $d_1 \neq 0$. Thus φ is injective, so a isomorphism.

Note $N_1 \simeq R^m$ with $m \le n$ owing to **(4.12)** with N for E. Hence $N \simeq R^{m+1}$. But $N \simeq R^n$. So **(5.32)**(2) yields $m + 1 = n$.

By induction on n, there exist a decomposition $M_1 = M_1' \oplus M''$, a basis $x_2, \ldots, x_n$ of M_1' and $d_2, \ldots, d_n \in R$ with

$$M_1' = Rx_2 \oplus \cdots \oplus Rx_n,\ \ N_1 = Rd_2x_2 \oplus \cdots \oplus Rd_nx_n,\ \ d_2 \mid \cdots \mid d_n \neq 0.$$

Then $M = M' \oplus M''$ and $M' = Rx_1 \oplus \cdots \oplus Rx_n$ and $N = Rd_1x_1 \oplus \cdots \oplus Rd_nx_n$. Now, Rx_1 is free, and $x_2, \ldots, x_n$ form a basis of M_1', and $M' = Rx_1 \oplus M_1'$; thus, $x_1, \ldots, x_n$ form a basis of M_1.

Next, consider the projection $\pi\colon M_1 \to R$ with $\pi(x_j) = \delta_{2j}$ for $j \le 2 \le n$ and $\pi|M'' = 0$. Define $\rho\colon M \to R$ by $\rho(ax_1 + m_1) := a + \pi(m_1)$. Then $\rho(d_1x_1) = d_1$. So $\rho(N) \supset \langle d_1\rangle = \alpha_1(N)$. By maximality, $\rho(N) = \alpha_1(N)$. But $d_2 = \rho(d_2x_2) \in \rho(N)$. Thus $d_2 \in \langle d_1\rangle$; that is, $d_1 \mid d_2$. Thus $d_1 \mid \cdots \mid d_n \neq 0$.

Moreover, given $m \in M'$, note $xm \in N$ where $x := d_1 \cdots d_n$; so $M' \subset Q$. Conversely, given $m \in Q$, say $xm \in N$ with $x \in R$ nonzero. Say $m = m' + m''$ with $m' \in M'$ and $m'' \in M''$. Then $xm'' = xm - xm' \in M'$ as $N \subset M'$. But $M' \cap M'' = 0$. So $xm'' = 0$. But M is free, x is nonzero, and R is a domain. So $m'' = 0$. So $m = m' \in M'$. Thus $M' \supset Q$. Thus $M'' = Q$.

Finally, note $M'/N = R/\langle d_1\rangle \oplus \cdots \oplus R/\langle d_m\rangle$ by **(5.3)** and **(5.4)**. Thus, by **(5.37)**(2), each d_i is unique up to unit multiple. □

Theorem (5.39). — *Let A be a local ring, M a finitely presented module.*

(1) *Then M can be generated by m elements if and only if $F_m(M) = A$.*

(2) *Then M is free of rank m if and only if $F_m(M) = A$ and $F_{m-1}(M) = \langle 0\rangle$.*

Proof: For (1), assume M can be generated by m elements. Then **(5.13)** yields a presentation $A^n \xrightarrow{\alpha} A^m \to M \to 0$ for some n. So $F_m(M) = A$ by **(5.31.1)**.

For the converse, assume $F_k(M) = A$ for some $k < m$. Then $F_{m-1}(M) = A$ by **(5.35.1)**. Hence one entry of the matrix (a_{ij}) of α does not belong to the maximal ideal, so is a unit by **(3.5)**. By **(5.33)**(2), we may assume $a_{11} = 1$ and the other entries in the first row and first column of $\mathbf{A}$ are 0. Thus $\mathbf{A} = \left(\begin{smallmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{B}\end{smallmatrix}\right)$ where $\mathbf{B}$ is an

$(m-1)\times(s-1)$ matrix. Then $\mathbf{B}$ defines a presentation $A^{s-1}\to A^{m-1}\to M\to 0$. So M can be generated by $m-1$ elements. Repeating, we see that M can be generated by k elements, as desired. Thus (1) holds.

In (2), if M is free of rank m, then there's a presentation $0\to A^m\to M\to 0$; so $F_m(M)=A$ and $F_{m-1}(M)=\langle 0\rangle$ by **(5.35)**. Conversely, if $F_m(M)=A$, then (1) and **(5.13)** yield a presentation $A^s \xrightarrow{\alpha} A^m \to M\to 0$ for some s. If also $F_{m-1}(M)=\langle 0\rangle$, then $\alpha=0$ by **(5.35)**. Thus M is free of rank m; so (2) holds. □

Proposition (5.40). — *Let R be a ring, and M a finitely presented module. Say M can be generated by m elements. Set $\mathfrak{a}:=\mathrm{Ann}(M)$. Then*

$$(1)\ \ \mathfrak{a}F_r(M)\subset F_{r-1}(M)\ \textit{for all}\ r>0 \quad \textit{and} \quad (2)\ \ \mathfrak{a}^m\subset F_0(M)\subset\mathfrak{a}.$$

Proof: As M can be generated by m elements, **(5.13)** yields a presentation $A^n \xrightarrow{\alpha} A^m \xrightarrow{\mu} M\to 0$ for some n. Say α has matrix $\mathbf{A}$.

In (1), if $r>m$, then trivially $\mathfrak{a}F_r(M)\subset F_{r-1}(M)$ owing to **(5.35.1)**. So assume $r\le m$ and set $s:=m-r+1$. Given $x\in\mathfrak{a}$, form the sequence

$$R^{n+m}\xrightarrow{\beta} R^m \xrightarrow{\mu} M\to 0 \text{ with } \beta:=\alpha+x1_{R^m}.$$

Note that this sequence is a presentation. Also, the matrix of β is $(\mathbf{A}|x\mathbf{I}_m)$, obtained by juxtaposition, where $\mathbf{I}_m$ is the $m\times m$ identity matrix.

Given an $(s-1)\times(s-1)$ submatrix $\mathbf{B}$ of $\mathbf{A}$, enlarge it to an $s\times s$ submatrix $\mathbf{B}'$ of $(\mathbf{A}|x\mathbf{I}_m)$ as follows: say the ith row of $\mathbf{A}$ is not involved in $\mathbf{B}$; form the $m\times s$ submatrix $\mathbf{B}''$ of $(\mathbf{A}|x\mathbf{I}_m)$ with the same columns as $\mathbf{B}$ plus the ith column of $x\mathbf{I}_m$ at the end; finally, form $\mathbf{B}'$ as the $s\times s$ submatrix of $\mathbf{B}''$ with the same rows as $\mathbf{B}$ plus the ith row in the appropriate position.

Expanding along the last column yields $\det(\mathbf{B}')=\pm x\det(\mathbf{B})$. By constuction, $\det(\mathbf{B}')\in I_s(\mathbf{A}|x\mathbf{I}_m)$. But $I_s(\mathbf{A}|x\mathbf{I}_m)=I_s(\mathbf{A})$ by **(5.34)**. Furthermore, $x\in\mathfrak{a}$ is arbitrary, and $I_m(\mathbf{A})$ is generated by all possible $\det(\mathbf{B})$. Thus (1) holds.

For (2), apply (1) repeatedly to get $\mathfrak{a}^kF_r(M)\subset F_{r-k}(M)$ for all r and k. But $F_m(M)=R$ by **(5.35.1)**. So $\mathfrak{a}^m\subset F_0(M)$.

For the second inclusion, given any $m\times m$ submatrix $\mathbf{B}$ of $\mathbf{A}$, say $\mathbf{B}=(b_{ij})$. Let $\mathbf{e}_i$ be the ith standard basis vector of R^m. Set $m_i:=\mu(\mathbf{e}_i)$. Then $\sum b_{ij}m_j=0$ for all i. Let $\mathbf{C}$ be the matrix of cofactors of $\mathbf{B}$: the (i,j)th entry of $\mathbf{C}$ is $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the jth row and the ith column of $\mathbf{B}$. Then $\mathbf{CB}=\det(\mathbf{B})\mathbf{I}_m$. Hence $\det(\mathbf{B})m_i=0$ for all i. So $\det(\mathbf{B})\in\mathfrak{a}$. But $I_m(\mathbf{A})$ is generated by all such $\det(\mathbf{B})$. Thus $F_0(M)\subset\mathfrak{a}$. Thus (2) holds. □

D. Appendix: Exercises

Exercise (5.41) (*Structure Theorem***) .** — Let R be a PID, M a finitely generated module. Set $T:=\{m\in M \mid xm=0 \text{ for some nonzero } x\in R\}$. Show:

(1) Then M has a free submodule F of finite rank with $M=T\oplus F$.

(2) Then $T\simeq\bigoplus_{j=1}^n R/\langle d_j\rangle$ with the d_j nonzero nonunits in R, unique up to unit multiple, and $d_j \mid d_{j+1}$ for $1\le j<n$.

(3) Then $T\simeq\bigoplus_{i=1}^m M(p_i)$ with $M(p_i):=\bigoplus_{j=1}^n R/\langle p_i^{e_{ij}}\rangle$, the p_i primes in R, unique up to unit multiple, and the e_{ij} unique with $0\le e_{ij}\le e_{i\,j+1}$ and $1\le e_{in}$.

(4) If M isn't finitely generated, there may be no free F with $M=T\oplus F$.

Exercise (5.42) . — Criticize the following misstatement of (5.8): given a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$, there is an isomorphism $M \simeq M' \oplus M''$ if and only if there is a section $\sigma\colon M'' \to M$ of β and α is injective.

Moreover, show that this construction (due to B. Noohi) yields a counterexample: For each integer $n \geq 2$, let M_n be the direct sum of countably many copies of $\mathbb{Z}/\langle n\rangle$. Set $M := \bigoplus M_n$. Then let p be a prime number, and take M' to be a cyclic subgroup of order p of one of the components of M isomorphic to $\mathbb{Z}/\langle p^2\rangle$.

6. Direct Limits

Category theory provides the right abstract setting for certain common concepts, constructions, and proofs. Here we treat adjoints and direct limits. We elaborate on two key special cases of direct limits: coproducts (direct sums) and coequalizers (cokernels). From them, we construct arbitrary direct limits of sets and of modules. Further, we prove direct limits are preserved by left adjoints; hence, direct limits commute with each other, and in particular, with coproducts and coequalizers.

Although this chapter is the most abstract of the entire book, all the material here is elementary, and none of it is very deep. In fact, the abstract statements here are, largely, just concise restatements, in more expressive language, of the essence of some mundane statements in Commutative Algebra. Experience shows that it pays to learn this more abstract language, but that doing so requires determined, yet modest effort.

A. Text

(6.1) (Categories). — A **category** $\mathcal{C}$ is a collection of elements, called **objects**. Each pair of objects A, B is equipped with a set $\mathrm{Hom}_{\mathcal{C}}(A,B)$ of elements, called **maps** or **morphisms**. We write $\alpha\colon A \to B$ or $A \xrightarrow{\alpha} B$ to mean $\alpha \in \mathrm{Hom}_{\mathcal{C}}(A,B)$.

Further, given objects A, B, C, there is a **composition law**

$$\mathrm{Hom}_{\mathcal{C}}(A,B) \times \mathrm{Hom}_{\mathcal{C}}(B,C) \to \mathrm{Hom}_{\mathcal{C}}(A,C), \quad \text{written} \quad (\alpha,\beta) \mapsto \beta\alpha,$$

and there is a distinguished map $1_B \in \mathrm{Hom}_{\mathcal{C}}(B,B)$, called the **identity** such that

(1) composition is **associative**, or $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ for $\gamma\colon C \to D$, and
(2) 1_B is **unitary**, or $1_B\alpha = \alpha$ and $\beta 1_B = \beta$.

We say α is an **isomorphism** with **inverse** $\beta\colon B \to A$ if $\alpha\beta = 1_B$ and $\beta\alpha = 1_A$.

For example, four common categories are those of sets ((Sets)), of rings ((Rings)), of R-modules ((R-mod)), and of R-algebras ((R-alg)); the corresponding maps are the set maps, and the ring, R-module, and R-algebra homomorphisms.

Given categories $\mathcal{C}$ and $\mathcal{C}'$, their **product** $\mathcal{C} \times \mathcal{C}'$ is the category whose objects are the pairs (A, A') with A an object of $\mathcal{C}$ and A' an object of $\mathcal{C}'$ and whose maps are the pairs (α, α') of maps α in $\mathcal{C}$ and α' in $\mathcal{C}'$.

(6.2) (Functors). — A map of categories is known as a functor. Namely, given categories $\mathcal{C}$ and $\mathcal{C}'$, a (**covariant**) **functor** $F\colon \mathcal{C} \to \mathcal{C}'$ is a rule that assigns to each object A of $\mathcal{C}$ an object $F(A)$ of $\mathcal{C}'$ and to each map $\alpha\colon A \to B$ of $\mathcal{C}$ a map $F(\alpha)\colon F(A) \to F(B)$ of $\mathcal{C}'$ preserving composition and identity; that is,

(1) $F(\beta\alpha) = F(\beta)F(\alpha)$ for maps $\alpha\colon A \to B$ and $\beta\colon B \to C$ of $\mathcal{C}$, and
(2) $F(1_A) = 1_{F(A)}$ for any object A of $\mathcal{C}$.

We also denote a functor F by $F(\bullet)$, by $A \mapsto F(A)$, or by $A \mapsto F_A$.

Note that a functor F preserves isomorphisms. Indeed, if $\alpha\beta = 1_B$ and $\beta\alpha = 1_A$, then $F(\alpha)F(\beta) = F(1_B) = 1_{F(B)}$ and $F(\beta)F(\alpha) = 1_{F(A)}$.

For example, let R be a ring, M a module. Then clearly $\mathrm{Hom}_R(M, \bullet)$ is a functor from ((R-mod)) to ((R-mod)). A second example is the **forgetful functor** from ((R-mod)) to ((Sets)); it sends a module to its underlying set and a homomorphism to its underlying set map.

A map of functors is known as a natural transformation. Namely, given two functors $F,\ F'\colon \mathcal{C} \rightrightarrows \mathcal{C}'$, a **natural transformation** $\theta\colon F \to F'$ is a collection of maps $\theta(A)\colon F(A) \to F'(A)$, one for each object A of $\mathcal{C}$, such that $\theta(B)F(\alpha) = F'(\alpha)\theta(A)$ for every map $\alpha\colon A \to B$ of $\mathcal{C}$; that is, the following diagram is commutative:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(\alpha)} & F(B) \\ {\scriptstyle\theta(A)}\downarrow & & {\scriptstyle\theta(B)}\downarrow \\ F'(A) & \xrightarrow{F'(\alpha)} & F'(B) \end{array}$$

For example, the identity maps $1_{F(A)}$ trivially form a natural transformation 1_F from any functor F to itself. We call F and F' **isomorphic** if there are natural transformations $\theta\colon F \to F'$ and $\theta'\colon F' \to F$ with $\theta'\theta = 1_F$ and $\theta\theta' = 1_{F'}$.

A **contravariant** functor G from $\mathcal{C}$ to $\mathcal{C}'$ is a rule similar to F, but G reverses the direction of maps; that is, $G(\alpha)$ carries $G(B)$ to $G(A)$, and G satisfies the analogues of (1) and (2). For example, fix a module N; then $\mathrm{Hom}(\bullet, N)$ is a contravariant functor from $((R\text{-mod}))$ to $((R\text{-mod}))$.

(6.3) (Adjoints). — Let $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ be functors. We call $(F,\ F')$ an **adjoint pair**, F the **left adjoint** of F', and F' the **right adjoint** of F if, for every pair of objects $A \in \mathcal{C}$ and $A' \in \mathcal{C}'$, there is given a natural bijection

$$\mathrm{Hom}_{\mathcal{C}'}(F(A),\ A') \ \simeq\ \mathrm{Hom}_{\mathcal{C}}(A,\ F'(A')). \tag{6.3.1}$$

Here **natural** means that maps $B \to A$ and $A' \to B'$ induce a commutative diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}'}(F(A),\ A') & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\ F'(A')) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}'}(F(B),\ B') & \simeq & \mathrm{Hom}_{\mathcal{C}}(B,\ F'(B')) \end{array}$$

Naturality serves to determine an adjoint up to canonical isomorphism. Indeed, let F and G be two left adjoints of F'. Given $A \in \mathcal{C}$, define $\theta(A)\colon G(A) \to F(A)$ to be the image of $1_{F(A)}$ under the adjoint bijections

$$\mathrm{Hom}_{\mathcal{C}'}(F(A),\ F(A)) \ \simeq\ \mathrm{Hom}_{\mathcal{C}}(A,\ F'F(A)) \ \simeq\ \mathrm{Hom}_{\mathcal{C}'}(G(A),\ F(A)).$$

To see that $\theta(A)$ is natural in A, take a map $\alpha\colon A \to B$. It induces the following diagram, which is commutative owing to the naturality of the adjoint bijections:

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathcal{C}'}(F(A),\ F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\ F'F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}'}(G(A),\ F(A)) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}'}(F(A),\ F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\ F'F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}'}(G(A),\ F(B)) \\ \uparrow & & \uparrow & & \uparrow \\ \mathrm{Hom}_{\mathcal{C}'}(F(B),\ F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(B,\ F'F(B)) & \simeq & \mathrm{Hom}_{\mathcal{C}'}(G(B),\ F(B)) \end{array}$$

Chase after $1_{F(A)}$ and $1_{F(B)}$. Both map to $F(\alpha) \in \mathrm{Hom}_{\mathcal{C}'}(F(A),\ F(B))$. So both map to the same image in $\mathrm{Hom}_{\mathcal{C}'}(G(A),\ F(B))$. But clockwise, $1_{F(A)}$ maps to $F(\alpha)\theta(A)$; counterclockwise, $1_{F(B)}$ maps to $\theta(B)G(\alpha)$. So $\theta(B)G(\alpha) = F(\alpha)\theta(A)$. Thus the $\theta(A)$ form a natural transformation $\theta\colon G \to F$.

Similarly, there is a natural transformation $\theta'\colon F \to G$. It remains to show

$\theta'\theta = 1_G$ and $\theta\theta' = 1_F$. But, by naturality, the following diagram is commutative:

$$\begin{array}{ccccc} \mathrm{Hom}_{\mathcal{C}'}(F(A),\, F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\, F'F(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(G(A),\, F(A)) \\ \big\downarrow & & \big\downarrow & & \big\downarrow \\ \mathrm{Hom}_{\mathcal{C}'}(F(A),\, G(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(A,\, F'G(A)) & \simeq & \mathrm{Hom}_{\mathcal{C}}(G(A),\, G(A)) \end{array}$$

Chase after $1_{F(A)}$. Clockwise, its image is $\theta'(A)\theta(A)$ in the lower right corner. Counterclockwise, its image is $1_{G(A)}$, owing to the definition of θ'. Thus $\theta'\theta = 1_G$. Similarly, $\theta\theta' = 1_F$, as required.

For example, the "free module" functor is the left adjoint of the forgetful functor from $((R\text{-mod}))$ to $((\text{Sets}))$, since owing to **(4.10)**,

$$\mathrm{Hom}_{((R\text{-mod}))}(R^{\oplus\Lambda},\, M) = \mathrm{Hom}_{((\text{Sets}))}(\Lambda,\, M).$$

Similarly, the "polynomial ring" functor is the left adjoint of the forgetful functor from $((R\text{-alg}))$ to $((\text{Sets}))$, since owing to **(1.3)**,

$$\mathrm{Hom}_{((R\text{-alg}))}\big(R[X_1, \dots, X_n],\, R'\big) = \mathrm{Hom}_{((\text{Sets}))}\big(\{X_1, \dots, X_n\},\, R'\big).$$

(6.4) (Direct limits). — Let Λ, $\mathcal{C}$ be categories. Assume Λ is **small**; that is, its objects form a set. Given a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$, its **direct limit** or **colimit**, denoted $\varinjlim M_\lambda$ or $\varinjlim_{\lambda\in\Lambda} M_\lambda$, is defined to be the object of $\mathcal{C}$ universal among objects P equipped with maps $\beta_\mu\colon M_\mu \to P$, called **insertions**, that are compatible with the **transition maps** $\alpha^\kappa_\mu\colon M_\kappa \to M_\mu$, which are the images of the maps of Λ. (Note: given κ and μ, there may be more than one map $\kappa \to \mu$, and so more than one transition map α^κ_μ.) In other words, there is a unique map β such that all of the following diagrams commute:

$$\begin{array}{ccccc} M_\kappa & \xrightarrow{\alpha^\kappa_\mu} & M_\mu & \xrightarrow{\alpha_\mu} & \varinjlim M_\lambda \\ \big\downarrow{\scriptstyle\beta_\kappa} & & \big\downarrow{\scriptstyle\beta_\mu} & & \big\downarrow{\scriptstyle\beta} \\ P & \xrightarrow{1_P} & P & \xrightarrow{1_P} & P \end{array}$$

To indicate this context, the functor $\lambda \mapsto M_\lambda$ is often called a **direct system.**

As usual, universality implies that, once equipped with its insertions α_μ, the limit $\varinjlim M_\lambda$ is determined up to unique isomorphism, assuming it exists. In practice, there is usually a canonical choice for $\varinjlim M_\lambda$, given by a construction. In any case, let us use $\varinjlim M_\lambda$ to denote a particular choice.

We say that $\mathcal{C}$ **has direct limits indexed by** Λ if, for every functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$, the direct limit $\varinjlim M_\lambda$ exists. We say that $\mathcal{C}$ **has direct limits** if it has direct limits indexed by every small category Λ.

Given a functor $F\colon \mathcal{C} \to \mathcal{C}'$, note that a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$ yields a functor $\lambda \mapsto F(M_\lambda)$ from Λ to $\mathcal{C}'$. Furthermore, whenever the corresponding two direct limits exist, the maps $F(\alpha_\mu)\colon F(M_\mu) \to F(\varinjlim M_\lambda)$ induce a canonical map

$$\varphi_F\colon \varinjlim F(M_\lambda) \to F(\varinjlim M_\lambda). \tag{6.4.1}$$

If φ_F is always an isomorphism, we say F **preserves direct limits**. At times, given $\varinjlim M_\lambda$, we construct $\varinjlim F(M_\lambda)$ by showing $F(\varinjlim M_\lambda)$ has the requisite UMP.

Assume $\mathcal{C}$ has direct limits indexed by Λ. Then, given a natural transformation from $\lambda \mapsto M_\lambda$ to $\lambda \mapsto N_\lambda$, universality yields unique commutative diagrams

$$\begin{array}{ccc} M_\mu & \to & \varinjlim M_\lambda \\ \downarrow & & \downarrow \\ N_\mu & \longrightarrow & \varinjlim N_\lambda \end{array}$$

To put it in another way, form the **functor category** $\mathcal{C}^\Lambda$: its objects are the functors $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$; its maps are the natural transformations (they form a set as Λ is one). Then taking direct limits yields a functor $\varinjlim$ from $\mathcal{C}^\Lambda$ to $\mathcal{C}$.

In fact, it is just a restatement of the definitions that the "direct limit" functor $\varinjlim$ is the left adjoint of the **diagonal functor**

$$\Delta\colon \mathcal{C} \to \mathcal{C}^\Lambda.$$

By definition, Δ sends each object M to the **constant functor** ΔM, which has the same value M at every $\lambda \in \Lambda$ and has the same value 1_M at every map of Λ; further, Δ carries a map $\gamma\colon M \to N$ to the natural transformation $\Delta\gamma\colon \Delta M \to \Delta N$, which has the same value γ at every $\lambda \in \Lambda$.

(6.5) (Coproducts). — Let $\mathcal{C}$ be a category, Λ a set, and M_λ an object of $\mathcal{C}$ for each $\lambda \in \Lambda$. The **coproduct** $\coprod_{\lambda\in\Lambda} M_\lambda$, or simply $\coprod M_\lambda$, is defined as the object of $\mathcal{C}$ universal among objects P equipped with a map $\beta_\mu\colon M_\mu \to P$ for each $\mu \in \Lambda$. The maps $\iota_\mu\colon M_\mu \to \coprod M_\lambda$ are called the **inclusions**. Thus, given such a P, there exists a unique map $\beta\colon \coprod M_\lambda \to P$ with $\beta\iota_\mu = \beta_\mu$ for all $\mu \in \Lambda$.

If $\Lambda = \emptyset$, then the coproduct is an object B with a unique map β to every other object P. There are no μ in Λ, so no inclusions $\iota_\mu\colon M_\mu \to B$, so no equations $\beta\iota_\mu = \beta_\mu$ to restrict β. Such a B is called an **initial object**.

For instance, suppose $\mathcal{C} = ((R\text{-mod}))$. Then the zero module is an initial object. For any Λ, the coproduct $\coprod M_\lambda$ is just the direct sum $\bigoplus M_\lambda$ (a convention if $\Lambda = \emptyset$). Next, suppose $\mathcal{C} = ((\text{Sets}))$. Then the empty set is an initial object. For any Λ, the coproduct $\coprod M_\lambda$ is the disjoint union $\bigsqcup M_\lambda$ (a convention if $\Lambda = \emptyset$).

Note that the coproduct is a special case of the direct limit. Indeed, regard Λ as a **discrete** category: its objects are the $\lambda \in \Lambda$, and it has just the required maps, namely, the 1_λ. Then $\varinjlim M_\lambda = \coprod M_\lambda$ with the insertions equal to the inclusions.

(6.6) (Coequalizers). — Let $\alpha, \alpha'\colon M \rightrightarrows N$ be two maps in a category $\mathcal{C}$. Their **coequalizer** is defined as the object of $\mathcal{C}$ universal among objects P equipped with a map $\eta\colon N \to P$ such that $\eta\alpha = \eta\alpha'$.

For instance, if $\mathcal{C} = ((R\text{-mod}))$, then the coequalizer is $\operatorname{Coker}(\alpha - \alpha')$. In particular, the coequalizer of α and 0 is just $\operatorname{Coker}(\alpha)$.

Suppose $\mathcal{C} = ((\text{Sets}))$. Take the smallest equivalence relation $\sim$ on N with $\alpha(m) \sim \alpha'(m)$ for all $m \in M$; explicitly, $n \sim n'$ if there are elements $m_1, \dots, m_r$ with $\alpha(m_1) = n$, with $\alpha'(m_r) = n'$, and with $\alpha(m_i) = \alpha'(m_{i-1})$ for $1 < i \le r$. Clearly, the coequalizer is the quotient $N/{\sim}$ equipped with the quotient map.

Note that the coequalizer is a special case of the direct limit. Indeed, let Λ be the category consisting of two objects κ, μ and two nontrivial maps $\varphi, \varphi'\colon \kappa \rightrightarrows \mu$. Define $\lambda \mapsto M_\lambda$ in the obvious way: set $M_\kappa := M$ and $M_\mu := N$; send φ to α and φ' to α'. Then the coequalizer is $\varinjlim M_\lambda$.

Lemma (6.7). — *A category $\mathcal{C}$ has direct limits if and only if $\mathcal{C}$ has coproducts and coequalizers. If a category $\mathcal{C}$ has direct limits, then a functor $F\colon \mathcal{C} \to \mathcal{C}'$ preserves them if and only if F preserves coproducts and coequalizers.*

Proof: If $\mathcal{C}$ has direct limits, then $\mathcal{C}$ has coproducts and coequalizers because they are special cases by (**6.5**) and (**6.6**). By the same token, if $F\colon \mathcal{C} \to \mathcal{C}'$ preserves direct limits, then F preserves coproducts and coequalizers.

Conversely, assume that $\mathcal{C}$ has coproducts and coequalizers. Let Λ be a small category, and $\lambda \mapsto M_\lambda$ a functor from Λ to $\mathcal{C}$. Let Σ be the set of all transition maps $\alpha^\lambda_\mu\colon M_\lambda \to M_\mu$. For each $\sigma := \alpha^\lambda_\mu \in \Sigma$, set $M_\sigma := M_\lambda$. Set $M := \coprod_{\sigma\in\Sigma} M_\sigma$ and $N := \coprod_{\lambda\in\Lambda} M_\lambda$. For each σ, there are two maps $M_\sigma := M_\lambda \to N$: the inclusion ι_λ and the composition $\iota_\mu\alpha^\lambda_\mu$. Correspondingly, there are two maps $\alpha, \alpha'\colon M \to N$. Let C be their coequalizer, and $\eta\colon N \to C$ the insertion.

Given maps $\beta_\lambda\colon M_\lambda \to P$ with $\beta_\mu\alpha^\lambda_\mu = \beta_\lambda$, there is a unique map $\beta\colon N \to P$ with $\beta\iota_\lambda = \beta_\lambda$ by the UMP of the coproduct. Clearly $\beta\alpha = \beta\alpha'$; so β factors uniquely through C by the UMP of the coequalizer. Thus $C = \varinjlim M_\lambda$, as desired.

Finally, if $F\colon \mathcal{C} \to \mathcal{C}'$ preserves coproducts and coequalizers, then F preserves arbitrary direct limits as F preserves the above construction. □

Theorem (6.8). — *The categories* $((R\text{-mod}))$ *and* $((\text{Sets}))$ *have direct limits.*

Proof: The assertion follows from (**6.7**) because $((R\text{-mod}))$ and $((\text{Sets}))$ have coproducts by (**6.5**) and have coequalizers by (**6.6**). □

Theorem (6.9). — *Every left adjoint* $F\colon \mathcal{C} \to \mathcal{C}'$ *preserves direct limits.*

Proof: Let Λ be a small category, $\lambda \mapsto M_\lambda$ a functor from Λ to $\mathcal{C}$ such that $\varinjlim M_\lambda$ exists. Given an object P' of $\mathcal{C}'$, consider all possible commutative diagrams

$$\begin{array}{ccccc} F(M_\kappa) & \xrightarrow{F(\alpha^\kappa_\mu)} & F(M_\mu) & \xrightarrow{F(\alpha_\mu)} & F(\varinjlim M_\lambda) \\ \big\downarrow{\scriptstyle \beta'_\kappa} & & \big\downarrow{\scriptstyle \beta'_\mu} & & \big\downarrow{\scriptstyle \beta'} \\ P' & \xrightarrow{\quad 1 \quad} & P' & \xrightarrow{\quad 1 \quad} & P' \end{array} \tag{6.9.1}$$

where α^κ_μ is any transition map and α_μ is the corresponding insertion. Given the β'_κ, we must show there is a unique β'.

Say F is the left adjoint of $F'\colon \mathcal{C}' \to \mathcal{C}$. Then giving (**6.9.1**) is equivalent to giving this corresponding commutative diagram:

$$\begin{array}{ccccc} M_\kappa & \xrightarrow{\alpha^\kappa_\mu} & M_\mu & \xrightarrow{\alpha_\mu} & \varinjlim M_\lambda \\ \big\downarrow{\scriptstyle \beta_\kappa} & & \big\downarrow{\scriptstyle \beta_\mu} & & \big\downarrow{\scriptstyle \beta} \\ F'(P') & \xrightarrow{1} & F'(P') & \xrightarrow{1} & F'(P') \end{array}$$

However, given the β_κ, there is a unique β by the UMP of $\varinjlim M_\lambda$. □

Proposition (6.10). — *Let* $\mathcal{C}$ *be a category,* Λ *and* Σ *small categories. Assume* $\mathcal{C}$ *has direct limits indexed by* Σ*. Then the functor category* $\mathcal{C}^\Lambda$ *does too.*

Proof: Let $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$ be a functor from Σ to $\mathcal{C}^\Lambda$. Then a map $\sigma \to \tau$ in Σ yields a natural transformation from $\lambda \mapsto M_{\sigma\lambda}$ to $\lambda \mapsto M_{\tau\lambda}$. So a map $\lambda \to \mu$ in Λ yields a commutative square

$$\begin{array}{ccc} M_{\sigma\lambda} & \to & M_{\sigma\mu} \\ \big\downarrow & & \big\downarrow \\ M_{\tau\lambda} & \to & M_{\tau\mu} \end{array} \tag{6.10.1}$$

in a manner compatible with composition in Σ. Hence, with λ fixed, the rule $\sigma \mapsto M_{\sigma\lambda}$ is a functor from Σ to $\mathcal{C}$.

By hypothesis, $\varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda}$ exists. So $\lambda \mapsto \varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda}$ is a functor from Λ to $\mathcal{C}$. Further, as $\tau \in \Sigma$ varies, there are compatible natural transformations from the $\lambda \mapsto M_{\tau\lambda}$ to $\lambda \mapsto \varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda}$. Finally, the latter is the direct limit of the functor $\tau \mapsto (\lambda \mapsto M_{\tau\lambda})$ from Σ to $\mathcal{C}^\Lambda$, because, given any functor $\lambda \mapsto P_\lambda$ from Λ to $\mathcal{C}$ equipped with, for $\tau \in \Sigma$, compatible natural transformations from the $\lambda \mapsto M_{\tau\lambda}$ to $\lambda \mapsto P_\lambda$, there are, for $\lambda \in \Lambda$, compatible unique maps $\varinjlim_{\sigma\in\Sigma} M_{\sigma\lambda} \to P_\lambda$. □

Theorem (6.11) (Direct limits commute). — *Let $\mathcal{C}$ be a category with direct limits indexed by small categories Σ and Λ. Let $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$ be a functor from Σ to $\mathcal{C}^\Lambda$. Then*

$$\varinjlim_{\sigma\in\Sigma} \varinjlim_{\lambda\in\Lambda} M_{\sigma,\lambda} = \varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma} M_{\sigma,\lambda}.$$

Proof: By (**6.4**), the functor $\varinjlim_{\lambda\in\Lambda}\colon \mathcal{C}^\Lambda \to \mathcal{C}$ is a left adjoint. By (**6.10**), the category $\mathcal{C}^\Lambda$ has direct limits indexed by Σ. So (**6.9**) yields the assertion. □

Corollary (6.12). — *Let Λ be a small category, R a ring, and $\mathcal{C}$ either* ((Sets)) *or* ((R-mod)). *Then functor $\varinjlim\colon \mathcal{C}^\Lambda \to \mathcal{C}$ preserves coproducts and coequalizers.*

Proof: By (**6.5**) and (**6.6**), both coproducts and coequalizers are special cases of direct limits, and $\mathcal{C}$ has them. So (**6.11**) yields the assertion. □

B. Exercises

Exercise (6.13) . — (1) Show that the condition (**6.2**)(1) is equivalent to the commutativity of the corresponding diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(C)\big) \end{array} \qquad \textbf{(6.13.1)}$$

(2) Given $\gamma\colon C \to D$, show (**6.2**)(1) yields the commutativity of this diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B,C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B),F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A,D) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A),F(D)\big) \end{array}$$

Exercise (6.14) . — Let $\mathcal{C}$ and $\mathcal{C}'$ be categories, $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ an adjoint pair. Let $\varphi_{A,A'}\colon \mathrm{Hom}_{\mathcal{C}'}(FA,\, A') \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{C}}(A,\, F'A')$ denote the natural bijection, and set $\eta_A := \varphi_{A,FA}(1_{FA})$. Do the following:

(1) Prove η_A is natural in A; that is, given $g\colon A \to B$, the induced square

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & F'FA \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle F'Fg} \\ B & \xrightarrow{\eta_B} & F'FB \end{array}$$

is commutative. We call the natural transformation $A \mapsto \eta_A$ the **unit** of $(F,\, F')$.

(2) Given $f'\colon FA \to A'$, prove $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

(3) Prove the canonical map $\eta_A\colon A \to F'FA$ is **universal** from A to F'; that is, given $f\colon A \to F'A'$, there is a unique map $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$.

(4) Conversely, instead of assuming (F, F') is an adjoint pair, assume given a natural transformation $\eta\colon 1_{\mathcal{C}} \to F'F$ satisfying (1) and (3). Prove the equation in (2) defines a natural bijection making (F, F') an adjoint pair, whose unit is η.

(5) Identify the units in the two examples in (**6.3**): the "free module" functor and the "polynomial ring" functor.

(Dually, we can define a **counit** $\varepsilon\colon FF' \to 1_{\mathcal{C}'}$, and prove analogous statements.)

Exercise (6.15) . — Show that the canonical map $\varphi_F\colon \varinjlim F(M_\lambda) \to F(\varinjlim M_\lambda)$ of (6.4.1) is compatible with any natural transformation $\theta\colon F \to G$.

Exercise (6.16) . — Let $\alpha\colon L \to M$ and $\beta\colon L \to N$ be two maps in a category $\mathcal{C}$. Their **pushout** is defined as the object of $\mathcal{C}$ universal among objects P equipped with a pair of maps $\gamma\colon M \to P$ and $\delta\colon N \to P$ such that $\gamma\alpha = \delta\beta$. Express the pushout as a direct limit. Show that, in ((Sets)), the pushout is the disjoint union $M \sqcup N$ modulo the smallest equivalence relation $\sim$ with $m \sim n$ if there is $\ell \in L$ with $\alpha(\ell) = m$ and $\beta(\ell) = n$. Show that, in ((R-mod)), the pushout is equal to the direct sum $M \oplus N$ modulo the image of L under the map $(\alpha, -\beta)$.

Exercise (6.17) . — Let R be a ring, M a module, N a submodule, $\mathcal{X}$ a set of variable. Prove $M \mapsto M[X]$ is the left adjoint of the restriction of scalars from $R[\mathcal{X}]$ to R. As a consequence, reprove the equation $(M/N)[\mathcal{X}] = M[\mathcal{X}]/N[\mathcal{X}]$.

Exercise (6.18) . — Let $\mathcal{C}$ be a category, Σ and Λ small categories. Prove:

(1) Then $\mathcal{C}^{\Sigma\times\Lambda} = (\mathcal{C}^{\Lambda})^{\Sigma}$ with $(\sigma, \lambda) \mapsto M_{\sigma,\lambda}$ corresponding to $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$.

(2) Assume $\mathcal{C}$ has direct limits indexed by Σ and by Λ. Then $\mathcal{C}$ has direct limits indexed by $\Sigma \times \Lambda$, and $\varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma} = \varinjlim_{(\sigma,\lambda)\in\Sigma\times\Lambda}$.

Exercise (6.19) . — Let $\lambda \mapsto M_\lambda$ and $\lambda \mapsto N_\lambda$ be two functors from a small category Λ to ((R-mod)), and $\{\theta_\lambda\colon M_\lambda \to N_\lambda\}$ a natural transformation. Show

$$\varinjlim \operatorname{Coker}(\theta_\lambda) = \operatorname{Coker}(\varinjlim M_\lambda \to \varinjlim N_\lambda).$$

Show that the analogous statement for kernels can be false by constructing a counterexample using the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
\mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \to & \mathbb{Z}/\langle 2\rangle & \to & 0 \\
\downarrow{\scriptstyle \mu_2} & & \downarrow{\scriptstyle \mu_2} & & \downarrow{\scriptstyle \mu_2} & & \\
\mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \to & \mathbb{Z}/\langle 2\rangle & \to & 0
\end{array}$$

Exercise (6.20) . — Let R be a ring, M a module. Define the map

$$D(M)\colon M \to \operatorname{Hom}\big(\operatorname{Hom}(M, R), R\big) \quad \text{by} \quad \big(D(M)(m)\big)(\alpha) := \alpha(m).$$

If $D(M)$ is an isomorphism, call M **reflexive**. Show:

(1) $D : 1_{((R\text{-mod}))} \to \operatorname{Hom}\big(\operatorname{Hom}(\bullet, R), R\big)$ is a natural transformation.

(2) Let M_i for $1 \le i \le n$ be modules. Then $D(\bigoplus_{i=1}^n M_i) = \bigoplus_{i=1}^n D(M_i)$.

(3) Assume M is finitely generated and projective. Then M is reflexive.

7. Filtered Direct Limits

Filtered direct limits are direct limits indexed by a filtered category, which is a more traditional sort of index set. After making the definitions, we study an instructive example where the limit is $\mathbb{Q}$. Then we develop an alternative construction of filtered direct limits for modules. We conclude that forming them preserves exact sequences, and so commutes with forming the module of homomorphisms out of a fixed finitely presented source.

A. Text

(7.1) (Filtered categories). — We call a small category Λ **filtered** if

(1) given objects κ and λ, for some μ there are maps $\kappa \to \mu$ and $\lambda \to \mu$,
(2) given two maps $\sigma, \tau\colon \eta \rightrightarrows \kappa$ with the same source and the same target, for some μ there is a map $\varphi\colon \kappa \to \mu$ such that $\varphi\sigma = \varphi\tau$.

Given a category $\mathcal{C}$, we say a functor $\lambda \mapsto M_\lambda$ from Λ to $\mathcal{C}$ is **filtered** if Λ is filtered. If so, then we say the direct limit $\varinjlim M_\lambda$ is **filtered** if it exists.

For example, let Λ be a partially ordered set. Suppose Λ is **directed**; that is, given $\kappa, \lambda \in \Lambda$, there is a μ with $\kappa \le \mu$ and $\lambda \le \mu$. Regard Λ as a category whose objects are its elements and whose sets $\mathrm{Hom}(\kappa, \lambda)$ consist of a single element if $\kappa \le \lambda$, and are empty if not; morphisms can be composed, because the ordering is transitive. Clearly, the category Λ is filtered.

Exercise (7.2) . — Let R be a ring, M a module, Λ a set, M_λ a submodule for each $\lambda \in \Lambda$. Assume $\bigcup M_\lambda = M$. Assume, given λ, $\mu \in \Lambda$, there is $\nu \in \Lambda$ such that M_λ, $M_\mu \subset M_\nu$. Order Λ by inclusion: $\lambda \le \mu$ if $M_\lambda \subset M_\mu$. Prove $M = \varinjlim M_\lambda$.

Example (7.3). — Let Λ be the set of all positive integers, and for each $n \in \Lambda$, set $M_n := \{r/n \mid r \in \mathbb{Z}\} \subset \mathbb{Q}$. Then $\bigcup M_n = \mathbb{Q}$ and $M_m, M_n \subset M_{mn}$. Then **(7.2)** yields $\mathbb{Q} = \varinjlim M_n$ where Λ is ordered by inclusion of the M_n.

However, $M_m \subset M_n$ if and only if $1/m = s/n$ for some s, if and only if $m \mid n$. Thus we may view Λ as ordered by divisibility of the $n \in \Lambda$.

For each $n \in \Lambda$, set $R_n := \mathbb{Z}$, and define $\beta_n\colon R_n \to M_n$ by $\beta_n(r) := r/n$. Clearly, β_n is a $\mathbb{Z}$-module isomorphism. And if $n = ms$, then this diagram is commutative:

$$\begin{tikzcd} R_m \arrow[r, "\mu_s"] \arrow[d, "\beta_m"', "\simeq"] & R_n \arrow[d, "\beta_n"', "\simeq"] \\ M_m \arrow[r, hook, "\iota_n^m"] & M_n \end{tikzcd} \qquad \textbf{(7.3.1)}$$

where μ_s is the map of multiplication by s and ι_n^m is the inclusion. Thus $\mathbb{Q} = \varinjlim R_n$ where the transition maps are the μ_s.

Theorem (7.4). — *Let Λ be a filtered category, R a ring, and $\mathcal{C}$ either ((Sets)) or ((R-mod)) or ((R-alg)). Let $\lambda \mapsto M_\lambda$ be a functor from Λ to $\mathcal{C}$. Define a relation $\sim$ on the set-theoretic disjoint union $\bigsqcup M_\lambda$ as follows: $m_1 \sim m_2$ for $m_i \in M_{\lambda_i}$ if there are transition maps $\alpha_\mu^{\lambda_i}\colon M_{\lambda_i} \to M_\mu$ such that $\alpha_\mu^{\lambda_1} m_1 = \alpha_\mu^{\lambda_2} m_2$. Then $\sim$ is an equivalence relation. Set $M := \big(\bigsqcup M_\lambda\big)/\sim$. Then $M = \varinjlim M_\lambda$, and for each μ, the canonical map $\alpha_\mu\colon M_\mu \to M$ is equal to the insertion map $M_\mu \to \varinjlim M_\lambda$.*

Proof: Clearly $\sim$ is reflexive and symmetric. Let's show it is transitive. Given $m_i \in M_{\lambda_i}$ for $i = 1, 2, 3$ with $m_1 \sim m_2$ and $m_2 \sim m_3$, there are $\alpha^{\lambda_i}_\mu$ for $i = 1, 2$ and $\alpha^{\lambda_i}_\nu$ for $i = 2, 3$ with $\alpha^{\lambda_1}_\mu m_1 = \alpha^{\lambda_2}_\mu m_2$ and $\alpha^{\lambda_2}_\nu m_2 = \alpha^{\lambda_3}_\nu m_3$. Then (**7.1**)(1) yields α^μ_ρ and α^ν_ρ. Possibly, $\alpha^\mu_\rho \alpha^{\lambda_2}_\mu \neq \alpha^\nu_\rho \alpha^{\lambda_2}_\nu$, but in any case, (**7.1**)(2) yields α^ρ_σ with $\alpha^\rho_\sigma(\alpha^\mu_\rho \alpha^{\lambda_2}_\mu) = \alpha^\rho_\sigma(\alpha^\nu_\rho \alpha^{\lambda_2}_\nu)$. In sum, we have this diagram of indices:

$$\begin{tikzcd}
\lambda_1 \arrow[dr] & & & \\
& \mu \arrow[dr] & & \\
\lambda_2 \arrow[ur] \arrow[dr] & & \rho \arrow[r] & \sigma \\
& \nu \arrow[ur] & & \\
\lambda_3 \arrow[ur] & & &
\end{tikzcd}$$

Hence, $(\alpha^\rho_\sigma \alpha^\mu_\rho)\alpha^{\lambda_1}_\mu m_1 = (\alpha^\rho_\sigma \alpha^\nu_\rho)\alpha^{\lambda_3}_\nu m_3$. Thus $m_1 \sim m_3$.

If $\mathcal{C} = ((R\text{-mod}))$, define addition in M as follows. Given $m_i \in M_{\lambda_i}$ for $i = 1, 2$, there are $\alpha^{\lambda_i}_\mu$ by (**7.1**)(1). Set

$$\alpha_{\lambda_1} m_1 + \alpha_{\lambda_2} m_2 := \alpha_\mu(\alpha^{\lambda_1}_\mu m_1 + \alpha^{\lambda_2}_\mu m_2).$$

We must check that this addition is well defined.

First, consider μ. Suppose there are $\alpha^{\lambda_i}_\nu$ too. Then (**7.1**)(1) yields α^μ_ρ and α^ν_ρ. Possibly, $\alpha^\mu_\rho \alpha^{\lambda_i}_\mu \neq \alpha^\nu_\rho \alpha^{\lambda_i}_\nu$, but (**7.1**)(2) yields α^ρ_σ with $\alpha^\rho_\sigma(\alpha^\mu_\rho \alpha^{\lambda_1}_\mu) = \alpha^\rho_\sigma(\alpha^\nu_\rho \alpha^{\lambda_1}_\nu)$ and then α^σ_τ with $\alpha^\sigma_\tau(\alpha^\rho_\sigma \alpha^\mu_\rho \alpha^{\lambda_2}_\mu) = \alpha^\sigma_\tau(\alpha^\rho_\sigma \alpha^\nu_\rho \alpha^{\lambda_2}_\nu)$. In sum, we have this diagram:

$$\begin{tikzcd}
\lambda_1 \arrow[r] \arrow[ddr] & \mu \arrow[dr] & & & \\
& & \rho \arrow[r] & \sigma \arrow[r] & \tau \\
\lambda_2 \arrow[r] \arrow[uur] & \nu \arrow[ur] & & &
\end{tikzcd}$$

Therefore, $(\alpha^\sigma_\tau \alpha^\rho_\sigma \alpha^\mu_\rho)(\alpha^{\lambda_1}_\mu m_1 + \alpha^{\lambda_2}_\mu m_2) = (\alpha^\sigma_\tau \alpha^\rho_\sigma \alpha^\nu_\rho)(\alpha^{\lambda_1}_\nu m_1 + \alpha^{\lambda_2}_\nu m_2)$. Thus both μ and ν yield the same value for $\alpha_{\lambda_1} m_1 + \alpha_{\lambda_2} m_2$.

Second, suppose $m_1 \sim m'_1 \in M_{\lambda'_1}$. Then a similar, but easier, argument yields $\alpha_{\lambda_1} m_1 + \alpha_{\lambda_2} m_2 \alpha_{\lambda'_1} = m'_1 + \alpha_{\lambda_2} m_2$. Thus addition is well defined on M.

Define scalar multiplication on M similarly. Then clearly M is an R-module.

If $\mathcal{C} = ((R\text{-alg}))$, then we can see similarly that M is canonically an R-algebra.

Finally, let $\beta_\lambda \colon M_\lambda \to N$ be maps with $\beta_\lambda \alpha^\kappa_\lambda = \beta_\kappa$ for all α^κ_λ. The β_λ induce a map $\bigsqcup M_\lambda \to N$. Suppose $m_1 \sim m_2$ for $m_i \in M_{\lambda_i}$; that is, $\alpha^{\lambda_1}_\mu m_1 = \alpha^{\lambda_2}_\mu m_2$ for some $\alpha^{\lambda_i}_\mu$. Then $\beta_{\lambda_1} m_1 = \beta_{\lambda_2} m_2$ as $\beta_\mu \alpha^{\lambda_i}_\mu = \beta_{\lambda_i}$. So there is a unique map $\beta \colon M \to N$ with $\beta \alpha_\lambda = \beta_\lambda$ for all λ. Further, if $\mathcal{C} = ((R\text{-mod}))$ or $\mathcal{C} = ((R\text{-alg}))$, then clearly β is a homomorphism. The proof is now complete. $\square$

Corollary (7.5). — *Preserve the conditions of* (**7.4**).

(1) *Given $m \in \varinjlim M_\lambda$, there are λ and $m_\lambda \in M_\lambda$ such that $m = \alpha_\lambda m_\lambda$.*

(2) *Given $m_i \in M_{\lambda_i}$ for $i = 1, 2$ such that $\alpha_{\lambda_1} m_1 = \alpha_{\lambda_2} m_2$, there are $\alpha^{\lambda_i}_\mu$ such that $\alpha^{\lambda_1}_\mu m_1 = \alpha^{\lambda_2}_\mu m_2$.*

(3) *Suppose $\mathcal{C} = ((R\text{–mod}))$ or $\mathcal{C} = ((R\text{–alg}))$. Then given λ and $m_\lambda \in M_\lambda$ such that $\alpha_\lambda m_\lambda = 0$, there is α^λ_μ such that $\alpha^\lambda_\mu m_\lambda = 0$.*

Proof: The assertions follow directly from (**7.4**). Specifically, (1) holds, since $\varinjlim M_\lambda$ is a quotient of the disjoint union $\bigsqcup M_\lambda$. Further, (2) holds owing to the definition of the equivalence relation involved. Finally, (3) is the special case of (2) where $m_1 := m_\lambda$ and $m_2 = 0$. $\square$

Definition (7.6). — Let R be a ring. We say an algebra R' is **finitely presented** if $R' \simeq R[X_1, \ldots, X_r]/\mathfrak{a}$ for some variables X_i and finitely generated ideal $\mathfrak{a}$.

Proposition (7.7). — *Let Λ be a filtered category, R a ring, $\mathcal{C}$ either $((R\text{-mod}))$ or $((R\text{-alg}))$, $\lambda \mapsto M_\lambda$ a functor from Λ to $\mathcal{C}$. Given $N \in \mathcal{C}$, form the map* **(6.4.1)***,*

$$\theta\colon \varinjlim \operatorname{Hom}(N, M_\lambda) \to \operatorname{Hom}(N, \varinjlim M_\lambda).$$

(1) *If N is finitely generated, then θ is injective.*
(2) *The following conditions are equivalent:*
  (a) *N is finitely presented;*
  (b) *θ is bijective for all filtered categories Λ and all functors $\lambda \mapsto M_\lambda$;*
  (c) *θ is surjective for all directed sets Λ and all $\lambda \mapsto M_\lambda$.*

Proof: Given a transition map $\alpha^\lambda_\mu\colon M_\lambda \to M_\mu$, set $\beta^\lambda_\mu := \operatorname{Hom}(N, \alpha^\lambda_\mu)$. Then the β^λ_μ are the transition maps of $\varinjlim \operatorname{Hom}(N, M_\lambda)$. Denote by α_λ and β_λ the insertions of $\varinjlim M_\lambda$ and $\varinjlim \operatorname{Hom}(N, M_\lambda)$.

For (1), let $n_1, \ldots, n_r$ generate N. Given φ and φ' in $\varinjlim \operatorname{Hom}(N, M_\lambda)$ with $\theta(\varphi) = \theta(\varphi')$, note that **(7.5)**(1) yields λ and $\varphi_\lambda\colon N \to M_\lambda$ and μ and $\varphi'_\mu\colon N \to M_\mu$ with $\beta_\lambda(\varphi_\lambda) = \varphi$ and $\beta_\mu(\varphi'_\mu) = \varphi'$. Then $\theta(\varphi) = \alpha_\lambda\varphi_\lambda$ and $\theta(\varphi') = \alpha_\mu\varphi'_\mu$ by construction of θ. Hence $\alpha_\lambda\varphi_\lambda = \alpha_\mu\varphi'_\mu$. So $\alpha_\lambda\varphi_\lambda(n_i) = \alpha_\mu\varphi'_\mu(n_i)$ for all i. So **(7.5)**(2) yields λ_i and $\alpha^\lambda_{\lambda_i}$ and $\alpha^\mu_{\lambda_i}$ such that $\alpha^\lambda_{\lambda_i}\varphi_\lambda(n_i) = \alpha^\mu_{\lambda_i}\varphi'_\mu(n_i)$ for all i.

Consider this commutative diagram, in which ν and the $\alpha^{\lambda_i}_\nu$ are to be constructed:

$$\begin{tikzcd}
N \arrow[r, "\varphi_\lambda"] \arrow[dr, "\varphi'_\mu"'] & M_\lambda \arrow[rr, "\alpha_\lambda"] \arrow[dr, "\alpha^\lambda_{\lambda_i}"] & & \varinjlim M_\lambda \\
& M_\mu \arrow[urr, "\alpha_\mu"] \arrow[r, "\alpha^\mu_{\lambda_i}"'] & M_{\lambda_i} \arrow[ur, "\alpha_{\lambda_i}"] \arrow[r, dotted, "\alpha^{\lambda_i}_\nu"'] & M_\nu \arrow[u, dotted, "\alpha_\nu"']
\end{tikzcd}$$

Let's prove, by induction on i, that there are ν_i and maps $\alpha^\lambda_{\nu_i}$ and $\alpha^\mu_{\nu_i}$ such that $\alpha^\lambda_{\nu_i}\varphi_\lambda(n_j) = \alpha^\mu_{\nu_i}\varphi'_\mu(n_j)$ for $1 \le j \le i$. Indeed, given ν_{i-1} and $\alpha^\lambda_{\nu_{i-1}}$ and $\alpha^\mu_{\nu_{i-1}}$, by **(7.1)**(1), there are ρ_i and $\alpha^{\nu_{i-1}}_{\rho_i}$ and $\alpha^{\lambda_i}_{\rho_i}$. By **(7.1)**(2), there are ν_i and $\alpha^{\rho_i}_{\nu_i}$ such that $\alpha^{\rho_i}_{\nu_i}\alpha^{\nu_{i-1}}_{\rho_i}\alpha^\lambda_{\nu_{i-1}} = \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\lambda_{\lambda_i}$ and $\alpha^{\rho_i}_{\nu_i}\alpha^{\nu_{i-1}}_{\rho_i}\alpha^\mu_{\nu_{i-1}} = \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\mu_{\lambda_i}$. Set $\alpha^\lambda_{\nu_i} := \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\lambda_{\lambda_i}$ and $\alpha^\mu_{\nu_i} := \alpha^{\rho_i}_{\nu_i}\alpha^{\lambda_i}_{\rho_i}\alpha^\mu_{\lambda_i}$. Then $\alpha^\lambda_{\nu_i}\varphi_\lambda(n_j) = \alpha^\mu_{\nu_i}\varphi'_\mu(n_j)$ for $1 \le j \le i$, as desired.

Set $\nu := \nu_r$. Then $\alpha^\lambda_\nu\varphi_\lambda(n_i) = \alpha^\mu_\nu\varphi'_\mu(n_i)$ for all i. Hence $\alpha^\lambda_\nu\varphi_\lambda = \alpha^\mu_\nu\varphi'_\mu$. But

$$\varphi = \beta_\lambda(\varphi_\lambda) = \beta_\nu\beta^\lambda_\nu(\varphi_\lambda) = \beta_\nu(\alpha^\lambda_\nu\varphi_\lambda).$$

Similarly, $\varphi' = \beta_\nu(\alpha^\mu_\nu\varphi'_\mu)$. Hence $\varphi = \varphi'$. Thus θ is injective. Notice that this proof works equally well for $((R\text{-mod}))$ and $((R\text{-alg}))$. Thus (1) holds.

For (2), let's treat the case $\mathcal{C} = ((R\text{-mod}))$ first. Assume (a). Say $N \simeq F/N'$ where $F := R^r$ and N' is finitely generated, say by $n'_1, \ldots, n'_s$. Let n_i be the image in N of the ith standard basis vector e_i of F. For all j, there's a linear polynomial L_j with $L_j(0, \ldots, 0) = 0$ and $L_j(e_1, \ldots, e_r) = n'_j$. So $L_j(n_1, \ldots, n_r) = 0$.

Given $\varphi\colon N \to \varinjlim M_\lambda$, set $m_i := \varphi(n_i)$ for $1 \le i \le r$. Repeated use of **(7.5)**(1) and **(7.1)**(1) yields λ and $m_{\lambda i} \in M_\lambda$ with $\alpha_\lambda m_{\lambda i} = m_i$ for all i. So for all j,

$$\alpha_\lambda(L_j(m_{\lambda 1}, \ldots, m_{\lambda r})) = L_j(m_1, \ldots, m_r) = \varphi(L_j(n_1, \ldots, n_r)) = 0.$$

Hence repeated use of **(7.5)**(2) and **(7.1)**(1), (2) yields μ and α^λ_μ with, for all j,

$$\alpha^\lambda_\mu(L_j(m_{\lambda 1}, \ldots, m_{\lambda r})) = 0.$$

Therefore, there is $\varphi_\mu\colon N \to M_\mu$ with $\varphi_\mu(n_i) := \alpha^\lambda_\mu(m_{\lambda i})$ by **(4.10)** and **(4.6)**. Set $\psi := \beta_\mu(\varphi_\mu)$. Then $\theta(\psi) = \alpha_\mu\varphi_\mu$. Hence $\theta(\psi)(n_i) = m_i := \varphi(n_i)$ for all i. So $\theta(\psi) = \varphi$. Thus θ is surjective. So (1) implies θ is bijective. Thus (b) holds.

Trivially (b) implies (c).

Finally, assume (c). Take Λ to be the directed set of finitely generated submodules N_λ of N. Then $N = \varinjlim N_\lambda$ by **(7.2)**. However, θ is surjective. So there is $\psi \in \varinjlim \operatorname{Hom}(N, N_\lambda)$ with $\theta(\psi) = 1_N$. So **(7.5)**(1) yields λ and $\psi_\lambda \in \operatorname{Hom}(N, N_\lambda)$ with $\beta_\lambda(\psi_\lambda) = \psi$. Hence $\alpha_\lambda\psi_\lambda = \theta(\psi)$. So $\alpha_\lambda\psi_\lambda = 1_N$. So α_λ is surjective. But $\alpha_\lambda\colon N_\lambda \to N$ is the inclusion. So $N_\lambda = N$. Thus N is finitely generated. Say $n_1, \dots, n_r$ generate N. Set $F := R^r$ and let e_i be the ith standard basis vector.

Define $\kappa\colon F \to N$ by $\kappa(e_i) := n_i$ for all i. Set $N' := \operatorname{Ker}(\kappa)$. Then $F/N' \xrightarrow{\sim} N$. Let's show N' is finitely generated.

Take Λ to be the directed set of finitely generated submodules N'_λ of N'. Then $N' = \varinjlim N'_\lambda$ by **(7.2)**. Set $N_\lambda := F/N'_\lambda$. Then $N = \varinjlim N_\lambda$ by **(6.19)**. Here the α^λ_μ and the α_λ are the quotient maps. Since θ is surjective, there is $\psi \in \operatorname{Hom}(N, N_\lambda)$ with $\theta(\psi) = 1_N$. So **(7.5)**(1) yields λ and $\psi_\lambda \in \operatorname{Hom}(N, N_\lambda)$ with $\beta_\lambda(\psi_\lambda) = \psi$. Hence $\alpha_\lambda\psi_\lambda = \theta(\psi)$. So $\alpha_\lambda\psi_\lambda = 1_N$. Set $\psi_\mu := \alpha^\lambda_\mu\psi_\lambda$ for all μ; note ψ_μ is well defined as Λ is directed. Then $\alpha_\mu\psi_\mu = \alpha_\lambda\psi_\lambda = 1_N$ for all μ. Let's show there is μ with $\psi_\mu\alpha_\mu = 1_{N_\mu}$.

For all μ and i, let $n_{\mu i}$ be the image in N_μ of e_i. Then $\alpha_\lambda n_{\lambda i} = \alpha_\lambda(\psi_\lambda\alpha_\lambda n_{\lambda i})$ as $\alpha_\lambda\psi_\lambda = 1_N$. Hence repeated use of **(7.5)**(2) and **(7.1)**(1) yields μ such that $\alpha^\lambda_\mu n_{\lambda i} = \alpha^\lambda_\mu(\psi_\lambda\alpha_\lambda n_{\lambda i})$ for all i. Hence $n_{\mu i} = (\psi_\mu\alpha_\mu)n_{\mu i}$. But the $n_{\mu i}$ generate N_μ for all i. So $1_{N_\mu} = \psi_\mu\alpha_\mu$, as desired.

So $\alpha_\mu\colon N_\mu \to N$ is an isomorphism. So $N'_\mu = N'$. Thus N' is finitely generated. Thus (a) holds for $((R\text{-mod}))$.

In the case $\mathcal{C} = ((R\text{-alg}))$, replace F by a polynomial ring $R[X_1, \dots, X_r]$, the submodule N' by the appropriate ideal $\mathfrak{a}$, and the n_j by polynomials that generate $\mathfrak{a}$. With these replacements, the above proof shows (a) implies (b). As to (c) implies (a), first take the N_λ to be the finitely generated subalgebras; then the above proof of finite generation works equally well as is. The rest of the proof works after we replace F by a polynomial ring, the e_i by the variables, N' by the appropriate ideal, and the N'_λ by the finitely generated subideals. □

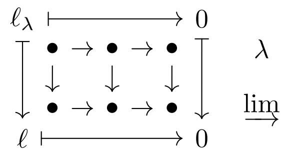
(7.8) (Finite presentations). — Let R be a ring, R' a finitely presented algebra. The proof of **(7.7)**(2) shows that, for any presentation $R[X_1, \dots, X_r]/\mathfrak{a}$ of R', where $R[X_1, \dots, X_r]$ is a polynomial ring and $\mathfrak{a}$ is an ideal, necessarily $\mathfrak{a}$ is finitely generated. Similarly, for a finitely presented module M, that proof gives another solution to **(5.18)**, one not requiring Schanuel's Lemma.

Theorem (7.9) (Exactness of Filtered Direct Limits). — *Let R be a ring, Λ a filtered category. Let $\mathcal{C}$ be the category of 3-term exact sequences of R-modules: its objects are the 3-term exact sequences, and its maps are the commutative diagrams*

$$\begin{array}{ccccc} L & \longrightarrow & M & \longrightarrow & N \\ \big\downarrow & & \big\downarrow & & \big\downarrow \\ L' & \to & M' & \to & N' \end{array}$$

Then, for any functor $\lambda \mapsto (L_\lambda \xrightarrow{\beta_\lambda} M_\lambda \xrightarrow{\gamma_\lambda} N_\lambda)$ from Λ to $\mathcal{C}$, the induced sequence $\varinjlim L_\lambda \xrightarrow{\beta} \varinjlim M_\lambda \xrightarrow{\gamma} \varinjlim N_\lambda$ is exact.

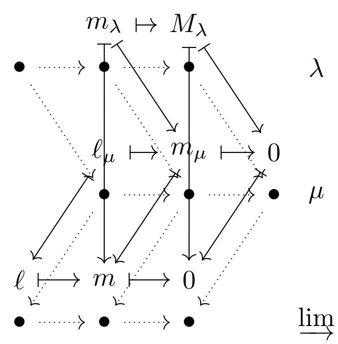
Proof: Abusing notation, in all three cases denote by α^κ_λ the transition maps and by α_λ the insertions. Then given $\ell \in \varinjlim L_\lambda$, there is $\ell_\lambda \in L_\lambda$ with $\alpha_\lambda \ell_\lambda = \ell$ by **(7.5)**(1). By hypothesis, $\gamma_\lambda \beta_\lambda \ell_\lambda = 0$; so $\gamma\beta\ell = 0$. In sum, we have the figure below. Thus $\mathrm{Im}(\beta) \subset \mathrm{Ker}(\gamma)$.



For the opposite inclusion, take $m \in \varinjlim M_\lambda$ with $\gamma m = 0$. By **(7.5)**(1), there is $m_\lambda \in M_\lambda$ with $\alpha_\lambda m_\lambda = m$. Now, $\alpha_\lambda \gamma_\lambda m_\lambda = 0$ by commutativity. So by **(7.5)**(3), there is α^λ_μ with $\alpha^\lambda_\mu \gamma_\lambda m_\lambda = 0$. So $\gamma_\mu \alpha^\lambda_\mu m_\lambda = 0$ by commutativity. Hence there is $\ell_\mu \in L_\mu$ with $\beta_\mu \ell_\mu = \alpha^\lambda_\mu m_\lambda$ by exactness. Apply α_μ to get

$$\beta\alpha_\mu \ell_\mu = \alpha_\mu \beta_\mu \ell_\mu = \alpha_\mu \alpha^\lambda_\mu m_\lambda = m.$$

In sum, we have this figure:



Thus $\mathrm{Ker}(\gamma) \subset \mathrm{Im}(\beta)$. So $\mathrm{Ker}(\gamma) = \mathrm{Im}(\beta)$ as asserted. □

(7.10) (Hom and direct limits again). — Let Λ a filtered category, R a ring, N a module, and $\lambda \mapsto M_\lambda$ a functor from Λ to $((R\text{-mod}))$. Here is an alternative proof that the map $\theta(N)$ of **(6.4.1)** is injective if N is finitely generated and bijective if N is finitely presented.

If $N := R$, then $\theta(N)$ is bijective by **(4.3)**. Assume N is finitely generated, and take a presentation $R^{\oplus\Sigma} \to R^n \to N \to 0$ with Σ finite if N is finitely presented. It induces the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \varinjlim \mathrm{Hom}(N, M_\lambda) \arrow[r] \arrow[d, "\theta(N)"'] & \varinjlim \mathrm{Hom}(R^n, M_\lambda) \arrow[r] \arrow[d, "\theta(R^n)"', "\simeq"] & \varinjlim \mathrm{Hom}(R^{\oplus\Sigma}, M_\lambda) \arrow[d, "\theta(R^{\oplus\Sigma})"'] \\
0 \arrow[r] & \mathrm{Hom}(N, \varinjlim M_\lambda) \arrow[r] & \mathrm{Hom}(R^n, \varinjlim M_\lambda) \arrow[r] & \mathrm{Hom}(R^{\oplus\Sigma}, \varinjlim M_\lambda)
\end{tikzcd}$$

The rows are exact owing to **(5.11)**, the left exactness of Hom, and to **(7.9)**, the exactness of filtered direct limits. Now, Hom preserves finite direct sums by **(4.13)**, and direct limit does so by **(6.12)** and **(6.5)**; hence, $\theta(R^n)$ is bijective, and $\theta(R^{\oplus\Sigma})$ is bijective if Σ is finite. A diagram chase yields the assertion.

B. Exercises

Exercise (7.11) . — Show that every module M is the filtered direct limit of its finitely generated submodules.

Exercise (7.12) . — Show that every direct sum of modules is the filtered direct limit of its finite direct subsums.

Exercise (7.13) . — Keep the setup of (7.3). For each $n \in \Lambda$, set $N_n := \mathbb{Z}/\langle n\rangle$; if $n = ms$, define $\alpha_n^m \colon N_m \to N_n$ by $\alpha_n^m(x) := xs \pmod{n}$. Show $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$.

Exercise (7.14) . — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha_\mu^\lambda \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$.

(1) Prove that all α_λ are injective if and only if all α_μ^λ are. What if $\varinjlim M_\lambda$ isn't filtered?
(2) Assume that all α_λ are injective. Prove $M = \bigcup \alpha_\lambda M_\lambda$.

Exercise (7.15) . — Let R be a ring, $\mathfrak{a}$ a finitely generated ideal, M a module. Show $\Gamma_{\mathfrak{a}}(M) = \varinjlim \operatorname{Hom}(R/\mathfrak{a}^n, M)$.

Exercise (7.16) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Show:

(1) Then $R = 0$ if and only if $R_\lambda = 0$ for some λ.
(2) Assune each R_λ is a domain. Then R is a domain.
(3) Assume each R_λ is a field. Then each insertion $\alpha_\lambda \colon R_\lambda \to R$ is injective, $R = \bigcup \alpha_\lambda R_\lambda$, and R is a field.

Exercise (7.17) . — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha_\mu^\lambda \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$. For each λ, let $N_\lambda \subset M_\lambda$ be a submodule, and let $N \subset M$ be a submodule. Prove that $N_\lambda = \alpha_\lambda^{-1} N$ for all λ if and only if (a) $N_\lambda = (\alpha_\mu^\lambda)^{-1} N_\mu$ for all α_μ^λ and (b) $\bigcup \alpha_\lambda N_\lambda = N$.

Exercise (7.18) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings, $\mathfrak{a}_\lambda \subset R_\lambda$ an ideal for each λ. Assume $\alpha_\mu^\lambda \mathfrak{a}_\lambda \subset \mathfrak{a}_\mu$ for each transition map α_μ^λ. Set $\mathfrak{a} := \varinjlim \mathfrak{a}_\lambda$. If each $\mathfrak{a}_\lambda$ is prime, show $\mathfrak{a}$ is prime. If each $\mathfrak{a}_\lambda$ is maximal, show $\mathfrak{a}$ is maximal.

Exercise (7.19) . — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha_\mu^\lambda \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$. Let $N_\lambda \subset M_\lambda$ be a be a submodule for all λ. Assume $\alpha_\mu^\lambda N_\lambda \subset N_\mu$ for all α_μ^λ. Prove $\varinjlim N_\lambda = \bigcup \alpha_\lambda N_\lambda$.

Exercise (7.20) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Prove that

$$\varinjlim \operatorname{nil}(R_\lambda) = \operatorname{nil}(R).$$

Exercise (7.21) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Assume each ring R_λ is local, say with maximal ideal $\mathfrak{m}_\lambda$, and assume each transition map $\alpha_\mu^\lambda \colon R_\lambda \to R_\mu$ is local. Set $\mathfrak{m} := \varinjlim \mathfrak{m}_\lambda$. Prove that R is local with maximal ideal $\mathfrak{m}$ and that each insertion $\alpha_\lambda \colon R_\lambda \to R$ is local.

Exercise (7.22) . — Let Λ and Λ' be small categories, $C \colon \Lambda' \to \Lambda$ a functor. Assume Λ' is filtered. Assume C is **cofinal**; that is,

(1) given $\lambda \in \Lambda$, there is a map $\lambda \to C\lambda'$ for some $\lambda' \in \Lambda'$, and
(2) given $\psi, \varphi \colon \lambda \rightrightarrows C\lambda'$, there is $\chi \colon \lambda' \to \lambda_1'$ with $(C\chi)\psi = (C\chi)\varphi$.

Let $\lambda \mapsto M_\lambda$ be a functor from Λ to $\mathcal{C}$ whose direct limit exists. Show that

$$\varinjlim_{\lambda' \in \Lambda'} M_{C\lambda'} = \varinjlim_{\lambda \in \Lambda} M_\lambda;$$

more precisely, show that the right side has the UMP characterizing the left.

Exercise (7.23) . — Show that every R-module M is the filtered direct limit over a directed set of finitely presented modules.

8. Tensor Products

Given two modules, their tensor product is the target of the universal bilinear map. We construct the product, and establish various properties: bifunctoriality, commutativity, associativity, cancellation, and most importantly, adjoint associativity; the latter relates the product to the module of homomorphisms. With one factor fixed, tensor product becomes a linear functor. We prove Watt's Theorem; it characterizes "tensor-product" functors as those linear functors that commute with direct sums and cokernels. Lastly, we discuss the tensor product of algebras.

A. Text

(8.1) (Bilinear maps). — Let R a ring, and M, N, P modules. We call a map

$$\alpha\colon M \times N \to P$$

bilinear if it is linear in each variable; that is, given $m \in M$ and $n \in N$, the maps

$$m' \mapsto \alpha(m', n) \quad \text{and} \quad n' \mapsto \alpha(m, n')$$

are R-linear. Denote the set of all these maps by $\mathrm{Bil}_R(M, N; P)$. It is clearly an R-module, with sum and scalar multiplication performed valuewise.

(8.2) (Tensor product). — Let R be a ring, and M, N modules. Their **tensor product**, denoted $M \otimes_R N$ or simply $M \otimes N$, is constructed as the quotient of the free module $R^{\oplus(M\times N)}$ modulo the submodule generated by the following elements, where (m, n) stands for the standard basis element $e_{(m,n)}$:

$$\begin{aligned} (m+m',\, n) - (m,\, n) - (m',\, n) \quad &\text{and} \quad (m,\, n+n') - (m, n) - (m, n'), \\ (xm,\, n) - x(m, n) \quad &\text{and} \quad (m,\, xn) - x(m, n) \end{aligned} \tag{8.2.1}$$

for all $m, m' \in M$ and $n, n' \in N$ and $x \in R$.

The above construction yields a canonical bilinear map

$$\beta\colon M \times N \to M \otimes N.$$

Set $m \otimes n := \beta(m, n)$.

Theorem (8.3) (UMP of tensor product). **—** *Let R be a ring, M, N modules. Then $\beta\colon M \times N \to M \otimes N$ is the universal bilinear map with source $M \times N$; in fact, β induces, not simply a bijection, but a module isomorphism,*

$$\theta\colon \mathrm{Hom}_R(M \otimes_R N, P) \xrightarrow{\sim} \mathrm{Bil}_R(M, N; P). \tag{8.3.1}$$

Proof: Note that, if we follow any bilinear map with any linear map, then the result is bilinear; hence, θ is well defined. Clearly, θ is a module homomorphism. Further, θ is injective since $M \otimes_R N$ is generated by the image of β. Finally, given any bilinear map $\alpha\colon M \times N \to P$, by (4.10) it extends to a map $\alpha'\colon R^{\oplus(M\times N)} \to P$, and α' carries all the elements in (8.2.1) to 0; hence, α' factors through β. Thus θ is also surjective, so an isomorphism, as asserted. □

(8.4) (Bifunctoriality). — Let R be a ring, $\alpha\colon M \to M'$ and $\alpha'\colon N \to N'$ module homomorphisms. Then there is a canonical commutative diagram:

$$\begin{array}{ccc} M \times N & \xrightarrow{\alpha\times\alpha'} & M' \times N' \\ \big\downarrow{\scriptstyle\beta} & & \big\downarrow{\scriptstyle\beta'} \\ M \otimes N & \xrightarrow{\alpha\otimes\alpha'} & M' \otimes N' \end{array}$$

Indeed, $\beta' \circ (\alpha \times \alpha')$ is clearly bilinear; so the UMP (**8.3**) yields $\alpha \otimes \alpha'$. Thus $\bullet \otimes N$ and $M \otimes \bullet$ are commuting **linear** functors — that is, linear on maps, see (**8.12**).

Proposition (8.5). — *Let R be a ring, M and N modules.*

(1) *Then the switch map $(m, n) \mapsto (n, m)$ induces an isomorphism*

$$M \otimes_R N = N \otimes_R M. \qquad \textbf{(Commutative Law)}$$

(2) *Then multiplication of R on M induces an isomorphism*

$$R \otimes_R M = M. \qquad \textbf{(Unitary Law)}$$

Proof: The switch map induces an isomorphism $R^{\oplus(M\times N)} \xrightarrow{\sim} R^{\oplus(N\times M)}$, and it preserves the elements of (**8.2.1**). Thus (1) holds.

Define $\beta\colon R \times M \to M$ by $\beta(x, m) := xm$. Clearly β is bilinear. Let's check β has the requisite UMP. Given a bilinear map $\alpha\colon R \times M \to P$, define $\gamma\colon M \to P$ by $\gamma(m) := \alpha(1, m)$. Then γ is linear as α is bilinear. Also, $\alpha = \gamma\beta$ as

$$\alpha(x, m) = x\alpha(1, m) = \alpha(1, xm) = \gamma(xm) = \gamma\beta(x, m).$$

Further, γ is unique as β is surjective. Thus β has the UMP, so (2) holds. □

(8.6) (Bimodules). — Let R and R' be rings. An abelian group N is an (R, R')-**bimodule** if it is both an R-module and an R'-module and if $x(x'n) = x'(xn)$ for all $x \in R$, all $x' \in R'$, and all $n \in N$. At times, we think of N as a left R-module, with multiplication xn, and as a right R'-module, with multiplication nx'. Then the compatibility condition becomes the Associative Law: $x(nx') = (xn)x'$. A (R, R')-**homomorphism** of bimodules is a map that is both R-linear and R'-linear.

Let M be an R-module, and let N be an (R, R')-bimodule. Then $M \otimes_R N$ is an (R, R')-bimodule with R-structure as usual and with R'-structure defined by $x'(m \otimes n) := m \otimes (x'n)$ for all $x' \in R'$, all $m \in M$, and all $n \in N$. The latter multiplication is well defined and the two multiplications commute because of bifunctoriality (**8.4**) with $\alpha := \mu_x$ and $\alpha' := \mu_{x'}$.

For instance, suppose R' is an R-algebra. Then R' is an (R, R')-bimodule. So $M \otimes_R R'$ is an R'-module. It is said to be obtained by **extension of scalars**.

In full generality, it is easy to check that $\mathrm{Hom}_R(M, N)$ is an (R, R')-bimodule under valuewise multiplication by elements of R'. Further, given an R'-module P, it is easy to check that $\mathrm{Hom}_{R'}(N, P)$ is an (R, R')-bimodule under sourcewise multiplication by elements of R.

Exercise (8.7) . — Let R be a ring, R' an R-algebra, and M, N two R'-modules.

(1) Show that there is a canonical R-linear map $\tau\colon M \otimes_R N \to M \otimes_{R'} N$.

(2) Let $K \subset M \otimes_R N$ denote the R-submodule generated by all the differences $(x'm) \otimes n - m \otimes (x'n)$ for $x' \in R'$ and $m \in M$ and $n \in N$. Show that $K = \mathrm{Ker}(\tau)$ and that τ is surjective.

(3) Suppose that R' is a quotient of R. Show that τ is an isomorphism.

(4) Let $\{t_\tau\}$ be a set of algebra generators of R' over R. Let $\{m_\mu\}$ and $\{n_\nu\}$

be sets of generators of M and N over R'. Regard $M \otimes_R N$ as an $(R' \otimes_R R')$-module. Let K' denote the $(R' \otimes_R R')$-submodule generated by all differences $(t_\tau m_\mu) \otimes n_\nu - m_\mu \otimes (t_\tau n_\nu)$. Show that $K' = K$.

Theorem (8.8). — *Let R and R' be rings, M an R-module, P an R'-module, N an (R, R')-bimodule. Then there are two canonical (R, R')-isomorphisms:*

(1) $M \otimes_R (N \otimes_{R'} P) = (M \otimes_R N) \otimes_{R'} P$. **(Associative Law)**

(2) $\mathrm{Hom}_{R'}(M \otimes_R N,\ P) = \mathrm{Hom}_R\big(M,\ \mathrm{Hom}_{R'}(N,\ P)\big)$. **(Adjoint Associativity)**

Proof: Note that $M \otimes_R (N \otimes_{R'} P)$ and $(M \otimes_R N) \otimes_{R'} P$ are (R, R')-bimodules. For each (R, R')-bimodule Q, call a map $\tau\colon M \times N \times P \to Q$ **trilinear** if it is R-bilinear in $M \times N$ and R'-bilinear in $N \times P$. Denote the set of all these τ by $\mathrm{Tril}_{(R,R')}(M, N, P;\ Q)$. It is, clearly, an (R, R')-bimodule.

A trilinear map τ yields an R-bilinear map $M \times (N \otimes_{R'} P) \to Q$, whence a map $M \otimes_R (N \otimes_{R'} P) \to Q$, which is both R-linear and R'-linear, and *vice versa*. Thus

$$\mathrm{Tril}_{(R,R')}(M, N, P;\, Q) = \mathrm{Hom}\big(M \otimes_R (N \otimes_{R'} P),\, Q\big).$$

Similarly, there is a canonical isomorphism of (R, R')-bimodules

$$\mathrm{Tril}_{(R,R')}(M, N, P;\, Q) = \mathrm{Hom}\big((M \otimes_R N) \otimes_{R'} P,\, Q\big).$$

Hence each of $M \otimes_R (N \otimes_{R'} P)$ and $(M \otimes_R N) \otimes_{R'} P$ is the universal target of a trilinear map with source $M \times N \times P$. Thus they are equal, as asserted.

To establish the isomorphism of Adjoint Associativity, define a map

$$\alpha\colon \mathrm{Hom}_{R'}(M \otimes_R N, P) \to \mathrm{Hom}_R\big(M,\, \mathrm{Hom}_{R'}(N, P)\big) \quad \text{by}$$
$$\big(\alpha(\gamma)(m)\big)(n) := \gamma(m \otimes n).$$

Let's check α is well defined. First, $\alpha(\gamma)(m)$ is R'-linear, because given $x' \in R'$,

$$\gamma(m \otimes (x'n)) = \gamma(x'(m \otimes n)) = x'\gamma(m \otimes n)$$

since γ is R'-linear. Further, $\alpha(\gamma)$ is R-linear, because given $x \in R$,

$$(xm) \otimes n = m \otimes (xn) \quad \text{and so} \quad \big(\alpha(\gamma)(xm)\big)(n) = \big(\alpha(\gamma)(m)\big)(xn).$$

Thus $\alpha(\gamma) \in \mathrm{Hom}_R\big(M,\, \mathrm{Hom}_{R'}(N, P)\big)$. Clearly, α is an (R, R')-homomorphism.

To obtain an inverse to α, given $\eta \in \mathrm{Hom}_R\big(M,\, \mathrm{Hom}_{R'}(N, P)\big)$, define a map $\zeta\colon M \times N \to P$ by $\zeta(m, n) := (\eta(m))(n)$. Clearly, ζ is $\mathbb{Z}$-bilinear, so ζ induces a $\mathbb{Z}$-linear map $\delta\colon M \otimes_{\mathbb{Z}} N \to P$. Given $x \in R$, clearly $(\eta(xm))(n) = (\eta(m))(xn)$; so $\delta((xm) \otimes n) = \delta(m \otimes (xn))$. Hence, δ induces a $\mathbb{Z}$-linear map $\beta(\eta)\colon M \otimes_R N \to P$ owing to **(8.7)** with $\mathbb{Z}$ for R and with R for R'. Clearly, $\beta(\eta)$ is R'-linear as $\eta(m)$ is so. Finally, it is easy to verify that $\alpha(\beta(\eta)) = \eta$ and $\beta(\alpha(\gamma)) = \gamma$, as desired. □

Corollary (8.9). — *Let R be a ring, and R' an algebra. First, let M be an R-module, and P an R'-module. Then there are two canonical R'-isomorphisms:*

(1) $(M \otimes_R R') \otimes_{R'} P = M \otimes_R P$. **(Cancellation Law)**

(2) $\mathrm{Hom}_{R'}(M \otimes_R R',\ P) = \mathrm{Hom}_R(M,\ P)$. **(Left Adjoint)**

Instead, let M be an R'-module, and P an R-module. Then there is a canonical R'-isomorphism:

(3) $\mathrm{Hom}_R(M,\ P) = \mathrm{Hom}_{R'}(M,\ \mathrm{Hom}_R(R',\ P))$. **(Right Adjoint)**

In other words, $\bullet \otimes_R R'$ is the left adjoint of restriction of scalars from R' to R, and $\mathrm{Hom}_R(R', \bullet)$ is its right adjoint.

Proof: The Cancellation Law results from the Associative Law (**8.8**)(1) and the Unitary Law (**8.5**)(2); the Adjoint Isomorphisms, from Adjoint Associativity (**8.8**)(2), from (**4.3**), and from the Unitary Law (**8.5**)(2). □

Corollary (8.10). — *Let R, R' be rings, N a bimodule. Then the functor $\bullet \otimes_R N$ preserves direct limits, or equivalently, direct sums and cokernels.*

Proof: By Adjoint Associativity (**8.8**)(2), the functor $\bullet \otimes_R N$ is the left adjoint of $\mathrm{Hom}_{R'}(N, \bullet)$. Thus the assertion results from (**6.9**) and (**6.7**). □

Example (8.11). — Tensor product does not preserve kernels, nor even injections. Indeed, consider the injection $\mu_2 \colon \mathbb{Z} \to \mathbb{Z}$. Tensor it with $N := \mathbb{Z}/\langle 2\rangle$, obtaining $\mu_2 \colon N \to N$. This map is zero, but not injective as $N \neq 0$.

(8.12) (Linear Functors). — Let R be a ring, R' an algebra, F a functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Call F **linear** or R**-linear** if this map is R-linear:

$$\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{R'}(FM,\, FN).$$

Assume so. If a map $\alpha \colon M \to N$ is 0, then $F\alpha \colon FM \to FN$ is too. But $M = 0$ if and only if $1_M = 0$. Further, $F(1_M) = 1_{FM}$. Thus if $M = 0$, then $FM = 0$.

Theorem (8.13) (Watts)**. —** *Let $F \colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a linear functor. Then there is a natural transformation $\theta(\bullet)\colon\ \bullet\otimes F(R) \to F(\bullet)$ with $\theta(R) = 1$, and $\theta(\bullet)$ is an isomorphism if and only if F preserves direct sums and cokernels.*

Proof: As F is a linear functor, there is, by definition, a natural R-linear map $\theta(M)\colon\ \mathrm{Hom}(R, M) \to \mathrm{Hom}(F(R),\, F(M))$. But $\mathrm{Hom}(R, M) = M$ by (**4.3**). Hence Adjoint Associativity (**8.8**)(2) yields the desired map

$$\theta(M) \in \mathrm{Hom}\big(M,\, \mathrm{Hom}(F(R),\, F(M))\big) = \mathrm{Hom}(M \otimes F(R),\, F(M)).$$

Explicitly, $\theta(M)(m \otimes n) = F(\rho)(n)$ where $\rho\colon R \to M$ is defined by $\rho(1) = m$. Alternatively, this formula can be used to construct $\theta(M)$, as $(m, n) \mapsto F(\rho)(n)$ is clearly bilinear. Either way, it's not hard to see $\theta(M)$ is natural in M and $\theta(R) = 1$.

If $\theta(\bullet)$ is an isomorphism, then F preserves direct sums and cokernels by (**8.10**).

To prove the converse, take a presentation $R^{\oplus\Sigma} \xrightarrow{\beta} R^{\oplus\Lambda} \xrightarrow{\alpha} M \to 0$; one exists by (**5.13**). Set $N := F(R)$. Applying θ, we get this commutative diagram:

$$\begin{tikzcd}
R^{\oplus\Sigma} \otimes N \arrow[r] \arrow[d, "\theta(R^{\oplus\Sigma})"] & R^{\oplus\Lambda} \otimes N \arrow[r] \arrow[d, "\theta(R^{\oplus\Lambda})"] & M \otimes N \arrow[r] \arrow[d, "\theta(M)"] & 0 \\
F(R^{\oplus\Sigma}) \arrow[r] & F(R^{\oplus\Lambda}) \arrow[r] & F(M) \arrow[r] & 0
\end{tikzcd} \qquad \textbf{(8.13.1)}$$

By construction, $\theta(R) = 1_N$. Suppose that F preserves direct sums. Then $\theta(R^{\oplus\Lambda}) = 1_{N^{\oplus\Lambda}}$ and $\theta(R^{\oplus\Sigma}) = 1_{N^{\oplus\Sigma}}$ by (**6.15**), as direct sum is a special case of direct limit by (**6.5**). Suppose also that F preserves cokernels. As $\bullet \otimes N$ does too, the rows of (**8.13.1**) are exact by (**5.2**)(2). Thus $\theta(M)$ is an isomorphism. □

Exercise (8.14) . — Let $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a linear functor, and $\mathcal{C}$ the category of finitely generated modules. Show that F always preserves finite direct sums. Show that $\theta(M)\colon M \otimes F(R) \to F(M)$ is surjective if F preserves surjections in $\mathcal{C}$ and M is finitely generated, and that $\theta(M)$ is an isomorphism if F preserves cokernels in $\mathcal{C}$ and M is finitely presented.

(8.15) (Additive functors). — Let R be a ring, M a module, and form the diagram

$$M \xrightarrow{\delta_M} M \oplus M \xrightarrow{\sigma_M} M$$

where $\delta_M := (1_M, 1_M)$ and $\sigma_M := 1_M + 1_M$.

Let $\alpha, \beta\colon M \to N$ be two maps of modules. Then

$$\sigma_N(\alpha \oplus \beta)\delta_M = \alpha + \beta, \tag{8.15.1}$$

because, for any $m \in M$, we have

$$(\sigma_N(\alpha \oplus \beta)\delta_M)(m) = \sigma_N(\alpha \oplus \beta)(m, m) = \sigma_N(\alpha(m),\, \beta(m)) = \alpha(m) + \beta(m).$$

Let $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a functor that preserves finite direct sums. Then $F(\alpha \oplus \beta) = F(\alpha) \oplus F(\beta)$. Also, $F(\delta_M) = \delta_{F(M)}$ and $F(\sigma_M) = \sigma_{F(M)}$ as $F(1_M) = 1_{F(M)}$. Hence $F(\alpha + \beta) = F(\alpha) + F(\beta)$ by **(8.15.1)**. Thus F is **additive**, that is, $\mathbb{Z}$-linear.

Conversely, every additive functor preserves finite direct sums owing to **(8.14)**.

However, not every additive functor is R-linear. For example, take $R := \mathbb{C}$. Define $F(M)$ to be M, but with the scalar product of $x \in \mathbb{C}$ and $m \in M$ to be $\overline{x}m$ where $\overline{x}$ is the conjugate. Define $F(\alpha)$ to be α. Then F is additive, but not linear.

Lemma (8.16) (Equational Criterion for Vanishing). — *Let R be a ring, M and N modules, and $\{n_\lambda\}_{\lambda \in \Lambda}$ a set of generators of N. Then any $t \in M \otimes N$ can be written as a finite sum $t = \sum m_\lambda \otimes n_\lambda$ with $m_\lambda \in M$. Further, $t = 0$ if and only if there are $m_\sigma \in M$ and $x_{\lambda\sigma} \in R$ for $\sigma \in \Sigma$ for some Σ such that*

$$\textstyle\sum_\sigma x_{\lambda\sigma} m_\sigma = m_\lambda \textit{ for all } \lambda \textit{ and } \sum_\lambda x_{\lambda\sigma} n_\lambda = 0 \textit{ for all } \sigma.$$

Proof: Owing to **(8.2)**, $M \otimes N$ is generated by all the $m \otimes n$ with $m \in M$ and $n \in N$, and if $n = \sum x_\lambda n_\lambda$ with $x_\lambda \in R$, then $m \otimes n = \sum (x_\lambda m) \otimes n_\lambda$. It follows that t can be written as a finite sum $t = \sum m_\lambda \otimes n_\lambda$ with $m_\lambda \in M$.

Assume the m_σ and the $x_{\lambda\sigma}$ exist. Then

$$\textstyle\sum m_\lambda \otimes n_\lambda = \sum_\lambda \left(\sum_\sigma x_{\lambda\sigma} m_\sigma \right) \otimes n_\lambda = \sum_\sigma \left(m_\sigma \otimes \sum_\lambda x_{\lambda\sigma} n_\lambda \right) = 0.$$

Conversely, by **(5.13)**, there is a presentation $R^{\oplus\Sigma} \xrightarrow{\beta} R^{\oplus\Lambda} \xrightarrow{\alpha} N \to 0$ with $\alpha(e_\lambda) = n_\lambda$ for all λ where $\{e_\lambda\}$ is the standard basis of $R^{\oplus\Lambda}$. Then by **(8.10)** the following sequence is exact:

$$M \otimes R^{\oplus\Sigma} \xrightarrow{1\otimes\beta} M \otimes R^{\oplus\Lambda} \xrightarrow{1\otimes\alpha} M \otimes N \to 0.$$

Further, $(1 \otimes \alpha)\left(\sum m_\lambda \otimes e_\lambda\right) = 0$. So the exactness implies there is an element $s \in M \otimes R^{\oplus\Sigma}$ such that $(1 \otimes \beta)(s) = \sum m_\lambda \otimes e_\lambda$. Let $\{e_\sigma\}$ be the standard basis of $R^{\oplus\Sigma}$, and write $s = \sum m_\sigma \otimes e_\sigma$ with $m_\sigma \in M$. Write $\beta(e_\sigma) = \sum_\lambda x_{\lambda\sigma} e_\lambda$. Then clearly $0 = \alpha\beta(e_\sigma) = \sum_\lambda x_{\lambda\sigma} n_\lambda$, and

$$\textstyle 0 = \sum_\lambda m_\lambda \otimes e_\lambda - \sum_\sigma m_\sigma \otimes \left(\sum_\lambda x_{\lambda\sigma} e_\lambda \right) = \sum_\lambda \left(m_\lambda - \sum_\sigma x_{\lambda\sigma} m_\sigma \right) \otimes e_\lambda.$$

Since the e_λ are independent, $m_\lambda = \sum_\sigma x_{\lambda\sigma} m_\sigma$, as asserted. □

(8.17) (Algebras). — Let R be a ring, R_1 and R_2 algebras with structure maps $\sigma\colon R \to R_1$ and $\tau\colon R \to R_2$. Set

$$R' := R_1 \otimes_R R_2.$$

It is an R-module. Now, define $R_1 \times R_2 \times R_1 \times R_2 \to R'$ by $(s, t, s', t') \mapsto ss' \otimes tt'$.

This map is clearly linear in each factor. So it induces a bilinear map

$$\mu\colon R'\times R'\to R' \quad\text{with}\quad \mu(s\otimes t,\, s'\otimes t')=(ss'\otimes tt').$$

It is easy to check that R' is a ring with μ as product. In fact, R' is an R-algebra with structure map ω given by $\omega(r):=\sigma(r)\otimes 1=1\otimes\tau(r)$, called the **tensor product** of R_1 and R_2 over R.

Define $\iota_1\colon R_1\to R'$ by $\iota_{R_1}(s):=s\otimes 1$. Clearly ι_1 is an R-algebra homomorphism. Define $\iota_2\colon R_2\to R_1\otimes R_2$ similarly. Given an R-algebra R'', define a map

$$\gamma\colon \operatorname{Hom}_{((R\text{-alg}))}(R',\,R'')\to \operatorname{Hom}_{((R\text{-alg}))}(R_1,\,R'')\times \operatorname{Hom}_{((R\text{-alg}))}(R_2,\,R'').$$

by $\gamma(\psi):=(\psi\iota_1,\,\psi\iota_2)$. Conversely, given R-algebra homomorphisms $\theta\colon R_1\to R''$ and $\zeta\colon R_2\to R''$, define $\eta\colon R_1\times R_2\to R''$ by $\eta(s,t):=\theta(s)\cdot\zeta(t)$. Then η is clearly bilinear, so it defines a linear map $\psi\colon R'\to R''$. It is easy to see that the map $(\theta,\zeta)\mapsto\psi$ is an inverse to γ. Thus γ is bijective.

In other words, $R':=R_1\otimes_R R_2$ is the **coproduct** $R_1\coprod R_2$ in $((R\text{-alg}))$:

$$\begin{tikzcd}
& R_1 \arrow[dr, "\iota_1"] \arrow[drr, "\theta"] & & \\
R \arrow[ur, "\sigma"] \arrow[dr, "\tau"'] & & R_1\otimes R_2 \arrow[r, "\psi"] & R'' \\
& R_2 \arrow[ur, "\iota_2"] \arrow[urr, "\zeta"'] & &
\end{tikzcd}$$

Example (8.18). — Let R be a ring, R' an algebra, and $\mathcal{X}:=\{X_\lambda\}$ a set of variables. Let's see that there is a canonical R'-algebra isomorphism

$$R'\otimes_R R[\mathcal{X}]=R'[\mathcal{X}].$$

Given an R'-algebra homomorphism $R'\to R''$ and elements x_λ of R'', there is an R-algebra homomorphism $R[\mathcal{X}]\to R''$ by **(1.3)**. So by **(8.17)**, there is a unique R'-algebra homomorphism $R'\otimes_R R[\mathcal{X}]\to R''$. Thus both $R'\otimes_R R[\mathcal{X}]\to R''$ and $R'[\mathcal{X}]$ have the same UMP. In particular, for another set of variables $\mathcal{Y}$, we obtain

$$R[\mathcal{X}]\otimes_R R[\mathcal{Y}]=R[\mathcal{X}][\mathcal{Y}]=R[\mathcal{X},\mathcal{Y}].$$

However, for formal power series rings, the corresponding statements may fail. For example, let k be a field, and X, Y variables. Then the image T of $k[[X]]\otimes k[[Y]]$ in $k[[X,Y]]$ consists of the H of the form $\sum_{i=1}^n F_iG_i$ for some n and $F_i\in k[[X]]$ and $G_i\in k[[Y]]$. Say $G_i=\sum_{j=0}^\infty g_{ij}Y^j$ with $g_{ij}\in k$. Then $F_iG_i=\sum_{j=0}^\infty F_ig_{ij}Y^j$. Say $H=\sum_{j=0}^\infty H_jY^j$ with $H_j\in k[[X]]$. Then $H_j=\sum_{i=1}^n F_ig_{ij}$. So all the H_j lie in the vector subspace of $k[[X]]$ spanned by $F_1,\dots,F_n$. Now, $1, X, X^2,\dots$ lie in no finite-dimensional subspace. Thus $\sum X^iY^j\notin T$. Thus $T\neq k[[X,Y]]$.

(8.19) (Diagonal Ideal). — Let R be a ring, R' an algebra, $\mu\colon R'\otimes_R R'\to R'$ the multiplication map. Call $\operatorname{Ker}(\mu)$ the **diagonal ideal** of R', and denote it by $\mathfrak{d}_{R'}$.

For example, take R' to be the polynomial ring in a set of variables $\mathcal{X}:=\{X_\lambda\}$. Then **(8.18)** yields $R'\otimes_R R'=R[\mathcal{T}\cup\mathcal{U}]$ where $\mathcal{T}:=\{T_\lambda\}$ with $T_\lambda:=X_\lambda\otimes 1$ and $\mathcal{U}:=\{U_\lambda\}$ with $U_\lambda:=1\otimes X_\lambda$ for all λ. Plainly $\mu(U_\lambda-T_\lambda)=0$. Further, **(1.17)**(5) yields $R[\mathcal{T}][\mathcal{U}]/\langle\{U_\lambda-T_\lambda\}\rangle=R[\mathcal{T}]$. Thus $\mathfrak{d}_{R'}=\langle\{U_\lambda-T_\lambda\}\rangle$.

More generally, let $\mathcal{G}$ be a set of generators of R' as an R-algebra, and $\mathfrak{d}$ the ideal of $R'\otimes_R R'$ generated by the elements $g\otimes 1-1\otimes g$ for $g\in\mathcal{G}$. Then $\mathfrak{d}=\mathfrak{d}_{R'}$ by **(8.7)**(4) with $M:=N:=R':=R'$, because $R\otimes_R R=R$ by **(8.5)**(2).

B. Exercises

Exercise (8.20) . — Let R be a ring, R' and R'' algebras, M' an R'-module and M'' an R''-module. Say $\{m'_\lambda\}$ generates M' over R' and $\{m''_\mu\}$ generates M'' over R''. Show $\{m'_\lambda \otimes m''_\mu\}$ generates $M' \otimes_R M''$ over $R' \otimes_R R''$.

Exercise (8.21) . — Let R be a ring, R' an R- algebra, and M an R'-module. Set $M' := R' \otimes_R M$. Define $\alpha\colon M \to M'$ by $\alpha m := 1 \otimes m$, and $\rho\colon M' \to M$ by $\rho(x \otimes m) := xm$. Prove M is a direct summand of M' with $\alpha = \iota_M$ and $\rho = \pi_M$.

Exercise (8.22) . — Let R be a domain, $\mathfrak{a}$ a nonzero ideal. Set $K := \mathrm{Frac}(R)$. Show that $\mathfrak{a} \otimes_R K = K$.

Exercise (8.23) . — In the setup of (8.9), find the unit η_M of each adjunction.

Exercise (8.24) . — Let M and N be nonzero k-vector spaces. Prove $M \otimes N \neq 0$.

Exercise (8.25) . — Let R be a nonzero ring. Show
(1) Assume there is a surjective map $\alpha\colon R^n \twoheadrightarrow R^m$. Then $n \geq m$.
(2) Assume $R^n \simeq R^m$. Then $n = m$.

Exercise (8.26) . — Under the conditions of (5.41)(1), set$K := \mathrm{Frac}(R)$. Show
$$\mathrm{rank}(F) = \dim_K(M \otimes K).$$

Exercise (8.27) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module.
(1) Use (8.10) to show that $(R/\mathfrak{a}) \otimes M = M/\mathfrak{a}M$.
(2) Use (1) and (4.21) to show that $(R/\mathfrak{a}) \otimes (M/\mathfrak{b}M) = M/(\mathfrak{a}+\mathfrak{b})M$.

Exercise (8.28) . — Let R be a ring, B an algebra, B' and B'' algebras over B. Regard B as an $(B \otimes_R B)$-algebra via the multiplication map. Set $C := B' \otimes_R B''$. Prove these formulas: (1) $B' \otimes_B B'' = C/\mathfrak{d}_B C$ and (2) $B' \otimes_B B'' = B \otimes_{B \otimes_R B} C$.

Exercise (8.29) . — Show $\mathbb{Z}/\langle m\rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle n\rangle = 0$ if m and n are relatively prime.

Exercise (8.30) . — Let R be a ring, R' and R'' algebras, $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ ideals. Let $\mathfrak{b} \subset R' \otimes_R R''$ denote the ideal generated by $\mathfrak{a}'$ and $\mathfrak{a}''$. Show that
$$(R' \otimes_R R'')/\mathfrak{b} = (R'/\mathfrak{a}') \otimes_R (R''/\mathfrak{a}'').$$

Exercise (8.31) . — Let R be a ring, M a module, $\mathcal{X}$ a set of variables. Prove the equation $M \otimes_R R[\mathcal{X}] = M[\mathcal{X}]$.

Exercise (8.32) . — Generalize (4.20) to several variables $X_1, \ldots, X_r$ via this standard device: reduce to the case of one variable Y by taking a suitably large d and defining $\varphi\colon R[X_1, \ldots, X_r] \to R[Y]$ by $\varphi(X_i) := Y^{d^i}$ and setting $\alpha := 1_M \otimes \varphi$.

Exercise (8.33) . — Let R be a ring, R_σ for $\sigma \in \Sigma$ algebras. For each finite subset J of Σ, let R_J be the tensor product of the R_σ for $\sigma \in J$. Prove that the assignment $J \mapsto R_J$ extends to a filtered direct system and that $\varinjlim R_J$ exists and is the coproduct $\coprod R_\sigma$.

Exercise (8.34) . — Let X be a variable, ω a complex cube root of 1, and $\sqrt[3]{2}$ the real cube root of 2. Set $k := \mathbb{Q}(\omega)$ and $K := k[\sqrt[3]{2}]$. Show $K = k[X]/\langle X^3 - 2\rangle$ and then $K \otimes_k K = K \times K \times K$.

9. Flatness

A module is called **flat** if tensor product with it is an exact functor, **faithfully flat** if this functor is also **faithful**—that is, carries nonzero maps to nonzero maps. First, we study exact functors, then flat and faithfully flat modules. Notably, we prove Lazard's Theorem, which characterizes flat modules as filtered direct limits of free modules of finite rank. Lazard's Theorem yields the Ideal Criterion, which characterizes the flat modules as those whose tensor product with any finitely generated ideal is equal to the ordinary product.

A. Text

Lemma (9.1). — *Let R be a ring, $\alpha\colon M \to N$ a homomorphism of modules. Then there is a commutative diagram with two short exact sequences involving N'*

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] & M \arrow[rr, "\alpha"] \arrow[dr, "\alpha'"'] & & N \arrow[r] & N'' \arrow[r] & 0 \\ & 0 \arrow[r] & & N' \arrow[ur, "\alpha''"'] \arrow[r] & 0 \end{tikzcd} \tag{9.1.1}$$

if and only if $M' = \mathrm{Ker}(\alpha)$ and $N' = \mathrm{Im}(\alpha)$ and $N'' = \mathrm{Coker}(\alpha)$.

Proof: If the equations hold, then the second short sequence is exact owing to the definitions, and the first is exact since $\mathrm{Coim}(\alpha) \xrightarrow{\sim} \mathrm{Im}(\alpha)$ by **(4.9)**.

Conversely, given the commutative diagram with two short exact sequences, α'' is injective. So $\mathrm{Ker}(\alpha) = \mathrm{Ker}(\alpha')$. So $M' = \mathrm{Ker}(\alpha)$. So $N' = \mathrm{Coim}(\alpha)$ as α' is surjective. So $N' = \mathrm{Im}(\alpha)$. Hence $N'' = \mathrm{Coker}(\alpha)$. Thus the equations hold. □

(9.2) (Exact Functors). — Let R be a ring, R' an algebra, F a linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Call F **faithful** if the associated map

$$\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{R'}(FM,\, FN).$$

is injective, or equivalently, if $F\alpha = 0$ implies $\alpha = 0$.

Call F **exact** if it preserves exact sequences. For example, $\mathrm{Hom}(P, \bullet)$ is exact if and only if P is projective by **(5.16)**.

Call F **left exact** if it preserves kernels. When F is contravariant, call F **left exact** if it takes cokernels to kernels. For example, $\mathrm{Hom}(N, \bullet)$ and $\mathrm{Hom}(\bullet, N)$ are left exact covariant and contravariant functors.

Call F **right exact** if it preserves cokernels. Thus $M \otimes \bullet$ is right exact by **(8.10)**.

Proposition (9.3). — *Let R be a ring, R' an algebra, F an R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Then the following conditions are equivalent:*

(1) *F preserves exact sequences; that is, F is exact.*
(2) *F preserves short exact sequences.*
(3) *F preserves kernels and surjections.*
(4) *F preserves cokernels and injections.*
(5) *F preserves kernels and images.*

Proof: Trivially, (1) implies (2). In view of **(5.2)**, clearly (1) yields (3) and (4).

Assume (3). Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Since F preserves kernels, $0 \to FM' \to FM \to FM''$ is exact; since F preserves surjections, $FM \to FM'' \to 0$ is also exact. Thus (2) holds. Similarly, (4) implies (2).

Assume (2). Given $\alpha\colon M \to N$, form the diagram **(9.1.1)**. Applying F to it and using (2), we obtain a similar diagram for $F(\alpha)$. Hence **(9.1)** yields (5).

Finally, assume (5). Let $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ be exact; that is, $\operatorname{Ker}(\beta) = \operatorname{Im}(\alpha)$. Now, (5) yields $\operatorname{Ker}(F(\beta)) = F(\operatorname{Ker}(\beta))$ and $\operatorname{Im}(F(\alpha)) = F(\operatorname{Im}(\alpha))$. Therefore, $\operatorname{Ker}(F(\beta)) = \operatorname{Im}(F(\alpha))$. Thus (1) holds. □

(9.4) (Flatness). — We say an R-module M is **flat** over R or is R-**flat** if the functor $M \otimes_R \bullet$ is exact. It is equivalent by **(9.3)** that $M \otimes_R \bullet$ preserve injections since it preserves cokernels by **(8.10)**.

We say M is **faithfully flat** if $M \otimes_R \bullet$ is exact and faithful.

We say an R-algebra is **flat** or **faithfully flat** if it is so as an R-module.

Lemma (9.5). — *A direct sum $M := \bigoplus M_\lambda$ is flat if and only if every M_λ is flat. Further, M is faithfully flat if every M_λ is flat and at least one is faithfully flat.*

Proof: Let $\beta\colon N' \to N$ be an injective map. Then **(6.5)** and **(6.15)** yield

$$\left(\bigoplus M_\lambda\right) \otimes \beta = \bigoplus (M_\lambda \otimes \beta).$$

But the map $\bigoplus (M_\lambda \otimes \beta)$ is injective if and only if each summand $M_\lambda \otimes \beta$ is injective by **(5.4)**. The first assertion follows.

Further, $M \otimes N = \bigoplus (M_\lambda \otimes N)$ by **(8.10)**. So if $M \otimes N = 0$, then $M_\lambda \otimes N = 0$ for all λ. If also at least one M_λ is faithfully flat, then $N = 0$, as desired. □

Proposition (9.6). — *A nonzero free module is faithfully flat. Every projective module is flat.*

Proof: It's easy to extend **(8.5)**(2) to maps α; that is, $R \otimes \alpha = \alpha$. So R is faithfully flat over R. Thus by **(9.5)**, a nonzero free module is faithfully flat.

Every projective module is a direct summand of a free module by **(5.16)**, and thus is flat again by **(9.5)**. □

Example (9.7). — In **(9.5)**, consider the second assertion. Its converse needn't hold. For example, take a product ring $R := R_1 \times R_2$ with $R_i \neq 0$. By **(9.6)**, R is faithfully flat over R. But neither R_i is so, as $R_1 \otimes R_2 = R_1 \otimes (R/R_1) = R_1/R_1^2 = 0$.

Proposition (9.8). — *Let R be a ring, $0 \to M' \to M \to M'' \to 0$ an exact sequence of modules. Assume M'' is flat.*

(1) *Then $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact for any module N.*

(2) *Then M is flat if and only if M' is flat.*

Proof: By **(5.13)**, there is an exact sequence $0 \to K \to R^{\oplus \Lambda} \to N \to 0$. Tensor it with the given sequence to obtain the following commutative diagram:

$$\begin{tikzcd}
 & & & 0 \arrow[d] & \\
 & M'\otimes K \arrow[r] \arrow[d] & M\otimes K \arrow[r] \arrow[d] & M''\otimes K \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & M'\otimes R^{\oplus\Lambda} \arrow[r, "\beta"] \arrow[d] & M\otimes R^{\oplus\Lambda} \arrow[r] \arrow[d] & M''\otimes R^{\oplus\Lambda} & \\
 & M'\otimes N \arrow[r, "\gamma"] \arrow[d] & M\otimes N \arrow[d] & & \\
 & 0 & 0 & &
\end{tikzcd}$$

Here α and β are injective by Definition **(9.4)**, as M'' and $R^{\oplus\Lambda}$ are flat by hypothesis and by **(9.6)**. So the rows and columns are exact, as tensor product is right exact. Finally, the Snake Lemma, **(5.10)**, implies γ is injective. Thus (1) holds.

To prove (2), take an injection $N' \to N$, and form this commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & M'\otimes N' \arrow[r] \arrow[d, "\alpha'"'] & M\otimes N' \arrow[r] \arrow[d, "\alpha"'] & M''\otimes N' \arrow[r] \arrow[d, "\alpha''"'] & 0 \\
0 \arrow[r] & M'\otimes N \arrow[r] & M\otimes N \arrow[r] & M''\otimes N \arrow[r] & 0
\end{tikzcd}$$

Its rows are exact by (1).

Assume M is flat. Then α is injective. Hence α' is too. Thus M' is flat.

Conversely, assume M' is flat. Then α' is injective. But α'' is injective as M'' is flat. Hence α is injective by the Snake lemma. Thus M is flat. Thus (2) holds. □

Proposition (9.9). — *A filtered direct limit of flat modules* $\varinjlim M_\lambda$ *is flat.*

Proof: Let $\beta\colon N' \to N$ be injective. Then $M_\lambda \otimes \beta$ is injective for each λ since M_λ is flat. So $\varinjlim(M_\lambda \otimes \beta)$ is injective by the exactness of filtered direct limits, **(7.9)**. So $(\varinjlim M_\lambda) \otimes \beta$ is injective by **(8.10)**. Thus $\varinjlim M_\lambda$ is flat. □

Proposition (9.10). — *Let R and R' be rings, M an R-module, N an (R, R')-bimodule, and P an R'-module. Then there is a canonical R'-homomorphism*

$$\theta\colon \operatorname{Hom}_R(M, N) \otimes_{R'} P \to \operatorname{Hom}_R(M, N \otimes_{R'} P). \qquad \textbf{(9.10.1)}$$

Assume P is flat. If M is finitely generated, then θ is injective; if M is finitely presented, then θ is an isomorphism.

Proof: The map θ exists by Watts's Theorem, **(8.13)**, with R' for R, applied to $\operatorname{Hom}_R(M, N \otimes_{R'} \bullet)$. Explicitly, $\theta(\varphi \otimes p)(m) = \varphi(m) \otimes p$.

Clearly, θ is bijective if $M = R$. So θ is bijective if $M = R^n$ for any n, as $\operatorname{Hom}_R(\bullet, Q)$ preserves finite direct sums for any Q by **(4.13)**.

Assume that M is finitely generated. Then from **(5.13)**, we obtain a presentation $R^{\oplus\Sigma} \to R^n \to M \to 0$, with Σ finite if M is finitely presented. Since θ is natural, it yields this commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Hom}_R(M, N) \otimes_{R'} P \arrow[r] \arrow[d, "\theta"'] & \operatorname{Hom}_R(R^n, N) \otimes_{R'} P \arrow[r] \arrow[d, "\simeq"'] & \operatorname{Hom}_R(R^{\oplus\Sigma}, N) \otimes_{R'} P \arrow[d] \\
0 \arrow[r] & \operatorname{Hom}_R(M, N \otimes_{R'} P) \arrow[r] & \operatorname{Hom}_R(R^n, N \otimes_{R'} P) \arrow[r] & \operatorname{Hom}_R(R^{\oplus\Sigma}, N \otimes_{R'} P)
\end{tikzcd}$$

Its rows are exact owing to the left exactness of Hom and to the flatness of P. The right-hand vertical map is bijective if Σ is finite. The assertions follow. □

Definition (9.11). — Let R be a ring, M a module. Let Λ_M be the category whose objects are the pairs (R^m, α) where $\alpha\colon R^m \to M$ is a homomorphism, and whose maps $(R^m, \alpha) \to (R^n, \beta)$ are the homomorphisms $\varphi\colon R^m \to R^n$ with $\beta\varphi = \alpha$.

Proposition (9.12). — *Let R be a ring, M a module, and $(R^m, \alpha) \mapsto R^m$ the forgetful functor from Λ_M to $((R\text{-mod}))$. Then $M = \varinjlim_{(R^m,\alpha)\in\Lambda_M} R^m$.*

Proof: By the UMP, the $\alpha\colon R^m \to M$ induce a map $\zeta\colon \varinjlim R^m \to M$. Let's show ζ is bijective. First, ζ is surjective, because each $x \in M$ is in the image of $(R,\, \alpha_x)$ where $\alpha_x(r) := rx$.

For injectivity, let $y \in \mathrm{Ker}(\zeta)$. By construction, $\bigoplus_{(R^m,\alpha)} R^m \to \varinjlim R^m$ is surjective; see the proof of (**6.7**). So y is in the image of some finite sum $\bigoplus_{(R^{m_i},\, \alpha_i)} R^{m_i}$. Set $m := \sum m_i$. Then $\bigoplus R^{m_i} = R^m$. Set $\alpha := \sum \alpha_i$. Then y is the image of some $y' \in R^m$ under the insertion $\iota_m\colon R^m \to \varinjlim R^m$. But $y \in \mathrm{Ker}(\zeta)$. So $\alpha(y') = 0$.

Let $\theta, \varphi\colon R \rightrightarrows R^m$ be the homomorphisms with $\theta(1) := y'$ and $\varphi(1) := 0$. They yield maps in Λ_M. So, by definition of direct limit, they have the same compositions with the insertion ι_m. Hence $y = \iota_m(y') = 0$. Thus ζ is injective, so bijective. □

Theorem (9.13) (Lazard). — *Let R be a ring, M a module. Then the following conditions are equivalent:*

(1) *M is flat.*
(2) *Given a finitely presented module P, this version of* (**9.10.1**) *is surjective:*
$$\mathrm{Hom}_R(P, R) \otimes_R M \to \mathrm{Hom}_R(P, M).$$
(3) *Given a finitely presented module P and a map $\beta\colon P \to M$, there exists a factorization $\beta\colon P \xrightarrow{\gamma} R^n \xrightarrow{\alpha} M$;*
(4) *Given an $\alpha\colon R^m \to M$ and a $k \in \mathrm{Ker}(\alpha)$, there exists a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi(k) = 0$.*
(5) *Given an $\alpha\colon R^m \to M$ and $k_1, \ldots, k_r \in \mathrm{Ker}(\alpha)$ there exists a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi(k_i) = 0$ for $i = 1, \ldots, r$.*
(6) *Given $R^r \xrightarrow{\rho} R^m \xrightarrow{\alpha} M$ such that $\alpha\rho = 0$, there exists a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi\rho = 0$.*
(7) *Λ_M is filtered.*
(8) *M is a filtered direct limit of free modules of finite rank.*

Proof: Assume (1). Then (**9.10**) yields (2).

Assume (2). Consider (3). There are $\gamma_1, \ldots, \gamma_n \in \mathrm{Hom}(P, R)$ and $x_1, \ldots, x_n \in M$ with $\beta(p) = \sum \gamma_i(p) x_i$ by (2). Let $\gamma\colon P \to R^n$ be $(\gamma_1, \ldots, \gamma_n)$, and let $\alpha\colon R^n \to M$ be given by $\alpha(r_1, \ldots, r_n) = \sum r_i x_i$. Then $\beta = \alpha\gamma$, just as (3) requires.

Assume (3), and consider (4). Set $P := R^m/Rk$, and let $\kappa\colon R^m \to P$ denote the quotient map. Then P is finitely presented, and there is $\beta\colon P \to M$ such that $\beta\kappa = \alpha$. By (3), there is a factorization $\beta\colon P \xrightarrow{\gamma} R^n \to M$. Set $\varphi := \gamma\kappa$. Then $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ is a factorization, and $\varphi(k) = 0$, just as (4) requires.

Assume (4), and consider (5). Set $m_0 := m$ and $\alpha_0 = \alpha$. Inductively, (4) yields
$$\alpha_{i-1}\colon R^{m_{i-1}} \xrightarrow{\varphi_i} R^{m_i} \xrightarrow{\alpha_i} M \quad \text{for} \quad i = 1, \ldots, r$$
such that $\varphi_i \cdots \varphi_1(k_i) = 0$. Set $\varphi := \varphi_r \cdots \varphi_1$ and $n := m_r$. Then (5) holds.

Assume (5), and consider (6). Let $e_1, \dots, e_r$ be the standard basis of R^r, and set $k_i := \rho(e_i)$. Then $\alpha(k_i) = 0$. So (5) yields a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ such that $\varphi(k_i) = 0$. Then $\varphi\rho = 0$, as required by (6).

Assume (6). Given (R^{m_1}, α_1) and (R^{m_2}, α_2) in Λ_M, set $m := m_1 + m_2$ and $\alpha := \alpha_1 + \alpha_2$. Then the inclusions $R^{m_i} \to R^m$ induce maps in Λ_M. Thus the first condition of **(7.1)** is satisfied.

Given $\sigma, \tau\colon (R^r, \omega) \rightrightarrows (R^m, \alpha)$ in Λ_M, set $\rho := \sigma - \tau$. Then $\alpha\rho = 0$. So (6) yields a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \to M$ with $\varphi\rho = 0$. Then φ is a map of Λ_M, and $\varphi\sigma = \varphi\tau$. Hence the second condition of **(7.1)** is satisfied. Thus (7) holds.

If (7) holds, then (8) does too, since $M = \varinjlim_{(R^m,\alpha)\in\Lambda_M} R^m$ by **(9.12)**.

Assume (8). Say $M = \varinjlim M_\lambda$ with the M_λ free. Each M_λ is flat by **(9.6)**, and a filtered direct limit of flat modules is flat by **(9.9)**. Thus M is flat, or (1) holds. □

Exercise (9.14) (*Equational Criterion for Flatness*) . — Prove that Condition **(9.13)**(4) can be reformulated as follows: Given any relation $\sum_i x_i m_i = 0$ with $x_i \in R$ and $m_i \in M$, there are $x_{ij} \in R$ and $m'_j \in M$ such that

$$\textstyle\sum_j x_{ij} m'_j = m_i \text{ for all } i \text{ and } \sum_i x_{ij} x_i = 0 \text{ for all } j. \qquad \textbf{(9.14.1)}$$

Lemma (9.15) (Ideal Criterion for Flatness)**. —** *A module M is flat if and only if, given any finitely generated ideal $\mathfrak{a}$, the inclusion $\mathfrak{a} \hookrightarrow R$ induces an injection $\mathfrak{a} \otimes M \hookrightarrow M$, or equivalently, an isomorphism $\mathfrak{a} \otimes M \xrightarrow{\sim} \mathfrak{a}M$.*

Proof: In any case, **(8.5)**(2) implies $R \otimes M \xrightarrow{\sim} M$ with $a \otimes m \mapsto am$. So the inclusion induces a map $\alpha\colon \mathfrak{a} \otimes M \to M$, with $\operatorname{Im}(\alpha) = \mathfrak{a}M$. Thus the two conditions are equivalent, and they hold if M is flat, as then α is injective.

To prove the converse, let's check **(9.14)**. Given $\sum_{i=1}^n x_i m_i = 0$ with $x_i \in R$ and $m_i \in M$, set $\mathfrak{a} := \langle x_1, \dots, x_n \rangle$. If $\mathfrak{a} \otimes M \xrightarrow{\sim} \mathfrak{a}M$, then $\sum_i x_i \otimes m_i = 0$; so **(8.5)**(1) and the Equational Criterion for Vanishing **(8.16)** yield **(9.14.1)**. □

Example (9.16). — Let R be a domain, and set $K := \operatorname{Frac}(R)$. Then K is flat, but K is not projective unless $R = K$. Indeed, **(8.22)** says $\mathfrak{a} \otimes_R K = K$, with $a \otimes x = ax$, for any ideal $\mathfrak{a}$ of R. So K is flat by **(9.15)**.

Suppose K is projective. Then $K \hookrightarrow R^\Lambda$ for some Λ by **(5.16)**. So there is a nonzero map $\alpha\colon K \to R$. So there is an $x \in K$ with $\alpha(x) \neq 0$. Set $a := \alpha(x)$. Take any nonzero $b \in R$. Then $ab \cdot \alpha(x/ab) = \alpha(x) = a$. Since R is a domain, $b \cdot \alpha(x/ab) = 1$. Hence $b \in R^\times$. Thus R is a field. So **(2.3)** yields $R = K$.

B. Exercises

Exercise (9.17) . — Let R be a ring, $\mathfrak{a}$ an ideal. Show $\Gamma_{\mathfrak{a}}(\bullet)$ is a left exact functor.

Exercise (9.18) . — Let R be a ring, N a module, N_1 and N_2 submodules, R' an algebra, F an exact R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Prove:

$$F(N_1 \cap N_2) = F(N_1) \cap F(N_2) \quad \text{and} \quad F(N_1 + N_2) = F(N_1) + F(N_2).$$

Exercise (9.19) . — Let R be a ring, R' an algebra, F an R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Assume F is exact. Prove the following equivalent:

(1) F is faithful.
(2) An R-module M vanishes if FM does.

(3) $F(R/\mathfrak{m}) \neq 0$ for every maximal ideal $\mathfrak{m}$ of R.
(4) A sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ is exact if $FM' \xrightarrow{F\alpha} FM \xrightarrow{F\beta} FM''$ is.

Exercise (9.20) . — Show that a ring of polynomials P is faithfully flat.

Exercise (9.21) . — Let R be a ring, M and N flat modules. Show that $M \otimes_R N$ is flat. What if “flat” is replaced everywhere by “faithfully flat”?

Exercise (9.22) . — Let R be a ring, M a flat module, R' an algebra. Show that $M \otimes_R R'$ is flat over R'. What if “flat” is replaced everywhere by “faithfully flat”?

Exercise (9.23) . — Let R be a ring, R' a flat algebra, M a flat R'-module. Show that M is flat over R. What if “flat” is replaced everywhere by “faithfully flat”?

Exercise (9.24) . — Let R be a ring, R' and R'' algebras, M' a flat R'-module, and M'' a flat R''-module. Show that $M' \otimes_R M''$ is a flat $(R' \otimes_R R'')$-module. What if “flat” is replaced everywhere by “faithfully flat”?

Exercise (9.25) . — Let R be a ring, R' an algebra, and M an R'-module. Assume that M is flat over R and faithfully flat over R'. Show that R' is flat over R.

Exercise (9.26) . — Let R be a ring, R' an algebra, R'' an R'-algebra, and M an R'-module. Assume that R'' is flat over R' and that M is flat over R. Show that $R'' \otimes_{R'} M$ is flat over R. Conversely, assume that R'' is faithfully flat over R' and that $R'' \otimes_{R'} M$ is flat over R. Show that M is flat over R.

Exercise (9.27) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $R/\mathfrak{a}$ is flat. Show $\mathfrak{a} = \mathfrak{a}^2$.

Exercise (9.28) . — Let R be a ring, R' a flat algebra. Prove equivalent:
(1) R' is faithfully flat over R.
(2) For every R-module M, the map $M \xrightarrow{\alpha} M \otimes_R R'$ by $\alpha m = m \otimes 1$ is injective.
(3) Every ideal $\mathfrak{a}$ of R is the contraction of its extension, or $\mathfrak{a} = (\mathfrak{a}R')^c$.
(4) Every prime $\mathfrak{p}$ of R is the contraction of some prime $\mathfrak{q}$ of R', or $\mathfrak{p} = \mathfrak{q}^c$.
(5) Every maximal ideal $\mathfrak{m}$ of R extends to a proper ideal, or $\mathfrak{m}R' \neq R'$.
(6) Every nonzero R-module M extends to a nonzero module, or $M \otimes_R R' \neq 0$.

Exercise (9.29) . — Let R be a ring, R' a faithfully flat algebra. Assume R' is local. Prove R is local too.

Exercise (9.30) . — Let R be a ring, $0 \to M' \xrightarrow{\alpha} M \to M'' \to 0$ an exact sequence with M flat. Assume $N \otimes M' \xrightarrow{N\otimes\alpha} N \otimes M$ is injective for all N. Prove M'' is flat.

Exercise (9.31) . — Prove that an R-algebra R' is faithfully flat if and only if the structure map $\varphi\colon R \to R'$ is injective and the quotient $R'/\varphi R$ is flat over R.

Exercise (9.32) . — Let R be a ring, $0 \to M_n \to \cdots \to M_1 \to 0$ an exact sequence of flat modules, and N any module. Then the following sequence is exact:

$$0 \to M_n \otimes N \to \cdots - \to M_1 \otimes N \to 0. \tag{9.32.1}$$

Exercise (9.33) . — Let R be a ring, R' an algebra, M and N modules.
(1) Show that there is a canonical R'-homomorphism

$$\sigma\colon \operatorname{Hom}_R(M, N) \otimes_R R' \to \operatorname{Hom}_{R'}(M \otimes_R R', N \otimes_R R').$$

(2) Assume M is finitely generated and projective. Show that σ is bijective.
(3) Assume R' is flat over R. Show that if M is finitely generated, then σ is injective, and that if M is finitely presented, then σ is bijective.

Exercise (9.34) . — Let R be a ring, M a module, and R' an algebra. Prove $\mathrm{Ann}_R(M)R' \subset \mathrm{Ann}_{R'}(M \otimes_R R')$, with equality if M is finitely generated, R' flat.

Exercise (9.35) . — Let R be a ring, M a module. Prove (1) if M is flat, then for $x \in R$ and $m \in M$ with $xm = 0$, necessarily $m \in \mathrm{Ann}(x)M$, and (2) the converse holds if R is a **Principal Ideal Ring** (PIR); that is, every ideal $\mathfrak{a}$ is principal.

10. Cayley–Hamilton Theorem

The Cayley–Hamilton Theorem says that a matrix satisfies its own characteristic polynomial. We prove it via a useful equivalent form, known as the "Determinant Trick." Using the Trick, we obtain various results, including the uniqueness of the rank of a finitely generated free module. We also obtain and apply Nakayama's Lemma, which asserts that a finitely generated module must vanish if it is equal to its product with any ideal lying in every maximal ideal containing its annihilator.

Then we turn to two important notions for an algebra: **integral dependence**, where every element of the algebra satisfies a monic polynomial equation, and **module finiteness**, where the algebra is a finitely generated module. Using the Trick, we relate these notions to each other, and study their properties. We end with a discussion of **normal domains**; they contain every element of their fraction field satisfying a monic polynomial equation.

A. Text

(10.1) (Cayley–Hamilton Theorem). — Let R be a ring, and $\mathbf{M} := (a_{ij})$ an $n \times n$ matrix with $a_{ij} \in R$. Let $\mathbf{I}_n$ be the $n \times n$ identity matrix, and T a variable. The **characteristic polynomial** of $\mathbf{M}$ is the following polynomial:

$$P_{\mathbf{M}}(T) := T^n + a_1 T^{n-1} + \cdots + a_n := \det(T\mathbf{I}_n - \mathbf{M}).$$

Let $\mathfrak{a}$ be an ideal. If $a_{ij} \in \mathfrak{a}$ for all i, j, then clearly $a_k \in \mathfrak{a}^k$ for all k.

The **Cayley–Hamilton Theorem** asserts that, in the ring of matrices,

$$P_{\mathbf{M}}(\mathbf{M}) = 0.$$

It is a special case of **(10.2)** below; indeed, take $M := R^n$, take $m_1, \ldots, m_n$ to be the standard basis, and take φ to be the endomorphism defined by $\mathbf{M}$.

Conversely, given the setup of **(10.2)**, form the surjection $\alpha\colon R^n \twoheadrightarrow M$ taking the ith standard basis element e_i to m_i, and form the map $\Phi\colon R^n \to R^n$ associated to the matrix $\mathbf{M}$. Then $\varphi\alpha = \alpha\Phi$. Hence, given any polynomial $F(T)$, we have $F(\varphi)\alpha = \alpha F(\Phi)$. Hence, if $F(\Phi) = 0$, then $F(\varphi) = 0$ as α is surjective. Thus *the Cayley–Hamilton Theorem and the Determinant Trick* **(10.2)** *are equivalent.*

Theorem (10.2) (Determinant Trick). **—** *Let M be an R-module generated by $m_1, \ldots, m_n$, and $\varphi\colon M \to M$ an endomorphism. Say $\varphi(m_i) =: \sum_{j=1}^n a_{ij} m_j$ with $a_{ij} \in R$, and form the matrix $\mathbf{M} := (a_{ij})$. Then $P_{\mathbf{M}}(\varphi) = 0$ in $\operatorname{End}(M)$.*

Proof: Let δ_{ij} be the Kronecker delta function, $\mu_{a_{ij}}$ the multiplication map. Let $\mathbf{\Delta}$ stand for the matrix $(\delta_{ij}\varphi - \mu_{a_{ij}})$ with entries in the commutative subring $R[\varphi]$ of $\operatorname{End}(M)$, and $\mathbf{X}$ for the column vector (m_j). Clearly $\mathbf{\Delta X} = 0$. Multiply on the left by the **matrix of cofactors $\mathbf{\Gamma}$** of $\mathbf{\Delta}$: the (i, j)th entry of $\mathbf{\Gamma}$ is $(-1)^{i+j}$ times the determinant of the matrix obtained by deleting the jth row and the ith column of $\mathbf{\Delta}$. Then $\mathbf{\Gamma\Delta X} = 0$. But $\mathbf{\Gamma\Delta} = \det(\mathbf{\Delta})\mathbf{I}_n$. So $\det(\mathbf{\Delta})m_j = 0$ for all j. Hence $\det(\mathbf{\Delta}) = 0$. But $\det(\mathbf{\Delta}) = P_{\mathbf{M}}(\varphi)$. Thus $P_{\mathbf{M}}(\varphi) = 0$. □

Proposition (10.3). — *Let M be a finitely generated module, $\mathfrak{a}$ an ideal. Then $M = \mathfrak{a}M$ if and only if there exists $a \in \mathfrak{a}$ such that $(1 + a)M = 0$.*

Proof: Assume $M = \mathfrak{a}M$. Say $m_1, \dots, m_n$ generate M, and $m_i = \sum_{j=1}^n a_{ij} m_j$ with $a_{ij} \in \mathfrak{a}$. Set $\mathbf{M} := (a_{ij})$. Say $P_{\mathbf{M}}(T) = T^n + a_1 T^{n-1} + \cdots + a_n$. Set $a := a_1 + \cdots + a_n \in \mathfrak{a}$. Then $(1 + a)M = 0$ by **(10.2)** with $\varphi := 1_M$.

Conversely, if there exists $a \in \mathfrak{a}$ such that $(1 + a)M = 0$, then $m = -am$ for all $m \in M$. So $M \subset \mathfrak{a}M \subset M$. Thus $M = \mathfrak{a}M$. □

Corollary (10.4). — *Let R be a ring, M a finitely generated module, and φ an endomorphism of M. If φ is surjective, then φ is an isomorphism.*

Proof: Note $\mathrm{End}(M)$ is an R-algebra; see **(4.4)**. Let X be a variable, and set $P := R[X]$. By the UMP of P, there's an R-algebra map $\mu\colon P \to \mathrm{End}(M)$ with $\mu(X) = \varphi$. So M is a P-module such that $F(X)M = F(\varphi)M$ for any $F(X) \in P$ again by **(4.4)**. Set $\mathfrak{a} := \langle X \rangle$. Since φ is surjective, $M = \mathfrak{a}M$. By **(10.3)**, there is $a \in \mathfrak{a}$ with $(1 + a)M = 0$. Say $a = XG(X)$ for some polynomial $G(X)$. Then $1_M + \varphi G(\varphi) = 0$. Set $\psi = -G(\varphi)$. Then $\varphi\psi = 1_M$ and $\psi\varphi = 1_M$. Thus φ is an isomorphism. □

Corollary (10.5). — *Let R be a nonzero ring, m and n positive integers.*

(1) *Then any n generators $v_1, \dots, v_n$ of the free module R^n form a free basis.*

(2) *If $R^m \simeq R^n$, then $m = n$.*

Proof: Form the surjection $\varphi\colon R^n \twoheadrightarrow R^n$ taking the ith standard basis element to v_i. Then φ is an isomorphism by **(10.4)**. So the v_i form a free basis by **(4.10)**(3).

To prove (2), say $m \le n$. Then R^n has m generators. Add to them $n - m$ zeros. The result is a free basis by (1); so it can contain no zeros. Thus $n - m = 0$. □

Lemma (10.6) (Nakayama's). — *Let R be a ring, M a module, $\mathfrak{m} \subset \mathrm{rad}(M)$ an ideal. Assume M is finitely generated and $M = \mathfrak{m}M$. Then $M = 0$.*

Proof: By **(10.3)**, there's $a \in \mathfrak{m}$ with $(1 + a)M = 0$. But $\mathfrak{m} \subset \mathrm{rad}(M)$. Thus **(4.15)** implies $M = 0$.

Alternatively, suppose $M \ne 0$. Say $m_1, \dots, m_n$ generate M with n minimal. Then $n \ge 1$ and $m_1 = a_1 m_1 + \cdots + a_n m_n$ with $a_i \in \mathfrak{m}$. Set $M' := M/\langle a_2, \dots, a_n \rangle M$, and let $m_1' \in M'$ be the residue of m_1. Then $m_1' \ne 0$ as n is minimal. But $(1 - a_1)m_1' = 0$ and $a_1 \in \mathrm{rad}(M) \subset \mathrm{rad}(M')$, contradicting **(4.15)**. □

Example (10.7). — Nakayama's Lemma **(10.6)** may fail if the module is not finitely generated. For example, let A be a local domain, $\mathfrak{m}$ the maximal ideal, and K the fraction field. Assume A is not a field, so that there's a nonzero $x \in \mathfrak{m}$. Then any $z \in K$ can be written in the form $z = x(z/x)$. Thus $K = \mathfrak{m}K$, but $K \ne 0$.

However, there are important cases where it does hold even if the module is not, a priori, finitely generated. See **(3.31)**, **(20.30)**, and **(22.69)**.

Proposition (10.8). — *Let R be a ring, $N \subset M$ modules, $\mathfrak{m} \subset \mathrm{rad}(M)$ an ideal.*

(1) *If M/N is finitely generated and if $N + \mathfrak{m}M = M$, then $N = M$.*

(2) *Assume M is finitely generated. Then $m_1, \dots, m_n \in M$ generate M if and only if their images $m_1', \dots, m_n'$ generate $M' := M/\mathfrak{m}M$.*

Proof: For (1), note $N + \mathfrak{m}M = M$ if and only if $\mathfrak{m}(M/N) = M/N$. Also $\mathrm{Ann}(M/N) \supset \mathrm{Ann}(M)$; so $\mathrm{rad}(M/N) \supset \mathrm{rad}(M)$. But $\mathrm{rad}(M) \supset \mathfrak{m}$. Apply **(10.6)** with M/N for M to conclude $M/N = 0$. Thus (1) holds.

For (2), let N be the submodule generated by $m_1, \dots, m_n$. Since M is finitely generated, so is M/N. Thus $N = M$ if the m_i' generate $M/\mathfrak{m}M$ by (1). The converse is obvious. Thus (2) holds. □

Exercise (10.9) . — Let A be a local ring, $\mathfrak{m}$ the maximal ideal, M a finitely generated A-module, and $m_1, \ldots, m_n \in M$. Set $k := A/\mathfrak{m}$ and $M' := M/\mathfrak{m}M$, and write m_i' for the image of m_i in M'. Prove that $m_1', \ldots, m_n' \in M'$ form a basis of the k-vector space M' if and only if $m_1, \ldots, m_n$ form a **minimal generating set** of M (that is, no proper subset generates M), and prove that every minimal generating set of M has the same number of elements.

Exercise (10.10) . — Let A be a local ring, k its residue field, M and N finitely generated modules. Show: (1) $M = 0$ if and only if $M \otimes_A k = 0$.
(2) $M \otimes_A N \neq 0$ if $M \neq 0$ and $N \neq 0$.

(10.11) (Local Homomorphisms). — Let $\varphi\colon A \to B$ be a map of local rings, $\mathfrak{m}$ and $\mathfrak{n}$ their maximal ideals. Then the following three conditions are equivalent:

$$(1)\ \varphi^{-1}\mathfrak{n} = \mathfrak{m}; \quad (2)\ 1 \notin \mathfrak{m}B; \quad (3)\ \mathfrak{m}B \subset \mathfrak{n}. \qquad \textbf{(10.11.1)}$$

Indeed, if (1) holds, then $\mathfrak{m}B = (\varphi^{-1}\mathfrak{n})B \subset \mathfrak{n}$; so (2) holds. If (2) holds, then $\mathfrak{m}B$ lies is some maximal ideal, but $\mathfrak{n}$ is the only one; thus (3) holds. If (3) holds, then $\mathfrak{m} \subset \varphi^{-1}(\mathfrak{m}B) \subset \varphi^{-1}\mathfrak{n}$; whence, (1) holds as $\mathfrak{m}$ is maximal.

If the above conditions hold, then $\varphi\colon A \to B$ is called a **local homomorphism.**

Proposition (10.12). — *Consider these conditions on an R-module P:*
(1) *P is free and of finite rank;*
(2) *P is projective and finitely generated;*
(3) *P is flat and finitely presented.*
Then (1) *implies* (2), *and* (2) *implies* (3)*; all three are equivalent if R is local.*

Proof: A free module is always projective by **(5.15)**, and a projective module is always flat by **(9.6)**. Further, all of (1)–(3) require P to be finitely generated; so assume it is. Thus (1) implies (2).

Let $p_1, \ldots, p_n \in P$ generate, and let $0 \to L \to R^n \to P \to 0$ be the short exact sequence defined by sending the ith standard basis element to p_i. Set $F := R^n$.

Assume P is projective. Then the sequence splits by **(5.16)**. So **(5.8)** yields a surjection $\rho\colon F \to L$. Hence L is finitely generated. Thus (2) implies (3).

Assume P is flat and R is local. Denote the residue field of R by k. Then, by **(9.8)**(1), the sequence $0 \to L \otimes k \to F \otimes k \to P \otimes k \to 0$ is exact. Now, $F \otimes k = (R \otimes k)^n = k^n$ by **(8.10)** and the Unitary Law **(8.5)**(2); so $\dim_k F \otimes k = n$. Finally, rechoose the p_i so that n is minimal. Then $\dim_k P \otimes k = n$, because the $p_i \otimes 1$ form a basis by **(10.9)**. Therefore, $\dim_k L \otimes k = 0$; so $L \otimes k = 0$.

Assume P is finitely presented. Then L is finitely generated by **(5.18)**. Hence $L = 0$ by **(10.10)**(1). So $F = P$. Thus (3) implies (1). □

Definition (10.13). — Let R be a ring, R' an R-algebra. Then R' is said to be **module finite** over R if R' is a finitely generated R-module.

An element $x \in R'$ is said to be **integral over** R or **integrally dependent on** R if there exist a positive integer n and elements $a_i \in R$ such that

$$x^n + a_1x^{n-1} + \cdots + a_n = 0. \qquad \textbf{(10.13.1)}$$

Such an equation is called an **equation of integral dependence of degree** n.

If every $x \in R'$ is integral over R, then R' is said to be **integral over** R.

Proposition (10.14). — *Let R be a ring, R' an R-algebra, n a positive integer, and $x \in R'$. Then the following conditions are equivalent:*

(1) *x satisfies an equation of integral dependence of degree n.*
(2) *$R[x]$ is generated as an R-module by $1, x, \ldots, x^{n-1}$.*
(3) *x lies in a subalgebra R'' generated as an R-module by n elements.*
(4) *There is a faithful $R[x]$-module M generated over R by n elements.*

Proof: Assume (1) holds. Say $F(X)$ is a monic polynomial of degree n with $F(x) = 0$. For any m, let $M_m \subset R[x]$ be the R-submodule generated by $1, \ldots, x^m$. For $m \geq n$, clearly $x^m - x^{m-n}F(x)$ is in M_{m-1}. But $F(x) = 0$. So also $x^m \in M_{m-1}$. So by induction, $M_m = M_{n-1}$. Hence $M_{n-1} = R[x]$. Thus (2) holds.

If (2) holds, then trivially (3) holds with $R'' := R[x]$.

If (3) holds, then (4) holds with $M := R''$, as $xM = 0$ implies $x = x \cdot 1 = 0$.

Assume (4) holds. In **(10.2)**, take $\varphi := \mu_x$. We obtain a monic polynomial F of degree n with $F(x)M = 0$. Since M is faithful, $F(x) = 0$. Thus (1) holds. □

Corollary (10.15). — *Let R be a ring, $P := R[X]$ the polynomial ring in one variable X, and $\mathfrak{A} \subset P$ an ideal. Set $R' := P/\mathfrak{A}$, let $\kappa\colon P \twoheadrightarrow R'$ be the canonical map, and set $x := \kappa(X)$. Fix $n \geq 1$. Then these conditions are equivalent:*

(1) *$\mathfrak{A} = \langle F \rangle$ where F is a monic polynomial of degree n;.*
(2) *Set $M := \sum_{i=0}^{n-1} RX^i \subset P$ and $\varphi := \kappa|M$. Then $\varphi\colon M \to R'$ is bijective.*
(3) *$1, x, \ldots, x^{n-1}$ form a free basis of R' over R.*
(4) *R' is a free R-module of rank n.*

Proof: Assume (1) holds. Then $F(x) = 0$ is an equation of integral dependence of degree n. So $1, \ldots, x^{n-1}$ generate R' by (1)⇒(2) of **(10.14)**. Thus φ is surjective.

Given $G \in \operatorname{Ker}\varphi$, note $G \in \mathfrak{A}$. So $G = HF$ for some $H \in P$. But F is monic of degree n, whereas G is of degree less than n. So $G = 0$. Thus (2) holds.

In (2), note $1, \ldots, X^{n-1}$ form a free basis of M. Thus (2) implies (3).

Trivially, (3) implies (4).

Finally, assume (4) holds. Then (4)⇒(1) of **(10.14)** yields a monic polynomial $F \in \mathfrak{A}$ of degree n. Form the induced homomorphism $\psi\colon P/\langle F \rangle \to R'$. It is obviously surjective. Since (1) implies (4), the quotient $P/\langle F \rangle$ is free of rank n. So ψ is an isomorphism by **(10.4)**. Hence $\langle F \rangle = \mathfrak{A}$. Thus (1) holds. □

Lemma (10.16). — *Let R be a ring, R' a module-finite R-algebra, and M a finitely generated R'-module. Then M is a finitely generated R-module. If M is free of rank r over R' and if R' is free of rank r' over R, then M is free of rank rr' over R.*

Proof: Say elements x_i generate R' as a module over R, and m_j generate M over R'. Given $m \in M$, say $m = \sum a_j m_j$ with $a_j \in R'$, and say $a_j = \sum b_{ij} x_i$ with $b_{ij} \in R$. Then $m = \sum b_{ij} x_i m_j$. Thus the $x_i m_j$ generate M over R.

If $m = 0$, then $\sum_j \big(\sum_i b_{ij} x_i\big) m_j = 0$. So if also the m_j are free over R', then $\sum_i b_{ij} x_i = 0$ for all j. If in addition the x_i are free over R, then $b_{ij} = 0$ for all i, j. Thus the $x_i m_j$ are free over R. □

Theorem (10.17) (Tower Laws). — *Let R be a ring, R' an algebra, R'' an R'-algebra, and $x \in R''$.*

(1) *If x is integral over R', and R' is integral over R, then x is integral over R.*
(2) *If R'' is integral over R', and R' is so over R, then R'' is so over R.*
(3) *If R'' is module finite over R', and R' is so over R, then R'' is so over R.*

Proof: For (1), say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in R'$. For $m = 1, \ldots, n$, set $R_m := R[a_1, \ldots, a_m] \subset R''$. Then R_m is module finite over R_{m-1} by (1)⇒(2) of **(10.14)**. So R_m is module finite over R by **(10.16)** and induction on m.

Moreover, x is integral over R_n. So $R_n[x]$ is module finite over R_n by (1)⇒(2) of **(10.14)**. Hence $R_n[x]$ is module finite over R by **(10.16)**. So x is integral over R by (3)⇒(1) of **(10.14)**. Thus (1) holds.

Notice (2) is an immediate consequence of (1).

Notice (3) is a special case of **(10.16)**. □

Theorem (10.18). — *Let R be a ring, and R' an R-algebra. Then the following conditions are equivalent:*

(1) *R' is algebra finite and integral over R.*
(2) *$R' = R[x_1, \ldots, x_n]$ with all x_i integral over R.*
(3) *R' is module finite over R.*

Proof: Trivially, (1) implies (2).

Assume (2) holds. To prove (3), set $R'' := R[x_1] \subset R'$. Then R'' is module finite over R by (1)⇒(2) of **(10.14)**. We may assume R' is module finite over R'' by induction on n. So **(10.16)** yields (3).

If (3) holds, then R' is integral over R by (3)⇒(1) of **(10.14)**; so (1) holds. □

Definition (10.19). — Let R be a ring, R' an algebra. The **integral closure** or **normalization** of R in R' is the subset $\overline{R}$ of elements that are integral over R. If $R \subset R'$ and $R = \overline{R}$, then R is said to be **integrally closed** in R'.

If R is a domain, then its integral closure $\overline{R}$ in its fraction field $\mathrm{Frac}(R)$ is called simply its **normalization**, and R is said to be **normal** if $R = \overline{R}$.

Theorem (10.20). — *Let R be a ring, R' an R-algebra, $\overline{R}$ the integral closure of R in R'. Then $\overline{R}$ is an R-algebra, and is integrally closed in R'.*

Proof: Take $a \in R$ and $x, y \in \overline{R}$. Then the ring $R[x, y]$ is integral over R by (2)⇒(1) of **(10.18)**. So ax and $x + y$ and xy are integral over R. Thus $\overline{R}$ is an R-algebra. Finally, $\overline{R}$ is integrally closed in R' owing to **(10.17)**. □

Theorem (10.21) (Gauss)**. —** *A UFD is normal.*

Proof: Let R be the UFD. Given $x \in \mathrm{Frac}(R)$, say $x = r/s$ with $r, s \in R$ relatively prime. Suppose x satisfies **(10.13.1)**. Then

$$r^n = -(a_1r^{n-1} + \cdots + a_ns^{n-1})s.$$

So any prime element dividing s also divides r. Hence s is a unit. Thus $x \in R$. □

Example (10.22). — (1) A polynomial ring in n variables over a field is a UFD, so normal by **(10.21)**.

(2) The ring $R := \mathbb{Z}[\sqrt{5}]$ is not a UFD, since

$$(1 + \sqrt{5})(1 - \sqrt{5}) = -4 = -2 \cdot 2,$$

and $1 + \sqrt{5}$, and $1 - \sqrt{5}$ and 2 are irreducible, but not associates. However, set $\tau := (1 + \sqrt{5})/2$, the "golden ratio." The ring $\mathbb{Z}[\tau]$ is known to be a PID; see [17, p. 292]. Hence, $\mathbb{Z}[\tau]$ is a UFD, so normal by **(10.21)**; hence, $\mathbb{Z}[\tau]$ contains the normalization $\overline{R}$ of R. On the other hand, $\tau^2 - \tau - 1 = 0$; hence, $\mathbb{Z}[\tau] \subset \overline{R}$. Thus $\mathbb{Z}[\tau] = \overline{R}$.

(3) Let $d \in \mathbb{Z}$ be square-free. In the field $K := \mathbb{Q}(\sqrt{d})$, form $R := \mathbb{Z} + \mathbb{Z}\delta$ where

$$\delta := \begin{cases} (1+\sqrt{d})/2, & \text{if } d \equiv 1 \pmod 4; \\ \sqrt{d}, & \text{if not.} \end{cases}$$

Then R is the normalization $\overline{\mathbb{Z}}$ of $\mathbb{Z}$ in K; see [3, pp. 412–3].

(4) Let k be a field, $k[T]$ the polynomial ring in one variable. Set $R := k[T^2, T^3]$. Then $\mathrm{Frac}(R) = k(T)$. Further, T is integral over R as T satisfies $X^2 - T^2 = 0$; hence, $k[T] \subset \overline{R}$. However, $k[T]$ is normal by (1); hence, $k[T] \supset \overline{R}$. Thus $k[T] = \overline{R}$.

Let $k[X, Y]$ be the polynomial ring in two variables, and $\varphi\colon k[X, Y] \to R$ the k-algebra homomorphism defined by $\varphi(X) := T^2$ and $\varphi(Y) := T^3$. Clearly φ is surjective. Set $\mathfrak{p} := \mathrm{Ker}\,\varphi$. Since R is a domain, but not a field, $\mathfrak{p}$ is prime by **(2.8)**, but not maximal by **(2.13)**. Clearly $\mathfrak{p} \supset \langle Y^2 - X^3\rangle$. Since $Y^2 - X^3$ is irreducible, **(2.20)** implies that $\mathfrak{p} = \langle Y^2 - X^3\rangle$. So $k[X, Y]/\langle Y^2 - X^3\rangle \xrightarrow{\sim} R$, which provides us with another description of R.

B. Exercises

Exercise (10.23) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a}$ is finitely generated and idempotent (or $\mathfrak{a} = \mathfrak{a}^2$). Prove there is a unique idempotent e with $\langle e\rangle = \mathfrak{a}$.

Exercise (10.24) . — Let R be a ring, $\mathfrak{a}$ an ideal. Prove the following conditions are equivalent:

(1) $R/\mathfrak{a}$ is projective over R.
(2) $R/\mathfrak{a}$ is flat over R, and $\mathfrak{a}$ is finitely generated.
(3) $\mathfrak{a}$ is finitely generated and idempotent.
(4) $\mathfrak{a}$ is generated by an idempotent.
(5) $\mathfrak{a}$ is a direct summand of R.

Exercise (10.25) . — Prove the following conditions on a ring R are equivalent:

(1) R is **absolutely flat**; that is, every module is flat.
(2) Every finitely generated ideal is a direct summand of R.
(3) Every finitely generated ideal is idempotent.
(4) Every principal ideal is idempotent.

Exercise (10.26) . — Let R be a ring. Prove the following statements:

(1) Assume R is Boolean. Then R is absolutely flat.
(2) Assume R is absolutely flat. Then any quotient ring R' is absolutely flat.
(3) Assume R is absolutely flat. Then every nonunit x is a zerodivisor.
(4) Assume R is absolutely flat and local. Then R is a field.

Exercise (10.27) . — Let R be a ring, $\alpha\colon M \to N$ a map of modules, $\mathfrak{m}$ an ideal. Assume that $\mathfrak{m} \subset \mathrm{rad}(N)$, that N is finitely generated, and that the induced map $\overline{\alpha}\colon M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. Show that α is surjective too.

Exercise (10.28) . — Let R be a ring, $\mathfrak{m}$ an ideal, E a module, M, N submodules. Assume N is finitely generated, $\mathfrak{m} \subset \mathrm{rad}(N)$, and $N \subset M + \mathfrak{m}N$. Show $N \subset M$.

Exercise (10.29) . — Let R be a ring, $\mathfrak{m}$ an ideal, and $\alpha, \beta\colon M \rightrightarrows N$ two maps of finitely generated modules. Assume α is an isomorphism, $\mathfrak{m} \subset \mathrm{rad}(N)$, and $\beta(M) \subset \mathfrak{m}N$. Set $\gamma := \alpha + \beta$. Show γ is an isomorphism.

Exercise (10.30) . — Let $A \to B$ be a local homomorphism, M a finitely generated B-module. Prove that M is faithfully flat over A if and only if M is flat over A and nonzero. Conclude that, if B is flat over A, then B is faithfully flat over A.

Exercise (10.31) . — Let $A \to B$ be a flat local homomorphism, M a finitely generated A-module. Set $N := M \otimes B$. Assume N is cyclic. Show M is cyclic too. Conclude that an ideal $\mathfrak{a}$ of A is principal if its extension $\mathfrak{a}B$ is so.

Exercise (10.32) . — Let R be a ring, X a variable, R' an algebra, $n \geq 0$. Assume R' is a free R-module of rank n. Set $\mathfrak{m} := \mathrm{rad}(R)$ and $k := R/\mathfrak{m}$. Given a k-isomorphism $\widetilde{\varphi}\colon k[X]/\langle \widetilde{F} \rangle \xrightarrow{\sim} R'/\mathfrak{m}R'$ with $\widetilde{F}$ monic, show we can lift $\widetilde{\varphi}$ to an R-isomorphism $\varphi\colon R[X]/\langle F \rangle \xrightarrow{\sim} R'$ with F monic. Show F must then lift $\widetilde{F}$.

Exercise (10.33) . — Let R be a ring, $\mathfrak{a}$ an ideal, $P := R[X]$ the polynomial ring in one variable X, and $G_1, G_2, H \in P$ with G_1 monic of degree n. Show:

(1) Assume G_1 and G_2 are coprime. Then there are unique $H_1, H_2 \in P$ with $H = H_1G_1 + H_2G_2$ and $\deg(H_2) < n$.
(2) Assume the images of G_1 and G_2 are coprime in $(R/\mathfrak{a})[X]$ and $\mathfrak{a} \subset \mathrm{rad}(R)$. Then G_1 and G_2 are coprime.

Exercise (10.34) . — Let R be a ring, $\mathfrak{a} \subset \mathrm{rad}(R)$ an ideal, $P := R[X]$ the polynomial ring in one variable X, and $F, G, H \in P$. Assume that $F \equiv GH \pmod{\mathfrak{a}P}$, that G and H are coprime, and that G is monic, say of degree n. Show that there are coprime polynomials G', $H' \in P$ with G' monic of degree n, with $\deg(H') \leq \max\{\deg(H), \deg(F) - n\}$, and with

$$G \equiv G' \text{ and } H \equiv H' \pmod{\mathfrak{a}P} \quad \text{and} \quad F \equiv G'H' \pmod{\mathfrak{a}^2P}.$$

Exercise (10.35) . — Let G be a finite group acting on a ring R. Show that every $x \in R$ is integral over R^G, in fact, over its subring R' generated by the elementary symmetric functions in the conjugates gx for $g \in G$.

Exercise (10.36) . — Let R be a ring, R' an algebra, G a group that acts on R'/R, and $\overline{R}$ the integral closure of R in R'. Show that G acts canonically on $\overline{R}/R$.

Exercise (10.37) . — Let R be a normal domain, K its fraction field, L/K a **Galois extension** with group G, and $\overline{R}$ the integral closure of R in L. (By definition, G is the group of automorphisms of L/K and $K = L^G$.) Show $R = \overline{R}^G$.

Exercise (10.38) . — Let R'/R be an extension of rings. Assume $R' - R$ is closed under multiplication. Show that R is integrally closed in R'.

Exercise (10.39) . — Let R be a ring; C, R' two R-algebras; R'' an R'-algebra. If R'' is either (1) integral over R', or (2) module finite over R', or (3) algebra finite over R', show $R'' \otimes_R C$ is so over $R' \otimes_R C$.

Exercise (10.40) . — Let k be a field, $P := k[X]$ the polynomial ring in one variable, $F \in P$. Set $R := k[X^2] \subset P$. Using the free basis $1, X$ of P over R, find an explicit equation of integral dependence of degree 2 on R for F.

Exercise (10.41) . — Let $R_1, \ldots, R_n$ be R-algebras, integral over R. Show that their product $\prod R_i$ is integral over R.

Exercise (10.42) . — For $1 \le i \le r$, let R_i be a ring, R_i' an extension of R_i, and $x_i \in R_i'$. Set $R := \prod R_i$, set $R' := \prod R_i'$, and set $x := (x_1, \ldots, x_r)$. Prove
(1) x is integral over R if and only if x_i is integral over R_i for each i;
(2) R is integrally closed in R' if and only if each R_i is integrally closed in R_i'.

Exercise (10.43) . — Let k be a field, X and Y variables. Set
$$R := k[X, Y]/\langle Y^2 - X^2 - X^3 \rangle,$$
and let $x, y \in R$ be the residues of X, Y. Prove that R is a domain, but not a field. Set $t := y/x \in \mathrm{Frac}(R)$. Prove that $k[t]$ is the integral closure of R in $\mathrm{Frac}(R)$.

11. Localization of Rings

Localization generalizes construction of the fraction field of a domain. We localize an arbitrary ring using as denominators the elements of any given multiplicative subset. The result is universal among algebras rendering all these elements units. When the multiplicative subset is the complement of a prime ideal, we obtain a local ring. We relate the ideals in the original ring to those in the localized ring. Lastly, we localize algebras, vary the set of denominators, and discuss **decomposable** rings, which are the finite products of local rings.

A. Text

(11.1) (Localization). — Let R be a ring, and S a multiplicative subset. Define a relation on $R \times S$ by $(x, s) \sim (y, t)$ if there is $u \in S$ such that $xtu = ysu$.

This relation is an equivalence relation. Indeed, it is reflexive as $1 \in S$ and is trivially symmetric. As to transitivity, let $(y, t) \sim (z, r)$. Say $yrv = ztv$ with $v \in S$. Then $xturv = ysurv = ztvsu$. Thus $(x, s) \sim (z, r)$.

Denote by $S^{-1}R$ the set of equivalence classes, and by x/s the class of (x, s).

Define $x/s \cdot y/t := xy/st$. This product is well defined. Indeed, say $y/t = z/r$. Then there is $v \in S$ such that $yrv = ztv$. So $xsyrv = xsztv$. Thus $xy/st = xz/sr$.

Define $x/s + y/t := (tx + sy)/(st)$. Then, similarly, this sum is well defined.

It is easy to check that $S^{-1}R$ *is a ring*, with $0/1$ for 0 and $1/1$ for 1. It is called the **ring of fractions with respect to** S or the **localization at** S.

Let $\varphi_S \colon R \to S^{-1}R$ be the map given by $\varphi_S(x) := x/1$. Then φ_S is a ring map, and *it carries elements of* S *to units in* $S^{-1}R$ *as* $s/1 \cdot 1/s = 1$.

(11.2) (Total quotient rings). — Let R be a ring. The set of nonzerodivisors S_0 is a saturated multiplicative subset, as noted in (**3.11**). The map $\varphi_{S_0} \colon R \to S_0^{-1}R$ is injective, because if $\varphi_{S_0} x = 0$, then $sx = 0$ for some $s \in S$, and so $x = 0$. We call $S_0^{-1}R$ the **total quotient ring** of R, and view R as a subring.

Let $S \subset S_0$ be a multiplicative subset. Clearly, $R \subset S^{-1}R \subset S_0^{-1}R$.

Suppose R is a domain. Then $S_0 = R - \{0\}$; so the total quotient ring is just the fraction field $\mathrm{Frac}(R)$, and φ_{S_0} is just the natural inclusion of R into $\mathrm{Frac}(R)$. Further, $S^{-1}R$ is a domain by (**2.3**) as $S^{-1}R \subset S_0^{-1}R = \mathrm{Frac}(R)$.

Theorem (11.3) (UMP)**. —** *Let R be a ring, S a multiplicative subset. Then $S^{-1}R$ is the R-algebra universal among algebras rendering all the $s \in S$ units. In fact, given a ring map $\psi \colon R \to R'$, then $\psi(S) \subset R'^{\times}$ if and only if there exists a ring map $\rho \colon S^{-1}R \to R'$ with $\rho\varphi_S = \psi$; that is, this diagram commutes:*

$$\begin{tikzcd} R \arrow[r, "\varphi_S"] \arrow[dr, "\psi"'] & S^{-1}R \arrow[d, "\rho"] \\ & R' \end{tikzcd}$$

If so, ρ is unique, and $\mathrm{Ker}(\rho) = \mathrm{Ker}(\psi)S^{-1}R$. *Finally, R' can be noncommutative.*

Proof: First, suppose that ρ exists. Let $s \in S$. Then $\psi(s) = \rho(s/1)$. Hence $\psi(s)\rho(1/s) = \rho(s/1 \cdot 1/s) = 1$. Thus $\psi(S) \subset R'^{\times}$.

Next, note that ρ is determined by ψ as follows:

$$\rho(x/s) = \rho(x/1)\rho(1/s) = \psi(x)\psi(s)^{-1}.$$

Conversely, suppose $\psi(S) \subset R'^{\times}$. Set $\rho(x/s) := \psi(s)^{-1}\psi(x)$. Let's check that ρ is well defined. Say $x/s = y/t$. Then there is $u \in S$ such that $xtu = ysu$. Hence

$$\psi(x)\psi(t)\psi(u) = \psi(y)\psi(s)\psi(u).$$

Since $\psi(u)$ is a unit, $\psi(x)\psi(t) = \psi(y)\psi(s)$. But $st = ts$; so

$$\psi(t)^{-1}\psi(s)^{-1} = \psi(s)^{-1}\psi(t)^{-1},$$

even if R' is noncommutative. Hence $\psi(x)\psi(s)^{-1} = \psi(y)\psi(t)^{-1}$. Thus ρ is well defined. Plainly, ρ is a ring map. Plainly, $\psi = \rho\varphi_S$.

Plainly, $\mathrm{Ker}(\rho) \supset \mathrm{Ker}(\psi)S^{-1}R$. Conversely, given $x/s \in \mathrm{Ker}(\rho)$, note that $\psi(x)\psi(s)^{-1} = 0$. So $\psi(x) = 0$. So $x \in \mathrm{Ker}(\psi)$. Thus $x/s \in \mathrm{Ker}(\psi)S^{-1}R$, □

Corollary (11.4). — *Let R be a ring, and S a multiplicative subset. Then the canonical map $\varphi_S\colon R \to S^{-1}R$ is an isomorphism if and only if S consists of units.*

Proof: If φ_S is an isomorphism, then S consists of units, because $\varphi_S(S)$ does so. Conversely, if S consists of units, then the identity map $R \to R$ has the UMP that characterizes φ_S; whence, φ_S is an isomorphism. □

Exercise (11.5) . — Let R' and R'' be rings. Consider $R := R' \times R''$ and set $S := \{(1,1), (1,0)\}$. Prove $R' = S^{-1}R$.

Definition (11.6). — Let R be a ring, $f \in R$. Set $S_f := \{f^n \mid n \ge 0\}$. We call the ring $S_f^{-1}R$ the **localization of R at f**, and set $R_f := S^{-1}R$ and $\varphi_f := \varphi_{S_f}$.

Proposition (11.7). — *Let R be a ring, $f \in R$, and X a variable. Then*

$$R_f = R[X]/\langle 1 - fX\rangle.$$

Proof: Set $R' := R[X]/\langle 1-fX\rangle$, and let $\varphi\colon R \to R'$ be the canonical map. Let's show that R' has the UMP characterizing localization (**11.3**).

First, let $x \in R'$ be the residue of X. Then $1 - x\varphi(f) = 0$. So $\varphi(f)$ is a unit. So $\varphi(f^n)$ is a unit for $n \ge 0$.

Second, let $\psi\colon R \to R''$ be a homomorphism carrying f to a unit. Define $\theta\colon R[X] \to R''$ by $\theta|R = \psi$ and $\theta X = \psi(f)^{-1}$. Then $\theta(1 - fX) = 0$. So θ factors via a homomorphism $\rho\colon R' \to R''$, and $\psi = \rho\varphi$. Further, ρ is unique, since every element of R' is a polynomial in x and since $\rho x = \psi(f)^{-1}$ as $1-(\rho x)(\rho\varphi f) = 0$. □

Proposition (11.8). — *Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal.*

(1) *Then* $\mathfrak{a}S^{-1}R = \{a/s \in S^{-1}R \mid a \in \mathfrak{a} \text{ and } s \in S\}$.

(2) *Then $\mathfrak{a} \cap S \neq \emptyset$ if and only if $\mathfrak{a}S^{-1}R = S^{-1}R$ if and only if $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = R$.*

Proof: Let $a, b \in \mathfrak{a}$ and $x/s, y/t \in S^{-1}R$. Then $ax/s + by/t = (axt + bys)/st$; further, $axt + bys \in \mathfrak{a}$ and $st \in S$. So $\mathfrak{a}S^{-1}R \subset \{a/s \mid a \in \mathfrak{a} \text{ and } s \in S\}$. But the opposite inclusion is trivial. Thus (1) holds.

As to (2), if $\mathfrak{a} \cap S \ni s$, then $\mathfrak{a}S^{-1}R \ni s/s = 1$, so $\mathfrak{a}S^{-1}R = S^{-1}R$; whence, $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = R$. Finally, suppose $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = R$. Then $\mathfrak{a}S^{-1}R \ni 1$. So (1) yields $a \in \mathfrak{a}$ and $s \in S$ such that $a/s = 1$. So there exists a $t \in S$ such that $at = st$. But $at \in \mathfrak{a}$ and $st \in S$. So $\mathfrak{a} \cap S \neq \emptyset$. Thus (2) holds. □

Definition (11.9). — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ a subset of R. The **saturation** of $\mathfrak{a}$ with respect to S is the set denoted by $\mathfrak{a}^S$ and defined by

$$\mathfrak{a}^S := \{a \in R \mid \text{there is } s \in S \text{ with } as \in \mathfrak{a}\}.$$

If $\mathfrak{a} = \mathfrak{a}^S$, then we say $\mathfrak{a}$ is **saturated**.

Proposition (11.10). — *Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal.*
(1) *Then* $\operatorname{Ker}(\varphi_S) = \langle 0\rangle^S$. (2) *Then* $\mathfrak{a} \subset \mathfrak{a}^S$. (3) *Then* $\mathfrak{a}^S$ *is an ideal.*

Proof: Clearly, (1) holds, for $a/1 = 0$ if and only if there is $s \in S$ with $as = 0$. Clearly, (2) holds as $1 \in S$. Clearly, (3) holds, for if $as,\ bt \in \mathfrak{a}$, then $(a+b)st \in \mathfrak{a}$, and if $x \in R$, then $xas \in \mathfrak{a}$. □

Proposition (11.11). — *Let R be a ring, S a multiplicative subset.*

(1) *Let $\mathfrak{b}$ be an ideal of $S^{-1}R$. Then*

(a) $\varphi_S^{-1}\mathfrak{b} = (\varphi_S^{-1}\mathfrak{b})^S$ *and* (b) $\mathfrak{b} = (\varphi_S^{-1}\mathfrak{b})(S^{-1}R)$.

(2) *Let $\mathfrak{a}$ be an ideal of R. Then*

(a) $\mathfrak{a}S^{-1}R = \mathfrak{a}^S S^{-1}R$ *and* (b) $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) = \mathfrak{a}^S$.

(3) *Let $\mathfrak{p}$ be a prime ideal of R, and assume $\mathfrak{p} \cap S = \emptyset$. Then*

(a) $\mathfrak{p} = \mathfrak{p}^S$ *and* (b) $\mathfrak{p}S^{-1}R$ *is prime.*

Proof: To prove (1)(a), take $a \in R$ and $s \in S$ with $as \in \varphi_S^{-1}\mathfrak{b}$. Then $as/1 \in \mathfrak{b}$; so $a/1 \in \mathfrak{b}$ because $1/s \in S^{-1}R$. Hence $a \in \varphi_S^{-1}\mathfrak{b}$. Therefore, $(\varphi_S^{-1}\mathfrak{b})^S \subset \varphi_S^{-1}\mathfrak{b}$. The opposite inclusion holds as $1 \in S$. Thus (1)(a) holds.

To prove (1)(b), take $a/s \in \mathfrak{b}$. Then $a/1 \in \mathfrak{b}$. So $a \in \varphi_S^{-1}\mathfrak{b}$. Hence $a/1 \cdot 1/s$ is in $(\varphi_S^{-1}\mathfrak{b})(S^{-1}R)$. Thus $\mathfrak{b} \subset (\varphi_S^{-1}\mathfrak{b})(S^{-1}R)$. Now, take $a \in \varphi_S^{-1}\mathfrak{b}$. Then $a/1 \in \mathfrak{b}$. So $\mathfrak{b} \supset (\varphi_S^{-1}\mathfrak{b})(S^{-1}R)$. Thus (1)(b) holds too.

To prove (2), take $a \in \mathfrak{a}^S$. Then there is $s \in S$ with $as \in \mathfrak{a}$. But $a/1 = as/1 \cdot 1/s$. So $a/1 \in \mathfrak{a}S^{-1}R$. Thus $\mathfrak{a}S^{-1}R \supset \mathfrak{a}^S S^{-1}R$ and $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) \supset \mathfrak{a}^S$.

Conversely, trivially $\mathfrak{a}S^{-1}R \subset \mathfrak{a}^S S^{-1}R$. Thus (2)(a) holds.

Take $x \in \varphi_S^{-1}(\mathfrak{a}S^{-1}R)$. Then $x/1 = a/s$ with $a \in \mathfrak{a}$ and $s \in S$ by **(11.8)**(1). So there's $t \in S$ with $xst = at \in \mathfrak{a}$. So $x \in \mathfrak{a}^S$. So $\varphi_S^{-1}(\mathfrak{a}S^{-1}R) \subset \mathfrak{a}^S$. Thus (2) holds.

To prove (3), note $\mathfrak{p} \subset \mathfrak{p}^S$ as $1 \in S$. Conversely, if $sa \in \mathfrak{p}$ with $s \in S \subset R - \mathfrak{p}$, then $a \in \mathfrak{p}$ as $\mathfrak{p}$ is prime. Thus (a) holds.

As for (b), first note $\mathfrak{p}S^{-1}R \neq S^{-1}R$ as $\varphi_S^{-1}(\mathfrak{p}S^{-1}R) = \mathfrak{p}^S = \mathfrak{p}$ by (2) and (3)(a) and as $1 \notin \mathfrak{p}$. Second, say $a/s \cdot b/t \in \mathfrak{p}S^{-1}R$. Then $ab \in \varphi_S^{-1}(\mathfrak{p}S^{-1}R)$, and the latter is equal to $\mathfrak{p}^S$ by (2), so to $\mathfrak{p}$ by (a). Hence $ab \in \mathfrak{p}$, so either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. So either $a/s \in \mathfrak{p}S^{-1}R$ or $b/t \in \mathfrak{p}S^{-1}R$. Thus $\mathfrak{p}S^{-1}R$ is prime. Thus (3) holds. □

Corollary (11.12). — *Let R be a ring, S a multiplicative subset.*

(1) *Then $\mathfrak{a} \mapsto \mathfrak{a}S^{-1}R$ is an inclusion-preserving bijection from the (set of all) ideals $\mathfrak{a}$ of R with $\mathfrak{a} = \mathfrak{a}^S$ to the ideals $\mathfrak{b}$ of $S^{-1}R$. The inverse is $\mathfrak{b} \mapsto \varphi_S^{-1}\mathfrak{b}$.*

(2) *Then $\mathfrak{p} \mapsto \mathfrak{p}S^{-1}R$ is an inclusion-preserving bijection from the primes $\mathfrak{p}$ of R with $\mathfrak{p} \cap S = \emptyset$ to the primes $\mathfrak{q}$ of $S^{-1}R$. The inverse is $\mathfrak{q} \mapsto \varphi_S^{-1}\mathfrak{q}$.*

Proof: In (1), the maps are inverses by **(11.11)**(1), (2); clearly, they preserve inclusions. Further, (1) implies (2) by **(11.11)**(3), by **(2.7)**, and by **(11.8)**(2). □

Definition (11.13). — Let R be a ring, $\mathfrak{p}$ a prime. Set $S_{\mathfrak{p}} := R - \mathfrak{p}$. We call the ring $S_{\mathfrak{p}}^{-1}R$ the **localization of R at $\mathfrak{p}$**, and set $R_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}R$ and $\varphi_{\mathfrak{p}} := \varphi_{S_{\mathfrak{p}}}$.

Proposition (11.14). — *Let R be a ring, $\mathfrak{p}$ a prime ideal. Then $R_{\mathfrak{p}}$ is local with maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$.*

Proof: Let $\mathfrak{b}$ be a proper ideal of $R_{\mathfrak{p}}$. Then $\varphi_{\mathfrak{p}}^{-1}\mathfrak{b} \subset \mathfrak{p}$ owing to (**11.8**)(2). Hence (**11.12**)(1) yields $\mathfrak{b} \subset \mathfrak{p}R_{\mathfrak{p}}$. Thus $\mathfrak{p}R_{\mathfrak{p}}$ is a maximal ideal, and the only one.

Alternatively, let $x/s \in R_{\mathfrak{p}}$. Suppose x/s is a unit. Then there is a y/t with $xy/st = 1$. So there is a $u \notin \mathfrak{p}$ with $xyu = stu$. But $stu \notin \mathfrak{p}$. Hence $x \notin \mathfrak{p}$.

Conversely, let $x \notin \mathfrak{p}$. Then $s/x \in R_{\mathfrak{p}}$. So x/s is a unit in $R_{\mathfrak{p}}$ if and only if $x \notin \mathfrak{p}$, so if and only if $x/s \notin \mathfrak{p}R_{\mathfrak{p}}$. Thus by (**11.8**)(1), the nonunits of $R_{\mathfrak{p}}$ form $\mathfrak{p}R_{\mathfrak{p}}$, which is an ideal. Hence (**3.5**) yields the assertion. □

(11.15) (Algebras). — Let R be a ring, S a multiplicative subset, R' an R-algebra. It is easy to generalize (**11.1**) as follows. Define a relation on $R' \times S$ by $(x, s) \sim (y, t)$ if there is $u \in S$ with $xtu = ysu$. It is easy to check, as in (**11.1**), that this relation is an equivalence relation.

Denote by $S^{-1}R'$ the set of equivalence classes, and by x/s the class of (x, s). Clearly, $S^{-1}R'$ is an $S^{-1}R$-algebra with addition and multiplication given by

$$x/s + y/t := (xt + ys)/(st) \quad \text{and} \quad x/s \cdot y/t := xy/st.$$

We call $S^{-1}R'$ the **localization of R' with respect to S**.

Let $\varphi'_S \colon R' \to S^{-1}R'$ be the map given by $\varphi'_S(x) := x/1$. Then φ'_S makes $S^{-1}R'$ into an R'-algebra, so also into an R-algebra, and φ'_S is an R-algebra map.

Note that elements of S become units in $S^{-1}R'$. Moreover, it is easy to check, as in (**11.3**), that $S^{-1}R'$ has the following UMP: *φ'_S is an algebra map, and elements of S become units in $S^{-1}R'$; further, given an algebra map $\psi \colon R' \to R''$ such that elements of S become units in R'', there is a unique R-algebra map $\rho \colon S^{-1}R' \to R''$ such that $\rho\varphi'_S = \psi$; that is, the following diagram is commutative:*

$$\begin{tikzcd} R' \arrow[r, "\varphi'_S"] \arrow[dr, "\psi"'] & S^{-1}R' \arrow[d, "\rho"] \\ & R'' \end{tikzcd}$$

In other words, $S^{-1}R'$ is *universal* among R'-algebras rendering the $s \in S$ units.

Let $\tau \colon R' \to R''$ be an R-algebra map. Then there is a commutative diagram of R-algebra maps

$$\begin{tikzcd} R' \arrow[r, "\tau"] \arrow[d, "\varphi'_S"'] & R'' \arrow[d, "\varphi''_S"] \\ S^{-1}R' \arrow[r, "S^{-1}\tau"] & S^{-1}R'' \end{tikzcd}$$

Further, $S^{-1}\tau$ is an $S^{-1}R$-algebra map.

Let $S' \subset R'$ be the image of $S \subset R$. Then S' is multiplicative. Further,

$$S^{-1}R' = S'^{-1}R', \tag{11.15.1}$$

even though $R' \times S$ and $R' \times S'$ are rarely equal, because the two UMPs are essentially the same; indeed, any ring map $R' \to R''$ may be viewed as an R-algebra map, and trivially the elements of S become units in R'' if and only if the elements of S' do.

Proposition (11.16). — *Let R be a ring, S a multiplicative subset. Let T' be a multiplicative subset of $S^{-1}R$, and set $T := \varphi_S^{-1}(T')$. Assume $S \subset T$. Then*

$$(T')^{-1}(S^{-1}R) = T^{-1}R.$$

Proof: Let's check $(T')^{-1}(S^{-1}R)$ has the UMP characterizing $T^{-1}R$. Clearly $\varphi_{T'}\varphi_S$ carries T into $\big((T')^{-1}(S^{-1}R)\big)^{\times}$. Next, let $\psi\colon R \to R'$ be a map carrying T into $R'^{\times}$. We must show ψ factors uniquely through $(T')^{-1}(S^{-1}R)$.

First, ψ carries S into $R'^{\times}$ since $S \subset T$. So ψ factors through a unique map $\rho\colon S^{-1}R \to R'$. Now, given $r \in T'$, write $r = x/s$. Then $x/1 = s/1 \cdot r \in T'$ since $S \subset T$. So $x \in T$. Hence $\rho(r) = \psi(x)\cdot\rho(1/s) \in (R')^{\times}$. So ρ factors through a unique map $\rho'\colon (T')^{-1}(S^{-1}R) \to R'$. Hence $\psi = \rho'\varphi_{T'}\varphi_S$, and ρ' is clearly unique, as required. □

Definition (11.17). — We call a ring **decomposable** if it's a finite product of local rings.

Proposition (11.18). — *Let R be a ring, $\{\mathfrak{m}_\lambda\}$ its set of maximal ideals. Assume R is decomposable; say $R = \prod_{i=1}^n R_i$ with all R_i local. Then R is semilocal with n maximal ideals, and after reindexing, $R_i = R_{\mathfrak{m}_i}$ for all i.*

Proof: Set $e_i := (\delta_{ij}) \in \prod R_j$ where δ_{ij} is the Kronecker delta. Then $R_i = Re_i$. Let $\mathfrak{n}_i$ be the maximal ideal of R_i. Set $\mathfrak{m}'_i := \mathfrak{n}_i \times \prod_{j\neq i} R_j$. Then $\mathfrak{m}'_i$ is maximal, and every maximal ideal of R has this form owing to **(1.23)**. Thus R is semilocal with n maximal ideals.

Reindex the $\mathfrak{m}_\lambda$ so that $\mathfrak{m}_i = \mathfrak{m}'_i$. Set $S_i := \{1, e_i\}$. Then $S_i^{-1}R = R_i$ by **(11.5)**. Also, the localization map $\varphi_{S_i}\colon R \to R_i$ is the projection. So $\varphi_{S_i}^{-1}(R_i - \mathfrak{n}_i) = R - \mathfrak{m}_i$. So $R_{\mathfrak{m}_i} = (R_i)_{\mathfrak{n}_i}$ by **(11.16)**. But $(R_i)_{\mathfrak{n}_i} = R_i$ by **(11.4)**. □

B. Exercises

Exercise (11.19) . — Let R be a ring, S a multiplicative subset. Prove $S^{-1}R = 0$ if and only if S contains a nilpotent element.

Exercise (11.20) . — Find all intermediate rings $\mathbb{Z} \subset R \subset \mathbb{Q}$, and describe each R as a localization of $\mathbb{Z}$. As a starter, prove $\mathbb{Z}[2/3] = S_3^{-1}\mathbb{Z}$ where $S_3 := \{3^i \mid i \geq 0\}$.

Exercise (11.21) . — Take R and S as in **(11.5)**. On $R \times S$, impose this relation:

$$(x, s) \sim (y, t) \quad \text{if} \quad xt = ys.$$

Show that it is not an equivalence relation.

Exercise (11.22) . — Let R be a ring, S a multiplicative subset, G be a group acting on R, Assume $g(S) \subset S$ for all $g \in G$. Set $S^G := S \cap R^G$. Show:

(1) The group G acts canonically on $S^{-1}R$.

(2) If G is finite, there's a canonical isomorphism $\rho\colon (S^G)^{-1}R^G \xrightarrow{\sim} (S^{-1}R)^G$.

Exercise (11.23) . — Let R be a ring, $S \subset T$ a multiplicative subsets, $\overline{S}$ and $\overline{T}$ their saturations; see **(3.25)**. Set $U := (S^{-1}R)^{\times}$. Show the following:

(1) $U = \{\, x/s \mid x \in \overline{S} \text{ and } s \in S \,\}$. (2) $\varphi_S^{-1}U = \overline{S}$.
(3) $S^{-1}R = T^{-1}R$ if and only if $\overline{S} = \overline{T}$. (4) $\overline{S}^{-1}R = S^{-1}R$.

Exercise (11.24) . — Let R be a ring, $S \subset T \subset U$ and W multiplicative subsets.

(1) Show there's a unique R-algebra map $\varphi^S_T\colon S^{-1}R \to T^{-1}R$ and $\varphi^T_U\varphi^S_T = \varphi^S_U$.

(2) Given a map $\varphi\colon S^{-1}R \to W^{-1}R$, show $S \subset \overline{S} \subset \overline{W}$ and $\varphi = \varphi^S_{\overline{W}}$.

Exercise (11.25) . — Let $R = \varinjlim R_\lambda$ be a filtered direct limit of rings with transitions maps $\varphi^\lambda_\mu\colon R_\lambda \to R_\mu$ and insertions $\varphi_\mu\colon R_\mu \to R$. For all λ, let $S_\lambda \subset R_\lambda$ be a multiplicative subset. For all φ^λ_μ, assume $\varphi^\lambda_\mu(S_\lambda) \subset S_\mu$. Set $S := \bigcup \varphi_\lambda S_\lambda$. Then $\varinjlim S_\lambda^{-1}R_\lambda = S^{-1}R$.

Exercise (11.26) . — Let R be a ring, S_0 the set of nonzerodivisors. Show:

(1) Then S_0 is the largest multiplicative subset S with $\varphi_S\colon R \to S^{-1}R$ injective.

(2) Every element x/s of $S_0^{-1}R$ is either a zerodivisor or a unit.

(3) Suppose every element of R is either a zerodivisor or a unit. Then $R = S_0^{-1}R$.

Exercise (11.27) . — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Show: (1) if $\mathfrak{a} \subset \mathfrak{b}$, then $\mathfrak{a}^S \subset \mathfrak{b}^S$; (2) $(\mathfrak{a}^S)^S = \mathfrak{a}^S$; and (3) $(\mathfrak{a}^S\mathfrak{b}^S)^S = (\mathfrak{a}\mathfrak{b})^S$.

Exercise (11.28) . — Let R be a ring, S a multiplicative subset. Prove that

$$\operatorname{nil}(R)(S^{-1}R) = \operatorname{nil}(S^{-1}R).$$

Exercise (11.29) . — Let R be a ring, S a multiplicative subset, R' an algebra. Assume R' is integral over R. Show $S^{-1}R'$ is integral over $S^{-1}R$.

Exercise (11.30) . — Let R be a domain, K its fraction field, L a finite extension field, and $\overline{R}$ the integral closure of R in L. Show $L = \operatorname{Frac}(\overline{R})$. Show every element of L can, in fact, be expressed as a fraction b/a with $b \in \overline{R}$ and $a \in R$.

Exercise (11.31) . — Let $R \subset R'$ be domains, K and L their fraction fields. Assume that R' is a finitely generated R-algebra, and that L is a finite dimensional K-vector space. Find an $f \in R$ such that R'_f is module finite over R_f.

Exercise (11.32) (*Localization and normalization commute*) . — Given a domain R and a multiplicative subset S with $0 \notin S$. Show that the localization of the normalization $S^{-1}\overline{R}$ is equal to the normalization of the localization $\overline{S^{-1}R}$.

Exercise (11.33) . — Let k be a field, A a local k-algebra with maximal ideal $\mathfrak{m}$. Assume that A is a localization of a k-algebra R and that $A/\mathfrak{m} = k$. Find a maximal ideal $\mathfrak{n}$ of R with $R_\mathfrak{n} = A$.

Exercise (11.34) . — Let R be a ring, S a multiplicative subset, $\mathcal{X} := \{X_\lambda\}$ a set of variables. Show $(S^{-1}R)[\mathcal{X}] = S^{-1}\big(R[\mathcal{X}]\big)$.

Exercise (11.35) . — Let R be a ring, S a multiplicative subset, $\mathcal{X}$ a set of variables, $\mathfrak{p}$ an ideal of $R[\mathcal{X}]$. Set $R' := S^{-1}R$, and let $\varphi\colon R[\mathcal{X}] \to R'[\mathcal{X}]$ be the canonical map. Show $\mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \emptyset$ if and only if $\mathfrak{p}R'[\mathcal{X}]$ is prime and $\mathfrak{p} = \varphi^{-1}\big(\mathfrak{p}R'[\mathcal{X}]\big)$.

12. Localization of Modules

Formally, we localize a module just as we do a ring. The result is a module over the localized ring, and comes equipped with a linear map from the original module; in fact, the result is universal among modules with those two properties. Consequently, Localization is a functor; in fact, it is the left adjoint of Restriction of Scalars from the localized ring to the base ring. So Localization preserves direct limits, or equivalently, direct sums and cokernels. Further, by uniqueness of left adjoints or by Watts's Theorem, Localization is naturally isomorphic to Tensor Product with the localized ring. Moreover, Localization is exact; so the localized ring is flat. We end the chapter by discussing various compatibilities and examples.

A. Text

Proposition (12.1). — *Let R be a ring, S a multiplicative subset. Then a module M has a compatible $S^{-1}R$-module structure if and only if, for all $s \in S$, the multiplication map $\mu_s \colon M \to M$ is bijective; if so, then the $S^{-1}R$-structure is unique.*

Proof: Assume M has a compatible $S^{-1}R$-structure, and take $s \in S$. Then $\mu_s = \mu_{s/1}$. So $\mu_s \cdot \mu_{1/s} = \mu_{(s/1)(1/s)} = 1$. Similarly, $\mu_{1/s} \cdot \mu_s = 1$. So μ_s is bijective.

Conversely, assume μ_s is bijective for all $s \in S$. Then $\mu_R \colon R \to \mathrm{End}_{\mathbb{Z}}(M)$ sends S into the units of $\mathrm{End}_{\mathbb{Z}}(M)$. Hence μ_R factors through a unique ring map $\mu_{S^{-1}R} \colon S^{-1}R \to \mathrm{End}_{\mathbb{Z}}(M)$ by **(11.3)**. Thus M has a compatible $S^{-1}R$-structure by **(4.4)**, which is unique by **(4.5)**. □

(12.2) (Localization of modules). — Let R be a ring, S a multiplicative subset, M a module. Define a relation on $M \times S$ by $(m, s) \sim (n, t)$ if there is $u \in S$ such that $utm = usn$. As in **(11.1)**, this relation is an equivalence relation.

Denote by $S^{-1}M$ the set of equivalence classes, and by m/s the class of (m, s). Then $S^{-1}M$ is an $S^{-1}R$-module with addition given by $m/s + n/t := (tm + sn)/st$ and scalar multiplication by $a/s \cdot m/t := am/st$ similar to **(11.1)**. We call $S^{-1}M$ the **localization of** M at S.

For example, let $\mathfrak{a}$ be an ideal. Then $S^{-1}\mathfrak{a} = \mathfrak{a}S^{-1}R$ by **(11.8)**(1). Similarly, $S^{-1}(\mathfrak{a}M) = S^{-1}\mathfrak{a}S^{-1}M = \mathfrak{a}S^{-1}M$. Further, given an R-algebra R', the $S^{-1}R$-module $S^{-1}R'$ constructed here underlies the $S^{-1}R$-algebra $S^{-1}R'$ of **(11.15)**.

Define $\varphi_S \colon M \to S^{-1}M$ by $\varphi_S(m) := m/1$. Clearly, φ_S is R-linear.

Note that $\mu_s \colon S^{-1}M \to S^{-1}M$ is bijective for all $s \in S$ by **(12.1)**.

Given $f \in R$, we call $S_f^{-1}M$ the **localization of** M **at** f, and set $M_f := S_f^{-1}M$ and $\varphi_f := \varphi_S$. Similarly, given a prime $\mathfrak{p}$, we call $S_{\mathfrak{p}}^{-1}M$ the **localization of** M **at** $\mathfrak{p}$, and set $M_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}M$ and $\varphi_{\mathfrak{p}} := \varphi_S$.

Theorem (12.3) (UMP). — *Let R be a ring, S a multiplicative subset, and M a module. Then $S^{-1}M$ equipped with $\varphi_s \colon M \to S^{-1}M$ is universal among $S^{-1}R$-modules equipped with an R-map from M; that is, given an R-map $\psi \colon M \to N$ with N an $S^{-1}R$-module, there's a unique $S^{-1}R$-map $\sigma \colon S^{-1}M \to N$ with $\sigma\varphi_S = \psi$. Moreover, given an R-map $\sigma' \colon S^{-1}M \to N$ with $\sigma'\varphi_S = \psi$, necessarily, $\sigma' = \sigma$.*

Proof: Given $m \in M$ and $s \in S$, note $s\sigma'(m/s) = \sigma'(sm/s) = \sigma'(\varphi_s(m)) = \psi(s)$. Multiply by $1/s$. Thus $\sigma'(m/s) = \psi(s)/s$, and so σ' is determined by ψ.

So set $\sigma(m/s) := \psi(m)/s$. Let's check σ is well defined. Say $m/s = n/t$ with $n \in M$ and $t \in S$. Then there's $u \in S$ with $utm = usn$. So $ut\psi(m) = us\psi(n)$. So $\psi(m)/s = \psi(n)/t$. Thus σ is well defined. Plainly, $\sigma\varphi_S = \psi$.

Finally, σ is plainly R-linear. Thus, by **(12.4)**(1) below, σ is $S^{-1}R$-linear. □

Exercise (12.4) . — Let R be a ring, S a multiplicative subset, and M, N modules. Show: (1) If M, N are $S^{-1}R$-modules, then $\operatorname{Hom}_{S^{-1}R}(M,N) = \operatorname{Hom}_R(M,N)$.

(2) M is an $S^{-1}R$-module if and only if $M = S^{-1}M$.

Exercise (12.5) . — Let R be a ring, $S \subset T$ multiplicative subsets, M a module. Set $T' := \varphi_S(T) \subset S^{-1}R$. Show $T^{-1}M = T'^{-1}(S^{-1}M)$.

Exercise (12.6) . — Let R be a ring, S a multiplicative subset. Show that S becomes a filtered category when equipped as follows: given $s, t \in S$, set

$$\operatorname{Hom}(s,t) := \{x \in R \mid xs = t\}.$$

Given a module M, define a functor $S \to ((R\text{-mod}))$ as follows: for $s \in S$, set $M_s := M$; to each $x \in \operatorname{Hom}(s,t)$, associate $\mu_x\colon M_s \to M_t$. Define $\beta_s\colon M_s \to S^{-1}M$ by $\beta_s(m) := m/s$. Show the β_s induce an isomorphism $\varinjlim M_s \xrightarrow{\sim} S^{-1}M$.

(12.7) (Functoriality). — Let R be a ring, S a multiplicative subset, $\alpha\colon M \to N$ an R-linear map. Then $\varphi_S\alpha$ carries M to the $S^{-1}R$-module $S^{-1}N$. So **(12.3)** yields a unique $S^{-1}R$-linear map $S^{-1}\alpha$ making the following diagram commutative:

$$\begin{array}{ccc} M & \xrightarrow{\varphi_S} & S^{-1}M \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle S^{-1}\alpha} \\ N & \xrightarrow{\varphi_S} & S^{-1}N \end{array}$$

The construction in the proof of **(12.3)** yields

$$(S^{-1}\alpha)(m/s) = \alpha(m)/s. \tag{12.7.1}$$

Thus, canonically, we obtain the following map, and clearly, it is R-linear:

$$\operatorname{Hom}_R(M,\, N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M,\, S^{-1}N). \tag{12.7.2}$$

Any R-linear map $\beta\colon N \to P$ yields $S^{-1}(\beta\alpha) = (S^{-1}\beta)(S^{-1}\alpha)$ owing to uniqueness or to **(12.7.1)**. Thus $S^{-1}(\bullet)$ *is a linear functor* from $((R\text{-mod}))$ to $((S^{-1}R\text{-mod}))$.

Theorem (12.8). — *Let R be a ring, S a multiplicative subset. Then the functor $S^{-1}(\bullet)$ is the left adjoint of the functor of restriction of scalars.*

Proof: Let M be an R-module, N an $S^{-1}R$-module. Then $\varphi_S\colon M \to N$ induces an isomorphism $\operatorname{Hom}_{S^{-1}R}(S^{-1}M, N) \xrightarrow{\sim} \operatorname{Hom}_R(M,N)$ by the UMP of Localization **(12.3)**. It's natural in M and N by **(12.7)** and the naturality of Hom. □

Corollary (12.9). — *Let R be a ring, S a multiplicative subset. Then the functor $S^{-1}(\bullet)$ preserves direct limits, or equivalently, direct sums and cokernels.*

Proof: By **(12.8)**, the functor is a left adjoint. Hence it preserves direct limits by **(6.9)**; equivalently, it preserves direct sums and cokernels by **(6.7)**. □

Corollary (12.10). — *Let R be a ring, S a multiplicative subset. Then the functors $S^{-1}(\bullet)$ and $S^{-1}R \otimes_R \bullet$ are canonically isomorphic.*

Proof: As $S^{-1}(\bullet)$ preserves direct sums and cokernels by **(12.9)**, the assertion is an immediate consequence of Watts' Theorem **(8.13)**.

Alternatively, both functors are left adjoints of the same functor by **(12.8)** and by **(8.9)**(2). So they are canonically isomorphic by **(6.3)**. □

(12.11) (Saturation). — Let R be a ring, S a multiplicative subset, M a module. Given a submodule N, its **saturation** N^S is defined by

$$N^S := \{m \in M \mid \text{there is } s \in S \text{ with } sm \in N\}.$$

Note $N \subset N^S$ as $1 \in S$. If $N = N^S$, then we say N is **saturated**.

Proposition (12.12). — *Let R be a ring, M a module, N and P submodules. Let S, and T be multiplicative subsets, and K an $S^{-1}R$-submodule of $S^{-1}M$.*

(1) *Then* (a) *N^S is a submodule of M, and* (b) *$S^{-1}N$ is a submodule of $S^{-1}M$.*
(2) *Then* (a) *$\varphi_S^{-1}K = (\varphi_S^{-1}K)^S$ and* (b) *$K = S^{-1}(\varphi_S^{-1}K)$.*
(3) *Then* (a) *$\varphi_S^{-1}(S^{-1}N) = N^S$; so $\operatorname{Ker}(\varphi_S) = 0^S$. And* (b) *$S^{-1}N = S^{-1}N^S$.*
(4) *Then* (a) *$(N^S)^T = N^{ST}$ and* (b) *$S^{-1}(S^{-1}N) = S^{-1}N$.*
(5) *Assume $N \subset P$. Then* (a) *$N^S \subset P^S$ and* (b) *$S^{-1}N \subset S^{-1}P$.*
(6) *Then* (a) *$(N \cap P)^S = N^S \cap P^S$ and* (b) *$S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.*
(7) *Then* (a) *$(N + P)^S \supset N^S + P^S$ and* (b) *$S^{-1}(N + P) = S^{-1}N + S^{-1}P$.*
(8) *Assume $S \subset T$. Then $N^S \subset N^T$.*

Proof: For (1)(a), (2), (3), argue much as for **(11.10)**(3) and **(11.11)**(1), (2).

For (1)(b), note $N \times S$ lies in $M \times S$ and has the induced equivalence relation.

For (4)(a), note $n \in (N^S)^T$ if and only if there exist $t \in T$ and $s \in S$ with $s(tn) = (st)n \in N$, so if and only if $n \in N^{ST}$.

For (4)(b), take $M := S^{-1}N$ in **(12.4)**(2).

For (5)(a), given $n \in N^S$, there's $s \in S$ with $sn \in N$. So $sn \in P$. Thus $n \in P^S$.

For (5)(b), take $M := P$ in (1)(b).

For (6)(a), note $(N \cap P)^S \subset N^S \cap P^S$. Conversely, given $n \in N^S \cap P^S$, there are $s, t \in S$ with $sn \in N$ and $tn \in P$. So $stn \in N \cap P$ and $st \in S$. Thus $n \in (N \cap P)^S$. Alternatively, (6)(a) follows from (6)(b) and (3).

For (6)(b), note $N \cap P \subset N, P$. So (1) yields $S^{-1}(N \cap P) \subset S^{-1}N \cap S^{-1}P$. Conversely, given $n/s = p/t \in S^{-1}N \cap S^{-1}P$, there's $u \in S$ with $utn = usp \in N \cap P$. Thus $utn/uts = usp/uts \in S^{-1}(N \cap P)$. Thus (6)(b) holds.

For (7)(a), given $n \in N^S$ and $p \in P^S$, there are $s, t \in S$ with $sn \in N$ and $tp \in P$. Then $st \in S$ and $st(n + p) \in N + P$. Thus (7)(a) holds.

For (7)(b), note $N, P \subset N + P$. So (1)(b) yields $S^{-1}(N + P) \supset S^{-1}N + S^{-1}P$. But the opposite inclusion holds as $(n + p)/s = n/s + p/s$. Thus (7)(b) holds.

For (8), given $n \in N^S$, there's $s \in S$ with $sn \in N$. But $s \in T$. Thus $n \in N^T$. □

Theorem (12.13) (Exactness of Localization). — *Let R be a ring, and S a multiplicative subset. Then the functor $S^{-1}(\bullet)$ is exact.*

Proof: Note that $S^{-1}(\bullet)$ preserves injections by **(12.12)**(1)(b) and cokernels by **(12.9)**. Thus it is exact by **(9.3)**.

Alternatively, given an exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$, for each $s \in S$, take a copy $M'_s \to M_s \to M''_s$. Using **(12.6)**, make S into a filtered category, and make these copies into a functor from S to the category of 3-term exact sequences; its limit is the following sequence, which is exact by **(7.9)**, as desired:

$$S^{-1}M' \xrightarrow{S^{-1}\alpha} S^{-1}M \xrightarrow{S^{-1}\beta} S^{-1}M''.$$

The alternative argument can be made more direct as follows. Since $\beta\alpha = 0$, we have $(S^{-1}\beta)(S^{-1}\alpha) = S^{-1}(\beta\alpha) = 0$. Hence $\operatorname{Ker}(S^{-1}\beta) \supset \operatorname{Im}(S^{-1}\alpha)$. Conversely, given $m/s \in \operatorname{Ker}(S^{-1}\beta)$, there is $t \in S$ with $t\beta(m) = 0$. So $\beta(tm) = 0$. So exactness yields $m' \in M'$ with $\alpha(m') = tm$. So $(S^{-1}\alpha)(m'/ts) = m/s$. Hence $\operatorname{Ker}(S^{-1}\beta) \subset \operatorname{Im}(S^{-1}\alpha)$. Thus $\operatorname{Ker}(S^{-1}\beta) = \operatorname{Im}(S^{-1}\alpha)$, as desired. □

Corollary (12.14). — *Let R be a ring, S a subset multiplicative. Then $S^{-1}R$ is flat over R.*

Proof: The functor $S^{-1}(\bullet)$ is exact by **(12.13)**, and is isomorphic to $S^{-1}R \otimes_R \bullet$ by **(12.10)**. Thus $S^{-1}R$ is flat.

Alternatively, using **(12.6)**, write $S^{-1}R$ as a filtered direct limit of copies of R. But R is flat by **(9.6)**. Thus $S^{-1}R$ is flat by **(9.9)**. □

Corollary (12.15). — *Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal, and M a module. Then $S^{-1}(M/\mathfrak{a}M) = S^{-1}M/S^{-1}(\mathfrak{a}M) = S^{-1}M/\mathfrak{a}S^{-1}M$.*

Proof: The assertion results from **(12.13)** and **(12.2)**. □

Corollary (12.16). — *Let R be a ring, $\mathfrak{p}$ a prime. Then*

$$\operatorname{Frac}(R/\mathfrak{p}) = (R/\mathfrak{p})_{\mathfrak{p}} = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

Proof: The assertion results from **(11.15)** and **(12.15)**. □

Exercise (12.17) . — Let R be a ring, S a multiplicative subset, M a module. Show: (1) $S^{-1}\operatorname{Ann}(M) \subset \operatorname{Ann}(S^{-1}M)$, with equality if M is finitely generated;

(2) $S^{-1}M = 0$ if $\operatorname{Ann}(M) \cap S \neq \emptyset$, and conversely if M is finitely generated.

Proposition (12.18). — *Let R be a ring, M a module, S a multiplicative subset.*

(1) *Let $m_1, \dots, m_n \in M$. If M is finitely generated and if the $m_i/1 \in S^{-1}M$ generate over $S^{-1}R$, then there's $f \in S$ so that the $m_i/1 \in M_f$ generate over R_f.*

(2) *Assume M is finitely presented and $S^{-1}M$ is a free $S^{-1}R$-module of rank n. Then there is $h \in S$ such that M_h is a free R_h-module of rank n.*

Proof: To prove (1), define $\alpha\colon R^n \to M$ by $\alpha(e_i) := m_i$ with e_i the ith standard basis vector. Set $C := \operatorname{Coker}(\alpha)$. Then $S^{-1}C = \operatorname{Coker}(S^{-1}\alpha)$ by **(12.9)**. Assume the $m_i/1 \in S^{-1}M$ generate over $S^{-1}R$. Then $S^{-1}\alpha$ is surjective by **(4.10)**(1) as $S^{-1}(R^n) = (S^{-1}R)^n$ by **(12.9)**. Hence $S^{-1}C = 0$.

In addition, assume M is finitely generated. Then so is C. Hence, **(12.17)**(2) yields $f \in S$ such that $C_f = 0$. Hence α_f is surjective. So the $m_i/1$ generate M_f over R_f again by **(4.10)**(1). Thus (1) holds.

For (2), let $m_1/s_1, \dots, m_n/s_n$ be a free basis of $S^{-1}M$ over $S^{-1}R$. Then so is $m_1/1, \dots, m_n/1$ as the $1/s_i$ are units. Form α and C as above, and set $K := \operatorname{Ker}(\alpha)$. Then **(12.13)** yields $S^{-1}K = \operatorname{Ker}(S^{-1}\alpha)$ and $S^{-1}C = \operatorname{Coker}(S^{-1}\alpha)$. But $S^{-1}\alpha$ is bijective. Hence $S^{-1}K = 0$ and $S^{-1}C = 0$.

Since M is finitely generated, C is too. Hence, as above, there is $f \in S$ such that $C_f = 0$. Then $0 \to K_f \to R_f^n \xrightarrow{\alpha_f} M_f \to 0$ is exact by **(12.13)**. Take a finite presentation $R^p \to R^q \to M \to 0$. By **(12.13)**, it yields a finite presentation $R_f^p \to R_f^q \to M_f \to 0$. Hence K_f is a finitely generated R_f-module by **(5.18)**.

Let $S_1 \subset R_f$ be the image of S. Then **(12.5)** yields $S_1^{-1}(K_f) = S^{-1}K$. But $S^{-1}K = 0$. Hence there is $g/1 \in S_1$ such that $(K_f)_{g/1} = 0$. Set $h := fg$. Let's show $K_h = 0$. Let $x \in K$. Then there is a such that $(g^a x)/1 = 0$ in K_f. Hence there is b such that $f^b g^a x = 0$ in K. Take $c \ge a, b$. Then $h^c x = 0$. Thus $K_h = 0$. But $C_f = 0$ implies $C_h = 0$. Hence $\alpha_h\colon R_h^n \to M_h$ is an isomorphism, as desired. □

Proposition (12.19). — *Let R be a ring, S a multiplicative subset, M and N modules. Then there is a canonical homomorphism*

$$\sigma\colon S^{-1}\operatorname{Hom}_R(M,N) \to \operatorname{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N).$$

Further, σ is injective if M is finitely generated, and σ is an isomorphism if M is finitely presented.

Proof: The assertions result from (**9.33**) with $R' := S^{-1}R$, since $S^{-1}R$ is flat by (**12.14**) and since $S^{-1}R \otimes P = S^{-1}P$ for every R-module P by (**12.10**). □

Example (12.20). — Set $R := \mathbb{Z}$ and $M := \mathbb{Q}/\mathbb{Z}$, and recall $S_0 := \mathbb{Z} - \langle 0\rangle$. Then M is faithful, as $z \in S_0$ implies $z \cdot (1/2z) = 1/2 \ne 0$; thus, $\mu_R\colon R \to \operatorname{Hom}_R(M,M)$ is injective. But $S_0^{-1}R = \mathbb{Q}$. So (**12.13**) yields $S_0^{-1}\operatorname{Hom}_R(M,M) \ne 0$. On the other hand, $S_0^{-1}M = 0$ as $s \cdot r/s = 0$ for any $r/s \in M$. So the map $\sigma(M,M)$ of (**12.19**) is not injective. Thus (**12.19**)) can fail if M is not finitely generated.

Example (12.21). — Set $R := \mathbb{Z}$, recall $S_0 := \mathbb{Z} - \langle 0\rangle$, and set $M_n := \mathbb{Z}/\langle n\rangle$ for $n \ge 2$. Then $S_0^{-1}M_n = 0$ for all n as $nm \equiv 0 \pmod n$ for all m. On the other hand, $(1,1,\dots)/1$ is nonzero in $S_0^{-1}\big(\prod M_n\big)$ as the kth component of $m\cdot(1,1,\dots)$ is nonzero in $\prod M_n$ for $k > |m|$ if m is nonzero. Thus $S_0^{-1}\big(\prod M_n\big) \ne \prod(S_0^{-1}M_n)$.

Also $S_0^{-1}\mathbb{Z} = \mathbb{Q}$. So (**12.10**) yields $\mathbb{Q}\otimes\big(\prod M_n\big) \ne \prod(\mathbb{Q}\otimes M_n)$, whereas (**8.10**) yields $\mathbb{Q}\otimes\big(\bigoplus M_n\big) = \bigoplus(\mathbb{Q}\otimes M_n)$.

(12.22) (Nilpotents). — Let R be a ring, $x \in R$. We say x is **nilpotent** on a module M if there is $n \ge 1$ with $x^n m = 0$ for all $m \in M$; that is, $x \in \sqrt{\operatorname{Ann}(M)}$. We denote the set of nilpotents on M by $\operatorname{nil}(M)$; that is, $\operatorname{nil}(M) := \sqrt{\operatorname{Ann}(M)}$.

Notice that, if $M = R$, then we recover the notions of nilpotent element and of $\operatorname{nil}(R)$ of (**3.13**). Moreover, given an ideal $\mathfrak{a} \subset R$, we have $\operatorname{nil}(R/\mathfrak{a}) = \sqrt{\mathfrak{a}}$.

Proposition (12.23). — *Let S be a multiplicatively closed subset, and $Q \subset M$ modules. Set $\mathfrak{p} := \operatorname{nil}(M/Q)$; assume $S \cap \mathfrak{p} \ne \emptyset$. Then $Q^S = M$ and $S^{-1}Q = S^{-1}M$.*

Proof: Say $s \in S \cap \mathfrak{p}$. Then there's $n \ge 0$ with $s^n M \subset Q$. But $s^n \in S$. Thus $Q^S = M$. Now, $S^{-1}Q = S^{-1}Q^S$ by (**12.12**)(3)(b). Thus $S^{-1}Q = S^{-1}M$. □

B. Exercises

Exercise (12.24) . — Let R be a ring, M a module, and S, T multiplicative subsets.

(1) Set $U := ST := \{st \in R \mid s \in S \text{ and } t \in T\}$. Show $U^{-1}M = T^{-1}(S^{-1}M)$.

(2) Assume $S \subset T$. Show $T^{-1}M = T^{-1}(S^{-1}M)$.

Exercise (12.25) . — Let R be a ring, S a multiplicative subset, M a module. Show: (1) Let T_1 be a multiplicative subset of $S^{-1}R$; set $T := \varphi_S^{-1}(T_1)$; and assume $S \subset T$. Then $T^{-1}M = T_1^{-1}(S^{-1}M)$.

(2) Let $\mathfrak{p}$ be a prime of R; assume $\mathfrak{p} \cap S = \emptyset$; and set $\mathfrak{P} := \mathfrak{p}S^{-1}R$. Then $M_{\mathfrak{p}} = (S^{-1}M)_{\mathfrak{p}} = (S^{-1}M)_{\mathfrak{P}}$.

(3) Let $\mathfrak{p} \subset \mathfrak{q}$ be primes of R. Set $\mathfrak{P} := \mathfrak{p}R_{\mathfrak{q}}$. Then $M_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{P}}$.

Exercise (12.26) . — Let R be a ring, S a multiplicative subset, $\varphi\colon R \to R'$ a map of rings, M' an R'-module. Set $S' := \varphi(S)$. Show $S'^{-1}M' = S^{-1}M'$.

Exercise (12.27) . — Let R be a ring, M a finitely generated module, $\mathfrak{a}$ an ideal.

(1) Set $S := 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ lies in the radical of $S^{-1}R$.

(2) Use (1), Nakayama's Lemma **(10.6)** and **(12.17)**(2), but not the determinant trick **(10.2)**, to prove this part of **(10.3)**: if $M = \mathfrak{a}M$, then $sM = 0$ for an $s \in S$.

Exercise (12.28) . — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal, M a module, N a submodule. Prove $(\mathfrak{a}N)^S = (\mathfrak{a}^S N^S)^S$.

Exercise (12.29) . — Let R be a ring, S a multiplicative subset, P a projective module. Then $S^{-1}P$ is a projective $S^{-1}R$-module.

Exercise (12.30) . — Let R be a ring, S a multiplicative subset, M, N modules. Show $S^{-1}(M \otimes_R N) = S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} S^{-1}N = S^{-1}M \otimes_R S^{-1}N$.

Exercise (12.31) . — Let R be a ring, S a multiplicative subset, $\mathfrak{X}$ a set of variables, and M a module. Prove $(S^{-1}M)[\mathfrak{X}] = S^{-1}(M[\mathfrak{X}])$.

Exercise (12.32) . — Let R be a ring, $\mathfrak{a}$ an ideal, S a multiplicative subset, $\mathfrak{X}$ a set of variables. Set $R' := R/\mathfrak{a}$ and $P := R[\mathfrak{X}]$. Let $T \subset P$ be a multiplicative subset, and assume $S \subset T$. Prove $T^{-1}P/\mathfrak{a}T^{-1}P = T^{-1}\big((S^{-1}R')[\mathfrak{X}]\big)$.

Exercise (12.33) . — Let R be a ring, S a multiplicative subset. For $i = 1, 2$, let $\varphi_i\colon R \to R_i$ be a ring map, $S_i \subset R_i$ a multiplicative subset with $\varphi_i S \subset S_i$, and M_i an R_i-module. Set $T := \{s_1 \otimes s_2 \mid s_i \in S_i\} \subset R_1 \otimes_R R_2$. Prove

$$S_1^{-1}M_1 \otimes_{S^{-1}R} S_2^{-1}M_2 = S_1^{-1}M_1 \otimes_R S_2^{-1}M_2 = T^{-1}(M_1 \otimes_R M_2).$$

Exercise (12.34) . — Let R be a ring, $\mathfrak{m}$ a maximal ideal, $n \ge 1$, and M a module. Show $M/\mathfrak{m}^n M = M_{\mathfrak{m}}/\mathfrak{m}^n M_{\mathfrak{m}}$.

Exercise (12.35) . — Let k be a field. For $i = 1, 2$, let R_i be an algebra, and $\mathfrak{n}_i \subset R_i$ a maximal ideal with $R_i/\mathfrak{n}_i = k$. Let $\mathfrak{n} \subset R_1 \otimes_k R_2$ denote the ideal generated by $\mathfrak{n}_1$ and $\mathfrak{n}_2$. Set $A_i := (R_i)_{\mathfrak{n}_i}$ and $\mathfrak{m} := \mathfrak{n}(A_1 \otimes_k A_2)$. Prove that both $\mathfrak{n}$ and $\mathfrak{m}$ are maximal with k as residue field and that $(A_1 \otimes_k A_2)_{\mathfrak{m}} = (R_1 \otimes_k R_2)_{\mathfrak{n}}$.

Exercise (12.36) . — Let R be a ring, R' an algebra, S a multiplicative subset, M a finitely presented module. Prove these properties of the rth Fitting ideal:

$$F_r(M \otimes_R R') = F_r(M)R' \quad \text{and} \quad F_r(S^{-1}M) = F_r(M)S^{-1}R = S^{-1}F_r(M).$$

Exercise (12.37) . — Let R be a ring, S a multiplicative subset. Prove this:

(1) Let $M_1 \xrightarrow{\alpha} M_2$ be a map of modules, which restricts to a map $N_1 \to N_2$ of submodules. Then $\alpha(N_1^S) \subset N_2^S$; that is, there is an induced map $N_1^S \to N_2^S$.

(2) Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$ be a left exact sequence, which restricts to a left exact sequence $0 \to N_1 \to N_2 \to N_3$ of submodules. Then there is an induced left exact sequence of saturations: $0 \to N_1^S \to N_2^S \to N_3^S$.

Exercise (12.38) . — Let R be a ring, M a module, and S a multiplicative subset. Set $T^S M := \langle 0 \rangle^S$. We call it the **$S$-torsion submodule of** M. Prove the following:

(1) $T^S(M/T^S M) = 0$. (2) $T^S M = \mathrm{Ker}(\varphi_S)$.

(3) Let $\alpha\colon M \to N$ be a map. Then $\alpha(T^S M) \subset T^S N$.

(4) Let $0 \to M' \to M \to M''$ be exact. Then so is $0 \to T^S M' \to T^S M \to T^S M''$.

(5) Let $S_1 \subset S$ be a multiplicative subset. Then $T^S(S_1^{-1}M) = S_1^{-1}(T^S M)$.

Exercise (12.39) . — Set $R := \mathbb{Z}$ and $S := S_0 := Z - \langle 0 \rangle$. Set $M := \bigoplus_{n \ge 2} \mathbb{Z}/\langle n \rangle$ and $N := M$. Show that the map σ of **(12.19)** is not injective.

Exercise (12.40) . — Let R be a ring, S a multiplicative subset, M a module. Show that $S^{-1}\operatorname{nil}(M) \subset \operatorname{nil}(S^{-1}M)$, with equality if M is finitely generated.

Exercise (12.41) . — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal, M a module, and N a submodule. Set $\mathfrak{n} := \operatorname{nil}(M/N)$. Show:

(1) Then $\mathfrak{n} \cap S \neq \emptyset$ if and only if $\mathfrak{n}^S = R$.
(2) Assume $\mathfrak{n} \cap S \neq \emptyset$. Then $S^{-1}N = S^{-1}M$ and $N^S = M$.
(3) Then $\mathfrak{n}^S \subset \operatorname{nil}(M/N^S)$, with equality if M is finitely generated.

Exercise (12.42) . — Let R be a ring, M a module, N, N' submodules. Show:

(1) $\sqrt{\operatorname{nil}(M)} = \operatorname{nil}(M)$.
(2) $\operatorname{nil}(M/(N \cap N')) = \operatorname{nil}(M/N) \bigcap \operatorname{nil}(M/N')$.
(3) $\operatorname{nil}(M/N) = R$ if and only if $N = M$.
(4) $\operatorname{nil}(M/(N + N')) \supset \sqrt{\operatorname{nil}(M/N) + \operatorname{nil}(M/N')}$.

Find an example where equality fails in (4), yet R is a field.

13. Support

The spectrum of a ring is the following topological space: its points are the prime ideals, and each closed set consists of those primes containing a given ideal. The support of a module is the following subset: its points are the primes at which the localized module is nonzero. We relate the support to the closed set of the annihilator. We prove that a sequence is exact if and only if it is exact after localizing at every maximal ideal. We end this chapter by proving that the following conditions on a module are equivalent: it is finitely generated and projective; it is finitely presented and flat; and it is locally free of finite rank.

A. Text

(13.1) (Spectrum of a ring). — Let R be a ring. Its set of prime ideals is denoted $\operatorname{Spec}(R)$, and is called the (prime) **spectrum** of R.

Let $\mathfrak{a}$ be an ideal. Let $\mathbf{V}(\mathfrak{a})$ denote the subset of $\operatorname{Spec}(R)$ consisting of those primes that contain $\mathfrak{a}$. We call $\mathbf{V}(\mathfrak{a})$ the **variety** of $\mathfrak{a}$.

Let $\mathfrak{b}$ be a second ideal. Obviously, if $\mathfrak{a} \subset \mathfrak{b}$, then $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$. Conversely, if $\mathbf{V}(\mathfrak{b}) \subset \mathbf{V}(\mathfrak{a})$, then $\mathfrak{a} \subset \sqrt{\mathfrak{b}}$, owing to the Scheinnullstellensatz **(3.14)**. Therefore, $\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{b})$ if and only if $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$. Further, **(2.23)** yields

$$\mathbf{V}(\mathfrak{a}) \cup \mathbf{V}(\mathfrak{b}) = \mathbf{V}(\mathfrak{a} \cap \mathfrak{b}) = \mathbf{V}(\mathfrak{a}\mathfrak{b}).$$

A prime ideal $\mathfrak{p}$ contains the ideals $\mathfrak{a}_\lambda$ in an arbitrary collection if and only if $\mathfrak{p}$ contains their sum $\sum \mathfrak{a}_\lambda$; hence,

$$\bigcap \mathbf{V}(\mathfrak{a}_\lambda) = \mathbf{V}\big(\sum \mathfrak{a}_\lambda\big). \tag{13.1.1}$$

Finally, $\mathbf{V}(R) = \emptyset$, and $\mathbf{V}(\langle 0 \rangle) = \operatorname{Spec}(R)$. Thus the subsets $\mathbf{V}(\mathfrak{a})$ of $\operatorname{Spec}(R)$ are the closed sets of a topology; it is called the **Zariski topology**. Moreover, $\mathfrak{a} \mapsto \mathbf{V}(\mathfrak{a})$ is a lattice-inverting bijection from the radical ideals to the closed sets.

Given an element $f \in R$, we call the open set

$$\mathbf{D}(f) := \operatorname{Spec}(R) - \mathbf{V}(\langle f \rangle) \tag{13.1.2}$$

a **principal open set**. These sets form a basis for the topology of $\operatorname{Spec}(R)$; indeed, given any prime $\mathfrak{p} \not\supset \mathfrak{a}$, there is an $f \in \mathfrak{a} - \mathfrak{p}$, and so $\mathfrak{p} \in \mathbf{D}(f) \subset \operatorname{Spec}(R) - \mathbf{V}(\mathfrak{a})$. Further, $f, g \notin \mathfrak{p}$ if and only if $fg \notin \mathfrak{p}$, for any $f, g \in R$ and prime $\mathfrak{p}$; in other words,

$$\mathbf{D}(f) \cap \mathbf{D}(g) = \mathbf{D}(fg). \tag{13.1.3}$$

A ring map $\varphi\colon R \to R'$ induces a set map

$$\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(R') \to \operatorname{Spec}(R) \quad \text{by} \quad \operatorname{Spec}(\varphi)(\mathfrak{p}') := \varphi^{-1}(\mathfrak{p}'). \tag{13.1.4}$$

Notice $\varphi^{-1}(\mathfrak{p}') \supset \mathfrak{a}$ if and only if $\mathfrak{p}' \supset \mathfrak{a}R'$; so $\operatorname{Spec}(\varphi)^{-1}\,\mathbf{V}(\mathfrak{a}) = \mathbf{V}(\mathfrak{a}R')$ and

$$\operatorname{Spec}(\varphi)^{-1}\,\mathbf{D}(g) = \mathbf{D}(\varphi(g)). \tag{13.1.5}$$

Hence $\operatorname{Spec}(\varphi)$ is continuous. Given another ring map $\varphi'\colon R' \to R''$, plainly

$$\operatorname{Spec}(\varphi)\operatorname{Spec}(\varphi') = \operatorname{Spec}(\varphi'\varphi). \tag{13.1.6}$$

Moreover, $\operatorname{Spec}(1_R) = 1_{\operatorname{Spec}(R)}$. Thus $\operatorname{Spec}(\bullet)$ is a contravariant functor from ((Rings)) to the category of topological spaces and continuous maps.

For example, owing to (**1.9**) and (**2.7**), the quotient map $R \twoheadrightarrow R/\mathfrak{a}$ induces a topological embedding

$$\operatorname{Spec}(R/\mathfrak{a}) \xrightarrow{\sim} \mathbf{V}(\mathfrak{a}) \hookrightarrow \operatorname{Spec}(R). \tag{13.1.7}$$

Owing to (**11.12**), the localization map $R \to R_f$ induces a topological embedding

$$\operatorname{Spec}(R_f) \xrightarrow{\sim} D(f) \hookrightarrow \operatorname{Spec}(R). \tag{13.1.8}$$

Proposition (13.2). — *Let R be a ring, $X := \operatorname{Spec}(R)$. Then X is* ***quasi-compact:*** *if $X = \bigcup_{\lambda\in\Lambda} U_\lambda$ with U_λ open, then $X = \bigcup_{i=1}^n U_{\lambda_i}$ for some $\lambda_i \in \Lambda$.*

Proof: Say $U_\lambda = X - \mathbf{V}(\mathfrak{a}_\lambda)$. As $X = \bigcup_{\lambda\in\Lambda} U_\lambda$, then $\emptyset = \bigcap \mathbf{V}(\mathfrak{a}_\lambda) = \mathbf{V}\big(\sum \mathfrak{a}_\lambda\big)$. So $\sum \mathfrak{a}_\lambda$ lies in no prime ideal. Hence there are $\lambda_1, \ldots, \lambda_n \in \Lambda$ and $f_{\lambda_i} \in \mathfrak{a}_{\lambda_i}$ with $1 = \sum f_{\lambda_i}$. So $R = \sum \mathfrak{a}_{\lambda_i}$. So $\emptyset = \bigcap \mathbf{V}(\mathfrak{a}_{\lambda_i}) = \mathbf{V}\big(\sum \mathfrak{a}_{\lambda_i}\big)$. Thus $X = \bigcup U_{\lambda_i}$. □

Definition (13.3). — Let R be a ring, M a module. Its **support** is the set

$$\operatorname{Supp}(M) := \operatorname{Supp}_R(M) := \{\, \mathfrak{p} \in \operatorname{Spec}(R) \mid M_\mathfrak{p} \neq 0 \,\}.$$

Proposition (13.4). — *Let R be a ring, M a module.*

(1) *Let $0 \to L \to M \to N \to 0$ be exact. Then $\operatorname{Supp}(L) \bigcup \operatorname{Supp}(N) = \operatorname{Supp}(M)$.*

(2) *Let M_λ be submodules with $\sum M_\lambda = M$. Then $\bigcup \operatorname{Supp}(M_\lambda) = \operatorname{Supp}(M)$.*

(3) *Then $\operatorname{Supp}(M) \subset \boldsymbol{V}(\operatorname{Ann}(M))$, with equality if M is finitely generated.*

(4) *Then $\operatorname{rad}(M)$ is contained in the intersection of all the maximal ideals in $\operatorname{Supp}(M)$, with equality if M is finitely generated..*

Proof: Consider (1). For every prime $\mathfrak{p}$, the sequence $0 \to L_\mathfrak{p} \to M_\mathfrak{p} \to N_\mathfrak{p} \to 0$ is exact by (**12.13**). So $M_\mathfrak{p} \neq 0$ if and only if $L_\mathfrak{p} \neq 0$ or $N_\mathfrak{p} \neq 0$. Thus (1) holds.

In (2), $M_\lambda \subset M$. So (1) yields $\bigcup \operatorname{Supp}(M_\lambda) \subset \operatorname{Supp}(M)$. To prove the opposite inclusion, take $\mathfrak{p} \notin \bigcup \operatorname{Supp}(M_\lambda)$. Then $(M_\lambda)_\mathfrak{p} = 0$ for all λ. By hypothesis, the natural map $\bigoplus M_\lambda \to M$ is surjective. So $\bigoplus (M_\lambda)_\mathfrak{p} \to M_\mathfrak{p}$ is surjective by (**12.9**). Hence $M_\mathfrak{p} = 0$. Alternatively, given $m/s \in M_\mathfrak{p}$, express m as a finite sum $m = \sum m_\lambda$ with $m_\lambda \in M_\lambda$. For each such λ, there is $t_\lambda \in R - \mathfrak{p}$ with $t_\lambda m_\lambda = 0$. Set $t := \prod t_\lambda$. Then $tm = 0$ and $t \notin \mathfrak{p}$. So $m/s = 0$ in $M_\mathfrak{p}$. Hence again, $M_\mathfrak{p} = 0$. Thus $\mathfrak{p} \notin \operatorname{Supp}(M)$, and so (2) holds.

Consider (3). Let $\mathfrak{p}$ be a prime. By (**12.17**)(2), $M_\mathfrak{p} = 0$ if $\operatorname{Ann}(M) \cap (R - \mathfrak{p}) \neq \emptyset$, and the converse holds if M is finitely generated. But $\operatorname{Ann}(M) \bigcap (R - \mathfrak{p}) \neq \emptyset$ if and only if $\operatorname{Ann}(M) \not\subset \mathfrak{p}$. Thus (3) holds.

For (4), recall from (**4.1**) that $\operatorname{rad}(M)$ is defined as the intersection of all the maximal ideals containing $\operatorname{Ann}(M)$. Thus (3) yields (4). □

(13.5) (Minimal primes of a module). — Let R be a ring, M a module, and $\mathfrak{p}$ a prime minimal in $\operatorname{Supp}(M)$. We call such a $\mathfrak{p}$ a **minimal prime** of M.

Suppose M is finitely generated. Then $\operatorname{Supp}(M) = \mathbf{V}(\operatorname{Ann}(M))$ by (**13.4**)(3). Thus $\mathfrak{p}$ is a minimal prime of M if and only if $\mathfrak{p}$ is a minimal prime of $\operatorname{Ann}(M)$. Also, (**3.17**) implies every prime in $\operatorname{Supp}(M)$ contains some minimal prime of M.

Warning: following a old custom, by the **minimal primes of** an ideal $\mathfrak{a}$, we mean not those of $\mathfrak{a}$ viewed as an abstract module, but rather those of $R/\mathfrak{a}$; however, by the **minimal primes** of R, we mean those of R viewed as an abstract module; compare (**3.17**).

Proposition (13.6). — *Let R be a ring, M a finitely generated module. Then*

$$\operatorname{nil}(M) = \textstyle\bigcap_{\mathfrak{p}\in\operatorname{Supp}(M)} \mathfrak{p}.$$

Proof: First, $\mathrm{nil}(M) = \bigcap_{\mathfrak{p}\supset \mathrm{Ann}(M)} \mathfrak{p}$ by the Scheinnullstellensatz (**3.14**). But $\mathfrak{p} \supset \mathrm{Ann}(M)$ if and only if $\mathfrak{p} \in \mathrm{Supp}(M)$ by (**13.4**)(3). □

Proposition (13.7). — *Let R be a ring, M and N modules. Then*

$$\mathrm{Supp}(M \otimes_R N) \subset \mathrm{Supp}(M) \cap \mathrm{Supp}(N), \tag{13.7.1}$$

with equality if M and N are finitely generated.

Proof: First, $(M\otimes_R N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}}$ by (**12.30**); whence, (**13.7.1**) holds. The opposite inclusion follows from (**10.10**)(2) if M and N are finitely generated. □

Proposition (13.8). — *Let R be a ring, M a module. These conditions are equivalent:* (1) $M = 0$; (2) $\mathrm{Supp}(M) = \emptyset$; (3) $M_{\mathfrak{m}} = 0$ *for every maximal ideal* $\mathfrak{m}$.

Proof: Trivially, if (1) holds, then $S^{-1}M = 0$ for any multiplicative subset S. In particular, (2) holds. Trivially, (2) implies (3).

Finally, assume $M \neq 0$, and take a nonzero $m \in M$, and set $\mathfrak{a} := \mathrm{Ann}(m)$. Then $1 \notin \mathfrak{a}$, so $\mathfrak{a}$ lies in some maximal ideal $\mathfrak{m}$. Given $f \in S_{\mathfrak{m}} := R - \mathfrak{m}$, note $fm \neq 0$. Hence $m/1 \neq 0$ in $M_{\mathfrak{m}}$. Thus (3) implies (1). □

Proposition (13.9). — *A sequence of modules $L \xrightarrow{\alpha} M \xrightarrow{\beta} N$ is exact if and only if its localization $L_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} M_{\mathfrak{m}} \xrightarrow{\beta_{\mathfrak{m}}} N_{\mathfrak{m}}$ is exact at each maximal ideal $\mathfrak{m}$.*

Proof: If the sequence is exact, then so is its localization by (**12.13**).

Consider the converse. First $\mathrm{Im}(\beta_{\mathfrak{m}}\alpha_{\mathfrak{m}}) = 0$. But $\mathrm{Im}(\beta_{\mathfrak{m}}\alpha_{\mathfrak{m}}) = \big(\mathrm{Im}(\beta\alpha)\big)_{\mathfrak{m}}$ by (**12.13**) and (**9.3**). So $\mathrm{Im}(\beta\alpha) = 0$ by (**13.8**). So $\beta\alpha = 0$. Thus $\mathrm{Im}(\alpha) \subset \mathrm{Ker}(\beta)$.

Set $H := \mathrm{Ker}(\beta)\big/\mathrm{Im}(\alpha)$. Then $H_{\mathfrak{m}} = \mathrm{Ker}(\beta_{\mathfrak{m}})\big/\mathrm{Im}(\alpha_{\mathfrak{m}})$ by (**12.13**) and (**9.3**). So $H_{\mathfrak{m}} = 0$ owing to the hypothesis. Hence $H = 0$ by (**13.8**), as required. □

Exercise (13.10) . — Let R be a ring, M a module, and $m_\lambda \in M$ elements. Prove the m_λ generate M if and only if, at every maximal ideal $\mathfrak{m}$, the fractions $m_\lambda/1$ generate $M_{\mathfrak{m}}$ over $R_{\mathfrak{m}}$.

Proposition (13.11). — *Let A be a semilocal ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ its maximal ideals, M, N finitely presented modules. Assume $M_{\mathfrak{m}_i} \simeq N_{\mathfrak{m}_i}$ for each i. Then $M \simeq N$.*

Proof: For each i, take an isomorphism $\psi_i\colon M_{\mathfrak{m}_i} \xrightarrow{\sim} N_{\mathfrak{m}_i}$. Then (**12.19**) yields $s_i \in A - \mathfrak{m}_i$ and $\varphi_i\colon M \to N$ with $(\varphi_i)_{\mathfrak{m}_i} = s_i\psi_i$. But $\bigcap_{j\neq i}\mathfrak{m}_j \not\subset \mathfrak{m}_i$ by (**2.23**); so there's $x_i \in \bigcap_{j\neq i}\mathfrak{m}_j$ with $x_i \notin \mathfrak{m}_i$. Set $\gamma := \sum_i x_i\varphi_i$, so $\gamma\colon M \to N$.

For each j, set $\alpha_j := x_j\varphi_j$. Then $(\alpha_j)_{\mathfrak{m}_j}\colon M_{\mathfrak{m}_j} \xrightarrow{\sim} N_{\mathfrak{m}_j}$ as $x_j, s_j \in A^\times$. Set $\beta_j := \sum_{i\neq j}\alpha_i$. Then $\beta_j(M_{\mathfrak{m}_j}) \subset \mathfrak{m}_j N_{\mathfrak{m}_j}$ as $x_i \in \mathfrak{m}_j$ for $i \neq j$. Also, $\gamma = \alpha_j + \beta_j$. So $\gamma_{\mathfrak{m}_j}$ is an isomorphism by (**10.29**). Thus (**13.9**) gives $\gamma\colon M \xrightarrow{\sim} N$. □

Proposition (13.12). — *Let R be a ring, M a module. Then M is flat over R if and only if, at every maximal ideal $\mathfrak{m}$, the localization $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$.*

Proof: If M is flat over R, then $M \otimes_R R_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$ by (**9.22**). But $M \otimes_R R_{\mathfrak{m}} = M_{\mathfrak{m}}$ by (**12.10**). Thus $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$.

Conversely, assume $M_{\mathfrak{m}}$ is flat over $R_{\mathfrak{m}}$ for every $\mathfrak{m}$. Let $\alpha\colon N' \to N$ be an injection of R-modules. Then $\alpha_{\mathfrak{m}}$ is injective by (**13.9**). Hence $M_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} \alpha_{\mathfrak{m}}$ is injective. But that map is equal to $(M\otimes\alpha)_{\mathfrak{m}}$ by (**12.30**). So $(M\otimes\alpha)_{\mathfrak{m}}$ is injective. Hence $M \otimes \alpha$ is injective by (**13.9**). Thus M is flat over R. □

Definition (13.13). — Let R be a ring, M a module. We say M is **locally finitely generated** if each $\mathfrak{p} \in \operatorname{Spec}(R)$ has a neighborhood on which M becomes finitely generated; more precisely, there exists $f \in R - \mathfrak{p}$ such that M_f is finitely generated over R_f. It is enough that an f exist for each maximal ideal $\mathfrak{m}$ as every $\mathfrak{p}$ lies in some $\mathfrak{m}$ by (**2.21**). Similarly, we define the properties **locally finitely presented**, **locally free of finite rank**, and **locally free of rank** n.

Proposition (13.14). — *Let R be a ring, M a module.*

(1) *If M is locally finitely generated, then it is finitely generated.*
(2) *If M is locally finitely presented, then it is finitely presented.*

Proof: By (**13.2**), there are $f_1, \dots, f_n \in R$ with $\bigcup \mathbf{D}(f_i) = \operatorname{Spec}(R)$ and finitely many $m_{ij} \in M$ such that, for some $n_{ij} \geq 0$, the $m_{ij}/f_i^{n_{ij}}$ generate M_{f_i} over R_{f_i}. Plainly, for each i, the $m_{ij}/1$ also generate M_{f_i} over R_{f_i}.

Given any maximal ideal $\mathfrak{m}$, there is i such that $f_i \notin \mathfrak{m}$. Let S_i be the image of $S_\mathfrak{m} := R - \mathfrak{m}$ in R_{f_i}. Then (**12.5**) yields $M_\mathfrak{m} = S_i^{-1}(M_{f_i})$. Hence the $m_{ij}/1$ generate $M_\mathfrak{m}$ over $R_\mathfrak{m}$. Thus (**13.10**) yields (1).

Assume M is locally finitely presented. Then M is finitely generated by (1). So there is a surjection $R^k \twoheadrightarrow M$. Let K be its kernel. Then K is locally finitely generated owing to (**5.18**). Hence K too is finitely generated by (1). So there is a surjection $R^\ell \twoheadrightarrow K$. It yields the desired finite presentation $R^\ell \to R^k \to M \to 0$. Thus (2) holds. □

Theorem (13.15). — *These conditions on an R-module P are equivalent:*

(1) *P is finitely generated and projective.*
(2) *P is finitely presented and flat.*
(3) *P is finitely presented, and $P_\mathfrak{m}$ is free over $R_\mathfrak{m}$ at each maximal ideal $\mathfrak{m}$.*
(4) *P is locally free of finite rank.*
(5) *P is finitely generated, and for each $\mathfrak{p} \in \operatorname{Spec}(R)$, there are f and n such that $\mathfrak{p} \in \boldsymbol{D}(f)$ and $P_\mathfrak{q}$ is free of rank n over $R_\mathfrak{q}$ at each $\mathfrak{q} \in \boldsymbol{D}(f)$.*

Proof: Condition (1) implies (2) by (**10.12**).

Let $\mathfrak{m}$ be a maximal ideal. Then $R_\mathfrak{m}$ is local by (**11.14**). If P is finitely presented, then $P_\mathfrak{m}$ is finitely presented, because localization preserves direct sums and cokernels by (**12.9**).

Assume (2). Then $P_\mathfrak{m}$ is flat by (**13.12**), so free by (**10.12**). Thus (3) holds.

Assume (3). Fix a surjective map $\alpha\colon M \to N$. Then $\alpha_\mathfrak{m}\colon M_\mathfrak{m} \to N_\mathfrak{m}$ is surjective. So $\operatorname{Hom}(P_\mathfrak{m}, \alpha_\mathfrak{m})\colon \operatorname{Hom}(P_\mathfrak{m}, M_\mathfrak{m}) \to \operatorname{Hom}(P_\mathfrak{m}, N_\mathfrak{m})$ is surjective by (**5.16**) and (**5.15**). But $\operatorname{Hom}(P_\mathfrak{m}, \alpha_\mathfrak{m}) = \operatorname{Hom}(P, \alpha)_\mathfrak{m}$ by (**12.19**) as P is finitely presented. Further, $\mathfrak{m}$ is arbitrary. Hence $\operatorname{Hom}(P, \alpha)$ is surjective by (**13.9**). Therefore, P is projective by (**5.16**). Thus (1) holds.

Again assume (3). Given any prime $\mathfrak{p}$, take a maximal ideal $\mathfrak{m}$ containing it. By hypothesis, $P_\mathfrak{m}$ is free; its rank is finite as $P_\mathfrak{m}$ is finitely generated. By (**12.18**)(2), there is $f \in S_\mathfrak{m} := R - \mathfrak{m}$ such that P_f is free of finite rank over R_f. Thus (4) holds.

Assume (4). Then P is locally finitely presented. So P is finitely presented by (**13.14**)(2). Further, given $\mathfrak{p} \in \operatorname{Spec}(R)$, there are $f \in S_\mathfrak{p} := R - \mathfrak{p}$ and n such that P_f is free of rank n over R_f. Given $\mathfrak{q} \in \mathbf{D}(f)$, let S be the image of $S_\mathfrak{q} := R - \mathfrak{q}$ in R_f. Then (**12.5**) yields $P_\mathfrak{q} = S^{-1}(P_f)$. Hence $P_\mathfrak{q}$ is free of rank n over $R_\mathfrak{q}$. Thus (5) holds. Further, (3) results from taking $\mathfrak{p} := \mathfrak{m}$ and $\mathfrak{q} := \mathfrak{m}$.

Finally, assume (5), and let's prove (4). Given $\mathfrak{p} \in \operatorname{Spec}(R)$, let f and n be provided by (5). Take a free basis $p_1/f^{k_1}, \dots, p_n/f^{k_n}$ of $P_\mathfrak{p}$ over $R_\mathfrak{p}$. The p_i define a map $\alpha\colon R^n \to P$, and $\alpha_\mathfrak{p}\colon R^n_\mathfrak{p} \to P_\mathfrak{p}$ is bijective, in particular, surjective.

As P is finitely generated, **(12.18)**(1) provides $g \in S_\mathfrak{p}$ such that $\alpha_g\colon R^n_g \to P_g$ is surjective. It follows that $\alpha_\mathfrak{q}\colon R^n_\mathfrak{q} \to P_\mathfrak{q}$ is surjective for every $\mathfrak{q} \in \mathbf{D}(g)$. If also $\mathfrak{q} \in \mathbf{D}(f)$, then by hypothesis $P_\mathfrak{q} \simeq R^n_\mathfrak{q}$. So $\alpha_\mathfrak{q}$ is bijective by **(10.4)**.

Set $h := fg$. Clearly, $\mathbf{D}(f) \cap \mathbf{D}(g) = \mathbf{D}(h)$. By **(13.1)**, $\mathbf{D}(h) = \operatorname{Spec}(R_h)$. Clearly, $\alpha_\mathfrak{q} = (\alpha_h)_{(\mathfrak{q}R_h)}$ for all $\mathfrak{q} \in \mathbf{D}(h)$. Hence $\alpha_h\colon R^n_h \to P_h$ is bijective owing to **(13.9)** with R_h for R. Thus (4) holds. □

B. Exercises

Exercise (13.16) . — Let R be a ring, $X := \operatorname{Spec}(R)$, and $\mathfrak{p}, \mathfrak{q} \in X$. Show:

(1) The closure $\overline{\{\mathfrak{p}\}}$ of $\mathfrak{p}$ is equal to $\mathbf{V}(\mathfrak{p})$; that is, $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$ if and only if $\mathfrak{p} \subset \mathfrak{q}$.
(2) Then $\mathfrak{p}$ is a closed point, that is, $\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}}$, if and only if $\mathfrak{p}$ is maximal.
(3) Then X is T_0; that is, if $\mathfrak{p} \neq \mathfrak{q}$ but every neighborhood of $\mathfrak{p}$ contains $\mathfrak{q}$, then some neighborhood of $\mathfrak{q}$ doesn't contain $\mathfrak{p}$.

Exercise (13.17) . — Describe $\operatorname{Spec}(\mathbb{R})$, $\operatorname{Spec}(\mathbb{Z})$, $\operatorname{Spec}(\mathbb{C}[X])$, and $\operatorname{Spec}(\mathbb{R}[X])$.

Exercise (13.18) . — Let R be a ring, and set $X := \operatorname{Spec}(R)$. Let $X_1, X_2 \subset X$ be closed subsets. Show that the following four statements are equivalent:

(1) Then $X_1 \sqcup X_2 = X$; that is, $X_1 \cup X_2 = X$ and $X_1 \cap X_2 = \emptyset$.
(2) There are complementary idempotents $e_1, e_2 \in R$ with $\mathbf{V}(\langle e_i \rangle) = X_i$.
(3) There are comaximal ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1\mathfrak{a}_2 = 0$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.
(4) There are ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = R$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.

Finally, given any e_i and $\mathfrak{a}_i$ satisfying (2) and either (3) or (4), necessarily $e_i \in \mathfrak{a}_i$.

Exercise (13.19) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Show:

(1) Then $\Gamma_\mathfrak{a}(M) = \{\, m \in M \mid \operatorname{Supp}(Rm) \subset \mathbf{V}(\mathfrak{a}) \,\}$.
(2) Then $\Gamma_\mathfrak{a}(M) = \{\, m \in M \mid m/1 = 0 \text{ in } M_\mathfrak{p} \text{ for all primes } \mathfrak{p} \not\supset \mathfrak{a} \,\}$.
(3) Then $\Gamma_\mathfrak{a}(M) = M$ if and only if $\operatorname{Supp}(M) \subset \mathbf{V}(\mathfrak{a})$.

Exercise (13.20) . — Let R be a ring, $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ a short exact sequence of finitely generated modules, and $\mathfrak{a}$ a finitely generated ideal. Assume $\operatorname{Supp}(M') \subset \mathbf{V}(\mathfrak{a})$. Show that $0 \to \Gamma_\mathfrak{a}(M') \to \Gamma_\mathfrak{a}(M) \to \Gamma_\mathfrak{a}(M'') \to 0$ is exact.

Exercise (13.21) . — Let R be a ring, S a multiplicative subset. Prove this:

(1) Assume R is absolutely flat. Then $S^{-1}R$ is absolutely flat.
(2) Then R is absolutely flat if and only if $R_\mathfrak{m}$ is a field for each maximal $\mathfrak{m}$.

Exercise (13.22) . — Let R be a ring; set $X := \operatorname{Spec}(R)$. Prove that the four following conditions are equivalent:

(1) $R/\operatorname{nil}(R)$ is absolutely flat.
(2) X is Hausdorff.
(3) X is T_1; that is, every point is closed.
(4) Every prime $\mathfrak{p}$ of R is maximal.

Assume (1) holds. Prove that X is **totally disconnected**; namely, no two distinct points lie in the same connected component.

Exercise (13.23) . — Let R be a ring, and $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} \subset \mathrm{nil}(R)$. Set $X := \mathrm{Spec}(R)$. Show that the following three statements are equivalent:

(1) Then R is decomposable. (2) Then $R/\mathfrak{a}$ is decomposable.
(3) Then $X = \bigsqcup_{i=1}^{n} X_i$ where $X_i \subset X$ is closed and has a unique closed point.

Exercise (13.24) . — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Prove these two statements:

(1) Every prime of R is the contraction of a prime if and only if φ^* is surjective.
(2) If every prime of R' is the extension of a prime, then φ^* is injective.

Is the converse of (2) true?

Exercise (13.25) . — Let R be a ring, and S a multiplicative subset of R. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(S^{-1}R)$. Set $\varphi_S^* := \mathrm{Spec}(\varphi_S)$ and $S^{-1}X := \mathrm{Im}\,\varphi_S^*$ in X. Show (1) that $S^{-1}X$ consists of the primes $\mathfrak{p}$ of R with $\mathfrak{p} \cap S = \emptyset$ and (2) that φ_S^* is a homeomorphism of Y onto $S^{-1}X$.

Exercise (13.26) . — Let $\theta\colon R \to R'$ be a ring map, $S \subset R$ a multiplicative subset. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$ and $\theta^* := \mathrm{Spec}(\theta)$. Via **(13.25)**(2) and **(11.15)**, identify $\mathrm{Spec}(S^{-1}R)$ and $\mathrm{Spec}(S^{-1}R')$ with their images $S^{-1}X \subset X$ and $S^{-1}Y \subset Y$. Show (1) $S^{-1}Y = \theta^{*-1}(S^{-1}X)$ and (2) $\mathrm{Spec}(S^{-1}\theta) = \theta^*\big|S^{-1}Y$.

Exercise (13.27) . — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{a} \subset R$ an ideal. Set $\mathfrak{b} := \mathfrak{a}R'$. Let $\overline{\theta}\colon R/\mathfrak{a} \to R'/\mathfrak{b}$ be the induced map. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$. Set $\theta^* := \mathrm{Spec}(\theta)$ and $\overline{\theta}^* := \mathrm{Spec}(\overline{\theta})$. Via **(13.1)**, identify $\mathrm{Spec}(R/\mathfrak{a})$ and $\mathrm{Spec}(R'/\mathfrak{b})$ with $\mathbf{V}(\mathfrak{a}) \subset X$ and $\mathbf{V}(\mathfrak{b}) \subset Y$. Show (1) $\mathbf{V}(\mathfrak{b}) = \theta^{*-1}(\mathbf{V}(\mathfrak{a}))$ and (2) $\overline{\theta}^* = \theta^*\big|\,\mathbf{V}(\mathfrak{b})$.

Exercise (13.28) . — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{p} \subset R$ a prime, k the residue field of $R_\mathfrak{p}$. Set $\theta^* := \mathrm{Spec}(\theta)$. Show (1) $\theta^{*-1}(\mathfrak{p})$ is canonically homeomorphic to $\mathrm{Spec}(R'_\mathfrak{p}/\mathfrak{p}R'_\mathfrak{p})$ and to $\mathrm{Spec}(k \otimes_R R')$ and (2) $\mathfrak{p} \in \mathrm{Im}\,\theta^*$ if and only if $k \otimes_R R' \neq 0$.

Exercise (13.29) . — Let R be a ring, $\mathfrak{p}$ a prime ideal. Show that the image of $\mathrm{Spec}(R_\mathfrak{p})$ in $\mathrm{Spec}(R)$ is the intersection of all open neighborhoods of $\mathfrak{p}$ in $\mathrm{Spec}(R)$.

Exercise (13.30) . — Let $\varphi\colon R \to R'$ and $\psi\colon R \to R''$ be ring maps, and define $\theta\colon R \to R' \otimes_R R''$ by $\theta(x) := \varphi(x) \otimes \psi(x)$. Show

$$\mathrm{Im}\,\mathrm{Spec}(\theta) = \mathrm{Im}\,\mathrm{Spec}(\varphi) \bigcap \mathrm{Im}\,\mathrm{Spec}(\psi).$$

Exercise (13.31) . — Let R be a filtered direct limit of rings R_λ with transition maps α_μ^λ and insertions α_λ. For each λ, let $\varphi_\lambda\colon R' \to R_\lambda$ be a ring map with $\varphi_\mu = \alpha_\mu^\lambda \varphi_\lambda$ for all α_μ^λ, so that $\varphi := \alpha_\lambda \varphi_\lambda$ is independent of λ. Show

$$\mathrm{Im}\,\mathrm{Spec}(\varphi) = \bigcap\nolimits_\lambda \mathrm{Im}\,\mathrm{Spec}(\varphi_\lambda).$$

Exercise (13.32) . — Let R be a ring, $\varphi_\sigma\colon R \to R_\sigma$ for $\sigma \in \Sigma$ ring maps. Let $\gamma_\Sigma\colon R \to \coprod R_\sigma$ and $\pi_\Sigma\colon R \to \prod R_\sigma$ be the induced maps. Set $X := \mathrm{Spec}(R)$. Show:

(1) Then $\mathrm{Im}\,\mathrm{Spec}(\gamma_\Sigma) = \bigcap \mathrm{Im}\,\mathrm{Spec}(\varphi_\sigma)$.
(2) Assume Σ is finite. Then $\mathrm{Im}\,\mathrm{Spec}(\pi_\Sigma) = \bigcup \mathrm{Im}\,\mathrm{Spec}(\varphi_\sigma)$.
(3) The subsets of X of the form $\mathrm{Im}\,\mathrm{Spec}(\varphi)$, where $\varphi\colon R \to R'$ is a ring map, are the closed sets of a topology, known as the **constructible topology**. It refines the Zariski topology.
(4) In the constructible topology, X is quasi-compact.

Exercise (13.33) . — Let R be a ring, $X := \mathrm{Spec}(R)$. Show:

(1) Given $g \in R$, the set $\mathbf{D}(g)$ is open and closed in the constructible toplogy.
(2) On X, any topology with all $\mathbf{D}(g)$ open and closed is Hausdorff and totally disconnected.
(3) On any set, nested topologies $\mathcal{T} \supset \mathcal{S}$ coincide if $\mathcal{T}$ is quasi-compact and $\mathcal{S}$ is Hausdorff.
(4) On X, the constructible and the Zariski topologies coincide if and only if the Zariski topology is Hausdorff, if and only if $R/\mathrm{nil}(R)$ is absolutely flat.
(5) On X, the construcible topology is smallest with all $\mathbf{D}(g)$ open and closed.
(6) On X, the constructible open sets are the arbitray unions U of the finite intersections of the $\mathbf{D}(g)$ and the $X - \mathbf{D}(g)$.

Exercise (13.34) . — Let $\varphi\colon R \to R'$ be a ring map. Show, in the constructible topology, $\mathrm{Spec}(\varphi)\colon \mathrm{Spec}(R') \to \mathrm{Spec}(R)$ is continuous and closed.

Exercise (13.35) . — Let A be a domain with just one nonzero prime $\mathfrak{p}$. Set $K := \mathrm{Frac}(A)$ and $R := (A/\mathfrak{p}) \times K$. Define $\varphi\colon A \to R$ by $\varphi(x) := (x', x)$ with x' the residue of x. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Show φ^* is bijective, but not a homeomorphism.

Exercise (13.36) . — Let $\varphi\colon R \to R'$ be a ring map, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Show (1) that the closure $\overline{\varphi^*(\mathbf{V}(\mathfrak{b}))}$ in $\mathrm{Spec}(R)$ is equal to $\mathbf{V}(\varphi^{-1}\mathfrak{b})$ and (2) that $\varphi^*(\mathrm{Spec}(R'))$ is dense in $\mathrm{Spec}(R)$ if and only if $\mathrm{Ker}(\varphi) \subset \mathrm{nil}(R)$.

Exercise (13.37) . — Let $\varphi\colon R \to R'$ be a ring map. Consider these statements:

(1) The map φ has the **Going-up Property**: given primes $\mathfrak{q}' \subset R'$ and $\mathfrak{p} \subset R$ with $\mathfrak{p} \supset \varphi^{-1}(\mathfrak{q}')$, there is a prime $\mathfrak{p}' \subset R'$ with $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ and $\mathfrak{p}' \supset \mathfrak{q}'$.
(2) Given a prime $\mathfrak{q}'$ of R', set $\mathfrak{q} := \varphi^{-1}(\mathfrak{q}')$. Then $\mathrm{Spec}(R'/\mathfrak{q}') \to \mathrm{Spec}(R/\mathfrak{q})$ is surjective.
(3) The map $\mathrm{Spec}(\varphi)$ is **closed**: it maps closed sets to closed sets.

Prove that (1) and (2) are equivalent, and are implied by (3).

Exercise (13.38) . — Let $\varphi\colon R \to R'$ be a ring map. Consider these statements:

(1) The map φ has the **Going-down Property**: given primes $\mathfrak{q}' \subset R'$ and $\mathfrak{p} \subset R$ with $\mathfrak{p} \subset \varphi^{-1}(\mathfrak{q}')$, there is a prime $\mathfrak{p}' \subset R'$ with $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ and $\mathfrak{p}' \subset \mathfrak{q}'$.
(2) Given a prime $\mathfrak{q}'$ of R', set $\mathfrak{q} := \varphi^{-1}(\mathfrak{q}')$. Then $\mathrm{Spec}(R'_{\mathfrak{q}'}) \to \mathrm{Spec}(R_{\mathfrak{q}})$ is surjective.
(3) The map $\mathrm{Spec}(\varphi)$ is **open**: it maps open sets to open sets.

Prove (1) and (2) are equivalent; using **(13.31)**, prove they're implied by (3).

Exercise (13.39) . — Let R be a ring; $f, g \in R$. Prove (1)–(8) are equivalent:

(1) $\mathbf{D}(g) \subset \mathbf{D}(f)$. (2) $\mathbf{V}(\langle g\rangle) \supset \mathbf{V}(\langle f\rangle)$. (3) $\sqrt{\langle g\rangle} \subset \sqrt{\langle f\rangle}$.
(4) $\overline{S}_f \subset \overline{S}_g$. (5) $g \in \sqrt{\langle f\rangle}$. (6) $f \in \overline{S}_g$.
(7) There is a unique R-algebra map $\varphi^f_g\colon \overline{S}_f^{-1} R \to \overline{S}_g^{-1} R$.
(8) There is an R-algebra map $R_f \to R_g$.

If these conditions hold, prove the map in (8) is equal to φ^f_g.

Exercise (13.40) . — Let R be a ring. Prove these statements:

(1) $\mathbf{D}(f) \mapsto R_f$ is a well-defined contravariant functor from the category of principal open sets and inclusions to $((R\text{-alg}))$.
(2) Given $\mathfrak{p} \in \mathrm{Spec}(R)$, then $\varinjlim_{\mathbf{D}(f)\ni\mathfrak{p}} R_f = R_{\mathfrak{p}}$.

Exercise (13.41) . — Let R be a ring, $X := \operatorname{Spec}(R)$, and U an open subset. Show U is quasi-compact if and only if $X - U = \mathbf{V}(\mathfrak{a})$ where $\mathfrak{a}$ is finitely generated.

Exercise (13.42) . — Let R be a ring, M a module. Set $X := \operatorname{Spec}(R)$. Assume $X = \bigcup_{\lambda\in\Lambda} \mathbf{D}(f_\lambda)$ for some set Λ and some $f_\lambda \in R$.

(1) Given $m \in M$, assume $m/1 = 0$ in M_{f_λ} for all λ. Show $m = 0$.

(2) Given $m_\lambda \in M_{f_\lambda}$ for each λ, assume the images of m_λ and m_μ in $M_{f_\lambda f_\mu}$ are equal. Show there is a unique $m \in M$ whose image in M_{f_λ} is m_λ for all λ. First assume Λ is finite.

Exercise (13.43) . — Let B be a Boolean ring, and set $X := \operatorname{Spec}(B)$. Show a subset $U \subset X$ is both open and closed if and only if $U = \mathbf{D}(f)$ for some $f \in B$. Further, show X is a compact Hausdorff space. (Following Bourbaki, we shorten "quasi-compact" to "compact" when the space is Hausdorff.)

Exercise (13.44) (*Stone's Theorem*) . — Show every Boolean ring B is isomorphic to the ring of continuous functions from a compact Hausdorff space X to $\mathbb{F}_2$ with the discrete topology. Equivalently, show B is isomorphic to the ring R of open and closed subsets of X; in fact, $X := \operatorname{Spec}(B)$, and $B \xrightarrow{\sim} R$ is given by $f \mapsto \mathbf{D}(f)$.

Exercise (13.45) . — Let L be a Boolean lattice. Show that L is isomorphic to the lattice of open and closed subsets of a compact Hausdorff space.

Exercise (13.46) . — Let R be a ring, $\mathfrak{q}$ an ideal, M a module. Show:

(1) $\operatorname{Supp}(M/\mathfrak{q}M) \subset \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q})$, with equality if M is finitely generated.

(2) Assume M is finitely generated. Then

$$\mathbf{V}(\mathfrak{q} + \operatorname{Ann}(M)) = \operatorname{Supp}(M/\mathfrak{q}M) = \mathbf{V}(\operatorname{Ann}(M/\mathfrak{q}M)).$$

Exercise (13.47) . — Let $\varphi\colon R \to R'$ be a ring map, M' a finitely generated R'-module. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Assume M' is flat over R. Then M' is faithfully flat if and only if $\varphi^* \operatorname{Supp}(M') = \operatorname{Spec}(R)$.

Exercise (13.48) . — Let $\varphi\colon R \to R'$ be a ring map, M' a finitely generated R'-module, and $\mathfrak{q} \in \operatorname{Supp}(M')$. Assume that M' is flat over R. Set $\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$. Show that φ induces a surjection $\operatorname{Supp}(M'_\mathfrak{q}) \twoheadrightarrow \operatorname{Spec}(R_\mathfrak{p})$.

Exercise (13.49) . — Let $\varphi\colon R \to R'$ be a map of rings, M an R-module. Prove

$$\operatorname{Supp}(M \otimes_R R') \subset \operatorname{Spec}(\varphi)^{-1}(\operatorname{Supp}(M)),$$

with equality if M is finitely generated.

Exercise (13.50) . — Let R be a ring, M a module, $\mathfrak{p} \in \operatorname{Supp}(M)$. Prove

$$\mathbf{V}(\mathfrak{p}) \subset \operatorname{Supp}(M).$$

Exercise (13.51) . — Set $M := \mathbb{Q}/\mathbb{Z}$. Find $\operatorname{Supp}(M)$, and show it's not Zariski closed in $\operatorname{Spec}(\mathbb{Z})$. Is $\operatorname{Supp}(M) = \mathbf{V}(\operatorname{Ann}(M))$? What about **(13.4)**(3)?

Exercise (13.52) . — Let R be a domain, M a module. Set $T(M) := T^{S_0}(M)$. Call $T(M)$ the **torsion submodule** of M, and M **torsionfree** if $T(M) = 0$.

Prove M is torsionfree if and only if $M_\mathfrak{m}$ is torsionfree for all maximal ideals $\mathfrak{m}$.

Exercise (13.53) . — Let R be a ring, P a module, M, N submodules. Assume $M_\mathfrak{m} = N_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$. Show $M = N$. First assume $M \subset N$.

Exercise (13.54) . — Let R be a ring, M a module, and $\mathfrak{a}$ an ideal. Suppose $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \supset \mathfrak{a}$. Show that $M = \mathfrak{a}M$.

Exercise (13.55) . — Let R be a ring, P a module, M a submodule, and $p \in P$ an element. Assume $p/1 \in M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Show $p \in M$.

Exercise (13.56) . — Let R be a domain, $\mathfrak{a}$ an ideal. Show $\mathfrak{a} = \bigcap_{\mathfrak{m}} \mathfrak{a}R_{\mathfrak{m}}$ where $\mathfrak{m}$ runs through the maximal ideals and the intersection takes place in $\mathrm{Frac}(R)$.

Exercise (13.57) . — Prove these three conditions on a ring R are equivalent:

(1) R is reduced.
(2) $S^{-1}R$ is reduced for all multiplicative subsets S.
(3) $R_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$.

Exercise (13.58) . — Let R be a ring, Σ the set of minimal primes. Prove this:

(1) If $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$, then the $\mathfrak{p} \in \Sigma$ are pairwise comaximal.
(2) $R = \prod_{i=1}^{n} R_i$ where R_i is a domain if and only if $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$ and Σ is finite. If so, then $R_i = R/\mathfrak{p}_i$ with $\{\mathfrak{p}_1, \dots, \mathfrak{p}_n\} = \Sigma$.

If $R_{\mathfrak{m}}$ is a domain for all maximal ideals $\mathfrak{m}$, is R necessarily a domain?

Exercise (13.59) . — Let R be a ring, M a module. Assume that there are only finitely many maximal ideals $\mathfrak{m}_i$ with $M_{\mathfrak{m}_i} \neq 0$. Show that the canonical map $\alpha\colon M \to \prod M_{\mathfrak{m}_i}$ is bijective if and only if $(M_{\mathfrak{m}_i})_{\mathfrak{m}_j} = 0$ whenever $i \neq j$.

Exercise (13.60) . — Let R be a ring, R' a flat algebra, $\mathfrak{p}'$ a prime in R', and $\mathfrak{p}$ its contraction in R. Prove that $R'_{\mathfrak{p}'}$ is a faithfully flat $R_{\mathfrak{p}}$-algebra.

Exercise (13.61) . — Let R be an absolutely flat ring, $\mathfrak{p}$ a prime. Show $\mathfrak{p}$ is maximal, $R_{\mathfrak{p}}$ is a field, and R is reduced,

Exercise (13.62) . — Given n, prove an R-module P is locally free of rank n if and only if P is finitely generated and $P_{\mathfrak{m}} \simeq R_{\mathfrak{m}}^n$ holds at each maximal ideal $\mathfrak{m}$.

Exercise (13.63) . — Let A be a semilocal ring, P a locally free module of rank n. Show that P is free of rank n.

Exercise (13.64) . — Let R be a ring, M a finitely presented module, $n \geq 0$. Show that M is locally free of rank n if and only if $F_{n-1}(M) = \langle 0 \rangle$ and $F_n(M) = R$.

14. Cohen–Seidenberg Theory

Cohen–Seidenberg Theory relates the prime ideals in a ring to those in an integral extension. We prove each prime has at least one prime lying over it — that is, contracting to it. The overprime can be taken to contain any ideal that contracts to an ideal contained in the given prime; this stronger statement is known as the Going-up Theorem. Further, one prime is maximal if and only if the other is, and two overprimes cannot be nested. On the other hand, the Going-down Theorem asserts that, given nested primes in the subring and a prime lying over the larger, there is a subprime lying over the smaller, either if the subring is normal, the overring is a domain, and the extension is ingeral, or if simply the extension is flat.

A. Text

Lemma (14.1). — *Let R'/R be an integral extension of domains. Then R' is a field if and only if R is.*

Proof: First, suppose R' is a field. Let $x \in R$ be nonzero. Then $1/x \in R'$, so satisfies an equation of integral dependence:

$$(1/x)^n + a_1(1/x)^{n-1} + \cdots + a_n = 0$$

with $n \geq 1$ and $a_i \in R$. Multiplying the equation by x^{n-1}, we obtain

$$1/x = -(a_1 + a_{n-2}x + \cdots + a_n x^{n-1}) \in R.$$

Conversely, suppose R is a field. Let $y \in R'$ be nonzero. Then y satisfies an equation of integral dependence

$$y^n + a_1 y^{n-1} + \cdots + a_{n-1}y + a_n = 0$$

with $n \geq 1$ and $a_i \in R$. Rewriting the equation, we obtain

$$y(y^{n-1} + \cdots + a_{n-1}) = -a_n.$$

Take n minimal. Then $a_n \neq 0$ as R' is a domain. So dividing by $-a_n y$, we obtain

$$1/y = (-1/a_n)(y^{n-1} + \cdots + a_{n-1}) \in R'. \qquad \square$$

Definition (14.2). — Let R be a ring, R' an R-algebra, $\mathfrak{p}$ a prime of R, and $\mathfrak{p}'$ a prime of R'. We say $\mathfrak{p}'$ **lies over** $\mathfrak{p}$ if $\mathfrak{p}'$ contracts to $\mathfrak{p}$; that is, $\mathfrak{p}'^c = \mathfrak{p}$.

Theorem (14.3). — *Let R'/R be an integral extension of rings, $\mathfrak{p}$ a prime of R. Let $\mathfrak{p}' \subset \mathfrak{q}'$ be nested primes of R', and $\mathfrak{a}'$ an arbitrary ideal of R'.*

(1) (Maximality) *Suppose $\mathfrak{p}'$ lies over $\mathfrak{p}$. Then $\mathfrak{p}'$ is maximal if and only if $\mathfrak{p}$ is.*
(2) (Incomparability) *Suppose both $\mathfrak{p}'$ and $\mathfrak{q}'$ lie over $\mathfrak{p}$. Then $\mathfrak{p}' = \mathfrak{q}'$.*
(3) (Lying over) *Then there is a prime $\mathfrak{r}'$ of R' lying over $\mathfrak{p}$.*
(4) (Going-up) *Suppose $\mathfrak{a}' \cap R \subset \mathfrak{p}$. Then in* (3) *we can take $\mathfrak{r}'$ to contain $\mathfrak{a}'$.*

Proof: Assertion (1) follows from (**14.1**) applied to the extension $R/\mathfrak{p} \hookrightarrow R'/\mathfrak{p}'$, which is integral as $R \hookrightarrow R'$ is, since, if $y \in R'$ satisfies $y^n + a_1 y^{n-1} + \cdots + a_n = 0$, then reduction modulo $\mathfrak{p}'$ yields an equation of integral dependence over $R/\mathfrak{p}$.

To prove (2), localize at $R - \mathfrak{p}$, and form this commutative diagram:

$$\begin{array}{ccc} R' & \longrightarrow & R'_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ R & \longrightarrow & R_{\mathfrak{p}} \end{array}$$

Here $R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$ is injective by **(12.12)**(1)(b), and it's integral by **(11.29)**.

Here $\mathfrak{p}'R'_{\mathfrak{p}}$ and $\mathfrak{q}'R'_{\mathfrak{p}}$ are nested primes of $R'_{\mathfrak{p}}$ by **(11.12)**(2). By the same token, both lie over $\mathfrak{p}R_{\mathfrak{p}}$, because both their contractions in $R_{\mathfrak{p}}$ contract to $\mathfrak{p}$ in R. Thus we may replace R by $R_{\mathfrak{p}}$ and R' by $R'_{\mathfrak{p}}$, and so assume R is local with $\mathfrak{p}$ as maximal ideal by **(11.14)**. Then $\mathfrak{p}'$ is maximal by (1); whence, $\mathfrak{p}' = \mathfrak{q}'$.

To prove (3), again we may replace R by $R_{\mathfrak{p}}$ and R' by $R'_{\mathfrak{p}}$: if $\mathfrak{r}''$ is a prime ideal of $R'_{\mathfrak{p}}$ lying over $\mathfrak{p}R_{\mathfrak{p}}$, then the contraction $\mathfrak{r}'$ of $\mathfrak{r}''$ in R' lies over $\mathfrak{p}$. So we may assume R is local with $\mathfrak{p}$ as unique maximal ideal. Now, R' has a maximal ideal $\mathfrak{r}'$ by **(2.21)**; further, $\mathfrak{r}'$ contracts to a maximal ideal $\mathfrak{r}$ of R by (1). Thus $\mathfrak{r} = \mathfrak{p}$.

Finally, (4) follows from (3) applied to the extension $R/(\mathfrak{a}' \cap R) \hookrightarrow R'/\mathfrak{a}'$. □

Lemma (14.4). — *Let R'/R be an extension of rings, X a variable, and $F \in R[X]$ a monic polynomial. Assume $F = GH$ with $G, H \in R'[X]$ and G monic.*

(1) *Then there's an extension R'' of R with $F(X) = \prod_{i=1}^{d}(X - x_i)$ in $R''[X]$. Moreover, R'' is a free R-module of rank $d!$ where $d := \deg(F)$.*

(2) *Then H is monic, and the coefficients of G and H are integral over R.*

Proof: For (1), set $R_1 := R'[X]/\langle F\rangle$. Let x_1 be the residue of X. As F is monic, $1, x_1, \ldots, x_1^{d-1}$ form a free basis of R_1 over R by **(10.15)**; note $R_1 \supset R$. Now, $F(x_1) = 0$; so $F = (X - x_1)F_1$ with $F_1 \in R_1[X]$ by **(1.19)**; note F_1 is monic and $\deg(F_1) = d - 1$. Induction on d yields an extension R'' of R_1 free of degree $(d-1)!$ with $F_1 = \prod_{i=2}^{d}(X - x_i)$. Then R'' is free over R of degree $d!$ by **(10.16)**. Thus (1) holds.

In (2), G is monic. So the leading coefficient of F is equal to that of H. But F is monic. Thus H is monic too.

Next, (1) yields an extension R'' of R' with $G(X) = \prod(X - x_i)$ in $R''[X]$, and an extension R''' of R'' with $H(X) = \prod(X - y_j)$ in $R'''[X]$. The x_i and y_j are integral over R as they are roots of F. But the coefficients of G and H are polynomials in the x_i and y_j; so they too are integral over R owing to **(10.20)**. □

Proposition (14.5). — *Let R be a normal domain, $K := \mathrm{Frac}(R)$, and L/K a field extension. Let $y \in L$ be integral over R, and $F \in K[X]$ its monic minimal polynomial. Then $F \in R[X]$, and so $F(y) = 0$ is an equation of integral dependence.*

Proof: Since y is integral, there is a monic polynomial $G \in R[X]$ with $G(y) = 0$. Write $G = FH$ with $H \in K[X]$. Then by **(14.4)**(2) the coefficients of F are integral over R, so in R since R is normal. □

Theorem (14.6) (Going-down for integral extensions). — *Let R'/R be an integral extension of domains with R normal, $\mathfrak{p} \subsetneqq \mathfrak{q}$ nested primes of R, and $\mathfrak{q}'$ a prime of R' lying over $\mathfrak{q}$. Then there is a prime $\mathfrak{p}'$ lying over $\mathfrak{p}$ and contained in $\mathfrak{q}'$.*

Proof: First, let's show $\mathfrak{p}R'_{\mathfrak{q}'} \cap R = \mathfrak{p}$. Given $y \in \mathfrak{p}R'_{\mathfrak{q}'} \cap R$ with $y \notin \mathfrak{p}$, say $y = x/s$ with $x \in \mathfrak{p}R'$ and $s \in R' - \mathfrak{q}'$. Say $x = \sum_{i=1}^{m} y_i x_i$ with $y_i \in \mathfrak{p}$ and $x_i \in R'$, and set $R'' := R[x_1, \ldots, x_m]$. Then R'' is module finite by **(10.18)** and $xR'' \subset \mathfrak{p}R''$. Let

$F(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be the characteristic polynomial of $\mu_x\colon R'' \to R''$. Then $a_i \in \mathfrak{p}^i \subset \mathfrak{p}$ by (**10.1**), and $F(x) = 0$ by (**10.2**).

Set $K := \operatorname{Frac}(R)$. Say $F = GH$ with $G, H \in K[X]$ monic. By (**14.4**) the coefficients of G, H lie in R as R is normal. Further, $F \equiv X^n \pmod{\mathfrak{p}}$. So $G \equiv X^r \pmod{\mathfrak{p}}$ and $H \equiv X^{n-r} \pmod{\mathfrak{p}}$ for some r by unique factorization in $\operatorname{Frac}(R/\mathfrak{p})[X]$. Hence G and H have all nonleading coefficients in $\mathfrak{p}$. Replace F by a monic factor of minimal degree. Then F is the minimal polynomial of x over K.

Recall $s = x/y$. So s satisfies the equation

$$s^n + b_1s^{n-1} + \cdots + b_n = 0 \quad \text{with} \quad b_i := a_i/y^i \in K. \qquad \textbf{(14.6.1)}$$

Conversely, any such equation yields one of the same degree for x as $y \in R \subset K$. So (**14.6.1**) is the minimal polynomial of s over K. So all b_i are in R by (**14.5**).

Recall $y \notin \mathfrak{p}$. Then $b_i \in \mathfrak{p}$ as $a_i = b_iy^i \in \mathfrak{p}$. So $s^n \in \mathfrak{p}R' \subset \mathfrak{q}R' \subset \mathfrak{q}'$. So $s \in \mathfrak{q}'$, a contradiction. Hence $y \in \mathfrak{p}$. Thus $\mathfrak{p}R'_{\mathfrak{q}'} \cap R \subset \mathfrak{p}$. But the opposite inclusion holds trivially. Thus $\mathfrak{p}R'_{\mathfrak{q}'} \cap R = \mathfrak{p}$.

Hence, there is a prime $\mathfrak{p}''$ of $R'_{\mathfrak{q}'}$ with $\mathfrak{p}'' \cap R = \mathfrak{p}$ by (**3.10**)(2). Then $\mathfrak{p}''$ lies in $\mathfrak{q}'R'_{\mathfrak{q}'}$ as it is the only maximal ideal. Set $\mathfrak{p}' := \mathfrak{p}'' \cap R'$. Then $\mathfrak{p}' \cap R = \mathfrak{p}$, and $\mathfrak{p}' \subset \mathfrak{q}'$ by (**11.12**)(2), as desired. □

Lemma (14.7). — *Always, a minimal prime consists entirely of zerodivisors.*

Proof: Let R be the ring, $\mathfrak{p}$ the minimal prime. Then $R_\mathfrak{p}$ has only one prime $\mathfrak{p}R_\mathfrak{p}$ by (**11.12**)(2). So by the Scheinnullstellensatz (**3.14**), $\mathfrak{p}R_\mathfrak{p}$ consists entirely of nilpotents. Hence, given $x \in \mathfrak{p}$, there is $s \in R - \mathfrak{p}$ with $sx^n = 0$ for some $n \ge 1$. Take n minimal. Then $sx^{n-1} \neq 0$, but $(sx^{n-1})x = 0$. Thus x is a zerodivisor. □

Theorem (14.8) (Going-down for flat modules). — *Let $R \to R'$ be a map of rings, M' a finitely generated R'-module, $\mathfrak{p} \subsetneqq \mathfrak{q}$ nested primes of R, and $\mathfrak{q}'$ a prime of* $\operatorname{Supp}(M')$ *lying over $\mathfrak{q}$. Assume M' is flat over R. Then there is a prime $\mathfrak{p}' \in \operatorname{Supp}(M')$ lying over $\mathfrak{p}$ and contained in $\mathfrak{q}'$.*

Proof: By (**13.48**), the map $\operatorname{Supp}(M'_{\mathfrak{q}'}) \to \operatorname{Spec}(R_\mathfrak{q})$ is surjective. But $\mathfrak{p}R_\mathfrak{q}$ is prime and lies over $\mathfrak{p}$ by (**11.12**)(2). Thus there's $\mathfrak{p}' \in \operatorname{Supp}(M'_{\mathfrak{q}'})$ lying over $\mathfrak{p}$.

However, $M'_{\mathfrak{q}'} = M' \otimes R'_{\mathfrak{q}'}$ by (**12.10**). Also $\operatorname{Spec}(R'_{\mathfrak{q}'})$ is equal to the set of primes contained in $\mathfrak{q}'$ by (**13.25**). So $\operatorname{Supp}(M'_{\mathfrak{q}'}) = \operatorname{Supp}(M') \cap \operatorname{Spec}(R'_{\mathfrak{q}'})$ by (**13.49**). Thus $\mathfrak{p}' \in \operatorname{Supp}(M')$ and $\mathfrak{p}' \subset \mathfrak{q}'$, as desired.

Alternatively, $M' \otimes_R (R/\mathfrak{p})$ is flat over $R/\mathfrak{p}$ by (**9.22**). Also, (**8.27**)(1) yields $M' \otimes_R (R/\mathfrak{p}) = M'/\mathfrak{p}M'$. So replacing R by $R/\mathfrak{p}$ and M' by $M'/\mathfrak{p}M'$, we may assume R is a domain and $\mathfrak{p} = \langle 0 \rangle$. By (**13.5**), $\mathfrak{q}'$ contains a minimal prime $\mathfrak{p}' \in \operatorname{Supp}(M') = \mathbf{V}(\operatorname{Ann}(M'))$. It suffices show that $\mathfrak{p}'$ lies over $\langle 0 \rangle$ in R.

Replace R' by $R'/\operatorname{Ann}(M')$. Then $\mathfrak{p}'$ is a minimal prime R'. Say $m'_1, \ldots, m'_n$ generate M'. Define a map $\alpha\colon R' \to M'^n$ by $\alpha(x') := (x'm'_1, \ldots, x'm'_n)$. Then α is injective as $\operatorname{Ann}(M') = \langle 0 \rangle$.

Given $x \in R$ nonzero, note $\mu_x\colon R \to R$ is injective. Since M' is flat, $\mu_x\colon M' \to M'$ is also injective. So $\mu_x\colon M'^n \to M'^n$ is injective too. Hence $\mu_x\colon R' \to R'$ is injective. So $x \notin \mathfrak{p}'$ by (**14.7**). Thus $\mathfrak{p}'$ lies over $\langle 0 \rangle$ in R, as desired. □

(14.9) (Arbitrary normal rings). — An arbitrary ring R is said to be **normal** if $R_\mathfrak{p}$ is a normal domain for every prime $\mathfrak{p}$. If R is a domain, then this definition recovers that in (**10.19**). Indeed, if R is normal, then $R_\mathfrak{p}$ is too for all $\mathfrak{p}$, as localization commutes with normalization by (**11.32**). Conversely, say R' is the normalization of R. Then $(R'/R)_{\mathfrak{p}} = 0$ for all $\mathfrak{p}$ by **(12.13)**. So $R'/R = 0$ by **(13.8)**.

B. Exercises

Exercise (14.10) . — Let R'/R be an integral extension of rings, $x \in R$. Show: (1) if $x \in R'^{\times}$, then $x \in R^{\times}$ and (2) $\operatorname{rad}(R) = \operatorname{rad}(R') \cap R$.

Exercise (14.11) . — Let $\varphi\colon R \to R'$ be a map of rings. Assume R' is integral over R. Show the map $\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(R') \to \operatorname{Spec}(R)$ is closed.

Exercise (14.12) . — Let R'/R be an integral extension of rings, $\rho\colon R \to \Omega$ a map to an algebraically closed field. Show ρ extends to a map $\rho'\colon R' \to \Omega$. First, assume R'/R is an algebraic extension of fields K/k, and use Zorn's lemma on the set $\mathcal{S}$ of all extensions $\lambda\colon L \to \Omega$ of ρ where $L \subset K$ is a subfield containing k.

Exercise (14.13) (*E. Artin*) . — Form the algebraic closure of a field k as follows:

(1) Let X be a variable, $\mathcal{S}$ the set of all monic $F \in k[X]$, and X_F a variable for each $F \in \mathcal{S}$. Set $P := k[\{X_F\}]$ and $\mathfrak{a} := \langle\{F(X_F)\}\rangle$. Show $1 \notin \mathfrak{a}$. Conclude k has an algebraic extension k_1 in which each $F \in \mathcal{S}$ has a root.

(2) Apply (1) repeatedly to obtain a chain $k_0 := k \subset k_1 \subset k_2 \subset \cdots$ such that every monic polynomial with coefficients in k_n has a root in k_{n+1} for all n. Set $K := \varinjlim k_n$. Show K is an algebraic closure of k.

(3) Using **(14.12)**, show any two algebraic closures K_1, K_2 are k-isomorphic.

Exercise (14.14) . — Let R be a domain, $\overline{R}$ its integral closure, $K := \operatorname{Frac}(R)$. Let L/K be a field extension, $y \in L$ algebraic with monic minimal polynomial $G(X) \in K[X]$. Show that y is integral over R if and only if $G \in \overline{R}[X]$.

Exercise (14.15) . — Let R'/R be an integral extension of rings, $\mathfrak{p}$ a prime of R. Assume R' has just one prime $\mathfrak{p}'$ over $\mathfrak{p}$. Show (1) that $\mathfrak{p}'R'_{\mathfrak{p}}$ is the only maximal ideal of $R'_{\mathfrak{p}}$, (2) that $R'_{\mathfrak{p}'} = R'_{\mathfrak{p}}$, and (3) that $R'_{\mathfrak{p}'}$ is integral over $R_{\mathfrak{p}}$.

Exercise (14.16) . — Let R'/R be an integral extension of rings, $\mathfrak{p} \subset R$ a prime, $\mathfrak{p}', \mathfrak{q}' \subset R'$ two distinct primes lying over $\mathfrak{p}$. Assume R' is a domain, or simply, $R'_{\mathfrak{p}} \subset R'_{\mathfrak{p}'}$. Show that $R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$. Show that, in fact, given $y \in \mathfrak{q}' - \mathfrak{p}'$, then $1/y \in R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$.

Exercise (14.17) . — Let k be a field, and X an indeterminate. Set $R' := k[X]$, and $Y := X^2$, and $R := k[Y]$. Set $\mathfrak{p} := (Y-1)R$ and $\mathfrak{p}' := (X-1)R'$. Is $R'_{\mathfrak{p}'}$ integral over $R_{\mathfrak{p}}$? Treat the case $\operatorname{char}(k) = 2$ separately. Explain.

Exercise (14.18) . — Let R be a ring, G be a finite group acting on R, and $\mathfrak{p}$ a prime of R^G. Let $\mathcal{P}$ denote the set of primes $\mathfrak{P}$ of R whose contraction in R^G is $\mathfrak{p}$. Prove: (1) G acts transitively on $\mathcal{P}$; and (2) $\mathcal{P}$ is nonempty and finite.

Exercise (14.19) . — Let R be a normal domain, K its fraction field, L/K a finite field extension, $\overline{R}$ the integral closure of R in L. Prove that only finitely many primes $\mathfrak{P}$ of $\overline{R}$ lie over a given prime $\mathfrak{p}$ of R as follows.

First, assume L/K is separable, and use **(14.18)**. Next, assume L/K is purely inseparable, and show that $\mathfrak{P}$ is unique; in fact, $\mathfrak{P} = \{x \in \overline{R} \mid x^{p^n} \in \mathfrak{p} \text{ for some } n\}$ where p denotes the characteristic of K. Finally, do the general case.

Exercise (14.20) . — Let R be a ring. For $i = 1, 2$, let R_i be an algebra, $P_i \subset R_i$ a subalgebra. Assume P_1, P_2, R_1, R_2 are R-flat domains. Denote their fraction fields by L_1, L_2, K_1, K_2. Form the following diagram, induced by the inclusions:

$$\begin{array}{ccc} L_1 \otimes_R L_2 & \longrightarrow & K_1 \otimes_R K_2 \\ \Big\uparrow & & \Big\uparrow \beta \\ P_1 \otimes_R P_2 & \xrightarrow{\alpha} & R_1 \otimes_R R_2 \end{array}$$

(1) Show $K_1 \otimes K_2$ is flat over $P_1 \otimes P_2$. (2) Show β is injective.
(3) Given a minimal prime $\mathfrak{p}$ of $R_1 \otimes R_2$, show $\alpha^{-1}\mathfrak{p} = 0$ if $P_1 \otimes P_2$ is a domain.

Exercise (14.21) . — Let R be a reduced ring, Σ the set of minimal primes. Prove that $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ and that $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ for any $\mathfrak{p} \in \Sigma$.

Exercise (14.22) . — Let R be a ring, Σ the set of minimal primes, and K the total quotient ring. Assume Σ is finite. Prove these three conditions are equivalent:

(1) R is reduced.
(2) $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, and $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$.
(3) $K/\mathfrak{p}K = \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p} \in \Sigma$, and $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$.

Exercise (14.23) . — Let A be a reduced local ring with residue field k and finite set Σ of minimal primes. For each $\mathfrak{p} \in \Sigma$, set $K(\mathfrak{p}) := \mathrm{Frac}(A/\mathfrak{p})$. Let P be a finitely generated module. Show that P is free of rank r if and only if $\dim_k(P \otimes_A k) = r$ and $\dim_{K(\mathfrak{p})}(P \otimes_A K(\mathfrak{p})) = r$ for each $\mathfrak{p} \in \Sigma$.

Exercise (14.24) . — Let A be a reduced semilocal ring with a finite set of minimal primes. Let P be a finitely generated A-module, and B an A-algebra such that $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective. For each prime $\mathfrak{q} \subset B$, set $L(\mathfrak{q}) := \mathrm{Frac}(B/\mathfrak{q})$. Given r, assume $\dim((P \otimes_A B) \otimes_B L(\mathfrak{q})) = r$ whenever $\mathfrak{q}$ is either maximal or minimal. Show that P is a free A-module of rank r.

Exercise (14.25) . — Let R be a ring, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ all its minimal primes, and K the total quotient ring. Prove that these three conditions are equivalent:

(1) R is normal.
(2) R is reduced and integrally closed in K.
(3) R is a finite product of normal domains R_i.

Assume the conditions hold. Prove the R_i are equal to the $R/\mathfrak{p}_j$ in some order.

Exercise (14.26) . — Let X be a nonempty compact Hausdorff space, R the ring of $\mathbb{R}$-valued continuous functions on X, and $\widetilde{X} \subset \mathrm{Spec}(R)$ the set of maximal ideals. Give $\widetilde{X}$ the induced topology. For all $x \in X$, set $\mathfrak{m}_x := \{f \in R \mid f(x) = 0\}$. Show:

(1) Given a maximal ideal $\mathfrak{m}$, set $V := \{x \in X \mid f(x) = 0 \text{ for all } f \in \mathfrak{m}\}$. Then $V \neq \emptyset$; otherwise, there's a contradiction. Moreover, $\mathfrak{m} = \mathfrak{m}_x$ for any $x \in V$.
(2) Urysohn's Lemma [15, Thm. 3.1, p. 207] implies $\mathfrak{m}_x \neq \mathfrak{m}_y$ if $x \neq y$..
(3) For any $f \in R$, set $U_f = \{x \in X \mid f(x) \neq 0\}$ and $\overline{U}_f = \{\mathfrak{m} \in \widetilde{X} \mid f \notin \mathfrak{m}\}$. Then $\mathfrak{m}_x \in \widetilde{X}$ for any $x \in X$, and $x \in U_f$ if and only if $\mathfrak{m}_x \in \overline{U}_f$; moreover, the $\overline{U}_f$ and, by Urysohn's Lemma, the U_f form bases of the topologies.
(4) Define $\varphi\colon X \to \widetilde{X}$ by $\varphi(x) = \mathfrak{m}_x$. Then φ is a well-defined homeomorphism.

15. Noether Normalization

The Noether Normalization Lemma describes the basic structure of a finitely generated algebra over a field; namely, given a chain of ideals, there is a polynomial subring over which the algebra is module finite, and the ideals contract to ideals generated by initial segments of variables. After proving this lemma, we derive several versions of the Nullstellensatz. The most famous is Hilbert's; namely, the radical of any ideal is the intersection of all the maximal ideals containing it.

Then we study the (Krull) dimension: the maximal length of any chain of primes. We prove our algebra is catenary; that is, if two chains have the same ends and maximal lengths, then the lengths are the same. Further, if the algebra is a domain, then its dimension is equal to the transcendence degree of its fraction field.

In an appendix, we give a simple direct proof of the Hilbert Nullstellensatz. At the same time, we prove it in significantly greater generality: for Jacobson rings.

A. Text

Lemma (15.1) (Noether Normalization). — *Let k be a field, $R := k[x_1, \ldots, x_n]$ a nonzero finitely generated k-algebra, $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_r$ nested proper ideals of R. Then there are algebraically independent elements $t_1, \ldots, t_\nu \in R$ with $\nu \le n$ such that*

(1) *R is module finite over $P := k[t_1, \ldots t_\nu]$ and*

(2) *for $i = 1, \cdots, r$, there is an h_i such that $\mathfrak{a}_i \cap P = \langle t_1, \ldots, t_{h_i} \rangle$.*

Proof: Let $R' := k[X_1, \ldots, X_n]$ be the polynomial ring, and $\varphi\colon R' \to R$ the k-algebra map with $\varphi X_i := x_i$. Set $\mathfrak{a}'_0 := \operatorname{Ker}\varphi$ and $\mathfrak{a}'_i := \varphi^{-1}\mathfrak{a}_i$ for $i = 1, \cdots, r$. It suffices to prove the lemma for R' and $\mathfrak{a}'_0 \subset \cdots \subset \mathfrak{a}'_r$: if $t'_i \in R'$ and h'_i work here, then $t_i := \varphi t'_{i+h'_0}$ and $h_i := h'_i - h'_0$ work for R and the $\mathfrak{a}_i$, because the t_i are algebraically independent by **(1.17)**(5), and clearly (1), (2), and $\nu \le n$ hold. Thus we may assume the x_i are algebraically independent.

The proof proceeds by induction on r, and shows $\nu := n$ works now.

First, assume $r = 1$ and $\mathfrak{a}_1 = t_1 R$ for some nonzero t_1. Then $t_1 \notin k$ because $\mathfrak{a}_1$ is proper. Suppose we have found $t_2, \ldots, t_n \in R$ so that x_1 is integral over $P := k[t_1, t_2, \ldots, t_n]$ and so that $P[x_1] = R$. Then **(10.18)** yields (1).

Further, by the theory of transcendence bases [**3**, (8.3), p. 526], [**14**, Thm. 1.1, p. 356], the elements $t_1, \ldots, t_n$ are algebraically independent. Now, take $x \in \mathfrak{a}_1 \cap P$. Then $x = t_1 x'$ where $x' \in R \cap \operatorname{Frac}(P)$. Also, $R \cap \operatorname{Frac}(P) = P$, for P is normal by **(10.22)** as P is a polynomial algebra. Hence $\mathfrak{a}_1 \cap P = t_1 P$. Thus (2) holds too.

To find $t_2, \ldots, t_n$, we are going to choose ℓ_i and set $t_i := x_i - x_1^{\ell_i}$. Then clearly $P[x_1] = R$. Now, say $t_1 = \sum a_{(j)} x_1^{j_1} \cdots x_n^{j_n}$ with $(j) := (j_1, \ldots, j_n)$ and $a_{(j)} \in k$. Recall $t_1 \notin k$, and note that x_1 satisfies this equation:

$$\sum a_{(j)} x_1^{j_1} (t_2 + x_1^{\ell_2})^{j_2} \cdots (t_n + x_1^{\ell_n})^{j_n} = t_1.$$

Set $e(j) := j_1 + \ell_2 j_2 + \cdots + \ell_n j_n$. Take $\ell > \max\{j_i\}$ and $\ell_i := \ell^i$. Then the $e(j)$ are distinct. Let $e(j')$ be largest among the $e(j)$ with $a_{(j)} \ne 0$. Then $e(j') > 0$, and the above equation may be rewritten as follows:

$$a_{(j')} x_1^{e(j')} + \textstyle\sum_{e<e(j')} p_e x_1^e = 0$$

where $p_e \in P$. Thus x_1 is integral over P, as desired.

Second, assume $r = 1$ and $\mathfrak{a}_1$ is arbitrary. We may assume $\mathfrak{a}_1 \neq 0$. The proof proceeds by induction on n. The case $n = 1$ follows from the first case (but is simpler) because $k[x_1]$ is a PID. Let $t_1 \in \mathfrak{a}_1$ be nonzero. By the first case, there exist elements $u_2, \ldots, u_n$ such that $t_1, u_2, \ldots u_n$ are algebraically independent and satisfy (1) and (2) with respect to R and $t_1 R$. By induction, there are $t_2, \ldots, t_n$ satisfying (1) and (2) with respect to $k[u_2, \ldots, u_n]$ and $\mathfrak{a}_1 \cap k[u_2, \ldots, u_n]$.

Set $P := k[t_1, \ldots, t_n]$. Since R is module finite over $k[t_1, u_2, \ldots, u_n]$ and the latter is so over P, the former is so over P by **(10.17)**(3). Thus (1) holds, and so $t_1, \ldots, t_n$ are algebraically independent. Further, by assumption,

$$\mathfrak{a}_1 \cap k[t_2, \ldots, t_n] = \langle t_2, \ldots, t_h \rangle$$

for some h. But $t_1 \in \mathfrak{a}_1$. So $\mathfrak{a}_1 \cap P \supset \langle t_1, \ldots, t_h \rangle$.

Conversely, given $x \in \mathfrak{a}_1 \cap P$, say $x = \sum_{i=0}^{d} f_i t_1^i$ with $f_i \in k[t_2, \ldots, t_n]$. Since $t_1 \in \mathfrak{a}_1$, we have $f_0 \in \mathfrak{a}_1 \cap k[t_2, \ldots, t_n]$; so $f_0 \in \langle t_2, \ldots, t_h \rangle$. Hence $x \in \langle t_1, \ldots, t_h \rangle$. Thus $\mathfrak{a}_1 \cap P = \langle t_1, \ldots, t_h \rangle$. Thus (2) holds for $r = 1$.

Finally, assume the lemma holds for $r - 1$. Let $u_1, \ldots, u_n \in R$ be algebraically independent elements satisfying (1) and (2) for the sequence $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_{r-1}$, and set $h := h_{r-1}$. By the second case, there exist elements $t_{h+1}, \ldots, t_n$ satisfying (1) and (2) for $k[u_{h+1}, \ldots, u_n]$ and $\mathfrak{a}_r \cap k[u_{h+1}, \ldots, u_n]$. Then, for some h_r,

$$\mathfrak{a}_r \cap k[t_{h+1}, \ldots, t_n] = \langle t_{h+1}, \ldots, t_{h_r} \rangle.$$

Set $t_i := u_i$ for $1 \leq i \leq h$. Set $P := k[t_1, \ldots, t_n]$. Then, by assumption, R is module finite over $k[u_1, \ldots, u_n]$, and $k[u_1, \ldots, u_n]$ is so over P; thus R is so over P by **(10.17)**(3). Thus (1) holds, and $t_1, \ldots, t_n$ are algebraically independent over k.

Fix i with $1 \leq i \leq r$. Set $m := h_i$. Then $t_1, \ldots, t_m \in \mathfrak{a}_i$. Given $x \in \mathfrak{a}_i \cap P$, say $x = \sum f_{(v)} t_1^{v_1} \cdots t_m^{v_m}$ with $(v) = (v_1, \ldots, v_m)$ and $f_{(v)} \in k[t_{m+1}, \ldots, t_n]$. Then $f_{(0)}$ lies in $\mathfrak{a}_i \cap k[t_{m+1}, \ldots, t_n]$. Let's see the latter intersection is equal to $\langle 0 \rangle$. It is so if $i \leq r - 1$ because it lies in $\mathfrak{a}_i \cap k[u_{m+1}, \ldots, u_n]$, which is equal to $\langle 0 \rangle$. Further, if $i = r$, then, by assumption, $\mathfrak{a}_i \cap k[t_{m+1}, \ldots, t_n] = \langle t_{m+1}, \ldots, t_m \rangle = 0$.

Thus $f_{(0)} = 0$. Hence $x \in \langle t_1, \ldots, t_{h_i} \rangle$. Thus $\mathfrak{a}_i \cap P \subset \langle t_1, \ldots, t_{h_i} \rangle$. So the two are equal. Thus (2) holds, and the proof is complete. □

Remark (15.2) (Noether Normalization over an infinite field). — In **(15.1)**, let's assume k is infinite, and let's see we can take $t_1, \ldots, t_\nu$ to be linear combinations of $x_1, \ldots, x_n$ so that (1) still holds, although (2) need not.

To prove (1), induct on n. If $n = 0$, then (1) is trivial.

So assume $n \geq 1$. If $x_1, \ldots, x_n$ are algebraically independent over k, then (1) holds with $\nu := n$ and $t_i := x_i$ for all i.

So assume there's a nonzero $F \in k[X_1, \ldots, X_n]$ with $F(x_1, \ldots, x_n) = 0$. Say $F = F_d + \cdots + F_0$ where $F_d \neq 0$ and where each F_i is **homogeneous of degree** i; that is, F_i is a linear combination of monomials of degree i. Then $d > 0$. But k is infinite. So by **(3.28)**(1) with $\mathcal{S} = k^\times$, there are $a_i \in k^\times$ with $F_d(a_1, a_2, \ldots, a_n) \neq 0$. Since F_d is homogeneous, we may replace a_i by a_i/a_1. Set $a := F_d(1, a_2, \ldots, a_n)$.

Set $y_i := x_i - a_i x_1$ for $2 \leq i \leq n$, and set $R' := k[y_2, \ldots, y_n]$. Then

$$\begin{aligned} 0 = F(x_1, x_2, \ldots, x_n) &= F(x_1,\, y_2 + a_2 x_1, \ldots, y_n + a_n x_1) \\ &= a x_1^d + A_1 x_1^{d-1} + \cdots + A_d \quad \text{with } 0 \neq a \in k \text{ and each } A_i \in R'. \end{aligned}$$

So x_1 is integral over R'. But $R'[x_1] = R$. So R is module finite over R' by **(10.14)**.

By induction, there are linear combinations $t_1, \ldots, t_\nu$ of $y_2, \ldots, y_n$ such that R' is module finite over $P := k[t_1, \ldots, t_\nu]$. So R is module finite over P by **(10.17)**(3). And plainly, the t_i are linear combinations of the x_i. Thus (1) holds.

Here's a simple example, due to P. Etingof, where (1) holds, but (2) doesn't. Let x be transcendental over k. Set $\mathfrak{a} := \langle x^2 \rangle$. Then any "linear combination" t of x is of the form $t = ax$. As (1) holds, $a \neq 0$. So $t \notin \mathfrak{a}$. Thus (2) doesn't hold.

Proposition (15.3). — *Let R be a domain, R' an algebra-finite extension. Then there are a nonzero $f \in R$ and algebraically independent $x_1, \ldots, x_n$ in R' such that R'_f is a module-finite and integral extension of $R[x_1, \ldots, x_n]_f$.*

Proof: Set $K := \operatorname{Frac}(R)$. Then $K = S_0^{-1}R$. Say $R' = R[z_1, \ldots, z_m]$. Then $S_0^{-1}R' = K[z_1/1, \ldots, z_m/1]$. So by **(15.1)** there are $y_1, \ldots, y_n \in S_0^{-1}R'$ that are algebraically independent over K and such that $S_0^{-1}R'$ is module finite over $K[y_1, \ldots, y_n]$. Say $y_i = x_i/g$ with $x_i \in R'$ and $g \in S_0$.

Suppose $\sum_{\mathbf{p}} a_{\mathbf{p}} M_{\mathbf{p}}(x_1, \ldots, x_n) = 0$ in R' with $a_{\mathbf{p}} \in R$ and $M_{\mathbf{p}}$ a monomial. Set $d_{\mathbf{p}} := \deg M_{\mathbf{p}}$. Then $\sum_{\mathbf{p}} a_{\mathbf{p}} g^{d_{\mathbf{p}}} M_{\mathbf{p}}(y_1, \ldots, y_n) = 0$ in $S_0^{-1}R'$. However, $y_1, \ldots, y_n$ are algebraically independent over K. So $a_{\mathbf{p}} g^{d_{\mathbf{p}}} = 0$. So $a_{\mathbf{p}} = 0$. Thus $x_1, \ldots, x_n$ are algebraically independent over R.

Each $z_j/1 \in S_0^{-1}R'$ is integral over $K[y_1, \ldots, y_n]$ by **(10.18)**. Say

$$(z_j/1)^{n_j} + A_{j,1}(z_j/1)^{n_j-1} + \cdots + A_{j,n_j} = 0 \quad \text{with} \quad A_{j,k} \in K[y_1, \ldots, y_n].$$

But $K = S_0^{-1}R$ and $y_i = x_i/g$. So $A_{j,k} = B_{j,k}/h$ for some $B_{j,k} \in R[x_1, \ldots, x_n]$ and $h \in S_0$. So $h(z_j/1)^{n_j} + (B_{j,1}/1)(z_j/1)^{n_j-1} + \cdots + (B_{j,n_j}/1) = 0$ in $S_0^{-1}R'$. So there's $h' \in S_0$ with $h'\big(hz_j^{n_j} + B_{j,1}z_j^{n_j-1} + \cdots + B_{j,n_j}\big) = 0$ in R'.

Set $f := h'h$. Then $R[x_1, \ldots, x_n]_f \subset R'_f$ by **(12.12)**(5)(b). Further, in R'_f,

$$(z_j/1)^{n_j} + (h'B_{j,1}/f)(z_j/1)^{n_j-1} + \cdots + (h'B_{j,n_j}/f) = 0.$$

But $R' = R[z_1, \ldots, z_m]$, so $R'_f = R[z_1, \ldots, z_m]_f$. And double inclusion shows $R[z_1, \ldots, z_m]_f = R_f[z_1/1, \ldots, z_m/1]$. Thus **(10.18)** implies R'_f is module finite and integral over $R[x_1, \ldots, x_n]_f$. □

Theorem (15.4) (Zariski Nullstellensatz). — *Let k be a field, R an algebra-finite extension. Assume R is a field. Then R/k is a finite algebraic extension.*

Proof: By the Noether Normalization Lemma **(15.1)**(1), R is module finite over a polynomial subring $P := k[t_1, \ldots, t_\nu]$. Then R/P is integral by **(10.18)**. As R is a field, so is P by **(14.1)**. So $\nu = 0$. So $P = k$. Thus R/k is finite, as asserted.

Alternatively, here's a short proof, not using **(15.1)**. Say $R = k[x_1, \ldots, x_n]$. Set $P := k[x_1]$ and $K := \operatorname{Frac}(P)$. Then $R = K[x_2, \ldots, x_n]$. By induction on n, assume R/K is finite. Suppose x_1 is transcendental over k, so P is a polynomial ring.

Note $R = P[x_2, \ldots, x_n]$. Hence **(11.31)** yields $f \in P$ with R_f/P_f module finite, so integral by **(10.18)**. But $R_f = R$. Thus P_f is a field by **(14.1)**. So $f \notin k$.

Set $g := 1 + f$. Then $1/g \in P_f$. So $1/g = h/f^r$ for some $h \in P$ and $r \geq 1$. Then $f^r = gh$. But f and g are relatively prime, a contradiction. Thus x_1 is algebraic over k. Hence $P = K$, and K/k is finite. But R/K is finite. Thus R/k is too. □

Corollary (15.5). — *Let k be a field, $R := k[x_1, \ldots, x_n]$ an algebra-finite extension, and $\mathfrak{m}$ a maximal ideal of R. Assume k is algebraically closed. Then there are $a_1, \ldots, a_n \in k$ such that $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.*

Proof: Set $K := R/\mathfrak{m}$. Then K is a finite extension field of k by the Zariski Nullstellensatz (**15.4**). But k is algebraically closed. Hence $k = K$. Let $a_i \in k$ be the residue of x_i, and set $\mathfrak{n} := \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Then $\mathfrak{n} \subset \mathfrak{m}$.

Let $R' := k[X_1, \ldots, X_n]$ be the polynomial ring, and $\varphi\colon R' \to R$ the k-algebra map with $\varphi X_i := x_i$. Set $\mathfrak{n}' := \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Then $\varphi(\mathfrak{n}') = \mathfrak{n}$. But $\mathfrak{n}'$ is maximal by (**2.14**). So $\mathfrak{n}$ is maximal. Hence $\mathfrak{n} = \mathfrak{m}$, as desired. □

Corollary (15.6). — *Let k be any field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, and $\mathfrak{m}$ a maximal ideal of P. Then $\mathfrak{m}$ is generated by n elements.*

Proof: Set $K := P/\mathfrak{m}$. Then K is a field. So K/k is finite by (**15.4**).

Induct on n. If $n = 0$, then $\mathfrak{m} = 0$. Assume $n \geq 1$. Set $R := k[X_1]$ and $\mathfrak{p} := \mathfrak{m} \cap R$. Then $\mathfrak{p} = \langle F_1 \rangle$ for some $F_1 \in R$ as R is a PID. Set $k_1 := R/\mathfrak{p}$. Then k_1 is isomorphic to the image of R in K. But K is a finite-dimensional k-vector space. So k_1 is too. So k_1/k is an integral extension by (**10.18**). Since k is a field, so is k_1 by (**14.1**).

Note $P/\mathfrak{p}P = k_1[X_2, \ldots, X_n]$ by (**1.16**). But $\mathfrak{m}/\mathfrak{p}$ is a maximal ideal. So by induction $\mathfrak{m}/\mathfrak{p}$ is generated by $n-1$ elements, say the residues of $F_2, \ldots, F_n \in \mathfrak{m}$. Then $\mathfrak{m} = \langle F_1, \ldots, F_n \rangle$, as desired. □

Theorem (15.7) (Hilbert Nullstellensatz). — *Let k be a field, and R a finitely generated k-algebra. Let $\mathfrak{a}$ be a proper ideal of R. Then*

$$\sqrt{\mathfrak{a}} = \textstyle\bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}$$

where $\mathfrak{m}$ runs through all maximal ideals containing $\mathfrak{a}$.

Proof: We may assume $\mathfrak{a} = 0$ by replacing R by $R/\mathfrak{a}$. Clearly $\sqrt{0} \subset \bigcap \mathfrak{m}$. Conversely, take $f \notin \sqrt{0}$. Then $R_f \neq 0$ by (**11.19**). So R_f has a maximal ideal $\mathfrak{n}$ by (**2.21**). Let $\mathfrak{m}$ be its contraction in R. Now, R is a finitely generated k-algebra by hypothesis; hence, R_f is one too owing to (**11.7**). Therefore, by the Zariski Nullstellensatz (**15.4**), $R_f/\mathfrak{n}$ is a finite extension field of k.

Set $K := R/\mathfrak{m}$. By construction, K is a k-subalgebra of $R_f/\mathfrak{n}$. Therefore, K is a finite-dimensional k-vector space. So K/k is an integral extension by (**10.18**). Since k is a field, so is K by (**14.1**). Thus $\mathfrak{m}$ is maximal. But $f/1$ is a unit in R_f; so $f/1 \notin \mathfrak{n}$. Hence $f \notin \mathfrak{m}$. So $f \notin \bigcap \mathfrak{m}$. Thus $\sqrt{0} = \bigcap \mathfrak{m}$. □

Lemma (15.8). — *Let k be a field, R a finitely generated k-algebra. Assume R is a domain. Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes. Set $K := \operatorname{Frac}(R)$ and $d := \operatorname{tr.deg}_k K$. Then $r \leq d$, with equality if and only if the chain is maximal in R.*

Proof: By the Noether Normalization Lemma (**15.1**), R is module finite over a polynomial subring $P := k[t_1, \ldots, t_\nu]$ such that $\mathfrak{p}_i \cap P = \langle t_1, \ldots, t_{h_i} \rangle$ for suitable h_i. Set $L := \operatorname{Frac}(P)$. Then $\nu = \operatorname{tr.deg}_k L$. But R/P is an integral extension by (**10.18**). So K/L is algebraic. Hence $\nu = d$. Now, Incomparability (**14.3**)(2) yields $h_i < h_{i+1}$ for all i. Hence $r \leq h_r$. But $h_r \leq \nu$ and $\nu = d$. Thus $r \leq d$.

If $r = d$, then r is maximal, as it was just proved that no chain can be longer. Conversely, assume r is maximal. Then $\mathfrak{p}_0 = \langle 0 \rangle$ since R is a domain. So $h_0 = 0$. Further, $\mathfrak{p}_r$ is maximal since $\mathfrak{p}_r$ is contained in some maximal ideal, which is prime. So $\mathfrak{p}_r \cap P$ is maximal by Maximality (**14.3**)(1). Hence $h_r = \nu$.

Suppose there is an i such that $h_i + 1 < h_{i+1}$. Then

$$(\mathfrak{p}_i \cap P) \subsetneqq \langle t_1, \ldots, t_{h_i+1} \rangle \subsetneqq (\mathfrak{p}_{i+1} \cap P).$$

But $P/(\mathfrak{p}_i \cap P)$ is, by **(1.17)**(3), equal to $k[t_{h_i+1}, \dots, t_\nu]$; the latter is a polynomial ring, so normal by **(10.22)**(1). Also, the extension $P/(\mathfrak{p}_i \cap P) \hookrightarrow R/\mathfrak{p}_i$ is integral as $P \subset R$ is. Hence, the Going-down Theorem **(14.6)** yields a prime $\mathfrak{p}$ with $\mathfrak{p}_i \subset \mathfrak{p} \subset \mathfrak{p}_{i+1}$ and $\mathfrak{p} \cap P = \langle t_1, \dots, t_{h_i+1} \rangle$. Then $\mathfrak{p}_i \subsetneqq \mathfrak{p} \subsetneqq \mathfrak{p}_{i+1}$, contradicting the maximality of r. Thus $h_i + 1 = h_{i+1}$ for all i. But $h_0 = 0$. Hence $r = h_r$. But $h_r = \nu$ and $\nu = d$. Thus $r = d$, as desired. □

(15.9) (Krull Dimension). — Given a ring R, its (Krull) **dimension** $\dim(R)$ is the supremum of the **lengths** r of all strictly ascending chains of primes:

$$\dim(R) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \text{ in } R \,\}.$$

For example, if R is a field, then $\dim(R) = 0$; more generally, $\dim(R) = 0$ if and only if every minimal prime is maximal. If R is a PID, but not a field, then $\dim(R) = 1$, as every nonzero prime is maximal by **(2.17)**.

Theorem (15.10). — *Let k be a field, R a finitely generated k-algebra. If R is a domain, then* $\dim(R) = \operatorname{tr.deg}_k(\operatorname{Frac}(R))$.

Proof: The assertion is an immediate consequence of **(15.8)**. □

Example (15.11). — Let k be a field, $P := k[X_1, \dots, X_n]$, the polynomial k-algebra in n variables. Then the transcendence degree of $k(X_1, \dots, X_n)$ over k is equal to n. So **(15.10)** yields $\dim(P) = n$.

Let $P' := k[Y_1, \dots, Y_m]$ be the polynomial k-algebra in m variables. Then **(8.18)** yields $P \otimes_k P' = k[X_1, \dots, X_n, Y_1, \dots, Y_m]$. So $\dim(P \otimes_k P') = m + n$.

Theorem (15.12). — *Let k be a field, R a finitely generated k-algebra, $\mathfrak{p}$ a prime ideal, and $\mathfrak{m}$ a maximal ideal. Suppose R is a domain. Then*

$$\dim(R_\mathfrak{p}) + \dim(R/\mathfrak{p}) = \dim(R) \quad \textit{and} \quad \dim(R_\mathfrak{m}) = \dim(R).$$

Proof: A chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in R gives rise to a pair of chains of primes, one in $R_\mathfrak{p}$ and one in $R/\mathfrak{p}$,

$$\mathfrak{p}_0 R_\mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p} R_\mathfrak{p} \quad \text{and} \quad 0 = \mathfrak{p}/\mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p}_r/\mathfrak{p},$$

owing to **(11.12)**(2) and to **(1.9)** and **(2.7)**; conversely, every such pair arises from a unique chain in R through $\mathfrak{p}$. But by **(15.8)**, every maximal chain through $\mathfrak{p}$ is of length $\dim(R)$. The first equation follows.

Clearly $\dim(R/\mathfrak{m}) = 0$, and so $\dim(R_\mathfrak{m}) = \dim(R)$. □

(15.13) (Catenary modules and rings). — Let R be a ring, M a module. We call M **catenary** if, given any two nested primes containing $\operatorname{Ann}(M)$, every maximal chain of primes between the two primes has the same finite length; here, **maximal** means that the chain is not a proper subchain of a longer chain of primes between tbe two given primes. We call R **catenary** if R is catenary as an R-module.

Note that M is catenary if and only if the ring $R/\operatorname{Ann}(M)$ is catenary.

Assume M is catenary. Then so is any quotient N of M as $\operatorname{Ann}(M) \subset \operatorname{Ann}(N)$. Further, so is the localization $S^{-1}M$ for any multiplicative set S, for this reason. As $R/\operatorname{Ann}(M)$ is catenary, so is $S^{-1}R/S^{-1}\operatorname{Ann}(M)$ owing to **(11.12)**(2). But plainly $S^{-1}\operatorname{Ann}(M) \subset \operatorname{Ann}(S^{-1}M)$. Thus $S^{-1}R/\operatorname{Ann}(S^{-1}M)$ is catenary.

Theorem (15.14). — *Over a field, a finitely generated algebra is catenary.*

Proof: Let R be the algebra, and $\mathfrak{q} \subset \mathfrak{p}$ two nested primes. Replacing R by $R/\mathfrak{q}$, we may assume R is a domain. Then the proof of **(15.12)** shows that any maximal chain of primes $\langle 0\rangle \subsetneqq \cdots \subsetneqq \mathfrak{p}$ is of length $\dim(R) - \dim(R/\mathfrak{p})$. □

B. Exercises

Exercise (15.15) . — Let $k := \mathbb{F}_q$ be the finite field with q elements, and $k[X, Y]$ the polynomial ring. Set $F := X^qY - XY^q$ and $R := k[X, Y]\big/\langle F\rangle$. Let $x, y \in R$ be the residues of X, Y. For every $a \in k$, show that R is not module finite over $P := k[y - ax]$. (Thus, in **(15.1)**, no k-linear combination works.) First, take $a = 0$.

Exercise (15.16) . — Let k be a field, and X, Y, Z variables. Set

$$R := k[X, Y, Z]\big/\langle X^2 - Y^3 - 1,\, XZ - 1\rangle,$$

and let $x, y, z \in R$ be the residues of X, Y, Z. Fix $a, b \in k$, and set $t := x + ay + bz$ and $P := k[t]$. Show that x and y are integral over P for any a, b and that z is integral over P if and only if $b \neq 0$.

Exercise (15.17) . — Let R'/R be a ring extension, X a variable, $\overline{R}$ the integral closure of R in R'. Show $\overline{R}[X]$ is the integral closure $\overline{R[X]}$ of $R[X]$ in $R'[X]$.

Exercise (15.18) . — Let R be a domain, $\varphi\colon R \hookrightarrow R'$ an algebra-finite extension. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Find a nonzero $f \in R$ such that $\varphi^*(\operatorname{Spec}(R')) \supset \mathbf{D}(f)$.

Exercise (15.19) . — Let R be a domain, R' an algebra-finite extension. Find a nonzero $f \in R$ such that, given an algebraically closed field Ω and a ring map $\varphi\colon R \to \Omega$ with $\varphi(f) \neq 0$, there's an extension of φ to R'.

Exercise (15.20) . — Let R be a domain, R' an algebra-finite extension. Assume $\operatorname{rad}(R) = \langle 0\rangle$. Prove $\operatorname{rad}(R') = \operatorname{nil}(R')$. First do the case where R' is a domain by applying **(15.19)** with $R' := R'_g$ for any given nonzero $g \in R'$.

Exercise (15.21) . — Let k be a field, K an algebraically closed extension field. Let $P := k[X_1, \ldots, X_n]$ be the polynomial ring, and $F, F_1, \ldots, F_r \in P$. Assume F vanishes at every zero in K^n of $F_1, \ldots, F_r$; that is, if $(\mathbf{a}) := (a_1, \ldots, a_n) \in K^n$ and $F_1(\mathbf{a}) = 0, \ldots, F_r(\mathbf{a}) = 0$, then $F(\mathbf{a}) = 0$ too. Prove that there are polynomials $G_1, \ldots, G_r \in P$ and an integer N such that $F^N = G_1F_1 + \cdots + G_rF_r$.

Exercise (15.22) . — (1) Find an example where **(15.21)** fails if K isn't required to be algebraically closed, say with $K := k := \mathbb{R}$ and $n := 1$ and $r := 1$.

(2) Find an example where **(15.21)** fails if the G_i are all required to be in k, say with $K := k := \mathbb{C}$ and $n := 1$ and $r := 2$.

Exercise (15.23) . — Let k be an algebraically closed field, $P := k[X_1, \ldots, X_n]$ the polynomial ring in n variables X_i, and $V \subset k^n$ the set of common zeroes of a set of polynomials F_μ. Assume $V \neq \emptyset$. Show there exist a linear subspace $L \subset k^n$ and a linear map $\lambda\colon k^n \twoheadrightarrow L$ such that $\lambda(V) = L$.

Exercise (15.24) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} \subset \operatorname{nil}(R)$. Show

$$\dim(R/\mathfrak{a}) = \dim(R). \qquad \textbf{(15.24.1)}$$

Exercise (15.25) . — Let R be a domain of (finite) dimension r, and $\mathfrak{p}$ a nonzero prime. Prove that $\dim(R/\mathfrak{p}) < r$.

Exercise (15.26) . — Given an integral extension of rings R'/R, show
$$\dim(R) = \dim(R'). \tag{15.26.1}$$

Exercise (15.27) . — Let R'/R be an integral extension of domains with R normal, $\mathfrak{m}$ a maximal ideal of R'. Show $\mathfrak{n} := \mathfrak{m} \cap R$ is maximal and $\dim(R'_{\mathfrak{m}}) = \dim(R_{\mathfrak{n}})$.

Exercise (15.28) . — (1) Given a product of rings $R := R' \times R''$, show
$$\dim(R) = \max\{\,\dim(R'),\, \dim(R'')\,\}. \tag{15.28.1}$$

(2) Find a ring R with a maximal chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$, yet $r < \dim(R)$.

Exercise (15.29) . — Let k be a field, R_1 and R_2 algebra-finite domains, and $\mathfrak{p}$ a minimal prime of $R_1 \otimes_k R_2$. Use Noether Normalization and **(14.20)** to prove this:
$$\dim\big((R_1 \otimes_k R_2)/\mathfrak{p}\big) = \dim(R_1) + \dim(R_2). \tag{15.29.1}$$

Exercise (15.30) . — Let k be a field, R a finitely generated k-algebra, $f \in R$ nonzero. Assume R is a domain. Prove that $\dim(R) = \dim(R_f)$.

Exercise (15.31) . — Let k be a field, $P := k[f]$ the polynomial ring in one variable f. Set $\mathfrak{p} := \langle f \rangle$ and $R := P_{\mathfrak{p}}$. Find $\dim(R)$ and $\dim(R_f)$.

Exercise (15.32) . — Let R be a ring, $R[X]$ the polynomial ring. Prove
$$1 + \dim(R) \le \dim(R[X]) \le 1 + 2\dim(R).$$
(In particular, $\dim(R[X]) = \infty$ if and only if $\dim(R) = \infty$.)

C. Appendix: Jacobson Rings

(15.33) (Jacobson Rings). — We call a ring R **Jacobson** if, given any ideal $\mathfrak{a}$, its radical is equal to the intersection of all maximal ideals containing it; that is,
$$\sqrt{\mathfrak{a}} = \textstyle\bigcap_{\mathfrak{m} \supset \mathfrak{a}} \mathfrak{m}. \tag{15.33.1}$$

Plainly, the nilradical of a Jacobson ring is equal to its Jacobson radical. Also, any quotient ring of a Jacobson ring is Jacobson too. In fact, a ring is Jacobson if and only if the the nilradical of every quotient ring is equal to its Jacobson radical.

In general, the right-hand side of **(15.33.1)** contains the left. So **(15.33.1)** holds if and only if every f outside $\sqrt{\mathfrak{a}}$ lies outside some maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$.

Recall the Scheinnullstellensatz, **(3.14)**: it says $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \supset \mathfrak{a}} \mathfrak{p}$ with $\mathfrak{p}$ prime. Thus R is Jacobson if and only if $\mathfrak{p} = \bigcap_{\mathfrak{m} \supset \mathfrak{p}} \mathfrak{m}$ for every prime $\mathfrak{p}$.

For example, a field k is Jacobson; in fact, a local ring A is Jacobson if and only if its maximal ideal is its only prime. Further, a Boolean ring B is Jacobson, as every prime is maximal by **(2.37)**, and so trivially $\mathfrak{p} = \bigcap_{\mathfrak{m} \supset \mathfrak{p}} \mathfrak{m}$ for every prime $\mathfrak{p}$.

Finally, a PID R is Jacobson if and only if it has infinitely many maximal ideals; in particular, $\mathbb{Z}$ and a polynomial ring in one variable over a field are Jacobson. Indeed, R is a UFD, and by **(15.9)**, every nonzero prime is maximal. Given a nonzero $x \in R$, say $x = \prod_{i=1}^{r} p_i^{n_i}$; then owing to **(2.25)**(1), the only maximal ideals containing x are the $\langle p_i \rangle$. Thus the next lemma does the trick.

Lemma (15.34). — *Let R be a 1-dimensional domain, $\{\mathfrak{m}_\lambda\}_{\lambda \in \Lambda}$ its set of maximal ideals. Assume every nonzero element lies in only finitely many $\mathfrak{m}_\lambda$. Then R is Jacobson if and only if Λ is infinite.*

Proof: If Λ is finite, take a nonzero $x_\lambda \in \mathfrak{m}_\lambda$ for each λ, and set $x := \prod x_\lambda$. Then $x \neq 0$ and $x \in \bigcap \mathfrak{m}_\lambda$. But $\sqrt{\langle 0\rangle} = \langle 0\rangle$ as R is a domain. So $\sqrt{\langle 0\rangle} \neq \bigcap \mathfrak{m}_\lambda$. Thus R is not Jacobson.

If Λ is infinite, then $\bigcap \mathfrak{m}_\lambda = \langle 0\rangle$ by hypothesis. But every nonzero prime is maximal as R is 1-dimensional. Thus $\mathfrak{p} = \bigcap_{\mathfrak{m}_\lambda \supset \mathfrak{p}} \mathfrak{m}_\lambda$ for every prime $\mathfrak{p}$. □

Proposition (15.35). — *A ring R is Jacobson if and only if, for any nonmaximal prime $\mathfrak{p}$ and any $f \notin \mathfrak{p}$, the extension $\mathfrak{p}R_f$ is not maximal.*

Proof: Assume R is Jacobson. Take a nonmaximal prime $\mathfrak{p}$ and $f \notin \mathfrak{p}$. Then $f \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$. So $\mathfrak{p}R_f$ is not maximal by (**11.12**)(2).

Conversely, let $\mathfrak{a}$ be an ideal, $f \notin \sqrt{\mathfrak{a}}$. Then $(R/\mathfrak{a})_f \neq 0$. So there is a maximal ideal $\mathfrak{n}$ in $(R/\mathfrak{a})_f$. Let $\mathfrak{m}$ be its contraction in R. Then $\mathfrak{m} \supset \mathfrak{a}$ and $f \notin \mathfrak{m}$. Also, (**4.8.1**) and (**12.15**) yield $R_f/\mathfrak{m}R_f = (R/\mathfrak{a}\big/\mathfrak{m}/\mathfrak{a})_f = (R/\mathfrak{a})_f/\mathfrak{n}$. As $\mathfrak{n}$ is maximal, $R_f/\mathfrak{m}R_f$ is a field. So $\mathfrak{m}$ is maximal by hypothesis. Thus R is Jacobson. □

Lemma (15.36). — *Let R'/R be an extension of domains. Assume $R' = R[x]$ for some $x \in R'$ and there is $y \in R'$ with R'_y a field. Then there is $z \in R$ with R_z a field and x algebraic over R_z. Further, if R is Jacobson, then R and R' are fields.*

Proof: Set $Q := \operatorname{Frac}(R)$. Then $Q \subset R'_y$, so $R'_y = R[x]_y \subset Q[x]_y \subset R'_y$. Hence $Q[x]_y = R'_y$. So $Q[x]_y$ is a field. Now, if x is transcendental over Q, then $Q[x]$ is a polynomial ring, so Jacobson by (**15.33**); whence, $Q[x]_y$ is not a field by (**15.35**), a contradiction. Thus x is algebraic over Q. Hence y is algebraic over Q too.

Let $a_0x^n + \cdots + a_n = 0$ and $b_0y^m + \cdots + b_m = 0$ be equations of minimal degree with $a_i, b_j \in R$. Set $z := a_0b_m$. Then $z \neq 0$. Further,

$$1/y = -a_0(b_0y^{m-1} + \cdots + b_{m-1})/z \in R_z[x].$$

Hence $R[x]_y \subset R_z[x] \subset R'_y$. So $R_z[x] = R'_y$. Therefore $R_z[x]$ is a field too. But $x^n + (a_1b_m/z)x^{n-1} + \cdots + (a_nb_m/z) = 0$, so is an equation of integral dependence of x on R_z. So $R_z[x]$ is integral over R_z (**10.18**) . Hence R_z is a field by (**14.1**).

Further, if R is Jacobson, then $\langle 0\rangle$ is a maximal ideal by (**15.35**), and so R is a field. Hence $R = R_z$. Thus R' is a field by (**14.1**). □

Theorem (15.37) (Generalized Hilbert Nullstellensatz). — *Let R be a Jacobson ring, R' an algebra-finite algebra, and $\mathfrak{m}'$ a maximal ideal of R'. Set $\mathfrak{m} := \mathfrak{m}'^c$. Then* (1) *$\mathfrak{m}$ is maximal, and $R'/\mathfrak{m}'$ is finite over $R/\mathfrak{m}$, and* (2) *R' is Jacobson.*

Proof: First, assume $R' = R[x]$ for some $x \in R'$. Given a prime $\mathfrak{q} \subset R'$ and a $y \in R' - \mathfrak{q}$, set $\mathfrak{p} := \mathfrak{q}^c$ and $R_1 := R/\mathfrak{p}$ and $R'_1 := R'/\mathfrak{q}$. Then R_1 is Jacobson by (**15.33**). Suppose $(R'_1)_y$ is a field. Then by (**15.36**), R'_1/R_1 is a finite extension of fields. Thus $\mathfrak{q}$ and $\mathfrak{p}$ are maximal. To obtain (1), simply take $\mathfrak{q} := \mathfrak{m}'$ and $y := 1$. To obtain (2), take $\mathfrak{q}$ nonmaximal, so R'_1 is not a field; conclude $(R'_1)_y$ is not a field; whence, (**15.35**) yields (2).

Second, assume $R' = R[x_1, \ldots, x_n]$ with $n \geq 2$. Set $R'' := R[x_1, \ldots, x_{n-1}]$ and $\mathfrak{m}'' := \mathfrak{m}'^c \subset R''$. Then $R' = R''[x_n]$. By induction on n, we may assume (1) and (2) hold for R''/R. So the first case for R'/R'' yields (2) for R'; by the same token, $\mathfrak{m}''$ is maximal, and $R'/\mathfrak{m}'$ is finite over $R''/\mathfrak{m}''$. Hence, $\mathfrak{m}$ is maximal, and $R''/\mathfrak{m}''$ is finite over $R/\mathfrak{m}$ by (1) for R''/R. Finally, (**10.16**) implies that $R'/\mathfrak{m}'$ is finite over $R/\mathfrak{m}$, as desired. □

Example (15.38). — Part (1) of (**15.37**) may fail if R is not Jacobson, even if $R' := R[Y]$ is the polynomial ring in one variable Y over R. For example, let k be a field, and $R := k[[X]]$ the formal power series ring. According to (**3.8**), the ideal $\mathfrak{m}' := \langle 1 - XY \rangle$ is maximal, but $\mathfrak{m}'^c$ is $\langle 0 \rangle$, not $\langle X \rangle$.

D. Appendix: Exercises

Exercise (15.39) . — Let X be a topological space. We say a subset Y is **locally closed** if Y is the intersection of an open set and a closed set; equivalently, Y is open in its closure $\overline{Y}$; equivalently, Y is closed in an open set containing it.

We say a subset X_0 of X is **very dense** if X_0 meets every nonempty locally closed subset Y. We say X is **Jacobson** if its set of closed points is very dense.

Show that the following conditions on a subset X_0 of X are equivalent:

(1) X_0 is very dense.
(2) Every closed set F of X satisfies $\overline{F \cap X_0} = F$.
(3) The map $U \mapsto U \cap X_0$ from the open sets of X to those of X_0 is bijective.

Exercise (15.40) . — Let R be a ring, $X := \operatorname{Spec}(R)$, and X_0 the set of closed points of X. Show that the following conditions are equivalent:

(1) R is a Jacobson ring.
(2) X is a Jacobson space.
(3) If $y \in X$ is a point such that $\{y\}$ is locally closed, then $y \in X_0$.

Exercise (15.41) . — Why is a field K finite if it's an algebra-finite $\mathbb{Z}$-algebra?

Exercise (15.42) . — Let $P := \mathbb{Z}[X_1, \ldots, X_n]$ be the polynomial ring. Assume $F \in P$ vanishes at every zero in K^n of $F_1, \ldots, F_r \in P$ for every finite field K; that is, if $(a) := (a_1, \ldots, a_n) \in K^n$ and $F_1(a) = 0, \ldots, F_r(a) = 0$ in K, then $F(a) = 0$ too. Prove there are $G_1, \ldots, G_r \in P$ and $N \geq 1$ with $F^N = G_1F_1 + \cdots + G_rF_r$.

Exercise (15.43) . — Prove that a ring R is Jacobson if and only if each algebra-finite algebra R' that is a field is module finite over R.

Exercise (15.44) . — Prove a ring R is Jacobson if and only if each nonmaximal prime $\mathfrak{p}$ is the intersection of the primes that properly contain $\mathfrak{p}$.

Exercise (15.45) . — Let R be a Jacobson ring, $\mathfrak{p}$ a prime, $f \in R - \mathfrak{p}$. Prove that $\mathfrak{p}$ is the intersection of all the maximal ideals containing $\mathfrak{p}$ but not f.

Exercise (15.46) . — Let R be a ring, R' an algebra. Prove that if R' is integral over R and R is Jacobson, then R' is Jacobson.

Exercise (15.47) . — Let R be a Jacobson ring, S a multiplicative subset, $f \in R$. True or false: prove or give a counterexample to each of the following statements.

(1) The localized ring R_f is Jacobson.
(2) The localized ring $S^{-1}R$ is Jacobson.
(3) The filtered direct limit $\varinjlim R_\lambda$ of Jacobson rings is Jacobson.
(4) In a filtered direct limit of rings R_λ, necessarily $\varinjlim \operatorname{rad}(R_\lambda) = \operatorname{rad}(\varinjlim R_\lambda)$.

Exercise (15.48) . — Let R be a reduced Jacobson ring with a finite set Σ of minimal primes, and P a finitely presented module. Show that P is locally free of rank r if and only if $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$ for any maximal ideal $\mathfrak{m}$.

16. Chain Conditions

Often in a ring, every ideal is finitely generated; if so, the ring is said to be **Noetherian**. Examples include any PID and any field. We characterize Noetherian rings as those in which every ascending chain of ideals stabilizes, or equivalently, in which every nonempty set of ideals has a member maximal under inclusion.

We prove the Hilbert Basis Theorem: if a ring is Noetherian, then so is any finitely generated algebra over it. We define and characterize Noetherian modules similarly, and we prove that, over a Noetherian ring, it is equivalent for a module to be Noetherian, to be finitely generated, or to be finitely presented. Conversely, given a Noetherian R-module M, we prove $R/\operatorname{Ann}(M)$ is a Noetherian ring, over which M is a finitely generated module. Lastly, we study Artinian rings and modules; in them, by definition, every descending chain of ideals or of submodules, stabilizes.

In an appendix, we discuss two types of topological spaces: **irreducible** and **Noetherian**. By definition, in the former, any two nonempty open sets meet, and in the latter, the open sets satisfy the acc. We prove that a Noetherian space is the union of finitely many **irreducible components**, which are the maximal irreducible subspaces. We prove that $\operatorname{Spec}(R)$ is Noetherian if R is, and that its irreducible components are the $\mathbf{V}(\mathfrak{p})$ with $\mathfrak{p}$ a minimal prime.

Lastly, we prove Chevalley's Theorem: given a map of rings, whose source is Noetherian and whose target is algebra finite over it, the induced map on their Spec's preserves the **constructible sets**, which are the finite unions of the subsets of the form the intersection of an open set and a closed set.

A. Text

(16.1) (Noetherian rings). — We call a ring **Noetherian** if every ideal is finitely generated. For example, a Principal Ideal Ring (PIR) is, trivially, Noetherian.

Here are two standard examples of non-Noetherian rings. More are given in (16.6), (16.57), (16.31), (16.67), (18.24), and (26.11)(2).

First, form the polynomial ring $k[X_1, X_2, \dots]$ in infinitely many variables. It is non-Noetherian as $\langle X_1, X_2, \dots\rangle$ is not finitely generated (but the ring is a UFD).

Second, in the polynomial ring $k[X, Y]$, form this subring R and its ideal $\mathfrak{a}$:

$$R := \big\{F := a + XG \mid a \in k \text{ and } G \in k[X, Y]\big\} \text{ and}$$
$$\mathfrak{a} := \langle X,\, XY,\, XY^2, \dots\rangle.$$

Then $\mathfrak{a}$ is not generated by any $F_1, \dots, F_m \in \mathfrak{a}$. Indeed, let n be the highest power of Y occurring in any F_i. Then $XY^{n+1} \notin \langle F_1, \dots, F_m\rangle$. Thus R is non-Noetherian.

Exercise (16.2) . — Let M be a finitely generated module over an arbitrary ring. Show every set that generates M contains a finite subset that generates.

Definition (16.3). — Given a ring, we say the **ascending chain condition** (acc) is satisfied if every ascending chain of ideals $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$ **stabilizes**; that is, there is a $j \geq 0$ such that $\mathfrak{a}_j = \mathfrak{a}_{j+1} = \cdots$.

We say the **maximal condition** (maxc) is satisfied if every nonempty set of ideals $\mathcal{S}$ contains ones *maximal* for inclusion, that is, properly contained in no other in $\mathcal{S}$.

Lemma (16.4). — *In a ring, the acc is satisfied if and only if maxc is satisfied.*

Proof: Let $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$ be a chain of ideals. If $\mathfrak{a}_j$ is maximal, then trivially $\mathfrak{a}_j = \mathfrak{a}_{j+1} = \cdots$. Thus maxc implies acc.

Conversely, given a nonempty set of ideals $\mathcal{S}$ with no maximal member, there's $\mathfrak{a}_0 \in \mathcal{S}$; for each $j \geq 0$, there's $\mathfrak{a}_{j+1} \in \mathcal{S}$ with $\mathfrak{a}_j \subsetneqq \mathfrak{a}_{j+1}$. So the Axiom of Countable Choice provides an infinite chain $\mathfrak{a}_0 \subsetneqq \mathfrak{a}_1 \subsetneqq \cdots$. Thus acc implies maxc. □

Proposition (16.5). — *The following conditions on a ring are equivalent:*

(1) *the ring is Noetherian;* (2) *the acc is satisfied;* (3) *the maxc is satisfied.*

Proof: Assume (1) holds. Let $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \cdots$ be a chain of ideals. Set $\mathfrak{a} := \bigcup \mathfrak{a}_n$. Clearly, $\mathfrak{a}$ is an ideal. So by hypothesis, $\mathfrak{a}$ is finitely generated, say by $x_1, \ldots, x_r$. For each i, there is a j_i with $x_i \in \mathfrak{a}_{j_i}$. Set $j := \max\{j_i\}$. Then $x_i \in \mathfrak{a}_j$ for all i. So $\mathfrak{a} \subset \mathfrak{a}_j \subset \mathfrak{a}_{j+1} \subset \cdots \subset \mathfrak{a}$. So $\mathfrak{a}_j = \mathfrak{a}_{j+1} = \cdots$. Thus (2) holds.

Assume (2) holds. Then (3) holds by (**16.4**).

Assume (3) holds. Let $\mathfrak{a}$ be an ideal, x_λ for $\lambda \in \Lambda$ generators, $\mathcal{S}$ the set of ideals generated by finitely many x_λ. Let $\mathfrak{b}$ be a maximal element of $\mathcal{S}$; say $\mathfrak{b}$ is generated by $x_{\lambda_1}, \ldots, x_{\lambda_m}$. Then $\mathfrak{b} \subset \mathfrak{b} + \langle x_\lambda \rangle$ for any λ. So by maximality, $\mathfrak{b} = \mathfrak{b} + \langle x_\lambda \rangle$. Hence $x_\lambda \in \mathfrak{b}$. So $\mathfrak{b} = \mathfrak{a}$; whence, $\mathfrak{a}$ is finitely generated. Thus (1) holds. □

Example (16.6). — In the field of rational functions $k(X, Y)$, form this ring:

$$R := k[X,\, Y,\, X/Y,\, X/Y^2,\, X/Y^3, \ldots].$$

Then R is non-Noetherian by (**16.5**). Indeed, X does not factor into irreducibles: $X = (X/Y) \cdot Y$ and $X/Y = (X/Y^2) \cdot Y$ and so on. Correspondingly, there is an ascending chain of ideals that does not stabilize:

$$\langle X \rangle \subsetneqq \langle X/Y \rangle \subsetneqq \langle X/Y^2 \rangle \subsetneqq \cdots.$$

Proposition (16.7). — *Let R be a Noetherian ring, S a multiplicative subset, $\mathfrak{a}$ an ideal. Then $R/\mathfrak{a}$ and $S^{-1}R$ are Noetherian.*

Proof: If R satisfies the acc, so do $R/\mathfrak{a}$ and $S^{-1}R$ by (**1.9**) and by (**11.12**)(1).

Alternatively, any ideal $\mathfrak{b}/\mathfrak{a}$ of $R/\mathfrak{a}$ is, clearly, generated by the images of generators of $\mathfrak{b}$. Similarly, any ideal $\mathfrak{b}$ of $S^{-1}R$ is generated by the images of generators of $\varphi_S^{-1}\mathfrak{b}$ by (**11.11**)(1)(b). □

Proposition (16.8) (Cohen). — *A ring R is Noetherian if every prime is finitely generated.*

Proof: Suppose there are non-finitely-generated ideals. Given a nonempty set of them $\{\mathfrak{a}_\lambda\}$ that is linearly ordered by inclusion, set $\mathfrak{a} := \bigcup \mathfrak{a}_\lambda$. If $\mathfrak{a}$ is finitely generated, then all the generators lie in some $\mathfrak{a}_\lambda$, so generate $\mathfrak{a}_\lambda$; so $\mathfrak{a}_\lambda = \mathfrak{a}$, a contradiction. Thus $\mathfrak{a}$ is non-finitely-generated. Hence, by Zorn's Lemma, there is a maximal non-finitely-generated ideal $\mathfrak{p}$. In particular, $\mathfrak{p} \neq R$.

Assume every prime is finitely generated. Then there are $a, b \in R - \mathfrak{p}$ with $ab \in \mathfrak{p}$. So $\mathfrak{p} + \langle a \rangle$ is finitely generated, say by $x_1 + w_1 a, \ldots, x_n + w_n a$ with $x_i \in \mathfrak{p}$. Then $\{x_1, \ldots, x_n, a\}$ generate $\mathfrak{p} + \langle a \rangle$.

Set $\mathfrak{b} = \operatorname{Ann}\big((\mathfrak{p} + \langle a \rangle)/\mathfrak{p}\big)$. Then $\mathfrak{b} \supset \mathfrak{p} + \langle b \rangle$ and $b \notin \mathfrak{p}$. So $\mathfrak{b}$ is finitely generated, say by $y_1, \ldots, y_m$. Take $z \in \mathfrak{p}$. Then $z \in \mathfrak{p} + \langle a \rangle$, so write

$$z = a_1 x_1 + \cdots + a_n x_n + ya$$

with $a_i, y \in R$. Then $ya \in \mathfrak{p}$. So $y \in \mathfrak{b}$. Hence $y = b_1 y_1 + \cdots + b_m y_m$ with $b_j \in R$.

Thus $\mathfrak{p}$ is generated by $\{x_1, \ldots, x_n, ay_1, \ldots, ay_m\}$, a contradiction. Thus there are no non-finitely-generated ideals; in other words, R is Noetherian. □

Lemma (16.9). — *If a ring R is Noetherian, then so is the polynomial ring $R[X]$.*

Proof: By way of contradiction, assume there is an ideal $\mathfrak{a}$ of $R[X]$ that is not finitely generated. Set $\mathfrak{a}_0 := \langle 0 \rangle$. For each $i \geq 1$, choose inductively $F_i \in \mathfrak{a} - \mathfrak{a}_{i-1}$ of least degree d_i. Set $\mathfrak{a}_i := \langle F_1, \ldots, F_i \rangle$. Let a_i be the leading coefficient of F_i, and $\mathfrak{b}$ the ideal generated by all the a_i. As R is Noetherian, $\mathfrak{b}$ is finitely generated. So $\mathfrak{b} = \langle a_1, \ldots, a_n \rangle$ for some n by **(16.2)**. Thus $a_{n+1} = r_1 a_1 + \cdots + r_n a_n$ with $r_i \in R$.

By construction, $d_i \leq d_{i+1}$ for all i. Set

$$F := F_{n+1} - (r_1 F_1 X^{d_{n+1}-d_1} + \cdots + r_n F_n X^{d_{n+1}-d_n}).$$

Then $\deg(F) < d_{n+1}$, so $F \in \mathfrak{a}_n$. Therefore, $F_{n+1} \in \mathfrak{a}_n$, a contradiction. □

Theorem (16.10) (Hilbert Basis)**. —** *Let R be a Noetherian ring, R' a finitely generated algebra. Then R' is Noetherian.*

Proof: Say $x_1, \ldots, x_r$ generate R' over R, and let $P := R[X_1, \ldots, X_r]$ be the polynomial ring in r variables. Then P is Noetherian by **(16.9)** and induction on r. Assigning x_i to X_i defines an R-algebra map $P \to R'$, and obviously, it is surjective. Hence R' is Noetherian by **(16.7)**. □

(16.11) (Noetherian modules). — We call a module M **Noetherian** if every submodule is finitely generated. In particular, *a ring is Noetherian as a ring if and only if it is Noetherian as a module,* because its submodules are just the ideals.

We say the **ascending chain condition** (acc) is satisfied in M if every ascending chain of submodules $M_0 \subset M_1 \subset \cdots$ stabilizes. We say the **maximal condition** (maxc) is satisfied in M if every nonempty set of submodules contains ones maximal under inclusion. It is simple to generalize **(16.5)**: *These conditions are equivalent:*

(1) *M is Noetherian;* (2) *acc is satisfied in M;* (3) *maxc is satisfied in M.*

Lemma (16.12). — *Let R be a ring, M a module, and N a submodule. Nested submodules $M_1 \subset M_2$ of M are equal if both these equations hold:*

$$M_1 \cap N = M_2 \cap N \quad \text{and} \quad (M_1 + N)/N = (M_2 + N)/N.$$

Proof: Given $m_2 \in M_2$, there is $m_1 \in M_1$ with $n := m_2 - m_1 \in N$. Then $n \in M_2 \cap N = M_1 \cap N$. Hence $m_2 \in M_1$. Thus $M_1 = M_2$. □

Proposition (16.13). — *Let R be a ring, M a module, N a submodule.*

(1) *Then M is finitely generated if N and M/N are finitely generated.*

(2) *Then M is Noetherian if and only if N and M/N are Noetherian.*

Proof: Assertion (1) is equivalent to **(5.5)** owing to **(5.2)**.

To prove (2), first assume M is Noetherian. A submodule N' of N is also a submodule of M, so N' is finitely generated; thus N is Noetherian. A submodule of M/N is finitely generated as its inverse image in M is so; thus M/N is Noetherian.

Conversely, assume N and M/N are Noetherian. Let P be a submodule of M. Then $P \cap N$ and $(P+N)/N$ are finitely generated. But $P/(P \cap N) \xrightarrow{\sim} (P+N)/N$ by **(4.8.2)**. So (1) implies P is finitely generated. Thus M is Noetherian.

Here is a second proof of (2). First assume M is Noetherian. Then any ascending chain in N is also a chain in M, so it stabilizes. And any chain in M/N is the image of a chain in M, so it too stabilizes. Thus N and M/N are Noetherian.

Conversely, assume N and M/N are Noetherian. Given $M_1 \subset M_2 \subset \cdots \subset M$, both $(M_1 \cap N) \subset (M_2 \cap N) \subset \cdots$ and $(M_1 + N)/N \subset (M_2 + N)/N \subset \cdots$ stabilize, say $M_j \cap N = M_{j+1} \cap N = \cdots$ and $(M_j + N)/N = (M_{j+1} + N)/N = \cdots$. Then $M_j = M_{j+1} = \cdots$ by **(16.12)**. Thus M is Noetherian. □

Corollary (16.14). — *Modules $M_1, \ldots, M_r$ are Noetherian if and only if their direct sum $M_1 \oplus \cdots \oplus M_r$ is Noetherian.*

Proof: The sequence $0 \to M_1 \to M_1 \oplus (M_2 \oplus \cdots \oplus M_r) \to M_2 \oplus \cdots \oplus M_r \to 0$ is exact. So the assertion results from **(16.13)**(2) by induction on r. □

Theorem (16.15). — *Let R be a Noetherian ring, and M a module. Then the following conditions on M are equivalent:*

(1) *M is Noetherian;* (2) *M is finitely generated;* (3) *M is finitely presented.*

Proof: Assume (2). Then there is an exact sequence $0 \to K \to R^n \to M \to 0$. Now, R^n is Noetherian by **(16.14)** and by **(16.11)**. Hence K is finitely generated, so (3) holds; further, (1) holds by **(16.13)**(2). Trivially, (1) or (3) implies (2). □

Theorem (16.16). — *Let R be a ring, M a module. Set $R' := R/\operatorname{Ann}(M)$. Then M is Noetherian if and only if R' is Noetherian and M is finitely generated.*

Proof: First, assume M is Noetherian. Say $m_1, \ldots, m_r$ generate M. Define $\alpha\colon R \to M^{\oplus r}$ by $\alpha(x) := (xm_1, \ldots, xm_r)$. Plainly $\operatorname{Ker}(\alpha) = \operatorname{Ann}(M)$. Hence α induces an injection $R' \hookrightarrow M^{\oplus r}$. But $M^{\oplus r}$ is Noetherian by **(16.14)**. Thus **(16.13)**(2) implies that R' is Noetherian. Trivially, M is finitely generated.

Conversely, assume R' is Noetherian and M is finitely generated. Apply **(16.15)** over R'. Thus M is Noetherian. □

Lemma (16.17) (Artin–Tate [**2**, Thm. 1]). — *Let R'/R and R''/R' be extensions of rings. Assume that R is Noetherian, that R''/R is algebra finite, and that R''/R' either is module finite or is integral. Then R'/R is algebra finite.*

Proof: Since R''/R is algebra finite, so is R''/R'. Hence, the two conditions on R''/R' are equivalent by **(10.18)**.

Say $x_1, \ldots, x_m$ generate R'' as an R-algebra, and $y_1, \ldots, y_n$ generate R'' as an R'-module. Then there exist $z_{ij} \in R'$ and $z_{ijk} \in R'$ with

$$x_i = \textstyle\sum_j z_{ij} y_j \quad \text{and} \quad y_i y_j = \sum_k z_{ijk} y_k. \tag{16.17.1}$$

Set $R'_0 := R[\{z_{ij},\, z_{ijk}\}] \subset R''$. Since R is Noetherian, so is R'_0 by **(16.10)**.

Any $x \in R''$ is a polynomial in the x_i with coefficients in R. So **(16.17.1)** implies x is a linear combination of the y_j with coefficients in R'_0. Thus R''/R'_0 is module finite. But R'_0 is a Noetherian ring. So R'' is a Noetherian R'_0-module by **(16.15)**, (2)⇒(1). But R' is an R'_0-submodule of R''. So R'/R'_0 is module finite by **(16.11)**.

So there are $w_1, \ldots, w_p \in R'$ such that, if $x \in R'$, then $x = \sum a_k w_k$ with $a_k \in R'_0$. But $R'_0 := R[\{z_{ij},\, z_{ijk}\}] \subset R''$. Thus $R' = R[\{z_{ij},\, z_{ijk},\, w_k\}] \subset R''$, as desired. □

Theorem (16.18) (Noether on Invariants). — *Let R be a Noetherian ring, R' an algebra-finite extension, and G a finite group of R-automorphisms of R'. Then the subring of invariants R'^G is also algebra finite; in other words, every invariant can be expressed as a polynomial in a certain finite number of "fundamental" invariants.*

Proof: By **(10.35)**, R' is integral over R'^G. So **(16.17)** yields the assertion. □

(16.19) (Artin–Tate proof [2, Thm. 2] of the Zariski Nullstellensatz (15.4)). — In the setup of (15.4), take a transcendence base $x_1, \ldots, x_r$ of R/k. Then R is integral over $k(x_1, \ldots, x_r)$ by definition of transcendence basis [3, (8.3), p. 526]. So $k(x_1, \ldots, x_r)$ is algebra finite over k by (16.17), say $k(x_1, \ldots, x_r) = k[y_1, \ldots, y_s]$.

Suppose $r \geq 1$. Write $y_i = F_i/G_i$ with $F_i, G_i \in k[x_1, \ldots, x_r]$. Let H be an irreducible factor of $G_1 \cdots G_s + 1$. Plainly $H \nmid G_i$ for all i.

Say $H^{-1} = P(y_1, \ldots, y_s)$ where P is a polynomial. Then $H^{-1} = Q/(G_1 \cdots G_s)^m$ for some $Q \in k[x_1, \ldots, x_r]$ and $m \geq 1$. But $H \nmid G_i$ for all i, a contradiction. Thus $r = 0$. So (10.18) implies R/k is module finite, as desired.

Example (16.20). — Set $\delta := \sqrt{-5}$, set $R := \mathbb{Z}[\delta]$, and set $\mathfrak{p} := \langle 2, 1 + \delta \rangle$. Let's prove that $\mathfrak{p}$ is finitely presented and that $\mathfrak{p}R_{\mathfrak{q}}$ is free of rank 1 over $R_{\mathfrak{q}}$ for every maximal ideal $\mathfrak{q}$ of R, but that $\mathfrak{p}$ is not free. Thus the equivalent conditions of (13.15) do not imply that $\mathfrak{p}$ is free.

Since $\mathbb{Z}$ is Noetherian and since R is finitely generated over $\mathbb{Z}$, the Hilbert Basis Theorem (16.10) yields that R is Noetherian. So since $\mathfrak{p}$ is generated by two elements, (16.15) yields that $\mathfrak{p}$ is finitely presented.

Recall from [3, pp. 417, 421, 425] that $\mathfrak{p}$ is maximal in R, but not principal. Now, $3 \notin \mathfrak{p}$; otherwise, $1 \in \mathfrak{p}$ as $2 \in \mathfrak{p}$, but $\mathfrak{p} \neq R$. So $(1 - \delta)/3 \in R_{\mathfrak{p}}$. Hence $(1 + \delta)R_{\mathfrak{p}}$ contains $(1 + \delta)(1 - \delta)/3$, or 2. So $(1 + \delta)R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$. Since $R_{\mathfrak{p}}$ is a domain, the map $\mu_{1+\delta} \colon R_{\mathfrak{p}} \to \mathfrak{p}R_{\mathfrak{p}}$ is injective, so bijective. Thus $\mathfrak{p}R_{\mathfrak{p}}$ is free of rank 1.

Let $\mathfrak{q}$ be a maximal ideal distinct from $\mathfrak{p}$. Then $\mathfrak{p} \cap (R - \mathfrak{q}) \neq \emptyset$; so, $\mathfrak{p}R_{\mathfrak{q}} = R_{\mathfrak{q}}$ by (11.8)(2). Thus $\mathfrak{p}R_{\mathfrak{q}}$ is free of rank 1.

Finally, suppose $\mathfrak{p} \simeq R^n$. Set $K := \operatorname{Frac}(R)$. Then $K = S_0^{-1}R$. So $S_0^{-1}\mathfrak{p} \simeq K^n$. But the inclusion $\mathfrak{p} \hookrightarrow R$ yields an injection $S_0^{-1}\mathfrak{p} \hookrightarrow K$. Also, $S_0^{-1}\mathfrak{p}$ is a nonzero K-vector space. Hence $S_0^{-1}\mathfrak{p} \xrightarrow{\sim} K$. Therefore, $n = 1$. So $\mathfrak{p} \simeq R$. Hence $\mathfrak{p}$ is generated by one element, so is principal, a contradiction. Thus $\mathfrak{p}$ is not free.

Definition (16.21). — We say a module is **Artinian** or the **descending chain condition** (dcc) is satisfied if every descending chain of submodules stabilizes.

We say the ring itself is **Artinian** if it is an Artinian module.

We say the **minimal condition** (minc) is satisfied in a module if every nonempty set of submodules has a minimal member.

Proposition (16.22). — *Let $M_1, \ldots, M_r$, M be modules, N a submodule of M.*

(1) *Then M is Artinian if and only if minc is satisfied in M.*
(2) *Then M is Artinian if and only if N and M/N are Artinian.*
(3) *Then $M_1, \ldots, M_r$ are Artinian if and only if $M_1 \oplus \cdots \oplus M_r$ is Artinian.*

Proof: It is easy to adapt the proof of (16.4), the second proof of (16.13)(2), and the proof of (16.14). □

B. Exercises

Exercise (16.23) . — Let M be a module. Assume that every nonempty set of finitely generated submodules has a maximal element. Show M is Noetherian.

Exercise (16.24) . — Let R be a Noetherian ring, $\{F_\lambda\}_{\lambda \in \Lambda}$ a set of polynomials in variables $X_1, \ldots, X_n$. Show there's a finite subset $\Lambda_0 \subset \Lambda$ such that the set V_0 of zeros in R^n of the F_λ for $\lambda \in \Lambda_0$ is precisely that V of the F_λ for $\lambda \in \Lambda$.

Exercise (16.25) . — Let R be a Noetherian ring, $F := \sum a_n X^n \in R[[X]]$ a power series in one variable. Show that F is nilpotent if and only if each a_n is too.

Exercise (16.26) . — Let R be a ring, X a variable, $R[X]$ the polynomial ring. Prove this statement or find a counterexample: if $R[X]$ is Noetherian, then so is R.

Exercise (16.27) . — Let R'/R be a ring extension with an R-linear retraction $\rho\colon R' \to R$. If R' is Noetherian, show R is too. What if R' is Artinian?

Exercise (16.28) . — Let R be a ring, M a module, R' a faithfully flat algebra. If $M \otimes_R R'$ is Noetherian over R', show M is Noetherian over R. What if $M \otimes_R R'$ is Artinian over R'?

Exercise (16.29) . — Let R be a ring. Assume that, for each maximal ideal $\mathfrak{m}$, the local ring $R_\mathfrak{m}$ is Noetherian and that each nonzero $x \in R$ lies in only finitely many maximal ideals. Show R is Noetherian: use **(13.10)** to show any ideal is finitely generated; alternatively, use **(13.9)** to show any ascending chain stabilizes.

Exercise (16.30) (*Nagata*) . — Let k be a field, $P := k[X_1, X_2, \dots]$ a polynomial ring, $m_1 < m_2 < \cdots$ positive integers with $m_{i+1} - m_i > m_i - m_{i-1}$ for $i > 1$. Set $\mathfrak{p}_i := \langle X_{m_i+1}, \dots, X_{m_{i+1}} \rangle$ and $S := P - \bigcup_{i \ge 1} \mathfrak{p}_i$. Show S is multiplicative, $S^{-1}P$ is Noetherian of infinite dimension, and the $S^{-1}\mathfrak{p}_i$ are the maximal ideals of $S^{-1}P$.

Exercise (16.31) . — Let z be a complex variable. Determine which of these rings R are Noetherian:

(1) the ring R of rational functions of z having no pole on the circle $|z| = 1$,
(2) the ring R of power series in z having a positive radius of convergence,
(3) the ring R of power series in z with an infinite radius of convergence,
(4) the ring R of polynomials in z whose first k derivatives vanish at the origin,
(5) the ring R of polynomials in two complex variables z, w whose first partial derivative with respect to w vanishes for $z = 0$.

Exercise (16.32) . — Let R be a ring, M a Noetherian module. Adapt the proof of the Hilbert Basis Theorem **(16.9)** to prove $M[X]$ is a Noetherian $R[X]$-module.

Exercise (16.33) . — Let R be a ring, S a multiplicative subset, M a Noetherian module. Show that $S^{-1}M$ is a Noetherian $S^{-1}R$-module.

Exercise (16.34) . — For $i = 1, 2$, let R_i be a ring, M_i a Noetherian R_i-module. Set $R := R_1 \times R_2$ and $M := M_1 \times M_2$. Show that M is a Noetherian R-module.

Exercise (16.35) . — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence of R-modules, and M_1, M_2 two submodules of M. Prove or give a counterexample to this statement: if $\beta(M_1) = \beta(M_2)$ and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2)$, then $M_1 = M_2$.

Exercise (16.36) . — Let R be a ring, $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ ideals such that each $R/\mathfrak{a}_i$ is a Noetherian ring. Prove (1) that $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module, and (2) that, if $\bigcap \mathfrak{a}_i = 0$, then R too is a Noetherian ring.

Exercise (16.37) . — Let R be a ring, and M and N modules. Assume that N is Noetherian and that M is finitely generated. Show that $\operatorname{Hom}(M, N)$ is Noetherian.

Exercise (16.38) . — Let R be a ring, M a module. If R is Noetherian, and M finitely generated, show $S^{-1}D(M) = D(S^{-1}M)$.

Exercise (16.39) . — Let R be a domain, R' an algebra, and set $K := \operatorname{Frac}(R)$. Assume R is Noetherian. Prove the following statements.

(1) [**2**, Thm. 3] Assume R' is a field containing R. Then R'/R is algebra finite if and only if K/R is algebra finite and R'/K is (module) finite.

(2) [**2**, bot. p. 77] Let $K' \supset R$ be a field that embeds in R'. Assume R'/R is algebra finite. Then K/R is algebra finite and K'/K is finite.

Exercise (16.40) . — Let R be a domain, $K := \operatorname{Frac}(R)$, and $x \in K$. If x is integral over R, show there is a nonzero $d \in R$ such that $dx^n \in R$ for all $n \geq 0$. Conversely, if such a d exists and if R is Noetherian, show x is integral over R.

Exercise (16.41) . — Let k be a field, V a vector space. Show these statements are equivalent: (1) V is finite dimensional; (2) V is Noetherian; (3) V is Artinian.

Exercise (16.42) . — Let k be a field, R an algebra, M an R-module. Assume M is finite dimensional as a k-vector space. Prove M is Noetherian and Artinian.

Exercise (16.43) . — Let R be a ring, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ maximal ideals. Assume $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Set $\mathfrak{a}_0 := R$, and for $1 \leq i \leq n$, set $\mathfrak{a}_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$ and $V_i := \mathfrak{a}_{i-1}/\mathfrak{a}_i$. Using the $\mathfrak{a}_i$ and V_i, show that R is Artinian if and only if R is Noetherian.

Exercise (16.44) . — Fix a prime number p. Set $M_n := \{\, q \in \mathbb{Q}/\mathbb{Z} \mid p^n q = 0 \,\}$ for $n \geq 0$. Set $M := \bigcup M_n$. Find a canonical isomorphism $\mathbb{Z}/\langle p^n \rangle \xrightarrow{\sim} M_n$. Given a proper $\mathbb{Z}$-submodule N of M, show $N = M_n$ for some n. Deduce M is Artinian, but not Noetherian. Find $\operatorname{Ann}(M)$, and deduce $\mathbb{Z}/\operatorname{Ann}(M)$ is not Artinian.

Exercise (16.45) . — Let R be an Artinian ring. Prove that R is a field if it is a domain. Deduce that, in general, every prime ideal $\mathfrak{p}$ of R is maximal.

Exercise (16.46) . — Let R be a ring, M an Artinian module, $\alpha\colon M \to M$ an endomorphism. Assume α is injective. Show that α is an isomorphism.

Exercise (16.47) . — Let R be a ring; M a module; N_1, N_2 submodules. If the M/N_i are Noetherian, show $M/(N_1 \cap N_2)$ is too. What if the M/N_i are Artinian?

C. Appendix: Noetherian Spaces

Definition (16.48). — We call a topological space **irreducible** if it is nonempty and if every pair of nonempty open subsets meet. A subspace is said to be an **irreducible component** if it is a maximal irreducible subspace.

Proposition (16.49). — *Let R be a ring. Set $X := \operatorname{Spec}(R)$ and $\mathfrak{n} := \operatorname{nil}(R)$. Then X is irreducible if and only if $\mathfrak{n}$ is prime.*

Proof: Given $g \in R$, take $f := 0$. Plainly, $D(f) = \emptyset$; see **(13.1)**. Thus, in **(13.39)**, the equivalence of (1) and (5) means this: $\mathbf{D}(g) = \emptyset$ if and only if $g \in \mathfrak{n}$.

Suppose $\mathfrak{n}$ is not prime. Then there are $f, g \in R$ with $f, g \notin \mathfrak{n}$ but $fg \in \mathfrak{n}$. The above observation yields $\mathbf{D}(f) \neq \emptyset$ and $\mathbf{D}(g) \neq \emptyset$ but $\mathbf{D}(fg) = \emptyset$. Further, $\mathbf{D}(f) \cap \mathbf{D}(g) = \mathbf{D}(fg)$ by **(13.1.3)**. Thus X is not irreducible.

Suppose X is not irreducible: say U, V are nonempty open sets with $U \cap V = \emptyset$. By **(13.1)**, the $D(f)$ form a basis of the topology: fix f, g with $\emptyset \neq \mathbf{D}(f) \subset U$ and $\emptyset \neq \mathbf{D}(g) \subset V$. Then $\mathbf{D}(f) \cap \mathbf{D}(g) = \emptyset$. But $\mathbf{D}(f) \cap \mathbf{D}(g) = \mathbf{D}(fg)$ by **(13.1.3)**. Hence, the first observation implies $f, g \notin \mathfrak{n}$ but $fg \in \mathfrak{n}$. Thus $\mathfrak{n}$ is not prime. $\square$

Lemma (16.50). — *Let X be a topological space, Y an irreducible subspace.*

(1) *Assume $Y = \bigcup_{i=1}^{n} Y_i$ with each Y_i closed in Y. Then $Y = Y_i$ for some i.*
(2) *Assume $Y \subset \bigcup_{i=1}^{n} X_i$ with each X_i closed in X. Then $Y \subset X_i$ for some i.*
(3) *Then the closure $\overline{Y}$ of Y is also irreducible.*
(4) *Then Y lies in an irreducible component of X.*
(5) *Then the irreducible components of X are closed, and cover X.*

Proof: For (1), induct on n. Assume $Y \neq Y_1$, else (1) holds. Then $n \geq 2$. Set $U := Y - Y_1$ and $V := Y - \bigcup_{i=2}^{n} Y_i$. Then U and V are open in Y, but don't meet. Also $U \neq \emptyset$. But Y is irreducible. So $V = \emptyset$. So $Y = \bigcup_{i=2}^{n} Y_i$. So by induction, $Y = Y_i$ for some $i \geq 2$. Thus (1) holds.

For (2), set $Y_i := Y \cap X_i$. Then each Y_i is closed in Y, and $Y = \bigcup_{i=1}^{n} Y_i$. So (1) implies $Y = Y_i$ for some i. Thus (2) holds.

For (3), let U, V be nonempty open sets of $\overline{Y}$. Then $U \cap Y$ and $V \cap Y$ are open in Y, and nonempty. But Y is irreducible. So $(U \cap Y) \bigcap (V \cap Y) \neq \emptyset$. So $U \cap V \neq \emptyset$. Thus (3) holds.

For (4), let $\mathcal{S}$ be the set of irreducible subspaces containing Y. Then $Y \in \mathcal{S}$, and $\mathcal{S}$ is partially ordered by inclusion. Given a totally ordered subset $\{Y_\lambda\}$ of $\mathcal{S}$, set $Y' := \bigcup_\lambda Y_\lambda$. Then Y' is irreducible: given nonempty open sets U, V of Y', there is λ with $U \cap Y_\lambda \neq \emptyset$ and $V \cap Y_\lambda \neq \emptyset$; so $(U \cap Y_\lambda) \bigcap (V \cap Y_\lambda) \neq \emptyset$ as Y_λ is irreducible; so $U \cap V \neq \emptyset$. Thus Zorn's Lemma yields (4).

For (5), note (3) implies the irreducible components are closed, as they're maximal. And (4) implies they cover, as every point is irreducible. Thus (4) holds. □

Exercise (16.51) . — Let R be a ring. Prove the following statements:

(1) $\mathfrak{a} \mapsto \mathbf{V}(\mathfrak{a}) = \operatorname{Spec}(R/\mathfrak{a})$ is an inclusion-reversing bijection β from the radical ideals $\mathfrak{a}$ of R onto the closed subspaces of $\operatorname{Spec}(R)$.
(2) β restricts to a bijection from the primes onto the irreducible closed subspaces.
(3) β restricts further to a bijection from the minimal primes onto the irreducible components.

Definition (16.52). — A topological space is said to be **Noetherian** if its closed subsets satisfy the dcc, or equivalently, if its open subsets satisfy the acc.

Lemma (16.53). — *Let X be a Noetherian space. Then X is quasi-compact, and every subspace Y is Noetherian.*

Proof: Given $X = \bigcup U_\lambda$ with the U_λ open, form the set of finite unions of the U_λ. Each such union is open, and X is Noetherian. So an adaptation of (16.4) yields a maximal element $V = \bigcup_{i=1}^{n} U_{\lambda_i}$. Then $V \cup U_\lambda = V$ for any U_λ. But every point of x lies in some U_λ. Hence $V = X$. Thus X is quasi-compact.

Let $C_0 \supset C_1 \supset \cdots$ be a descending chain of closed subsets of Y. Then their closures in X form a descending chain $\overline{C}_0 \supset \overline{C}_1 \supset \cdots$. It stabilizes, as X is Noetherian. But $\overline{C}_n \cap Y = C_n$ for all n. So $C_0 \supset C_1 \supset \cdots$ stabilizes too. Thus Y is Noetherian. □

Lemma (16.54). — *A nonempty Noetherian space X is the union of finitely many irreducible closed subspaces.*

Proof (Noetherian induction): Let $\mathcal{S}$ be the set of nonempty closed subspaces of X that are not the union of finitely many irreducible closed subspaces. Suppose $\mathcal{S} \neq \emptyset$. Since X is Noetherian, an adaptation of (**16.4**) yields a minimal element $Y \in \mathcal{S}$. Then Y is nonempty and reducible. So $Y = Y_1 \cup Y_2$ with each Y_i closed and $Y_i \subsetneqq Y$. By minimality, $Y_i \notin \mathcal{S}$. So Y_i is a finite union of irreducible closed subspaces. Hence Y is too, a contradiction. Thus $\mathcal{S} = \emptyset$, as desired. □

Proposition (16.55). — *Let X be a Noetherian space, X_λ for $\lambda \in \Lambda$ its distinct irreducible components, $\mu \in \Lambda$. Then Λ is finite, $X = \bigcup_{\lambda\in\Lambda} X_\lambda$, but $X \neq \bigcup_{\lambda\neq\mu} X_\lambda$.*

Proof: By (**16.54**), $X = \bigcup_{i=1}^n Y_i$ with each Y_i irreducible. By (**16.50**)(4), each Y_i lies in an irreducible component X_{λ_i} of X. Thus $X = \bigcup_{i=1}^n X_{\lambda_i} = \bigcup_{\lambda\in\Lambda} X_\lambda$.

So $X_\mu \subset \bigcup_{i=1}^n X_{\lambda_i}$. But the X_λ are closed by (**16.50**)(5). Hence $X_\mu \subset X_{\lambda_i}$ for some i by (**16.50**)(2). But X_μ is maximal irreducible. So $X_\mu = X_{\lambda_i}$. Thus Λ has at most n elements.

Finally, if $X = \bigcup_{\lambda\neq\mu} X_\lambda$, then the above reasoning yields $X_\mu = X_\lambda$ for $\lambda \neq \mu$, a contradiction. □

Exercise (16.56) . — Let R be a ring. Prove the following statements:

(1) $\mathrm{Spec}(R)$ is Noetherian if and only if the radical ideals satisfy the acc.
(2) If $\mathrm{Spec}(R)$ is Noetherian, then the primes satisfy the acc.
(3) If R is Noetherian, then $\mathrm{Spec}(R)$ is too.

Example (16.57). — In (**16.56**)(2), the converse is false.

For example, take $R := \mathbb{F}_2^{\mathbb{N}}$ where $\mathbb{N} := \{1, 2, 3, \dots\}$. Then R is Boolean by (**1.2**), so absolutely flat by (**10.26**)(1). So every prime is maximal by (**13.61**). Thus the primes trivially satisfy the acc.

Since R is Boolean, $f^n = f$ for all $f \in R$ and $n \geq 1$. So every ideal is radical. For each $m \in \mathbb{N}$, let $\mathfrak{a}_m$ be the set of vectors $(x_1, x_2, \dots)$ with $x_n = 0$ for $n \geq m$. The $\mathfrak{a}_m$ form an ascending chain of ideals, which doesn't stabilize. Thus the radical ideals do not satisfy the acc. Thus by (**16.56**)(1), $\mathrm{Spec}(R)$ is not Noetherian.

Example (16.58). — In (**16.56**)(3), the converse is false.

For example, take a field k and an infinite set $\mathcal{X}$ of variables. Set $P := k[\mathcal{X}]$ and $\mathfrak{m} := \langle\{\mathcal{X}\}\rangle$ and $R := P/\mathfrak{m}^2$. Given any prime $\mathfrak{p}$ of R containing $\mathfrak{m}^2$, note $\mathfrak{p} \supset \mathfrak{m}$ by (**2.23**). But $\mathfrak{m}$ is maximal by (**2.32**) with $R := k$ and $\mathfrak{p} := \langle 0\rangle$. So $\mathfrak{p} = \mathfrak{m}$. Thus $\mathfrak{m}/\mathfrak{m}^2$ is the only prime of R. Thus $\mathrm{Spec}(R)$ has one point, so is Noetherian.

However, $\mathfrak{m}/\mathfrak{m}^2$ is not finitely generated. Thus R is not Noetherian.

Proposition (16.59). — *Let $\varphi\colon R \to R'$ be a ring map. Assume that $\mathrm{Spec}(R')$ is Noetherian. Then φ has the Going-up Property if and only if $\mathrm{Spec}(\varphi)$ is closed.*

Proof: Set $\varphi^* := \mathrm{Spec}(\varphi)$. Recall from (**13.37**) that, if φ^* is closed, then φ has the Going-up Property, even if $\mathrm{Spec}(R')$ is not Noetherian.

Conversely, assume φ has the Going-up Property. Given a closed subset Y of $\mathrm{Spec}(R')$, we must show φ^*Y is closed.

Since $\mathrm{Spec}(R')$ is Noetherian, Y is too by (**16.53**). So $Y = \bigcup_{i=1}^n Y_i$ for some n and irreducible closed Y_i by (**16.54**). Then $\varphi^*Y = \bigcup_{i=1}^n \varphi^*Y_i$. So it suffices to show each φ^*Y_i is closed. Thus we may assume Y is irreducible and closed.

Then $Y = \mathrm{Spec}(R'/\mathfrak{q}')$ for some prime $\mathfrak{q}'$ of R' by (**16.51**)(2). Set $\mathfrak{q} := \varphi^{-1}\mathfrak{q}'$. Then $\varphi^*Y = \mathrm{Spec}(R/\mathfrak{q})$ by (**13.37**)(2). Thus φ^*Y is closed by (**13.1.7**). □

Definition (16.60). — A subset Y of a topological space is called **constructible** if $Y = \bigcup_{i=1}^n (U_i \cap C_i)$ for some n, open sets U_i, and closed sets C_i.

Exercise (16.61) . — Let X be a topological space, Y and Z constructible subsets, $\varphi\colon X' \to X$ a continuous map, $A \subset Z$ an arbitrary subset. Prove the following:

(1) Open and closed sets are constructible.
(2) $Y \cup Z$ and $Y \cap Z$ are constructible.
(3) $\varphi^{-1}Y$ is constructible in X'.
(4) A is constructible in Z if and only if A is constructible in X.

Lemma (16.62). — *Let X be a topological space, Y a constructible subset. Then its complement $X - Y$ is constructible.*

Proof: Say $Y = \bigcup_{i=1}^n (U_i \cap C_i)$ with U_i open and C_i closed. Set $V_i := X - C_i$ and $D_i := X - U_i$. Then V_i is open, D_i is closed, and $X - Y = \bigcap_{i=1}^n (V_i \cup D_i)$.

Induct on n. If $n = 0$, then $X - Y = X$. But X is plainly contructible.

Assume $n \geq 1$. Set $A := \bigcap_{i=1}^{n-1} (V_i \cup D_i)$. By induction, A is constructible. Now, V_n and D_n are constructible by **(16.61)**(1); so $V_n \cup D_n$ is too by **(16.61)**(2). But $X - Y = A \cap (V_n \cup D_n)$. Thus **(16.61)**(2) implies $X - Y$ is constructible. □

Proposition (16.63). — *Let X be a topological space, $\mathcal{F}$ the smallest family of subsets that contains all open sets and that is stable under finite intersection and under complement in X. Then $\mathcal{F}$ consists precisely of the constructible sets.*

Proof: Let $\mathcal{F}'$ be the family of all constructible sets. Then $\mathcal{F}'$ contains all open sets by **(16.61)**(1). It is stable under finite intersection by **(16.61)**(2) and induction. It is stable under complement in X by **(16.62)**. Thus $\mathcal{F}' \supset \mathcal{F}$.

Conversely, given $Y \in \mathcal{F}'$, say $Y = \bigcup_{i=1}^n (U_i \cap C_i)$ with U_i open and C_i closed. Set $Z_i := U_i \cap C_i$. Then $Y = X - \bigcap (X - Z_i)$. But U_i and $X - C_i$ are open, so lie in $\mathcal{F}$. So $C_i = X - (X - C_i) \in \mathcal{F}$. So $Z_i \in \mathcal{F}$. So $X - Z_i \in \mathcal{F}$. So $\bigcap (X - Z_i) \in \mathcal{F}$. Thus $Y \in \mathcal{F}$. Thus $\mathcal{F}' \subset \mathcal{F}$. Thus $\mathcal{F}' = \mathcal{F}$. □

Lemma (16.64). — *Let X be an irreducible topological space, Y a constructible subset. Then Y is dense in X if and only if Y contains a nonempty open set.*

Proof: First, assume Y contains a nonempty open set U. As X is irreducible, every nonempty open set V meets U. So V meets Y. Thus Y is dense in X.

Conversely, assume $\overline{Y} = X$. Say $Y = \bigcup_{i=1}^n (U_i \cap C_i)$ with U_i open and C_i closed. As X is irreducible, $X \neq \emptyset$. So $Y \neq \emptyset$. Discard U_i if $U_i = \emptyset$. Then $U_i \neq \emptyset$ for all i.

Note $\overline{Y} \subset \bigcup_{i=1}^n C_i$. Also $\overline{Y} = X$, and X is irreducible. So $X = C_i$ for some i by **(16.50)**(1). Hence $Y \supset U_i \cap C_i = U_i$. Thus Y contains a nonempty open set. □

Lemma (16.65). — *Let X be a Noetherian topological space. Then a subset Y is constructible if and only if this condition holds: given a closed irreducible subset Z of X, either $Y \cap Z$ isn't dense in Z or it contains a nonempty set that's open in Z.*

Proof: Assume Y is constructible. Given a closed irreducible subset Z of X, note $Y \cap Z$ is constructible in Z by **(16.61)**(1), (2), (4). If $Y \cap Z$ is dense in Z, then it contains a nonempty set that's open in Z by **(16.64)**. Thus the condition holds.

Conversely, assume the condition holds. Use Noetherian induction: form the set $\mathcal{S}$ of closed sets C with $Y \cap C$ not constructible (in X). Assume $\mathcal{S} \neq \emptyset$. As X is Noetherian, an adaptation of **(16.4)** yields a minimal element $Z \in \mathcal{S}$.

Note that $Z \neq \emptyset$ as $Y \cap Z$ is not constructible.

Suppose $Z = Z_1 \cup Z_2$ with each Z_i closed and $Z_i \subsetneqq Z$. By minimality, $Z_i \notin \mathcal{S}$. So $Y \cap Z_i$ is constructible. But $Y \cap Z = (Y \cap Z_1) \cup (Y \cup Z_2)$. So (**16.61**)(2) implies $Y \cap Z$ is constructible, a contradiction. Thus Z is irreducible.

Assume $Y \cap Z$ isn't dense in Z, and let A be its closure. Then $A \subsetneqq Z$. So $A \notin \mathcal{S}$. So $Y \cap A$ is constructible. But $Y \cap Z \subset Y \cap A \subset Y \cap Z$, so $Y \cap A = Y \cap Z$. Thus $Y \cap Z$ is constructible, a contradiction. Thus $Y \cap Z$ is dense in Z.

So by the condition, $Y \cap Z$ contains a nonempty set U that's open in Z. So by definition of the topology on Z, we have $U = V \cap Z$ where V is open in X. But Z is closed in X. Thus U is constructible in X.

Set $B := Z - U$. Then B is closed in Z, so in X. Also $B \subsetneqq Z$. So $B \notin \mathcal{S}$. So $Y \cap B$ is constructible. But $Y \cap Z = (Y \cap B) \cup U$. So (**16.61**)(2) implies $Y \cap Z$ is constructible, a contradiction. Thus $\mathcal{S} = \emptyset$. Thus Y is constructible. □

Theorem (16.66) (Chevalley's)**. —** *Let $\varphi\colon R \to R'$ be a map of rings. Assume R is Noetherian and R' is algebra finite over R. Set $X := \operatorname{Spec}(R)$ and $X' := \operatorname{Spec}(R')$ and $\varphi^* := \operatorname{Spec}(\varphi)$. Let $Y' \subset X'$ be constructible. Then $\varphi^* Y' \subset X$ is constructible.*

Proof: Say that $Y' = \bigcup_{i=1}^n (U_i' \cap C_i')$ where U_i' is open and that C_i' is closed. Then $\varphi^* Y' = \bigcup \varphi^*(U_i' \cap C_i')$. So by (**16.61**)(2) it suffices to show each $\varphi^*(U_i' \cap C_i')$ is constructible. So assume $Y' = U' \cap C'$ with U' open and C' closed.

Since R is Noetherian and R' is algebra finite, R' is Noetherian by (**16.10**). Thus (**16.56**)(3) implies X and X' are Noetherian.

Since X is Noetherian, let's use (**16.65**) to show $\varphi^* Y'$ is constructible. Given a closed irreducible subset Z of X such that $(\varphi^* Y') \cap Z$ is dense in Z, set $Z' := \varphi^{*-1} Z$. Then $(\varphi^* Y') \cap Z = \varphi^*(Y' \cap Z')$. Set $D' := C' \cap Z'$. Then $Y' \cap Z' = U' \cap D'$. We have to see that $\varphi^*(U' \cap D')$ contains a nonempty set that's open in Z.

Owing to (**16.51**)(2), (1), there's a prime $\mathfrak{p}$ of R and a radical ideal $\mathfrak{a}'$ of R' such that $Z = \mathbf{V}(\mathfrak{p})$ and $D' = \mathbf{V}(\mathfrak{a}')$; moreover, $\mathfrak{p}$ and $\mathfrak{a}'$ are uniquely determined. Since $\varphi^*(U' \cap D')$ is dense in Z, so is $\varphi^* D'$. So $Z = \mathbf{V}(\varphi^{-1}\mathfrak{a}')$ owing to (**13.36**)(1). But $\varphi^{-1}\mathfrak{a}'$ is radical. Thus $\varphi^{-1}\mathfrak{a}' = \mathfrak{p}$.

So φ induces an injection $\psi\colon R/\mathfrak{p} \hookrightarrow R'/\mathfrak{a}'$. Further, $R/\mathfrak{p}$ is Noetherian by (**16.7**), and plainly, $R'/\mathfrak{a}'$ is algebra finite over $R/\mathfrak{p}$. But $Z = \operatorname{Spec}(R/\mathfrak{p})$ and $D' = \operatorname{Spec}(R'/\mathfrak{a}')$ by (**13.1.7**). Replace φ and Y' by ψ and $U' \cap D'$. Then ψ is injective, R is a domain, and Y' is an open set of X' such that $\varphi^* Y'$ is dense in X. We have to see that $\varphi^* Y'$ contains a nonempty set that's open in X.

By (**13.1**), the principal open sets $D(f')$ with $f' \in R'$ form a basis for the topology of X'. Since X' is Noetherian, Y' is too by (**16.53**); so Y' is quasi-compact again by (**16.53**). Thus $Y' = \bigcup_{j=1}^m D(f_j')$ for some m and $f_j' \in R'$. So $\varphi^* Y' = \bigcup_{j=1}^m \varphi^* D(f_j')$. But $\varphi^* Y'$ is dense in X. Thus $\bigcup_{j=1}^m \overline{\varphi^* D(f_j')} = X$.

However, X is irreducible. So $\overline{\varphi^* D(f_j')} = X$ for some j by (**16.50**)(1). But $D(f_j') = \operatorname{Spec}(R'_{f_j'})$ by (**13.1.8**). So the composition $R \to R' \to R'_{f_j'}$ is injective by (**13.36**)(2). Plainly, $R'_{f_j'}$ is algebra finite over R. Hence $\varphi^* D(f_j')$ contains a nonempty set V that's open in X by (**15.18**). Then $V \subset \varphi^* Y'$, as desired. □

D. Appendix: Exercises

Exercise (16.67) . — Find a non-Noetherian ring R with $R_{\mathfrak{p}}$ Noetherian for every prime $\mathfrak{p}$.

Exercise (16.68) . — Describe $\operatorname{Spec}(\mathbb{Z}[X])$.

Exercise (16.69) . — What are the irreducible components of a Hausdorff space?

Exercise (16.70) . — Are these conditions on a topological space X equivalent?

(1) X is Noetherian.
(2) Every subspace Y is quasi-compact.
(3) Every open subspace V is quasi-compact.

Exercise (16.71) . — Let $\varphi\colon R \to R'$ a map of rings. Assume R' is algebra finite over R. Show that the fibers of $\operatorname{Spec}(\varphi)$ are Noetherian subspaces of $\operatorname{Spec}(R')$.

Exercise (16.72) . — Let M be a Noetherian module over a ring R. Show that $\operatorname{Supp}(M)$ is a closed Noetherian subspace of $\operatorname{Spec}(R)$. Conclude that M has only finitely many minimal primes.

Exercise (16.73) . — Let X be a Noetherian topological space. Then a subset U is open if and only if this condition holds: given a closed irreducible subset Z of X, either $U \cap Z$ is empty or it contains a nonempty subset that's open in Z.

Exercise (16.74) . — Let $\varphi\colon R \to R'$ a map of rings. Assume R is Noetherian and R' is algebra finite over R. Set $X := \operatorname{Spec}(R)$, set $Y := \operatorname{Spec}(R')$, and set $\varphi^* := \operatorname{Spec}(\varphi)$. Prove that φ^* is open if and only if it has the Going-down Property.

Exercise (16.75) . — Let $\varphi\colon R \to R'$ a map of rings, M' a finitely generated R'-module. Assume R is Noetherian, R' is algebra finite, and M' is flat over R. Show $\operatorname{Spec}(\varphi)$ is open.

17. Associated Primes

Given a module, a prime is **associated** to it if the prime is equal to the annihilator of an element. Given a subset of the set of all associated primes, we prove there is a submodule whose own associated primes constitute that subset. If the ring is Noetherian, then the set of annihilators of elements has maximal members; we prove the latter are prime, so associated. Assume just the module is Noetherian. Then the union of all the associated primes is the set of zerodivisors on the module, and the intersection is the set of nilpotents. Furthermore, there is then a finite chain of submodules whose successive quotients are cyclic with prime annihilators; these primes include all associated primes, which are, therefore, finite in number.

A. Text

Definition (17.1). — Let R be a ring, M a module. A prime ideal $\mathfrak{p}$ is said to be **associated** to M, or simply a **prime of** M, if there is a (nonzero) $m \in M$ with $\mathfrak{p} = \mathrm{Ann}(m)$. The set of associated primes is denoted by $\mathrm{Ass}(M)$ or $\mathrm{Ass}_R(M)$.

A $\mathfrak{p} \in \mathrm{Ass}(M)$ is said to be **embedded** if it properly contains a $\mathfrak{q} \in \mathrm{Ass}(M)$.

Warning: following an old custom, by the **associated primes of** a proper ideal $\mathfrak{a}$, we mean not those of $\mathfrak{a}$ viewed as an abstract module, but rather those of $R/\mathfrak{a}$; however, by the **associated primes** of R, we do mean those of R viewed as an abstract module.

Example (17.2). — Here's an example of a local ring R whose maximal ideal $\mathfrak{m}$ is an embedded (associated) prime. Let k be a field, and X, Y variables. Set $P := k[[X, Y]]$ and $\mathfrak{n} := \langle X, Y\rangle$. By **(3.7)**, P is a local ring with maximal ideal $\mathfrak{n}$.

Set $\mathfrak{a} := \langle XY, Y^2\rangle$. Set $R := P/\mathfrak{a}$ and $\mathfrak{m} := \mathfrak{n}/\mathfrak{a}$. Then R is local with maximal ideal $\mathfrak{m}$. Let $x, y \in R$ be the residues of X, Y. Then $x, y \in \mathrm{Ann}(y) \subset \mathfrak{m} = \langle x, y\rangle$. So $\mathfrak{m} = \mathrm{Ann}(y)$. Thus $\mathfrak{m} \in \mathrm{Ass}(R)$.

Note $y \in \mathrm{Ann}(x)$. Given $\sum_{ij} a_{ij}x^iy^j \in \mathrm{Ann}(x)$, note $\sum_i a_{i0}x^{i+1} = 0$. Hence $\sum_i a_{i0}X^{i+1} \in \mathfrak{a}$. So $\sum_i a_{i0}X^{i+1} = 0$. So $\sum_{ij} a_{ij}x^iy^j \in \langle y\rangle$. Thus $\langle y\rangle = \mathrm{Ann}(x)$.

Plainly, $Y \in P$ is a prime element; so $\langle Y\rangle \subset P$ is a prime ideal by **(2.5)**; so $\langle y\rangle \subset R$ is a prime ideal by **(2.7)**. Thus $\langle y\rangle \in \mathrm{Ass}(x)$. Thus $\mathfrak{m}$ is embedded.

Proposition (17.3). — *Let R be a ring, M a module, and $\mathfrak{p}$ a prime ideal. Then $\mathfrak{p} \in \mathrm{Ass}(M)$ if and only if there is an R-injection $R/\mathfrak{p} \hookrightarrow M$.*

Proof: Assume $\mathfrak{p} = \mathrm{Ann}(m)$ with $m \in M$. Define a map $R \to M$ by $x \mapsto xm$. This map induces an R-injection $R/\mathfrak{p} \hookrightarrow M$.

Conversely, suppose there is an R-injection $R/\mathfrak{p} \hookrightarrow M$, and let $m \in M$ be the image of 1. Then $\mathfrak{p} = \mathrm{Ann}(m)$, so $\mathfrak{p} \in \mathrm{Ass}(M)$. □

Exercise (17.4) . — Let R be a ring, M a module, $\mathfrak{a} \subset \mathrm{Ann}(M)$ an ideal. Set $R' := R/\mathfrak{a}$. Let $\kappa\colon R \twoheadrightarrow R'$ be the quotient map. Show that $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ is a bijection from $\mathrm{Ass}_R(M)$ to $\mathrm{Ass}_{R'}(M)$ with inverse $\mathfrak{p}' \mapsto \kappa^{-1}(\mathfrak{p}')$.

Lemma (17.5). — *Let R be a ring, $\mathfrak{p}$ a prime ideal, $m \in R/\mathfrak{p}$ a nonzero element. Then* (1) $\mathrm{Ann}(m) = \mathfrak{p}$ *and* (2) $\mathrm{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$.

Proof: To prove (1), say m is the residue of $y \in R$. Let $x \in R$. Then $xm = 0$ if and only if $xy \in \mathfrak{p}$, so if and only if $x \in \mathfrak{p}$, as $\mathfrak{p}$ is prime and $m \neq 0$. Thus (1) holds.

Trivially, (1) implies (2). $\square$

Proposition (17.6). — *Let M be a module, N a submodule. Then*

$$\mathrm{Ass}(N) \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(M/N).$$

Proof: Take $m \in N$. Then the annihilator of m is the same whether m is regarded as an element of N or of M. So $\mathrm{Ass}(N) \subset \mathrm{Ass}(M)$.

Let $\mathfrak{p} \in \mathrm{Ass}(M)$. Then **(17.3)** yields an R-injection $R/\mathfrak{p} \hookrightarrow M$. Denote its image by E. If $E \cap N = 0$, then the composition $R/\mathfrak{p} \to M \to M/N$ is injective; hence, $\mathfrak{p} \in \mathrm{Ass}(M/N)$ by **(17.3)**. Else, take a nonzero $m \in E \cap N$. Then $\mathrm{Ann}(m) = \mathfrak{p}$ by **(17.5)**(1). Thus $\mathfrak{p} \in \mathrm{Ass}(N)$. $\square$

Proposition (17.7). — *Let M be a module, and Ψ a subset of* $\mathrm{Ass}(M)$. *Then there is a submodule N of M with* $\mathrm{Ass}(M/N) = \Psi$ *and* $\mathrm{Ass}(N) = \mathrm{Ass}(M) - \Psi$.

Proof: Given submodules N_λ of M totally ordered by inclusion, set $N := \bigcup N_\lambda$. Given $\mathfrak{p} \in \mathrm{Ass}(N)$, say $\mathfrak{p} = \mathrm{Ann}(m)$. Then $m \in N_\lambda$ for some λ; so $\mathfrak{p} \in \mathrm{Ass}(N_\lambda)$. Conversely, $\mathrm{Ass}(N_\lambda) \subset \mathrm{Ass}(N)$ for all λ by **(17.6)**. Thus $\mathrm{Ass}(N) = \bigcup \mathrm{Ass}(N_\lambda)$.

So we may apply Zorn's Lemma to obtain a submodule N of M that is maximal with $\mathrm{Ass}(N) \subset \mathrm{Ass}(M) - \Psi$. By **(17.6)**, it suffices to show that $\mathrm{Ass}(M/N) \subset \Psi$.

Take $\mathfrak{p} \in \mathrm{Ass}(M/N)$. Then M/N has a submodule N'/N isomorphic to $R/\mathfrak{p}$ by **(17.3)**. So $\mathrm{Ass}(N') \subset \mathrm{Ass}(N) \cup \{\mathfrak{p}\}$ by **(17.6)** and **(17.5)**(2). Now, $N' \supsetneqq N$ and N is maximal with $\mathrm{Ass}(N) \subset \mathrm{Ass}(M) - \Psi$. Hence $\mathfrak{p} \in \mathrm{Ass}(N') \subset \mathrm{Ass}(M)$, but $\mathfrak{p} \notin \mathrm{Ass}(M) - \Psi$. Thus $\mathfrak{p} \in \Psi$. $\square$

Proposition (17.8). — *Let R be a ring, S a multiplicative subset, M a module, and $\mathfrak{p}$ a prime ideal. If $\mathfrak{p} \cap S = \emptyset$ and $\mathfrak{p} \in \mathrm{Ass}(M)$, then $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$; the converse holds if $\mathfrak{p}$ is finitely generated modulo* $\mathrm{Ann}(M)$.

Proof: Assume $\mathfrak{p} \in \mathrm{Ass}(M)$. Then **(17.3)** yields an injection $R/\mathfrak{p} \hookrightarrow M$. It induces an injection $S^{-1}(R/\mathfrak{p}) \hookrightarrow S^{-1}M$ by **(12.13)**. But $S^{-1}(R/\mathfrak{p}) = S^{-1}R/S^{-1}\mathfrak{p}$ by **(12.15)**. Assume $\mathfrak{p} \cap S = \emptyset$ also. Then $\mathfrak{p}S^{-1}R$ is prime by **(11.11)**(3)(b). But $\mathfrak{p}S^{-1}R = S^{-1}\mathfrak{p}$ by **(12.2)**. Thus $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$.

Conversely, assume $S^{-1}\mathfrak{p} \in \mathrm{Ass}(S^{-1}M)$. Then there are $m \in M$ and $t \in S$ with $S^{-1}\mathfrak{p} = \mathrm{Ann}(m/t)$. Set $\mathfrak{a} := \mathrm{Ann}(M)$. Assume there are $x_1, \dots, x_n \in \mathfrak{p}$ whose residues generate $(\mathfrak{a} + \mathfrak{p})/\mathfrak{a}$. Fix i. Then $x_i m/t = 0$. So there is $s_i \in S$ with $s_i x_i m = 0$. Set $s := \prod s_i$ and $\mathfrak{b} := \mathrm{Ann}(sm)$. Then $x_i \in \mathfrak{b}$. Given $x \in \mathfrak{p}$, say $x = a + \sum a_i x_i$ with $a \in \mathfrak{a}$ and $a_i \in R$. Then a, $x_i \in \mathfrak{b}$. So $x \in \mathfrak{b}$. Thus $\mathfrak{p} \subset \mathfrak{b}$.

Take $b \in \mathfrak{b}$. Then $bsm/st = 0$. So $b/1 \in S^{-1}\mathfrak{p}$. So $b \in \mathfrak{p}$ by **(11.11)**(2)(b) and **(11.11)**(3)(a). Thus $\mathfrak{p} \supset \mathfrak{b}$. So $\mathfrak{p} = \mathfrak{b} := \mathrm{Ann}(sm)$. Thus $\mathfrak{p} \in \mathrm{Ass}(M)$.

Finally, $\mathfrak{p} \cap S = \emptyset$ by **(11.12)**(2), as $S^{-1}\mathfrak{p}$ is prime. $\square$

Lemma (17.9). — *Let R be a ring, M a module, and $\mathfrak{p}$ an ideal. Suppose $\mathfrak{p}$ is maximal in the set of annihilators of nonzero elements m of M. Then $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Proof: Say $\mathfrak{p} := \mathrm{Ann}(m)$ with $m \neq 0$. Then $1 \notin \mathfrak{p}$ as $m \neq 0$. Now, take $b, c \in R$ with $bc \in \mathfrak{p}$, but $c \notin \mathfrak{p}$. Then $bcm = 0$, but $cm \neq 0$. Plainly, $\mathfrak{p} \subset \mathrm{Ann}(cm)$. So $\mathfrak{p} = \mathrm{Ann}(cm)$ by maximality. But $b \in \mathrm{Ann}(cm)$, so $b \in \mathfrak{p}$. Thus $\mathfrak{p}$ is prime. $\square$

Proposition (17.10). — *Let R be a ring, M a module. Assume R is Noetherian, or assume M is Noetherian. Then $M = 0$ if and only if $\mathrm{Ass}(M) = \emptyset$.*

Proof: Plainly, if $M = 0$, then $\mathrm{Ass}(M) = \emptyset$. For the converse, assume $M \neq 0$.

First, assume R is Noetherian. Let $\mathcal{S}$ be the set of annihilators of nonzero elements of M. Then $\mathcal{S}$ has a maximal element $\mathfrak{p}$ by **(16.5)**. By **(17.9)**, $\mathfrak{p} \in \mathrm{Ass}(M)$.

Second, assume M is Noetherian. Set $R' := R/\mathrm{Ann}(M)$. Then R' is Noetherian by **(16.16)**. By the above, $\mathrm{Ass}_{R'}(M) \neq \emptyset$. So **(17.4)** yields $\mathrm{Ass}_R(M) \neq \emptyset$. □

(17.11) (Zerodivisors). — Let R be a ring, M a module, $x \in R$. We say x is a **zerodivisor** on M if there is a nonzero $m \in M$ with $xm = 0$; otherwise, we say x is a **nonzerodivisor**. We denote the set of zerodivisors by $\mathrm{z.div}(M)$ or $\mathrm{z.div}_R(M)$.

Plainly the set of nonzerodivisors on M is a saturated multiplicative subset of R.

Assume $M \neq 0$. Given $x \in \mathrm{nil}(M)$, take $n \geq 1$ minimal with $x^n \in \mathrm{Ann}(M)$. Then there's $m \in M$ with $x^{n-1}m \neq 0$. But $x(x^{n-1}m) = 0$. Thus

$$\mathrm{nil}(M) \subset \mathrm{z.div}(M). \tag{17.11.1}$$

Proposition (17.12). — *Let R be a ring, M a module. Assume R is Noetherian, or assume M is Noetherian. Then* $\mathrm{z.div}(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$.

Proof: Given $x \in \mathrm{z.div}(M)$, there exists a nonzero $m \in M$ with $xm = 0$. Then $x \in \mathrm{Ann}(m)$. Assume R is Noetherian. Then $\mathrm{Ann}(m)$ lies in an ideal $\mathfrak{p}$ maximal among annihilators of nonzero elements because of **(16.5)**; hence, $\mathfrak{p} \in \mathrm{Ass}(M)$ by **(17.9)**. Thus $\mathrm{z.div}(M) \subset \bigcup \mathfrak{p}$. The opposite inclusion results from the definitions.

Assume instead M is Noetherian. By **(16.16)**, $R' := R/\mathrm{Ann}(M)$ is Noetherian. So by the above, $\mathrm{z.div}_{R'}(M) = \bigcup_{\mathfrak{p}' \in \mathrm{Ass}(M)} \mathfrak{p}'$. Let $\kappa\colon R \twoheadrightarrow R'$ be the quotient map. Given $x \in R$ and $m \in M$, note $xm = \kappa(x)m$; so $\kappa^{-1}(\mathrm{z.div}_{R'}(M)) = \mathrm{z.div}_R(M)$. But $\kappa^{-1}\bigcup \mathfrak{p}' = \bigcup \kappa^{-1}\mathfrak{p}'$. Thus **(17.4)** yields $\mathrm{z.div}_R(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(M)} \mathfrak{p}$. □

Lemma (17.13). — *Let M be a module. Then*

$$\mathrm{Ass}(M) \subset \bigcup\nolimits_{\mathfrak{q} \in \mathrm{Ass}(M)} \boldsymbol{V}(\mathfrak{q}) \subset \mathrm{Supp}(M) \subset \boldsymbol{V}(\mathrm{Ann}(M)).$$

Proof: First, $\mathrm{Ass}(M) \subset \bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \mathbf{V}(\mathfrak{q})$ as $\mathfrak{q} \in \mathbf{V}(\mathfrak{q})$.

Next, fix $\mathfrak{q} \in \mathrm{Ass}(M)$ and $\mathfrak{p} \in \mathbf{V}(\mathfrak{q})$. Say $\mathfrak{q} = \mathrm{Ann}(m)$. Then $m/1 \neq 0$ in $M_\mathfrak{p}$; else, there's $x \in R - \mathfrak{p}$ with $xm = 0$, and so $x \in \mathrm{Ann}(m) = \mathfrak{q} \subset \mathfrak{p}$, a contradiction. Thus $\mathfrak{p} \in \mathrm{Supp}(M)$. Thus $\bigcup_{\mathfrak{q} \in \mathrm{Ass}(M)} \mathbf{V}(\mathfrak{q}) \subset \mathrm{Supp}(M)$.

Finally, **(13.4)**(3) asserts $\mathrm{Supp}(M) \subset \mathbf{V}(\mathrm{Ann}(M))$. □

Theorem (17.14). — *Let R be a ring, M a module, $\mathfrak{p} \in \mathrm{Supp}(M)$. Assume R is Noetherian, or assume M is Noetherian. Then $\mathfrak{p}$ contains some $\mathfrak{q} \in \mathrm{Ass}(M)$; if $\mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$, then $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Proof: Assume R is Noetherian. Then $R_\mathfrak{p}$ is too by **(16.7)**. But $M_\mathfrak{p} \neq 0$. So there's $\mathfrak{Q} \in \mathrm{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p})$ by **(17.10)**. Set $\mathfrak{q} := \varphi_{S_\mathfrak{p}}^{-1}\mathfrak{Q}$. Then $\mathfrak{q}R_\mathfrak{p} = \mathfrak{Q}$ by **(11.12)**(2). As R is Noetherian, $\mathfrak{q}$ is finitely generated. So $\mathfrak{q} \in \mathrm{Ass}(M)$ by **(17.8)**. But $\mathfrak{q} \cap S_\mathfrak{p} = \emptyset$ and $S_\mathfrak{p} := R - \mathfrak{p}$. Thus $\mathfrak{q} \subset \mathfrak{p}$, as desired.

Next, assume M is Noetherian. Then M is finitely generated. So **(13.4)**(3) gives $\mathrm{Supp}_R(M) = \mathbf{V}(\mathrm{Ann}_R(M))$. So $\mathfrak{p} \supset \mathrm{Ann}_R(M)$. Set $R' := R/\mathrm{Ann}_R(M)$, and set $\mathfrak{p}' := \mathfrak{p}/\mathrm{Ann}_R(M)$. Then $\mathfrak{p}' \supset \mathrm{Ann}_{R'}(M) = 0$. So **(13.4)**(3) gives $\mathfrak{p}' \in \mathrm{Supp}_{R'}(M)$.

Moreover, R' is Noetherian by **(16.16)**. So by the first paragraph, $\mathfrak{p}'$ contains some $\mathfrak{q}' \in \mathrm{Ass}_{R'}(M)$. Let $\kappa\colon R \twoheadrightarrow R'$ be the quotient map. Set $\mathfrak{q} := \kappa^{-1}\mathfrak{q}'$. Thus $\mathfrak{p} \supset \mathfrak{q}$, and **(17.4)** yields $\mathfrak{q} \in \mathrm{Ass}(M)$, as desired.

Finally, $\mathfrak{q} \in \mathrm{Supp}(M)$ by **(17.13)**. Thus $\mathfrak{p} = \mathfrak{q} \in \mathrm{Ass}(M)$ if $\mathfrak{p}$ is minimal. □

Theorem (17.15). — *Let M be a Noetherian module. Then*

$$\mathrm{nil}(M) = \textstyle\bigcap_{\mathfrak{p}\in\mathrm{Ass}(M)} \mathfrak{p}.$$

Proof: Since M is finitely generated, $\mathrm{nil}(M) = \bigcap_{\mathfrak{p}\in\mathrm{Supp}(M)} \mathfrak{p}$ by (**13.6**). Since M is Noetherian, given $\mathfrak{p} \in \mathrm{Supp}(M)$, there is $\mathfrak{q} \in \mathrm{Ass}(M)$ with $\mathfrak{q} \subset \mathfrak{p}$ by (**17.14**). The assertion follows. □

Lemma (17.16). — *Let R be a ring, M a nonzero Noetherian module. Then there exists a finite chain of submodules*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$$

with $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for some prime $\mathfrak{p}_i$ for $i = 1, \ldots, n$. For any such chain,

$$\mathrm{Ass}(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset \mathrm{Supp}(M). \tag{17.16.1}$$

Proof: There are submodules of M having such a chain by (**17.10**). So there's a maximal such submodule N by (**16.11**). Suppose submodule N'/N isomorphic to $R/\mathfrak{p}$ for some prime $\mathfrak{p}$. Then $N \subsetneqq N'$, contradicting maximality. Hence $N = M$. Thus a chain exists.

The first inclusion of (**17.16.1**) follows by induction from (**17.6**) and (**17.5**)(2). Now, $\mathfrak{p}_i \in \mathrm{Supp}(R/\mathfrak{p}_i)$ by (**13.4**)(3) with $M := R/\mathfrak{p}_i$. Thus (**13.4**)(1) yields (**17.16.1**). □

Theorem (17.17). — *Let M be a Noetherian module. Then $\mathrm{Ass}(M)$ is finite.*

Proof: The assertion follows directly from (**17.16**). □

Proposition (17.18). — *Let R be a ring, M and N modules. Assume that M is Noetherian. Then* $\mathrm{Ass}(\mathrm{Hom}(M, N)) = \mathrm{Supp}(M) \bigcap \mathrm{Ass}(N)$.

Proof: Set $\mathfrak{a} := \mathrm{Ann}(M)$ and $N' := \{\, n \in N \mid \mathfrak{a}n = 0 \,\}$. Then $\mathrm{Hom}(M, N')$ lies in $\mathrm{Hom}(M, N)$. Conversely, given $\alpha\colon M \to N$ and $m \in M$, plainly $\mathfrak{a}(\alpha(m)) = 0$; so $\alpha(M) \subset N'$. Thus $\mathrm{Hom}(M, N) = \mathrm{Hom}(M, N')$.

Let's see that $\mathrm{Supp}(M) \bigcap \mathrm{Ass}(N) = \mathrm{Ass}(N')$ by double inclusion. First, given $\mathfrak{p} \in \mathrm{Supp}(M) \bigcap \mathrm{Ass}(N)$, say $\mathfrak{p} = \mathrm{Ann}(n)$ for $n \in N$. But $\mathrm{Supp}(M) \subset \mathbf{V}(\mathfrak{a})$ by (**13.4**)(3); so $\mathfrak{p} \supset \mathfrak{a}$. Hence $\mathfrak{a}n = 0$. So $n \in N'$. Thus $\mathfrak{p} \in \mathrm{Ass}(N')$.

Conversely, given $\mathfrak{p} \in \mathrm{Ass}(N')$, say $\mathfrak{p} = \mathrm{Ann}(n)$ for $n \in N'$. Then $\mathfrak{a}n = 0$. So $\mathfrak{p} \supset \mathfrak{a}$. But $\mathrm{Supp}(M) = \mathbf{V}(\mathfrak{a})$ by (**13.4**)(3) as M is Noetherian. So $\mathfrak{p} \in \mathrm{Supp}(M)$. But $n \in N' \subset N$. Thus $\mathfrak{p} \in \mathrm{Ass}(N)$. Thus $\mathrm{Supp}(M) \bigcap \mathrm{Ass}(N) = \mathrm{Ass}(N')$.

Thus we have to prove

$$\mathrm{Ass}(\mathrm{Hom}(M, N')) = \mathrm{Ass}(N'). \tag{17.18.1}$$

Set $R' := R/\mathfrak{a}$. Plainly $\mathrm{Hom}_{R'}(M, N') = \mathrm{Hom}_R(M, N')$. Let $\kappa\colon R \twoheadrightarrow R'$ be the quotient map. Owing to (**17.4**), $\mathfrak{p}' \mapsto \kappa^{-1}(\mathfrak{p}')$ sets up two bijections: one from $\mathrm{Ass}_{R'}(\mathrm{Hom}_{R'}(M, N'))$ to $\mathrm{Ass}_R(\mathrm{Hom}_R(M, N'))$, and one from $\mathrm{Ass}_{R'}(N')$ to $\mathrm{Ass}_R(N')$. Thus we may replace R by R'. Then by (**16.16**), R is Noetherian.

Given $\mathfrak{p} \in \mathrm{Ass}\big(\mathrm{Hom}(M, N')\big)$, there's an R-injection $R/\mathfrak{p} \hookrightarrow \mathrm{Hom}(M, N')$ by (**17.3**). Set $k(\mathfrak{p}) := \mathrm{Frac}(R/\mathfrak{p})$. Then $k(\mathfrak{p}) = (R/\mathfrak{p})_{\mathfrak{p}}$ by (**12.16**). But, R is Noetherian, so M is finitely presented by (**16.15**); so by (**12.19**),

$$\mathrm{Hom}_R(M, N')_{\mathfrak{p}} = \mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N'_{\mathfrak{p}}). \tag{17.18.2}$$

Hence, by exactness, localizing yields an injection $\varphi\colon k(\mathfrak{p}) \hookrightarrow \mathrm{Hom}_{R_{\mathfrak{p}}}(M_{\mathfrak{p}}, N'_{\mathfrak{p}})$.

For any $m \in M_{\mathfrak{p}}$ with $\varphi(1)(m) \neq 0$, the map $k(\mathfrak{p}) \to N'_{\mathfrak{p}}$ given by $x \mapsto \varphi(x)(m)$

is nonzero, so an injection. But $k(\mathfrak{p}) = R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$ by (**12.16**). Hence by (**17.3**), we have $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(N'_\mathfrak{p})$. Thus by (**17.8**) also $\mathfrak{p} \in \operatorname{Ass}(N')$.

Conversely, given $\mathfrak{p} \in \operatorname{Ass}(N')$, recall from the third paragraph that $\mathfrak{p} \in \operatorname{Supp}(M)$. So $M_\mathfrak{p} \neq 0$. So by Nakayama's Lemma, $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ is a nonzero vector space over $k(\mathfrak{p})$. Take any nonzero R-map $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p} \to k(\mathfrak{p})$, precede it by the quotient map $M_\mathfrak{p} \to M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$, and follow it by an R-injection $k(\mathfrak{p}) \hookrightarrow N'_\mathfrak{p}$; the latter exists by (**17.3**) and (**17.8**) since $\mathfrak{p} \in \operatorname{Ass}(N')$.

We obtain a nonzero element of $\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N'_\mathfrak{p})$, annihilated by $\mathfrak{p}R_\mathfrak{p}$. But $\mathfrak{p}R_\mathfrak{p}$ is maximal; so the annihilator is too. So $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}\big(\operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N'_\mathfrak{p})\big)$ by (**17.9**). So $\mathfrak{p} \in \operatorname{Ass}(\operatorname{Hom}(M, N'))$ by (**17.18.2**) and (**17.8**). Thus (**17.18.1**) holds. □

Proposition (17.19). — *Let R be a ring, M a Noetherian module, $\mathfrak{p}$ a prime, $x, y \in \mathfrak{p} - \operatorname{z.div}(M)$. Assume $\mathfrak{p} \in \operatorname{Ass}(M/xM)$. Then $\mathfrak{p} \in \operatorname{Ass}(M/yM)$.*

Proof: Form the sequence $0 \to K \to M/xM \xrightarrow{\mu_y} M/xM$ with $K := \operatorname{Ker}(\mu_y)$. Apply the functor $\operatorname{Hom}(R/\mathfrak{p}, \bullet)$ to that sequence, and get the following one:

$$0 \to \operatorname{Hom}(R/\mathfrak{p}, K) \to \operatorname{Hom}(R/\mathfrak{p}, M/xM) \xrightarrow{\mu_y} \operatorname{Hom}(R/\mathfrak{p}, M/xM).$$

It is exact by (**5.11**)(2). But $y \in \mathfrak{p}$; so the right-hand map vanishes. Thus

$$\operatorname{Hom}(R/\mathfrak{p}, K) \xrightarrow{\sim} \operatorname{Hom}(R/\mathfrak{p}, M/xM).$$

Form the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 \to & M & \xrightarrow{\mu_x} & M & \to & M/xM & \to 0 \\ & {\scriptstyle\mu_y}\downarrow & & {\scriptstyle\mu_y}\downarrow & & {\scriptstyle\mu_y}\downarrow & \\ 0 \to & M & \xrightarrow{\mu_x} & M & \to & M/xM & \to 0 \end{array}$$

The Snake Lemma (**5.10**) yields an exact sequence $0 \to K \to M/yM \xrightarrow{\mu_x} M/yM$ as $\operatorname{Ker}(\mu_y|M) = 0$. Hence, similarly, $\operatorname{Hom}(R/\mathfrak{p}, K) \xrightarrow{\sim} \operatorname{Hom}(R/\mathfrak{p}, M/yM)$. Hence,

$$\operatorname{Hom}(R/\mathfrak{p}, M/yM) = \operatorname{Hom}(R/\mathfrak{p}, M/xM). \qquad \textbf{(17.19.1)}$$

Assume for a moment that R is Noetherian. Then (**17.18**) yields

$$\operatorname{Ass}(\operatorname{Hom}(R/\mathfrak{p}, M/xM)) = \operatorname{Supp}(R/\mathfrak{p}) \bigcap \operatorname{Ass}(M/xM). \qquad \textbf{(17.19.2)}$$

But $\mathfrak{p} \in \operatorname{Supp}(R/\mathfrak{p})$ by (**13.4**)(3) with $M := R/\mathfrak{p}$. Also $\mathfrak{p} \in \operatorname{Ass}(M/xM)$ by hypothesis. So $\mathfrak{p}$ lies in the left side of (**17.19.2**). So $\mathfrak{p} \in \operatorname{Ass}(\operatorname{Hom}(R/\mathfrak{p}, M/yM))$ by (**17.19.1**). But (**17.19.2**) holds with y in place of x. Thus $\mathfrak{p} \in \operatorname{Ass}(M/yM)$ as desired.

In general, set $\mathfrak{a} := \operatorname{Ann}_R(M)$ and $R' := R/\mathfrak{a}$. Then R' is Noetherian by (**16.16**). But $\mathfrak{p} \in \operatorname{Ass}_R(M/xM)$. So (**17.13**) yields $\mathfrak{p} \supset \operatorname{Ann}_R(M/xM)$. But $\operatorname{Ann}_R(M/xM) \supset \mathfrak{a}$. Set $\mathfrak{p}' := \mathfrak{p}/\mathfrak{a}$. Then $\mathfrak{p}' \in \operatorname{Ass}_{R'}(M/xM)$ by (**17.4**). Let $x', y' \in \mathfrak{p}'$ be the residues of x, y. Then $M/x'M = M/xM$ and $M/y'M = M/yM$. But R' is Noetherian. Hence the above argument yields $\mathfrak{p}' \in \operatorname{Ass}_{R'}(M/yM)$. But $\operatorname{Ann}_R(M/yM) \supset \mathfrak{a}$. Thus (**17.4**) yields $\mathfrak{p} \in \operatorname{Ass}(M/yM)$ as desired. □

Proposition (17.20). — *Let R be a ring, $\mathfrak{q}$ an ideal, and M a Noetherian module. Then the following conditions are equivalent:*

(1) $\boldsymbol{V}(\mathfrak{q}) \cap \operatorname{Ass}(M) = \emptyset$. (2) $\mathfrak{q} \not\subset \mathfrak{p}$ *for any* $\mathfrak{p} \in \operatorname{Ass}(M)$.

(3) $\mathfrak{q} \not\subset \operatorname{z.div}(M)$*; that is, there is a nonzerodivisor x on M in $\mathfrak{q}$.*

(4) $\operatorname{Hom}(N, M) = 0$ *for all finitely generated modules N with* $\operatorname{Supp}(N) \subset \boldsymbol{V}(\mathfrak{q})$.

(5) $\operatorname{Hom}(N, M) = 0$ *for some finitely generated module* N *with* $\operatorname{Supp}(N) = \boldsymbol{V}(\mathfrak{q})$.

Proof: Plainly (1) and (2) are equivalent.

Next, $\operatorname{z.div}(M) = \bigcup_{\mathfrak{p}\in\operatorname{Ass}(M)} \mathfrak{p}$ by **(17.12)**. So (3) implies (2). But $\operatorname{Ass}(M)$ is finite by **(17.17)**; so **(3.12)** and (2) yield (3). Thus (2) and (3) are equivalent.

Note that (4) implies (5) with $N := R/\mathfrak{q}$ as $\operatorname{Supp}(N) = \mathbf{V}(\mathfrak{q})$ by **(13.4)**(3).

Thus it remains to prove that (1) implies (4) and that (5) implies (1).

Assume (1) and R is Noetherian. Given any module N with $\operatorname{Supp}(N) \subset \mathbf{V}(\mathfrak{q})$, then $\operatorname{Supp}(N) \cap \operatorname{Ass}(M) = \emptyset$. Hence if N is finitely generated too, then **(17.18)** yields $\operatorname{Ass}(\operatorname{Hom}(N, M)) = \emptyset$, and so $\operatorname{Hom}(N, M) = 0$ by **(17.10)**. Thus (4) holds.

Assume (5) and R is Noetherian. Plainly $\operatorname{Ass}(\operatorname{Hom}(N, M)) = \emptyset$. So **(17.18)** yields $\mathbf{V}(\mathfrak{q}) \cap \operatorname{Ass}(M) = \emptyset$. Thus (1) holds.

Set $\mathfrak{a} := \operatorname{Ann}(M)$ and $R' := R/\mathfrak{a}$. Let $\kappa\colon R \twoheadrightarrow R'$ be the quotient map, and set $\mathfrak{q}' := \kappa(\mathfrak{q})$. Let (1′), (4′), and (5′) stand for (1), (4), and (5) over R'. By **(16.16)**, R' is Noetherian; so by the above, (1′) implies (4′), and (5′) implies (1′).

Let's see that (1) and (1′) are equivalent. Since $\operatorname{Ass}(M) \subset \mathbf{V}(\mathfrak{a})$ by **(17.13)**, any $\mathfrak{p} \in \mathbf{V}(\mathfrak{q}) \cap \operatorname{Ass}(M)$ contains $\mathfrak{q} + \mathfrak{a}$. So $\kappa(\mathfrak{p}) \in \mathbf{V}(\mathfrak{q}')$. But κ carries $\operatorname{Ass}_R(M)$ bijectively onto $\operatorname{Ass}_{R'}(M)$ by **(17.4)**. Also, given $\mathfrak{p}' \in \mathbf{V}(\mathfrak{q}')$, plainly $\kappa^{-1}\mathfrak{p}' \in \mathbf{V}(\mathfrak{q})$. Thus κ induces a bijection from $\mathbf{V}(\mathfrak{q}) \cap \operatorname{Ass}_R(M)$ onto $\mathbf{V}(\mathfrak{q}') \cap \operatorname{Ass}_{R'}(M)$. Thus $\mathbf{V}(\mathfrak{q}) \cap \operatorname{Ass}_R(M) = \emptyset$ if and only if $\mathbf{V}(\mathfrak{q}') \cap \operatorname{Ass}_{R'}(M) = \emptyset$, as desired.

Let's derive (4) from (4′), and (5′) from (5). Given a finitely generated R-module N, set $N' := N/\mathfrak{a}N$. Then $N' = N \otimes_R R'$ by **(8.27)**(1). So **(8.9)**(2) yields

$$\operatorname{Hom}_R(N, M) = \operatorname{Hom}_{R'}(N', M). \qquad \textbf{(17.20.1)}$$

Also, $\operatorname{Supp}_{R'}(N') = \operatorname{Spec}(\kappa)^{-1} \operatorname{Supp}_R(N)$ by **(13.49)**. Hence, given $\mathfrak{p}' \in \operatorname{Spec}(R')$,

$$\mathfrak{p}' \in \operatorname{Supp}_{R'}(N') \quad \text{if and only if} \quad \mathfrak{p} := \kappa^{-1}\mathfrak{p}' \in \operatorname{Supp}_R(N).$$

Plainly $\mathfrak{p}' \in \mathbf{V}(\mathfrak{q}')$ if and only if $\mathfrak{p} \in \mathbf{V}(\mathfrak{q})$. Thus if $\operatorname{Supp}_R(N) \subset \mathbf{V}(\mathfrak{q})$, then $\operatorname{Supp}_{R'}(N') \subset \mathbf{V}(\mathfrak{q}')$, since if $\mathfrak{p}' \in \operatorname{Supp}_{R'}(N')$, then $\mathfrak{p} \in \operatorname{Supp}_R(N)$, so $\mathfrak{p} \in \mathbf{V}(\mathfrak{q})$, so $\mathfrak{p}' \in \mathbf{V}(\mathfrak{q}')$. Similarly, if $\operatorname{Supp}_R(N) \supset \mathbf{V}(\mathfrak{q})$, then $\operatorname{Supp}_{R'}(N') \supset \mathbf{V}(\mathfrak{q}')$.

Assume (4′), and let's prove (4). Given a finitely generated R-module N with $\operatorname{Supp}_R(N) \subset \mathbf{V}(\mathfrak{q})$, set $N' := N/\mathfrak{a}N$. By the above, $\operatorname{Supp}_{R'}(N') \subset \mathbf{V}(\mathfrak{q}')$. So $\operatorname{Hom}_{R'}(N', M) = 0$ by (4′). So $\operatorname{Hom}_R(N, M) = 0$ by **(17.20.1)**. Thus (4) holds.

Assume (5); it provides an N. Let's prove (5′) with $N' := N/\mathfrak{a}N$. Since $\operatorname{Supp}_R(N) = \mathbf{V}(\mathfrak{q})$, the above yields $\operatorname{Supp}_{R'}(N') = \mathbf{V}(\mathfrak{q}')$. Since $\operatorname{Hom}_R(N', M) = 0$, also $\operatorname{Hom}_{R'}(N', M) = 0$ by **(17.20.1)**. Thus (5′) holds.

Summarizing, we've proved the following two chains of implications:

$$(1) \Rightarrow (1') \Rightarrow (4') \Rightarrow (4) \quad \text{and} \quad (5) \Rightarrow (5') \Rightarrow (1') \Rightarrow (1).$$

Thus (1) implies (4), and (5) implies (1), as desired. □

B. Exercises

Exercise (17.21) . — Given modules $M_1, \ldots, M_r$, set $M := M_1 \oplus \cdots \oplus M_r$. Prove:

$$\mathrm{Ass}(M) = \mathrm{Ass}(M_1) \cup \cdots \cup \mathrm{Ass}(M_r).$$

Exercise (17.22) . — Let R be a ring, M a module, M_λ for $\lambda \in \Lambda$ submodules. Assume $M = \bigcup M_\lambda$. Show $\mathrm{Ass}(M) = \bigcup \mathrm{Ass}(M_\lambda)$.

Exercise (17.23) . — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 2\rangle \oplus \mathbb{Z}$. Find $\mathrm{Ass}(M)$ and find two submodules $L, N \subset M$ with $L + N = M$ but $\mathrm{Ass}(L) \cup \mathrm{Ass}(N) \subsetneqq \mathrm{Ass}(M)$.

Exercise (17.24) . — If a prime $\mathfrak{p}$ is sandwiched between two primes in $\mathrm{Ass}(M)$, is $\mathfrak{p}$ necessarily in $\mathrm{Ass}(M)$ too?

Exercise (17.25) . — Let R be a ring, S a multiplicative subset, M a module, N a submodule. Prove $\mathrm{Ass}(M/N^S) \supset \{\mathfrak{p} \in \mathrm{Ass}(M/N) \mid \mathfrak{p} \cap S = \emptyset\}$, with equality if either R is Noetherian or M/N is Noetherian.

Exercise (17.26) . — Let R be a ring, and suppose $R_\mathfrak{p}$ is a domain for every prime $\mathfrak{p}$. Prove every associated prime of R is minimal.

Exercise (17.27) . — Let R be a ring, M a module, N a submodule, $x \in R$. Assume that R is Noetherian or M/N is and that $x \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}(M/N)$. Show $xM \cap N = xN$.

Exercise (17.28) . — Let R be a ring, M a module, $\mathfrak{p}$ a prime. Show (1)–(3) are equivalent if R is Noetherian, and (1)–(4) are equivalent if M is Noetherian:

(1) $\mathfrak{p}$ is a minimal prime of M. (2) $\mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$.
(3) $\mathfrak{p}$ is minimal in $\mathrm{Ass}(M)$. (4) $\mathfrak{p}$ is a minimal prime of $\mathrm{Ann}(M)$.

Exercise (17.29) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $R/\mathfrak{a}$ is Noetherian. Show the minimal primes of $\mathfrak{a}$ are associated to $\mathfrak{a}$, and they are finite in number.

Exercise (17.30) . — Let M a Noetherian module. Show that $\mathrm{Supp}(M)$ has only finitely many irreducible components Y.

Exercise (17.31) . — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}$ in **(17.16)**. Determine when a chain $0 \subset M_1 \subsetneqq M$ is **acceptable** — that is, it's like the chain in **(17.16)** — and show that then $\mathfrak{p}_2 \notin \mathrm{Ass}(M)$.

Exercise (17.32) . — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 12\rangle$ in **(17.16)**. Find all three acceptable chains, and show that, in each case, $\{\mathfrak{p}_i\} = \mathrm{Ass}(M)$.

Exercise (17.33) . — Let R be a ring, M a nonzero Noetherian module, $x, y \in R$ and $a \in \mathrm{rad}(M)$. Assume $a^r + x \in \mathrm{z.div}(M)$ for all $r \geq 1$. Show $a + xy \in \mathrm{z.div}(M)$.

Exercise (17.34) (*Grothendieck Group $K_0(R)$*) . — Let R be a ring, $\mathcal{C}$ a subcategory of $((R\text{-mod}))$ such that the isomorphism classes of its objects form a set Λ. Let C be the free Abelian group $\mathbb{Z}^{\oplus\Lambda}$. Given M in $\mathcal{C}$, let $(M) \in \Lambda$ be its class. To each short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ in $\mathcal{C}$, associate the element $(M_2) - (M_1) - (M_3)$ of C. Let $D \subset C$ be the subgroup generated by all these elements. Set $K(\mathcal{C}) := C/D$, and let $\gamma_\mathcal{C} \colon C \to K(\mathcal{C})$ be the quotient map.

In particular, let $\mathcal{N}$ be the subcategory of all Noetherian modules and all linear maps between them; set $K_0(R) := K(\mathcal{N})$ and $\gamma_0 := \gamma_\mathcal{N}$. Show:

(1) Then $K(\mathcal{C})$ has this UMP: for each Abelian group G and function $\lambda\colon \Lambda \to G$ with $\lambda(M_2) = \lambda(M_1) + \lambda(M_3)$ for all exact sequences as above, there's an induced $\mathbb{Z}$-map $\lambda_0\colon K(\mathcal{C}) \to G$ with $\lambda(M) = \lambda_0(\gamma_{\mathcal{C}}(M))$ for all $M \in \mathcal{C}$.
(2) Then $K_0(R)$ is generated by the various elements $\gamma_0(R/\mathfrak{p})$ with $\mathfrak{p}$ prime.
(3) Assume R is a Noetherian domain. Find a surjective $\mathbb{Z}$-map $\kappa : K_0(R) \twoheadrightarrow \mathbb{Z}$.
(4) Assume R is a field or a PID. Then $K_0(R) = \mathbb{Z}$.
(5) Assume R is Noetherian. Let $\varphi\colon R \to R'$ and $\psi\colon R' \to R''$ be module-finite maps of rings. Then (a) restriction of scalars gives rise to a $\mathbb{Z}$-map $\varphi_!\colon K_0(R') \to K_0(R)$, and (b) we have $(\psi\varphi)_! = \varphi_!\psi_!$.

Exercise (17.35) (*Grothendieck Group* $K^0(R)$**) .** — Keep the setup of (17.34). Assume R is Noetherian. Let $\mathcal{F}$ be the subcategory of $((R\text{-mod}))$ of all finitely generated *flat* R-modules M and all linear maps between them; set $K^0(R) := K(\mathcal{F})$ and $\gamma^0 := \gamma_{\mathcal{F}}$. Let $\varphi\colon R \to R'$ and $\psi\colon R' \to R''$ be maps of Noetherian rings. Show:
(1) Setting $\gamma^0(M)\gamma^0(N) := \gamma^0(M\otimes N)$ makes $K^0(R)$ a $\mathbb{Z}$-algebra with $\gamma^0(R) = 1$.
(2) Setting $\gamma^0(M)\gamma_0(L) := \gamma_0(M \otimes L)$ makes $K_0(R)$ a $K^0(R)$-module.
(3) Assume R is local. Then $K^0(R) = \mathbb{Z}$.
(4) Setting $\varphi^!\gamma^0(M) := \gamma^0(M \otimes_R R')$ defines a ring map $\varphi^!\colon K^0(R) \to K^0(R')$. Moreover, $(\varphi\psi)^! = \varphi^!\psi^!$.
(5) If $\varphi\colon R \to R'$ is module finite, then $\varphi_!\colon K_0(R') \to K_0(R)$ is linear over $K^0(R)$.

18. Primary Decomposition

Primary decomposition of a submodule generalizes factorization of an integer into powers of primes. A proper submodule is called **primary** if the quotient module has only one associated prime. There's an older notion, which we call **old-primary**; it requires that, given an element of the ring and one of the module whose product lies in the submodule, but whose second element doesn't, then some power of the first annihilates the quotient of the module by the submodule.

The two notions coincide when the quotient is Noetherian. In this case, we characterize primary submodules in various ways, and we study primary decompositions, representations of an arbitrary submodule as a finite intersection of primary submodules. A decomposition is called **irredundant**, or **minimal**, if it cannot be shortened. We consider several illustrative examples in a polynomial ring over a field. Then we prove the celebrated Lasker–Noether Theorem: every proper submodule with Noetherian quotient has an irredundant primary decomposition.

We prove two uniqueness theorems. The first asserts the uniqueness of the primes that arise; they are just the associated primes of the quotient. The second asserts the uniqueness of those primary components whose primes are minimal among these associated primes; the other primary components may vary. To prove it, we study the behavior of primary decomposition under localization. Lastly, we derive the important Krull Intersection Theorem: given an ideal $\mathfrak{a}$ and a Noetherian module M, the infinite intersection $\bigcap_{n\geq 0} \mathfrak{a}^n M$ is annihilated by some y with $y-1 \in \mathfrak{a}$. Another and more common proof is considered in Exercise (**20.22**).

In an appendix, we study old-primary submodules further. In the Noetherian case, we thus obtain alternative proofs of some of the earlier results; also we obtain some new results about primary submodules.

A. Text

Definition (18.1). — Let R be a ring, $Q \subsetneqq M$ modules. If $\operatorname{Ass}(M/Q)$ consists of a single prime $\mathfrak{p}$, we say Q is **primary** or $\mathfrak{p}$-primary in M. We say Q is **old-primary** if given $x \in R$ and $m \in M$ with $xm \in Q$, either $m \in Q$ or $x \in \operatorname{nil}(M/Q)$.

Example (18.2). — A prime $\mathfrak{p}$ is $\mathfrak{p}$-primary, as $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by (**17.5**)(2). Plainly, $\mathfrak{p}$ is old-primary too.

Theorem (18.3). — *Let R be a ring, $Q \subsetneqq M$ modules. Set $\mathfrak{p} := \operatorname{nil}(M/Q)$.*

(1) *Then Q is old-primary if and only if $\operatorname{z.div}(M/Q) = \mathfrak{p}$.*
(2) *If Q is old-primary, then $\mathfrak{p}$ is the smallest prime containing $\operatorname{Ann}(M/Q)$.*
(3) *If Q is old-primary and $\operatorname{Ass}(M/Q) \neq \emptyset$, then Q is $\mathfrak{p}$-primary.*
(4) *If Q is old-primary, and if M/Q is Noetherian or R is, then Q is $\mathfrak{p}$-primary,*
(5) *If Q is $\mathfrak{q}$-primary and M/Q is Noetherian, then $\mathfrak{q} = \mathfrak{p}$ and Q is old-primary.*

Proof: For (1), first assume Q is old-primary. Given $x \in \operatorname{z.div}(M/Q)$, there's $m \in M - Q$ with $xm \in Q$. So $x \in \mathfrak{p}$. Thus $\operatorname{z.div}(M/Q) \subset \mathfrak{p}$. But $\operatorname{z.div}(M/Q) \supset \mathfrak{p}$ by (**17.11.1**). Thus $\operatorname{z.div}(M/Q) = \mathfrak{p}$.

Conversely, assume $\operatorname{z.div}(M/Q) = \mathfrak{p}$. Given $x \in R$ and $m \in M$ with $xm \in Q$, but $m \notin Q$, note $x \in \operatorname{z.div}(M/Q)$. So $x \in \mathfrak{p}$. So Q is old-primary. Thus (1) holds.

For (2), let $x, y \in R$ with $xy \in \mathfrak{p}$, but $y \notin \mathfrak{p}$. As $xy \in \mathfrak{p}$, there's $n \geq 1$ with $(xy)^n M \subset Q$. As $y \notin \mathfrak{p}$, there's $m \in M$ with $y^n m \notin Q$. But Q is old-primary. So $x^n \in \mathfrak{p}$. So $x \in \mathfrak{p}$. Thus $\mathfrak{p}$ is prime.

Given a prime $\mathfrak{q} \supset \mathrm{Ann}(M/Q)$ and $x \in \mathfrak{p}$, there's $n \geq 1$ with $x^n \in \mathrm{Ann}(M/Q)$, so $x^n \in \mathfrak{q}$. So $x \in \mathfrak{q}$. Thus $\mathfrak{q} \supset \mathfrak{p}$. Thus (2) holds.

For (3), assume Q is old-primary, and say $\mathfrak{q} \in \mathrm{Ass}(M/Q)$. Say $\mathfrak{q} = \mathrm{Ann}(m)$ with $m \in M/Q$ nonzero. Then $\mathrm{Ann}(M/Q) \subset \mathfrak{q} \subset \mathrm{z.div}(M/Q)$. But $\mathrm{z.div}(M/Q) = \mathfrak{p}$ by (1). Hence (2) gives $\mathfrak{q} = \mathfrak{p}$. Thus (3) holds.

For (4), note $M/Q \neq 0$. So if M/Q is Noetherian or R is, then $\mathrm{Ass}(M/Q) \neq \emptyset$ by **(17.10)**. Thus (3) yields (4).

For (5), note $\mathfrak{p} = \mathfrak{q}$ owing to **(17.15)**, and $\mathrm{z.div}(M/Q) = \mathfrak{q}$ owing to **(17.12)**. So $\mathrm{z.div}(M/Q) = \mathfrak{p}$. Thus (1) yields (5). □

Lemma (18.4). — *Let R be a ring, N a Noetherian module. Set $\mathfrak{n} := \mathrm{nil}(N)$. Then $\mathfrak{n}^n N = 0$ for some $n \geq 1$.*

Proof: Set $\mathfrak{a} := \mathrm{Ann}(N)$ and $R' := R/\mathfrak{a}$. Then $\mathfrak{n} := \sqrt{\mathfrak{a}}$, and R' is Noetherian by **(16.16)**. Set $\mathfrak{n}' := \mathfrak{n}/\mathfrak{a}$. Then $\mathfrak{n}'$ is finitely generated. So $\mathfrak{n}'^n = 0$ for some $n \geq 1$ by **(3.38)**. So $\mathfrak{n}^n \subset \mathfrak{a}$. Thus $\mathfrak{n}^n N = 0$. □

Proposition (18.5). — *Let M be a module, Q a submodule. If Q is $\mathfrak{p}$-primary and M/Q is Noetherian, then $\mathfrak{p} = \mathrm{nil}(M/Q)$ and $\mathfrak{p}^n(M/Q) = 0$ for some $n \geq 1$.*

Proof: The assertion follows immediately from **(17.15)** and **(18.4)**. □

Exercise (18.6) . — Let $\varphi\colon R \twoheadrightarrow R'$ be a surjective ring map, M an R-module, $Q' \subsetneqq M'$ two R'-modules, $\alpha\colon M \twoheadrightarrow M'$ a surjective R-map, $\mathfrak{p}'$ a prime of R'. Set $\mathfrak{p} := \varphi^{-1}(\mathfrak{p}')$ and $Q := \alpha^{-1}Q'$. Show Q is $\mathfrak{p}$-primary if and only if Q' is $\mathfrak{p}'$-primary.

Exercise (18.7) . — Let R be a ring, and $\mathfrak{p} = \langle p \rangle$ a principal prime generated by a nonzerodivisor p. Show every positive power $\mathfrak{p}^n$ is old-primary and $\mathfrak{p}$-primary. Show conversely, an ideal $\mathfrak{q}$ is equal to some $\mathfrak{p}^n$ if either (1) $\mathfrak{q}$ is old-primary and $\sqrt{\mathfrak{q}} = \mathfrak{p}$ or (2) R is Noetherian and $\mathfrak{q}$ is $\mathfrak{p}$-primary.

Proposition (18.8). — *Let R be a ring, $\mathfrak{m}$ a maximal ideal, $Q \subsetneqq M$ modules.*

(1) *Assume $\mathrm{nil}(M/Q) = \mathfrak{m}$. Then Q is old-primary.*

(2) *Assume $\mathfrak{m}^n(M/Q) = 0$ with $n \geq 1$. Then $\mathrm{nil}(M/Q) = \mathfrak{m}$ and Q is $\mathfrak{m}$-primary.*

Proof: Set $\mathfrak{a} := \mathrm{Ann}(M/Q)$. Then $\sqrt{\mathfrak{a}} =: \mathrm{nil}(M/Q)$.

For (1), fix $x \in R$ and $m \in M$ with $xm \in Q$, but $x \notin \mathfrak{m}$. As $\mathfrak{m}$ is maximal, x is a unit mod $\mathfrak{a}$ by **(3.37)**(3)⇒(2); so there's $y \in R$ with $1 - xy \in \mathfrak{a}$. But $\mathfrak{a}(M/Q) = 0$. So $m - xym \in \mathfrak{a}M \subset Q$. But $xm \in Q$; so $xym \in Q$. Thus $m \in Q$. Thus (1) holds.

For (2), note $\mathfrak{m}^n \subset \mathfrak{a}$. So $\mathfrak{m} \subset \sqrt{\mathfrak{a}}$. But $Q \neq M$, so $\sqrt{\mathfrak{a}} \neq R$. But $\mathfrak{m}$ is maximal. Thus $\mathfrak{m} = \sqrt{\mathfrak{a}} =: \mathrm{nil}(M/Q)$. Thus (1) implies Q is old-primary.

Take $n \geq 1$ minimal with $\mathfrak{m}^n(M/Q) = 0$. Then there's $m \in \mathfrak{m}^{n-1}(M/Q)$ with $m \neq 0$ but $\mathfrak{m}m = 0$. So $\mathfrak{m} \subset \mathrm{Ann}(m) \subsetneqq R$. But $\mathfrak{m}$ is maximal. So $\mathfrak{m} = \mathrm{Ann}(m)$. Thus $\mathfrak{m} \in \mathrm{Ass}(M/Q)$. Thus Q is $\mathfrak{m}$-primary by **(18.3)**(3). Thus (2) holds. □

Corollary (18.9). — *Let R be a ring, $\mathfrak{m}$ and $\mathfrak{q}$ ideals. Assume $\mathfrak{m}$ is maximal, $\mathfrak{q}$ is proper, and $\mathfrak{m}^n \subset \mathfrak{q}$ for some $n \geq 1$. Then $\mathfrak{m} = \sqrt{\mathfrak{q}}$, and $\mathfrak{q}$ is old-primary and $\mathfrak{m}$-primary.*

Proof: In **(18.8)**, just take $M := R$ and $Q := \mathfrak{q}$. □

Proposition (18.10). — *Let R be a ring, $\mathfrak{m}$ a maximal ideal, M a module, Q a proper submodule. Assume M/Q is Noetherian. Then* (1)–(3) *are equivalent:*

$$(1)\ Q \textit{ is } \mathfrak{m}\textit{-primary};\quad (2)\ \mathfrak{m} = \mathrm{nil}(M/Q);\quad (3)\ \mathfrak{m}^n(M/Q) = 0 \textit{ for some } n \ge 1.$$

Proof: First, (1) implies (2) and (3) by **(18.5)**. Second, (2) implies (3) by **(18.4)**. Third, (3) implies (1) and (2) by **(18.8)**(2). □

Corollary (18.11). — *Let R be a ring, $\mathfrak{m}$ and $\mathfrak{q}$ an ideals. Assume $\mathfrak{m}$ is maximal, $\mathfrak{q}$ is proper, and $R/\mathfrak{q}$ is Noetherian. Then* (1)–(3) *are equivalent:*

$$(1)\ \mathfrak{q} \textit{ is } \mathfrak{m}\textit{-primary};\quad (2)\ \mathfrak{m} = \sqrt{\mathfrak{q}};\quad (3)\ \mathfrak{m}^n \subset \mathfrak{q} \textit{ for some } n \ge 1.$$

Proof: In **(18.10)**, just take $M := R$ and $Q := \mathfrak{q}$. □

Lemma (18.12). — *Let R be a ring, $Q_1, Q_2 \subsetneqq M$ modules. Set $Q_3 := Q_1 \cap Q_2$.*

(1) *Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$. If Q_1, Q_2 are old-primary, and if $\mathfrak{p}_1 = \mathfrak{p}_2$, then $\mathfrak{p}_3 = \mathfrak{p}_2$ and Q_3 is old-primary.*

(2) *If M/Q_3 is Noetherian or R is, and if Q_1, Q_2 are $\mathfrak{p}$-primary, then so is Q_3.*

Proof: For (1), note $\mathfrak{p}_3 = \mathfrak{p}_1 \cap \mathfrak{p}_2$ by **(12.42)**(2). Thus if $\mathfrak{p}_1 = \mathfrak{p}_2$, then $\mathfrak{p}_3 = \mathfrak{p}_2$.

Given $x \in R$ and $m \in M$ with $xm \in Q_3$ but $m \notin Q_3$, say $m \notin Q_1$. Then $x \in \mathfrak{p}_1$ if Q_1 is old-primary. But if $\mathfrak{p}_1 = \mathfrak{p}_2$, then $\mathfrak{p}_3 = \mathfrak{p}_2$. Thus (1) holds.

For (2), form the canonical map $M \to M/Q_1 \oplus M/Q_2$. Its kernel is Q_3. So it induces an injection $M/Q_3 \hookrightarrow M/Q_1 \oplus M/Q_2$. Assume M/Q_3 is Noetherian or R is. Then **(17.10)** and **(17.6)** and **(17.21)** yield

$$\emptyset \ne \mathrm{Ass}(M/Q_3) \subset \mathrm{Ass}(M/Q_1 \oplus M/Q_2) \subset \mathrm{Ass}(M/Q_1) \cup \mathrm{Ass}(M/Q_2).$$

If the latter two sets are each equal to $\{\mathfrak{p}\}$, then so is $\mathrm{Ass}(M/Q_3)$, as desired. □

(18.13) (Primary decomposition). — Let R be a ring, M a module, and N a submodule. A **primary decomposition** of N in M is a decomposition

$$N = Q_1 \cap \cdots \cap Q_r \quad \text{with the } Q_i \text{ primary.}$$

We call the decomposition **irredundant** or **minimal** if these conditions hold:

(1) $N \ne \bigcap_{i\ne j} Q_i$, or equivalently, $\bigcap_{i\ne j} Q_i \not\subset Q_j$ for $j = 1, \dots, r$.

(2) Set $\mathfrak{p}_i := \mathrm{Ann}(M/Q_i)$ for $i = 1, \dots, r$. Then $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct.

If so, then we call Q_i the **$\mathfrak{p}_i$-primary component** of the decomposition.

Assume M/N is Noetherian or R is. If M/N is Noetherian, so is M/Q for any $N \subset Q \subset M$ by **(16.13)**(2). Hence, any primary decomposition of N can be made irredundant owing to **(18.12)**: simply intersect all the primary submodules with the same prime, and then repeatedly discard the first unnecessary component.

Finally, say $N = Q_1 \cap \cdots \cap Q_r$. Assume M/N is Noetherian; so the N/Q_i are too. Then by **(18.3)**(4)–(5), the Q_i are old-primary if and only if they're primary.

Example (18.14). — Let k be a field, $R := k[X, Y]$ the polynomial ring. Set $\mathfrak{a} := \langle X^2, XY\rangle$. Below, it is proved that, for any $n \ge 1$,

$$\mathfrak{a} = \langle X\rangle \cap \langle X^2, XY, Y^n\rangle = \langle X\rangle \cap \langle X^2, Y\rangle. \qquad \textbf{(18.14.1)}$$

Here $\langle X^2, XY, Y^n\rangle$ and $\langle X^2, Y\rangle$ contain $\langle X, Y\rangle^n$; so they are $\langle X, Y\rangle$-primary by **(18.9)**. Thus **(18.14.1)** gives infinitely many primary decompositions of $\mathfrak{a}$. They are clearly irredundant. Note: *the $\langle X, Y\rangle$-primary component is not unique!*

Plainly, $\mathfrak{a} \subset \langle X\rangle$ and $\mathfrak{a} \subset \langle X^2, XY, Y^n\rangle \subset \langle X^2, Y\rangle$. To see $\mathfrak{a} \supset \langle X\rangle \cap \langle X^2, Y\rangle$, take $F \in \langle X\rangle \cap \langle X^2, Y\rangle$. Then $F = GX = AX^2 + BY$ where $A, B, G \in R$. Then

$X(G - AX) = BY$. So $X \mid B$. Say $B = B'X$. Then $F = AX^2 + B'XY \in \mathfrak{a}$.

Example (18.15). — Let k be a field, $R := k[X, Y]$ the polynomial ring, $a \in k$. Set $\mathfrak{a} := \langle X^2, XY\rangle$. Define an automorphism α of R by $X \mapsto X$ and $Y \mapsto aX + Y$. Then α preserves $\mathfrak{a}$ and $\langle X\rangle$, and carries $\langle X^2, Y\rangle$ onto $\langle X^2, aX + Y\rangle$. So **(18.14)** implies that $\mathfrak{a} = \langle X\rangle \cap \langle X^2, aX + Y\rangle$ is an irredundant primary decomposition. Moreover, if $a \neq b$, then $\langle X^2, aX+Y, bX+Y\rangle = \langle X, Y\rangle$. Thus *two $\langle X, Y\rangle$-primary components are not always contained in a third, although their intersection is one by* **(18.12)**.

Example (18.16). — Let k be a field, $P := k[X, Y, Z]$ the polynomial ring. Set $R := P/\langle XZ - Y^2\rangle$. Let x, y, z be the residues of X, Y, Z in R. Set $\mathfrak{p} := \langle x, y\rangle$. Clearly $\mathfrak{p}^2 = \langle x^2, xy, y^2\rangle = x\langle x, y, z\rangle$. Let's show that $\mathfrak{p}^2 = \langle x\rangle \cap \langle x^2, y, z\rangle$ is an irredundant primary decomposition.

First note the inclusions $x\langle x, y, z\rangle \subset \langle x\rangle \cap \langle x, y, z\rangle^2 \subset \langle x\rangle \cap \langle x^2, y, z\rangle$.

Conversely, given $f \in \langle x\rangle \cap \langle x^2, y, z\rangle$, represent f by GX with $G \in P$. Then

$$GX = AX^2 + BY + CZ + D(XZ - Y^2) \quad \text{with} \quad A, B, C, D \in P.$$

So $(G - AX)X = B'Y + C'Z$ with $B', C' \in P$. Say $G - AX = A'' + B''Y + C''Z$ with $A'' \in k[X]$ and $B'', C'' \in P$. Then

$$A''X = -B''XY - C''XZ + B'Y + C'Z = (B' - B''X)Y + (C' - C''X)Z;$$

whence, $A'' = 0$. Therefore, $GX \in X\langle X, Y, Z\rangle$. Thus $\mathfrak{p}^2 = \langle x\rangle \cap \langle x^2, y, z\rangle$.

Let's show that $\langle x\rangle$ is $\langle x, y\rangle$-primary in R. Note that the preimage in P of $\langle x\rangle$ is $\langle X, Y^2\rangle$ and of $\langle x, y\rangle$ is $\langle X, Y\rangle$. Also, form the $k[Y, Z]$-map $\varphi\colon P \twoheadrightarrow k[Y, Z]$ with $\varphi(X) = 0$; plainly, $\langle X, Y^2\rangle = \varphi^{-1}\langle Y^2\rangle$ and $\langle X, Y\rangle = \varphi^{-1}\langle Y\rangle$. But $\langle Y^2\rangle$ is $\langle Y\rangle$-primary by **(18.7)**. So $\langle X, Y^2\rangle$ is $\langle X, Y\rangle$-primary by **(18.6)**. But R is a quotient of P. Thus by **(18.6)** again, $\langle x\rangle$ is $\langle x, y\rangle$-primary.

Finally $\langle x, y, z\rangle^2 \subset \langle x^2, y, z\rangle \subset \langle x, y, z\rangle$ and $\langle x, y, z\rangle$ is maximal. So $\langle x^2, y, z\rangle$ is $\langle x, y, z\rangle$-primary by **(18.9)**.

Thus $\mathfrak{p}^2 = \langle x\rangle \cap \langle x^2, y, z\rangle$ is a primary decomposition. It is irredundant since $\langle x, y\rangle \neq \langle x, y, z\rangle$. Moreover, $\langle x\rangle$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^2$.

Lemma (18.17). — *Let R be a ring, $N = Q_1 \cap \cdots \cap Q_r$ a primary decomposition in a module M. Say Q_i is $\mathfrak{p}_i$-primary for all i. Then*

$$\operatorname{Ass}(M/N) \subseteqq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}. \qquad \textbf{(18.17.1)}$$

If equality holds and if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct, then the decomposition is irredundant; the converse holds if R is Noetherian or if M/N is Noetherian.

Proof: Since $N = \bigcap Q_i$, the canonical map is injective: $M/N \hookrightarrow \bigoplus M/Q_i$. So **(17.6)** and **(17.21)** yield $\operatorname{Ass}(M/N) \subseteqq \bigcup \operatorname{Ass}(M/Q_i)$. Thus **(18.17.1)** holds.

If $N = Q_2 \cap \cdots \cap Q_r$, then $\operatorname{Ass}(M/N) \subseteqq \{\mathfrak{p}_2, \ldots, \mathfrak{p}_r\}$ too. Thus if equality holds in **(18.17.1)** and if $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct, then $N = Q_1 \cap \cdots \cap Q_r$ is irredundant.

Conversely, assume $N = Q_1 \cap \cdots \cap Q_r$ is irredundant. Given i, set $P_i := \bigcap_{j \neq i} Q_j$. Then $P_i \cap Q_i = N$ and $P_i/N \neq 0$. Consider these two canonical injections:

$$P_i/N \hookrightarrow M/Q_i \quad \text{and} \quad P_i/N \hookrightarrow M/N.$$

Assume R is Noetherian or M/N is Noetherian. If M/N is Noetherian, so is P_i/N by **(16.13)**(2). So in both cases $\operatorname{Ass}(P_i/N) \neq \emptyset$ by **(17.10)**. So the first injection yields $\operatorname{Ass}(P_i/N) = \{\mathfrak{p}_i\}$ by **(17.6)**; then the second yields $\mathfrak{p}_i \in \operatorname{Ass}(M/N)$. Thus $\operatorname{Ass}(M/N) \supseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, and **(18.17.1)** yields equality, as desired. $\square$

Theorem (18.18) (First Uniqueness). — *Let R be a ring, $N = Q_1 \cap \cdots \cap Q_r$ an irredundant primary decomposition in a module M. Say Q_i is $\mathfrak{p}_i$-primary for all i. Assume R is Noetherian or M/N is Noetherian. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are uniquely determined; in fact, they are just the distinct associated primes of M/N.*

Proof: The assertion is just part of **(18.17)**. □

Theorem (18.19) (Lasker–Noether). — *A proper submodule N of a module M has an irredundant primary decomposition if M/N is Noetherian.*

Proof: First, M/N has finitely many distinct associated primes, say $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, by **(17.17)**. But by **(17.7)**, for each i, there is a $\mathfrak{p}_i$-primary submodule Q_i of M with $\operatorname{Ass}(Q_i/N) = \operatorname{Ass}(M/N) - \{\mathfrak{p}_i\}$. Set $P := \bigcap Q_i$. Fix i. Then $P/N \subset Q_i/N$. So $\operatorname{Ass}(P/N) \subset \operatorname{Ass}(Q_i/N)$ by **(17.6)**. But i is arbitrary. So $\operatorname{Ass}(P/N) = \emptyset$. But P/N is Noetherian as M/N is. So $P/N = 0$ by **(17.10)**. Finally, the decomposition $N = \bigcap Q_i$ is irredundant by **(18.17)**. □

Lemma (18.20). — *Let R be a ring, S a multiplicative subset, $\mathfrak{p}$ a prime ideal, M a module, Q a submodule. Assume M/Q is Noetherian and $S \cap \mathfrak{p} = \emptyset$. Then Q is $\mathfrak{p}$-primary if and only if $S^{-1}Q$ is $S^{-1}\mathfrak{p}$-primary. Moreover, if so, then $Q^S = Q$.*

Finally, if M is Noetherian, then $Q \mapsto S^{-1}Q$ is a bijection from the $\mathfrak{p}$-primary submodules of M with $S \cap \mathfrak{p} = \emptyset$ onto the $S^{-1}\mathfrak{p}$-primary submodules of $S^{-1}M$.

Proof: Note $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$ is a bijection from the primes $\mathfrak{q}$ of R with $S \cap \mathfrak{q} = \emptyset$ onto the primes of $S^{-1}R$ by **(11.12)**(2) and **(12.2)**. But M/Q is Noetherian, so $R/\operatorname{Ann}(M/Q)$ is too by **(16.16)**. So $\mathfrak{q} \mapsto S^{-1}\mathfrak{q}$ restricts to a bijection from the subset of $\operatorname{Ass}(M/Q)$ of $\mathfrak{q}$ with $S \cap \mathfrak{q} = \emptyset$ onto $\operatorname{Ass}(S^{-1}(M/Q))$ by **(17.8)**. But $S^{-1}(M/Q) = S^{-1}M/S^{-1}Q$ by **(12.13)**. And $S \cap \mathfrak{p} = \emptyset$. Thus Q is $\mathfrak{p}$-primary if and only if $S^{-1}Q$ is $S^{-1}\mathfrak{p}$-primary.

Moreover, assume Q is $\mathfrak{p}$-primary. Now, $Q^S = \varphi_S^{-1}(S^{-1}Q)$ by **(12.12)**(3)(a). So, given $m \in Q^S$, there's $s \in S$ with $sm \in Q$. But $s \notin \mathfrak{p}$. Also, Q is old-primary, and $\mathfrak{p} = \operatorname{nil}(M/Q)$ by **(18.3)**(5). So $m \in Q$. Thus $Q^S \subset Q$. But $Q^S \supset Q$ as $1 \in S$. Thus $Q^S = Q$.

Finally, assume M is Noetherian. Then the map $Q \mapsto S^{-1}Q$ maps $\mathfrak{p}$-primary submodules with $\mathfrak{p} \cap S = \emptyset$ to $S^{-1}\mathfrak{p}$-primary submodules K by the first paragraph above. It is injective because $\varphi_S^{-1}S^{-1}Q = Q^S$ by **(12.12)**(3)(a) and $Q^S = Q$ by the second paragraph above. It is surjective because $S^{-1}\varphi_S^{-1}K = K$ by **(12.12)**(2)(b) and $\varphi_S^{-1}K$ is $\mathfrak{p}$-primary by the first paragraph above. □

Proposition (18.21). — *Let R be a ring, S a multiplicative subset, M a module, $N = Q_1 \cap \cdots \cap Q_r \subset M$ an irredundant primary decomposition. Assume M/N is Noetherian. Say Q_i is $\mathfrak{p}_i$-primary for all i, and $S \cap \mathfrak{p}_i = \emptyset$ just for $i \le h$. Then*

$$S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_h \subset S^{-1}M \quad \textit{and} \quad N^S = Q_1 \cap \cdots \cap Q_h \subset M$$

are irredundant primary decompositions.

Proof: Note $S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_r$ by **(12.12)**(6)(b). But $S^{-1}Q_i$ is $S^{-1}\mathfrak{p}_i$-primary for $i \le h$ by **(18.20)**, and $S^{-1}Q_i = S^{-1}M$ for $i > h$ by **(12.23)**. Therefore, $S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_h$ is a primary decomposition.

It is irredundant by **(18.17)**. Indeed, $\operatorname{Ass}(S^{-1}M/S^{-1}N) = \{S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_h\}$ by an argument like that in the first part of **(18.20)**. Further, $S^{-1}\mathfrak{p}_1, \ldots, S^{-1}\mathfrak{p}_h$ are distinct by **(11.12)**(2) as the $\mathfrak{p}_i$ are distinct.

Apply φ_S^{-1} to $S^{-1}N = S^{-1}Q_1 \cap \cdots \cap S^{-1}Q_h$. We get $N^S = Q_1^S \cap \cdots \cap Q_h^S$ by **(12.12)**(3)(a). Each M/Q_i is Noetherian as it is a quotient of M/N. So $Q_i^S = Q_i$ by **(18.20)**. So $N^S = Q_1 \cap \cdots \cap Q_h$ is a primary decomposition. It is irredundant as, clearly, **(18.13)**(1), (2) hold for it, as they do for $N = Q_1 \cap \cdots \cap Q_r$. □

Theorem (18.22) (Second Uniqueness)**. —** *Let R be a ring, M a module, N a submodule. Assume M/N is Noetherian. Let $\mathfrak{p}$ be minimal in* $\mathrm{Ass}(M/N)$. *Recall that $S_\mathfrak{p} := R - \mathfrak{p}$. Then, in any irredundant primary decomposition of N in M, the $\mathfrak{p}$-primary component Q is uniquely determined; in fact, $Q = N^{S_\mathfrak{p}}$.*

Proof: In **(18.21)**, take $S := S_\mathfrak{p}$. Then $h = 1$ as $\mathfrak{p}$ is minimal in $\mathrm{Ass}(M/N)$. □

Theorem (18.23) (Krull Intersection)**. —** *Let $\mathfrak{a}$ be an ideal, and M a Noetherian module. Set $N := \bigcap_{n\ge 0} \mathfrak{a}^n M$. Then there is $x \in \mathfrak{a}$ such that $(1+x)N = 0$.*

Proof: Since N is finitely generated, the desired $x \in \mathfrak{a}$ exists by **(10.3)** provided $N = \mathfrak{a}N$. Clearly $N \supset \mathfrak{a}N$. To prove $N \subset \mathfrak{a}N$, note that, as M is Noetherian, $M/\mathfrak{a}N$ is too by **(16.13)**(2). So **(18.19)** gives a decomposition $\mathfrak{a}N = \bigcap Q_i$ where Q_i is $\mathfrak{p}_i$-primary, so old-primary by **(18.3)**(5). Fix i. So, if there's $a \in \mathfrak{a} - \mathfrak{p}_i$, then $aN \subset Q_i$, and so $N \subset Q_i$. If $\mathfrak{a} \subset \mathfrak{p}_i$, then there's n_i with $\mathfrak{a}^{n_i} M \subset Q_i$ by **(18.5)**, and so again $N \subset Q_i$. Thus $N \subset \bigcap Q_i = \mathfrak{a}N$, as desired. □

Example (18.24) (Another non-Noetherian ring). — Let A be the local ring of germs of C^∞-functions $F(x)$ at $x = 0$ on $\mathbb{R}$, and $\mathfrak{m}$ the ideal of $F \in A$ with $F(0) = 0$. Note that $\mathfrak{m}$ is maximal, as $F \mapsto F(0)$ defines an isomorphism $A/\mathfrak{m} \xrightarrow{\sim} \mathbb{R}$.

Given $F \in A$ and $n \ge 1$, apply Taylor's Formula to $f(t) := F(xt)$ from $t = 0$ to $t = 1$ (see [**13**, Theorem 3.1, p. 109]); as $f^{(n)}(t) = x^n F^{(n)}(xt)$, we get

$$\begin{gathered} F(x) = F(0) + F'(0)x + \cdots + \tfrac{F^{(n-1)}(0)}{(n-1)!}x^{n-1} + x^n F_n(x) \\ \text{where} \quad F_n(x) := \int_0^1 \tfrac{(1-t)^{n-1}}{(n-1)!} F^{(n)}(xt)\,dt. \end{gathered} \tag{18.24.1}$$

Note F_n is C^∞: just differentiate under the integral sign (by [**13**, Thm. 7.1, p. 276]).

If $F^{(k)}(0) = 0$ for $k < n$, then **(18.24.1)** yields $F \in \langle x^n \rangle$. Conversely, assume $F(x) = x^n G(x)$ for some $G \in A$. By Leibniz's Product Rule,

$$F^{(k)}(x) = \textstyle\sum_{j=0}^{k} \binom{k}{j} \frac{n!}{(n-j)!} x^{n-j} G^{(k-j)}(x).$$

So $F^{(k)}(0) = 0$ if $k < n$. So $\langle x^n \rangle = \{\, F \in A \mid F^{(k)}(0) = 0 \text{ for } k < n \,\}$. So $\mathfrak{m} = \langle x \rangle$. Thus $\langle x^n \rangle = \mathfrak{m}^n$. Set $\mathfrak{n} := \bigcap_{n\ge 0} \mathfrak{m}^n$. Thus $\mathfrak{n} = \{\, F \in A \mid F^{(k)}(0) = 0 \text{ for all } k \,\}$.

Taylor's Formula defines a map $\tau\colon A \to \mathbb{R}[[x]]$ by $\tau(F) := \sum_{n=0}^{\infty} \frac{F^{(n)}(0)}{n!} x^n$. Plainly τ is $\mathbb{R}$-linear and, by Leibniz's Product Rule, τ is a ring map. Moreover, by the previous paragraph, $\mathrm{Ker}(\tau) = \mathfrak{n}$.

Cauchy's Function is a well-known nonzero C^∞-function $H \in \mathfrak{n}$; namely,

$$H(x) := \begin{cases} e^{-1/x^2} & \text{if } x \ne 0, \\ 0 & \text{if } x = 0; \end{cases}$$

see [**13**, Ex. 7, p. 82]. Thus $\mathfrak{n} \ne 0$.

Given $G \in \mathfrak{m}$, let's show $(1+G)H \ne 0$. Since $G(0) = 0$ and G is continuous, there is $\delta > 0$ such that $|G(x)| < 1/2$ if $|x| < \delta$. Hence $1 + G(x) \ge 1/2$ if $|x| < \delta$. Hence $\big(1 + G(x)\big)H(x) > (1/2)h(x) > 0$ if $0 < |x| < \delta$. Thus $(1+G)\mathfrak{n} \ne 0$. Thus the Krull Intersection Theorem **(18.23)** fails for A, and so A is non-Noetherian.

B. Exercises

Exercise (18.25) . — Fix a prime $p \in \mathbb{Z}$. Set $M := \bigoplus_{n=1}^{\infty} \mathbb{Z}/\langle p^n \rangle$ and $Q := 0$ in M. Show Q is $\langle p \rangle$-primary, but not old-primary (even though $\mathbb{Z}$ is Noetherian).

Exercise (18.26) . — Let k be a field, and $k[X,Y]$ the polynomial ring. Let $\mathfrak{a}$ be the ideal $\langle X^2,\ XY \rangle$. Show $\mathfrak{a}$ is not primary, but $\sqrt{\mathfrak{a}}$ is prime. Show $\mathfrak{a}$ satisfies this condition: $FG \in \mathfrak{a}$ implies $F^2 \in \mathfrak{a}$ or $G^2 \in \mathfrak{a}$.

Exercise (18.27) . — Let R be PIR, $\mathfrak{q}$ a primary ideal, and $\mathfrak{p}$, $\mathfrak{r}$ prime ideals.

(1) Assume $\mathfrak{q} \subset \mathfrak{p}$ and $\mathfrak{r} \subsetneqq \mathfrak{p}$. Show $\mathfrak{r} \subset \mathfrak{q}$. (2) Assume $\mathfrak{r} = \sqrt{\mathfrak{q}} \subsetneqq \mathfrak{p}$. Show $\mathfrak{r} = \mathfrak{q}$.
(3) Assume $\mathfrak{r} \subsetneqq \mathfrak{p}$. Show $\mathfrak{r}$ is the intersection of all primary ideals contained in $\mathfrak{p}$.
(4) Assume $\mathfrak{p}$ and $\mathfrak{r}$ are not comaximal. Show one contains the other.

Exercise (18.28) . — Let $\mathbb{Z}[X]$ be the polynomial ring, and set $\mathfrak{m} := \langle 2, X \rangle$ and $\mathfrak{q} := \langle 4, X \rangle$. Show $\mathfrak{m}$ is maximal, $\mathfrak{q}$ is $\mathfrak{m}$-primary, and $\mathfrak{q}$ is not a power of $\mathfrak{m}$.

Exercise (18.29) . — Let k be a field, $R := k[X,Y,Z]$ the polynomial ring in three variables. Set $\mathfrak{p}_1 := \langle X, Y \rangle$, set $\mathfrak{p}_2 := \langle X, Z \rangle$, set $\mathfrak{m} := \langle X, Y, Z \rangle$, and set $\mathfrak{a} := \mathfrak{p}_1\mathfrak{p}_2$. Show that $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is an irredundant primary decomposition. Which associated primes are minimal, and which are embedded?

Exercise (18.30) . — Let k be a field, $R := k[X,Y,Z]$ be the polynomial ring. Set $\mathfrak{a} := \langle XY,\ X - YZ \rangle$, set $\mathfrak{q}_1 := \langle X, Z \rangle$ and set $\mathfrak{q}_2 := \langle Y^2, X - YZ \rangle$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ holds and that this expression is an irredundant primary decomposition.

Exercise (18.31) . — For $i = 1, 2$, let R_i be a ring, M_i a R_i-module with $0 \subset M_i$ primary. Find an irredundant primary decomposition for $0 \subset M_1 \times M_2$ over $R_1 \times R_2$.

Exercise (18.32) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} = \sqrt{\mathfrak{a}}$. Prove (1) every prime $\mathfrak{p}$ associated to $\mathfrak{a}$ is minimal over $\mathfrak{a}$ and (2) if R is Noetherian, then the converse holds, and $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}(R/\mathfrak{a})} \mathfrak{p}$ is an irredundant primary decomposition. Find a simple example showing (1) doesn't generalize to modules.

Exercise (18.33) . — Let R be a ring, M a module. We call a proper submodule Q **irreducible** if $Q = N_1 \cap N_2$ implies $Q = N_1$ or $Q = N_2$. Prove: (1) an irreducible submodule Q is primary if M/Q is Noetherian; and (2) a proper submodule N is the intersection of finitely many irreducible submodules if M/N is Noetherian.

Exercise (18.34) . — Let R be a ring, M a module, N a submodule. Consider:

(1) The submodule N is old-primary.
(2) Given any multiplicative subset S, there is $s \in S$ with $N^S = (N : \langle s \rangle)$.
(3) Given any $x \in R$, the sequence $(N : \langle x \rangle) \subset (N : \langle x^2 \rangle) \subset \cdots$ stabilizes.

Prove (1) implies (2), and (2) implies (3). Prove (3) implies (1) if N is irreducible.

Exercise (18.35) . — Let R be a ring, M a Noetherian module, N a submodule, $\mathfrak{m} \subset \mathrm{rad}(M)$ an ideal. Show $N = \bigcap_{n \geq 0}(\mathfrak{m}^n M + N)$.

C. Appendix: Old-primary Submodules

Lemma (18.36). — *Let R be a ring, and $Q \subsetneqq P \subset M$ modules. Assume Q is old-primary in M. Then $\mathrm{nil}(M/Q) = \mathrm{nil}(P/Q)$ and Q is old-primary in P.*

Proof: First, $\mathrm{nil}(M/Q) \subset \mathrm{nil}(P/Q)$ since $\mathrm{Ann}(M/Q) \subset \mathrm{Ann}(P/Q)$ because $P/Q \subset M/Q$. Second, $\mathrm{nil}(P/Q) \subset \mathrm{z.div}(P/Q)$ by **(17.11.1)**. Third, again as $P/Q \subset M/Q$, so $\mathrm{z.div}(P/Q) \subset \mathrm{z.div}(M/Q)$. Fourth, Q is old-primary in M; so $\mathrm{z.div}(M/Q) = \mathrm{nil}(M/Q)$ by **(18.3)**(1). Thus $\mathrm{nil}(M/Q) = \mathrm{nil}(P/Q) = \mathrm{z.div}(P/Q)$. Finally, by **(18.3)**(1) again, Q is old-primary in P. □

Proposition (18.37). — *Let R be a ring, and L, N, $Q_1, \dots, Q_n \subset M$ modules with $N = \bigcap_{i=1}^n Q_i$. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$.*

(1) *Then $\sqrt{(N:L)} = \bigcap_{i=1}^n \sqrt{(Q_i:L)}$.* (2) *Then $\mathrm{nil}(M/N) = \bigcap_{i=1}^n \mathfrak{p}_i$.*

(3) *Assume $N \subsetneqq \bigcap_{i=2}^n Q_i$. Given $m \in \big(\bigcap_{i=2}^n Q_i\big) - N$, let $\overline{m} \in M/N$ denote its residue. Then $\mathfrak{p}_1 \subset \sqrt{\mathrm{Ann}(\overline{m})} \subset \mathrm{z.div}(M/N)$. Further, if Q_1 is old-primary too, then $\mathrm{Ann}(\overline{m})$ is old-primary and $\mathfrak{p}_1 = \sqrt{\mathrm{Ann}(\overline{m})}$.*

(4) *Let $\overline{m} \in M/N$ be any nonzero element, and $\mathfrak{p}$ any minimal prime of $\mathrm{Ann}(\overline{m})$. Assume $Q_1, \dots, Q_n$ are old-primary. Then $\mathfrak{p} = \mathfrak{p}_i$ for some i.*

(5) *Assume $Q_1, \dots, Q_n$ are old-primary. Then $\mathrm{z.div}(M/N) \subset \bigcup_{i=1}^n \mathfrak{p}_i$.*

(6) *Assume $N \subsetneqq \bigcap_{i \neq j} Q_i$ for all j, and $Q_1, \dots, Q_n$ are old-primary. Then $\mathrm{z.div}(M/N) = \bigcup_{i=1}^n \mathfrak{p}_i$.*

Proof: For (1), recall **(4.17)**(5) asserts $(N:L) = \bigcap_{i=1}^n (Q_i:L)$. And **(3.32)**(1) asserts $\sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$ for any ideals $\mathfrak{a}$, $\mathfrak{b}$. Thus (1) holds.

For (2), note $(N:M) = \mathrm{Ann}(M/N)$ and $(Q_i:M) = \mathrm{Ann}(Q_i/N)$ owing to **(4.17)**(2). Thus (1) with $L := M$ yields (2).

For (3), given $x \in \mathfrak{p}_1$, say $x^h \in \mathrm{Ann}(M/Q_1)$ with $h \geq 1$. Then $x^h m \subset Q_i$ for all i. So $x^h m \in N$. Thus $\mathfrak{p}_1 \subset \sqrt{\mathrm{Ann}(\overline{m})}$.

Next, given $y \in \sqrt{\mathrm{Ann}(\overline{m})}$, take $k \geq 0$ minimal with $y^k \overline{m} = 0$. But $m \notin N$. So $k \geq 1$. Set $m' := y^{k-1} m$. Then $m' \notin N$, but $ym' \in N$. Thus $y \in \mathrm{z.div}(M/N)$. Thus $\sqrt{\mathrm{Ann}(\overline{m})} \subset \mathrm{z.div}(M/N)$.

Further, assume Q_1 is old-primary too. Given $x, y \in R$ with $xy \in \mathrm{Ann}(\overline{m})$ but $y \notin \mathrm{Ann}(\overline{m})$, then $xym \in Q_1$ but $ym \notin Q_1$. Hence $x \in \mathfrak{p}_1$ as Q_1 is old-primary. Thus $\mathrm{Ann}(\overline{m})$ is old-primary.

Finally, given $z \in \sqrt{\mathrm{Ann}(\overline{m})}$, there's $l \geq 1$ with $z^l m \in N$. So $z^l m \in Q_1$. But $m \notin Q_1$, and Q_1 is old-primary. So $z^l \in \mathfrak{p}_1$. But $\mathfrak{p}_1$ is prime by **(18.3)**(2). So $z \in \mathfrak{p}_1$. Thus $\mathfrak{p}_1 \supset \sqrt{\mathrm{Ann}(\overline{m})}$. Thus (3) holds.

For (4), take an $m \in M - N$ that represents $\overline{m}$. Reorder the Q_i so that $m \notin Q_i$ if and only if $i \leq h$. Apply (1) with $L := Rm$, and let's identify the terms. First, $(N:L) = \mathrm{Ann}((N+L)/N)$ and $(Q_i:L) = \mathrm{Ann}((Q_i+L)/Q_i)$ for all i by **(4.17)**(2).

Note $\mathrm{Ann}((N+L)/N) = \mathrm{Ann}(\overline{m})$. So $\sqrt{(N:L)} \subset \mathfrak{p}$. Moreover, $Q_i \subsetneqq Q_i + L$ for $i \leq h$, and Q_i is old-primary; so $\mathrm{nil}((Q_i+L)/Q_i) = \mathfrak{p}_i$ by **(18.36)**. But $Q_i + L = Q_i$ for $i > h$; so $\mathrm{nil}((Q_i+L)/Q_i) = R$. So (1) yields $\mathfrak{p} \supset \bigcap_{i \leq h} \mathfrak{p}_i$. Thus, as $\mathfrak{p}$ is prime, **(2.25)**(1) yields $\mathfrak{p} \supset \mathfrak{p}_j$ for some $j \leq h$.

Given $x \in \mathrm{Ann}(\overline{m})$, note $xm \in N \subset Q_j$. But $m \notin Q_j$ as $j \leq h$. So $x \in \mathfrak{p}_j$ as Q_j is old-primary. Thus $\mathfrak{p}_j \supset \mathrm{Ann}(\overline{m})$. But $\mathfrak{p}$ is a minimal prime of $\mathrm{Ann}(\overline{m})$. Thus $\mathfrak{p} = \mathfrak{p}_j$. Thus (4) holds.

In (5), given $x \in \mathrm{z.div}(M/N)$, take $m \in M - N$ with $xm \in N$. Then $m \notin Q_i$ for some i. But $xm \in Q_i$, and Q_i is old-primary. So $x \in \mathfrak{p}_i$. Thus (5) holds.

Finally, (6) follows immediately from (3) and (5). □

Lemma (18.38). — *Let R be a ring, M a module, Q an old-primary submodule $m \in M$, and $\overline{m}$ its residue in M/Q. Set $\mathfrak{p} := \operatorname{nil}(M/Q)$. Then*

(1) *If $m \notin Q$, then $\operatorname{Ann}(\overline{m})$ is old-primary and $\mathfrak{p} = \sqrt{\operatorname{Ann}(\overline{m})}$.*

(2) *Given $x \in R - \mathfrak{p}$, then $(Q : \langle x \rangle) = Q$.*

Proof: Note (1) is just **(18.37)**(3) with $N = Q_1$ and $n = 1$ as $\bigcap_{i=2}^{1} Q_i = R$ by convention.

For (2), suppose $m \in (Q : \langle x \rangle)$. Then $xm \in Q$. But $x \notin \mathfrak{p}$. So $m \in Q$ as Q is old-primary. Thus $(Q : \langle x \rangle) \subset Q$. Conversely, $(Q : \langle x \rangle) \supset Q$ by **(4.16)**(2). Thus (2) holds. □

Theorem (18.39). — *Let R be a ring, M a module. Let $\mathcal{D}(M)$ or $\mathcal{D}_R(M)$ denote the set of primes $\mathfrak{p}$ each minimal over some $\operatorname{Ann}(m)$ for $m \in M$.*

(1) *Then $\operatorname{z.div}(M) = \bigcup_{\mathfrak{p} \in \mathcal{D}(M)} \mathfrak{p}$.* (2) *Set $N := \bigcap_{\mathfrak{p} \in \mathcal{D}(M)} 0^{S_\mathfrak{p}}$. Then $N = 0$.*

(3) *Let $S \subset R$ be a multiplicatively closed subset. Then*

$$\mathcal{D}_{S^{-1}R}(S^{-1}M) = \{\, S^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathcal{D}_R(M) \text{ and } \mathfrak{p} \cap S = \emptyset \,\}.$$

(4) *Assume $0 = \bigcap_{i=1}^{n} Q_i$ with the Q_i old-primary. For all j, assume $\bigcap_{i \neq j} Q_i \neq 0$. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$. Then $\mathcal{D}(M) = \{\mathfrak{p}_i\}_{i=1}^{n}$.*

(5) *Then $\operatorname{Ass}(M) \subset \mathcal{D}(M)$, with equality if R or M is Noetherian.*

Proof: In (1), given $x \in \operatorname{z.div}(M)$, there's $m \in M$ nonzero with $x \in \operatorname{Ann}(m)$. As $\operatorname{Ann}(m)$ is proper, there's a prime $\mathfrak{p}$ minimal over it owing to **(2.21)**, **(2.15)**, and **(3.16)**. Thus $x \in \mathfrak{p} \in \mathcal{D}(M)$. Thus $\operatorname{z.div}(M) \subset \bigcup_{\mathfrak{p} \in \mathcal{D}(M)} \mathfrak{p}$..

Conversely, given $\mathfrak{p} \in \mathcal{D}(M)$ and $x \in \mathfrak{p}$, say $\mathfrak{p}$ is minimal over $\operatorname{Ann}(m)$. Then $\mathfrak{p}$ consists of zerodivisors modulo $\operatorname{Ann}(m)$ by **(14.7)**. So there 's $y \in R - \operatorname{Ann}(m)$ with $xym = 0$. But $ym \neq 0$. Thus $x \in \operatorname{z.div}(M)$. Thus $\operatorname{z.div}(M) \supset \bigcup_{\mathfrak{p} \in \mathcal{D}(M)} \mathfrak{p}$. Thus (1) holds.

In (2), given $m \in M$ nonzero, again as $\operatorname{Ann}(m)$ is proper, there's a prime $\mathfrak{p}$ minimal over it owing to **(2.21)**, **(2.15)**, and **(3.16)**. So there's no $s \in S_\mathfrak{p}$ with $sm = 0$. So $m \notin 0^{S_\mathfrak{p}}$. Thus $m \notin N$. Thus (2) holds.

In (3), given any $m \in M$ with $\operatorname{Ann}_R(m) \cap S = \emptyset$ and any $s \in S$, it's easy to show:

$$\operatorname{Ann}_R(m)^S = \operatorname{Ann}_R(m/1) = \operatorname{Ann}_R(m/s) \supset \operatorname{Ann}_R(m). \tag{18.39.1}$$

Next, given $\mathfrak{p} \in \mathcal{D}_R(M)$ with $\mathfrak{p} \cap S = \emptyset$, say $\mathfrak{p}$ is minimal over $\operatorname{Ann}_R(m)$. Set $\mathfrak{P} := S^{-1}\mathfrak{p}$. Then $\mathfrak{P} \supset S^{-1}\operatorname{Ann}_R(m)$; also $\mathfrak{P}$ is prime by **(11.12)**(2). Given a prime $\mathfrak{Q}$ of $S^{-1}R$ with $\mathfrak{P} \supset \mathfrak{Q} \supset S^{-1}\operatorname{Ann}_R(m)$, set $\mathfrak{q} := \varphi_S^{-1}\mathfrak{Q}$. Then $\mathfrak{q}$ is prime, and $\varphi_S^{-1}\mathfrak{P} \supset \mathfrak{q} \supset \varphi_S^{-1}S^{-1}\operatorname{Ann}_R(m)$. So $\mathfrak{p} \supset \mathfrak{q} \supset \operatorname{Ann}_R(m)^S$ by **(12.12)**(3)(a) and **(11.11)**(3)(a). But $\mathfrak{p}$ is minimal over $\operatorname{Ann}_R(m)^S$ owing to **(18.39.1)**. So $\mathfrak{p} = \mathfrak{q}$. So $\mathfrak{P} = \mathfrak{Q}$ by **(11.12)**(2). Thus $\mathfrak{P}$ is minimal over $S^{-1}\operatorname{Ann}_R(m)$. But **(12.17)**(1) with $M := Rm$ yields $S^{-1}\operatorname{Ann}_R(m) = \operatorname{Ann}_{S^{-1}R}(m/1)$. Thus $\mathfrak{P} \in \mathcal{D}_{S^{-1}R}(S^{-1}M)$.

Here $\mathfrak{p} \mapsto \mathfrak{P}$ is injective by **(11.12)**(2). So we have left to show it's surjective.

Given $\mathfrak{P} \in \mathcal{D}_{S^{-1}R}(S^{-1}M)$, set $\mathfrak{p} := \varphi_S^{-1}\mathfrak{P}$. Then $\mathfrak{p}$ is prime, $\mathfrak{p} \cap S = \emptyset$, and $\mathfrak{P} = S^{-1}\mathfrak{p}$ by **(11.12)**(2). Thus we have left to show $\mathfrak{p} \in \mathcal{D}_R(M)$.

Say $\mathfrak{P}$ is minimal over $\operatorname{Ann}_{S^{-1}R}(m/s)$. But $\operatorname{Ann}_{S^{-1}R}(m/s) = \operatorname{Ann}_{S^{-1}R}(m/1)$ as $1/s$ is a unit. Moreover, again $\operatorname{Ann}_{S^{-1}R}(m/1) = S^{-1}\operatorname{Ann}_R(m)$ by **(12.17)**(1) with $M := Rm$. Thus $\mathfrak{P}$ is minimal over $S^{-1}\operatorname{Ann}_R(m)$.

So $\mathfrak{p} \supset \varphi_S^{-1} S^{-1} \operatorname{Ann}_R(m)$. So **(12.12)**(3)(a) yields $\mathfrak{p} \supset \operatorname{Ann}_R(m)$. Now, given a prime $\mathfrak{q}$ of R with $\mathfrak{p} \supset \mathfrak{q} \supset \operatorname{Ann}_R(m)$, note $\mathfrak{P} \supset S^{-1}\mathfrak{q} \supset S^{-1} \operatorname{Ann}_R(m)$. But $\mathfrak{P}$ is minimal over $S^{-1} \operatorname{Ann}_R(m)$. So $\mathfrak{P} = S^{-1}\mathfrak{q}$. So $\mathfrak{p} = \mathfrak{q}$ by **(11.12)**(2). Thus $\mathfrak{p}$ is minimal over $\operatorname{Ann}_R(m)$. Thus $\mathfrak{p} \in \mathcal{D}_R(M)$, as desired. Thus (3) holds.

For (4), given $\mathfrak{p} \in \mathcal{D}(M)$, say $\mathfrak{p}$ is minimal over $\operatorname{Ann}(m)$. Thus by **(18.37)**(4), $\mathfrak{p} = \mathfrak{p}_i$ for some i. Thus $\mathcal{D}(M) \subset \{\mathfrak{p}_i\}_{i=1}^n$.

Conversely, each $\mathfrak{p}_i$ is of the form $\sqrt{\operatorname{Ann}(m)}$ for some $m \neq 0$ by **(18.37)**(3). Then $\mathfrak{p}_i$ is minimal over $\operatorname{Ann}(m)$; indeed, given a prime $\mathfrak{q} \supset \operatorname{Ann}(M/Q_i)$ and $x \in \mathfrak{p}_i$, there's $n \geq 1$ with $x^n \in \operatorname{Ann}(M/Q_i)$, so $x^n \in \mathfrak{q}$, so $x \in \mathfrak{q}$, and thus $\mathfrak{q} \supset \mathfrak{p}_i$. Thus $\mathcal{D}(M) \supset \{\mathfrak{p}_i\}$. Thus (4) holds.

In (5), given $\mathfrak{p} := \operatorname{Ann}(m) \in \operatorname{Ass}(M)$, note $\mathfrak{p} \in \mathcal{D}(M)$. Thus $\operatorname{Ass}(M) \subset \mathcal{D}_R(M)$.

If M is Noetherian, so is $R/\operatorname{Ann}(M)$ by **(16.16)**. Fix $\mathfrak{p} \in \mathcal{D}(M)$. Then, under either Noetherian hypothesis, $\mathfrak{p}$ is finitely generated modulo $\operatorname{Ann}(M)$. Therefore, $\mathfrak{p} \in \operatorname{Ass}(M)$ if $S_\mathfrak{p}^{-1}\mathfrak{p} \in \operatorname{Ass}(S_\mathfrak{p}^{-1}M)$ by **(17.8)**. But $S_\mathfrak{p}^{-1}\mathfrak{p} \in \mathcal{D}_{S_\mathfrak{p}^{-1}R}(S_\mathfrak{p}^{-1}M)$ by (3). Thus we may localize at $\mathfrak{p}$ and so assume R is local and $\mathfrak{p}$ is its maximal ideal.

Say $\mathfrak{p}$ is minimal over $\operatorname{Ann}(m)$. Then $m \neq 0$. Also if M is Noetherian, so is Rm. So under either Noetherian hypothesis, **(17.10)** gives a $\mathfrak{q} \in \operatorname{Ass}(Rm) \subset \operatorname{Ass}(M)$. Then $\mathfrak{q} = \operatorname{Ann}(m')$ with $m' \in Rm$; so $\mathfrak{q} \supset \operatorname{Ann}(m)$. As $\mathfrak{p}$ is maximal, $\mathfrak{p} \supset \mathfrak{q}$. But $\mathfrak{p}$ is minimal over $\operatorname{Ann}(m)$. So $\mathfrak{p} = \mathfrak{q}$. Thus $\operatorname{Ass}(M) \supset \mathcal{D}_R(M)$. Thus (5) holds. □

Lemma (18.40). — *Let R be a ring, $N \subsetneqq M$ modules, $\mathfrak{p}$ be a minimal prime of $\operatorname{Ann}(M/N)$. Assume M/N is finitely generated. Recall $S_\mathfrak{p} := R - \mathfrak{p}$, and set $Q := N^{S_\mathfrak{p}}$. Then $\mathfrak{p} = \operatorname{nil}(M/Q)$ and Q is old-primary.*

Proof: Set $\mathfrak{a} := \operatorname{Ann}(M/N)$. Then $\mathfrak{p}$ is a minimal prime of $\mathfrak{a}$. So $\mathfrak{p}R_\mathfrak{p}$ is the only prime of $R_\mathfrak{p}$ containing $\mathfrak{a}R_\mathfrak{p}$ by **(11.12)**(2). Thus **(3.14)** yields $\mathfrak{p}R_\mathfrak{p} = \sqrt{\mathfrak{a}R_\mathfrak{p}}$.

Set $\mathfrak{n} := \operatorname{nil}(M/Q)$ and $\mathfrak{b} := \operatorname{Ann}(M/Q)$. Given $x \in \mathfrak{n}$, there's $n \geq 1$ with $x^n \in \mathfrak{b}$. So $x^n/1 \in \mathfrak{b}_\mathfrak{p}$. But $\mathfrak{b}_\mathfrak{p} \subset \operatorname{Ann}(M_\mathfrak{p}/Q_\mathfrak{p})$ by **(12.17)**(1). Now, $Q_\mathfrak{p} = N_\mathfrak{p}$ by **(12.12)**(3)(b). Also $M_\mathfrak{p}/N_\mathfrak{p} = (M/N)_\mathfrak{p}$ by **(12.13)**. But M/N is finitely generated. So $\operatorname{Ann}(M/N)_\mathfrak{p} = \mathfrak{a}_\mathfrak{p}$ again by **(12.17)**(1). Thus $x^n/1 \in \mathfrak{a}_\mathfrak{p}$. So there's $s \in S_\mathfrak{p}$ with $sx^n \in \mathfrak{a}$. But $\mathfrak{a} \subset \mathfrak{p}$, and $\mathfrak{p}$ is prime. Hence $x \in \mathfrak{p}$. Thus $\mathfrak{n} \subset \mathfrak{p}$.

Conversely, let $x \in \mathfrak{p}$. Then $x/1 \in \mathfrak{p}R_\mathfrak{p}$. Recall $\mathfrak{p}R_\mathfrak{p} = \sqrt{\mathfrak{a}R_\mathfrak{p}}$. So there's $n \geq 1$ with $x^n/1 \in \mathfrak{a}R_\mathfrak{p}$. So there's $s \in S_\mathfrak{p}$ with $sx^n \in \mathfrak{a}$. So $sx^nM \subset N$. Hence $x^nM \subset Q$. So $x^n \in \mathfrak{b}$. So $x \in \mathfrak{n}$. Thus $\mathfrak{p} \subset \mathfrak{n}$. Thus $\mathfrak{p} = \mathfrak{n}$.

As M/N is finitely generated, $\mathbf{V}(\mathfrak{a}) = \operatorname{Supp}(M/N)$ by **(13.4)**(3). But $\mathfrak{p} \in \mathbf{V}(\mathfrak{a})$. So $\mathfrak{p} \in \operatorname{Supp}(M/N)$. So $(M/N)_\mathfrak{p} \neq 0$. So $N_\mathfrak{p} \neq M_\mathfrak{p}$ by **(12.13)**. Thus $N^{S_\mathfrak{p}} \neq M$.

Let $x \in R$ and $m \in M$ with $xm \in Q$, but $m \notin Q$. Recall $Q_\mathfrak{p} = N_\mathfrak{p}$. Hence $xm/1 \in N_\mathfrak{p}$, but $m/1 \notin N_\mathfrak{p}$. So $x/1 \notin R_\mathfrak{p}^\times$. Thus $x \in \mathfrak{p}$. But $\mathfrak{p} = \mathfrak{n}$. Thus Q is old-primary, as desired. □

Proposition (18.41). — *Let R be a ring, and M a module with this property:*

(L1) *Given any submodule N and prime $\mathfrak{p}$, there's $x \in S_\mathfrak{p}$ with $xN^{S_\mathfrak{p}} \subset N$.*

Assume M finitely generated. Let $N \subsetneqq M$ be a submodule.

(1) *Given a minimal prime $\mathfrak{p}$ of $\operatorname{Ann}(M/N)$ and x as in* (L1)*, set $Q := N^{S_\mathfrak{p}}$ and $P := N + xM$. Then Q is old-primary, $\mathfrak{p} = \operatorname{nil}(M/Q)$, and $P \supsetneqq N = Q \cap P$.*

(2) *Then N is an intersection of old-primary submodules.*

Proof: In (1), note that $N \subset Q \cap P$. Conversely, given $m \in Q \cap P$, say that $m = n + xm'$ with $n \in N$ and $m' \in M$. But $m \in Q$ and $N \subset Q$. So $xm' \in Q$. But Q is old-primary and $\mathfrak{p} = \operatorname{nil}(M/Q)$ by **(18.40)**. Also $x \notin \mathfrak{p}$. So $m' \in Q$. But

$xQ \subset N$. So $xm' \in N$. So $m \in N$. Thus $N \supset Q \cap P$. Thus $N = Q \cap P$.

Finally, $x \notin \mathfrak{p}$ and $\mathfrak{p} \supset \operatorname{Ann}(M/N)$. So $xM \not\subset N$. Thus $P \supsetneqq N$. Thus (1) holds.

For (2), let $\mathcal{S}$ be the set of pairs $(\mathcal{Q}, P)$ where $\mathcal{Q}$ is a set of old-primary submodules Q and where P is a submodule with $N = (\bigcap_{Q\in\mathcal{Q}} Q) \cap P$. Order $\mathcal{S}$ by coordinatewise inclusion. Note $\mathcal{S}$ is nonempty as $(\emptyset, N) \in \mathcal{S}$. Every linearly ordered subset $(\mathcal{Q}_\lambda,\ P_\lambda)$ has an upper bound, namely $(\mathcal{Q}, P)$ with $\mathcal{Q} := \bigcup \mathcal{Q}_\lambda$, where this union takes place in the set of subsets of M, and with $P := \bigcup P_\lambda$. Thus Zorn's Lemma implies $\mathcal{S}$ has a maximal element $(\mathcal{Q}, P)$.

Suppose $P \neq M$. Then (1) yields $P = Q_1 \cap P_1$ where Q_1 is old-primary and P_1 is a submodule with $P_1 \supsetneqq P$. Set $\mathcal{Q}_1 := \mathcal{Q} \cup \{Q_1\}$. Then $(\mathcal{Q}_1, P_1) > (\mathcal{Q}, P)$, a contradiction. Thus $P = M$ and $N = \bigcap_{Q\in\mathcal{Q}} Q$, as required. Thus (2) holds. □

Proposition (18.42). — *Let R be a ring, M a Noetherian module.*

(1) *Then the condition* (L1) *of* (**18.41**) *holds.*
(2) *Then each proper submodule N is a finite intersection of old-primary submodules.*

Proof: In (1), given any submodule N and prime $\mathfrak{p}$, as M is Noetherian, there are $m_1, \dots, m_r \in N^{S_\mathfrak{p}}$ that generate $N^{S_\mathfrak{p}}$. For each i, there's $x_i \in S_\mathfrak{p}$ with $x_i m_i \in N$. Set $x := \prod x_i$. Then $xN^{S_\mathfrak{p}} \subset N$. Thus (1) holds.

For (2), form the set $\mathcal{S}$ of all submodules P of M for which there are finitely many old-primary submodules Q_i with $N = (\bigcap Q_i) \cap P$. As M is Noetherian, there's a maximal P. If $P \neq M$, then (**18.41**)(1) provides a submodule $P' \supsetneqq P$ and an old-primary submodule Q with $P = Q \cap P'$. So $N = ((\bigcap Q_i) \cap Q) \cap P'$, in contradiction to the maximality of P. Thus $P = M$. Thus (2) holds. □

Proposition (18.43). — *Let R be a ring, S a multiplicatively closed subset, and $Q \subsetneqq M$ modules. Set $\mathfrak{p} := \operatorname{nil}(M/Q)$. Assume Q is old-primary and $S \cap \mathfrak{p} = \emptyset$. Then $Q^S = Q$ and $S^{-1}Q$ is old-primary in $S^{-1}M$ over $S^{-1}R$.*

Proof: Given $s \in S$ and $m \in M$ with $sm \in Q$, note $m \in Q$, as $s \notin \mathfrak{p}$ and Q is old-primary. Thus $Q^S \subset Q$. But $Q^S \supset Q$ always. Thus $Q^S = Q$.

Note $S^{-1}Q \subsetneqq S^{-1}M$ as $\varphi_S^{-1} S^{-1}Q = Q^S$ by (**12.12**)(3)(a), but $Q^S = Q \subsetneqq M$.

Given $x \in R$, $m \in M$ and $s, t \in S$ with $xm/st \in S^{-1}Q$, but $m/t \notin S^{-1}Q$, there's $u \in S$ with $uxm \in Q$, but $um \notin Q$. So $x \in \mathfrak{p}$ as Q is old-primary. So $x/s \in S^{-1}\mathfrak{p}$. But $S^{-1}\mathfrak{p} \subset \operatorname{nil}(S^{-1}M/S^{-1}Q)$ by (**12.40**). Thus $S^{-1}Q$ is old-primary. □

Proposition (18.44). — *Let R be a ring, M a finitely generated module. Along with* (L1) *of* (**18.41**), *consider this property of M:*

(L2) *Given any submodule $N \subsetneqq M$ and given any descending chain $S_1 \supset S_2 \supset \cdots$ of multiplicatively closed subsets, the chain $N^{S_1} \supset N^{S_2} \supset \cdots$ stabilizes.*

If every submodule $N \subsetneqq M$ is a finite intersection of old-primary submodules, then (L1) *and* (L2) *hold. Conversely, assume N isn't such an intersection and* (L1) *holds. Then there are submodules $Q_1, \dots, Q_m$ and $N_0, N_1, \dots, N_m$ such that:*

(1) *Each Q_i is old-primary. Also $N_0 := N$, and $N_{m-1} \subsetneqq N_m \subsetneqq M$ if $m \geq 1$.*
(2) *If $m \geq 1$, then N_m is maximal among the P such that $N = \bigcap_{i=1}^m Q_i \cap P$.*
(3) *For $i \leq m$, set $\mathfrak{p}_i := \operatorname{Ann}(M/Q_i)$. If $m \geq 1$, then $\operatorname{Ann}(M/N_m) \not\subset \mathfrak{p}_i$ for $i \leq m$.*
(4) *If $m \geq 1$, set $S_m := R - \bigcup_{i\leq m} \mathfrak{p}_i$. Then $N^{S_m} = \bigcap_{i=1}^m Q_i$.*
(5) *If $m \geq 1$, then $S_{m-1} \supset S_m$, but $N^{S_{m-1}} \supsetneqq N^{S_m}$.*

Proof: First, say $N=\bigcap_{i=1}^m Q_i$ with old-primary Q_i. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$.

Given a multiplicatively closed subset S, note $N^S=\bigcap_{i=1}^m Q_i^S$ by **(12.12)**(6)(a). Say $S\cap\mathfrak{p}_i=\emptyset$ if and only if $i\le n$. Then $Q_i^S=Q_i$ for $i\le n$ by **(18.43)**. But $Q_i^S=M$ for $i>n$ by **(12.41)**(2). Thus $N^S=\bigcap_{i=1}^n Q_i$ and $N=N^S\cap\bigcap_{i>n}Q_i$.

To check (L1), let $\mathfrak{p}$ be a prime, and take $S:=S_{\mathfrak{p}}$. Then $\mathfrak{p}_i\subset\mathfrak{p}$ if and only if $i\le n$. For each $i>n$, take $x_i\in\mathfrak{p}_i-\mathfrak{p}$. Say $n_i\ge 0$ with $x_i^{n_i}\in\mathrm{Ann}(M/Q_i)$. Set $x:=\prod x_i^{n_i}$; so $x=1$ if $n=m$. Then $x\in\mathrm{Ann}(M/Q_i)$ for each $i>n$, and $x\notin\mathfrak{p}$. So $xM\subset Q_i$, and $x\in S_{\mathfrak{p}}$. Hence $xN^{S_{\mathfrak{p}}}\subset N^{S_{\mathfrak{p}}}\cap\bigcap_{i>n}Q_i=N$. Thus (L1) holds.

As to (L2), for each i, say $S_i\cap\mathfrak{p}_j=\emptyset$ if and only if $j\le n_i$. But $S_1\supset S_2\supset\cdots$. So $n_1\le n_2\le\cdots\le m$. So the n_i stabilize. But $N^{S_i}=\bigcap_{j=1}^{n_i}Q_j$. Thus (L2) holds.

Conversely, assume N isn't a finite intersection of old-primary submodules, and (L1) holds. Set $N_0:=N$, and given $n\ge 0$, say $Q_1,\dots,Q_n$ and $N_0,N_1,\dots,N_n$ satisfy (1)–(5) for $m=n$. Let's find suitable Q_{n+1} and N_{n+1}.

Note $N_n\subsetneqq M$ by (1). So $\mathrm{Ann}(M/N_n)\neq R$. So there's a minimal prime $\mathfrak{p}_{n+1}$ of $\mathrm{Ann}(M/N_n)$, and so an x as in (L1). Set $Q_{n+1}:=N_n^{S_{\mathfrak{p}_{n+1}}}$ and $P:=N_n+xM$. Then Q_{n+1} is old-primary, $\mathfrak{p}_{n+1}=\mathrm{nil}(M/Q_{n+1})$, and $P\supsetneqq N_n=Q_{n+1}\cap P$ by **(18.41)**(1).

Form the set $\mathcal{S}$ of submodules U of M with $U\supset P$ and $N=\bigcap_{i=1}^{n+1}Q_i\cap U$. Then $P\in\mathcal{S}$ as $N=\bigcap_{i=1}^n Q_i\cap N_n$ by (2). Given a linearly ordered subset $\{P_\lambda\}$ of $\mathcal{S}$, set $U:=\bigcup P_\lambda$. If $u\in\bigcap_{i=1}^{n+1}Q_i\cap U$, then $u\in\bigcap_{i=1}^{n+1}Q_i\cap P_\lambda$ for some λ; so $U\in\mathcal{S}$. So U is an upper bound. So Zorn's Lemma yields a maximal element in $\mathcal{S}$, say N_{n+1}.

Note $N_n\subsetneqq N_{n+1}$ as $N_n\subsetneqq P\subset N_{n+1}$. And $N_{n+1}\subsetneqq M$; otherwise, $N=\bigcap_{i=1}^{n+1}Q_i$ but N isn't a finite intersection of old-primary submodules. Thus $Q_1,\dots,Q_{n+1}$ and $N_0,N_1,\dots,N_{n+1}$ satisfy (1)–(2) for $m=n+1$.

As to (3) for $m=n+1$, note $\mathrm{Ann}(M/N_n)\subset\mathrm{Ann}(M/N_{n+1})$ as $N_n\subset N_{n+1}$. So $\mathrm{Ann}(M/N_{n+1})\not\subset\mathfrak{p}_i$ for $i\le n$ by (3) for $m=n$. But $x\in\mathrm{Ann}(M/N_{n+1})$ as $N_{n+1}\supset P$. But $x\notin\mathfrak{p}_{n+1}$. So $\mathrm{Ann}(M/N_{n+1})\not\subset\mathfrak{p}_{n+1}$. Thus (3) holds for $m=n+1$.

As to (4) for $m=n+1$, note $\mathrm{Ann}(M/N_{n+1})\not\subset\bigcup_{i=1}^{n+1}\mathfrak{p}_i$ by (3) for $m=n+1$ and by Prime Avoidance **(3.12)**. Hence there's $y\in\mathrm{Ann}(M/N_{n+1})-\bigcup_{i=1}^{n+1}\mathfrak{p}_i$. Then $yM\subset N_{n+1}$. Hence $M=N_{n+1}^{S_{n+1}}$. Now, $N=\bigcap_{i=1}^{n+1}Q_i\cap N_{n+1}$ by (2) for $m=n+1$. So $N^{S_{n+1}}=\bigcap_{i=1}^{n+1}Q_i^{S_{n+1}}\cap N_{n+1}^{S_{n+1}}$ by **(12.12)**(6)(a). And $Q_i^{S_{n+1}}=Q_i$ by **(18.43)**(1). Thus (4) holds for $m=n+1$.

As to (5) for $m=n+1$, plainly $S_n\supset S_{n+1}$. Now, $N_n\subsetneqq N_{n+1}$ by (1) for $m=n+1$. So (2) for $m=n$ gives $N\subsetneqq\bigcap_{i=1}^n Q_i\cap N_{n+1}$. But $N=\bigcap_{i=1}^{n+1}Q_i\cap N_{n+1}$ by (2) for $m=n+1$. Hence $\bigcap_{i=1}^n Q_i\supsetneqq\bigcap_{i=1}^{n+1}Q_i$. So (4) for $m=n,n+1$ implies $N^{S_n}\supsetneqq N^{S_{n+1}}$. Thus (5) holds for $m=n+1$.

Finally, (5) for all m implies that the S_m form a descending chain $S_1\supset S_2\supset\cdots$, but that the chain $N^{S_1}\supset N^{S_2}\supset\cdots$ doesn't stabilize, as desired. □

Exercise (18.45) . — Let $\varphi\colon R\to R'$ be a ring map, M an R-module, $Q'\subsetneqq M'$ R'-modules, $\alpha\colon M\to M'$ an R-map. Set $Q:=\alpha^{-1}Q'$, and assume $Q\subsetneqq M$. Set $\mathfrak{p}:=\mathrm{nil}(M/Q)$ and $\mathfrak{p}':=\mathrm{nil}(M'/Q')$. If Q' is old-primary, show Q is and $\varphi^{-1}\mathfrak{p}'=\mathfrak{p}$. Conversely, when φ and α are surjective, show Q' is old-primary if Q is.

Proposition (18.46). — *Let R be a ring, S a multiplicative subset, and M a module. Then the map $Q\mapsto S^{-1}Q$ is an inclusion-preserving bijection from the old-primary submodules of M with $\mathrm{nil}(M/Q)\cap S=\emptyset$ onto the old-primary $S^{-1}R$-submodules K of $S^{-1}M$. The inverse is $K\mapsto\varphi_S^{-1}K$.*

Proof: The map in question is well defined by **(18.43)**. It is injective because $\varphi_S^{-1}S^{-1}Q = Q^S$ by **(12.12)**(3)(a) and $Q = Q^S$ by **(18.43)**. Finally, it's surjective with inverse $K \mapsto \varphi_S^{-1}K$ as $\varphi_S^{-1}K$ is old-primary by **(18.45)** and $S^{-1}\varphi_S^{-1}K = K$ for any submodule K of $S^{-1}R$ by **(12.12)**(2)(b). □

Proposition (18.47). — *Let R be a ring, S a multiplicative subset, and M a module. Let $N, Q_1, \ldots, Q_n$ be submodules with $N = \bigcap_{i=1}^n Q_i$ and the Q_i old-primary. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$, and assume $S \cap \mathfrak{p}_i = \emptyset$ just for $i \le t$. Then*

(1) *Then $S^{-1}N = \bigcap_{i=1}^t S^{-1}Q_i \subset S^{-1}M$ and $N^S = \bigcap_{i=1}^t Q_i \subset M$.*
(2) *Then the $S^{-1}Q_i$ are old primary just for $i \le t$.*
(3) *Set $\mathfrak{P}_i := \operatorname{nil}(S^{-1}M/S^{-1}Q_i)$. For $i \ne j$ and $j \le t$, if $\mathfrak{p}_i \ne \mathfrak{p}_j$, then $\mathfrak{P}_i \ne \mathfrak{P}_j$.*
(4) *For $j \le t$, if $Q_j \not\supset \bigcap_{i\le t,\ i\ne j} Q_i$, then $S^{-1}Q_j \not\supset \bigcap_{i \le t,\ i \ne j} S^{-1}Q_i$.*

Proof: In (1), note $S^{-1}N = \bigcap_{i=1}^r S^{-1}Q_i$ and $N^S = \bigcap_{i=1}^r Q_i^S$ by **(12.12)**(6). But $S^{-1}Q_i = S^{-1}M$ and $Q_i^S = M$ for $i > t$ by **(12.23)**. Thus (1) holds.

Note (2) results immediately from **(18.43)** and **(12.23)**.

Note (3) holds as $\mathfrak{p}_j = \varphi_S^{-1}\mathfrak{P}_j$ for $j \le t$ by **(18.45)**.

Note (4) holds as $Q_j = Q_j^S = \varphi_S^{-1}S^{-1}Q_j$ by **(18.43)** and **(12.12)**(3)(a). □

Theorem (18.48). — *Let $N, Q_1, \ldots, Q_r \subsetneqq M$ be modules, $\mathcal{S}$ some set of minimal primes of $\operatorname{Ann}(M/N)$. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$ and $S := \bigcap_{\mathfrak{p}\in\mathcal{S}} S_{\mathfrak{p}}$. Assume $\mathfrak{p}_i \in \mathcal{S}$ just for $i \le t$, the Q_i are old-primary, and $N = \bigcap_{i=1}^r Q_i$. Then $N^S = \bigcap_{i=1}^t Q_i$.*

Proof: Fix $1 \le i \le r$. First, assume $i \le t$. Then $\mathfrak{p}_i \in \mathcal{S}$. Thus $S \cap \mathfrak{p}_i = \emptyset$.

Next, assume $t < i$ and $S \cap \mathfrak{p}_i = \emptyset$. Then $\mathfrak{p}_i \subset \bigcup_{\mathfrak{p}\in\mathcal{S}} \mathfrak{p}$. So **(3.12)** provides $\mathfrak{p} \in \mathcal{S}$ with $\mathfrak{p}_i \subset \mathfrak{p}$. But $N \subset Q_i$; hence, $\operatorname{Ann}(M/N) \subset \operatorname{Ann}(M/Q_i) \subset \mathfrak{p}_i$. But $\mathfrak{p}$ is minimal over $\operatorname{Ann}(M/N)$. Hence $\mathfrak{p}_i = \mathfrak{p} \in \mathcal{S}$, contradicting $t < i$. Thus $S \cap \mathfrak{p}_i \ne \emptyset$.

Finally, **(18.47)**(1) yields $N^S = \bigcap_{i=1}^t Q_i$. □

Proposition (18.49). — *Let $N, Q_1, \ldots, Q_n \subsetneqq M$ be modules with $N = \bigcap_{i=1}^n Q_i$. Assume the Q_i are old-primary. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$ and $X := \operatorname{Supp}(M/N)$. Then*

(1) *Set $\mathfrak{a} := \operatorname{Ann}(M/N)$. Then every minimal prime $\mathfrak{p}$ of $\mathfrak{a}$ is one of the $\mathfrak{p}_i$.*
(2) *If M/N is finitely generated, then X has at most n irreducible components.*

Proof: In (1), $\mathfrak{p} \supset \operatorname{nil}(M/N)$. So **(18.37)**(2) gives $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. Note $\mathfrak{p}_i \supset \mathfrak{a}$. Also $\mathfrak{p}_i$ is prime by **(18.3)**(2). So $\mathfrak{p} = \mathfrak{p}_i$ as $\mathfrak{p}$ is minimal. Thus (1) holds.

For (2), assume M/N is finitely generated. So $\operatorname{Supp}(M/N) = \mathbf{V}(\mathfrak{a})$ by **(13.4)**(3). But $\mathfrak{a}$ has at most n minimal primes by (1). Thus **(16.51)**(3) yields (2). □

D. Appendix: Exercises

Exercise (18.50) . — Let $\mathfrak{q} \subset \mathfrak{p}$ be primes, M a module, and Q an old-primary submodule with $\operatorname{nil}(M/Q) = \mathfrak{q}$. Then $0^{S_{\mathfrak{p}}} \subset Q$.

Exercise (18.51) . — Let R be an absolutely flat ring, $\mathfrak{q}$ an old-primary ideal. Show that $\mathfrak{q}$ is maximal.

Exercise (18.52) . — Let X be an infinite compact Hausdorff space, R the ring of continuous $\mathbb{R}$-valued functions on X. Using **(14.26)**, show that $\langle 0\rangle$ is not a finite intersection of old-primary ideals.

Exercise (18.53) . — Let R be a ring, X a variable, $N, Q \subset M$ modules, and $N = \bigcap_{i=1}^{r} Q_i$ a decomposition. Assume Q is old-primary. Assume $N = \bigcap_{i=1}^{r} Q_i$ is irredundant; that is, **(18.13)**(1)–(2) hold. Show:

(1) Assume M is finitely generated. Let $\mathfrak{p}$ be a minimal prime of M. Then $\mathfrak{p}[X]$ is a minimal prime of $M[X]$.
(2) Then $\mathrm{nil}\big(M[X]/N[X]\big) = \mathrm{nil}(M/N)[X]$.
(3) Then $Q[X]$ is old-primary in $M[X]$.
(4) Then $N[X] = \bigcap_{i=1}^{r} Q_i[X]$ is irredundant in $M[X]$.

Exercise (18.54) . — Let k be a field, $P := k[X_1, \dots, X_n]$ the polynomial ring. Given i, set $\mathfrak{p}_i := \langle X_1, \dots, X_i\rangle$. Show $\mathfrak{p}_i$ is prime, and all its powers are $\mathfrak{p}_i$ -primary.

Exercise (18.55) . — Let R be a ring, $\mathfrak{p}$ a prime, M a finitely generated module. Set $Q := 0^{S_\mathfrak{p}} \subset M$. Show (1) and (2) below are equivalent, and imply (3):

(1) $\mathrm{nil}(M/Q) = \mathfrak{p}$. (2) $\mathfrak{p}$ is minimal over $\mathrm{Ann}(M)$. (3) Q is old-primary.

Also, if M/Q is Noetherian, show (1) and (2) above and (3′) below are equivalent:

(3′) Q is $\mathfrak{p}$-primary.

Exercise (18.56) . — Let R be a ring, M a module, Σ the set of minimal primes of $\mathrm{Ann}(M)$. Assume M is finitely generated. Set $N := \bigcap_{\mathfrak{p}\in\Sigma} 0^{S_\mathfrak{p}}$. Show:

(1) Given $\mathfrak{p} \in \Sigma$, the saturation $0^{S_\mathfrak{p}}$ is the smallest old-primary submodule Q with $\mathrm{nil}(M/Q) = \mathfrak{p}$.
(2) Say $0 = \bigcap_{i=1}^{r} Q_i$ with the Q_i old-primary. For all j, assume $Q_j \not\supset \bigcap_{i\neq j} Q_i$. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$. Then $N = 0$ if and only if $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} = \Sigma$.
(3) If $M = R$, then $N \subset \mathrm{nil}(R)$.

Exercise (18.57) . — Let R be a ring, $N \subsetneqq M$ modules. Assume there exists a decomposition $N = \bigcap_{i=1}^{n} Q_i$ with the Q_i old-primary. Show that there are at most finitely many submodules of M of the form N^S where S is a multiplicative subset.

Exercise (18.58) . — Let R be a ring, M a module, $\mathfrak{p} \in \mathrm{Supp}(M)$. Fix m, $n \geq 1$. Set $(\mathfrak{p}M)^{(n)} := (\mathfrak{p}^n M)^{S_\mathfrak{p}}$ and $\mathfrak{p}^{(n)} := (\mathfrak{p})^{(n)}$. (We call $\mathfrak{p}^{(n)}$ the ***n*th symbolic power** of $\mathfrak{p}$.) Assume M is finitely generated. Set $N := \mathfrak{p}^{(m)}(\mathfrak{p}M)^{(n)}$. Show:

(1) Then $\mathfrak{p}$ is the smallest prime containing $\mathrm{Ann}(M/\mathfrak{p}^n M)$.
(2) Then $(\mathfrak{p}M)^{(n)}$ is old-primary, and $\mathrm{nil}\big(M/(\mathfrak{p}M)^{(n)}\big) = \mathfrak{p}$.
(3) Say $\mathfrak{p}^n M = \bigcap_{i=1}^{r} Q_i$ with Q_i old-primary. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$. Assume $\mathfrak{p}_i = \mathfrak{p}$ if and only if $i \leq t$. Then $(\mathfrak{p}M)^{(n)} = \bigcap_{i=1}^{t} Q_i$.
(4) Then $(\mathfrak{p}M)^{(n)} = \mathfrak{p}^n M$ if and only if $\mathfrak{p}^n M$ is old-primary.
(5) Let Q be an old-primary submodule with $\mathrm{nil}(M/Q) = \mathfrak{p}$. Assume $\mathfrak{p}$ is finitely generated modulo $\mathrm{Ann}(M/Q)$. Then $Q \supset (\mathfrak{p}M)^{(n)}$ if $n \gg 0$.
(6) Then $N^{S_\mathfrak{p}} = (\mathfrak{p}M)^{(m+n)}$ and $\mathfrak{p}$ is the smallest prime containing $\mathrm{Ann}(M/N)$.
(7) Say $N = \bigcap_{i=1}^{r} Q_i$ with all Q_i old-primary. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$. Assume $\mathfrak{p}_i = \mathfrak{p}$ if and only if $i \leq t$. Then $Q_i = (\mathfrak{p}M)^{(m+n)}$ for some i.

Exercise (18.59) . — Let R be a ring, $f \in R$, and $N, Q_1, \dots, Q_n \subsetneqq M$ modules with $N = \bigcap_{i=1}^{n} Q_i$ and the Q_i old-primary. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$ for all i. Assume $f \in \mathfrak{p}_i$ just for $i > h$. Show $\bigcap_{i=1}^{h} Q_i = N^{S_f} = (N : \langle f^n\rangle)$ for $n \gg 0$.

Exercise (18.60) . — Let R be a ring, $\mathfrak{p}$ a prime ideal, M a Noetherian module. Denote the intersection of all $\mathfrak{p}$-primary submodules by N. Show $N = 0^{S_\mathfrak{p}}$.

Exercise (18.61) . — Let R be a ring, M a module, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Supp}(M)$ distinct primes, none minimal in $\operatorname{Supp}(M)$. Assume M is finitely generated, and (*) below holds (it does, by **(18.60)** and **(18.3)**(4)–(5), if M is Noetherian):

(*) For every prime $\mathfrak{p}$, the saturation $0^{S_\mathfrak{p}}$ is equal to the intersection of all the old-primary submodules Q with $\operatorname{nil}(M/Q) = \mathfrak{p}$.

(1) For $1 \le i < n$, assume $\mathfrak{p}_i \not\supset \mathfrak{p}_n$ and let Q_i be an old-primary submodule with $\operatorname{nil}(M/Q_i) = \mathfrak{p}_i$ and $\bigcap_{j \ne i} Q_j \not\subset Q_i$. Set $P := \bigcap_{j<n} Q_j$. Show $P \not\subset 0^{S_{\mathfrak{p}_n}}$.

(2) In the setup of (1), show there is an old-primary submodule Q_n such that $\operatorname{nil}(M/Q_n) = \mathfrak{p}_n$ and $P \not\subset Q_n$. Then show $\bigcap_{j \ne i} Q_j \not\subset Q_i$ for all i.

(3) Use (2) and induction on n to find old-primary submodules $Q_1, \ldots, Q_n$ with $\operatorname{nil}(M/Q_i) = \mathfrak{p}_i$ and $\bigcap_{j \ne i} Q_j \not\subset Q_i$ for all i.

Exercise (18.62) . — Let R be a ring, M a module, Q an old-primary submodule. Set $\mathfrak{q} := \operatorname{Ann}(M/Q)$. Show that $\mathfrak{q}$ is old-primary.

Exercise (18.63) . — Let $\varphi\colon R \to R'$ be a ring map, and M an R-module. Set $M' := M \otimes_R R'$ and $\alpha := 1_M \otimes \varphi$. Let $N' = \bigcap_{i=1}^r Q_i'$ be a decomposition in M' with each Q_i' old-primary. Set $N := \alpha^{-1}N'$ and $Q_i := \alpha^{-1}Q_i'$. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$ and $\mathfrak{p}_i' := \operatorname{nil}(M'/Q_i')$. Show:

(1) Then $N = \bigcap_{i=1}^r Q_i$ with Q_i old-primary, and $\mathfrak{p}_i = \varphi^{-1}\mathfrak{p}_i'$ for all i.

(2) Assume R' is flat and $N' = R'\alpha(N)$. Assume $N' \ne \bigcap_{i \ne j} Q_i'$ for all j, but $N = \bigcap_{i=1}^t Q_i$ with $t < r$. Fix $t < i \le r$. Then $\mathfrak{p}_i \subset \mathfrak{p}_j$ for some $j \le t$.

Exercise (18.64) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module, $0 = \bigcap Q_i$ a finite decomposition with Q_i old-primary. Set $\mathfrak{p}_i = \operatorname{nil}(M/Q_i)$. Show $\Gamma_\mathfrak{a}(M) = \bigcap_{\mathfrak{a} \not\subset \mathfrak{p}_i} Q_i$. (If $\mathfrak{a} \subset \mathfrak{p}_i$ for all i, then $\bigcap_{\mathfrak{a} \not\subset \mathfrak{p}_i} Q_i = M$ by convention.)

Exercise (18.65) . — Let R be a ring; N, $Q_i \subset M$ modules with Q_i old-primary.

(1) Assume $N = \bigcap_{i=1}^r Q_i$. Set $\mathfrak{p}_i = \operatorname{nil}(M/Q_i)$. Show $N = \bigcap_{i=1}^r \varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i})$.

(2) Assume M/N is Noetherian. Show $\bigcap_{\mathfrak{p} \in \operatorname{Ass}(M/N)} \varphi_\mathfrak{p}^{-1}(N_\mathfrak{p}) = N$.

Exercise (18.66) . — Let $\varphi\colon R \to R'$ be a ring map, M' an R'-module, $M \subset M'$ an R-submodule, and $\mathfrak{p} \in \mathcal{D}_R(M)$. Assume $0 = \bigcap_{i=1}^r Q_i'$ with the Q_i' old-primary R'-submodules. Show there's $\mathfrak{p}' \in \mathcal{D}_{R'}(M')$ with $\varphi^{-1}\mathfrak{p}' = \mathfrak{p}$.

Exercise (18.67) . — Let R be a ring, M a module, $0 = \bigcap_{i=1}^n Q_i$ an old-primary decomposition in M. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$. Assume $\bigcap_{j \ne i} Q_j \ne 0$ for all i, the $\mathfrak{p}_i$ are distinct, M is finitely generated, and $\mathfrak{p}_1$ is finitely generated mod $\operatorname{Ann}(M)$. Show:

(1) Suppose that $\mathfrak{p}_1$ is minimal over $\operatorname{Ann}(M)$. Then $Q_1 = (\mathfrak{p}_1 M)^{(r)}$ for $r \gg 0$.

(2) Suppose that $\mathfrak{p}_1$ is not minimal over $\operatorname{Ann}(M)$. Show that replacing Q_1 by $(\mathfrak{p}_1 M)^{(r)}$ for $r \gg 0$ gives infinitely many distinct old-primary decompositions of 0, still with $\bigcap_{j \ne i} Q_j \ne 0$ for all i and the $\mathfrak{p}_i$ distinct. (Thus, when R is Noetherian, then 0 has infinitely many irredundant primary decompositions, which differ only in the first component.)

19. Length

The length of a module is a generalization of the dimension of a vector space. The length is the number of links in a **composition series**, which is a finite chain of submodules whose successive quotients are simple — that is, their only proper submodules are zero. Our main result is the Jordan–Hölder Theorem: any two composition series do have the same length and even the same successive quotients; further, their annihilators are just the primes in the support of the module, and the module is equal to the product of its localizations at these primes. Hence, the length is finite if and only if the module is both Artinian and Noetherian.

We also prove the Akizuki–Hopkins Theorem: a ring is Artinian if and only if it is Noetherian and every prime is maximal. Consequently, a ring is Artinian if and only if its length is finite; if so, then it is the product of Artinian local rings.

Lastly, we study **parameter ideals** $\mathfrak{q}$ of a module M; by definition, $M/\mathfrak{q}M$ is of finite length, and $\mathfrak{q}$ lies in the **radical** $\mathrm{rad}(M)$, which is the intersection of all the maximal ideals containing the annihilator $\mathrm{Ann}(M)$. So if M is the ring R itself, then $R/\mathfrak{q}$ is a product of Artinian local rings; moreover, we prove that then $R/\mathfrak{q}$ has at least as many idempotents as R, with equality if and only if R is decomposable.

A. Text

(19.1) (Length). — Let R be a ring, and M a module. We call M **simple** if it is nonzero and its only proper submodule is 0. We call a chain of submodules,

$$M = M_0 \supset M_1 \supset \cdots \supset M_m = 0 \qquad \textbf{(19.1.1)}$$

a **composition series** of **length** m if each successive quotient M_{i-1}/M_i is simple.

We define the **length** $\ell(M)$ or $\ell_R(M)$ to be the infimum of all those lengths:

$$\ell(M) := \inf\{\, m \mid M \text{ has a composition series of length } m \,\}. \qquad \textbf{(19.1.2)}$$

By convention, if M has no composition series, then $\ell(M) := \infty$. Further, $\ell(M) = 0$ if and only if $M = 0$.

For example, if R is a field, then M is a vector space and $\ell(M) = \dim_R(M)$. Also, the chains in **(17.32)** are composition series, but those in **(17.31)** are not.

Given a submodule $N \subset M$, we call $\ell(M/N)$ the **colength** of N.

Exercise (19.2) . — Let R be a ring, M a module. Prove these statements:

(1) If M is simple, then any nonzero element $m \in M$ generates M.
(2) M is simple if and only if $M \simeq R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and if so, then $\mathfrak{m} = \mathrm{Ann}(M)$.
(3) If M has finite length, then M is finitely generated.

Theorem (19.3) (Jordan–Hölder)**. —** *Let R be a ring, and M a module with a composition series* **(19.1.1)***. Then any chain of submodules can be refined to a composition series, and every composition series is of length $\ell(M)$. Also,*

$$\mathrm{Supp}(M) = \{\, \mathfrak{m} \in \mathrm{Spec}(R) \mid \mathfrak{m} = \mathrm{Ann}(M_{i-1}/M_i) \text{ for some } i \,\};$$

the $\mathfrak{m} \in \mathrm{Supp}(M)$ are maximal; given i, there is an $\mathfrak{m} \in \mathrm{Supp}(M)$ such that

$M_{i-1}/M_i \simeq R/\mathfrak{m}_i$; there is a canonical isomorphism

$$M \xrightarrow{\sim} \textstyle\prod_{\mathfrak{m}\in \mathrm{Supp}(M)} M_{\mathfrak{m}}; \tag{19.3.1}$$

and $\ell(M_{\mathfrak{m}})$ is equal to the number of i with $\mathfrak{m} = \mathrm{Ann}(M_{i-1}/M_i)$.

Proof: First, let M' be a proper submodule of M. Let's show that

$$\ell(M') < \ell(M). \tag{19.3.2}$$

To do so, set $M'_i := M_i \cap M'$. Then $M'_{i-1} \cap M_i = M'_i$. So

$$M'_{i-1}/M'_i = (M'_{i-1} + M_i)/M_i \subset M_{i-1}/M_i.$$

Since M_{i-1}/M_i is simple, either $M'_{i-1}/M'_i = 0$, or $M'_{i-1}/M'_i = M_{i-1}/M_i$ and so

$$M'_{i-1} + M_i = M_{i-1}. \tag{19.3.3}$$

If **(19.3.3)** holds and if $M_i \subset M'$, then $M_{i-1} \subset M'$. Hence, if **(19.3.3)** holds for all i, then $M \subset M'$, a contradiction. Therefore, there is an i with $M'_{i-1}/M'_i = 0$. Now, $M' = M'_0 \supset \cdots \supset M'_m = 0$. Omit M'_i whenever $M'_{i-1}/M'_i = 0$. Thus M' has a composition series of length strictly less than m. Therefore, $\ell(M') < m$ for any choice of **(19.1.1)**. Thus **(19.3.2)** holds.

Next, given a chain $N_0 \supsetneqq \cdots \supsetneqq N_n = 0$, let's prove $n \le \ell(M)$ by induction on $\ell(M)$. If $\ell(M) = 0$, then $M = 0$; so also $n = 0$. Assume $\ell(M) \ge 1$. If $n = 0$, then we're done. If $n \ge 1$, then $\ell(N_1) < \ell(M)$ by **(19.3.2)**; so $n - 1 \le \ell(N_1)$ by induction. Thus $n \le \ell(M)$.

If N_{i-1}/N_i is not simple, then there is N' with $N_{i-1} \supsetneqq N' \supsetneqq N_i$. The new chain can have length at most $\ell(M)$ by the previous paragraph. Repeating, we can refine the given chain into a composition series in at most $\ell(M) - n$ steps.

Suppose the given chain is a composition series. Then $\ell(M) \le n$ by **(19.1.2)**. But we proved $n \le \ell(M)$ above. Thus $n = \ell(M)$, and the first assertion is proved.

To proceed, fix a prime $\mathfrak{p}$. Exactness of Localization, **(12.13)**, yields this chain:

$$M_{\mathfrak{p}} = (M_0)_{\mathfrak{p}} \supset (M_1)_{\mathfrak{p}} \supset \cdots \supset (M_m)_{\mathfrak{p}} = 0. \tag{19.3.4}$$

Now, consider a maximal ideal $\mathfrak{m}$. If $\mathfrak{p} = \mathfrak{m}$, then $(R/\mathfrak{m})_{\mathfrak{p}} \simeq R/\mathfrak{m}$ by **(12.4)**(2) and **(12.1)**. If $\mathfrak{p} \ne \mathfrak{m}$, then there is $s \in \mathfrak{m} - \mathfrak{p}$; so $(R/\mathfrak{m})_{\mathfrak{p}} = 0$.

Set $\mathfrak{m}_i := \mathrm{Ann}(M_{i-1}/M_i)$. So $M_{i-1}/M_i \simeq R/\mathfrak{m}_i$ and $\mathfrak{m}_i$ is maximal by **(19.2)**(2). Then Exactness of Localization yields $(M_{i-1}/M_i)_{\mathfrak{p}} = (M_{i-1})_{\mathfrak{p}}/(M_i)_{\mathfrak{p}}$. Hence

$$(M_{i-1})_{\mathfrak{p}}/(M_i)_{\mathfrak{p}} = \begin{cases} 0, & \text{if } \mathfrak{p} \ne \mathfrak{m}_i; \\ M_{i-1}/M_i \simeq R/\mathfrak{m}_i, & \text{if } \mathfrak{p} = \mathfrak{m}_i. \end{cases}$$

Thus $\mathrm{Supp}(M) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_m\}$.

If we omit the duplicates from the chain **(19.3.4)**, then we get a composition series from the $(M_i)_{\mathfrak{p}}$ with $M_{i-1}/M_i \simeq R/\mathfrak{p}$. Thus the number of such i is $\ell(M_{\mathfrak{p}})$.

Finally, $(M_{\mathfrak{m}_i})_{\mathfrak{m}_j} = 0$ if $i \ne j$ by the above. So **(13.59)** yields **(19.3.1)**. □

Exercise (19.4) . — Let R be a ring, M a Noetherian module. Show that the following three conditions are equivalent:

(1) M has finite length;
(2) $\mathrm{Supp}(M)$ consists entirely of maximal ideals;
(3) $\mathrm{Ass}(M)$ consists entirely of maximal ideals.

Show that, if the conditions hold, then $\mathrm{Ass}(M)$ and $\mathrm{Supp}(M)$ are equal and finite.

Corollary (19.5). — *A module M is both Artinian and Noetherian if and only if M is of finite length.*

Proof: Any chain $M \supset N_0 \supsetneqq \cdots \supsetneqq N_n = 0$ has $n \le \ell(M)$ by the Jordan–Hölder Theorem, (**19.3**). So if $\ell(M) < \infty$, then M satisfies both the dcc and the acc.

Conversely, assume M is both Artinian and Noetherian. Form a chain as follows. Set $M_0 := M$. For $i \ge 1$, if $M_{i-1} \ne 0$, take a maximal $M_i \subsetneqq M_{i-1}$ by the maxc. By the dcc, this recursion terminates. Then the chain is a composition series. □

Example (19.6). — Any simple $\mathbb{Z}$-module is finite owing to (**19.2**)(2). Hence, a $\mathbb{Z}$-module is of finite length if and only if it is finite. In particular, $\ell(\mathbb{Z}) = \infty$.

Of course, $\mathbb{Z}$ is Noetherian, but not Artinian.

Let $p \in \mathbb{Z}$ be a prime, and set $M := \mathbb{Z}[1/p]\big/\mathbb{Z}$. Then M is an Artinian $\mathbb{Z}$-module, but not Noetherian by (**16.44**). Also, as M is infinite, $\ell(M) = \infty$.

Theorem (19.7) (Additivity of Length). — *Let M be a module, and M' a submodule. Then $\ell(M) = \ell(M') + \ell(M/M')$.*

Proof: If M has a composition series, then the Jordan–Hölder Theorem yields another one of the form $M = M_0 \supset \cdots \supset M' \supset \cdots \supset M_m = 0$. The latter yields a pair of composition series: $M/M' = M_0/M' \supset \cdots \supset M'/M' = 0$ and $M' \supset \cdots \supset M_m = 0$. Conversely, every such pair arises from a unique composition series in M through M'. Therefore, $\ell(M) < \infty$ if and only if $\ell(M/M') < \infty$ and $\ell(M') < \infty$; furthermore, if so, then $\ell(M) = \ell(M') + \ell(M/M')$, as desired. □

Theorem (19.8) (Akizuki–Hopkins). — *A ring R is Artinian if and only if R is Noetherian and $\dim(R) = 0$. If so, then R has only finitely many primes.*

Proof: Assume $\dim(R) = 0$. Then, by definition, every prime is both maximal and minimal. Assume also R is Noetherian.

Then R has finite length by (**19.4**). Thus R is Artinian by (**19.5**).

Alternatively, recall that any minimal prime is associated by (**17.14**), and that $\operatorname{Ass}(R)$ is finite by (**17.17**). Thus R has only finitely many primes, all maximal.

Set $\mathfrak{n} := \operatorname{nil}(R)$. It is the intersection of all the primes by (**3.14**), so of finitely many maximal ideals. So $\mathfrak{n}$ is their product by (**1.21**)(4)(b). But $\mathfrak{n}$ is finitely generated, as R is Noetherian. So $\mathfrak{n}^k = 0$ for $k >> 0$ by (**3.38**). Thus some (finite) product of maximal ideals is 0. Thus (**16.43**) implies that R is Artinian.

Conversely, assume R is Artinian. Let $\mathfrak{m}$ be a minimal (finite) product of maximal ideals of R. Then $\mathfrak{m}^2 = \mathfrak{m}$. Let $\mathcal{S}$ be the set of ideals $\mathfrak{a}$ contained in $\mathfrak{m}$ such that $\mathfrak{a}\mathfrak{m} \ne 0$. If $\mathcal{S} \ne \emptyset$, take $\mathfrak{a} \in \mathcal{S}$ minimal. Then $\mathfrak{a}\mathfrak{m}^2 = \mathfrak{a}\mathfrak{m} \ne 0$; hence, $\mathfrak{a}\mathfrak{m} = \mathfrak{a}$ by minimality of $\mathfrak{a}$. Given $x \in \mathfrak{a}$ with $x\mathfrak{m} \ne 0$, note $\mathfrak{a} = \langle x \rangle$ by minimality of $\mathfrak{a}$.

Given any maximal ideal $\mathfrak{n}$, note $\mathfrak{n}\mathfrak{m} = \mathfrak{m}$ by minimality of $\mathfrak{m}$. But $\mathfrak{n}\mathfrak{m} \subset \mathfrak{n}$. Thus $\mathfrak{m} \subset \operatorname{rad}(R)$. But $\mathfrak{a} = \langle x \rangle$; so $\mathfrak{a}$ is finitely generated. So Nakayama's Lemma yields $\mathfrak{a} = 0$, a contradiction. So $x\mathfrak{m} = 0$ for any $x \in \mathfrak{a}$. Thus $\mathfrak{a}\mathfrak{m} = 0$, a contradiction. Thus $\mathcal{S} = \emptyset$. So $\mathfrak{m}^2 = 0$. But $\mathfrak{m}^2 = \mathfrak{m}$. So $\mathfrak{m} = 0$. Thus some product of maximal ideals is 0. Thus (**16.43**) implies that R is Noetherian, and (**2.24**) implies that R has only finitely many primes, all maximal; in particular, $\dim(R) = 0$. □

Corollary (19.9). — *Let R be an Artinian ring, and M a finitely generated module. Then M has finite length, and $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ are equal and finite.*

Proof: By (**19.8**) every prime is maximal, so $\mathrm{Supp}(M)$ consists of maximal ideals. Also R is Noetherian by (**19.8**). So M is Noetherian by (**16.15**). Hence (**19.4**) yields the assertions. □

Corollary (19.10). — *A ring R is Artinian if and only if $\ell(R) < \infty$.*

Proof: Simply take $M := R$ in (**19.9**) and (**19.5**). □

Corollary (19.11). — *A ring R is Artinian if and only if R is a finite product of Artinian local rings; if so, then $R = \prod_{\mathfrak{m}\in\mathrm{Spec}(R)} R_{\mathfrak{m}}$.*

Proof: A finite product of rings is Artinian if and only if each factor is Artinian by (**16.22**)(3). If R is Artinian, then $\ell(R) < \infty$ by (**19.10**); whence, $R = \prod R_{\mathfrak{m}}$ by the Jordan–Hölder Theorem, (**19.3.1**). Thus the assertion holds. □

Definition (19.12). — Let R be a ring, $\mathfrak{q}$ an ideal, M a nonzero module. If $\mathfrak{q} \subset \mathrm{rad}(M)$ and $\ell(M/\mathfrak{q}M) < \infty$, call $\mathfrak{q}$ a **parameter ideal of** M.

Lemma (19.13). — *Let R be a ring, $\mathfrak{q}$ an ideal, M a nonzero module. Assume that M is Noetherian or just that M is finitely generated and $M/\mathfrak{q}M$ is Noetherian. Set $\mathfrak{m} := \mathrm{rad}(M)$ and $\mathfrak{q}' := \mathrm{Ann}(M/\mathfrak{q}M)$. Then these conditions are equivalent:*

(1) *$\mathfrak{q}$ is a parameter ideal.*
(2) *$\mathfrak{q} \subset \mathfrak{m}$, and $\mathrm{Supp}(M/\mathfrak{q}M)$ consists of finitely many maximal ideals.*
(3) *$\mathfrak{q} \subset \mathfrak{m}$, and $\boldsymbol{V}(\mathfrak{q}')$ consists of finitely many maximal ideals.*
(4) *M is semilocal, and $\boldsymbol{V}(\mathfrak{q}') = \boldsymbol{V}(\mathfrak{m})$.*
(5) *M is semilocal, and $\sqrt{\mathfrak{q}'} = \mathfrak{m}$.*
(6) *M is semilocal, and $\mathfrak{m}^n \subset \mathfrak{q}' \subset \mathfrak{m}$ for some $n \geq 1$.*

Proof: First, (1) and (2) are equivalent by (**19.4**), as $M/\mathfrak{q}M$ is Noetherian.

Next, (2) and (3) are equivalent, as $\mathbf{V}(\mathfrak{q}') = \mathrm{Supp}(M/\mathfrak{q}M)$ by (**13.4**)(3).

Assume (3). As M is finitely generated, $\mathbf{V}(\mathfrak{q}') = \mathbf{V}(\mathfrak{q} + \mathrm{Ann}(M))$ by (**13.46**)(2). But $\mathfrak{q}, \mathrm{Ann}(M) \subset \mathfrak{m}$. So $\mathbf{V}(\mathfrak{q} + \mathrm{Ann}(M)) \supset \mathbf{V}(\mathfrak{m})$. Thus $\mathbf{V}(\mathfrak{q}') \supset \mathbf{V}(\mathfrak{m})$.

Conversely, given $\mathfrak{n} \in \mathbf{V}(\mathfrak{q}')$, note $\mathfrak{n} \supset \mathfrak{q}' \supset \mathrm{Ann}(M)$. But $\mathfrak{n}$ is maximal by (3). So $\mathfrak{n} \supset \mathfrak{m}$. Thus $\mathbf{V}(\mathfrak{q}') \subset \mathbf{V}(\mathfrak{m})$. Thus $\mathbf{V}(\mathfrak{q}') = \mathbf{V}(\mathfrak{m})$. So $\mathbf{V}(\mathfrak{m})$ consists of finitely many maximal ideals by (3). Thus M is semilocal. Thus (4) holds.

To see that (4) and (5) are equivalent, note that $\mathbf{V}(\mathfrak{q}') = \mathbf{V}(\mathfrak{m})$ if and only if $\sqrt{\mathfrak{q}'} = \sqrt{\mathfrak{m}}$ by (**13.1**). But plainly $\sqrt{\mathfrak{m}} = \mathfrak{m}$. Thus (4) and (5) are equivalent.

Let's see that (4) and (5) together imply (3). First, $\sqrt{\mathfrak{q}'} = \mathfrak{m}$ by (5). But plainly $\mathfrak{q} \subset \mathfrak{q}' \subset \sqrt{\mathfrak{q}'}$. Thus $\mathfrak{q} \subset \mathfrak{m}$.

By (4) or (5), M is semilocal; say the maximal ideals containing $\mathrm{Ann}(M)$ are $\mathfrak{m}_1, \dots, \mathfrak{m}_r$. So $\mathfrak{m} := \bigcap \mathfrak{m}_i$. Given $\mathfrak{p} \in \mathbf{V}(\mathfrak{m})$, note $\mathfrak{p} \supset \mathfrak{m} \supset \prod \mathfrak{m}_i$. But $\mathfrak{p}$ is prime. So $\mathfrak{p} \supset \mathfrak{m}_{i_0}$ for some i_0. But $\mathfrak{m}_{i_0}$ is maximal. So $\mathfrak{p} = \mathfrak{m}_{i_0}$. Thus $\mathbf{V}(\mathfrak{m}) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_r\}$. But $\mathbf{V}(\mathfrak{q}') = \mathbf{V}(\mathfrak{m})$ by (4). Thus (3) holds.

Assume (5). Then $\mathfrak{q}' \subset \sqrt{\mathfrak{q}'} = \mathfrak{m}$. Further, as $M/\mathfrak{q}M$ is Noetherian, so is $R/\mathfrak{q}'$ by (**16.16**). So $\mathfrak{m}/\mathfrak{q}'$ is finitely generated. But $\mathfrak{m}/\mathfrak{q}' = \sqrt{0}$. So $(\mathfrak{m}/\mathfrak{q}')^n = 0$ for some $n \geq 1$ by (**3.38**). So $\mathfrak{m}^n \subset \mathfrak{q}'$. Thus (6) holds.

Finally, assume (6). Then $\sqrt{\mathfrak{q}'} = \sqrt{\mathfrak{m}}$. But $\sqrt{\mathfrak{m}} = \mathfrak{m}$. Thus (5) holds. □

Proposition (19.14). — *Let R be a ring, and M a nonzero Noetherian module. Set $\mathfrak{m} := \mathrm{rad}(M)$. If M has a parameter ideal, then M is semilocal; conversely, if M is semilocal, then $\mathfrak{m}^n$ is a parameter ideal for any $n \geq 1$.*

Moreover, if R has a parameter ideal $\mathfrak{q}$, then $\mathfrak{q}$ is a parameter ideal of M too.

Proof: The first assertion results immediately from (1)⇔(6) of **(19.13)**.

Assume R has a parameter ideal $\mathfrak{q}$. Then $\ell(R/\mathfrak{q}) < \infty$. So $R/\mathfrak{q}$ is Noetherian by **(19.5)**. Apply (1)⇒(3) of **(19.13)** with $M := R$. Thus $\mathfrak{q} \subset \operatorname{rad}(R)$, and $\mathbf{V}(\mathfrak{q})$ consists of finitely many maximal ideals (as $\mathfrak{q}' = \mathfrak{q}$ in **(19.13)**).

Note $\operatorname{rad}(R) \subset \operatorname{rad}(M)$. So $\mathfrak{q} \subset \operatorname{rad}(M)$. Set $\mathfrak{q}' := \operatorname{Ann}(M/\mathfrak{q}M)$. Then $\mathfrak{q}' \supset \mathfrak{q}$, so $\mathbf{V}(\mathfrak{q}') \subset \mathbf{V}(\mathfrak{q})$. Apply (3)⇒(1) of **(19.13)**. Thus $\mathfrak{q}$ is a parameter ideal of M. □

Theorem (19.15). — *Let R be a ring, $\mathfrak{q}$ a parameter ideal. Let $\kappa\colon R \to R/\mathfrak{q}$ be the quotient map, $\{\mathfrak{m}_i\}$ the set of maximal ideals, δ_{ij} the Kronecker delta function.*

(1) *Then R is semilocal, and the $\mathfrak{m}_i$ are precisely the primes containing $\mathfrak{q}$.*

(2) *Then $R/\mathfrak{q}$ is decomposable; in fact, $R/\mathfrak{q} = \prod (R/\mathfrak{q})_{\mathfrak{m}_i}$.*

(3) *Then* $\operatorname{Idem}(\kappa)$ *is injective.*

(4) *Given* (2), *set $\overline{e}_i := (\delta_{ij}) \in R/\mathfrak{q}$; assume $\overline{e}_i$ lifts to an idempotent $e_i \in R$. Then* $\operatorname{Idem}(\kappa)$ *is bijective, $Re_i = R_{m_i}$, and R is decomposable; in fact, $R = \prod Re_i$.*

(5) *Then* $\operatorname{Idem}(\kappa)$ *is bijective if and only if R is decomposable.*

Proof: For (1), note $\mathfrak{q} = \operatorname{Ann}(R/\mathfrak{q})$ by **(4.7)**. And $R/\mathfrak{q}$ is Noetherian by **(19.5)** as $\ell(R/\mathfrak{q})$ is finite. Thus **(19.13)**(1)⇒(3), (4) gives (1).

For (2), note $R/\mathfrak{q}$ is Artinian by **(19.10)**. Thus (1) and **(19.11)** give (2).

For (3), note $\mathfrak{q} \subset \operatorname{rad}(R)$. Thus **(3.3)** gives (3).

In (4), given an idempotent $\overline{e} \in R/\mathfrak{q}$, note that, for all i, its projection in $(R/\mathfrak{q})_{\mathfrak{m}_i}$ is either 1 or 0 by **(3.22)**. So $\overline{e}$ is a sum of certain of the $\overline{e}_i$. Form the corresponding sum of the e_i in R. Its residue is $\overline{e}$. Thus $\operatorname{Idem}(\kappa)$ is surjective, so by (3), bijective.

Note that $\sum e_i$ and $e_j e_k$ for all j, k are idempotents. But $\sum \overline{e}_i = 1$, and $\overline{e}_j\overline{e}_k = 0$ for $j \neq k$. Also, $\operatorname{Idem}(\kappa)$ is injective. So $\sum e_i = 1$, and $e_j e_k = 0$ for $j \neq k$. Thus by induction, **(1.12)** yields $R = \prod Re_i$.

Given any maximal ideal $\mathfrak{n}_1 \subset Re_1$, set $\mathfrak{n} := \mathfrak{n}_1 \times \prod_{i=2} Re_i$. Then $\mathfrak{n}$ is maximal; see **(2.29)**. So $\mathfrak{n} \supset \mathfrak{q}$. So $\mathfrak{n}_1 \supset \mathfrak{q}e_1$. So $\mathfrak{n}_1/\mathfrak{q}e_1$ is a maximal ideal of $(R/q)\overline{e}_1$. But plainly $(R/q)\overline{e}_1 = (R/\mathfrak{q})_{\mathfrak{m}_1}$. So $(R/q)\overline{e}_1$ is local. Thus Re_1 is local. Similarly, all the Re_i are local. Thus R is decomposable.

Hence $Re_1 = R_{\mathfrak{m}_j}$ for some j by **(11.18)**. So $Re_1/\mathfrak{q}e_1 = R_{\mathfrak{m}_j}/\mathfrak{q}R_{\mathfrak{m}_j}$. However, $Re_1/\mathfrak{q}e_1 = R\overline{e}_1$ and $R_{\mathfrak{m}_j}/\mathfrak{q}R_{\mathfrak{m}_j} = (R/\mathfrak{q})_{\mathfrak{m}_j} = R\overline{e}_j$; hence, $j = 1$. Thus $Re_1 = R_{\mathfrak{m}_1}$. Similarly, $Re_i = R_{\mathfrak{m}_i}$ for all i. Thus (4) holds.

For (5), first assume R is decomposable. So $R = \prod R_{\mathfrak{m}_i}$ by **(11.18)**. In R, set $e_i := (\delta_{ij})$. Then e_i reduces to $\overline{e}_i$ in (4). Thus (4) implies $\operatorname{Idem}(\kappa)$ is bijective.

Conversely, assume $\operatorname{Idem}(\kappa)$ is bijective. Then each $\overline{e}_i$ in (4) lifts to an idempotent in R. Thus (4) implies R is decomposable. Thus (5) holds. □

B. Exercises

Exercise (19.16) . — Let R be a ring, M a module, Q a $\mathfrak{p}$-primary submodule, and $Q_1 \supsetneqq \cdots \supsetneqq Q_m := Q$ a chain of $\mathfrak{p}$-primary submodules. Set $M' := M/Q$. Assume that M' is Noetherian. Show that $m \le \ell(M'_{\mathfrak{p}}) < \infty$, and that $m = \ell(M'_{\mathfrak{p}})$ if and only if m is maximal.

Exercise (19.17) . — Let k be a field, R an algebra-finite extension. Prove that R is Artinian if and only if R is a finite-dimensional k-vector space.

Exercise (19.18) . — Given a prime $p \in \mathbb{Z}$, find all four different Artinian rings R with p^2 elements. Which R are $\mathbb{F}_p$-algebras?

Exercise (19.19) . — Let k be a field, A a local k-algebra. Assume the map from k to the residue field is bijective. Given an A-module M, prove $\ell(M) = \dim_k(M)$.

Exercise (19.20) . — Prove these conditions on a Noetherian ring R equivalent:
(1) R is Artinian. (2) $\operatorname{Spec}(R)$ is discrete and finite. (3) $\operatorname{Spec}(R)$ is discrete.

Exercise (19.21) . — Let $\varphi\colon R \to R'$ be a map of rings. Assume R' is algebra finite over R. Given $\mathfrak{p} \in \operatorname{Spec}(R)$, set $k := \operatorname{Frac}(R/\mathfrak{p})$. Consider these statements:

(1) The fibers of $\operatorname{Spec}(\varphi)$ are finite.
(2) The fibers of $\operatorname{Spec}(\varphi)$ are discrete.
(3) All $R' \otimes_R k$ are finite-dimensional k-vector spaces.
(4) R' is module finite over R.

Show (1), (2), and (3) are equivalent and follow from (4). Show (4) holds if R' is integral over R. If R' is integral, but not algebra finite, and if (1) holds, does (4)?

Exercise (19.22) . — Let A be a local ring, $\mathfrak{m}$ its maximal ideal, B a module-finite algebra, and $\{\mathfrak{n}_i\}$ its set of maximal ideals. Show the $\mathfrak{n}_i$ are precisely the primes lying over $\mathfrak{m}$, and $\mathfrak{m}B$ is a parameter ideal of B; conclude B is semilocal.

Exercise (19.23) . — Let R be an Artinian ring. Show that $\operatorname{rad}(R)$ is nilpotent.

Exercise (19.24) . — Find another solution to **(18.67)**(1). Begin by setting $\mathfrak{p} := \mathfrak{p}_1$ and $A := (R/\operatorname{Ann}(M))_{\mathfrak{p}}$ and showing A is Artinian.

Exercise (19.25) . — Let R be a ring, $\mathfrak{p}$ a prime ideal, and R' a module-finite R-algebra. Show that R' has only finitely many primes $\mathfrak{p}'$ over $\mathfrak{p}$, as follows: reduce to the case that R is a field by localizing at $\mathfrak{p}$ and passing to the residue rings.

Exercise (19.26) . — Let R be a ring, and M a Noetherian module. Show the following four conditions are equivalent:

(1) M has finite length;
(2) M is annihilated by some finite product of maximal ideals $\prod \mathfrak{m}_i$;
(3) every prime $\mathfrak{p}$ containing $\operatorname{Ann}(M)$ is maximal;
(4) $R/\operatorname{Ann}(M)$ is Artinian.

Exercise (19.27) . — (1) Prove that a finite product rings $R := \prod_{i=1}^{r} R_i$ is a PIR if and only if each R_i is a PIR.

(2) Using **(18.27)**, prove that a PIR R is uniquely a finite product of PIDs and Artinian local PIRs.

Exercise (19.28) . — Let $A \to B$ be a local homomorphism of Artinian rings, N an A-flat B-module, $\mathfrak{m}$ the maximal ideal of A. Show $\ell_B(N) = \ell_A(A) \cdot \ell_B(N/\mathfrak{m}N)$.

Exercise (19.29) . — Let R be a decomposable ring; say $R := \prod R_i$ with R_i local. For all i, let $\mathfrak{q}_i \subset R_i$ be a parameter ideal. Set $\mathfrak{q} := \prod \mathfrak{q}_i \subset R$. Show that $\mathfrak{q}$ is a parameter ideal. Conclude that R has a parameter ideal.

Exercise (19.30) . — Let R be a ring, $\mathfrak{a} \subset \operatorname{nil}(R)$ an ideal. Set $R' := R/\mathfrak{a}$. Use **(19.15)**(3) to reprove **(13.23)**(1) $\Leftrightarrow$ (2): R is decomposable if and only if R' is.

20. Hilbert Functions

The **Hilbert Function** of a graded module lists the lengths of its components. The corresponding generating function is called the **Hilbert Series**. We prove the Hilbert–Serre Theorem: under suitable hypotheses, this series is a rational function with poles just at 0 and 1. Hence these lengths are eventually given by a polynomial, called the **Hilbert Polynomial**.

Passing to an arbitrary module, we study its **Hilbert–Samuel Series**, the generating function of the colengths of the submodules in a **filtration**, which is a descending chain of submodules F^nM. We derive Samuel's Theorem: this series is a similar rational function under suitable hypotheses. Hence these colengths are eventually given by a polynomial, called the **Hilbert–Samuel Polynomial**. In the next chapter, we relate its degree to the dimension of M. Here we consider its normalized leading coefficient, called the **multiplicity** of M.

Lastly, we relate the Hilbert polynomial of a Noetherian module M to the sum of the polynomials of a submodule N and their quotient M/N in the case of a **stable $\mathfrak{q}$-filtration** for an ideal $\mathfrak{q}$; that is, $\mathfrak{q}F^nM \subset \mathfrak{q}F^{n+1}$ for all n, with equality for $n \gg 0$. Our key is the Artin–Rees Lemma: if the F^nM form a stable $\mathfrak{q}$-filtration of M, then the intersections $N \cap F^nM$ form a stable $\mathfrak{q}$-filtration of N.

In a brief appendix, we study further one notion that arose: homogeneity.

A. Text

(20.1) (Graded rings and modules). — We call a ring R **graded** if there are additive subgroups R_n for $n \ge 0$ with $R = \bigoplus R_n$ and $R_mR_n \subset R_{m+n}$ for all m, n.

For example, a polynomial ring R with coefficient ring R_0 is graded if R_n is the R_0-submodule generated by the monomials of (total) degree n.

In general, R_0 is a *subring*. Obviously, R_0 is closed under addition and under multiplication, but we must check $1 \in R_0$. So say $1 = \sum x_m$ with $x_m \in R_m$. Given $z \in R$, say $z = \sum z_n$ with $z_n \in R_n$. Fix n. Then $z_n = 1 \cdot z_n = \sum x_m z_n$ with $x_m z_n \in R_{m+n}$. So $\sum_{m>0} x_m z_n = z_n - x_0 z_n \in R_n$. Hence $x_m z_n = 0$ for $m > 0$. But n is arbitrary. So $x_m z = 0$ for $m > 0$. But z is arbitrary. Taking $z := 1$ yields $x_m = x_m \cdot 1 = 0$ for $m > 0$. Thus $1 = x_0 \in R_0$.

We call an R-module M (compatibly) **graded** if there are additive subgroups M_n for $n \in \mathbb{Z}$ with $M = \bigoplus M_n$ and $R_mM_n \subset M_{m+n}$ for all m, n. We call M_n the nth **homogeneous component**; we say its elements are **homogeneous**. Obviously, M_n is an R_0-module.

Given $m \in \mathbb{Z}$, set $M(m) := \bigoplus M_{m+n}$. Then $M(m)$ is another graded module; its nth homogeneous component $M(m)_n$ is M_{m+n}. Thus $M(m)$ is obtained from M by **shifting** m places to the left.

Lemma (20.2). — *Let $R = \bigoplus R_n$ be a graded ring, and $M = \bigoplus M_n$ a graded R-module. If R is a finitely generated R_0-algebra and if M is a finitely generated R-module, then each M_n is a finitely generated R_0-module and $M_n = 0$ if $n << 0$.*

Proof: Say $R = R_0[x_1, \dots, x_r]$. If $x_i = \sum_j x_{ij}$ with $x_{ij} \in R_j$, then replace the x_i by the nonzero x_{ij}. Similarly, say M is generated over R by $m_1, \dots, m_s$ with $m_i \in M_{l_i}$. Then any $m \in M_n$ is a sum $m = \sum f_i m_i$ where $f_i \in R$. Say $f_i = \sum f_{ij}$

with $f_{ij} \in R_j$, and replace f_i by f_{ik} with $k := n - l_i$ or by 0 if $n < l_i$. Then f_i is an R_0-linear combination of monomials $x_1^{i_1} \cdots x_r^{i_r} \in R_k$. Thus, m is an R_0-linear combination of the products $x_1^{i_1} \cdots x_r^{i_r} m_i \in M_n$, and $M_n = 0$ if $m < \min\{l_i\}$. □

(20.3) (Hilbert Function). — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded R-module. Assume R_0 is Artinian, R is algebra finite over R_0, and M is finitely generated over R. Then each M_n is a finitely generated R_0-module by **(20.2)**, so is of finite length $\ell(M_n)$ by **(19.9)**. We call $n \mapsto \ell(M_n)$ the **Hilbert Function** of M and its generating function

$$H(M,\, t) := \textstyle\sum_{n\in\mathbb{Z}} \ell(M_n) t^n$$

the **Hilbert Series** of M. This series is a rational function by **(20.5)** below.

Given any $k \in \mathbb{Z}$, recall $M(-k)_n := M_{n-k}$ for all n. Hence,

$$H(M(-k),\, t) = t^k H(M,\, t). \tag{20.3.1}$$

If $R = R_0[x_1, \ldots, x_r]$ with $x_i \in R_1$, then by **(20.6)** below, the Hilbert Function is, for $n \gg 0$, a polynomial $h(M,\, n)$, called the **Hilbert Polynomial** of M.

Example (20.4). — Let $R := R_0[X_1, \ldots, X_r]$ be the polynomial ring, graded by degree. Then R_n is free over R_0 on the monomials of degree n, so of rank $\binom{r-1+n}{r-1}$.

Let M_0 be an R_0-module. Form the set of polynomials $M := M_0[X_1, \ldots, X_r]$. Then M is a graded R-module, with M_n the direct sum of $\binom{r-1+n}{r-1}$ copies of M_0.

Assume $\ell(M_0) < \infty$. Then $\ell(M_n) = \ell(M_0)\binom{r-1+n}{r-1}$ by Additivity of Length, **(19.7)**. Thus the Hilbert Function is, for $n \ge 0$, a polynomial of degree $r-1$.

Formal manipulation yields $\binom{r-1+n}{r-1} = (-1)^n\binom{-r}{n}$. Therefore, Newton's binomial theorem for negative exponents yields this computation for the Hilbert Series:

$$H(M,\, t) = \textstyle\sum_{n\ge 0} \ell(M_0)\binom{r-1+n}{r-1} t^n = \sum_{n\ge 0} \ell(M_0)\binom{-r}{n}(-t)^n = \ell(M_0)\big/(1-t)^r.$$

Theorem (20.5) (Hilbert–Serre)**. —** *Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded R-module. Assume R_0 is Artinian, $R = R_0[x_1, \ldots, x_r]$ with $x_i \in R_{k_i}$ and $k_i \ge 1$. Assume M is finitely generated, $M_n = 0$ for $n < n_0$, but $M_{n_0} \ne 0$. Then*

$$H(M,\, t) = f(t)t^{n_0}\big/(1-t^{k_1})\cdots(1-t^{k_r}) \quad \textit{with } f(t) \in \mathbb{Z}[t] \textit{ and } f(0) \ne 0.$$

Proof: Assume $r = 0$; so $R = R_0$. Say $m_1, \ldots, m_s$ generate M with $m_i \in M_{l_i}$ nonzero and with $l_i \le l_{i+1}$. Then $n_0 = l_1$ and $M_n = 0$ for $n > l_s$. Therefore, $H(M,\, t) = \sum_{i=n_0}^{l_s} \ell(M_i)t^i$. Thus $H(M,\, t) = t^{n_0} f(t)$ with $f(t) \in \mathbb{Z}[t]$ and $f(0) \ne 0$.

Assume $r \ge 1$. Form this exact sequence, where μ_{x_1} means multiplication by x_1:

$$0 \to K \to M(-k_1) \xrightarrow{\mu_{x_1}} M \to L \to 0.$$

The grading on M induces a grading on K and on L. Also, $M(-k_1)_{n_0} = 0$ as $k_1 \ge 1$. Thus $K_n = 0$ for $n \le n_0$. Also, $L_n = 0$ for $n < n_0$, but $L_{n_0} \ne 0$.

As R_0 is Artinian, R_0 is Noetherian by **(19.8)**. So, as R is a finitely generated R_0-algebra, R is Noetherian by **(16.10)**. As M is a finitely generated R-module, it's Noetherian by **(16.15)**. So $M(-k_1)$ is too. Thus, by **(16.13)**(2), both K and L are too; in particular, they're finitely generated R-modules.

Set $R' := R_0[x_2, \ldots, x_r]$. Note μ_{x_1} vanishes on K and on L. So they're finitely generated graded R'-modules. Induct on r. Set $d(t) := (1-t^{k_2})\cdots(1-t^{k_r})$. Thus $H(L,\, t) = b(t)t^{n_0}/d(t)$ with $b(t) \in \mathbb{Z}[t]$ and $b(0) \ne 0$. Also, if $K \ne 0$, then $H(K,\, t) = a(t)t^{p_0}/d(t)$ with $a(t) \in \mathbb{Z}[t]$ and $p_0 > n_0$; if $K = 0$, set $a(t) := 0$ and

$p_0 := n_0 + 1$.

Note $H(M,\,t) - H(M(-k_1),\,t) = H(L,\,t) - H(K,\,t)$ by **(19.7)**. But **(20.3.1)** gives $H(M(-k_1),\,t) = t^{k_1}H(M,\,t)$. Set $f(t) := b(t) - a(t)t^{p_0-n_0}$. Then $f(0) \neq 0$; also $H(L,\,t) - H(K,\,t) = f(t)t^{n_0}\big/d(t)$. Thus $(1-t^{k_1})H(M,\,t) = f(t)t^{n_0}\big/d(t)$. □

Corollary (20.6). — *In the setup of* **(20.5)**, *assume $k_i = 1$ for all i. Then uniquely*

$$H(M,\,t) = e(t)t^{n_0}\big/\,(1-t)^d \qquad \textbf{(20.6.1)}$$

with $e(t) \in \mathbb{Z}[t]$ and $e(0),\ e(1) \neq 0$ and $r \geq d \geq 0$. Also, there is a polynomial $h(M,\,n) \in \mathbb{Q}[n]$ with degree $d-1$ and leading coefficient $e(1)\,/\,(d-1)\,!$ such that

$$\ell(M_n) = h(M,\,n) \quad \textit{for } n \geq \deg e(t) + n_0. \qquad \textbf{(20.6.2)}$$

Proof: Note that **(20.5)** yields $H(M,\,t) = f(t)t^{n_0}\big/\,(1-t)^r$ with $f(0) \neq 0$. Say $f(t) = e(t)(1-t)^s$ with $e(1) \neq 0$. Set $d := r - s$. Then $d \geq 0$; otherwise, $0 = H(M,\,1) \geq \ell(M_{n_0})$, a contradiction. Thus **(20.6.1)** holds.

Suppose $H(M,\,t) = g(t)t^{n_0}\big/\,(1-t)^q$ with $g(t) \in \mathbb{Z}[t]$ and $g(1) \neq 0$ and $q \geq 0$. Then $e(t)(1-t)^q = g(t)(1-t)^d$. So $e(t) = g(t)$ and $d = q$. Thus **(20.6.1)** is unique.

Say $e(t) = \sum_{i=0}^{h} e_i t^i$ with $e_h \neq 0$. Now, $(1-t)^{-d} = \sum \binom{-d}{n}(-t)^n = \sum \binom{d-1+n}{d-1}t^n$. So $\ell(M_n) = \sum_{i=0}^{h} e_i \binom{d-1+n-n_0-i}{d-1}$ for $n - n_0 \geq h$. But $\binom{d-1+n-i}{d-1}$ is a polynomial in n of degree $d-1$ and leading coefficient $1/(d-1)\,!$. Thus **(20.6.2)** holds. □

(20.7) (Filtrations). — Let R be an arbitrary ring, $\mathfrak{q}$ an ideal, and M a module. A (descending) **filtration** $F^\bullet M$ of M is an infinite descending chain of submodules:

$$\cdots \supset F^n M \supset F^{n+1} M \supset \cdots.$$

Call it a **$\mathfrak{q}$-filtration** if $\mathfrak{q}F^nM \subset F^{n+1}M$ for all n, and a **stable $\mathfrak{q}$-filtration** if also $M = F^nM$ for $n \ll 0$ and $\mathfrak{q}F^nM = F^{n+1}M$ for $n \gg 0$. This condition means that there are μ and ν with $M = F^\mu M$ and $\mathfrak{q}^n F^\nu M = F^{n+\nu}M$ for $n > 0$.

For example, set $\mathfrak{q}^n := R$ for $n \leq 0$ and $F^nM := \mathfrak{q}^nM$ for all n. Thus we get a stable $\mathfrak{q}$-filtration, called the **$\mathfrak{q}$-adic filtration**.

The $\mathfrak{q}$-adic filtration of R yields two canonical graded rings:

$$\mathcal{R}(\mathfrak{q}) := \textstyle\bigoplus_{n\in\mathbb{Z}} \mathfrak{q}^n \quad\text{and}\quad G_{\mathfrak{q}}(R) := G(R) := \mathcal{R}(\mathfrak{q})\big/\big(\mathcal{R}(\mathfrak{q})(1)\big). \qquad \textbf{(20.7.1)}$$

They're called the **extended Rees Algebra** and **associated graded ring** of $\mathfrak{q}$. Notice that $G(R) = \bigoplus_{n\geq 0} G_n(R)$ where $G_n(R) := \mathfrak{q}^n/\mathfrak{q}^{n+1}$.

Say $x_1, \ldots, x_r \in \mathfrak{q}$ generate. In $\mathcal{R}(\mathfrak{q})$, regard the x_i as in $\mathfrak{q}^1$ and $1 \in R$ as in $\mathfrak{q}^{-1}$. Those $r+1$ elements generate $\mathcal{R}(\mathfrak{q})$ as an R-algebra. Thus if $\mathfrak{q}$ is finitely generated, then $\mathcal{R}(\mathfrak{q})$ is R-algebra finite, and $G_{\mathfrak{q}}(R)$ is $(R/\mathfrak{q})$-algebra finite.

As each F^nM is an R-module, so are the direct sums

$$\mathcal{R}(F^\bullet M) := \textstyle\bigoplus_{n\in\mathbb{Z}} F^nM \quad\text{and}\quad G(M) := \mathcal{R}(F^\bullet M)\big/\big(\mathcal{R}(F^\bullet M)(1)\big). \qquad \textbf{(20.7.2)}$$

Notice that $G(M) = \bigoplus_{n\in\mathbb{Z}} G_n(M)$ where $G_n(M) := \mathfrak{q}^nM/\mathfrak{q}^{n+1}M$.

If $F^\bullet M$ is a $\mathfrak{q}$-filtration, then $\mathcal{R}(F^\bullet M)$ is a graded $\mathcal{R}(F^\bullet R)$-module, and $G(M)$ is a graded $G(R)$-module. If $F^\bullet M$ is the $\mathfrak{q}$-adic filtration, set $G_{\mathfrak{q}}(M) := G(M)$.

Given $m \in \mathbb{Z}$, let $M[m]$ denote M with the filtration $F^\bullet M$ reindexed by **shifting** it m places to the left; that is, $F^n(M[m]) := F^{n+m}M$ for all n. Then

$$\mathcal{R}(F^\bullet M[m]) = \mathcal{R}(F^\bullet M)(m) \quad\text{and}\quad G(M[m]) = (G(M))(m).$$

If the quotients M/F^nM have finite length, call $n \mapsto \ell(M/F^nM)$ the **Hilbert–Samuel Function**, and call the generating function

$$P(F^\bullet M,\, t) := \textstyle\sum_{n\ge 0} \ell(M/F^nM)t^n$$

the **Hilbert–Samuel Series**. If the function $n \mapsto \ell(M/F^nM)$ is, for $n \gg 0$, a polynomial $p(F^\bullet M,\, n)$, then call it the **Hilbert–Samuel Polynomial**. If the filtration is the $\mathfrak{q}$-adic filtration, we also denote $P(F^\bullet M,\, t)$, and $p(F^\bullet M,\, n)$ by $P_{\mathfrak{q}}(M, t)$ and $p_{\mathfrak{q}}(M, n)$.

Lemma (20.8). — *Let R be a ring, $\mathfrak{q}$ an ideal, M a module, $F^\bullet M$ a $\mathfrak{q}$-filtration. If $\mathcal{R}(F^\bullet M)$ is finitely generated over $\mathcal{R}(\mathfrak{q})$, then $G(M)$ is finitely generated over $G(R)$. Moreover, if $\mathcal{R}(F^\bullet M)$ is finitely generated over $\mathcal{R}(\mathfrak{q})$ and $\bigcup F^nM = M$, then $F^\bullet M$ is stable; the converse holds if M is Noetherian.*

Proof: First, assume $\mathcal{R}(F^\bullet M)$ is finitely generated over $\mathcal{R}(\mathfrak{q})$.

By **(20.7.2)**, $G(M)$ is a quotient of $\mathcal{R}(F^\bullet M)$. So $G(M)$ too is finitely generated over $\mathcal{R}(\mathfrak{q})$. But $G(R)$ is a quotient of $\mathcal{R}(\mathfrak{q})$ by **(20.7.1)**. Thus $G(M)$ is finitely generated over $G(R)$, as desired.

Say $m_1, \dots, m_s \in \mathcal{R}(F^\bullet M)$ generate over $\mathcal{R}(\mathfrak{q})$. Write $m_i = \sum_{j=\mu}^{\nu} m_{ij}$ with $m_{ij} \in F^jM$ for some uniform $\mu \le \nu$. Given any n and any $m \in F^nM$, note $m = \sum f_{ij}m_{ij}$ with $f_{ij} \in \mathcal{R}_{n-j}(\mathfrak{q}) := \mathfrak{q}^{n-j}$. Hence, if $n \le \mu$, then $m \in F^\mu M$, and so $F^nM \subset F^\mu M$. Thus, if $\bigcup F^nM = M$ too, then $F^\mu M = M$. But, if $n \ge \nu$, then $f_{ij} \in \mathfrak{q}^{n-j} = \mathfrak{q}^{n-\nu}\mathfrak{q}^{\nu-j}$, and so $\mathfrak{q}^{n-\nu}F^\nu M = F^nM$. Thus $F^\bullet M$ is stable.

Conversely, assume $F^\bullet M$ is stable: say $F^\mu M = M$ and $\mathfrak{q}^nF^\nu M = F^{n+\nu}M$ for $n > 0$. Then $\bigcup F^nM = M$. Further, $F^\mu M, \dots, F^\nu M$ generate $\mathcal{R}(F^\bullet M)$ over $\mathcal{R}(\mathfrak{q})$. Assume M is Noetherian too. Then $F^nM \subset M$ is finitely generated over R for all n. Thus $\mathcal{R}(F^\bullet M)$ is finitely generated over $\mathcal{R}(\mathfrak{q})$, as desiered. □

Lemma (20.9). — *Let R be a ring, $\mathfrak{q}$ an ideal, M a module with a stable $\mathfrak{q}$-filtration $F^\bullet M$. Assume M is Noetherian, and $\ell(M/\mathfrak{q}M) < \infty$. Then $\ell(F^nM/F^{n+1}M) < \infty$ and $\ell(M/F^nM) < \infty$ for every $n \ge 0$; further,*

$$P(F^\bullet M,\, t) = H(G(M),\, t)\, t\big/(1-t). \qquad \textbf{(20.9.1)}$$

Proof: Set $\mathfrak{a} := \mathrm{Ann}(M)$. Set $R' := R/\mathfrak{a}$ and $\mathfrak{q}' := (\mathfrak{a}+\mathfrak{q})/\mathfrak{a}$. As M is Noetherian, so is R' by **(16.16)**. So $R'/\mathfrak{q}'$ is Noetherian too. Also, M can be viewed as a finitely generated R'-module, and $F^\bullet M$ as a stable $\mathfrak{q}'$-filtration. So $G(R')$ is generated as an $R'/\mathfrak{q}'$-algebra by finitely many elements of degree 1, and $G(M)$ is a finitely generated $G(R')$-module by **(20.8)** applied with R' for R. Therefore, each $F^nM/F^{n+1}M$ is finitely generated over $R'/\mathfrak{q}'$ by **(20.2)** or by the proof of **(20.8)**.

However, $\mathbf{V}(\mathfrak{a}+\mathfrak{q}) = \mathrm{Supp}(M/\mathfrak{q}M)$ by **(13.46)**(2). Hence $\mathbf{V}(\mathfrak{a}+\mathfrak{q})$ consists entirely of maximal ideals, because $\mathrm{Supp}(M/\mathfrak{q}M)$ does by **(19.4)** as $\ell(M/\mathfrak{q}M) < \infty$. Thus $\dim(R'/\mathfrak{q}') = 0$. But $R'/\mathfrak{q}'$ is Noetherian. Therefore, $R'/\mathfrak{q}'$ is Artinian by the Akizuki–Hopkins Theorem, **(19.8)**.

Hence $\ell(F^nM/F^{n+1}M) < \infty$ for every n by **(19.9)**. Form the exact sequence

$$0 \to F^nM/F^{n+1}M \to M/F^{n+1}M \to M/F^nM \to 0.$$

Then Additivity of Length, **(19.7)**, yields

$$\ell(F^nM/F^{n+1}M) = \ell(M/F^{n+1}M) - \ell(M/F^nM). \qquad \textbf{(20.9.2)}$$

So induction on n yields $\ell(M/F^{n+1}M) < \infty$ for every n. Further, multiplying that equation by t^n and summing over n yields the desired expression in another form:

$$H(G(M),\,t) = (t^{-1}-1)P(F^\bullet M,\,t) = P(F^\bullet M,\,t)\,(1-t)/t. \qquad \square$$

Theorem (20.10) (Samuel's)**. —** *In the setup of* **(20.9)***, assume* $\mathfrak{q}$ *is generated by* r *elements, and assume* $F^nM = M$ *for* $n < l$*, but* $F^lM \neq M$*. Then uniquely*

$$P(F^\bullet M,\,t) = e(t)t^l/(1-t)^{d+1} \tag{20.10.1}$$

with $e(t) \in \mathbb{Z}[t]$ *and* $e(0),\ e(1) \neq 0$ *and* $r \geq d \geq 0$*. Also, there is a polynomial* $p(F^\bullet M,\,n) \in \mathbb{Q}[n]$ *with degree* d *and leading coefficient* $e(1)/d\,!$ *such that*

$$\ell(M/F^nM) = p(F^\bullet M,\,n) \quad \text{for } n \geq \deg e(t) + l. \tag{20.10.2}$$

If nonzero, $p_{\mathfrak{q}}(M,\,n) - p(F^\bullet M,\,n)$ *is a polynomial of degree at most* $d-1$ *and positive leading coefficient; also,* d *and* $e(1)$ *are the same for every stable* $\mathfrak{q}$*-filtration.*

Proof: The proof of **(20.9)** shows that $G(R')$ and $G(M)$ satisfy the hypotheses of **(20.6)** with $n_0 = l-1$. So **(20.6.1)** and **(20.9.1)** yield **(20.10.1)**. In turn, **(20.10.1)** yields **(20.10.2)** by the argument at the end of the proof of **(20.6)**.

Finally, as $F^\bullet M$ is a stable $\mathfrak{q}$-filtration, there is an m such that

$$F^nM \supset \mathfrak{q}^nM \supset \mathfrak{q}^nF^mM = F^{n+m}M$$

for all $n \geq 0$. Forming the quotients and extracting their lengths, we get

$$\ell(M/F^nM) \leq \ell(M/\mathfrak{q}^nM) \leq \ell(M/F^{n+m}M).$$

Therefore, **(20.10.2)** yields

$$p(F^\bullet M,\,n) \leq p_{\mathfrak{q}}(M,\,n) \leq p(F^\bullet M,\,n+m) \quad \text{for } n \gg 0.$$

The two extremes are polynomials in n with the same degree d and the same leading coefficient c where $c := e(1)/d\,!$. Dividing by n^d and letting $n \to \infty$, we conclude that the polynomial $p_{\mathfrak{q}}(M,\,n)$ also has degree d and leading coefficient c.

Thus the degree and leading coefficient are the same for every stable $\mathfrak{q}$-filtration. Also $p_{\mathfrak{q}}(M,\,n) - p(F^\bullet M,\,n)$ has degree at most $d-1$ and positive leading coefficient, owing to cancellation of the two leading terms and to the first inequality. $\square$

(20.11) (Multiplicity). — Preserve the conditions of **(20.10)**. The "normalized" leading coefficient $e(1)$ of the Hilbert–Samuel polynomial $p(F^\bullet M, n)$ is called the **multiplicity of** $\mathfrak{q}$ **on** M and is also denoted $e(\mathfrak{q},\,M)$.

Note that $e(\mathfrak{q},\,M)$ is the same number for every stable $\mathfrak{q}$-filtration $F^\bullet M$ by **(20.10)**. Moreover, $\ell(M/\mathfrak{q}^nM) > 0$ for all $n > 0$; hence, $e(\mathfrak{q}, M)$ is a positive integer.

Set $d := \deg p(F^\bullet M, n)$, Then **(20.3)** and **(20.9.2)** yield, for $n \gg 0$,

$$\begin{aligned} h(G_{\mathfrak{q}}(M),\,n) :=& \ell(\mathfrak{q}^nM/\mathfrak{q}^{n+1}M) \\ =& \big(e(\mathfrak{q},\,M)/(d-1)!\big)n^{d-1} + \text{ lower degree terms.} \end{aligned}$$

Lemma (20.12) (Artin–Rees)**. —** *Let* R *be a ring,* M *a module,* N *a submodule,* $\mathfrak{q}$ *an ideal,* $F^\bullet M$ *a stable* $\mathfrak{q}$*-filtration. Set*

$$F^nN := N \cap F^nM \quad \text{for } n \in \mathbb{Z}.$$

Assume M *is Noetherian. Then the* F^nN *form a stable* $\mathfrak{q}$*-filtration* $F^\bullet N$*.*

Proof: Set $\mathfrak{a} := \mathrm{Ann}(M)$, set $R' := R/\mathfrak{a}$, and set $\mathfrak{q}' := (\mathfrak{q}+\mathfrak{a})/\mathfrak{a}$. Then M and N are R'-modules, and $F^\bullet M$ is a stable $\mathfrak{q}'$-filtration. So we may replace R by R' (and $\mathfrak{q}$ by $\mathfrak{q}'$), and thus by **(16.16)**, assume R is Noetherian.

By **(20.7)**, the extended Rees Algebra $\mathcal{R}(\mathfrak{q})$ is finitely generated over R, so Noetherian by the Hilbert Basis Theorem **(16.10)**. By **(20.8)**, the module $\mathcal{R}(F^\bullet M)$ is finitely generated over $\mathcal{R}(\mathfrak{q})$, so Noetherian by **(16.15)**. Clearly, $F^\bullet N$ is a $\mathfrak{q}$-filtration; hence, $\mathcal{R}(F^\bullet N)$ is a submodule of $\mathcal{R}(F^\bullet M)$, so finitely generated. But $\bigcup F^n M = M$, so $\bigcup F^n N = N$. Thus $F^\bullet N$ is stable by **(20.8)**. □

Proposition (20.13). — *Let R be a ring, $\mathfrak{q}$ an ideal, and*

$$0 \to M' \to M \to M'' \to 0$$

an exact sequence of Noetherian modules.

(1) *Then $\ell(M/\mathfrak{q}M) < \infty$ if and only if $\ell(M'/\mathfrak{q}M') < \infty$ and $\ell(M''/\mathfrak{q}M'') < \infty$.*

(2) *Assume $\ell(M/\mathfrak{q}M) < \infty$. Then the polynomial*

$$p_{\mathfrak{q}}(M', n) - p_{\mathfrak{q}}(M, n) + p_{\mathfrak{q}}(M'', n)$$

has degree at most $\deg(p_{\mathfrak{q}}(M', n)) - 1$ and has positive leading coefficient; also then

$$\deg p_{\mathfrak{q}}(M, n) = \max\{\, \deg p_{\mathfrak{q}}(M', n),\ \deg p_{\mathfrak{q}}(M'', n)\,\}.$$

Proof: For (1), note **(13.46)**(1) and **(13.4)**(1) and **(13.46)**(1) yield

$$\begin{aligned}\mathrm{Supp}(M/\mathfrak{q}M) &= \mathrm{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q}) = \big(\mathrm{Supp}(M') \bigcup \mathrm{Supp}(M'')\big) \bigcap \mathbf{V}(\mathfrak{q})\\ &= \big(\mathrm{Supp}(M') \bigcap \mathbf{V}(\mathfrak{q})\big) \bigcup \big(\mathrm{Supp}(M'') \bigcap \mathbf{V}(\mathfrak{q})\big)\\ &= \mathrm{Supp}(M'/\mathfrak{q}M') \bigcup \mathrm{Supp}(M''/\mathfrak{q}M'').\end{aligned}$$

Thus **(19.4)** yields (1).

For (2), given $n \in \mathbb{Z}$, set $F^n M' := M' \bigcap \mathfrak{q}^n M$. Then the $F^n M'$ form a stable $\mathfrak{q}$-filtration $F^\bullet M'$ by the Artin–Rees Lemma **(20.12)**. Form the following canonical commutative diagram:

$$\begin{array}{ccccccccc} 0 & \to & F^n M' & \to & \mathfrak{q}^n M & \to & \mathfrak{q}^n M'' & \to & 0\\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

Its rows are exact. So the Nine Lemma **(5.24)** yields this exact sequence:

$$0 \to M'/F^n M' \to M/\mathfrak{q}^n M \to M''/\mathfrak{q}^n M'' \to 0.$$

As $M/\mathfrak{q}M < \infty$, Additivity of Length, **(19.7)**, and **(20.10.2)** yield

$$p(F^\bullet M',\, n) - p_{\mathfrak{q}}(M,\, n) + p_{\mathfrak{q}}(M'',\, n) = 0. \qquad \textbf{(20.13.1)}$$

Hence $p_{\mathfrak{q}}(M',\, n) - p_{\mathfrak{q}}(M,\, n) + p_{\mathfrak{q}}(M'',\, n)$ is equal to $p_{\mathfrak{q}}(M',\, n) - p(F^\bullet M',\, n)$. But by **(20.10)** again, the latter is a polynomial with degree at most $\deg p_{\mathfrak{q}}(M',\, n) - 1$ and positive leading coefficient.

Finally, $\deg p_{\mathfrak{q}}(M, n) = \max\{\, \deg p(F^\bullet M', n),\ \deg p_{\mathfrak{q}}(M'', n)\,\}$ by **(20.13.1)**, as the leading coefficients of $p(F^\bullet M', n)$ and $p_{\mathfrak{q}}(M'', n)$ are both positive, so cannot cancel. But $\deg p(F^\bullet M', n) = \deg p_{\mathfrak{q}}(M', n)$ by **(20.10)**. Thus (2) holds. □

B. Exercises

Exercise (20.14) . — Let k be a field, $k[X,Y]$ the polynomial ring. Show $\langle X, Y^2\rangle$ and $\langle X^2, Y^2\rangle$ have different Hilbert Series, but the same Hilbert Polynomial.

Exercise (20.15) . — Let k be a field, $P := k[X,Y,Z]$ the polynomial ring in three variables, $F \in P$ a homogeneous polynomial of degree $d \geq 1$. Set $R := P/\langle F\rangle$. Find the coefficients of the Hilbert Polynomial $h(R,\, n)$ explicitly in terms of d.

Exercise (20.16) . — Let K be a field, $X_1,\dots,X_r$ variables, $k_1,\dots,k_r$ positive integers. Set $R := K[X_1,\dots,X_r]$, and define a grading on R by $\deg(X_i) := k_i$. Set $q_r(t) := \prod_{i=1}^r (1-t^{k_i}) \in \mathbb{Z}[t]$. Show $H(R,\, t) = 1/q_r(t)$.

Exercise (20.17) . — Under the conditions of (20.6), assume there is a homogeneous nonzerodivisor $f \in R$ with $M_f = 0$. Prove $\deg h(R,n) > \deg h(M,n)$; start with the case $M := R/\langle f^k\rangle$.

Exercise (20.18) . — Let R be a ring, $\mathfrak{q}$ an ideal, and M a Noetherian module. Assume $\ell(M/\mathfrak{q}M) < \infty$. Set $\mathfrak{m} := \sqrt{\mathfrak{q}}$. Show

$$\deg p_{\mathfrak{m}}(M,n) = \deg p_{\mathfrak{q}}(M,n).$$

Exercise (20.19) . — In the setup of (20.10), prove these two formulas:

$$(1)\;\; e(\mathfrak{q},M) = \lim_{n\to\infty} d!\,\ell(M/\mathfrak{q}^n M)/n^d \quad \text{and} \quad (2)\;\; e(\mathfrak{q}^k,M) = k^d e(\mathfrak{q},M).$$

Exercise (20.20) . — Let R be a ring, $\mathfrak{q} \subset \mathfrak{q}'$ nested ideals, and M a Noetherian module. Assume $\ell(M/\mathfrak{q}M) < \infty$. Prove these two statements:

(1) Then $e(\mathfrak{q},M) \leq e(\mathfrak{q},M)$, with equality if the $\mathfrak{q}'$-adic filtration is $\mathfrak{q}$-stable.

(2) If $\ell(M) < \infty$ and $\mathfrak{q} \subset \operatorname{rad}(M)$, then $e(\mathfrak{q},M) = \ell(M)$.

Exercise (20.21) . — Let R be a ring, $\mathfrak{q}$ an ideal, and M a Noetherian module with $\ell(M/\mathfrak{q}M) < \infty$. Set $S := \operatorname{Supp}(M) \cap \mathbf{V}(\mathfrak{q})$. Set $d := \max_{\mathfrak{m}\in S} \dim(M_{\mathfrak{m}})$ and $\Lambda := \{\mathfrak{m} \in S \mid \dim(M_{\mathfrak{m}}) = d$. Show

$$e(\mathfrak{q},M) = \textstyle\sum_{\mathfrak{m}\in\Lambda} e(\mathfrak{q}R_{\mathfrak{m}}, M_{\mathfrak{m}}).$$

Exercise (20.22) . — Derive the Krull Intersection Theorem, (18.23), from the Artin–Rees Lemma, (20.12).

C. Appendix: Homogeneity

(20.23) (Homogeneity). — Let R be a graded ring, and $M = \bigoplus M_n$ a graded module. Given $m \in M$, write $m = \sum m_n$ with $m_n \in M_n$. Call the finitely many nonzero m_n the **homogeneous components** of m. Say that a component m_n is **homogeneous of degree** n. If n is lowest, call m_n the **initial component** of m.

Call a submodule $N \subset M$ **homogeneous** if, whenever $m \in N$, also $m_n \in N$, or equivalently, $N = \bigoplus(M_n \cap N)$. Call an ideal **homogeneous** if it's a homogeneous submodule of R.

Consider a map $\alpha\colon M' \to M$ of graded modules with components M'_n and M_n. Call α **homogeneous of degree** r if $\alpha(M'_n) \subset M_{n+r}$ for all n. If so, then clearly $\operatorname{Ker}(\alpha)$ is a homogeneous submodule of M. Further, $\operatorname{Coker}(\alpha)$ is canonically graded, and the quotient map $M \to \operatorname{Coker}(\alpha)$ is homogeneous of degree 0.

Proposition (20.24). — *Let R be a graded ring, M a graded module, Q a proper homogeneous submodule. Set $\mathfrak{p} := \mathrm{nil}(M/Q)$. Assume that Q has this property: given any homogeneous $x \in R$ and homogeneous $m \in M$ with $xm \in Q$ but $m \notin Q$, necessarily $x \in \mathfrak{p}$. Then Q is old-primary.*

Proof: Given $x \in R$ and $m \in M$, decompose them into their homogeneous components: $x = \sum_{i \ge r} x_i$ and $m = \sum_{j \ge s} m_j$. Suppose $xm \in Q$, but $m \notin Q$. Then $m_t \notin Q$ for some t; take t minimal. Set $m' := \sum_{j<t} m_j$. Then $m' \in Q$. Set $m'' := m - m'$. Then $xm'' \in Q$.

Either $x_r m_t$ vanishes or it's the initial component of xm''. But Q is homogeneous. So $x_r m_t \in Q$. But $m_t \notin Q$. Hence $x_r \in \mathfrak{p}$ by the hypothesis. Say $x_r, \dots, x_u \in \mathfrak{p}$ with u maximal. Set $x' := \sum_{i=r}^{u} x_i$. Then $x' \in \mathfrak{p}$. So $x'^k \in \mathrm{Ann}(M/Q)$ for some $k \ge 1$. So $x'^k m'' \in Q$. Set $x'' := x - x'$. Since $xm'' \in Q$, also $x''^k m'' \in Q$.

Suppose $x \notin \mathfrak{p}$. Then $x'' \neq 0$. And its initial component is x_v with $v > u$. Either $x''_v m''_t$ vanishes or it is the initial component of xm. But Q is homogeneous. So $x_v m_t \in Q$. But $m_t \notin Q$. Hence $x_v \in \mathfrak{p}$ by the hypothesis, contradicting $v > u$. Thus $x \in \mathfrak{p}$. Thus Q is old-primary. $\square$

Exercise (20.25) . — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, and M a graded module. Show that $\sqrt{\mathfrak{a}}$ and $\mathrm{Ann}(M)$ and $\mathrm{nil}(M)$ are homogeneous.

Exercise (20.26) . — Let R be a graded ring, M a graded module, and Q an old-primary submodule. Let $Q^* \subset Q$ be the submodule generated by the homogeneous elements of Q. Show that Q^* is old-primary.

Theorem (20.27). — *Let R be a graded ring, M a graded module, and N a proper homogeneous submodule. Assume M/N is Noetherian. Then N admits an irredundant primary decomposition in which all the primary submodules are homogeneous; moreover, the associated primes $\mathfrak{p}_i$ of M/N are homogeneous.*

Proof: Let $N = \bigcap Q_j$ be any primary decomposition; one exists by **(18.19)**. Also, each Q_j is old-primary by **(18.3)**(5). Let $Q_j^* \subset Q_j$ be the submodule generated by the homogeneous elements of Q_j. Trivially, $\bigcap Q_j^* \subset \bigcap Q_j = N \subset \bigcap Q_j^*$. Further, each Q_j^* is plainly homogeneous, and is primary by **(20.26)** and **(18.3)**(4). Thus $N = \bigcap Q_j^*$ is a decomposition into homogeneous primary submodules. And, owing to **(18.17)**, it is irredundant if $N = \bigcap Q_j$ is, as both decompositions have minimal length.

Moreover, the $\mathfrak{p}_i$ are the $\mathrm{nil}(M/Q_i^*)$ by **(18.18)**. The M/Q_i^* are graded by **(20.23)**. Thus by **(20.25)** the $\mathfrak{p}_i$ are homogeneous. $\square$

(20.28) (Graded Domains). — Let $R = \bigoplus_{n \ge 0} R_n$ be a graded domain, and set $K := \mathrm{Frac}(R)$. We call $z \in K$ **homogeneous of degree** $n \in \mathbb{Z}$ if $z = x/y$ with $x \in R_m$ and $y \in R_{m-n}$. Clearly, n is well defined.

Let K_n be the set of all such z, plus 0. Then $K_m K_n \subset K_{m+n}$. Clearly, the canonical map $\bigoplus_{n \in \mathbb{Z}} K_n \to K$ is injective. Thus $\bigoplus_{n \ge 0} K_n$ is a graded subring of K. Further, K_0 is a field.

The n with $K_n \neq 0$ form a subgroup of $\mathbb{Z}$. So by renumbering, we may assume $K_1 \neq 0$. Fix any nonzero $x \in K_1$. Clearly, x is transcendental over K_0. If $z \in K_n$, then $z/x^n \in K_0$. Hence $R \subset K_0[x]$. So **(2.3)** yields $K = K_0(x)$.

Any $w \in \bigoplus K_n$ can be written $w = a/b$ with $a, b \in R$ and b homogeneous: say $w = \sum (a_n/b_n)$ with $a_n, b_n \in R$ homogeneous; set $b := \prod b_n$ and $a := \sum (a_n b/b_n)$.

Theorem (20.29). — *Let R be a Noetherian graded domain, $K := \mathrm{Frac}(R)$, and $\overline{R}$ the integral closure of R in K. Then $\overline{R}$ is a graded R-algebra.*

Proof: Use the setup of (**20.28**). Since $K_0[x]$ is a polynomial ring over a field, it is normal by (**10.22**). Hence $\overline{R} \subset K_0[x]$. So every $y \in \overline{R}$ can be written as $y = \sum_{i=r}^{r+n} y_i$, with y_i homogeneous and nonzero. Let's show $y_i \in \overline{R}$ for all i.

Since y is integral over R, the R-algebra $R[y]$ is module finite by (**10.14**). So (**20.28**) yields a homogeneous $b \in R$ with $bR[y] \subset R$. Hence $by^j \in R$ for all $j \geq 0$. But R is graded. Hence $by_r^j \in R$. Set $z := 1/b$. Then $y_r^j \in Rz$. Since R is Noetherian, the R-algebra $R[y_r]$ is module finite. Hence $y_r \in \overline{R}$. Then $y - y_r \in \overline{R}$. Thus $y_i \in \overline{R}$ for all i by induction on n. Thus $\overline{R}$ is graded. □

D. Appendix: Exercises

Exercise (20.30) (*Nakayama's Lemma for graded modules***) .** — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, M a graded module. Assume $\mathfrak{a} = \sum_{i \geq i_0} \mathfrak{a}_i$ with $i_0 > 0$ and $M = \sum_{n \geq n_0} M_n$ for some n_0. Assume $\mathfrak{a}M = M$. Show $M = 0$.

Exercise (20.31) (*Homogeneous prime avoidance***) .** — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, $\mathfrak{a}^\flat$ its subset of homogeneous elements, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ primes. Adapt the method of (**3.12**) to prove the following assertions:

(1) If $\mathfrak{a}^\flat \not\subset \mathfrak{p}_j$ for all j, then there is $x \in \mathfrak{a}^\flat$ such that $x \notin \mathfrak{p}_j$ for all j.

(2) If $\mathfrak{a}^\flat \subset \bigcup_{i=1}^n \mathfrak{p}_i$, then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.

Exercise (20.32) . — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded module, $N = \bigoplus N_n$ a homogeneous submodule. Assume M/N is Noetherian. Set

$$N' := \{\, m \in M \mid R_n m \in N \text{ for all } n \gg 0 \,\}.$$

(1) Show that N' is the largest homogeneous submodule of M containing N and having, for all $n \gg 0$, its degree-n homogeneous component N'_n equal to N_n.

(2) Let $N = \bigcap Q_i$ be a primary decomposition. Say Q_i is $\mathfrak{p}_i$-primary. Set $R_+ := \bigoplus_{n>0} R_n$. Show that $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$.

Exercise (20.33) . — Under the conditions of (**20.6**), assume R is a domain whose integral closure $\overline{R}$ in $\mathrm{Frac}(R)$ is module finite (see (**24.18**)). Prove the following:

(1) There is a homogeneous $f \in R$ with $R_f = \overline{R}_f$.

(2) The Hilbert Polynomials of R and $\overline{R}$ have the same degree and same leading coefficient.

Exercise (20.34) . — Let $R = \bigoplus R_n$ be a graded ring with R_0 Artinian. Assume $R = R_0[x_1, \ldots, x_r]$ with $x_i \in R_{k_i}$ and $k_i \geq 1$. Set $q(t) := \prod_{i=1}^r (1 - t^{k_i})$. Let $\mathcal{C}$ be the subcategory of $((R\text{-mod}))$ of all finitely generated *graded* R-modules $M = \bigoplus M_n$ and all homogeneous maps of degree 0; let $\mathcal{C}_0$ be its subcategory of all M with $M_n = 0$ for all $n < 0$. Using the notation of (**17.34**), let $\lambda_0 \colon K_0(R_0) \to \mathbb{Z}$ be a $\mathbb{Z}$-map. Show that assigning to each $M \in \mathcal{C}$ the series $\sum_{n \in \mathbb{Z}} \lambda_0(\gamma_0(M_n)) t^n$ gives rise to $\mathbb{Z}$-maps $K(\mathcal{C}) \to (1/q(t))\mathbb{Z}[t, 1/t]$ and $K(\mathcal{C}_0) \to (1/q(t))\mathbb{Z}[t]$.

21. Dimension

The dimension of a module is defined as the supremum of the lengths of the chains of primes in its support. The Dimension Theorem, which we prove, characterizes the dimension of a nonzero Noetherian semilocal module in two ways. First, the dimension is the degree of the Hilbert–Samuel Polynomial of the adic filtration associated to the radical of the module. Second, the dimension is the smallest number of elements in the radical that span a submodule of finite colength.

Next, in an arbitrary Noetherian ring, we study the height of a prime, which is the length of the longest chain of subprimes. We bound the height by the minimal number of generators of an ideal over which the prime is minimal. In particular, when this number is 1, we obtain Krull's Principal Ideal Theorem.

Given any ring R and R-module M, we define the M-quasi-regularity of a sequence of elements $x_1, \ldots, x_s \in R$. Under appropriate hypotheses, including $s = \dim(M)$, we prove $x_1, \ldots, x_s$ is M-quasi-regular if and only if the multiplicity of M is equal to the length of $M/\langle x_1, \ldots, x_s\rangle M$. Finally, we study **regular local rings**: they are the Noetherian local rings whose maximal ideal has the minimum number of generators, namely, the dimension.

A. Text

(21.1) (Dimension of a module). — Let R be a ring, and M a nonzero module. The **dimension** of M, denoted $\dim(M)$, is defined by this formula:

$$\dim(M) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r \text{ in } \operatorname{Supp}(M)\,\}.$$

Assume M is Noetherian. Then M has finitely many minimal (associated) primes by **(17.16)**. They are also the minimal primes $\mathfrak{p}_0 \in \operatorname{Supp}(M)$ by **(17.13)** and **(17.14)**. Thus **(1.9)** yields

$$\dim(M) = \max\{\, \dim(R/\mathfrak{p}_0) \mid \mathfrak{p}_0 \in \operatorname{Supp}(M) \text{ is minimal}\,\}. \qquad \textbf{(21.1.1)}$$

(21.2) (The invariants $d(M)$ and $s(M)$). — Let R be a ring, M a nonzero Noetherian module, $\mathfrak{q}$ a parameter ideal of M. Set $\mathfrak{m} := \operatorname{rad}(M)$ and $\mathfrak{q}' := \operatorname{Ann}(M/\mathfrak{q}M)$.

Then the Hilbert–Samuel Polynomial $p_{\mathfrak{q}}(M, n)$ exists by **(20.10)**. Similarly, $p_{\mathfrak{m}}(M, n)$ exists, and the two polynomials have the same degree by **(20.18)** since $\mathfrak{m} = \sqrt{\mathfrak{q}'}$ by (1)⇔(5) of **(19.13)**, since $\sqrt{\mathfrak{q}'} = \sqrt{\mathfrak{q}''}$ where $\mathfrak{q}'' := \mathfrak{q} + \operatorname{Ann}(M)$ owing to **(13.46)**(2) and **(13.1)**, and since plainly $p_{\mathfrak{q}''}(M, n) = p_{\mathfrak{q}}(M, n)$. Thus the degree is the same for every parameter ideal. Denote this common degree by $d(M)$.

Alternatively, $d(M)$ can be viewed as the order of pole at 1 of the Hilbert Series $H(G_{\mathfrak{q}}(M), t)$. Indeed, that order is 1 less than the order of pole at 1 of the Hilbert–Samuel Series $P_{\mathfrak{q}}(M, t)$ by **(20.9)**. In turn, the latter order is $d(M)+1$ by **(20.10)**.

Denote by $s(M)$ the smallest s such that there are $x_1, \ldots, x_s \in \mathfrak{m}$ with

$$\ell(M/\langle x_1, \ldots, x_s\rangle M) < \infty. \qquad \textbf{(21.2.1)}$$

By convention, if $\ell(M) < \infty$, then $s(M) = 0$. If $s = s(M)$ and **(21.2.1)** holds, we say that $x_1, \ldots, x_s \in \mathfrak{m}$ form a **system of parameters** (sop) for M. Note that a sop generates a parameter ideal.

Lemma (21.3). — *Let R be a ring, M a nonzero Noetherian semilocal module, $\mathfrak{q}$ a parameter ideal of M, and $x \in \mathrm{rad}(M)$. Set $K := \mathrm{Ker}(M \xrightarrow{\mu_x} M)$.*

(1) *Then $s(M) \le s(M/xM) + 1$.*
(2) *Then $\dim(M/xM) \le \dim(M) - 1$ if $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$.*
(3) *Then $\deg\big(p_{\mathfrak{q}}(K, n) - p_{\mathfrak{q}}(M/xM, n)\big) \le d(M) - 1$.*

Proof: For (1), set $s := s(M/xM)$. There are $x_1, \ldots, x_s \in \mathrm{rad}(M/xM)$ with

$$\ell(M/\langle x, x_1, \ldots, x_s\rangle M) < \infty.$$

Now, $\mathrm{Supp}(M/xM) = \mathrm{Supp}(M) \cap \mathbf{V}(\langle x\rangle)$ by **(13.46)**. But $x \in \mathrm{rad}(M)$. Hence, $\mathrm{Supp}(M/xM)$ and $\mathrm{Supp}(M)$ have the same maximal ideals owing to **(13.4)**(4). Therefore, $\mathrm{rad}(M/xM) = \mathrm{rad}(M)$. Hence $s(M) \le s + 1$. Thus (1) holds.

To prove (2), take a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in $\mathrm{Supp}(M/xM)$. Again, $\mathrm{Supp}(M/xM) = \mathrm{Supp}(M) \cap \mathbf{V}(\langle x\rangle)$ by **(13.46)**. So $x \in \mathfrak{p}_0 \in \mathrm{Supp}(M)$. So, by hypothesis, $\dim(R/\mathfrak{p}_0) < \dim(M)$. Hence $r \le \dim(M) - 1$. Thus (2) holds.

To prove (3), note that $xM := \mathrm{Im}(\mu_x)$, and form these two exact sequences:

$$0 \to K \to M \to xM \to 0, \quad \text{and} \quad 0 \to xM \to M \to M/xM \to 0.$$

Then **(20.13)** yields $d(K) \le d(M)$ and $d(xM) \le d(M)$. So by **(20.13)** again, both $p_{\mathfrak{q}}(K, n) + p_{\mathfrak{q}}(xM, n) - p_{\mathfrak{q}}(M, n)$ and $p_{\mathfrak{q}}(xM, n) + p_{\mathfrak{q}}(M/xM, n) - p_{\mathfrak{q}}(M, n)$ are of degree at most $d(M) - 1$. So their difference is too. Thus (3) holds. □

Theorem (21.4) (Dimension). — *Let R be a ring, and M a nonzero Noetherian semilocal module. Then*

$$\dim(M) = d(M) = s(M) < \infty.$$

Proof: Let's prove a cycle of inequalities. Set $\mathfrak{m} := \mathrm{rad}(M)$.

First, let's prove $\dim(M) \le d(M)$ by induction on $d(M)$. Suppose $d(M) = 0$. Then $\ell(M/\mathfrak{m}^n M)$ stabilizes. So $\mathfrak{m}^n M = \mathfrak{m}^{n+1} M$ for some n. But $m^n M$ is finitely generated as M is Noetherian. Also, $\mathrm{Ann}(M) \subset \mathrm{Ann}(\mathfrak{m}^n M)$; so $\mathfrak{m} \subset \mathrm{rad}(\mathfrak{m}^n M)$. So $\mathfrak{m}^n M = 0$ by Nakayama's Lemma **(10.6)**. But $\ell(M/\mathfrak{m}^n M) < \infty$. So $\ell(M) < \infty$. Thus **(19.4)** yields $\dim(M) = 0$.

Suppose $d(M) \ge 1$. By **(21.1.1)**, $\dim(R/\mathfrak{p}_0) = \dim(M)$ for some $\mathfrak{p}_0 \in \mathrm{Supp}(M)$. Then $\mathfrak{p}_0$ is minimal. So $\mathfrak{p}_0 \in \mathrm{Ass}(M)$ by **(17.14)**. Hence M has a submodule N isomorphic to $R/\mathfrak{p}_0$ by **(17.3)**. Further, **(20.13)**(2) yields $d(N) \le d(M)$.

Take a chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in $\mathrm{Supp}(N)$. If $r = 0$, then $r \le d(M)$. Suppose $r \ge 1$. Then there's an $x_1 \in \mathfrak{p}_1 - \mathfrak{p}_0$. Further, since $\mathfrak{p}_0$ is not maximal, for each maximal ideal $\mathfrak{n}$ in $\mathrm{Supp}(M)$, there is an $x_{\mathfrak{n}} \in \mathfrak{n} - \mathfrak{p}_0$. Set $x := x_1 \prod x_{\mathfrak{n}}$. Then $x \in (\mathfrak{p}_1 \cap \mathfrak{m}) - \mathfrak{p}_0$. Then $\mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ lies in $\mathrm{Supp}(N) \bigcap \mathbf{V}(\langle x\rangle)$. But the latter is equal to $\mathrm{Supp}(N/xN)$ by **(13.46)**(1). So $r - 1 \le \dim(N/xN)$.

However, μ_x is injective on N as $N \simeq R/\mathfrak{p}_0$ and $x \notin \mathfrak{p}_0$. So **(21.3)**(3) yields $d(N/xN) \le d(N) - 1$. But $d(N) \le d(M)$. So $\dim(N/xN) \le d(N/xN)$ by the induction hypothesis. Therefore, $r \le d(M)$. Thus $\dim(M) \le d(M)$.

Second, let's prove $d(M) \le s(M)$. Let $\mathfrak{q}$ be a parameter ideal of M with $s(M)$ generators. Then $d(M) := \deg p_{\mathfrak{q}}(M, n)$. But $\deg p_{\mathfrak{q}}(M, n) \le s(M)$ owing to **(20.10)**. Thus $d(M) \le s(M)$.

Finally, let's prove $s(M) \le \dim(M)$. Set $r := \dim(M)$, which is finite since $r \le d(M)$ by the first step. The proof proceeds by induction on r. If $r = 0$, then M has finite length by **(19.4)**; so by convention $s(M) = 0$.

Suppose $r \geq 1$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the primes of $\operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}_i) = r$. No $\mathfrak{p}_i$ is maximal as $r \geq 1$. So $\mathfrak{m}$ lies in no $\mathfrak{p}_i$. Hence, by Prime Avoidance **(3.12)**, there is an $x \in \mathfrak{m}$ such that $x \notin \mathfrak{p}_i$ for all i. So **(21.3)**(1), (2) yield $s(M) \leq s(M/xM)+1$ and $\dim(M/xM)+1 \leq r$. By the induction hypothesis, $s(M/xM) \leq \dim(M/xM)$. Hence $s(M) \leq r$, as desired. □

Corollary (21.5). — *Let R be a ring, M a nonzero Noetherian semilocal module, $x \in \operatorname{rad}(M)$. Then $\dim(M/xM) \geq \dim(M) - 1$, with equality if and only if $x \notin \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$; equality holds if $x \notin \operatorname{z.div}(M)$.*

Proof: By **(21.3)**(1), we have $s(M/xM) \geq s(M) - 1$. So the asserted inequality holds by **(21.4)**. If $x \notin \mathfrak{p} \in \operatorname{Supp}(M)$ when $\dim(R/\mathfrak{p}) = \dim(M)$, then **(21.3)**(2) yields the opposite inequality, so equality.

Conversely, assume $x \in \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$. Now, $\operatorname{Supp}(M/xM) = \operatorname{Supp}(M) \cap \mathbf{V}(\langle x\rangle)$ by **(13.46)**(1). So $\mathbf{V}(\mathfrak{p}) \subset \operatorname{Supp}(M/xM)$. Hence $\dim(M/xM) \geq \dim(R/\mathfrak{p}) = \dim(M)$. Thus the equality in question fails.

Finally, assume $x \notin \operatorname{z.div}(M)$. Then $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Ass}(M)$ by **(17.12)**. So $x \notin \mathfrak{p}$ for any $\mathfrak{p}$ minimal in $\operatorname{Supp}(M)$ by **(17.14)**. Thus $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \operatorname{Supp}(M)$ with $\dim(R/\mathfrak{p}) = \dim(M)$, and so the desired equality follows from the above. □

(21.6) (Height). — Let R be a ring, and $\mathfrak{p}$ a prime. The **height** of $\mathfrak{p}$, denoted $\operatorname{ht}(\mathfrak{p})$, is defined by this formula:

$$\operatorname{ht}(\mathfrak{p}) := \sup\{\, r \mid \text{there's a chain of primes } \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{p} \,\}.$$

The bijective correspondence $\mathfrak{p} \mapsto \mathfrak{p}R_{\mathfrak{p}}$ of **(11.12)**(2) yields this formula:

$$\operatorname{ht}(\mathfrak{p}) = \dim(R_{\mathfrak{p}}). \tag{21.6.1}$$

If $\operatorname{ht}(\mathfrak{p}) = h$, then we say that $\mathfrak{p}$ is a **height-h prime**.

Corollary (21.7). — *Let $\varphi\colon A \to B$ be a local map of Noetherian local rings, $\mathfrak{m}$ and $\mathfrak{n}$ their maximal ideals. Then*

$$\dim(B) \leq \dim(A) + \dim(B/\mathfrak{m}B),$$

with equality if either (a) *φ has the Going-down Property or* (b) *φ is* **quasi-flat**, *that is, there's a finitely generated B-module M flat over A with $\operatorname{Supp}(M) = \operatorname{Spec}(B)$.*

Proof: Set $s := \dim(A)$. There's a parameter ideal $\mathfrak{q}$ generated by s elements by **(21.4)**. Then $\mathfrak{m}/\mathfrak{q}$ is nilpotent by **(19.13)**(1)⇒(6). So $\mathfrak{m}B/\mathfrak{q}B$ is nilpotent. Apply **(15.24)** with $R := B/\mathfrak{q}B$ and $\mathfrak{a} := \mathfrak{m}B/\mathfrak{q}B$. Thus $\dim(B/\mathfrak{m}B) = \dim(B/\mathfrak{q}B)$.

Say $\mathfrak{q} = \langle x_1, \ldots, x_s\rangle$. Set $M_0 := B$ and $M_i := M/\langle x_1, \ldots, x_i\rangle M$ for $1 \leq i \leq s$. Then **(4.21)** with $\mathfrak{a} := \langle x_1, \ldots, x_i\rangle$ and $\mathfrak{b} := \langle x_{i+1}\rangle$ yields $M_{i+1} \xrightarrow{\sim} M_i/x_{i+1}M_i$. So $\dim(M_{i+1}) \geq \dim(M_i) - 1$ by **(21.5)**. But $M_s = B/\mathfrak{q}B$ and $M_0 := B$. Hence $\dim(B/\mathfrak{q}B) \geq \dim(B) - s$. Thus the inequality holds.

For the equality, note that Case (b) is a special case of Case (a) owing to **(14.8)**. So assume Case (a) obtains; that is, φ has the Going-down Property.

Given any prime $\mathfrak{p}$ of B, note that $\dim(B) \geq \operatorname{ht}(\mathfrak{p}) + \dim(B/\mathfrak{p})$, as concatenating a maximal chain of primes contained in $\mathfrak{p}$ with a maximal chain of primes containing $\mathfrak{p}$ yields a chain of primes of length $\operatorname{ht}(\mathfrak{p}) + \dim(B/\mathfrak{p})$. Fix $\mathfrak{p} \supset \mathfrak{m}B$ such that $\dim(B/\mathfrak{p}) = \dim(B/\mathfrak{m}B)$. Thus it suffices to show that $\operatorname{ht}(\mathfrak{p}) \geq \dim(A)$.

As φ is local, $\varphi^{-1}\mathfrak{n} = \mathfrak{m}$. But $\mathfrak{n} \supset \mathfrak{p} \supset \mathfrak{m}B$, so $\varphi^{-1}\mathfrak{n} \supset \varphi^{-1}\mathfrak{p} \supset \varphi^{-1}\mathfrak{m}B \supset \mathfrak{m}$. Thus $\varphi^{-1}\mathfrak{p} = \mathfrak{m}$. But φ has the Going-down Property. So induction yields a chain of primes of B descending from $\mathfrak{p}$ and lying over any given chain in A. Thus

$\mathrm{ht}(\mathfrak{p}) \ge \dim(A)$, as desired. □

Corollary (21.8). — *Let R be a Noetherian ring, $\mathfrak{p}$ a prime. Then $\mathrm{ht}(\mathfrak{p}) \le r$ if and only if $\mathfrak{p}$ is a minimal prime of some ideal generated by r elements.*

Proof: Assume $\mathfrak{p}$ is minimal over an ideal $\mathfrak{a}$ generated by r elements. Now, any prime of $R_\mathfrak{p}$ over $\mathfrak{a}R_\mathfrak{p}$ is of the form $\mathfrak{q}R_\mathfrak{p}$ where $\mathfrak{q}$ is a prime of R with $\mathfrak{a} \subset \mathfrak{q} \subset \mathfrak{p}$ by (**11.12**). So $\mathfrak{q} = \mathfrak{p}$. So $\mathfrak{p}R_\mathfrak{p} = \sqrt{\mathfrak{a}R_\mathfrak{p}}$ by the Scheinnullstellensatz (**3.14**). So $\mathfrak{a}R_\mathfrak{p}$ is a parameter ideal by (**19.13**)(5)⇒(1). Hence $r \ge s(R_\mathfrak{p})$ by (**21.2**). But $s(R_\mathfrak{p}) = \dim(R_\mathfrak{p})$ by (**21.4**), and $\dim(R_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$ by (**21.6.1**). Thus $\mathrm{ht}(\mathfrak{p}) \le r$.

Conversely, assume $\mathrm{ht}(\mathfrak{p}) \le r$. Then $R_\mathfrak{p}$ has a parameter ideal $\mathfrak{b}$ generated by r elements, say $y_1, \ldots, y_r$ by (**21.6.1**) and (**21.4**). Say $y_i = x_i/s_i$ with $s_i \notin \mathfrak{p}$. Set $\mathfrak{a} := \langle x_1, \ldots, x_r\rangle$. Then $\mathfrak{a}R_\mathfrak{p} = \mathfrak{b}$.

Suppose there is a prime $\mathfrak{q}$ with $\mathfrak{a} \subset \mathfrak{q} \subset \mathfrak{p}$. Then $\mathfrak{b} = \mathfrak{a}R_\mathfrak{p} \subset \mathfrak{q}R_\mathfrak{p} \subset \mathfrak{p}R_\mathfrak{p}$, and $\mathfrak{q}R_\mathfrak{p}$ is prime by (**11.12**)(2). But $\sqrt{\mathfrak{b}} = \mathfrak{p}R_\mathfrak{p}$. So $\mathfrak{q}R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$. Hence $\mathfrak{q} = \mathfrak{p}$ by (**11.12**)(2). Thus $\mathfrak{p}$ is minimal containing $\mathfrak{a}$, which is generated by r elements. □

Theorem (21.9) (Krull Principal Ideal). — *Let R be a Noetherian ring, $x \in R$, and $\mathfrak{p}$ a minimal prime of $\langle x\rangle$. If $x \notin \mathrm{z.div}(R)$, then $\mathrm{ht}(\mathfrak{p}) = 1$.*

Proof: By (**21.8**), $\mathrm{ht}(\mathfrak{p}) \le 1$. But by (**14.7**), $x \in \mathrm{z.div}(R)$ if $\mathrm{ht}(\mathfrak{p}) = 0$. □

Exercise (21.10) . — (1) Let A be a Noetherian local ring with a principal prime $\mathfrak{p}$ of height at least 1. Prove A is a domain by showing any prime $\mathfrak{q} \subsetneqq \mathfrak{p}$ is $\langle 0\rangle$.

(2) Let k be a field, $P := k[[X]]$ the formal power series ring in one variable. Set $R := P \times P$. Prove that R is Noetherian and semilocal, and that R contains a principal prime $\mathfrak{p}$ of height 1, but that R is not a domain.

(21.11) (Quasi-regularity). — Let R be a ring, $x_1, \ldots, x_s$ elements, $X_1, \ldots, X_s$ variables, and M a module. Set $\mathfrak{q} := \langle x_1, \ldots, x_s\rangle$, and define a map of R-modules

$$\phi_s \colon P \to G_\mathfrak{q}(M) \quad \text{with} \quad P := (M/\mathfrak{q}M)[X_1, \ldots, X_s] \tag{21.11.1}$$

by sending a homogeneous polynomial $F(X_1, \ldots, X_s)$ of degree r with coefficients in M to the residue of $F(x_1, \ldots, x_s)$ in $\mathfrak{q}^r M/\mathfrak{q}^{r+1}M$. Note that ϕ_s is well defined, surjective, and homogeneous of degree 0 when P is graded by degree.

If ϕ_s is bijective and $\mathfrak{q}M \ne M$, then $x_1, \ldots, x_s$ is said to be M**-quasi-regular**.

Proposition (21.12). — *Let R be a ring, M a Noetherian semilocal module. Let $x_1, \ldots, x_s$ be a sop for M, and set $\mathfrak{q} := \langle x_1, \ldots, x_s\rangle$. Then $e(\mathfrak{q}, M) \le \ell(M/\mathfrak{q}M)$, with equality if and only if $x_1, \ldots, x_s$ is M-quasi-regular.*

Proof: For $n \ge 0$, using (**21.11**), define N_n by the exact sequence

$$0 \to N_n \to P_n \xrightarrow{(\phi_s)_n} \mathfrak{q}^n M/\mathfrak{q}^{n+1}M \to 0. \tag{21.12.1}$$

Note that $\ell(P_n) = \ell(M/\mathfrak{q}M)\binom{s-1+n}{s-1}$ by (**20.4**). Thus

$$\ell(P_n) = \big(\ell(M/\mathfrak{q}M) \;/\; (s-1)!\big)n^{s-1} + \text{lower degree terms.} \tag{21.12.2}$$

Also $\deg p_\mathfrak{q}(M, n) = d(M)$ by (**21.2**), and $d(M) = s(M)$ by (**21.4**), and $s(M) = s$ by (**21.4**) again; so $\deg p_\mathfrak{q}(M, n) = s$. So (**20.11**) with $d = s$ yields, for $n \gg 0$,

$$\ell(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) = \big(e(\mathfrak{q}, M) \;/\; (s-1)!\big)n^{s-1} + \text{ lower degree terms.} \tag{21.12.3}$$

But (**19.7**) yields $\ell(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) \le \ell(P_n)$ for all n. Thus (**21.12.2**) and (**21.12.3**) yield $e(\mathfrak{q}, M) \le \ell(M/\mathfrak{q}M)$.

By (**21.11**), $x_1, \dots, x_s$ is M-quasi-regular if and only if ϕ_s is bijective. If ϕ_s is so, then $\ell(P_n) = \ell(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M)$ for all n by (**21.12.1**). Thus (**21.12.2**) and (**21.12.3**) yield $e(\mathfrak{q}, M) = \ell(M/\mathfrak{q}M)$.

Assume ϕ_s isn't bijective. Then (**21.12.1**) yields q with a nonzero $G \in N_q$.

Say $\mathbf{V}(\mathfrak{q}) = \{\mathfrak{m}_1, \dots, \mathfrak{m}_h\}$, and set $\mathfrak{m} := \mathfrak{m}_1 \cdots \mathfrak{m}_h$. Then $\mathfrak{m}^r(M/\mathfrak{q}M) = 0$ for some r by (1)⇒(6) of (**19.13**). Hence $\mathfrak{m}^r P = 0$. So $\mathfrak{m}^r G = 0$. Take p so that $\mathfrak{m}^p G = 0$, but $\mathfrak{m}^{p-1} G \neq 0$. Then take k so that $\mathfrak{m}_1 \cdots \mathfrak{m}_k \mathfrak{m}^{p-1} G = 0$, but $\mathfrak{m}_1 \cdots \mathfrak{m}_{k-1} \mathfrak{m}^{p-1} G \neq 0$. Then there's $x \in \mathfrak{m}_1 \cdots \mathfrak{m}_{k-1} \mathfrak{m}^{p-1}$ with $xG \neq 0$. Replace G by xG. Then $G \neq 0$, but $\mathfrak{m}_k G = 0$. Also $G \in N_q$.

Set $K := R/\mathfrak{m}_k$ and $Q := K[X_1, \dots, X_s]$. Grade Q by degree, and for each $n \geq q$, form the R-linear map

$$\nu\colon Q_{n-q} \to P_n \quad \text{by} \quad \nu(F) := FG.$$

It's well defined as $\mathfrak{m}_k G = 0$. Let's see that it's injective.

Let $F \in Q_{n-q}$ be nonzero. As in (**2.4**), consider the grlex leading coefficients a of F and b of G. Then $a \in K^\times$. So $ab \in M/\mathfrak{q}M$ is nonzero. Hence ab is the grlex leading coefficient of FG, and so FG is nonzero. Thus ν is injective.

Given $F \in Q_{n-q}$, lift F to $\widetilde{F} \in R[X_1, \dots, X_n]$. Then $\widetilde{F}(x_1, \dots, x_s) \in \mathfrak{q}^{n-q}$. Denote its residue in $\mathfrak{q}^{n-q}/\mathfrak{q}^{n-q+1}$ by f. Then $\phi_s(FG) = f\phi_s(G) = 0$. Hence $\nu(F) \in N_n$. Thus $\nu(Q_{n-q}) \subset N_n$.

As ν is injective, $\ell(Q_{n-q}) \leq \ell(N_n)$. But $\ell(Q_{n-q}) = \binom{s-1+n-q}{s-1}$ by (**20.4**). Also $\binom{s-1+n-q}{s-1} = n^{s-1}/(s-1)! + \text{lower degree terms}$. Further, (**21.12.1**) and (**19.7**) yield $\ell(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) = \ell(P_n) - \ell(N_n)$. So (**21.12.2**) yields

$$\ell(\mathfrak{q}^n M/\mathfrak{q}^{n+1}M) \leq \big((\ell(M/\mathfrak{q}M) - 1) \,/\, (s-1)! \big) n^{s-1} + \text{lower degree terms}.$$

Thus (**21.12.3**) yields $e(\mathfrak{q}, M) \leq \ell(M/\mathfrak{q}M) - 1$, as desired. □

Exercise (21.13) . — Let A be a Noetherian local ring of dimension r. Let $\mathfrak{m}$ be the maximal ideal, and $k := A/\mathfrak{m}$ the residue class field. Prove that

$$r \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2),$$

with equality if and only if $\mathfrak{m}$ is generated by r elements.

(21.14) (Regular local rings). — Let A be a Noetherian local ring of dimension r with maximal ideal $\mathfrak{m}$ and residue field k. We say A is **regular** if $\mathfrak{m}$ is generated by r elements. If so, then, as $r = s(R)$ by (**21.4**), any such r elements form a system of parameters; it is known as a **regular** system of parameters, or **regular** sop.

By (**21.13**), A is regular if and only if $r = \dim_k(\mathfrak{m}/\mathfrak{m}^2)$. If so, then, by (**10.9**), elements of $\mathfrak{m}$ form a regular sop if and only if their residues form a k-basis of $\mathfrak{m}/\mathfrak{m}^2$.

For example, a field is a regular local ring of dimension 0, and conversely. An example of a regular local ring of given dimension n is the localization $P_\mathfrak{m}$ of a polynomial ring P in n variables over a field at any maximal ideal $\mathfrak{m}$, as $\dim(P_\mathfrak{m}) = n$ by (**15.10**) and (**15.12**) and as $\mathfrak{m}$ is generated by n elements by (**15.6**).

Corollary (21.15). — *Let A be a Noetherian local ring of dimension r, and $\mathfrak{m}$ its maximal ideal. Then A is regular if and only if its associated graded ring $G(A)$ is a polynomial ring; if so, then the number of variables is r and $e(\mathfrak{m}, A) = 1$.*

Proof: Say $G(A)$ is a polynomial ring in s variables. Then $\dim(\mathfrak{m}/\mathfrak{m}^2) = s$. By (**20.4**), $\deg h(G(A), n) = s-1$. So $s = d(A)$ by (**20.11**) and (**21.2**). But $d(A) = r$ by (**21.4**). Thus $s = r$, and by (**21.14**), A is regular.

Conversely, assume A is regular. By **(21.14)**, $\mathfrak{m}$ is generated by r elements. which form a system of parameters. So **(21.12)** yields $1 \le e(\mathfrak{m},\, A) \le \ell(A/\mathfrak{m}) = 1$. Thus $e(\mathfrak{m},\, A) = 1$, and so by **(21.12)** again, the map ϕ_s of **(21.11.1)** is bijective. □

Exercise (21.16) . — Let A be a Noetherian local ring of dimension r, and let $x_1, \ldots, x_s \in A$ with $s \le r$. Set $\mathfrak{a} := \langle x_1, \ldots, x_s\rangle$ and $B := A/\mathfrak{a}$. Prove equivalent:

(1) A is regular, and there are $x_{s+1}, \ldots, x_r \in A$ with $x_1, \ldots, x_r$ a regular sop.
(2) B is regular of dimension $r - s$.

Theorem (21.17). — *A regular local ring A is a domain.*

Proof: Use induction on $r := \dim A$. If $r = 0$, then A is a field, so a domain.

Assume $r \ge 1$. Let x be a member of a regular sop. Then $A/\langle x\rangle$ is regular of dimension $r - 1$ by **(21.16)**. By induction, $A/\langle x\rangle$ is a domain. So $\langle x\rangle$ is prime. Thus A is a domain by **(21.10)**(1). (Another proof is found in **(22.39)**(2).) □

Lemma (21.18). — *Let A be a local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{a}$ a proper ideal. Set $\mathfrak{n} := \mathfrak{m}/\mathfrak{a}$ and $k := A/\mathfrak{m}$. Then this sequence of k-vector spaces is exact:*

$$0 \to (\mathfrak{m}^2 + \mathfrak{a})/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2 \to 0.$$

Proof: The assertion is very easy to check. □

Proposition (21.19). — *Let A be a regular local ring of dimension r, and $\mathfrak{a}$ an ideal. Set $B := A/\mathfrak{a}$, and assume B is regular of dimension $r - s$. Then $\mathfrak{a}$ is generated by s elements, and any such s elements form part of a regular sop.*

Proof: In its notation, **(21.18)** yields $\dim((\mathfrak{m}^2 + \mathfrak{a})/\mathfrak{m}^2) = s$. Hence, any set of generators of $\mathfrak{a}$ includes s members of a regular sop of A. Let $\mathfrak{b}$ be the ideal the s generate. Then $A/\mathfrak{b}$ is regular of dimension $r - s$ by **(21.16)**. By **(21.17)**, both $A/\mathfrak{b}$ and B are domains of dimension $r - s$; whence, **(15.25)** implies $\mathfrak{a} = \mathfrak{b}$. □

B. Exercises

Exercise (21.20) . — Let R be a ring, R' an algebra, and N a nonzero R'-module that's a Noetherian R-module. Prove the following statements:

(1) $\dim_R(N) = \dim_{R'}(N)$.
(2) Each prime in $\mathrm{Supp}_{R'}(N)$ contracts to a prime in $\mathrm{Supp}_R(N)$. Moreover, one is maximal if and only if the other is.
(3) Each maximal ideal in $\mathrm{Supp}_R(N)$ is the contraction of at least one and at most finitely many maximal ideals in $\mathrm{Supp}_{R'}(N)$.
(4) $\mathrm{rad}_R(N)R' \subset \mathrm{rad}_{R'}(N)$.
(5) N is semilocal over R if and only if N is semilocal over R'.

Exercise (21.21) . — Let R be a ring, M a nonzero Noetherian semilocal module, $\mathfrak{q}$ a parameter ideal, and $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ a chain of submodules with $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in \mathrm{Supp}(M)$. Set $d := \dim(M)$ and set

$$I := \{\, i \mid \dim(R/\mathfrak{p}_i) = d \,\} \quad \text{and} \quad \Phi := \{\, \mathfrak{p} \in \mathrm{Supp}(M) \mid \dim(R/\mathfrak{p}) = d \,\}.$$

Prove: (1) $e(\mathfrak{q}, M) = \sum_{i\in I} e(\mathfrak{q},\, R/\mathfrak{p}_i)$ and (2) $e(\mathfrak{q}, M) = \sum_{\mathfrak{p}\in\Phi} \ell_{R_\mathfrak{p}}(M_\mathfrak{p}) e(\mathfrak{q},\, R/\mathfrak{p})$.

Exercise (21.22) . — Let k be a field, R a finitely generated k-algebra, $\overline{k}$ an algebraic closure of k. Let A be the localization of R at a maximal ideal $\mathfrak{m}$. Set $K := A/\mathfrak{m}A$, set $\overline{A} := A \otimes_k \overline{k}$, and let $\mathfrak{n}$ be a maximal ideal of $\overline{A}$. Show:

(1) $\overline{A}$ is semilocal and for each $\mathfrak{n}$ the residue field of $\overline{A}_\mathfrak{n}$ is equal to $\overline{k}$.

(2) Assume $\overline{A}$ is regular; that is $\overline{A}_\mathfrak{n}$ is regular for each $\mathfrak{n}$. Then A is regular.

Exercise (21.23) . — Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{q}$ a parameter ideal, $P := (A/\mathfrak{q})[X_1, \ldots, X_s]$ a polynomial ring for some $s \ge 0$. Show:

(1) Set $\mathfrak{M} := (\mathfrak{m}/\mathfrak{q})[X_1, \ldots, X_s]$. Then $\mathrm{z.div}(P) = \mathfrak{M}$.

(2) Assume $\mathfrak{q}$ is generated by a sop $x_1, \ldots, x_s$. Let $\phi_s \colon P \to G_\mathfrak{q}(A)$ be the map of **(21.11.1)**. Then $\mathrm{Ker}(\phi_s) \subset \mathrm{z.div}(P)$.

Exercise (21.24) . — Let A be a Noetherian local ring, $k \subset A$ a **coefficient** field (or field of representatives) — that is, k maps isomorphically onto the residue field — $x_1, \ldots, x_s$ a sop. Using **(21.23)**, show the x_i are algebraically independent over k.

Exercise (21.25) . — Let k be an algebraically closed field, R an algebra-finite domain, $\mathfrak{m}$ a maximal ideal of R. Using the dimension theory in this chapter and **(15.1)**(1), but not (2), show $\dim(R) = \dim(R_\mathfrak{m}) = \mathrm{tr.deg}_k(\mathrm{Frac}(R))$. (Compare with **(15.10)** and **(15.12)**.)

Exercise (21.26) . — Let R be a ring, N a Noetherian semilocal module, and $y_1, \ldots, y_r$ a sop for N. Set $N_i := N/\langle y_1, \ldots, y_i\rangle N$. Show $\dim(N_i) = r - i$.

Exercise (21.27) . — Let R be a ring, $\mathfrak{p}$ a prime, M a finitely generated module. Set $R' := R/\mathrm{Ann}\, M$. Prove these two statements: (1) $\dim(M_\mathfrak{p}) = \dim(R'_\mathfrak{p})$.

(2) If $\mathrm{Ann}(M) = \langle 0\rangle$, then $\dim(M_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$.

Exercise (21.28) . — Let R be a Noetherian ring, and $\mathfrak{p}$ be a prime minimal containing $x_1, \ldots, x_r$. Given r' with $1 \le r' \le r$, set $R' := R/\langle x_1, \ldots, x_{r'}\rangle$ and $\mathfrak{p}' := \mathfrak{p}/\langle x_1, \ldots, x_{r'}\rangle$. Assume $\mathrm{ht}(\mathfrak{p}) = r$. Prove $\mathrm{ht}(\mathfrak{p}') = r - r'$.

Exercise (21.29) . — Let R be a Noetherian ring, $\mathfrak{p}$ a prime of height at least 2. Prove that $\mathfrak{p}$ is the union of height-1 primes, but not of finitely many.

Exercise (21.30) . — Let R be a Noetherian ring of dimension at least 1. Show that the following conditions are equivalent:

(1) R has only finitely many primes.

(2) R has only finitely many height-1 primes.

(3) R is semilocal of exactly dimension 1.

Exercise (21.31) (*Artin–Tate* [2, Thm. 4]**) . —** Let R be a Noetherian domain, and set $K := \mathrm{Frac}(R)$. Prove the following statements are equivalent:

(1) $\langle fX - 1\rangle \subset R[X]$ is a maximal ideal for some nonzero $f \in R$.

(2) $K = R_f$ for some nonzero $f \in R$.

(3) K is algebra finite over R.

(4) Some nonzero $f \in R$ lies in every nonzero prime.

(5) R has only finitely many height-1 primes.

(6) R is semilocal of dimension 1.

Exercise (21.32) . — Let R be a Noetherian domain, p a prime element. Show that $\langle p\rangle$ is a height-1 prime ideal.

Exercise (21.33) . — Let R be a UFD, and $\mathfrak{p}$ a height-1 prime ideal. Show that $\mathfrak{p} = \langle p \rangle$ for some prime element p.

Exercise (21.34) . — Let R be a Noetherian domain such that every height-1 prime ideal $\mathfrak{p}$ is principal. Show that R is a UFD.

Exercise (21.35) (*Gauss' Lemma*) . — Let R be a UFD; X a variable; $F,\ G \in R[X]$ nonzero. Call F **primitive** if its coefficients have no common prime divisor.

(1) Show that F is primitive if and only if $c(F)$ lies in no height-1 prime ideal.
(2) Assume that F and G are primitive. Show that FG is primitive.
(3) Let $f,\ g,\ h$ be the gcd's of the coefficients of $F,\ G,\ FG$. Show $fg = h$.
(4) Assume $c(F) = \langle f \rangle$ with $f \in R$. Show f is the gcd of the coefficients of F.

Exercise (21.36) . — Let R be a finitely generated algebra over a field. Assume R is a domain of dimension r. Let $x \in R$ be neither 0 nor a unit. Set $R' := R/\langle x \rangle$. Prove that $r-1$ is the length of any chain of primes in R' of maximal length.

Exercise (21.37) . — Let k be a field, $P = k[X_1, \ldots, X_n]$ the polynomial ring, R_1 and R_2 two P-algebra-finite domains, and $\mathfrak{p}$ a minimal prime of $R_1 \otimes_P R_2$.

(1) Set $C := R_1 \otimes_k R_2$, and let $\mathfrak{q} \subset C$ denote the preimage of $\mathfrak{p}$. Use (8.28)(1) to prove that $\mathfrak{q}$ is a minimal prime of an ideal generated by n elements.

(2) Use (15.12) and (15.29) to prove this inequality:

$$\dim(R_1) + \dim(R_2) \le n + \dim\big((R_1 \otimes_P R_2)/\mathfrak{p}\big). \tag{21.37.1}$$

Exercise (21.38) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, R' a P-algebra-finite domain. Let $\mathfrak{p}$ be a prime of P, and $\mathfrak{p}'$ a minimal prime of $\mathfrak{p}R'$. Prove this inequality: $\operatorname{ht}(\mathfrak{p}') \le \operatorname{ht}(\mathfrak{p})$.

Exercise (21.39) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ primes of P, and $\mathfrak{p}$ a minimal prime of $\mathfrak{p}_1 + \mathfrak{p}_2$. Prove this inequality:

$$\operatorname{ht}(\mathfrak{p}) \le \operatorname{ht}(\mathfrak{p}_1) + \operatorname{ht}(\mathfrak{p}_2). \tag{21.39.1}$$

Exercise (21.40) . — Let k be a field, $k[X,Y,Z,W]$ the polynomial ring. Set

$$\mathfrak{q}_1 := \langle X,\ Y \rangle \quad\text{and}\quad \mathfrak{q}_2 := \langle Z,\ W \rangle \quad\text{and}\quad \mathfrak{q} := \langle X,\ Y,\ Z,\ W \rangle \quad\text{and}$$
$$R := k[X,\ Y,\ Z,\ W]\big/\langle XZ - YW \rangle \quad\text{and}\quad \mathfrak{p}_i := \mathfrak{q}_i R \quad\text{and}\quad \mathfrak{p} := \mathfrak{q}R.$$

Show that $\mathfrak{p}_1,\ \mathfrak{p}_2,\ \mathfrak{p}$ are primes of heights $1, 1,\ 3$. Does (21.39.1) hold with $P := R$?

Exercise (21.41) . — Let R be a Noetherian ring, $X, X_1, \ldots, X_n$ variables. Show:

$$\dim(R[X]) = 1 + \dim(R) \quad\text{and}\quad \dim(R[X_1, \ldots, X_n]) = n + \dim(R).$$

Exercise (21.42) (*Jacobian Criterion*) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, $\mathfrak{A} \subset P$ an ideal, $\mathbf{x} := (x_1, \ldots, x_n) \in k^n$. Set $R := P/\mathfrak{A}$ and $\mathfrak{M} := \langle X_1 - x_1, \ldots, X_n - x_n \rangle$. Prove the following statements:

(1) Say $\mathfrak{A} = \langle F_1, \ldots, F_m \rangle$. Assume $F_i(\mathbf{x}) = 0$ for all i. For all i, j, define $\partial F_i/\partial X_j \in P$ formally as in (1.18.1), and set $a_{ij} := (\partial F_i/\partial X_j)(\mathbf{x})$. Let r be the rank of the m by n matrix (a_{ij}). Set $d := \dim R_{\mathfrak{M}}$. Then these conditions are equivalent: (a) $R_{\mathfrak{M}}$ is regular; (b) $r = n - d$; and (c) $r \ge n - d$.

(2) Assume $\mathfrak{A}$ is prime, $F \notin \mathfrak{A}$, and k is algebraically closed. Then there's a choice of $\mathbf{x}$ with $F(\mathbf{x}) \ne 0$ and $\mathfrak{A} \subset \mathfrak{M}$ and $R_{\mathfrak{M}}$ regular.

Start with the case $\mathfrak{A} = \langle G \rangle$. Then reduce to it by using a separating transcendence basis for $K := \operatorname{Frac}(R)$ over k and a primitive element.

22. Completion

Completion is used to simplify a ring and its modules beyond localization. First, we discuss the topology of a filtration, and use Cauchy sequences to construct the (separated) completion. Then we discuss the inverse limit, the dual notion of the direct limit; using it, we obtain an alternate construction. We conclude that, if we use the $\mathfrak{a}$-adic filtration, for any ideal $\mathfrak{a}$, then the functor of completion is exact on the Noetherian modules. Moreover, if the ring is Noetherian, then the completion of a finitely generated module is equal to its tensor product with the completion of the ring; hence, the latter is flat. Lastly, we prove that the completion of a Noetherian module is Noetherian over the completion of the ring.

In an appendix, we study **Henselian rings**, the local rings such that, given a monic univariate polynomial F, any factorization of F, modulo the maximal ideal, into monic and coprime factors, lifts to a factorization of F itself. The completion of any local ring is Henselian by Hensel's Lemma, which we prove. We characterize Henselian rings as the local rings over which any module-finite algebra is decomposable; hence, such an algebra, if local, is Henselian too. Next, we consider an **equicharacteristic** local ring: it and its residue field k have the same characteristic. Its completion contains a **coefficient field**, one mappng isomorphically onto k, by the Cohen Existence Theorem, which we prove using Hensel's lemma.

Lastly, we prove the Weierstraß Division Theorem and Preparation Theorem. The former is a version of the Division Algorithm for formal power series in one variable X over a ring R that is separated and complete in the $\mathfrak{a}$-adic topology for some ideal $\mathfrak{a}$; the divisor $F = \sum f_i X^i$ must have f_n a unit in R for some $n \geq 0$ but $f_i \in \mathfrak{a}$ for $i < n$. The Preparation Theorem asserts $F = UV$ uniquely, where U is an invertible power series and V is a monic polynomial. We adapt these theorems to the local ring A of convergent complex power series in several variables, and conclude that A is Henselian, regular, and a UFD.

A. Text

(22.1) (Topology and completion). — Let R be a ring, M a filtered module with filtration $F^\bullet M$. Then M has a (linear) *topology*: the open sets are the arbitrary unions of sets of the form $m+F^nM$ for various m and n. Indeed, the intersection of two open sets is open, as the intersection of two unions is the union of the pairwise intersections; further, if the intersection U of $m+F^nM$ and $m'+F^{n'}M$ is nonempty and if $n \geq n'$, then $U = m + F^nM$, because, if say $m'' \in U$, then

$$m + F^nM = m'' + F^nM \subset m'' + F^{n'}M = m' + F^{n'}M. \tag{22.1.1}$$

Let $K \subset M$ be a submodule. If $K \supset F^nM$ for some n, then K is both open and closed for this reason: given $m \in K$, we have $m + F^nM \subset K$; given $m \in M - K$, we have $m + F^nM \subset M - K$. In particular, *each F^nM is both open and closed.*

The addition map $M \times M \to M$, given by $(m, m') \mapsto m + m'$, *is continuous,* as

$$(m + F^nM) + (m' + F^nM) \subset (m + m') + F^nM.$$

So, with m' fixed, *the translation $m \mapsto m + m'$ is a homeomorphism $M \to M$.* (Similarly, inversion $m \mapsto -m$ is a homeomorphism; so M is a topological group.)

Given another filtration $\widetilde{F}^{\bullet}M$ such that, for any m, there's n with $F^mM \supset \widetilde{F}^nM$, and for any p, there's q with $\widetilde{F}^pM \supset F^qM$, both filtrations yield the same topology.

Let $\mathfrak{a}$ be an ideal, and give R the $\mathfrak{a}$-adic filtration. If the filtration on M is an $\mathfrak{a}$-filtration, then scalar multiplication $(x, m) \mapsto xm$ too is continuous, because

$$(x + \mathfrak{a}^n)(m + F^nM) \subset xm + F^nM.$$

Further, if the filtration is $\mathfrak{a}$-stable, then it yields the same topology as the $\mathfrak{a}$-adic filtration, because for some n' and any n,

$$F^nM \supset \mathfrak{a}^nM \supset \mathfrak{a}^nF^{n'}M = F^{n+n'}M.$$

Thus *any two stable* $\mathfrak{a}$*-filtrations give the same topology*: the **$\mathfrak{a}$-adic topology**.

When $\mathfrak{a}$ is given, it is *conventional* to use the $\mathfrak{a}$-adic filtration and $\mathfrak{a}$-adic topology unless there's explicit mention to the contrary. Moreover, if M is semilocal, then it is *conventional* to take $\mathfrak{a}$ to be $\mathrm{rad}(M)$ or another parameter ideal $\mathfrak{q}$; the topology is the same for all $\mathfrak{q}$ owing to (1)⇒(6) of **(19.13)**. Further, if R is semilocal, then it is *conventional* to take $\mathfrak{a}$ to be $\mathrm{rad}(R)$ or another parameter ideal $\mathfrak{r}$ for R; recall from **(21.2)** that $\mathfrak{r}$ is also a parameter ideal for M.

Let $\overline{K}$ denote the closure of the submodule $K \subset M$. Then $m \in M - \overline{K}$ means there's n with $(m + F^nM) \cap K = \emptyset$, or equivalently $m \notin (K + F^nM)$. Thus $\overline{K} = \bigcap_n (K + F^nM)$. In particular, $\{0\}$ *is closed if and only* if $\bigcap F^nM = \{0\}$.

Also, M *is* **separated** — that is, Hausdorff — *if and only if* $\{0\}$ *is closed.* For, if $\{0\}$ is closed, so is each $\{m\}$. So given $m' \neq m$, there's n' with $m \notin (m' + F^{n'}M)$. Take $n \geq n'$. Then $(m + F^nM) \cap (m' + F^{n'}M) = \emptyset$ owing to **(22.1.1)**.

Finally, M is **discrete** — that is, every $\{m\}$ is both open and closed — *if and only if* $\{0\}$ *is just open, if and only if* $F^nM = 0$ *for some* n.

A sequence $(m_n)_{n\geq 0}$ in M is called **Cauchy** if, given n_0, there's n_1 with

$$m_n - m_{n'} \in F^{n_0}M, \quad \text{or simply } \ m_n - m_{n+1} \in F^{n_0}M, \quad \text{for all } \ n, n' \geq n_1;$$

the two conditions are equivalent because $F^{n_0}M$ is a subgroup and

$$m_n - m_{n'} = (m_n - m_{n+1}) + (m_{n+1} - m_{n+2}) + \cdots + (m_{n'-1} - m_{n'}).$$

An $m \in M$ is called a **limit** of (m_n) if, given n_0, there's n_1 with $m - m_n \in F^{n_0}M$ for all $n \geq n_1$. If so, we say (m_n) **converge** to m, and write $m = \lim m_n$.

Plainly, if (m_n) converges, then it's Cauchy If every Cauchy sequence converges, then M is called **complete.** Plainly, the notions of Cauchy sequence and limit depend only on the topology.

The Cauchy sequences form a module $C(M)$ under termwise addition and scalar multiplication. The sequences with 0 as a limit form a submodule $Z(M)$. Set

$$\widehat{M} := C(M)/Z(M).$$

Call $\widehat{M}$ the (separated) **completion** of M; this name is justified by **(22.13)**(2), **(22.16)**(4), and **(22.54)** below.

Form the R-map $M \to C(M)$ that carries m to the constant sequence (m). Composing it with the quotient map $C(M) \to \widehat{M}$ yields this canonical R-map:

$$\kappa_M \colon M \to \widehat{M} \quad \text{by} \quad \kappa_M m := \text{the residue of } (m). \qquad \textbf{(22.1.2)}$$

If M *is discrete,* then every Cauchy sequence stabilizes; hence, *then* κ_M *is bijective; moreover,* M *is separated and complete.* For example, an Artinian ring R is discrete as its radical is nilpotent by **(19.23)**; so R is separated and complete.

The submodule $K \subset M$ carries an induced filtration: $F^nK := K \cap F^nM$. Plainly $C(K) \subset C(M)$ and $Z(K) = C(K) \cap Z(M)$. Thus $\widehat{K} \subset \widehat{M}$ and $\kappa_K = \kappa_M|K$. In particular, the $\widehat{F^nM}$ form a filtration of $\widehat{M}$.

Note $\widehat{F^nM} \bigcap \widehat{K} \supset \widehat{F^nK}$. Conversely, given $m \in \widehat{F^nM} \bigcap \widehat{K}$, lift it to (m_k) in $C(M)$. Then $m_k \in F^nM \cap K$ for $k \gg 0$. So $m \in \widehat{F^nK}$. Thus $\widehat{F^nM} \bigcap \widehat{K} = \widehat{F^nK}$; that is, on $\widehat{K}$, the $\widehat{F^nM}$ induce the filtration formed by the $\widehat{F^nK}$.

Note $\kappa_M^{-1}\widehat{F^nM} \supset F^nM$ as $\kappa_M|F^nM = \kappa_{F^nM}$. Conversely, given a constant sequence $(m) \in C(F^nM)$, note $m \in F^nM$. Thus $\kappa_M^{-1}\widehat{F^nM} = F^nM$.

Let $\alpha\colon M \to N$ be a **map of filtered modules** with filtrations $F^\bullet M$ and $F^\bullet N$; that is, $\alpha(F^nM) \subset F^nN$ for all n. Plainly α is continuous, and preserves Cauchy sequences and limits. So α induces an R-map $C(M) \to C(N)$ by $(m_n) \mapsto (\alpha m_n)$, and it carries $Z(M)$ into $Z(N)$. Thus α induces an R-map $\widehat{\alpha}\colon \widehat{M} \to \widehat{N}$ with $\widehat{\alpha}\kappa_M = \kappa_N\alpha$. Plainly, $(\alpha|F^nM)\widehat{\ }\colon \widehat{F^nM} \to \widehat{F^nN}$ is equal to $\widehat{\alpha} \bigm| \widehat{F^nM}$; thus $\widehat{\alpha}$ is a map of filtered modules. Moreover, *$M \mapsto \widehat{M}$ is an R-linear functor.*

Again, let $\mathfrak{a}$ be an ideal. Under termwise multiplication of Cauchy sequences, *$\widehat{R}$ is a ring, $\kappa_R\colon R \to \widehat{R}$ is a ring map, and $\widehat{M}$ is an $\widehat{R}$-module.* Similarly, given an ideal $\mathfrak{b} \subset R$ equipped with the $\mathfrak{a}$-adic topology, define the $\widehat{R}$-submodule $\widehat{\mathfrak{b}}\widehat{M} \subset \widehat{M}$, even if the natural map $\widehat{\mathfrak{b}} \to \widehat{R}$ isn't injective. A priori, the $\mathfrak{a}$-adic filtration of $\widehat{M}$ might differ from the induced filtration, which is given by $F^nM := \widehat{\mathfrak{a}^nM}$ for all n; however, when M is Noetherian, the two coincide by **(22.21)**.

Example (22.2). — Let R be a ring, $X_1, \dots, X_r$ variables. Set $P := R[X_1, \dots, X_r]$ and $\mathfrak{a} := \langle X_1, \dots, X_r\rangle$. Then a sequence $(F_n)_{n\ge0}$ of polynomials is Cauchy in the $\mathfrak{a}$-adic topology if and only if, given n_0, there's n_1 such that, for all $n \ge n_1$, the F_n agree in degree less than n_0. So (F_n) determines a power series, and it is 0 if and only if (F_n) converges to 0. Thus $\widehat{P}$ is just the power series ring $R[[X_1, \dots, X_r]]$.

Given $n \ge 0$, note $\mathfrak{a}^n$ consists of the polynomials with no monomial of degree less than n. So a Cauchy sequence of polynomials in $\mathfrak{a}^n$ converges to a power series with no monomial of degree less than n. Hence $\widehat{\mathfrak{a}^n} = \mathfrak{a}^n\widehat{P}$. Thus $\widehat{P}$ has the $\mathfrak{a}$-adic topology. Note $\bigcap \mathfrak{a}^n\widehat{P} = \{0\}$; thus $\widehat{P}$ is separated. Further, a sequence $(m_n)_{n\ge0}$ of power series is Cauchy if and only if, given n_0, there's n_1 such that, for all $n \ge n_1$, the m_n agree in degree less than n_0. Thus $\widehat{P}$ is complete.

For another example, take a prime integer p, and set $\mathfrak{a} := \langle p\rangle$. Then a sequence $(x_n)_{n\ge0}$ of integers is Cauchy if and only if, given n_0, there's n_1 such that, for all $n, n' \ge n_1$, the difference $x_n - x_{n'}$ is a multiple of p^{n_0}. The completion, denoted $\widehat{\mathbb{Z}}_p$, is called the **ring of p-adic integers**, and consists of the sums $\sum_{i=0}^\infty z_ip^i$ with $0 \le z_i < p$. Moreover, $\widehat{\mathbb{Z}}_p$ has the p-adic topology, and is separated and complete.

Exercise (22.3) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Prove that

$$\operatorname{Ker}(\kappa_M) = \bigcap F^nM. \qquad \textbf{(22.3.1)}$$

where κ_M is the map of **(22.1.2)**. Conclude that these conditions are equivalent:

(1) $\kappa_M\colon M \to \widehat{M}$ is injective; (2) $\bigcap F^nM = \{0\}$; (3) M is separated.

Assume M is Noetherian and $F^\bullet M$ is the $\mathfrak{a}$-adic filtration for a proper ideal $\mathfrak{a}$ with either (a) $\mathfrak{a} \subset \operatorname{rad}(M)$ or (b) R a domain and M torsionfree. Prove $M \subset \widehat{M}$.

Proposition (22.4). — *Let R be a ring, and $\mathfrak{a}$ an ideal. Then $\widehat{\mathfrak{a}} \subset \operatorname{rad}(\widehat{R})$.*

Proof: Given $a \in \widehat{\mathfrak{a}}$, represent a by $(a_n) \in C(\mathfrak{a})$. For all n, set $b_n := 1 - a_n$ and $c_n := 1 + a_n + \cdots + a_n^n$ and $d_n := 1 - a_n^{n+1}$; then $b_n c_n = d_n$. Note (b_n) and (c_n) and (d_n) are Cauchy. Also, (b_n) and (d_n) represent $1 - a$ and 1 in $\widehat{R}$. Say (c_n) represents c. Then $(1 - a)c = 1$. Thus (**3.2**) implies $\widehat{\mathfrak{a}} \subset \operatorname{rad}(\widehat{R})$. □

(22.5) (Inverse limits). — Let R be a ring. A sequence of modules Q_n and maps $\alpha_n^{n+1} \colon Q_{n+1} \to Q_n$ for $n \geq 0$ is called an **inverse system**. Its **inverse limit** $\varprojlim Q_n$ is the submodule of $\prod Q_n$ of all vectors (q_n) with $\alpha_n^{n+1} q_{n+1} = q_n$ for all n.

Define $\theta \colon \prod Q_n \to \prod Q_n$ by $\theta(q_n) := (q_n - \alpha_n^{n+1} q_{n+1})$. Then

$$\varprojlim Q_n = \operatorname{Ker}\theta. \quad \text{Set } \varprojlim{}^1 Q_n := \operatorname{Coker}\theta. \tag{22.5.1}$$

Plainly, $\varprojlim Q_n$ *has this UMP: given maps $\beta_n \colon P \to Q_n$ with $\alpha_n^{n+1}\beta_{n+1} = \beta_n$, there's a unique map $\beta \colon P \to \varprojlim Q_n$ with $\pi_n \beta = \beta_n$ for all n.*

Further, owing to the UMP, a map of inverse systems, in the obvious sense of the term, induces a map between their inverse limits. (The notion of inverse limit is formally dual to that of direct limit.)

For instance, a module M with a filtration $F^\bullet M$ yields the inverse system with $Q_n := M/F^n M$ and α_n^{n+1} the quotient maps for $n \geq 0$. Moreover, let $\alpha \colon M \to N$ be a map of filtered modules, $F^\bullet N$ the filtration on N, and $\alpha_n \colon M/F^n M \to N/F^n N$ the induced maps. The α_n form a map of inverse systems, as they respect the quotient maps. In (**22.7**) below, we prove $\widehat{M} = \varprojlim (M/F^n M)$ and $\widehat{\alpha} = \varprojlim \alpha_n$.

Example (22.6). — First, let R be a ring, $P := R[X_1, \ldots, X_r]$ the polynomial ring in r variables. Set $\mathfrak{m} := \langle X_1, \ldots, X_r \rangle$ and $P_n := P/\mathfrak{m}^{n+1}$. Then P_n is just the algebra of polynomials of degree at most n, and the quotient map $\alpha_n^{n+1} \colon P_{n+1} \to P_n$ is just truncation. Thus $\varprojlim P_n$ is equal to the power series ring $R[[X_1, \ldots, X_r]]$.

Second, take a prime integer p, and set $\mathbb{Z}_n := \mathbb{Z}/\langle p^{n+1} \rangle$. Then $\mathbb{Z}_n$ is just the ring of sums $\sum_{i=0}^n z_i p^i$ with $0 \leq z_i < p$, and the quotient map $\alpha_n^{n+1} \colon \mathbb{Z}_{n+1} \to \mathbb{Z}_n$ is just truncation. Thus $\varprojlim \mathbb{Z}_n$ is just the ring of p-adic integers.

Proposition (22.7). — *Let $\alpha \colon M \to N$ be a map of filtered modules with filtrations $F^\bullet M$ and $F^\bullet N$, and $\alpha_n \colon M/F^n M \to N/F^n N$ the induced maps for $n \geq 0$. Then*

$$\widehat{M} = \varprojlim (M/F^n M) \quad \textit{and} \quad \widehat{\alpha} = \varprojlim \alpha_n.$$

Moreover, $\kappa_M \colon M \to \widehat{M}$ is induced by the quotient maps $M \to M/F^n M$.

Proof: Let's define an R-map $\gamma \colon C(M) \to \varprojlim (M/F^n M)$. Given $(m_\nu) \in C(M)$, let $q_n \in M/F^n M$ be the residue of m_ν for $\nu \gg 0$. Then q_n is independent of ν, because (m_ν) is Cauchy. Further, q_n is the residue of q_{n+1} in $M/F^n M$; so $(q_n) \in \varprojlim (M/F^n M)$. Define $\gamma(m_\nu) := (q_n)$. Plainly, γ is R-linear.

Above, it's easy to see that $(m_\nu) \in Z(M)$ if and only if $q_n = 0$ for all n. Hence γ factors through an injective R-map $\lambda \colon \widehat{M} \to \varprojlim (M/F^n M)$.

Next, given $(q_n) \in \varprojlim (M/F^n M)$, lift $q_\nu \in M/F^\nu M$ to some $m_\nu \in M$ for all ν. Then $m_\mu - m_\nu \in F^\nu M$ for $\mu \geq \nu$, as $q_\mu \in M/F^\mu M$ maps to $q_\nu \in M/F^\nu M$. Hence $(m_\nu) \in C(M)$. Thus γ is surjective. So λ is too. Thus λ is an isomorphism.

Next, $\widehat{\alpha} = \varprojlim \alpha_n$ as $\alpha_n(q_n)$ is the residue of $\alpha(m_\nu)$ in $N/F^n N$ for $\nu \gg 0$.

Moreover, given $m \in M$, assume $m_\nu = m$ for all ν. Then $q_n \in M/F^n M$ is the residue of m for all n. Thus $\kappa_M \colon M \to \widehat{M}$ is induced by the $M \to M/F^n M$. □

Exercise (22.8) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Use (22.7) to compute $\widehat{F^k M} \subset \widehat{M}$. Then use (22.3) to show $\widehat{M}$ is separated.

Exercise (22.9) . — Let $Q_0 \supset Q_1 \supset Q_2 \supset \cdots$ be a descending chain of modules, $\alpha_n^{n+1}\colon Q_{n+1} \hookrightarrow Q_n$ the inclusions. Show $\bigcap Q_n = \varprojlim Q_n$.

Lemma (22.10). — (1) *Let (M_n, μ_n^{n+1}) be an inverse system. Assume the μ_n^{n+1} are surjective for all n. Then $\varprojlim^1_n M_n = 0$.*

(2) *For $n \geq 0$, given commutative diagrams with exact rows*

$$\begin{array}{ccccccccc}
0 & \to & M_{n+1} & \xrightarrow{\alpha_{n+1}} & N_{n+1} & \xrightarrow{\beta_{n+1}} & P_{n+1} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_n & \xrightarrow{\alpha_n} & N_n & \xrightarrow{\beta_n} & P_n & \longrightarrow & 0
\end{array}$$

they induce the following exact sequence:

$$0 \to \varprojlim M_n \to \varprojlim N_n \to \varprojlim P_n \to \varprojlim{}^1 M_n \to \varprojlim{}^1 N_n \to \varprojlim{}^1 P_n \to 0.$$

Proof: In (1), the μ_n^{n+1} are surjective. So given $(m_n) \in \prod M_n$, we can solve $q_n - \mu_n^{n+1}(q_{n+1}) = m_n$ recursively, starting with $q_0 = 0$, to get $(q_n) \in \prod M_n$ with $\theta((q_n)) = (m_n)$, where θ is the map of (22.5). So θ is surjective. Thus (1) holds.

For (2), note that the given diagrams induce the next one:

$$\begin{array}{ccccccccc}
0 & \to & \prod M_n & \xrightarrow{\prod \alpha_n} & \prod N_n & \xrightarrow{\prod \beta_n} & \prod P_n & \to & 0 \\
 & & \theta\downarrow & & \theta\downarrow & & \theta\downarrow & & \\
0 & \to & \prod M_n & \xrightarrow{\prod \alpha_n} & \prod N_n & \xrightarrow{\prod \beta_n} & \prod P_n & \to & 0
\end{array}$$

Its rows are exact by (5.4). So the Snake Lemma (5.10) and (22.5.1) give (2). □

Example (22.11). — Let R be a ring, M a module, $F^\bullet M$ a filtration. For $n \geq 0$, consider the following natural commutative diagrams with exact rows:

$$\begin{array}{ccccccccc}
0 & \to & F^{n+1}M & \to & M & \to & M/F^{n+1}M & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & F^n M & \longrightarrow & M & \longrightarrow & M/F^n M & \longrightarrow & 0
\end{array}$$

with vertical maps, respectively, the inclusion, the identity, and the quotient map. By (22.9) and (22.7), the exact sequence of inverse limits in (22.10)(2) yields

$$0 \to \varprojlim F^n M \to M \xrightarrow{\kappa_M} \widehat{M}.$$

But κ_M is not always surjective; for examples, see (22.2). Thus $\varprojlim$ is not always exact, nor is $\varprojlim^1$ always 0.

Exercise (22.12) . — Let R be a ring, M a module, $F^\bullet M$ a filtration, and $N \subset M$ a submodule. Give N and M/N the induced filtrations: $F^n N := N \cap F^n M$ and $F^n(M/N) := F^n M / F^n N$. Show the following: (1) $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = \widehat{M/N}$.

(2) If $N \supset F^k M$ for some k, then $\kappa_{M/N}$ is a bijection, $\kappa_{M/N}\colon M/N \xrightarrow{\sim} \widehat{M/N}$.

Exercise (22.13) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Show:

(1) The canonical map $\kappa_M\colon M \to \widehat{M}$ is surjective if and only if M is complete.

(2) Given $(m_n) \in C(M)$, its residue $m \in \widehat{M}$ is the limit of the sequence $(\kappa_M m_n)$.

Exercise (22.14) . — Let R be a ring, M a module, and $F^\bullet M$ a filtration. Show that the following statements are equivalent: (1) κ_M is bijective;
(2) M is separated and complete; (3) κ_M is an isomorphism of filtered modules.

Assume M is Noetherian and $F^\bullet M$ is the $\mathfrak{a}$-adic filtration for a proper ideal $\mathfrak{a}$ with either (a) $\mathfrak{a} \subset \operatorname{rad}(M)$ or (b) R a domain and M torsionfree. Prove that M is complete if and only if $M = \widehat{M}$.

Exercise (22.15) . — Let R be a ring, $\alpha\colon M \to N$ a map of filtered modules, $\alpha'\colon \widehat{M} \to \widehat{N}$ a continuous map such that $\alpha'\kappa_M = \kappa_N\alpha$. Show $\alpha' = \widehat{\alpha}$.

Exercise (22.16) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Show:
(1) $G(\kappa_M)\colon G(M) \to G(\widehat{M})$ is bijective. (2) $\widehat{\kappa_M}\colon \widehat{M} \to \widehat{\widehat{M}}$ is bijective.
(3) $\kappa_{\widehat{M}} = \widehat{\kappa_M}$. (4) $\widehat{M}$ is separated and complete.

Lemma (22.17). — *Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module, N a submodule. Then the ($\mathfrak{a}$-adic) topology on M induces that on N.*

Proof: Set $F^nN := N \cap \mathfrak{a}^nM$. The F^nN form an $\mathfrak{a}$-stable filtration by the Artin–Rees Lemma (20.12). Thus by (22.1), it defines the $\mathfrak{a}$-adic topology. □

Theorem (22.18) (Exactness of Completion). — *Let R be a ring, $\mathfrak{a}$ an ideal. Then on the Noetherian modules M, the functor $M \mapsto \widehat{M}$ is exact.*

Proof: Let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of Noetherian modules. Then $0 \to \widehat{M'} \to \widehat{M} \to \widehat{M''} \to 0$ is exact by (22.12)(1) and (22.17). □

Corollary (22.19). — *Let R be a ring, $\mathfrak{a}$ an ideal, M a finitely generated module. Then the canonical map $\widehat{R} \otimes M \to \widehat{M}$ is surjective; it's bijective if R is Noetherian.*

Proof: On $((R\text{-mod}))$, the functor $N \mapsto \widehat{N}$ preserves surjections by (22.12)(1); on the Noetherian modules, it is exact by (22.18). But if R is Noetherian, then every finitely generated module is Noetherian and finitely presented by (16.15). Thus (8.14) yields both assertions. □

Corollary (22.20). — *Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, M a module. Use the $\mathfrak{a}$-adic topology. Assume either* (a) *M and $\mathfrak{b}M$ are finitely generated and $\mathfrak{b} \supset \mathfrak{a}$, or* (b) *$M$ is Noetherian. Then $\widehat{\mathfrak{b}^nM} = \mathfrak{b}^n\widehat{M} = \widehat{\mathfrak{b}^n}\widehat{M} = \widehat{\mathfrak{b}}^n\widehat{M}$ for any $n \geq 1$.*

Proof: To do $n = 1$, form the square induced by the inclusion $\mathfrak{b}M \to M$:

$$\begin{array}{ccc} \widehat{R} \otimes (\mathfrak{b}M) & \xrightarrow{\alpha} & \widehat{R} \otimes M \\ \Big\downarrow \beta & & \Big\downarrow \gamma \\ \widehat{\mathfrak{b}M} & \xrightarrow{\delta} & \widehat{M} \end{array}$$

It's commutative. Moreover, both β and γ are surjective by (22.19) as both $\mathfrak{b}M$ and M are finitely generated under either (a) or (b)

Plainly $\operatorname{Im}(\alpha) = \mathfrak{b}(\widehat{R} \otimes M)$. But γ is surjective. Thus $\operatorname{Im}(\gamma\alpha) = \mathfrak{b}\widehat{M}$.

At the bottom, δ is injective by (22.12)(1), as the topology on M induces that on $\mathfrak{b}M$ for these reasons. It does if (a) holds, namely if $\mathfrak{a} \subset \mathfrak{b} \subset R$, as then for any $k \geq 0$, multiplying by $\mathfrak{a}^kM$ yields $\mathfrak{a}^{k+1}M \subset \mathfrak{a}^k\mathfrak{b}M \subset \mathfrak{a}^kM$. And it does by (22.17) if (b) holds. Hence $\operatorname{Im}(\delta\beta) = \widehat{\mathfrak{b}M}$. But $\operatorname{Im}(\delta\beta) = \operatorname{Im}(\gamma\alpha)$. Thus $\widehat{\mathfrak{b}M} = \mathfrak{b}\widehat{M}$.

Plainly $\mathfrak{b}\widehat{M} \subset \widehat{\mathfrak{b}}\widehat{M}$. Also, $\widehat{\mathfrak{b}}\widehat{M} \subset \widehat{\mathfrak{b}M}$ as, given a Cauchy sequence in $\mathfrak{b}$ and one in M, their product is one in $\mathfrak{b}M$. But $\widehat{\mathfrak{b}M} = \mathfrak{b}\widehat{M}$. Thus the case $n = 1$ holds.

For $n \ge 2$, on any module, the $\mathfrak{a}^n$-adic topology is the same as the $\mathfrak{a}$-adic. So the case $n = 1$ applies with $\mathfrak{a}^n$ and $\mathfrak{b}^n$ for $\mathfrak{a}$ and $\mathfrak{b}$. Thus $\widehat{\mathfrak{b}^n M} = \mathfrak{b}^n\widehat{M} = \widehat{\mathfrak{b}}^n\widehat{M}$.

So it remains to show $\mathfrak{b}^n\widehat{M} = \widehat{\mathfrak{b}}^n\widehat{M}$. Induct on n. For $n = 1$, recall $\mathfrak{b}\widehat{M} = \widehat{\mathfrak{b}}\,\widehat{M}$.

Assume $\mathfrak{b}^{n-1}\widehat{M} = \widehat{\mathfrak{b}}^{n-1}\widehat{M}$ with $n \ge 2$. Multiplying by $\mathfrak{b}$ gives $\mathfrak{b}^n\widehat{M} = \widehat{\mathfrak{b}}^{n-1}\mathfrak{b}\widehat{M}$. But $\mathfrak{b}\widehat{M} = \widehat{\mathfrak{b}}\,\widehat{M}$. Thus $\mathfrak{b}^n\widehat{M} = \widehat{\mathfrak{b}}^n\widehat{M}$, as desired. □

Corollary (22.21). — *Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Assume M is Noetherian, or just M and $\mathfrak{a}M$ are finitely generated. Then these filtrations of $\widehat{M}$ coincide: the induced (for which $F^n\widehat{M} := \widehat{\mathfrak{a}^n M}$), the $\widehat{\mathfrak{a}}$-adic, and the $\mathfrak{a}$-adic.*

Proof: The assertion is an immediate consequence of (22.20) with $\mathfrak{b} := \mathfrak{a}$. □

Corollary (22.22). — *Let R be a Noetherian ring, $\mathfrak{a}$ an ideal, and M a finitely generated module. Assume M is flat. Then $\widehat{M}$ is flat both over $\widehat{R}$ and over R.*

Proof: First, $\widehat{M}$ is flat over $\widehat{R}$ by (9.22) as $\widehat{M} = M \otimes_R \widehat{R}$ by (22.19).

Second, fix an ideal $\mathfrak{b}$. Note $\mathfrak{b}\widehat{M} = \widehat{\mathfrak{b}M}$ by (22.20). And $\widehat{\mathfrak{b}M} = \widehat{R} \otimes \mathfrak{b}M$ by (22.19). But M is flat; so $\mathfrak{b}M = \mathfrak{b} \otimes M$ by (9.15). Thus $\mathfrak{b}\widehat{M} = \widehat{R} \otimes \mathfrak{b} \otimes M$. But $\widehat{R} \otimes M = \widehat{M}$ by (22.19). Thus $\mathfrak{b}\widehat{M} = \mathfrak{b} \otimes \widehat{M}$. So $\widehat{M}$ is flat over R by (9.15). □

Lemma (22.23). — *Let R be a ring, $\alpha\colon M \to N$ a map of filtered modules with filtrations $F^\bullet M$ and $F^\bullet N$.*

(1) *Assume $F^n M = M$ for $n \ll 0$ and $G(\alpha)$ is injective. Then $\widehat{\alpha}$ is injective.*
(2) *Assume $F^n N = N$ for $n \ll 0$ and $G(\alpha)$ is surjective. Then $\widehat{\alpha}$ is surjective.*

Proof: Given $n \in \mathbb{Z}$, form the following commutative diagram:

$$\begin{CD}
0 @>>> F^nM/F^{n+1}M @>>> M/F^{n+1}M @>>> M/F^nM @>>> 0\\
@. @VV{G_n(\alpha)}V @VV{\alpha_{n+1}}V @VV{\alpha_n}V\\
0 @>>> F^nN/F^{n+1}N @>>> N/F^{n+1}N @>>> N/F^nN @>>> 0
\end{CD}$$

Its rows are exact. So the Snake Lemma (5.10) yields this exact sequence:

$$\operatorname{Ker} G_n(\alpha) \to \operatorname{Ker}\alpha_{n+1} \xrightarrow{\beta_n} \operatorname{Ker}\alpha_n \to \operatorname{Coker} G_n(\alpha) \to \operatorname{Coker}\alpha_{n+1} \xrightarrow{\gamma_n} \operatorname{Coker}\alpha_n.$$

In (1), $\operatorname{Ker} G_n(\alpha) = 0$ for all n; so β_n is injective for all n. Also $M/F^nM = 0$ for $n \ll 0$; so $\operatorname{Ker}\alpha_n = 0$ for $n \ll 0$. Hence by induction, $\operatorname{Ker}\alpha_n = 0$ for all n. So $\varprojlim \alpha_n$ is injective by (22.10)(2). Thus (22.7) yields (1).

In (2), note $\operatorname{Coker} G_n(\alpha) = 0$ for all n. So β_n is surjective for all n. Thus (22.10)(1) yields $\varprojlim^1 \operatorname{Ker}\alpha_n = 0$.

Again, $\operatorname{Coker} G_n(\alpha) = 0$ for all n. So γ_n is injective for all n. Also $N/F^nN = 0$ for $n \ll 0$; so $\operatorname{Coker}\alpha_n = 0$ for $n \ll 0$. So by induction, $\operatorname{Coker}\alpha_n = 0$ for all n. So α_n is surjective for all n. So for all n, the following sequence is exact:

$$0 \to \operatorname{Ker}\alpha_n \to M/F^nM \xrightarrow{\alpha_n} N/F^nN \to 0$$

So $\varprojlim \alpha_n$ is surjective by (22.10)(2). Thus (22.7) yields (2). □

Lemma (22.24). — *Let R be a ring, $\mathfrak{a}$ an ideal, M a module, $F^\bullet M$ an $\mathfrak{a}$-filtration. Assume R is complete, M is separated, $F^nM = M$ for $n \ll 0$, and $G(M)$ is finitely generated over $G(R)$. Then M is complete, and finitely generated over R.*

Proof: Take finitely many generators μ_i of $G(M)$, and replace them by their homogeneous components. Set $n_i := \deg(\mu_i)$. Lift μ_i to $m_i \in F^{n_i}M$.

Filter R $\mathfrak{a}$-adically. Set $E := \bigoplus_i R[-n_i]$. Filter E with $F^nE := \bigoplus_i F^n(R[-n_i])$. Then $F^nE = E$ for $n \ll 0$. Define $\alpha\colon E \to M$ by sending $1 \in R[-n_i]$ to $m_i \in M$. Then $\alpha F^nE \subset F^nM$ for all n. Also, $G(\alpha)\colon G(E) \to G(M)$ is surjective as the μ_i generate. Thus $\widehat{\alpha}$ is surjective by **(22.23)**.

Form the following canonical commutative diagram:

$$\begin{tikzcd} E \arrow[r, "\kappa_E"] \arrow[d, "\alpha"'] & \widehat{E} \arrow[d, "\widehat{\alpha}"'] \\ M \arrow[r, "\kappa_M"] & \widehat{M} \end{tikzcd}$$

Plainly, $\kappa_E = \bigoplus_i \kappa_{R[-n_i]}$. But κ_R is surjective by **(22.13)**(1), as R is complete. Hence κ_E is surjective. So $\widehat{\alpha}\circ\kappa_E$ is surjective. So κ_M is surjective. Thus **(22.13)**(1) implies M is complete.

By hypothesis, M is separated. So κ_M is injective by **(22.3)**. Hence κ_M is bijective. So α is surjective. Thus M is finitely generated. □

Proposition (22.25). — *Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Assume R is complete, and M separated. Assume $G(M)$ is a Noetherian $G(R)$-module. Then M is Noetherian over R, and every submodule N is complete.*

Proof: Let $F^\bullet M$ denote the $\mathfrak{a}$-adic filtration, and $F^\bullet N$ the induced filtration: $F^nN := N \cap F^nM$. Then N is separated, and $F^nN = N$ for $n \ll 0$. Further, $G(N) \subset G(M)$. However, $G(M)$ is Noetherian. So $G(N)$ is finitely generated. Thus N is complete and finitely generated over R by **(22.24)**. Thus M is Noetherian. □

Theorem (22.26). — *Let R be a ring, $\mathfrak{a}$ an ideal, and M a Noetherian module. Then $\widehat{M}$ is Noetherian over $\widehat{R}$, and every $\widehat{R}$-submodule is complete.*

Proof: Set $R' := R/\operatorname{Ann}(M)$ and $\mathfrak{a}' := \mathfrak{a}R'$. Then R' is Noetherian by **(16.16)**. Also, ${\mathfrak{a}'}^r = \mathfrak{a}^rR'$ and ${\mathfrak{a}'}^rM = \mathfrak{a}^rM$ for all $r \geq 0$. So the ($\mathfrak{a}$-adic) topology on R' and on M is equal to the $\mathfrak{a}'$-adic topology. Also, $\widehat{R'}$ is a quotient of $\widehat{R}$ by **(22.12)**(1). Hence, the $\widehat{R}$-submodules of $\widehat{M}$ are the same as the $\widehat{R'}$-submodules; morevoer, each one is finitely generated or complete as an $\widehat{R}$-module if and only if it's so as an $\widehat{R'}$-module. Thus we may replace R by R', and thus assume R is Noetherian.

Since M is Noetherian and its $\mathfrak{a}$-adic filtration is (trivially) stable, $G(M)$ is a finitely generated $G(R)$-module owing to **(20.8)**. But R is Noetherian. So $\mathfrak{a}$ is finitely generated. So $G(R)$ is algebra finite over $R/\mathfrak{a}$ by **(20.7)**. But $R/\mathfrak{a}$ is Noetherian as R is. So $G(R)$ is Noetherian by the Hilbert Basis Theorem, **(16.10)**. But $G(R) = G(\widehat{R})$ and $G(M) = G(\widehat{M})$ owing to **(22.16)**(1) and **(22.17)**. So $G(\widehat{M})$ is a Noetherian $G(\widehat{R})$-module. But $\widehat{R}$ is complete and $\widehat{M}$ is separated by **(22.16)**(4). Thus **(22.25)** now yields both assertions. □

Example (22.27). — Let k be a Noetherian ring, $P := k[X_1, \ldots, X_r]$ the polynomial ring, and $A := k[[X_1, \ldots, X_r]]$ the formal power series ring. Then A is the completion of P in the $\langle X_1, \ldots, X_r\rangle$-adic topology by **(22.2)**. Further, P is Noetherian by the Hilbert Basis Theorem, **(16.10)**. Thus A *is Noetherian* by **(22.26)**.

Assume k is a domain. Then A is a domain. Indeed, A is one if $r = 1$, because

$$(a_mX_1^m + \cdots)(b_nX_1^n + \cdots) = a_mb_nX_1^{m+n} + \cdots .$$

If $r > 1$, then $A = k[[X_1, \ldots, X_i]]\,[[X_{i+1}, \ldots, X_r]]$; so A is a domain by induction.

Set $\mathfrak{p}_i := \langle X_{i+1}, \ldots, X_r\rangle$. Then $A/\mathfrak{p}_i = k[[X_1, \ldots, X_i]]$ by **(3.7)**. Hence $\mathfrak{p}_i$ is prime. So $0 = \mathfrak{p}_r \subsetneqq \cdots \subsetneqq \mathfrak{p}_0$ is a chain of primes of length r. Thus $\dim A \ge r$.

Assume k is a field. Then A is local with maximal ideal $\langle X_1, \ldots, X_r\rangle$ and residue field k by **(3.7)**. So $\dim A \le r$ by **(21.13)**. Thus $\dim A = r$, and so A *is regular* r.

B. Exercises

Exercise (22.28) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable. Filter $R[[X]]$ with the ideals $\mathfrak{b}_n$ consisting of the $H =: \sum h_i X^i$ with $h_i \in \mathfrak{a}^n$ for all i. Show: (1) that $\widehat{R}[[X]] = R[[X]]\widehat{\ }$ and (2) that if R is separated and complete, then so is $R[[X]]$.

Exercise (22.29) . — In $\widehat{\mathbb{Z}}_2$, evaluate the sum $s := 1 + 2 + 4 + 8 + \cdots$.

Exercise (22.30) . — Let R be a ring, $\alpha_n^{n+1}\colon Q_{n+1} \to Q_n$ linear maps for $n \ge 0$. Set $\alpha_n^m := \alpha_n^{n+1} \cdots \alpha_{m-1}^m$ for $m > n$ and $\alpha_n^n = 1$. Assume the **Mittag-Leffler Condition**: for all $n \ge 0$, there's $m \ge n$ such that

$$Q_n \supset \alpha_n^{n+1} Q_{n+1} \supset \cdots \supset \alpha_n^m Q_m = \alpha_n^{m+1} Q_{m+1} = \cdots.$$

Set $P_n := \bigcap_{m \ge n} \alpha_n^m Q_m$, and prove $\alpha_n^{n+1} P_{n+1} = P_n$. Conclude that $\varprojlim^1 Q_n = 0$.

Exercise (22.31) . — Let R be a ring, and $\mathfrak{a}$ an ideal. Set $S := 1 + \mathfrak{a}$ and set $T := \kappa_R^{-1}(\widehat{R}^\times)$. Given $t \in R$, let $t_n \in R/\mathfrak{a}^n$ be its residue for all n. Show:

(1) Given $t \in R$, then $t \in T$ if and only if $t_n \in (R/\mathfrak{a}^n)^\times$ for all n.
(2) Then $T = \{t \in R \mid t$ lies in no maximal ideal containing $\mathfrak{a}\}$.
(3) Then $S \subset T$, and $\widehat{R}$ is the completion of $S^{-1}R$ and of $T^{-1}R$.
(4) Assume $\kappa_R\colon R \to \widehat{R}$ is injective. Then $\kappa_{S^{-1}R}$ and $\kappa_{T^{-1}R}$ are too.
(5) Assume $\mathfrak{a}$ is a maximal ideal $\mathfrak{m}$. Then $\widehat{R} = \widehat{R_\mathfrak{m}}$.

Exercise (22.32) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a finitely generated module. Show $\widehat{R} \cdot \kappa_M(M) = \widehat{M}$.

Exercise (22.33) . — Let R be a ring, M a module, $F^\bullet M$ a filtration, and N a submodule. Give N the induced filtration: $F^n N := N \cap F^n M$ for all n. Show:

(1) $\widehat{N}$ is the closure of $\kappa_M N$ in $\widehat{M}$. (2) $\kappa_M^{-1}\widehat{N}$ is the closure of N in M.

Exercise (22.34) . — Let R be a ring, $\mathfrak{a}$ an ideal. Show that every closed maximal ideal $\mathfrak{m}$ contains $\mathfrak{a}$.

Exercise (22.35) . — Let R be a ring, $\mathfrak{a}$ an ideal. Show equivalent:

(1) $\mathfrak{a} \subset \operatorname{rad}(R)$. (2) Every element of $1 + \mathfrak{a}$ is invertible.
(3) Given any finitely generated R-module M, if $M = \mathfrak{a}M$, then $M = 0$.
(4) Every maximal ideal $\mathfrak{m}$ is closed.

Show, moreover, that (1)–(4) hold if R is separated and complete.

Exercise (22.36) . — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Show equivalent:

(1) R is a **Zariski ring**; that is, R is Noetherian, and $\mathfrak{a} \subset \operatorname{rad}(R)$.
(2) Every finitely generated module M is separated.
(3) Every submodule N of every finitely generated module M is closed.
(4) Every ideal $\mathfrak{b}$ is closed. (5) Every maximal ideal $\mathfrak{m}$ is closed.
(6) Every faithfully flat, finitely generated module M has a faithfully R-flat $\widehat{M}$.

(7) The completion $\widehat{R}$ is faithfully R-flat.

Exercise (22.37) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module. Prove:

(1) $\bigcap_{n=1}^{\infty} \mathfrak{a}^n M = \bigcap_{\mathfrak{m}\in\Psi} \operatorname{Ker}(M \xrightarrow{\varphi_{\mathfrak{m}}} M_{\mathfrak{m}})$ where $\Psi := \{\, \mathfrak{m} \supset \mathfrak{a} \mid \mathfrak{m} \text{ maximal} \,\}$.

(2) $\widehat{M} = 0$ if and only if $\operatorname{Supp}(M) \cap \mathbf{V}(\mathfrak{a}) = \emptyset$.

Exercise (22.38) . — Let R be a ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ maximal ideals, and M module. Set $\mathfrak{m} := \bigcap \mathfrak{m}_i$, and give M the $\mathfrak{m}$-adic topology. Show $\widehat{M} = \prod \widehat{M}_{\mathfrak{m}_i}$.

Exercise (22.39) . — (1) Let R be a ring, $\mathfrak{a}$ an ideal. If $G_{\mathfrak{a}}(R)$ is a domain, show $\widehat{R}$ is a domain. If also $\bigcap_{n\ge 0} \mathfrak{a}^n = 0$, show R is a domain.

(2) Use (1) to give an alternative proof that a regular local ring A is a domain.

Exercise (22.40) . — (1) Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Assume that $G_{\mathfrak{a}}(R)$ is a normal domain and that $\bigcap_{n\ge 0}(sR + \mathfrak{a}^n) = sR$ for any $s \in R$. Show using induction on n and applying **(16.40)** that R is a normal domain.

(2) Use (1) to prove a regular local ring A is normal.

Exercise (22.41) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module with $\ell_R(M) < \infty$.

(1) Assume M is simple. Show $\widehat{M}$ is simple if $\mathfrak{a} \subset \operatorname{Ann}(M)$, but $\widehat{M} = 0$ if not.

(2) Show $\ell_{\widehat{R}}(\widehat{M}\,) \le \ell_R(M)$, with equality if and only if $\mathfrak{a} \subset \operatorname{rad}(M)$.

Exercise (22.42) . — Let R be a ring, M a module with two filtrations $F^\bullet M$ and $G^\bullet M$. For all m, give $G^m M$ the filtration induced by $F^\bullet M$, and let $(G^m M)^F$ be its completion; filter M^F by the $(G^m M)^F$, and let $(M^F)^G$ be the completion. Define $H^\bullet M$ by $H^p M := F^p M + G^p M$, and let M^H be the completion. Show:

$$(M^F)^G = \varprojlim_m \varprojlim_n M/(F^n M + G^m M) = M^H. \qquad \textbf{(22.42.1)}$$

Exercise (22.43) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Given any module M, let $M^{\mathfrak{a}}$ be its $\mathfrak{a}$-adic completion. Set $\mathfrak{c} := \mathfrak{a} + \mathfrak{b}$. Assume M is Noetherian. Show:

(1) Then $(M^{\mathfrak{a}})^{\mathfrak{b}} = M^{\mathfrak{c}}$. (2) Assume $\mathfrak{a} \supset \mathfrak{b}$ and $M^{\mathfrak{a}} = M$. Then $M^{\mathfrak{b}} = M$

Exercise (22.44) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, F_n, $G \in R[[X]]$ for $n \ge 0$. In $R[[X]]$, set $\mathfrak{b} := \langle \mathfrak{a}, X \rangle$. Show the following:

(1) Then $\mathfrak{b}^m$ consists of all $H =: \sum h_i X^i$ with $h_i \in \mathfrak{a}^{m-i}$ for all $i < m$.
(2) Say $F_n =: \sum f_{n,i} X^i$. Then (F_n) is Cauchy if and only if every $(f_{n,i})$ is.
(3) Say $G =: \sum g_i X^i$. Then $G = \lim F_n$ if and only if $g_i = \lim f_{n,i}$ for all i.
(4) If R is separated or complete, then so is $R[[X]]$.
(5) The $\langle \mathfrak{a}, X\rangle$-adic completion of $R[X]$ is $\widehat{R}[[X]]$.

Exercise (22.45) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module, $x \in R$. Prove: if $x \notin \operatorname{z.div}(M)$, then $x \notin \operatorname{z.div}(\widehat{M})$; and the converse holds if $\mathfrak{a} \subset \operatorname{rad}(M)$.

Exercise (22.46) . — Let k be a field with $\operatorname{char}(k) \ne 2$, and X, Y variables. Set $P := k[X, Y]$ and $R := P/\langle Y^2 - X^2 - X^3 \rangle$. Let x, y be the residues of X, Y, and set $\mathfrak{m} := \langle x, y \rangle$. Prove R is a domain, but its completion $\widehat{R}$ with respect to $\mathfrak{m}$ isn't.

Exercise (22.47) . — Given modules $M_1, M_2, \ldots$, set $P_k := \prod_{n=1}^{k} M_n$, and let $\pi_k^{k+1} \colon P_{k+1} \to P_k$ be the projections. Show $\varprojlim_{k\ge 1} P_k = \prod_{n=1}^{\infty} M_n$.

Exercise (22.48) . — Let $p \in \mathbb{Z}$ be prime. For $n > 0$, define a $\mathbb{Z}$-linear map
$$\alpha_n \colon \mathbb{Z}/\langle p\rangle \to \mathbb{Z}/\langle p^n\rangle \quad\text{by}\quad \alpha_n(1) = p^{n-1}.$$
Set $A := \bigoplus_{n\ge1} \mathbb{Z}/\langle p\rangle$ and $B := \bigoplus_{n\ge1} \mathbb{Z}/\langle p^n\rangle$. Set $\alpha := \bigoplus \alpha_n$; so $\alpha\colon A \to B$.

(1) Show that α is injective and that the p-adic completion $\widehat{A}$ is just A.

(2) Show that, in the topology on A induced by the p-adic topology on B, the completion $\overline{A}$ is equal to $\prod_{n=1}^{\infty} \mathbb{Z}/\langle p\rangle$.

(3) Show that the natural sequence of p-adic completions
$$\widehat{A} \xrightarrow{\widehat{\alpha}} \widehat{B} \xrightarrow{\widehat{\beta}} (B/A)\widehat{\ }$$
is not exact at $\widehat{B}$. (Thus p-adic completion is *neither* left exact *nor* right exact.)

Exercise (22.49) . — Preserve the setup of (22.48). Set $A_k := \alpha^{-1}(p^k B)$ and $P := \prod_{k=1}^{\infty} \mathbb{Z}/\langle p\rangle$. Show $\varprojlim^1_{k\ge1} A_k = P/A$, and conclude $\varprojlim$ is not right exact.

Exercise (22.50) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Show that $\operatorname{Ann}_R(M)\widehat{R} \subset \operatorname{Ann}_{\widehat{R}}(\widehat{M})$, with equality if R is Noetherian and if M is finitely generated.

Exercise (22.51) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Assume $\mathfrak{a}M = 0$. Set $\mathfrak{b} := \operatorname{Ann}_R(M)$. Show $\widehat{\mathfrak{b}} = \operatorname{Ann}_{\widehat{R}}(\widehat{M})$.

Exercise (22.52) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M, N, P modules. Assume $\mathfrak{a}M \subset P \subset N \subset M$. Prove:

(1) The ($\mathfrak{a}$-adic) topology on M induces that on N.

(2) Then $(\mathfrak{a}M)\widehat{\ } \subset \widehat{P} \subset \widehat{N} \subset \widehat{M}$, and $N/P = \widehat{N}/\widehat{P}$.

(3) The map $Q \mapsto \widehat{Q}$ is a bijection from the R-submodules Q with $P \subset Q \subset N$ to the $\widehat{R}$-submodules Q' with $\widehat{P} \subset Q' \subset \widehat{N}$. Its inverse is $Q' \mapsto \kappa_M^{-1}(Q')$.

Exercise (22.53) . — Let R be a ring, $\mathfrak{a} \subset \mathfrak{b}$ ideals, and M a finitely generated module. Let Φ be the set of maximal ideals $\mathfrak{m} \in \operatorname{Supp}(M)$ with $\mathfrak{m} \supset \mathfrak{a}$. Use the $\mathfrak{a}$-adic topology. Prove:

(1) Then $\widehat{M}$ is a finitely generated $\widehat{R}$-module, and $\widehat{\mathfrak{b}}\widehat{M} = \widehat{\mathfrak{b}M} \subset \widehat{M}$.

(2) The map $\mathfrak{p} \mapsto \widehat{\mathfrak{p}}$ is a bijection $\operatorname{Supp}(M/\mathfrak{b}M) \xrightarrow{\sim} \operatorname{Supp}(\widehat{M}/\widehat{\mathfrak{b}}\widehat{M})$. Its inverse is $\mathfrak{p}' \mapsto \kappa_R^{-1}\mathfrak{p}'$. It restricts to a bijection on the subsets of maximal ideals.

(3) Then $\operatorname{Supp}(\widehat{M}/\widehat{\mathfrak{a}}\widehat{M})$ and $\operatorname{Supp}(\widehat{M})$ have the same maximal ideals.

(4) Then the $\widehat{\mathfrak{m}}$ with $\mathfrak{m} \in \Phi$ are precisely the maximal ideals of $\widehat{R}$ in $\operatorname{Supp}(\widehat{M})$.

(5) Then $\kappa_R^{-1}\operatorname{rad}(\widehat{M}) = \bigcap_{\mathfrak{m}\in\Phi} \mathfrak{m}$ and $\operatorname{rad}(\widehat{M}) = \big(\bigcap_{\mathfrak{m}\in\Phi} \mathfrak{m}\big)\widehat{\ }$.

(6) Then Φ is finite if and only if $\widehat{M}$ is semilocal.

(7) If $M = R$, then $\Phi = \{\mathfrak{b}\}$ if and only if $\widehat{R}$ is local with maximal ideal $\widehat{\mathfrak{b}}$.

Exercise (22.54) (*UMP of completion*) . — (1) Let R be a ring, M a filtered module. Show $\kappa_M \colon M \to \widehat{M}$ is the universal example of a map of filtered modules $\alpha\colon M \to N$ with N separated and complete. (2) Let R be a filtered ring. Show κ_R is the universal filtered ring map $\varphi\colon R \to R'$ with R' separated and complete.

Exercise (22.55) (*UMP of formal power series*) . — Let R be a ring, R' an algebra, $\mathfrak{b}$ an ideal of R', and $x_1, \dots, x_n \in \mathfrak{b}$. Let $A := R[[X_1, \dots, X_n]]$ be the formal power series ring. Assume R' is separated and complete in the $\mathfrak{b}$-adic topology. Show there's a unique map of R-algebras $\varphi\colon A \to R'$ with $\varphi(X_i) = x_i$ for all i, and φ is surjective if the induced map $R \to R'/\mathfrak{b}$ is surjective and the x_i generate $\mathfrak{b}$.

Exercise (22.56) . — Let R be a ring, $\mathfrak{a}$ a finitely generated ideal, $X_1, \ldots, X_n$ variables. Set $P := R[[X_1, \ldots, X_n]]$. Prove $P/\mathfrak{a}P = (R/\mathfrak{a})[[X_1, \ldots, X_n]]$. (But, it's not always true that $R' \otimes_R P = R'[[X_1, \ldots, X_n]]$ for an R-algebra R'; see (8.18).)

Exercise (22.57) (*Cohen Structure Theorem I***) .** — Let $A \to B$ be a local homomorphism, $\mathfrak{b} \subset B$ an ideal. Assume that $A = B/\mathfrak{b}$ and that B is separated and complete in the $\mathfrak{b}$-adic topology. Prove the following statements:

(1) The hypotheses hold if B is a complete Noetherian local ring, $\mathfrak{b}$ is its maximal ideal, and A is a coefficient field.
(2) Then $B \simeq A[[X_1, \ldots, X_r]]/\mathfrak{a}$ for some r, variables X_i, and some ideal $\mathfrak{a}$.

Exercise (22.58) (*Cohen Structure Theorem II***) .** — Let $A \to B$ be a flat local homomorphism of complete Noetherian local rings, and $\mathfrak{b} \subset B$ an ideal. Denote the maximal ideal of A by $\mathfrak{m}$, and set $B' := B/\mathfrak{m}B$. Assume that $A \xrightarrow{\sim} B/\mathfrak{b}$ and that B' is regular of dimension r. Find an A-isomorphism $\psi\colon B \xrightarrow{\sim} A[[X_1, \ldots, X_r]]$ for variables X_i with $\psi(\mathfrak{b}) = \langle X_1, \ldots, X_r \rangle$. In fact, if $\mathfrak{b} = \langle x_1, \ldots, x_r \rangle$ for given x_i, find such a ψ with $\psi(x_i) = X_i$.

Exercise (22.59) . — Let k be a field, $A := k[[X_1, \ldots, X_n]]$ the power series ring in variables X_i with $n \geq 1$, and $F \in A$ nonzero. Find an algebra automorphism φ of A such that $\varphi(F)$ contains the monomial X_n^s for some $s \geq 0$; do so as follows. First, find suitable $m_i \geq 1$ and use (22.55) to define φ by

$$\varphi(X_i) := X_i + X_n^{m_i} \text{ for } 1 \leq i \leq n-1 \text{ and } \varphi(X_n) := X_n. \qquad \textbf{(22.59.1)}$$

Second, if k is infinite, find suitable $a_i \in k^\times$ and use (22.55) to define φ by

$$\varphi(X_i) := X_i + a_i X_n \text{ for } 1 \leq i \leq n-1 \text{ and } \varphi(X_n) := X_n. \qquad \textbf{(22.59.2)}$$

Exercise (22.60) . — Let A be a complete Noetherian local ring, k a coefficient field, $x_1, \ldots, x_s$ a sop, $X_1, \ldots, X_s$ variables. Set $B := k[[X_1, \ldots, X_s]]$. Find an injective map $\varphi\colon B \to A$ such that $\varphi(X_i) = x_i$ and A is B-module finite.

Exercise (22.61) . — Let R be a ring, M a nonzero Noetherian module, and $\mathfrak{q}$ a parameter ideal of M. Show: (1) $\widehat{M}$ is a nonzero Noetherian $\widehat{R}$-module, and $\widehat{\mathfrak{q}}$ is a parameter ideal of $\widehat{M}$; and (2) $e(\mathfrak{q}, M) = e(\widehat{\mathfrak{q}}, \widehat{M})$ and $\dim(M) = \dim(\widehat{M}\,)$.

Exercise (22.62) . — Let A be a Noetherian local ring, $\mathfrak{m}$ the maximal ideal, k the residue field. Show: (1) $\widehat{A}$ is a Noetherian local ring with $\widehat{\mathfrak{m}}$ as maximal ideal and k as residue field; and (2) A is regular of dimension r if and only if $\widehat{A}$ is so.

Exercise (22.63) . — Let A be a Noetherian local ring, $k \subset A$ a coefficient field. Show A is regular if and only if, given any surjective k-map of finite-dimensional local k-algebras $B \twoheadrightarrow C$, every local k-map $A \to C$ lifts to a local k-map $A \to B$.

Exercise (22.64) . — Let k be a field, $\varphi\colon B \to A$ a local homomorphism of Noetherian local k-algebras, and $\mathfrak{n}$, $\mathfrak{m}$ the maximal ideals. Assume $k = A/\mathfrak{m} = B/\mathfrak{n}$, the induced map $\varphi'\colon \mathfrak{n}/\mathfrak{n}^2 \to \mathfrak{m}/\mathfrak{m}^2$ is injective, and A is regular. Show B is regular.

Exercise (22.65) . — Let R be a Noetherian ring, and $X_1, \ldots, X_n$ variables. Show that $R[[X_1, \ldots, X_n]]$ is faithfully flat.

Exercise (22.66) (*Gabber–Ramero* [8, Lem. 7.1.6]**) .** — Let R be a ring, $\mathfrak{a}$ an ideal, N a module. Assume N is flat. Prove the following:

(1) The functor $M \mapsto (M \otimes N)\widehat{\ }$ is exact on the Noetherian modules M.
(2) Assume R is Noetherian. Then for all finitely generated modules M, there's a canonical isomorphism $M \otimes \widehat{N} \xrightarrow{\sim} (M \otimes N)\widehat{\ }$, and $\widehat{N}$ is flat over R.

Exercise (22.67) . — Let P be the polynomial ring over $\mathbb{C}$ in variables $X_1, \dots, X_n$, and A its localization at $\langle X_1, \dots, X_n \rangle$. Let C be the ring of all formal power series in $X_1, \dots, X_n$, and B its subring of series converging about the origin in $\mathbb{C}^n$. Assume basic Complex Analysis (see [**7**, pp. 105–9]). Show B is local, and its maximal ideal is generated by $X_1, \dots, X_n$. Show $P \subset A \subset B \subset C$, and $\widehat{P} = \widehat{A} = \widehat{B} = C$. Show C is faithfully flat over both A and B, and B is faithfully flat over A.

Exercise (22.68) . — Let R be a Noetherian ring, and $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Assume $\mathfrak{a} \subset \operatorname{rad}(R)$, and use the $\mathfrak{a}$-adic topology. Prove $\mathfrak{b}$ is principal if $\mathfrak{b}\widehat{R}$ is.

Exercise (22.69) (*Nakayama's Lemma for adically complete rings*) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Assume R is complete, and M separated. Show $m_1, \dots, m_n \in M$ generate assuming their images $m'_1, \dots, m'_n$ in $M/\mathfrak{a}M$ generate.

Exercise (22.70) . — Let $A \to B$ be a local homomorphism of Noetherian local rings, $\mathfrak{m}$ the maximal ideal of A. Assume B is **quasi-finite** over A; that is, $B/\mathfrak{m}B$ is a finite-dimensional $A/\mathfrak{m}$-vector space. Show that $\widehat{B}$ is module finite over $\widehat{A}$.

Exercise (22.71) . — Let A be the non-Noetherian local ring of (**18.24**). Using E. Borel's theorem that every formal power series in x is the Taylor expansion of some C^∞-function (see [**13**, Ex. 5, p. 244]), show $\widehat{A} = \mathbb{R}[[x]]$, and $\widehat{A}$ is Noetherian; moreover, show $\widehat{A}$ is a quotient of A (so module finite).

Exercise (22.72) . — Let R be a ring, $\mathfrak{q}$ an ideal, M a module. Prove that, if M is free, then $M/\mathfrak{q}M$ is free over $R/\mathfrak{q}$ and multiplication of $G_\mathfrak{q}(R)$ on $G_\mathfrak{q}(M)$ induces an isomorphism $\sigma_M \colon G_\mathfrak{q}(R) \otimes_{R/\mathfrak{q}} M/\mathfrak{q}M \xrightarrow{\sim} G_\mathfrak{q}(M)$. Prove the converse holds if either (a) $\mathfrak{q}$ is nilpotent, or (b) M is Noetherian, and $\mathfrak{q} \subset \operatorname{rad}(M)$.

C. Appendix: Henselian Rings

(22.73) (Henselian pairs and Rings). — Let R be a ring, $\mathfrak{a}$ an ideal. We call the pair $(R, \mathfrak{a})$ **Henselian** if $\mathfrak{a} \subset \operatorname{rad}(R)$ and if, given any variable X and any monic polynomial $F \in R[X]$ whose residue $\overline{F} \in (R/\mathfrak{a})[X]$ factors as $\overline{F} = \widetilde{G}\widetilde{H}$ with $\widetilde{G}$ and $\widetilde{H}$ monic and coprime, then F itself factors as $F = GH$ where G and H are monic with residues $\widetilde{G}, \widetilde{H} \in (R/\mathfrak{a})[X]$.

Note that G and H too are coprime by (**10.33**)(2).

The factorization $F = GH$ is unique: given $F = G'H'$ where G' and H' are monic with residues $\widetilde{G}$ and $\widetilde{H}$, then $G = G'$ and $H = H'$. Indeed, G and H' are coprime by (**10.33**)(2). So there are $A, B \in R[X]$ with $AG + BH' = 1$. Then

$$G' = AGG' + BH'G' = AGG' + BGH = (AG' + BH)G.$$

But G and G' are monic of degree $\deg(\widetilde{G})$. Thus $G = G'$. So $GH = GH'$. So $G(H - H') = 0$. As G is monic, $H = H'$.

For future application, note that, even if we don't require F and H to be monic, the preceding argument establishes the uniqueness of the factorization $F = GH$.

If $(R, \mathfrak{a})$ is Henselian, then so is $(R/\mathfrak{b}\,, \mathfrak{a}/\mathfrak{b})$ for any ideal $\mathfrak{b} \subset \mathfrak{a}$.

We call a local ring A with maximal ideal $\mathfrak{m}$ **Henselian** if $(A, \mathfrak{m})$ is Henselian.

Example (22.74) (Some Henselian Rings). — (1) Any field is Henselian.

(2) Any separated and complete local ring is Henselian by **(22.75)** just below.

(3) Let A be the localization of $\mathbb{Z}$ at $\langle p\rangle$. Set $F := X(X-1)+p \in A[X]$. Then $\overline{F} = X(X-1)$ in $(A/\langle p\rangle A)[X]$ with X and $X-1$ coprime and monic. But plainly F does not factor in $A[X]$. Thus A is not Henselian.

Theorem (22.75) (Hensel's Lemma). — *Let R be a ring, $\mathfrak{a}$ an ideal. Assume R is separated and complete (in the $\mathfrak{a}$-adic topology). Then $(R,\mathfrak{a})$ is Henselian.*

In fact, given any variable X and any $F \in R[X]$ whose image $\overline{F} \in (R/\mathfrak{a})[X]$ factors as $\overline{F} = \widetilde{G}\widetilde{H}$ where $\widetilde{G}$ is monic and $\widetilde{G}$ and $\widetilde{H}$ are coprime, then $F = GH$ uniquely where G is monic and G and H are coprime with residues $\widetilde{G}$ and $\widetilde{H}$.

Proof: As R is separated and complete, **(22.35)** yields $\mathfrak{a} \subset \operatorname{rad}(R)$.

Set $P := R[X]$. Lift $\widetilde{G}$, $\widetilde{H}$ to some G_0, $H_0 \in P$ with G_0 monic. By **(10.33)**(2), G_0 and H_0 are relatively prime. Set $n := \deg G_0$ and $m := \max\{\deg H_0, \deg F - n\}$.

Starting with G_0, H_0, by induction let's find G_k, $H_k \in P$ for $k \ge 1$ with G_k monic of degree n, with $\deg(H_k) \le m$, and with

$$G_{k-1} \equiv G_k \text{ and } H_{k-1} \equiv H_k \pmod{\mathfrak{a}^{2^{k-1}}P} \quad\text{and}\quad F \equiv G_kH_k \pmod{\mathfrak{a}^{2^k}P}.$$

Plainly, applying **(10.34)** to G_{k-1}, H_{k-1}, and $\mathfrak{a}^{2^{k-1}}$ yields suitable G_k and H_k.

Set $p := \max\{\deg(H_0), \deg(F)\}$ and $M := \sum_{i=0}^{p} RX^i$. As R is separated and complete, plainly so is M. But the G_k and H_k form Cauchy sequences in M. So they have limits, say G and H; in fact, the coefficients of G and H are the limits of the coefficients of the G_k and H_k.

As the G_k are monic of degree n, so is G. As all G_k and H_k have residues $\widetilde{G}$ and $\widetilde{H}$, so do G and H. Now, F is the limit of G_kH_k; so $F = GH$; this factorization is unique by **(22.73)**. As $\widetilde{G}$ and $\widetilde{H}$ are coprime, so are G and H by **(10.33)**(2). □

Exercise (22.76) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $F \in R[X]$. Assume its residue $\overline{F} \in (R/\mathfrak{a})[X]$ has a supersimple root $\widetilde{a} \in R/\mathfrak{a}$, and R is separated and complete. Then F has a unique supersimple root $a \in R$ with residue $\widetilde{a}$.

Proposition (22.77). — *Let A be a local domain, R an overdomain. Assume A is Henselian, and R is integral over A. Then R is local.*

Proof: Let $\mathfrak{m}$ be the maximal ideal of A, and $\mathfrak{m}'$, $\mathfrak{m}''$ maximal ideals of R. The latter lie over $\mathfrak{m}$ by **(14.3)**(1). By way of contradiction, assume there's $x \in \mathfrak{m}' - \mathfrak{m}''$.

As R/A is integral, x satisfies a monic polynomial of minimal degree, say

$$F(X) := X^n + c_1X^{n-1} + \cdots + c_n \in A[x].$$

Then F is irreducible; for if $F = GH$, then $G(x)H(x) = 0$, but R is a domain.

Note $x \in \mathfrak{m}'$. So $c_n = -x(x^{n-1} + \cdots + c_{n-1})) \in A \cap \mathfrak{m}' = \mathfrak{m}$. Now, $c_i \notin \mathfrak{m}$ for some i; else, $x^n = -(c_1x^{n-1} + \cdots + c_n) \in \mathfrak{m}''$, but $x \notin \mathfrak{m}''$. Let j be maximal such that $c_j \notin \mathfrak{m}$. Then $1 \le j < n$.

Set $k := A/\mathfrak{m}$. Let $\overline{c}_i \in k$ be the residue of c_i. Set $\widetilde{G} := X^j + \overline{c}_1X^{j-1} + \cdots + \overline{c}_j$ and $\widetilde{H} := X^{n-j}$. Then the residue $\overline{F} \in k[X]$ factors as $\overline{F} = \widetilde{G}\widetilde{H}$. But $\overline{c}_j \ne 0$. So $\widetilde{G}$ and $\widetilde{H}$ are coprime by **(2.33)** or **(2.18)**. But A is Henselian. Thus F is reducible, a contradiction. So $\mathfrak{m}' \subset \mathfrak{m}''$. But $\mathfrak{m}'$ is maximal. So $\mathfrak{m}' = \mathfrak{m}''$. Thus R is local. □

Theorem (22.78). — *Let A be a local ring, and X a variable. Then the following four conditions are equivalent:* (1) *A is Henselian.*

(2) *For any monic polynomial $F \in A[X]$, the algebra $A[X]/\langle F\rangle$ is decomposable.*

(3) *Any module-finite A-algebra B is decomposable.*

(4) *Any module-finite A-algebra B that is free is decomposable.*

Proof: Let $\mathfrak{m}$ be the maximal ideal of A, and set $k := A/\mathfrak{m}$.

Assume (1). To prove (2), set $B := A[X]/\langle F\rangle$. Let $\overline{F} \in k[X]$ be the image of F. Note $A[X]/\mathfrak{m}A[X] = k[X]$ by **(1.16)**. So Noether's Isomorphism, **(4.8.1)**, yields $A[X]/\langle \mathfrak{m}, F\rangle = B/\mathfrak{m}B$ and $A[X]/\langle \mathfrak{m}, F\rangle = k[X]/\langle \overline{F}\rangle$; so $B/\mathfrak{m}B = k[X]/\langle \overline{F}\rangle$. If $\overline{F}$ is a power of an irreducible polynomial, then $k[X]/\langle \overline{F}\rangle$ is local, and so B is local.

Otherwise, $\overline{F} = \overline{G}\,\overline{H}$ with $\overline{G}$, $\overline{H}$ monic and coprime of positive degrees. So (1) yields $F = GH$ with G, H monic and coprime with residues $\overline{G}$ and $\overline{H}$. Hence

$$B = \big(A[X]/\langle G\rangle\big) \times \big(A[X]/\langle H\rangle\big)$$

by **(1.21)**(1)(b). So B is decomposable by recursion. Thus (2) holds.

Assume (2). To prove (3), set $\overline{B} := B/\mathfrak{m}B$. By **(19.15)**(2), $\overline{B} = \prod \overline{B}_{\mathfrak{n}_i}$ where the $\mathfrak{n}_i$ are the maximal ideals of B. Correspondingly, set $\overline{e}_i := (\delta_{ij}) \in \overline{B}$ with δ_{ij} the Kronecker delta function.

Fix i. Let $b \in B$ lift $\overline{e}_i \in \overline{B}$. Set $B' := A[b]$. As B is a module-finite A-algebra, B is a module-finite B'-algebra. For all j, set $\mathfrak{n}'_j := \mathfrak{n}_j \cap B'$. By **(14.3)**(1), the $\mathfrak{n}'_j$ are maximal (but not necessarily distinct). Now, $\overline{e}_i \notin \mathfrak{n}_i\overline{B}$, but $\overline{e}_i \in \mathfrak{n}_j\overline{B}$ for $j \neq i$. So $b \notin \mathfrak{n}_i$, but $b \in \mathfrak{n}_j$ for $j \neq i$. Thus $\mathfrak{n}'_j \neq \mathfrak{n}'_i$ for $j \neq i$.

By **(10.14)**(3)⇒(1), $F(b) = 0$ for a monic $F \in A[X]$. Set $B'' := A[X]/\langle F\rangle$. Let $x \in B''$ be the residue of X. Define $\varphi\colon B'' \twoheadrightarrow B'$ by $\varphi(x) := b$. For all j, set $\mathfrak{n}''_j := \varphi^{-1}\mathfrak{n}'_j$. Then as φ is surjective, the $\mathfrak{n}''_j$ are maximal, and $\mathfrak{n}''_j \neq \mathfrak{n}''_i$ for $j \neq i$.

By **(10.15)**(1)⇒(3), B'' is a module-finite A-algebra. So B'' is decomposable by (2). For all j, set $B''_j := B''_{\mathfrak{n}''_j}$. Then $B'' = \prod B''_j$ by **(11.18)**.

Set $e''_i := (\delta_{ij}) \in B''$. Let $\overline{e}''_i$ be the residue of $\varphi(e''_i)$ in $\overline{B}$. Then $\overline{e}''_i$ projects to 1 in $\overline{B}_{\mathfrak{n}_i}$ and to 0 in $\overline{B}_{\mathfrak{n}_j}$ for $j \neq i$. Hence $\overline{e}''_i = \overline{e}_i$. So $\varphi(e''_i) \in B$ is idempotent, and lifts $\overline{e}_i$. So B is decomposable by **(19.15)**(4). Thus (3) holds.

Trivially, (3) implies (4). And (4) implies (2) by **(10.15)**.

Assume (2) again. To prove (1), let F be a monic polynomial whose residue $\overline{F} \in k[X]$ factors as $\overline{F} = \overline{G}_1\overline{G}_2$ with the $\overline{G}_i$ monic and coprime. Set $B := A[X]/\langle F\rangle$. Then **(1.21)**(1)(b) yields $B/\mathfrak{m}B \xrightarrow{\sim} \big(k[X]/\langle \overline{G}_1\rangle\big) \times \big(k[X]/\langle \overline{G}_2\rangle\big)$.

By (2), B is decomposable. So idempotents of $B/\mathfrak{m}B$ lift to idempotents of B by **(19.15)**(3). Thus $B = B_1 \times B_2$ with $B_i/\mathfrak{m}B_i = k[X]/\langle \overline{G}_i\rangle$.

By **(10.15)**(1)⇒(4), B is free over A. So each B_i is projective by **(5.16)**(3)⇒(1). But A is local, and B_i is module-finite. Thus **(10.12)**(2)⇒(1) implies B_i is free.

By **(10.32)**, each $B_i = A[X]/\langle G_i\rangle$ where G_i is monic and lifts $\overline{G}_i$. Plainly, $\deg(G_i) = \deg(\overline{G}_i)$. By **(10.33)**(2), the G_i are coprime. So $B_1 \times B_2 = A[X]/\langle G_1G_2\rangle$ by **(1.21)**(1)(b). So $A[X]/\langle F\rangle = A[X]/\langle G_1G_2\rangle$. So $\langle F\rangle = \langle G_1G_2\rangle$. But F and G_1G_2 are monic of the same degree. Hence $F = G_1G_2$. Thus (1) holds. □

Corollary (22.79). — *Let A be a Henselian local ring, B be a module-finite local A-algebra. Then B is Henselian.*

Proof: Apply **(22.78)**(3)⇒(1): a module-finite B-algebra C is a module-finite A-algebra by **(10.16)**; thus, **(22.78)**(1)⇒(3) implies C is decomposable. □

(22.80) (Equicharacteristic). — A local ring A is said to be **equicharacteristic** if it has the same characteristic as its residue field.

Assume A is equicharacteristic. Let $\mathfrak{m}$ be its maximal ideal, p its characteristic, and A_0 the image of the canonical map $\varphi\colon \mathbb{Z} \to A$. If $p > 0$, then $\mathrm{Ker}(\varphi) = \langle p \rangle$, and so $\mathbb{F}_p \xrightarrow{\sim} A_0$. Suppose $p = 0$. Then $\varphi\colon \mathbb{Z} \xrightarrow{\sim} A_0$. But $A/\mathfrak{m}$ too has characteristic 0. Hence $A_0 \cap \mathfrak{m} = \langle 0 \rangle$. So $A_0 - 0 \subset A^\times$. Hence A contains $\mathbb{Q} = \mathrm{Frac}(A_0)$. In sum, A contains a field isomorphic to the prime field, either $\mathbb{F}_p$ or $\mathbb{Q}$.

Conversely, if a local ring contains a field, then that field is isomorphic to a subfield of the residue field, and so the local ring is equicharacteristic.

Any quotient of A is, plainly, equicharacteristic too. Moreover, given any local subring B of A with $B \cap \mathfrak{m}$ as maximal ideal, plainly B has the same characteristic as A, and its residue field is a subfield of that of A; so B is equicharacteristic too.

Theorem (22.81) (Cohen Existence)**. —** *A separated and complete equicharacteristic local ring contains a coefficient field.*

Proof: Let A be the local ring, $\mathfrak{m}$ its maximal ideal, K its residue field, and $\kappa\colon A \to K$ the quotient map. Let p be the characteristic of A and K.

First, assume $p = 0$. Then $\mathbb{Q} \subset A$ by **(22.80)**. Apply Zorn's Lemma to the subfields of A ordered by inclusion; it yields a maximal subfield E. Set $L = \kappa(E)$. Suppose there's an $x \in A$ with $\kappa(x)$ transcendental over L. Then $E[x] \cap \mathfrak{m} = 0$. So $E[x] - 0 \subset A^\times$. So $E(x) \subset A$, contradicting maximality. Thus K/L is algebraic.

Suppose there's $y \in K - L$. Let $\overline{F}(X) \in L[X]$ be its monic minimal polynomial. Set $\overline{F}'(X) := \partial\overline{F}(X)/\partial X$; see **(1.18.1)**. Then $\overline{F}'(X) \neq 0$ as $p = 0$. So $\overline{F}'(y) \neq 0$ as $\deg(\overline{F}') < \deg(\overline{F})$. Thus **(1.19)** implies y is a supersimple root of $\overline{F}$.

Note $\kappa|E$ is injective. Let $F \in E[X]$ be the (only) lift of $\overline{F}$. Then by **(22.76)**, there's a root $x \in A$ of F lifting y. But F is irreducible, as $\overline{F}$ is. So $E[X]/\langle F \rangle$ is a field by **(2.17)**. So the canonical surjection $E[X]/\langle F \rangle \twoheadrightarrow E[x]$ is bijective. Thus $E[x]$ is a field. But $x \notin E$ as $y \notin L$. Thus $E[x] \supsetneqq E$, contradicting maximality. Thus $K = L$, as desired.

So assume $p > 0$ instead. For all $n \geq 1$, set $A_n := A/\mathfrak{m}^n$. Then $A_1 = K$. Set $K_1 := A_1$. For $n \geq 2$, let's find a field $K_n \subset A_n$ that's carried isomorphically onto K_{n-1} by the canonical surjection $\psi_n\colon A_n \twoheadrightarrow A_{n-1}$. Suppose we have K_{n-1}.

Set $B := \psi_n^{-1}(K_{n-1})$ and $\mathfrak{n} := \mathrm{Ker}(\psi_n)$. Then $\mathfrak{n} \subset B$ as $0 \in K_{n-1}$. Let's show B is local with $\mathfrak{n}$ as maximal ideal. Given $x \in B - \mathfrak{n}$, set $y := \psi_n(x)$. Then $y \neq 0$ in K_{n-1}. So there's $z \in K_{n-1}$ with $yz = 1$. So $y \notin \mathfrak{m}/\mathfrak{m}^{n-1}$. So $x \notin \mathfrak{m}/\mathfrak{m}^n$. So there's $u \in A_n$ with $xu = 1$. So $y\psi_n(u) = 1$. So $\psi_n(u) = z$. So $u \in B$. Thus by **(3.5)**, B is local with $\mathfrak{n}$ as maximal ideal.

Note $\mathfrak{n} := \mathrm{Ker}(\psi_n) = \mathfrak{m}^{n-1}/\mathfrak{m}^n$. So $\mathfrak{n}^2 = 0$. Set $B^p = \{x^p \mid x \in B\}$. Then B^p is a ring. Given $y \in B^p - 0$, say $y = x^p$. Then $x \notin \mathfrak{n}$ as $\mathfrak{n}^2 = 0$. So there's $z \in B$ with $xz = 1$. Then $yz^p = 1$. Thus B^p is a field.

Zorn's Lemma yields a maximal subfield K_n of B containing B^p. Suppose there's $x \in B$ with $\psi_n(x) \notin \psi_n(K_n)$. Then $x^p \in B^p \subset K_n$. So $\psi_n(x)^p \in \psi_n(K_n)$. So its monic minimal polynomial is $X^p - \psi_n(x)^p$. So $X^p - x^p$ is irreducible in $B[X]$, as any nontrivial monic factor would reduce to one of $X^p - \psi_n(x)^p$. So $K_n[X]/\langle X^p - x^p \rangle$ is a field by **(22.76)**. Hence, as above, it is isomorphic to $K_n[x]$, and $K_n[x]$ is a field, contradicting maximality. So $\psi_n(K_n) \supset K_{n-1}$. But $K_n \subset B := \psi_n^{-1}(K_{n-1})$; so $\psi_n(K_n) \subset K_{n-1}$. Thus $\psi_n(K_n) = K_{n-1}$, as desired.

Finally, given $x_1 \in K_1$, define $x_n \in K_n$ inductively by $x_n := (\psi_n|K_n)^{-1}(x_{n-1})$.

Then $(x_n) \in \varprojlim A_n \subset \prod A_n$ as $\psi_n(x_n) = x_{n-1}$ for all n. But $\varprojlim A_n = \widehat{A}$ by **(22.7)**, and $A = \widehat{A}$ by **(22.14)**(2)⇒(1) as A is separated and complete. Define $\psi\colon K_1 \to A$ by $\psi(x_1) := (x_n)$. Then $\psi(K_1) \subset A$ is a field, and $\kappa\psi(K_1) = K$. Thus $\psi(K_1)$ is a coefficient field of A. □

Theorem (22.82) (Hensel's Lemma, ver. 2)**. —** *Let R be a ring, $\mathfrak{a}$ an ideal, $x \in R$. Let X be a variable, $F \in R[X]$ a polynomial. Set $F'(X) := \partial F(X)/\partial X$ as in* **(1.18.1)***, and set $e := F'(x)$. Assume that R is separated and complete and that $F(x) \equiv 0 \pmod{e^2\mathfrak{a}}$. Then there's a root $y \in R$ of F with $y \equiv x \pmod{e\mathfrak{a}}$. Moreover, if e is a nonzerodivisor, then y is unique.*

Proof: By hypothesis, $F(x) = e^2 a$ for some $a \in \mathfrak{a}$. So by **(1.18)**, there's some $H(X) \in R[X]$ with $F(X) = e^2 a + e(X - x) + (X - x)^2 H(X)$. Thus

$$F(x + eX) = e^2\big(a + X + X^2 H(x + eX)\big). \tag{22.82.1}$$

Set $H_1(X) := H(x + eX)$ and $\mathfrak{b} := \langle X \rangle$. Then $R[[X]]$ is $\mathfrak{b}$-adically separated and complete by **(22.2)**. So **(22.55)** yields an R-algebra map $\varphi\colon R[[X]] \to R[[X]]$ with $\varphi(X) = X + X^2 H_1(X)$. But $G_{\mathfrak{b}}(\varphi)$ is, plainly, the identity of $R[X]$. So φ is an automorphism by **(22.23)**. Thus we may apply φ^{-1} to **(22.82.1)**, and obtain

$$F(x + e\varphi^{-1}(X)) = e^2(a + X). \tag{22.82.2}$$

By hypothesis, R is $\mathfrak{a}$-adically separated and complete. So **(22.55)** yields an R-algebra map $\psi\colon R[[X]] \to R$ with $\psi(X) = -a$. Applying ψ to **(22.82.2)** yields $F(x + e\psi\varphi^{-1}(X)) = 0$. So set $y := x + e\psi\varphi^{-1}(X)$. Then $F(y) = 0$. But $\varphi^{-1}(X) \in \mathfrak{b}$ and $\psi(\mathfrak{b}) \subset \mathfrak{a}$. So $y \equiv x \pmod{e\mathfrak{a}}$. Thus y exists.

Moreover, assume e is a nonzerodivisor. Given two roots y_1, y_2 of F such that $y_i = x + ea_i$ with $a_i \in \mathfrak{a}$, note $0 = F(y_i) = e^2(a + a_i + a_i^2 H_1(a_i))$ by **(22.82.1)**. So $a_1 + a_1^2 H_1(a_1) = a_2 + a_2^2 H_1(a_2)$. But, **(22.55)** gives R-algebra maps $\theta_i\colon R[[X]] \to R$ with $\theta_i(X) = a_i$. So $\theta_1\varphi(X) = \theta_2\varphi(X)$. So $\theta_1\varphi = \theta_2\varphi$ by uniqueness in **(22.55)**. But φ is an isomorphism. So $\theta_1 = \theta_2$. Thus $y_1 = y_2$, as desired. □

Example (22.83). — Let's determine the nonzero squares z in the p-adic numbers $\widehat{\mathbb{Z}}_p$, introduced in **(22.2)**. Say $z = \sum_{i=n}^{\infty} z_i p^i$ with $0 \le z_i < p$ and $z_n \ne 0$. Set $y = \sum_{i=o}^{\infty} z_{i+n} p^i$. Then $z = p^n y$ and y isn't divisible by p.

Suppose $z = x^2$. Say $x = p^m w$ with $w \in \widehat{\mathbb{Z}}_p$ not divisible by p. Then $z = p^{2m} w^2$. If $n \ge 2m$, then $p^{n-2m} y = w^2$; so $n = 2m$ as w^2 isn't divisible by p. Similarly, if $n \le 2m$, then $n = 2m$. Thus n is even, and y is a square. Conversely, if n is even, and y is a square, then z is a square. Thus it remains to see when y is a square.

If y is a square, then so is its residue $\overline{y} \in \mathbb{F}_p = \widehat{\mathbb{Z}}_p/\langle p \rangle$. Conversely, suppose $\overline{y} = \widetilde{w}^2$ for some $\widetilde{w} \in \mathbb{F}_p$. Form $F(X) := X^2 - y \in \widehat{\mathbb{Z}}_p[X]$. Then $\widetilde{w}$ is a root of the residue $\overline{F}(X)$. Set $\overline{F}'(X) := \partial \overline{F}(X)/\partial X$ as in **(1.18.1)**. Then $\overline{F}'(X) = 2X$.

First, assume $p > 2$. Then $\overline{F}'(w) = 2\widetilde{w} \ne 0$ as $\widetilde{w} \ne 0$. So $\widetilde{w}$ is a supersimple root of $\overline{F}$ by **(1.19)**. So **(22.76)** yields a root w of F in A. So $y = w^2$. Thus y is a square if and only if $\overline{y}$ is a square.

For instance, 2 is a square in $\widehat{\mathbb{Z}}_7$ as $3^2 \equiv 2 \pmod 7$.

Lastly, assume $p = 2$. Then $2X \equiv 0 \pmod 2$. So the above reasoning fails. But suppose $y \equiv 1 \pmod 8$. Then $(\partial F(X)/\partial X)(1) = 2$ and $F(1) = 1 - y \equiv 0 \pmod{2^2 \cdot 2}$. So **(22.82)** yields a root w of F. Thus y is a square in $\widehat{\mathbb{Z}}_2$.

Conversely, suppose $y = w^2$ for some $w \in \widehat{\mathbb{Z}}_2$. Recall y isn't divisible by 2.

So $\overline{y} = 1 \in \mathbb{F}_2 = \widehat{\mathbb{Z}}_2/\langle 2\rangle$. So $\overline{w} = 1$. So $w = 1 + 2v$ for some $v \in \widehat{\mathbb{Z}}_2$. So $y = (1+2v)^2 = 1 + 4v(1+v)$. But $v(1+v) \equiv 0 \pmod 2$. Hence $y \equiv 1 \pmod 8$. Thus y is a square if and only if $y \equiv 1 \pmod 8$.

Theorem (22.84) (Weierstraß Division). — *Let R be a ring, $\mathfrak{a}$ an ideal. Assume R is separated and complete (in the $\mathfrak{a}$-adic topology). Fix $F = \sum f_i X^i \in R[[X]]$. Assume there's $n \geq 0$ with $f_n \in R^\times$ but $f_i \in \mathfrak{a}$ for $i < n$. Then given $G \in R[[X]]$, there are unique $Q \in R[[X]]$ and $P \in R[X]$ with either $P = 0$ or $\deg(P) < n$ such that $G = QF + P$. Moreover, if $F, G \in R[X]$ and $\deg(F) = n$, then $Q \in R[X]$ with either $Q = 0$ or $\deg(Q) = \deg(G) - n$.*

Proof: Given $H = \sum h_i X^i \in R[[X]]$, set $\alpha(H) := h_0 + \cdots + h_{n-1}X^{n-1}$ and $\tau(H) := h_n + h_{n+1}X + \cdots$. As $f_n \in R^\times$, then $\tau(F) \in R[[X]]^\times$ by **(3.7)**. Set $M := -\alpha(F)\tau(F)^{-1}$ and $\mu(H) := \tau(MH)$. Then $\alpha, \tau, \mu \in \mathrm{End}_R(R[[X]])$.

Assume F, $G \in R[X]$ and $\deg(F) = n$. Then the usual Division Algorithm (DA) yields Q, P. Let's review it, then modify it so that it yields Q, P for any F, G.

The DA is this: set $Q := 0$ and $P := G$; while $P =: \sum_{i=0}^m p_i X^i$ with $p_m \neq 0$ and $m \geq n$, replace Q by $Q + p_m f_n^{-1} X^{m-n}$ and replace P by $P - p_m f_n^{-1} X^{m-n} F$.

Note $G = QF + P$ holds initially. and is preserved on each iteration of the loop:

$$G = QF + P = (Q + p_m f_n^{-1} X^{m-n})F + (P - p_m f_n^{-1} X^{m-n} F).$$

Moreover, when the DA terminates, $P = 0$ or $\deg(P) < n$. So if $Q \neq 0$, then $\deg(G) = \deg(Q) + n$ as $G = QF + P$ and $f_n \in R^\times$. Thus Q, P work.

The algorithm does, in fact, terminate. Indeed, replacing P by $P - p_m f_n^{-1} X^{m-n} F$ eliminates p_m and modifies the p_i for $i < m$, but adds no new $p_i X^i$ for $i > m$. Thus on each iteration of the loop, either P becomes 0 or its degree drops.

The Modified Dvision Algorithm (MDA) is similar, with F, G still polynomials, but it de-emphasizes m. Also, n can be made implicit as $f_n = \tau(F)$. The MDA is this: set $Q := 0$ and $P := G$; while $\tau(P) \neq 0$, replace Q by $Q + \tau(P)\tau(F)^{-1}$ and P by $P - \tau(P)\tau(F)^{-1}F$.

Initially, $G = QF + P$. And $G = QF + P$ remains true when we replace Q, P as

$$G = QF + P = (Q + \tau(P)\tau(F)^{-1})F + (P - \tau(P)\tau(F)^{-1}F).$$

When the MDA terminates, $\tau(P) = 0$, and so $P = 0$ or $\deg(P) < n$.

At any stage, $P = \tau(P)X^n + \alpha(P)$. Moreover, $F = \tau(F)X^n + \alpha(F)$, and $M := -\tau(F)^{-1}\alpha(F)$. Thus $P - \tau(P)\tau(F)^{-1}F = M\tau(P) + \alpha(P)$.

Note $M = 0$ or $\deg(M) < n$. So $M\tau(P) = 0$ or $\deg(M\tau(P)) < \deg(P)$. Further, if $\tau(P) \neq 0$ and $\alpha(P) \neq 0$, then $\deg(\alpha(P)) < \deg(P)$. So when we replace P, either P becomes 0 or $\deg(P)$ drops. Thus the MDA does terminate.

Note $\tau\big(M\tau(P) + \alpha(P)\big) = \tau(M\tau(P)) + \tau(\alpha(P)) = \mu(\tau(P))$; that is, when we replace P, the new value of $\tau(P)$ is equal to the old value of $\mu(\tau(P))$. Initially, $P := G$. So for $r \geq 1$, after r interations, $\tau(P) = \mu^r(\tau(G))$. Initially, $Q := 0$. Thus after r interations, $Q = \sum_{i=0}^{r-1} \mu^i(\tau(G))\tau(F)^{-1}$ where $\mu^0 := 1$ in $\mathrm{End}_R(R[[X]])$.

As before, if $Q \neq 0$, then $\deg(G) = \deg(Q) + n$ as $G = QF + P$ and $f_n \in R^\times$ and either $P = 0$ or $\deg(P) < n$. Thus the MDA too yields Q, P that work. The uniqueness statement, proved at the very end, implies that these Q, P coincide with those given by the DA.

For the general case, filter $R[[X]]$ with the ideals $\mathfrak{b}_n$ of all $H =: \sum h_i X^i$ with $h_i \in \mathfrak{a}^n$ for all i. Correspondingly, $R[[X]]$ is separated and complete by **(22.28)**(2). Let's prove that the sum $\sum_{i\geq 0} \mu^i(\tau(G))\tau(F)^{-1}$ converges to a Q that works.

Note $\alpha(F) \in \mathfrak{b}_1$. So $M \in \mathfrak{b}_1$. So for any $i \geq 1$ and $H \in \mathfrak{b}_{i-1}$, we have $\mu(H) \in \mathfrak{b}_i$. So by induction, for any $i \geq 0$ and $H \in R[[X]]$, we have $\mu^i(H) \in \mathfrak{b}_i$. Thus for any $H, H_1 \in R[[X]]$, the sum $\sum_{i\geq 0} \mu^i(H)H_1$ converges uniquely.

Set $Q := \sum_{i\geq 0} \mu^i(\tau(G))\tau(F)^{-1}$. Let's find $\tau(QF)$. Note $F = \tau(F)X^n + \alpha(F)$. Also $\tau(X^n H) = H$ for any $H \in R[[X]]$. Hence $\tau(QF) = Q\tau(F) + \tau(Q\alpha(F))$. But $Q\tau(F) = \sum_{i\geq 0} \mu^i(\tau(G))$. Furthermore, $Q\alpha(F) = -\sum_{i\geq 0} \mu^i(\tau(G))M$, and $\tau(\mu^i(\tau(G))M) = \mu^{i+1}(\tau(G))$. But $\tau(\mathfrak{b}_s) \subset \mathfrak{b}_s$ for all s; so τ is continuous. Hence $\tau(Q\alpha(F)) = \sum_{i\geq 1} \mu^i(\tau(G))$. Thus $\tau(QF) = \tau(G)$.

Set $P := G - QF$. Then $\tau(P) = \tau(G) - \tau(QF) = 0$. So $P \in R[X]$ with either $P = 0$ or $\deg(P) < n$. Thus Q, P work.

It remains to show Q, P are unique. Suppose $G = Q_1F + P_1$ with $P_1 \in R[X]$ and either $P_1 = 0$ or $\deg(P_1) < n$. Then $\tau(G) = \tau(Q_1F) + \tau(P_1) = \tau(Q_1F)$. But $F = \tau(F)X^n + \alpha(F)$. So $\tau(Q_1F) = Q_1\tau(F) + \tau(Q_1\alpha(F))$. Set $H := Q_1\tau(F)$. Then $Q_1\alpha(F) = -HM$. Thus $\tau(G) = H - \tau(HM) = H - \mu(H)$.

So $\mu^i(\tau(G)) = \mu^i(H) - \mu^{i+1}(H)$ for all i. So $\sum_{i=0}^{s-1} \mu^i(\tau(G)) = H - \mu^s(H)$ for all s. But $\mu^s(H) \in \mathfrak{b}_s$. So $\sum_{i\geq 0} \mu^i(\tau(G)) = H$. So $Q\tau(F) = H := Q_1\tau(F)$. Thus $Q = Q_1$. But $P = G - QF$ and $P_1 = G - Q_1F$. Thus $P = P_1$, as desired. □

Theorem (22.85) (Weierstraß Preparation)**. —** *In* **(22.84)**, *further $F = UV$ where $U \in R[[X]]^\times$ and $V = X^n + v_{n-1}X^{n-1} + \cdots + v_0$; both U and V are unique, and all $v_i \in \mathfrak{a}$. And if $F \in R[X]$, then $U \in R[X]$ and $\deg(U) = \deg(F) - n$.*

Proof: Say **(22.84)** yields $X^n = QF + P$ where $Q = \sum q_iX^i \in R[[X]]$ and $P \in R[X]$ with $P = 0$ or $\deg(P) < n$. But $F = \sum f_iX^i$ with $f_i \in \mathfrak{a}$ for $i < n$. Hence $q_0f_n = 1 + a$ with $a \in \mathfrak{a}$. But R is separated and complete. So $1 + a \in R^\times$ by **(22.35)**. Hence $q_0 \in R^\times$. Thus **(3.7)** yields $Q \in R[[X]]^\times$.

Set $U := Q^{-1}$ and $V := X^n - P$. Then $F = UV$, as desired.

Say $P =: p_{n-1}X^{n-1} + \cdots + p_0$. Then $V = X^n - (p_{n-1}X^{n-1} + \cdots + p_0)$. But $P = X^n - QF$ and $f_i \in \mathfrak{a}$ for $i < n$. Thus all $p_i \in \mathfrak{a}$, as desired.

Suppose $F = U_1V_1$ too, with $U_1 \in R[[X]]^\times$ and $V_1 \in R[[X]]$ monic of degree n. Set $Q_1 := U_1^{-1}$ and $P_1 := X^n - V_1$. Then $X^n = Q_1F + P_1$, and either $P_1 = 0$ or $\deg(P_1) < n$. So $Q_1 = Q$ and $P_1 = P$ by the uniqueness of Q and P, which is part of **(22.84)**. Thus $U_1 = U$ and $V_1 = V$, as desired.

Finally, suppose $F \in R[X]$. Apply **(22.84)** with $F := V$ and $G := F$. Thus, by uniqueness, $U \in R[X]$ and $\deg(U) = \deg(F) - n$, as desired. □

Exercise (22.86) . — Show that **(22.75)** is a formal consequence of **(22.85)** when R is a local ring with maximal ideal $\mathfrak{a}$ such that $k := A/\mathfrak{a}$ is algebraically closed.

Exercise (22.87) . — Let k be a field, $B_n := k[[X_1, \ldots, X_n]]$ the local ring of power series in n variables X_i. Use **(22.59)** and **(22.84)** to recover, by induction, the conclusion of **(22.27)**, that B_n is Noetherian.

Exercise (22.88) . — Let k be a field, $B_n := k[[X_1, \ldots, X_n]]$ the local ring of power series in n variables X_i. Use **(22.27)** and **(22.59)** and **(22.85)** to show, by induction, that B_n is a UFD.

(22.89) (Analysis). — Let's adapt the Weierstraß Division Theorem **(22.84)** and its consequences **(22.85)**–**(22.88)** to convergent complex power series. Specifically, let A be the ring of complex power series in variables $X_1, \ldots, X_r$ converging about the origin in $\mathbb{C}^r$. Then A is local with maximal ideal $\mathfrak{m} := \langle X_1, \ldots, X_r\rangle$ by **(22.67)**.

Let's now see A is Henselian, Noetherian, regular of dimension r, and a UFD.

Consider the Weierstraß Division Theorem **(22.84)**. First, suppose $F, G \in R[X]$ with $\deg(F) = n$ and $f_n \in R^\times$. Then for any R whatsoever, the DA and the MDA work as before to provide $P, Q \in R[X]$ with either $P = 0$ or $\deg(P) < n$ and with either $Q = 0$ or $\deg(Q) = \deg(G) - n$ such that $G = QF + P$. Moreover, P and Q are unique. Indeed, suppose $P_1, Q_1 \in R[X]$ with either $P_1 = 0$ or $\deg(P_1) < n$ such that $G = Q_1F + P_1$. Then $(Q - Q_1)F = P_1 - P$. If $Q \neq Q_1$, then $\deg(Q - Q_1)F \geq n$, but $\deg(P_1 - P) < n$, a contradiction. Thus $Q = Q_1$ and so $P = P_1$.

Next, take R to be A and $\mathfrak{a}$ to be $\mathfrak{m}$. Let B be the ring of complex power series in $X_1, \ldots, X_r, X$ converging about the origin $\mathbf{0} := (0, \ldots, 0, 0)$ in $\mathbb{C}^{r+1}$. Then $B \subset A[[X]]$. Suppose $F, G \in B$. Distilling and adapting the discussion in [**7**, pp. 105–115]), let's see that the sum $\sum_{i\geq 0} \mu^i(\tau(G))\tau(F)^{-1}$, defined in the proof of **(22.84)**, converges, complex analytically, to a $Q \in B$ that works.

Fix a vector $\mathbf{t} := (t_1, \ldots, t_r, t)$ of positive real numbers. Given a complex power series $H = \sum a_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$ where $\mathbf{i} := (i_1, \ldots, i_r, i)$ is a vector of nonnegative integers and $\mathbf{X}^{\mathbf{i}} := X_1^{i_1} \cdots X_r^{i_r} X^i$, set $\|H\| := \sum |a_{\mathbf{i}}|\mathbf{t}^{\mathbf{i}}$ and $C := \{H \mid \|H\| < \infty\}$. Then $C \subset B$.

Note $\|H\| = 0$ if and only if $H = 0$. Moreover, $\|aH\| = |a|\|H\|$ for any $a \in \mathbb{C}$ as $aH = \sum aa_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$ and $|aa_{\mathbf{i}}| = |a||a_{\mathbf{i}}|$. Furthermore, given $H' = \sum a'_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$, note $\|HH'\| \leq \|H\|\|H'\|$ as $HH' = \sum b_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$ where $b_{\mathbf{i}} := \sum_{\mathbf{j}+\mathbf{k}=\mathbf{i}} a_{\mathbf{j}}a'_{\mathbf{k}}$ and where by the triangle inequality $|b_{\mathbf{i}}| \leq \sum_{\mathbf{j}+\mathbf{k}=\mathbf{i}} |a_{\mathbf{j}}||a'_{\mathbf{k}}|$. Similarly, $\|H + H'\| \leq \|H\| + \|H'\|$.

Let's see C is complete in this norm. Let (E_n) be Cauchy. Say $E_n = \sum b_{n,\mathbf{i}}\mathbf{X}^{\mathbf{i}}$. Given $\varepsilon > 0$, there's n_ε with $\sum |b_{n,\mathbf{i}} - b_{n',\mathbf{i}}|\mathbf{t}^{\mathbf{i}} < \varepsilon$ for all $n, n' \geq n_\varepsilon$. But $\mathbf{t}^{\mathbf{i}} \neq 0$ for all $\mathbf{i}$. So $|b_{n,\mathbf{i}} - b_{n',\mathbf{i}}| < \varepsilon/\mathbf{t}^{\mathbf{i}}$. Thus $(b_{n,\mathbf{i}})$ is Cauchy in $\mathbb{C}$, so has a limit $b_{\mathbf{i}}$. Given any set I of m vectors $\mathbf{i}$ for any m, there's $n' \geq n_\varepsilon$ with $|b_{n',\mathbf{i}} - b_{\mathbf{i}}| < \varepsilon/\mathbf{t}^{\mathbf{i}}m$ for all $\mathbf{i} \in I$. So $\sum_{\mathbf{i}\in I} |b_{n',\mathbf{i}} - b_{\mathbf{i}}|\mathbf{t}^{\mathbf{i}} < \varepsilon$. But $b_{n,\mathbf{i}} - b_{\mathbf{i}} = b_{n,\mathbf{i}} - b_{n',\mathbf{i}} + b_{n',\mathbf{i}} - b_{\mathbf{i}}$. Thus $\sum_{\mathbf{i}\in I} |b_{n,\mathbf{i}} - b_{\mathbf{i}}|\mathbf{t}^{\mathbf{i}} < 2\varepsilon$ for all $n \geq n_\varepsilon$. Set $E := \sum b_{\mathbf{i}}\mathbf{X}^{\mathbf{i}}$. Then $\|E_n - E\| \leq 2\varepsilon$ for all $n \geq n_\varepsilon$. Hence $E_n - E \in C$. But $E = (E - E_n) + E_n$. Thus $E \in C$, and $\lim E_n = E$. Thus C is complete. In sum, C is a complex Banach algebra.

Replacing the t_i and t by smaller values just decreases $\|H\|$ and so enlarges C. In particular, given any $E \in B$, replace the t_i and t by smaller values so that $\mathbf{t}$ lies in the open polydisk of convergence of E; then $E \in C$.

Next, given $E \in C$ with $E(\mathbf{0}) = 0$ and given $\varepsilon > 0$, let's see we can replace the t_i and t by smaller values so that $\|E\| < \varepsilon$. Note $E = X_1E_1 + \cdots + X_rE_r + XE_{r+1}$ for some formal power series E_i. But, as shown in the solution to **(22.67)**, the E_i can be altered so that they have distinct monomials. Then

$$\|E\| = t_1\|E_1\| + \cdots + t_r\|E_r\| + t\|E_{r+1}\|.$$

So all $E_i \in C$. Thus replacing the t_i and t by small enough values gives $\|E\| < \varepsilon$.

Given $H \in B$ with $a := H(\mathbf{0}) \neq 0$, let's see why $H \in B^\times$. First replace the t_i and t by smaller values so that $H \in C$. Set $E := 1 - H/a$. Then $E(\mathbf{0}) = 0$. So, as just observed, we can replace the t_i and t by even smaller values so that $\|E\| < 1$. Then $\sum_{i\geq 0} E^i$ converges, say to $E' \in C$. Then $(1 - E)E' = 1$. Thus $H \cdot (E'/a) = 1$.

Returning to $\sum_{i\geq 0} \mu^i(\tau(G))\tau(F)^{-1}$, let's see it converges. Replace the t_i and t by smaller values so that $F, G \in C$. Note $F = \sum f_iX^i$ with $f_i \in A$; also, $f_n(\mathbf{0}) \neq 0$, but $f_i\mathbf{0}) = 0$ for $i < n$. Recall $\alpha(F) := \sum_{i=0}^{n-1} f_iX^i$ and $\tau(F) := \sum_{i\geq n} f_iX^{i-n}$. So $\tau(F)(\mathbf{0}) \neq 0$. Replace the t_i and t by even smaller values so that $\tau(F)^{-1} \in C$. Set $c := \|\tau(F)^{-1}\|$. Fix $0 < \varepsilon < 1$. Replace the t_i, but not t, by yet smaller values so that $\|f_i\| < t^{n-i}\varepsilon/cn$ for $i < n$. Then $\|\alpha(F)\| < t^n\varepsilon/c$. Recall $M := -\alpha(F)\tau(F)^{-1}$.

Hence $\|M\| \le \|\alpha(F)\|\|\tau(F)^{-1}\| < t^n\varepsilon$. For all $H \in C$, note $t^n\|\tau(H)\| \le \|H\|$. Recall $\mu(H) := \tau(MH)$. So $\|\mu(H)\| \le t^{-n}\|M\|\|H\| \le \varepsilon\|H\|$. So $\|\mu^i(H)\| \le \varepsilon^i\|H\|$ for $i \ge 0$. But C is complete. Thus $\sum_{i\ge 0}\mu^i(\tau(G))\tau(F)^{-1}$ converges.

Note $\tau(H)$ is continuous in H, as $\|\tau(H)\| \le t^{-n}\|H\|$. So the rest of the existence proof in **(22.84)** carries over here without change. Uniqueness here is a special case of uniqueness in **(22.84)**. Thus the Weierstraß Division Theorem can be adapted.

To adapt the Weierstraß Preparation Theorem **(22.85)**, note that the Division Theorem above yields $X^n = FQ + P$ where $Q \in B$ and $P \in A[X]$ with $\deg(P) < n$. The proof of **(22.85)** shows $Q(\mathbf{0}) \ne 0$. So $Q \in B^\times$. Set $U := Q^{-1}$ and set $V := X^n - P$. Then $F = UV$ where $U \in B^\times$ and $V = X^n + v_{n-1}X^{n-1} + \cdots + v_0$ with $v_i \in A$. By **(22.85)**, U and V are unique; also, if $F \in R[X]$, then $U \in R[X]$ and $\deg(U) = \deg(F) - n$. Thus we can adapt the Weierstraß Preparation Theorem.

To prove A is Henselian, adapt the solution to **(22.86)** by replacing **(22.85)** with its counterpart above.

Consider the automorphism φ of $\mathbb{C}[[X_1,\ldots,X_r,X]]$ in **(22.59.2)** for use in the next three assertions. Let $H \in B$. If H converges at $(x_1,\ldots,x_r,x)$, then $\varphi(H)$ converges at $(x_1',\ldots,x_r',x)$ where $x_i' := x_i - a_i x$, and so $\varphi(H) \in B$. Thus φ induces an automorphism of B.

To prove B is Noetherian, adapt the solution to **(22.87)** by replacing **(22.84)** with its analytic counterpart. Thus, as r is arbitrary, A is Noetherian too.

To prove A is regular of dimension r, recall from **(22.67)** that A is local with completion $\mathbb{C}[[X_1,\ldots,X_r]]$. By **(22.27)**, the latter ring is regular of dimension r. Thus, by **(22.62)**(2), A too is regular of dimension r.

Finally, to prove A is a UFD, adapt the solution to **(22.88)** by replacing **(22.27)** and **(22.59)** and **(22.85)** by their analytic counterparts.

D. Appendix: Exercises

Exercise (22.90) . — (Implicit Function Theorem) Let R be a ring, $T_1,\ldots,T_n,X$ variables. Given a polynomial $F \in R[T_1,\ldots,T_n,X]$ such that $F(0,\ldots,0,X)$ has a supersimple root $a_0 \in R$. Show there's a unique power series $a \in R[[T_1,\ldots,T_n]]$ with $a(0,\ldots,0) = a_0$ and $F(T_1,\ldots,T_n,a) = 0$.

Exercise (22.91) . — Let A be the filtered direct limit of Henselian local rings A_λ with local transition maps. Show that A is a Henselian local ring.

Exercise (22.92) . — Let A be a local Henselian ring, $\mathfrak{m}$ its maximal ideal, B an integral A-algebra, and $\mathfrak{n}$ a maximal ideal of B. Set $\overline{B} = B/\mathfrak{m}B$. Show:

(1) $\mathrm{Idem}(B) \to \mathrm{Idem}(\overline{B})$ is bijective. (2) $B_\mathfrak{n}$ is integral over A, and Henselian.

Exercise (22.93) . — Let A be local ring. Show that A is Henselian if and only if, given any module-finite algebra B and any maximal ideal $\mathfrak{n}$ of B, the localization $B_\mathfrak{n}$ is integral over A.

Exercise (22.94) . — Let A be a local ring, and $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} \subset \mathrm{nil}(A)$. Set $A' := A/\mathfrak{a}$. Show that A is Henselian if and only if A' is so.

Exercise (22.95) . — Let A be a local ring. Assume A is separated and complete. Use **(22.78)**(4)⇒(1) to give a second proof (compare **(22.75)**) that A is Henselian.

Exercise (22.96) . — Let R be a ring, $\mathfrak{a}$ an ideal, $u \in R^{\times}$, and $n \geq 2$. Assume R is separated and complete, and $u \equiv 1 \pmod{n^2\mathfrak{a}}$. Find an nth root of u.

Exercise (22.97) . — Let p, $a_1, \ldots, a_s$, k be integers, and $X_1, \ldots, X_s$ variables. Set $F := a_1X_1^k + \cdots + a_sX_s^k$. Assume p prime, each a_i and k prime to p, and $s > k > 0$. Using (**2.46**), show F has a nontrivial zero in $\widehat{\mathbb{Z}}_p^s$.

Exercise (22.98) . — Find a cube root of 2 in $\widehat{\mathbb{Z}}_5$.

Exercise (22.99) . — Find a cube root of 10 in $\widehat{\mathbb{Z}}_3$.

Exercise (22.100) . — In the setup of (**22.84**), if $n \geq 1$, find an alternative proof for the existence of Q and P as follows: take a variable Y; view $R[[X]]$ as an $R[[Y]]$-algebra via the map φ with $\varphi(Y) := F$: and show $1, X, \ldots, X^{n-1}$ generate $R[[X]]$ as a module by using Nakayama's Lemma for adically complete rings (**22.69**).

23. Discrete Valuation Rings

A **discrete valuation** is a homomorphism from the multiplicative group of a field to the additive group of integers such that the value of a sum is at least the minimum value of the summands. The corresponding **discrete valuation ring** consists of the elements whose values are nonnegative, plus 0. We characterize these rings in various ways; notably, we prove they are the normal Noetherian local domains of dimension 1. Then we prove that any normal Noetherian domain is the intersection of all the discrete valuation rings obtained by localizing at its height-1 primes. Finally, we prove Serre's Criterion for normality of a Noetherian domain.

Along the way, we consider two important notions for a module M over any ring R. We say $x_1, \dots, x_n$ is an M-**sequence** or is M-**regular** if $x_{i+1} \in R$ is a nonzerodivisor on $M_i := M/\langle x_1, \dots, x_i \rangle M$ for $0 \le i \le n$ and if $M_n \ne 0$. If R is local, we call the supremum of the lengths n of the M-sequences, the **depth** of M.

In an appendix, we study those two notions and one more: we call M **Cohen–Macaulay** if M is nonzero Noetherian and if, for all maximal ideals $\mathfrak{m} \in \mathrm{Supp}(M)$, the depth of $M_{\mathfrak{m}}$ equals its dimension. We prove the Unmixedness Theorem: if there are only finitely many $\mathfrak{m}$ and the dimensions are equal, then every associated prime of M is minimal, and all maximal chains of primes in $\mathrm{Supp}(M)$ have the same length. We end by proving, under appropriate hypotheses, the equivalence of the following conditions where $n := \dim(M)$: (1) the multiplicity of M is equal to the length of M_n; (2) $x_1, \dots, x_n$ is M-quasi-regular; (3) $x_1, \dots, x_n$ is M-regular; (4) M is Cohen–Macaulay.

A. Text

(23.1) (Discrete Valuations). — Let K be a field. We define a **discrete valuation** of K to be a surjective function $v\colon K^\times \to \mathbb{Z}$ such that, for every $x, y \in K^\times$,

$$(1)\ v(x \cdot y) = v(x) + v(y), \quad (2)\ v(x+y) \ge \min\{v(x), v(y)\} \text{ if } x \ne -y. \quad \textbf{(23.1.1)}$$

Condition (1) just means v is a group homomorphism. Hence, for any $x \in K^\times$,

$$(1)\ v(1) = 0 \quad \text{and} \quad (2)\ v(x^{-1}) = -v(x). \qquad \textbf{(23.1.2)}$$

As a convention, we define $v(0) := \infty$. Consider the sets

$$A := \{x \in K \mid v(x) \ge 0\} \quad \text{and} \quad \mathfrak{m} := \{x \in K \mid v(x) > 0\}.$$

Clearly, A is a subring, so a domain, and $\mathfrak{m}$ is an ideal. Further, $\mathfrak{m}$ is nonzero as v is surjective. We call A the **discrete valuation ring** (DVR) of v.

Notice that, if $x \in K$, but $x \notin A$, then $x^{-1} \in \mathfrak{m}$; indeed, $v(x) < 0$, and so $v(x^{-1}) = -v(x) > 0$. Hence, $\mathrm{Frac}(A) = K$. Further,

$$A^\times = \{x \in K \mid v(x) = 0\} = A - \mathfrak{m}.$$

Indeed, if $x \in A^\times$, then $v(x) \ge 0$ and $-v(x) = v(x^{-1}) \ge 0$; so $v(x) = 0$. Conversely, if $v(x) = 0$, then $v(x^{-1}) = -v(x) = 0$; so $x^{-1} \in A$, and so $x \in A^\times$. Therefore, by the nonunit criterion, *A is a local domain, not a field, and $\mathfrak{m}$ is its maximal ideal.*

An element $t \in \mathfrak{m}$ with $v(t) = 1$ is called a (local) **uniformizing parameter**. Such a t is irreducible, as $t = ab$ with $v(a) \ge 0$ and $v(b) \ge 0$ implies $v(a) = 0$ or $v(b) = 0$ since $1 = v(a) + v(b)$. Further, given $x \in K^\times$, set $n := v(x)$ and

$u := xt^{-n}$. Then $v(u) = 0$. Thus $x = ut^n$ and $u \in A^\times$. In particular, t_1 is uniformizing parameter if and only if $t_1 = ut$ with $u \in A^\times$.

Moreover, A *is a* PID, *so a* UFD; *in fact, any nonzero ideal* $\mathfrak{a}$ *of* A *has the form*

$$\mathfrak{a} = \langle t^m \rangle \quad \text{where} \quad m := \min\{\, v(x) \mid x \in \mathfrak{a} \,\}. \tag{23.1.3}$$

Indeed, given a nonzero $x \in \mathfrak{a}$, say $x = ut^n$ where $u \in A^\times$. Then $t^n \in \mathfrak{a}$. So $n \geq m$. Set $y := ut^{n-m}$. Then $y \in A$ and $x = yt^m$, as desired.

In particular, $\mathfrak{m} = \langle t \rangle$ and $\dim(A) = 1$. Thus A is regular local of dimension 1.

Example (23.2). — The prototype of a DVR is the following example. Let k be a field, and $K := k((t))$ the field of **formal Laurent series** $x := \sum_{i \geq n} a_i t^i$ with $n \in \mathbb{Z}$ and $a_i \in k$. If $a_n \neq 0$, set $v(x) := n$, the "order of vanishing" of x. Plainly, v is a discrete valuation, the formal power series ring $k[[t]]$ is its DVR, and $\mathfrak{m} := \langle t \rangle$ is its maximal ideal.

The preceding example can be extended to cover any DVR A that contains a field k with $k \xrightarrow{\sim} A/tA$ where t is a uniformizing power. Indeed, A is a subring of its completion $\widehat{A}$ by **(22.3)**, and $k \xrightarrow{\sim} \widehat{A}/(tA)\widehat{\ }$ by **(22.12)**. But $\widehat{A}$ is separated and complete in the topology of the filtration with $F^n\widehat{A} := (t^nA)\widehat{\ }$. And that topology is just the $(tA)\widehat{\ }$-adic by **(22.21)**. Hence $\widehat{A} = k[[t]]$ by the Cohen Structure Theorem II, **(22.58)**. Further, plainly, the valuation on $\widehat{A}$ restricts to that on A.

A second old example is this. Let $p \in \mathbb{Z}$ be prime. Given $x \in \mathbb{Q}$, write $x = ap^n/b$ with $a, b \in \mathbb{Z}$ relatively prime and prime to p. Set $v(x) := n$. Clearly, v is a discrete valuation, the localization $\mathbb{Z}_{\langle p \rangle}$ is its DVR, and $p\mathbb{Z}_{\langle p \rangle}$ is its maximal ideal. We call v the **p-adic valuation** of $\mathbb{Q}$.

Lemma (23.3). — *Let A be a local domain, $\mathfrak{m}$ its maximal ideal. Assume that $\mathfrak{m}$ is nonzero and principal and that $\bigcap_{n \geq 0} \mathfrak{m}^n = 0$. Then A is a DVR.*

Proof: Given a nonzero $x \in A$, there is an $n \geq 0$ such that $x \in \mathfrak{m}^n - \mathfrak{m}^{n+1}$. Say $\mathfrak{m} = \langle t \rangle$. Then $x = ut^n$, and $u \notin \mathfrak{m}$, so $u \in A^\times$. Set $K := \operatorname{Frac}(A)$. Given $x \in K^\times$, write $x = y/z$ where $y = bt^m$ and $z = ct^k$ with $b, c \in A^\times$. Then $x = ut^n$ with $u := b/c \in A^\times$ and $n := m - k \in \mathbb{Z}$. Define $v\colon K^\times \to \mathbb{Z}$ by $v(x) := n$. If $ut^n = wt^h$ with $n \geq h$, then $(u/w)t^{n-h} = 1$, and so $n = h$. Thus v is well defined.

Since $v(t) = 1$, clearly v is surjective. To verify **(23.1.1)**, take $x = ut^n$ and $y = wt^h$ with $u, w \in A^\times$. Then $xy = (uw)t^{n+h}$. Thus (1) holds. To verify (2), we may assume $n \geq h$. Then $x + y = t^h(ut^{n-h} + w)$. Hence

$$v(x+y) \geq h = \min\{n, h\} = \min\{v(x), v(y)\}.$$

Thus (2) holds. So $v\colon K^\times \to \mathbb{Z}$ is a valuation. Clearly, A is the DVR of v. □

(23.4) (Depth). — Let R be a ring, M a nonzero module, and $x_1, \ldots, x_n \in R$. Set $M_i := M/\langle x_1, \ldots, x_i \rangle M$. We say the sequence $x_1, \ldots, x_n$ is M-**regular**, or is an M-**sequence**, and we call n its **length** if $M_n \neq 0$ and $x_i \notin \operatorname{z.div}(M_{i-1})$ for all i.

For reference, note that **(4.21)** with $\mathfrak{a} := \langle x_1, \ldots, x_i \rangle$ and $\mathfrak{b} := \langle x_{i+1} \rangle$ yields

$$M_{i+1} \xrightarrow{\sim} M_i/x_{i+1}M_i. \tag{23.4.1}$$

If M is finitely generated, **(13.46)**(1) with $\mathfrak{a} := \langle x_1, \ldots, x_i \rangle$ and **(13.4)**(4) yield

$$\operatorname{rad}(M_i) = \operatorname{rad}(M) \quad \text{if and only if} \quad x_1, \ldots, x_i \in \operatorname{rad}(M). \tag{23.4.2}$$

Call the supremum of the lengths n of the M-sequences found in an ideal $\mathfrak{a}$, the **depth** of $\mathfrak{a}$ on M, and denote it by $\operatorname{depth}(\mathfrak{a}, M)$. By convention, $\operatorname{depth}(\mathfrak{a}, M) = 0$

means $\mathfrak{a}$ contains no nonzerodivisor on M.

Call the depth of $\operatorname{rad}(M)$ on M just the **depth** of M, and denote it by $\operatorname{depth}(M)$ or $\operatorname{depth}_R(M)$. Notice that, in this case, if M is finitely generated, then $M_n \neq 0$ automatically owing to Nakayama's Lemma **(10.6)**.

Lemma (23.5). — *Let R be a ring, M a nonzero Noetherian semilocal module.*

(1) *Then* $\operatorname{depth}(M) = 0$ *if and only if there's a maximal ideal* $\mathfrak{m} \in \operatorname{Ass}(M)$.

(2) *Then* $\operatorname{depth}(M) = 1$ *if and only if there's an* $x \in \operatorname{rad}(M)$ *with* $x \notin \operatorname{z.div}(M)$ *and there's a maximal ideal* $\mathfrak{m} \in \operatorname{Ass}(M/xM)$.

(3) *Then* $\operatorname{depth}(M) \le \dim(M)$.

Proof: Consider (1). First, if there's a maximal ideal $\mathfrak{m} \in \operatorname{Ass}(M)$, then the definitions readily yield $\operatorname{rad}(M) \subset \mathfrak{m} \subset \operatorname{z.div}(M)$, and so $\operatorname{depth}(M) = 0$.

Conversely, assume that $\operatorname{depth}(M) = 0$. Then $\operatorname{rad}(M) \subset \operatorname{z.div}(M)$. Since M is Noetherian, $\operatorname{z.div}(M) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(M)} \mathfrak{p}$ by **(17.12)**. Since M is nonzero and finitely generated, $\operatorname{Ass}(M)$ is nonempty and finite by **(17.10)** and **(17.17)**. So $\operatorname{rad}(M) \subset \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Ass}(M)$ by Prime Avoidance, **(3.12)**. But M is semilocal; so owing to its definition, $\operatorname{rad}(M)$ is the intersection finitely many maximal ideals $\mathfrak{m}$. So **(2.23)** yields an $\mathfrak{m} \subset \mathfrak{p}$. But $\mathfrak{m}$ is maximal. So $\mathfrak{m} = \mathfrak{p}$. Thus $\mathfrak{m} \in \operatorname{Ass}(M)$. Thus (1) holds.

Consider (2). Assume $\operatorname{depth}(M) = 1$. Then there is an M-sequence of length 1 in $\operatorname{rad}(M)$, but none longer; that is, there's an $x \in \operatorname{rad}(M)$ with $x \notin \operatorname{z.div}(M)$ and $\operatorname{depth}(M/xM) = 0$. Then (1) yields a maximal ideal $\mathfrak{m} \in \operatorname{Ass}(M/xM)$.

Conversely, assume there's $x \in \operatorname{Ass}(M)$ with $x \notin \operatorname{z.div}(M)$. Then by definition, $\operatorname{depth}(M) \ge 1$. Assume also there's a maximal ideal $\mathfrak{m} \in \operatorname{Ass}(M/xM)$. Then given any $y \in \operatorname{rad}(M)$ with $y \notin \operatorname{z.div}(M)$, also $\mathfrak{m} \in \operatorname{Ass}(M/yM)$ by **(17.19)**. So $\operatorname{depth}(M/yM) = 0$ by (1). So there is no $z \in \operatorname{rad}(M)$ such that y, z is an M-sequence. Thus $\operatorname{depth}(M) \le 1$. Thus $\operatorname{depth}(M) = 1$. Thus (2) holds.

Consider (3). Given any M-sequence $x_1, \ldots, x_n$, set $M_i := M/\langle x_1, \ldots, x_i \rangle M$. Then $M_{i+1} \xrightarrow{\sim} M_i/x_{i+1}M_i$ by **(23.4.1)**. Assume $x_i \in \operatorname{rad}(M)$ for all i. Then $\dim(M_{i+1}) = \dim(M_i) - 1$ by **(21.5)**. Hence $\dim(M) - n = \dim(M_n) \ge 0$. But $\operatorname{depth}(M) := \sup\{n\}$. Thus (3) holds. □

Theorem (23.6) (Characterization of DVRs). — *Let A be a local ring, $\mathfrak{m}$ its maximal ideal. Assume A is Noetherian. Then these five conditions are equivalent:*

(1) *A is a* DVR.

(2) *A is a normal domain of dimension* 1.

(3) *A is a normal domain of depth* 1.

(4) *A is a regular local ring of dimension* 1.

(5) *$\mathfrak{m}$ is principal and of height at least* 1.

Proof: Assume (1). Then A is UFD by **(23.1)**; so A is normal by **(10.21)**. Further, A has just two primes, $\langle 0 \rangle$ and $\mathfrak{m}$; so $\dim(A) = 1$. Thus (2) holds. Further, (4) holds by **(23.1)**. Clearly, (4) implies (5).

Assume (2). As $\dim(A) = 1$, there's $x \in \mathfrak{m}$ nonzero; $x \notin \operatorname{z.div}(A)$ as A is a domain. So $1 \le \operatorname{depth}(A)$. But $\operatorname{depth}(A) \le \dim(A)$ by **(23.5)**(3). Thus (3) holds.

Assume (3). By **(23.5)**(2), there are $x, y \in \mathfrak{m}$ such that x is nonzero and y has residue $\overline{y} \in A/\langle x \rangle$ with $\mathfrak{m} = \operatorname{Ann}(\overline{y})$. So $y\mathfrak{m} \subset \langle x \rangle$. Set $z := y/x \in \operatorname{Frac}(A)$. Then $z\mathfrak{m} = (y\mathfrak{m})/x \subset A$. Suppose $z\mathfrak{m} \subset \mathfrak{m}$. Then z is integral over A by **(10.14)**(4)⇒(1). But A is normal, so $z \in A$. So $y = zx \in \langle x \rangle$, a contradiction. Hence, $1 \in z\mathfrak{m}$; so there is $t \in \mathfrak{m}$ with $zt = 1$. Given $w \in \mathfrak{m}$, therefore $w = (wz)t$ with $wz \in A$. Thus

$\mathfrak{m}$ is principal. Finally, $\operatorname{ht}(\mathfrak{m}) \ge 1$ because $x \in \mathfrak{m}$ and $x \ne 0$. Thus (5) holds.

Assume (5). Set $N := \bigcap \mathfrak{m}^n$. The Krull Intersection Theorem **(18.23)** yields an $x \in \mathfrak{m}$ with $(1+x)N = 0$. Then $1 + x \in A^\times$. So $N = 0$. Further, A is a domain by **(21.10)**(1). Thus (1) holds by **(23.3)**. □

Exercise (23.7) . — Let R be a normal Noetherian domain, $x \in R$ a nonzero nonunit, $\mathfrak{a}$ an ideal. Show that every $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ has height 1. Conversely, if R is a UFD and if every $\mathfrak{p} \in \operatorname{Ass}(R/\mathfrak{a})$ has height 1, show that $\mathfrak{a}$ is principal.

Theorem (23.8) (Nagata)**.** — *Let $A \subset B$ be a faithfully flat extension of Noetherian local domains. Assume B is a UFD. Then so is A.*

Proof: By **(21.34)**, it suffices to show every height-1 prime $\mathfrak{p}$ of A is principal.

Let k and ℓ be the residue fields of A and B. Owing to **(10.8)**(2), $\mathfrak{p}$ is principal if and only if $\mathfrak{p} \otimes_A k \simeq k$; similarly, $\mathfrak{p}B$ is principal if and only if $(\mathfrak{p}B) \otimes_B \ell \simeq \ell$. But B is flat; so $\mathfrak{p}B = \mathfrak{p} \otimes_A B$ by **(9.15)**. But $\mathfrak{p} \otimes_A B \otimes_B \ell = \mathfrak{p} \otimes_A \ell = \mathfrak{p} \otimes_A k \otimes_k \ell$ by **(8.9)**(1). Hence $\mathfrak{p}$ is principal if and only if $\mathfrak{p}B$ is. But B is a UFD. Thus by **(23.7)**, it suffices to show every $\mathfrak{P} \in \operatorname{Ass}(B/\mathfrak{p}B)$ has height 1.

As B is faithfully flat, $\mathfrak{p}B \cap A = \mathfrak{p}$ by **(9.28)**(3). So $\mathfrak{P} \cap A \subset \mathfrak{p}$ owing to **(18.63)**(2) and **(18.17)**. Hence $\mathfrak{p} = \mathfrak{P} \cap A$. Set $S := A - \mathfrak{p}$. Then $S^{-1}\mathfrak{P} \in \operatorname{Ass}(S^{-1}(B/\mathfrak{p}B))$ by **(17.8)**. But $S^{-1}(B/\mathfrak{p}B) = S^{-1}B/\mathfrak{p}S^{-1}B$ by **(12.15)**. Thus it suffices to show every $\mathfrak{Q} \in \operatorname{Ass}(S^{-1}B/\mathfrak{p}S^{-1}B)$ has height 1.

Next, let's show $S^{-1}A$ is normal. Set $K := \operatorname{Frac}(A)$ and $L := \operatorname{Frac}(B)$. Then $K \subset L$ as $A \subset B$. Given $x/y \in K \cap B$ with $x, y \in A$, note $x \in yB \cap A$. But $yB \cap A = yA$ by **(9.28)**(3). Thus $K \cap B = A$. But B is a UFD, so normal by **(10.21)**. Hence A too is normal. Thus by **(11.32)** also $S^{-1}A$ is normal.

Recall $\mathfrak{p}$ has height 1. So $S^{-1}A$ has dimension 1. So $\mathfrak{p}S^{-1}A$ is principal by **(23.6)**(2)⇒(5). But $(\mathfrak{p}S^{-1}A)S^{-1}B = \mathfrak{p}S^{-1}B$. So $\mathfrak{p}S^{-1}B$ is principal. But B is normal, so $S^{-1}B$ is too by **(11.32)**. Thus by **(23.7)**, $\mathfrak{Q}$ has height 1, as desired. □

Exercise (23.9) . — Let A be a DVR with fraction field K, and $f \in A$ a nonzero nonunit. Prove A is a maximal proper subring of K. Prove $\dim(A) \ne \dim(A_f)$.

(23.10) (Serre's Conditions). — We say a ring R satisfies **Serre's Condition** (R_n) if, for any prime $\mathfrak{p}$ with height m with $m \le n$, the localization $R_\mathfrak{p}$ is regular of dimension m.

For example, (R_0) holds if and only if $R_\mathfrak{p}$ is a field for any minimal prime $\mathfrak{p}$. Also, (R_1) holds if and only if (R_0) does and $R_\mathfrak{p}$ is a DVR for any $\mathfrak{p}$ with height 1.

We say **Serre's Condition** (S_n) holds for a nonzero semilocal R-module M if

$$\operatorname{depth}(M_\mathfrak{p}) \ge \min\{\dim(M_\mathfrak{p}),\, n\} \quad \text{for any } \mathfrak{p} \in \operatorname{Supp}(M),$$

where $M_\mathfrak{p}$ is regarded as an $R_\mathfrak{p}$-module.

Assume M is Noetherian. Then $\operatorname{depth}(M_\mathfrak{p}) \le \dim(M_\mathfrak{p})$ by **(23.5)**(3). Thus (S_n) *holds if and only if* $\operatorname{depth}(M_\mathfrak{p}) = \dim(M_\mathfrak{p})$ *when* $\operatorname{depth}(M_\mathfrak{p}) < n$.

In particular, (S_1) holds if and only if $\mathfrak{p}$ is minimal whenever $\operatorname{depth}(M_\mathfrak{p}) = 0$. But $\operatorname{depth}(M_\mathfrak{p}) = 0$ and only if $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(M_\mathfrak{p})$ by **(23.5)**(1); so if and only if $\mathfrak{p} \in \operatorname{Ass}(M)$ by **(17.8)**. Thus (S_1) *holds if and only if M has no embedded primes.*

Exercise (23.11) . — Let R be a domain, M a Noetherian module. Show that M is torsionfree if and only if it satisfies (S_1).

Exercise (23.12) . — Let R be a Noetherian ring. Show that R is reduced if and only if (R_0) and (S_1) hold.

Lemma (23.13). — *Let R be a domain, M a nonzero torsionfree Noetherian module. Set $\Phi := \{\mathfrak{p}$ prime $| \operatorname{ht}(\mathfrak{p}) = 1\}$ and $\Sigma := \{\mathfrak{p}$ prime $| \operatorname{depth}(M_\mathfrak{p}) = 1\}$. Then $\Phi \subset \Sigma$, and $\Phi = \Sigma$ if and only if M satisfies (S_2). Further, $M = \bigcap_{\mathfrak{p}\in\Sigma} M_\mathfrak{p} \subset M_{\langle 0\rangle}$.*

Proof: By hypothesis, M is torsionfree. So given $s \in R$ and $m \in M$, if $s \neq 0$ but $sm = 0$, then $m = 0$. Thus, by construction, $M \subset M_\mathfrak{p} \subset M_{\langle 0\rangle}$ for all primes $\mathfrak{p}$.

So $\operatorname{Supp}(M) = \operatorname{Spec}(R)$ as $M \neq 0$. Thus $\dim(M_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p})$ for any $\mathfrak{p} \in \operatorname{Spec}(R)$.

So given $\mathfrak{p} \in \Phi$, we have $\dim(M_\mathfrak{p}) = 1$. So $\operatorname{depth}(M_\mathfrak{p}) \le 1$ by **(23.5)**(3). But if $\operatorname{depth}(M_\mathfrak{p}) = 0$, then $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}(M_\mathfrak{p})$ by **(23.5)**(1). So $\mathfrak{p} = \operatorname{Ann}(m)$ for some nonzero $m \in M$ by **(17.8)**. But M is torsionfree. So $\mathfrak{p} = \langle 0\rangle$, a contradiction. Thus $\operatorname{depth}(M_\mathfrak{p}) = 1$. Thus $\Phi \subset \Sigma$.

If M satisfies (S_2), then $\dim(M_\mathfrak{p}) = 1$ for any $\mathfrak{p} \in \Sigma$, so $\mathfrak{p} \in \Phi$; thus then $\Phi = \Sigma$.

Conversely, assume $\Phi = \Sigma$. Then given any prime $\mathfrak{p}$ with $\dim(M_\mathfrak{p}) \ge 2$, also $\operatorname{depth}(M_\mathfrak{p}) \ge 2$. But M satisfies (S_1) by **(23.11)**. Thus M satisfies (S_2).

We noted that $M \subset M_\mathfrak{p}$ for all primes $\mathfrak{p}$. Thus $M \subset \bigcap_{\mathfrak{p}\in\Sigma} M_\mathfrak{p}$.

Conversely, given $m \in \bigcap_{\mathfrak{p}\in\Sigma} M_\mathfrak{p}$, say $m = m'/s$ with $m' \in M$ and $s \in R - \langle 0\rangle$. Then $m' \in sM_\mathfrak{p}$ for all $\mathfrak{p} \in \Sigma$.

Given $\mathfrak{p} \in \operatorname{Ass}(M/sM)$, note $\mathfrak{p}R_\mathfrak{p} \in \operatorname{Ass}((M/sM)_\mathfrak{p})$ by **(17.8)**. But by **(12.15)**, $(M/sM)_\mathfrak{p} = M_\mathfrak{p}/sM_\mathfrak{p}$. Also, $s \in \mathfrak{p}$ and $s \notin \operatorname{z.div}(M_\mathfrak{p})$. Thus **(23.5)**(2) gives $\mathfrak{p} \in \Sigma$.

Note $sM = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(M/sM)} sM_\mathfrak{p}$ by **(18.65)**(2) applied with $N = sM$. Hence

$$sM = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(M/sM)} sM_\mathfrak{p} \supset \bigcap_{\mathfrak{p}\in\Sigma} sM_\mathfrak{p} \supset sM.$$

Thus $sM = \bigcap_{\mathfrak{p}\in\Sigma} sM_\mathfrak{p}$. Hence $m' \in sM$. So $m' = sm''$ for some $m'' \in M$. So $m = m'' \in M$. Thus $M \supset \bigcap_{\mathfrak{p}\in\Sigma} M_\mathfrak{p}$, as desired. □

Theorem (23.14). — *Let R be a normal Noetherian domain. Then*

$$R = \bigcap\nolimits_{\mathfrak{p}\in\Phi} R_\mathfrak{p} \quad \textit{where} \quad \Phi := \{\,\mathfrak{p}\ \textit{prime} \mid \operatorname{ht}(\mathfrak{p}) = 1\,\}.$$

Proof: As R is normal, so is $R_\mathfrak{p}$ for any prime $\mathfrak{p}$ by **(11.32)**. So $\operatorname{depth}(R_\mathfrak{p}) = 1$ if and only if $\dim(R_\mathfrak{p}) = 1$ by **(23.6)**. Thus **(23.13)** yields the assertion. □

Theorem (23.15) (Serre's Criterion). — *Let R be a Noetherian domain. Then R is normal if and only if (R_1) and (S_2) hold.*

Proof: As R is a domain, (R_0) and (S_1) hold by **(23.12)**. If R is normal, then so is $R_\mathfrak{p}$ for any prime $\mathfrak{p}$ by **(11.32)**; whence, (R_1) and (S_2) hold by **(23.6)**.

Conversely, assume R satisfies (R_1) and (S_2). Let x be integral over R. Then x is integral over $R_\mathfrak{p}$ for any prime $\mathfrak{p}$. Now, $R_\mathfrak{p}$ is a DVR for all $\mathfrak{p}$ of height 1 as R satisfies (R_1). Hence, $x \in R_\mathfrak{p}$ for all $\mathfrak{p}$ of height 1, so for all $\mathfrak{p}$ of depth 1 as R satisfies (S_2). So $x \in R$ owing to **(23.13)**. Thus R is normal. □

B. Exercises

Exercise (23.16) . — Show an equicharacteristic regular local ring A is a UFD.

Exercise (23.17) . — Let R be a ring, $0 \to N \to M \to L \to 0$ a short exact sequence, and $x_1, \dots, x_n \in R$. Set $\mathfrak{a}_i : \langle x_1, \dots, x_i \rangle$ for $0 \le i \le n$. Prove:

(1) Assume $x_1, \dots, x_n$ is L-regular. Then $\mathfrak{a}_i M \cap N \mathfrak{a}_i N$ for $0 \le i \le n$.
(2) Then $x_1, \dots, x_n$ is both N-regular and L-regular if and only if $x_1, \dots, x_n$ is M-regular, $\mathfrak{a}_i M \cap N = \mathfrak{a}_i N$ for $0 \le i \le n$, and $N/\mathfrak{a}_n N \ne 0$ and $L/\mathfrak{a}_n L \ne 0$.

Exercise (23.18) . — Let R be a ring, M a module, $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ a left-exact functor. Assume $F(M)$ is nonzero and finitely generated. Show that, for $d = 1, 2$, if M has depth at least d, then so does $F(M)$.

Exercise (23.19) . — Let k be a field, A a ring intermediate between the polynomial ring and the formal power series ring in one variable: $k[X] \subset A \subset k[[X]]$. Suppose that A is local with maximal ideal $\langle X \rangle$. Prove that A is a DVR. (Such local rings arise as rings of power series with curious convergence conditions.)

Exercise (23.20) . — Let L/K be an algebraic extension of fields; $X_1, \dots, X_n$ variables; P and Q the polynomial rings over K and L in $X_1, \dots, X_n$. Prove this:

(1) Let $\mathfrak{q}$ be a prime of Q, and $\mathfrak{p}$ its contraction in P. Then $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q})$.
(2) Let $F, G \in P$ be two polynomials with no common prime factor in P. Then F and G have no common prime factor $H \in Q$.

Exercise (23.21) . — Prove that a Noetherian domain R is normal if and only if, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_{\mathfrak{p}}$ is principal.

Exercise (23.22) . — Let R be a ring, M a nonzero Noetherian module. Set

$$\Phi := \{\, \mathfrak{p} \text{ prime} \mid \dim(M_{\mathfrak{p}}) = 1 \,\} \quad \text{and} \quad \Sigma := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{depth}(M_{\mathfrak{p}}) = 1 \,\}.$$

Assume M satisfies (S_1). Show $\Phi \subset \Sigma$, with equality if and only if M satisfies (S_2).
Set $S := R - \operatorname{z.div}(M)$. Without assuming (S_1), show this sequence is exact:

$$M \to S^{-1}M \to \textstyle\prod_{\mathfrak{p} \in \Sigma} S^{-1}M_{\mathfrak{p}}/M_{\mathfrak{p}}. \tag{23.22.1}$$

Exercise (23.23) (*Serre's Criterion*) . — Let R be a Noetherian ring, and K its total quotient ring. Set $\Phi := \{\, \mathfrak{p} \text{ prime} \mid \operatorname{ht}(\mathfrak{p}) = 1 \,\}$. Prove equivalent:

(1) R is normal.
(2) (R_1) and (S_2) hold.
(3) (R_1) and (S_1) hold, and $R \to K \to \prod_{\mathfrak{p} \in \Phi} K_{\mathfrak{p}}/R_{\mathfrak{p}}$ is exact.

C. Appendix: M-sequences

Exercise (23.24) . — Let R be a ring, M a module, and x, y an M-sequence.

(1) Given $m, n \in M$ with $xm = yn$, find $p \in M$ with $m = yp$ and $n = xp$.
(2) Assume $y \notin \operatorname{z.div}(M)$. Show y, x is an M-sequence too.

Proposition (23.25). — *Let R be a ring, M a nonzero Noetherian module, and $x, y \in \operatorname{rad}(M)$. Assume that, given any $m, n \in M$ with $xm = yn$, there exists $p \in M$ with $m = yp$ and $n = xp$. Then x, y is an M-sequence.*

Proof: First, as noted in **(23.4)**, automatically $M/\langle x,y\rangle M \neq 0$.

Next, we have to prove $x \notin \operatorname{z.div}(M)$. Given $m \in M$ with $xm = 0$, set $n := 0$. Then $xm = yn$; so there exists $p \in M$ with $m = yp$ and $n = xp$. Repeat with p in place of m, obtaining $p_1 \in M$ such that $p = yp_1$ and $0 = xp_1$. Induction yields $p_i \in M$ for $i \geq 2$ such that $p_{i-1} = yp_i$ and $0 = xp_i$. Note $m = p^{i+1}p_i$ for all i.

Then $Rp_1 \subset Rp_2 \subset \cdots$ is an ascending chain. It stabilizes as M is Noetherian. Say $Rp_n = Rp_{n+1}$. So $p_{n+1} = zp_n$ for some $z \in R$. Then $p_n = yp_{n+1} = yzp_n$. So $(1 - yz)p_n = 0$. Set $R' := R/\operatorname{Ann}(M)$, and let y', $z' \in R'$ be the residues of y, z.

But $y \in \operatorname{rad}(M)$. Also $\operatorname{rad}(M)/\operatorname{Ann}(M) = \operatorname{rad}(R')$ by **(4.1.1)**. Hence $1 - y'z'$ is a unit by **(3.2)**. But $(1-y'z')p_n = (1-yz)p_n = 0$. Hence $p_n = 0$. But $m = y^{n+1}p_n$. Thus $m = 0$, as desired. Thus $x \notin \operatorname{z.div}(M)$.

Finally, set $M_1 := M/xM$. We must prove $y \notin \operatorname{z.div}(M_1)$. Given $n_1 \in M_1$ with $yn_1 = 0$, lift n_1 to $n \in M$. Then $yn = xm$ for some $m \in M$. So there's $p \in M$ with $n = xp$. Thus $n_1 = 0$, as desired. Thus x, y is an M-sequence, as desired. □

Exercise (23.26) . — Let R be a ring, $\mathfrak{a} \subset R$ an ideal, M a module, $x_1, \ldots, x_r$ an M-sequence in $\mathfrak{a}$, and R' an algebra. Set $M' := M \otimes_R R'$. Assume R' flat and $M'/\mathfrak{a}M' \neq 0$. Prove $x_1, \ldots, x_r$ is an M'-sequence in $\mathfrak{a}R'$.

Exercise (23.27) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module with $M/\mathfrak{a}M \neq 0$. Let $x_1, \ldots, x_r$ be an M-sequence in $\mathfrak{a}$, and $\mathfrak{p} \in \operatorname{Supp}(M/\mathfrak{a}M)$. Prove: (1) $x_1/1, \ldots, x_r/1$ is an $M_\mathfrak{p}$-sequence in $\mathfrak{a}_\mathfrak{p}$, and (2) $\operatorname{depth}(\mathfrak{a}, M) \leq \operatorname{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p})$.

(23.28) (Maximal sequences). — Let R be a ring, $\mathfrak{a}$ an ideal, M a nonzero module. We say an M-sequence in $\mathfrak{a}$ is **maximal in** $\mathfrak{a}$, if it can not be lengthened in $\mathfrak{a}$.

In particular, the sequence of length 0 (the empty sequence) is maximal in $\mathfrak{a}$ if and only if there are no nonzerodivisors on M in $\mathfrak{a}$, that is, $\mathfrak{a} \subset \operatorname{z.div}(M)$.

Theorem (23.29). — *Let R be a ring, $\mathfrak{a}$ an ideal, and M a Noetherian module. Then there exists a finite maximal M-sequence in $\mathfrak{a}$ if and only if $M/\mathfrak{a}M \neq 0$. If so, then any finite M-sequence in $\mathfrak{a}$ can be lengthened until maximal in $\mathfrak{a}$, and every maximal M-sequence in $\mathfrak{a}$ is of the same length, namely,* $\operatorname{depth}(\mathfrak{a}, M)$.

Proof: First, assume $M/\mathfrak{a}M \neq 0$. Then there's $\mathfrak{p} \in \operatorname{Supp}(M/\mathfrak{a}M)$ by **(13.8)**. Hence successively **(23.27)**(2) and **(23.5)**(3) and **(21.4)** yield

$$\operatorname{depth}(\mathfrak{a}, M) \leq \operatorname{depth}(M_\mathfrak{p}) \leq \dim(M_\mathfrak{p}) < \infty.$$

However, every M-sequence in $\mathfrak{a}$ is of length at most $\operatorname{depth}(\mathfrak{a}, M)$ by **(23.4)**. Hence the M-sequences in $\mathfrak{a}$ are of bounded length. Thus in finitely many steps, any one can be lengthened until maximal in $\mathfrak{a}$. In particular, the empty sequence can be so lengthened. Thus there exists a finite maximal M-sequence in $\mathfrak{a}$.

Instead, assume there exists a finite maximal M-sequence $x_1, \ldots, x_m$ in $\mathfrak{a}$. Set $M_i := M/\langle x_1, \ldots, x_i\rangle M$ for all i. Suppose $M_m = \mathfrak{a}M_m$. Then there's $a \in \mathfrak{a}$ with $(1 + a)M = 0$ by **(10.3)**. But $\mathfrak{a} \subset \operatorname{z.div}(M_m)$ by maximality. So $a\mu = 0$ for some nonzero $\mu \in M_m$. So $\mu + a\mu = 0$. So $\mu = 0$, a contradiction. Hence $M_m/\mathfrak{a}M_m \neq 0$. But $M_m/\mathfrak{a}M_m$ is a quotient of $M/\mathfrak{a}M$. Thus $M/\mathfrak{a}M \neq 0$.

Given any other maximal M-sequence $y_1, \ldots, y_n$ in $\mathfrak{a}$, it now suffices to prove $m = n$. Indeed, then $m = \operatorname{depth}(\mathfrak{a}, M)$ by **(23.4)**, completing the proof.

To prove $m = n$, induct on m. If $m = 0$, then $\mathfrak{a} \subset \operatorname{z.div}(M)$, and so $n = 0$ too.

Assume $m \geq 1$. Set $N_j := M/\langle y_1, \ldots, y_j\rangle M$ for all j, and set

$$U := \textstyle\bigcup_{i=0}^{m-1} \operatorname{z.div}(M_i) \cup \bigcup_{j=0}^{n-1} \operatorname{z.div}(N_j).$$

Then U is equal to the union of all associated primes of M_i for $i < m$ and of N_j for $j < n$ by **(17.12)**. And these primes are finite in number by **(17.17)**.

Suppose $\mathfrak{a} \subset U$. Then $\mathfrak{a}$ lies in one of the primes, say $\mathfrak{p} \in \mathrm{Ass}(M_i)$, by **(3.12)**. But $x_{i+1} \in \mathfrak{a} - \mathrm{z.div}(M_i)$ and $\mathfrak{a} \subset \mathfrak{p} \subset \mathrm{z.div}(M_i)$, a contradiction. Thus $\mathfrak{a} \not\subset U$.

Take $z \in \mathfrak{a} - U$. Then $z \notin \mathrm{z.div}(M_i)$ for $i < m$ and $z \notin \mathrm{z.div}(N_j)$ for $j < n$. In particular, $x_1, \ldots, x_{m-1}, z$ and $y_1, \ldots, y_{n-1}, z$ are M-regular.

By maximality, $\mathfrak{a} \subset \mathrm{z.div}(M_m)$. So $\mathfrak{a} \subset \mathfrak{q}$ for some $\mathfrak{q} \in \mathrm{Ass}(M_m)$ by **(17.12)** and **(3.12)**. But $M_m = M_{m-1}/x_m M_{m-1}$ by **(23.4.1)**. Also, $x_m,\, z \notin \mathrm{z.div}(M_{m-1})$. Further, $x_m,\, z \in \mathfrak{a} \subset \mathfrak{q}$. So $\mathfrak{q} \in \mathrm{Ass}(M_{m-1}/zM_{m-1})$ by **(17.19)**. Hence

$$\mathfrak{a} \subset \mathrm{z.div}(M/\langle x_1, \ldots, x_{m-1}, z\rangle M).$$

Thus $x_1, \ldots, x_{m-1}, z$ is maximal in $\mathfrak{a}$. Similarly, $y_1, \ldots, y_{n-1}, z$ is maximal in $\mathfrak{a}$.

Note $M_{m-1} = M_{m-2}/x_{m-1}M_{m-2}$ by **(23.4.1)**. Hence x_{m-1}, z is M_{m-2}-regular. However, $z \notin \mathrm{z.div}(M_{m-2})$. So z, x_{m-1} is M_{m-2}-regular by **(23.24)**(2). Therefore, $x_1, \ldots, x_{m-2}, z, x_{m-1}$ is a maximal M-regular sequence in $\mathfrak{a}$. Continuing shows that $z, x_1, \ldots, x_{m-1}$ is one too. Similarly, $z, y_1, \ldots, y_{n-1}$ is another one.

Thus we may assume $x_1 = y_1$. Then $M_1 = N_1$. Further, $x_2, \ldots, x_m$ and $y_2, \ldots, y_n$ are maximal M_1-sequences in $\mathfrak{a}$. So by induction, $m - 1 = n - 1$. Thus $m = n$. □

Example (23.30). — For any $n \ge 0$, here's an example of a Noetherian local ring R_n of depth n that does not satisfy (S_1), so not (S_n). Let $R := k[[X, Y]]/\langle XY, Y^2\rangle$ be the local ring of **(17.2)**. Take additional variables $Z_1, \ldots, Z_n$. Set $R_0 := R$ and $R_n := R[[Z_1, \ldots, Z_n]]$ if $n \ge 1$. By **(22.27)**, R_n is a Noetherian local ring.

If $n \ge 1$, then Z_n is a nonzerodivisor on R_n. But $R_n = R_{n-1}[[Z_n]]$. So **(3.7)** yields $R_n/\langle Z_n\rangle = R_{n-1}$. Thus $Z_1, \ldots, Z_n$ is an R_n-sequence by induction on n.

Set $\mathfrak{m} := \langle x, y, Z_1, \cdots, Z_n\rangle \subset R_n$ where x, y are the residues of X, Y. Then $\mathfrak{m} \subset \mathrm{z.div}_{R_n}(R_0)$. So $Z_1, \ldots, Z_n$ is a maximal R_n-sequence in $\mathfrak{m}$. Thus **(23.29)** yields $\mathrm{depth}(R_n) = n$.

Set $P := k[[X, Y, Z_1, \ldots, Z_n]]$, Then P is a power series ring in $n + 2$ variables. The ideals $\langle Y\rangle$ and $\langle X, Y\rangle$ are prime by **(22.27)**. Set $\mathfrak{a} := \langle XY, Y^2\rangle$. Then $P/\mathfrak{a}P = R_n$ by **(22.56)**. Thus $\langle y\rangle$ and $\langle x, y\rangle$ are prime ideals of R_n.

Plainly $\langle x, y\rangle \subset \mathrm{Ann}(y)$. Given $F \in R_n$, say $F = \sum a_{ij}x^iy^jF_{ij}$ with $a_{ij} \in k$ and $F_{ij} \in k[[Z_1, \ldots, Z_n]]$. Assume $F \in \mathrm{Ann}(y)$. Then $\sum a_{ij}x^iy^{j+1}F_{ij} = 0$. So $\sum a_{ij}X^iY^{j+1}F_{ij} \in \mathfrak{a}$. Hence $a_{00}YF_{00} \in \mathfrak{a}$. So $a_{00}F_{00} = 0$. So $F \in \langle x, y\rangle$. Thus $\langle x, y\rangle = \mathrm{Ann}(y)$. But $\langle x, y\rangle$ is prime. Thus $\langle x, y\rangle \in \mathrm{Ass}(R_n)$.

Plainly $\langle y\rangle \subset \mathrm{Ann}(x)$. Assume $F \in \mathrm{Ann}(x)$. Then $\sum a_{ij}x^{i+1}y^jF_{ij} = 0$. So $\sum a_{ij}X^{i+1}Y^jF_{ij} \in \mathfrak{a}$. So $a_{i0}X^iF_{i0} \in \mathfrak{a}$ for all i as $\mathfrak{a}$ is homogeneous. So $a_{i0}x^iF_{i0}$ is 0. So $F \in \langle y\rangle$. Thus $\langle y\rangle = \mathrm{Ann}(x)$. But $\langle y\rangle$ is prime. Thus $\langle y\rangle \in \mathrm{Ass}(R_n)$. So $\langle x, y\rangle$ is an embedded prime of R_n. Thus **(23.10)** implies R_n doesn't satisfy (S_1).

Exercise (23.31) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module with $M/\mathfrak{a}M \ne 0$, and $x \in \mathfrak{a} - \mathrm{z.div}(M)$. Show $\mathrm{depth}(\mathfrak{a},\, M/xM) = \mathrm{depth}(\mathfrak{a},\, M) - 1$.

Exercise (23.32) . — Let R be a ring, M a nonzero Noetherian semilocal module, and $x \in \mathrm{rad}(M) - \mathrm{z.div}(M)$. Show that $\mathrm{depth}(M) = \dim(M)$ if and only if $\mathrm{depth}(M/xM) = \dim(M/xM)$.

Exercise (23.33) . — Let R be a ring, R' an algebra, and N a nonzero R'-module that's a Noetherian R-module. Assume N is semilocal over R (or equivalently by **(21.20)**(5), semilocal over R'). Show $\mathrm{depth}_R(N) = \mathrm{depth}_{R'}(N)$.

Proposition (23.34). — *Let $R \to R'$ be a map of rings, $\mathfrak{a} \subset R$ an ideal, and M an R-module with $M/\mathfrak{a}M \neq 0$. Set $M' := M \otimes_R R'$. Assume R' is faithfully flat over R, and M and M' are Noetherian. Then* $\operatorname{depth}(\mathfrak{a}R', M') = \operatorname{depth}(\mathfrak{a}, M)$.

Proof: By **(23.29)**, there is a maximal M-sequence $x_1, \ldots, x_r$ in $\mathfrak{a}$. For all i, set $M_i := M/\langle x_1, \ldots, x_i\rangle M$ and $M_i' := M'/\langle x_1, \ldots, x_i\rangle M'$. By **(8.10)**, we have

$$M'/\mathfrak{a}M' = M/\mathfrak{a}M \otimes_R R' \quad \text{and} \quad M_i' = M_i \otimes_R R'.$$

So $M'/\mathfrak{a}M' \neq 0$ by faithful flatness. Hence $x_1, \ldots, x_r$ is an M'-sequence by **(23.26)**.
Since $x_1, \ldots, x_r$ is maximal, $\mathfrak{a} \subset \operatorname{z.div}(M_r)$. Therefore, $\operatorname{Hom}_R(R/\mathfrak{a}, M_r) \neq 0$ by **(17.20)**(3)⇐(5). So $\operatorname{Hom}_R(R/\mathfrak{a}, M_r) \otimes_R R' \neq 0$ by faithful flatness. But **(9.10)** and **(8.9)**(2) yield

$$\operatorname{Hom}_R(R/\mathfrak{a}, M_r) \otimes_R R' \hookrightarrow \operatorname{Hom}_R(R/\mathfrak{a}, M_r') = \operatorname{Hom}_{R'}(R'/\mathfrak{a}R', M_r').$$

So $\operatorname{Hom}_{R'}(R'/\mathfrak{a}R', M_r') \neq 0$. So $\mathfrak{a}R' \subset \operatorname{z.div}(M_r')$ by **(17.20)**. So $x_1, \ldots, x_r$ is a maximal M'-sequence in $\mathfrak{a}R'$. Thus **(23.29)** yields the assertion. □

Lemma (23.35). — *Let R be a ring, $\mathfrak{a}$ an ideal, M a nonzero Noetherian module, $x \in \operatorname{rad}(M) - \operatorname{z.div}(M)$. Assume $\mathfrak{a} \subset \operatorname{z.div}(M)$. Set $M' := M/xM$. Then there is $\mathfrak{p} \in \operatorname{Ass}(M')$ with $\mathfrak{p} \supset \mathfrak{a}$.*

Proof: Set $\mathfrak{a}' := \operatorname{Ann}(M)$ and $\mathfrak{q} := \mathfrak{a} + \mathfrak{a}'$. Given any $a \in \mathfrak{a}$, there's a nonzero $m \in M$ with $am = 0$. So given any $a' \in \mathfrak{a}'$, also $(a + a')m = 0$. Thus $\mathfrak{q} \subset \operatorname{z.div}(M)$.
Set $R' := R/\mathfrak{a}'$. Then R' is Noetherian by **(16.16)**. Set $N := R/\mathfrak{q}$. Then N is a quotient of R'. Thus N is Noetherian.
Set $H := \operatorname{Hom}(N, M)$. Then H is Noetherian by **(16.37)**. Also $\operatorname{Supp}(N) = \mathbf{V}(\mathfrak{q})$ by **(13.4)**(3). But $\mathfrak{q} \subset \operatorname{z.div}(M)$. So $H \neq 0$ by **(17.20)**. Further, $\mathfrak{a}' \subset \operatorname{Ann}(H)$; so $\operatorname{rad}(M) \subset \operatorname{rad}(H)$. So Nakayama's Lemma **(10.6)** yields $H/xH \neq 0$.
As $0 \to M \xrightarrow{\mu_x} M \to M' \to 0$ is exact, so is $0 \to H \xrightarrow{\mu_x} H \to \operatorname{Hom}(N, M')$ by **(5.11)**(2). Hence, $H/xH \subset \operatorname{Hom}(N, M')$. So $\operatorname{Hom}(N, M') \neq 0$. Thus **(17.20)** yields $\mathfrak{p} \in \operatorname{Ass}(M')$ with $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{a}$. □

Lemma (23.36). — *Let R be a ring, $M \neq 0$ a Noetherian module, $\mathfrak{p}_0 \in \operatorname{Ass}(M)$, $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ a maximal chain of primes. Then* $\operatorname{depth}(\mathfrak{p}_r, M) \le \operatorname{depth}(M_{\mathfrak{p}_r}) \le r$.

Proof: If $r = 0$, then $\mathfrak{p}_0 \subset \operatorname{z.div}(M)$. So $\operatorname{depth}(\mathfrak{p}_0, M) = 0$, as desired. Induct on r. Assume $r \ge 1$. As $\mathfrak{p}_0 \in \operatorname{Ass}(M)$, we have $\mathfrak{p}_r \in \operatorname{Supp}(M)$ by **(17.13)**; so $M_{\mathfrak{p}_r} \neq 0$. So Nakayama's Lemma **(10.6)** yields $M_{\mathfrak{p}_r}/\mathfrak{p}_r M_{\mathfrak{p}_r} \neq 0$. Further, $\operatorname{depth}(\mathfrak{p}_r, M) \le \operatorname{depth}(M_{\mathfrak{p}_r})$ by **(23.27)**(2). So localizing at $\mathfrak{p}_r$, we may assume R is local, $\mathfrak{p}_r$ is the maximal ideal, and $M = M_{\mathfrak{p}_r}$. Then $\operatorname{depth}(\mathfrak{p}_r, M) = \operatorname{depth}(M)$.
As $\mathfrak{p}_{r-1} \subset \mathfrak{p}_r$, clearly $M/\mathfrak{p}_{r-1}M \neq 0$. So **(23.29)**, yields a maximal M-sequence $x_1, \ldots, x_s$ in $\mathfrak{p}_{r-1}$ where $s = \operatorname{depth}(\mathfrak{p}_{r-1}, M)$. So by induction $s \le r - 1$. Set $M_s := M/\langle x_1, \ldots, x_s\rangle M$. Then $\mathfrak{p}_{r-1} \subset \operatorname{z.div}(M_s)$ by maximality.
Suppose $\mathfrak{p}_r \subset \operatorname{z.div}(M_s)$. Then $x_1, \ldots, x_s$ is maximal in $\mathfrak{p}_r$. So $s = \operatorname{depth}(M)$ by **(23.29)**, as desired.
Suppose instead $\mathfrak{p}_r \not\subset \operatorname{z.div}(M_s)$. Then there's $x \in \mathfrak{p}_r - \operatorname{z.div}(M_s)$. So $x_1, \ldots, x_s, x$ is an M-sequence in $\mathfrak{p}_r$. By **(23.35)**, there is $\mathfrak{p} \in \operatorname{Ass}(M_s/xM_s)$ with $\mathfrak{p} \supset \mathfrak{p}_{r-1}$. But $\mathfrak{p} = \operatorname{Ann}(m)$ for some $m \in M_s/xM_s$, so $x \in \mathfrak{p}$. Hence $\mathfrak{p}_{r-1} \subsetneqq \mathfrak{p} \subset \mathfrak{p}_r$. Hence, by hypothesis, $\mathfrak{p} = \mathfrak{p}_r$. Hence $x_1, \ldots, x_s, x$ is maximal in $\mathfrak{p}_r$ as $\mathfrak{p}_r = \operatorname{Ann}(m)$. So **(23.29)** yields $s + 1 = \operatorname{depth}(M)$. Thus $\operatorname{depth}(M) \le r$, as desired. □

Theorem (23.37) (Unmixedness). — *Let R be a ring, M a nonzero Noetherian semilocal module. Assume* $\operatorname{depth}(M) = \dim(M)$*. Then M has no embedded primes, and all maximal chains of primes in* $\operatorname{Supp}(M)$ *are of length* $\dim(M)$*.*

Proof: Given $\mathfrak{p}_0 \in \operatorname{Ass}(M)$, take any maximal chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$. Then $\mathfrak{p}_r$ is a maximal ideal in $\operatorname{Supp}(M)$. So $\mathfrak{p}_r \supset \operatorname{rad}(M)$ by **(13.4)**(4). So **(23.29)** yields $\operatorname{depth}(M) \le \operatorname{depth}(\mathfrak{p}_r, M)$. But **(23.36)** yields $\operatorname{depth}(\mathfrak{p}_r, M) \le r$. Also $\operatorname{depth}(M) = \dim(M)$. Moreover, $r \le \dim(M)$ by definition **(21.1)**. So $r = \dim(M)$. Hence $\mathfrak{p}_0$ is minimal. Thus M has no embedded primes.

Given any maximal chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in $\operatorname{Supp}(M)$, necessarily $\mathfrak{p}_0$ is minimal. So $\mathfrak{p}_0 \in \operatorname{Ass}(M)$ by **(17.14)**. Thus, as above, $r = \dim(M)$, as desired. □

Proposition (23.38). — *Let R be a ring, M a nonzero Noetherian semilocal module, and $x_1, \ldots, x_n \in \operatorname{rad}(M)$. Set $M_i := M/\langle x_1, \ldots, x_i\rangle M$ for all i. Assume* $\operatorname{depth}(M) = \dim(M)$*. Then $x_1, \ldots, x_n$ is M-regular if and only if it is part of a sop; if so, then* $\operatorname{depth}(M_i) = \dim(M_i)$ *for all i.*

Proof: Assume $x_1, \ldots, x_n$ is M-regular. Then $\operatorname{depth}(M_i) = \dim(M_i)$ for all i by **(23.32)** and **(23.4.1)** applied inductively. Moreover, $x_1, \ldots, x_n$ can be extended to a maximal M-sequence by **(23.29)**; so assume it is already maximal. Then $\operatorname{depth}(M_n) = 0$. Hence $\dim(M_n) = 0$. Thus $x_1, \ldots, x_n$ is a sop.

Conversely, assume $x_1, \ldots, x_n$ is part of a sop $x_1, \ldots, x_s$. Induct on n. If n is 0, there is nothing to prove. Assume $n \ge 1$. By induction $x_1, \ldots, x_{n-1}$ is M-regular. So as above, $\operatorname{depth}(M_{n-1}) = \dim(M_{n-1})$. Thus, by **(23.37)**, M_{n-1} has no embedded primes, and $\dim(R/\mathfrak{p}) = \dim(M_{n-1})$ for all minimal primes $\mathfrak{p}$ of M_{n-1}.

However, $\dim(M_n) = \dim(M_{n-1}) - 1$ by **(21.26)**. Also $M_n \xrightarrow{\sim} M_{n-1}/x_n M_{n-1}$ by **(23.4.1)**. Hence x_n lies in no minimal prime of M_{n-1} by **(21.5)**. But M_{n-1} has no embedded primes. So $x_n \notin \mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Ass}(M_{n-1})$. So $x_n \notin \operatorname{z.div}(M_{n-1})$ by **(17.12)**. Thus $x_1, \ldots, x_n$ is M-regular. □

Proposition (23.39). — *Let R be a ring, M a Noetherian semilocal module, $\mathfrak{p}$ in* $\operatorname{Supp}(M)$*. If* $\operatorname{depth}(M) = \dim(M)$*, then* $\operatorname{depth}(\mathfrak{p}, M) = \operatorname{depth}(M_{\mathfrak{p}}) = \dim(M_{\mathfrak{p}})$*.*

Proof: Set $s := \operatorname{depth}(\mathfrak{p}, M)$. Induct on s. Assume $s = 0$. Then $\mathfrak{p} \subset \operatorname{z.div}(M)$. So $\mathfrak{p}$ lies in some $\mathfrak{q} \in \operatorname{Ass}(M)$ by **(17.20)**. But $\mathfrak{q}$ is minimal in $\operatorname{Supp}(M)$ by **(23.37)**. So $\mathfrak{q} = \mathfrak{p}$. Hence $\dim(M_{\mathfrak{p}}) = 0$. Thus **(23.5)**(3) yields $\operatorname{depth}(M_{\mathfrak{p}}) = \dim(M_{\mathfrak{p}}) = 0$.

Assume $s \ge 1$. Then there is $x \in \mathfrak{p} - \operatorname{z.div}(M)$. Set $M' := M/xM$, and set $s' := \operatorname{depth}(\mathfrak{p}, M')$. As $M_{\mathfrak{p}} \ne 0$, also $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \ne 0$ owing to **(10.6)**. But $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} = (M/\mathfrak{p}M)_{\mathfrak{p}}$ by **(12.15)**. So $M/\mathfrak{p}M \ne 0$. Thus $s' = s - 1$ by **(23.31)**, and $\operatorname{depth}(M') = \dim(M')$ by **(23.32)**.

Further, $M'_{\mathfrak{p}} = M_{\mathfrak{p}}/xM_{\mathfrak{p}}$ by **(12.15)**. But $x \in \mathfrak{p}$. So $M'_{\mathfrak{p}} \ne 0$ by Nakayama's Lemma **(10.6)**. Thus $\mathfrak{p} \in \operatorname{Supp}(M')$. So by induction, $\operatorname{depth}(M'_{\mathfrak{p}}) = \dim(M'_{\mathfrak{p}}) = s'$.

As $x \notin \operatorname{z.div}(M)$, also $x/1 \notin \operatorname{z.div}(M_{\mathfrak{p}})$ by **(23.27)**(1). But $x/1 \in \mathfrak{p}R_{\mathfrak{p}}$ and $\mathfrak{p}R_{\mathfrak{p}} = \operatorname{rad}(M_{\mathfrak{p}})$. Hence $\operatorname{depth}(M_{\mathfrak{p}}) = \dim(M_{\mathfrak{p}})$ by **(23.32)**. Finally, $\dim(M_{\mathfrak{p}}) = s$ by **(21.5)**. □

Exercise (23.40) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a Noetherian module with $M/\mathfrak{a}M \ne 0$. Find a maximal ideal $\mathfrak{m} \in \operatorname{Supp}(M/\mathfrak{a}M)$ with

$$\operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(\mathfrak{a}_{\mathfrak{m}},\, M_{\mathfrak{m}}).$$

Definition (23.41). — Let R be a ring. A nonzero Noetherian module M is called **Cohen–Macaulay** if $\operatorname{depth}(M_{\mathfrak{m}}) = \dim(M_{\mathfrak{m}})$ for all maximal ideals $\mathfrak{m} \in \operatorname{Supp}(M)$.

It's equivalent that $\operatorname{depth}(\mathfrak{m}, M) = \dim(M_{\mathfrak{m}})$ for all $\mathfrak{m}$ by (**23.40**) with $\mathfrak{a} := \mathfrak{m}$.

It's equivalent that $M_{\mathfrak{p}}$ be a Cohen–Macaulay $R_{\mathfrak{p}}$-module for all $\mathfrak{p} \in \operatorname{Supp}(M)$, since if $\mathfrak{p}$ lies in the maximal ideal $\mathfrak{m}$, then $M_{\mathfrak{p}}$ is the localization of $M_{\mathfrak{m}}$ at the prime ideal $\mathfrak{p}R_{\mathfrak{m}}$ by (**12.25**)(3), and hence $M_{\mathfrak{p}}$ is Cohen–Macaulay if $M_{\mathfrak{m}}$ is by (**23.39**).

The ring R is called **Cohen–Macaulay** if R is so as an R-module.

Exercise (23.42) . — Let R be a ring, and M a nonzero Noetherian semilocal module. Set $d := \dim(M)$. Show $\operatorname{depth}(M) = d$ if and only if M is Cohen–Macaulay and $\dim(M_{\mathfrak{m}}) = d$ for all maximal $\mathfrak{m} \in \operatorname{Supp}(M)$.

Proposition (23.43). — *Let R be a ring, and M a module. Then M is Cohen–Macaulay if and only if the polynomial module $M[X]$ is so over $R[X]$.*

Proof: First, assume $M[X]$ is Cohen–Macaulay. Given $\mathfrak{m} \in \operatorname{Supp}(M)$ maximal, set $\mathfrak{M} := \mathfrak{m}R[X] + \langle X \rangle$. Then $\mathfrak{M}$ is maximal in $R[X]$ and $\mathfrak{M} \cap R = \mathfrak{m}$ by (**2.32**). So $\mathfrak{M} \in \operatorname{Supp}(M[X])$ by (**13.49**) and (**8.31**). Thus $M[X]_{\mathfrak{M}}$ is Cohen–Macaulay.

Form the ring map $\varphi\colon R[X] \to R$ with $\varphi(X) = 0$, and view M as an $R[X]$-module via φ. Then $\varphi(\mathfrak{M}) = \mathfrak{m}$. So $M_{\mathfrak{M}} = M_{\mathfrak{m}}$ by (**12.26**).

There is a unique $R[X]$-map $\beta\colon M[X] \to M$ with $\beta|M = 1_M$ by (**4.18**)(1). Plainly $\operatorname{Ker}(\beta) = XM[X]$, and β is surjective. So $M[X]/XM[X] \xrightarrow{\sim} M$. Hence $M[X]_{\mathfrak{M}}/XM[X]_{\mathfrak{M}} = M_{\mathfrak{M}}$. But $X \notin \operatorname{z.div}(M[X]_{\mathfrak{M}})$. So $M_{\mathfrak{M}}$ is Cohen–Macaulay over $R[X]_{\mathfrak{M}}$ by (**23.32**). But $M_{\mathfrak{M}} = M_{\mathfrak{m}}$. So $M_{\mathfrak{m}}$ is Cohen–Macaulay over $R_{\mathfrak{m}}$ owing to (**23.33**) and (**21.20**)(1) with $R := R[X]_{\mathfrak{M}}$ and $R' := R_{\mathfrak{m}}$. Thus M is Cohen–Macaulay over R.

Conversely, assume M is Cohen–Macaulay over R. Given a maximal ideal $\mathfrak{M}$ in $\operatorname{Supp}(M[X])$, set $\mathfrak{m} := \mathfrak{M} \cap R$. Then $M[X]_{\mathfrak{M}} = (M[X]_{\mathfrak{m}})_{\mathfrak{M}}$ by (**12.25**)(2). Also $M[X]_{\mathfrak{m}} = M_{\mathfrak{m}}[X]$ by (**12.31**). So $\mathfrak{m} \in \operatorname{Supp}(M)$. So $M_{\mathfrak{m}}$ is Cohen–Macaulay over $R_{\mathfrak{m}}$. Thus, to show $M[X]_{\mathfrak{M}}$ is Cohen–Macaulay over $R[X]_{\mathfrak{M}}$, replace R by $R_{\mathfrak{m}}$ and M by $M_{\mathfrak{m}}$, so that R is local with maximal ideal $\mathfrak{m}$.

Set $k := R/\mathfrak{m}$. Note $R[X]/\mathfrak{m}R[X] = k[X]$ by (**1.16**). Also, $\mathfrak{M}/\mathfrak{m}R[X]$ is maximal in $k[X]$, so contains a nonzero polynomial $\overline{F}$. As k is a field, we may take $\overline{F}$ monic. Lift $\overline{F}$ to a monic polynomial $F \in \mathfrak{M}$. Set $B := R[X]/\langle F \rangle$ and $n := \deg F$. Then B is a free R-module of rank n by (**10.15**).

Set $N := M[X]/\langle F \rangle M[X]$. Then $N = B \otimes_{R[X]} M[X]$ by (**8.27**)(1). But (**8.31**) yields $M[X] = R[X] \otimes_R M$. So $N = B \otimes_R M$ by (**8.9**)(1). Thus $N = M^{\oplus n}$.

Plainly $\operatorname{Supp}(N) = \operatorname{Supp}(M)$. Hence $\dim(N) = \dim(M)$. Now, given a sequence $x_1, \ldots, x_r \in \mathfrak{m}$, plainly it's an N-sequence if and only if it's an M-sequence. Hence $\operatorname{depth}(N) = \operatorname{depth}(M)$. Thus N is Cohen–Macaulay over R, as M is.

Note $\dim_R(N) = \dim_B(N)$ by (**21.20**)(1), and B is semilocal by (**21.20**)(5). Note $\operatorname{depth}_R(N) = \operatorname{depth}_B(N)$ by (**23.33**). But N is Cohen–Macaulay over R. Hence $\operatorname{depth}_B(N) = \dim_B(N)$. Thus by (**23.42**), N is Cohen–Macaulay over B.

Set $\mathfrak{n} := \mathfrak{M}B$. Then $N_{\mathfrak{n}}$ is Cohen–Macaulay over $B_{\mathfrak{n}}$ as N is Cohen–Macaulay over B. But $N_{\mathfrak{n}} = N_{\mathfrak{M}}$ by (**12.26**). So $N_{\mathfrak{M}}$ is Cohen–Macaulay over $R[X]_{\mathfrak{M}}$ by (**23.33**) and (**21.20**)(1) with $R := R[X]_{\mathfrak{M}}$ and $R' := R_{\mathfrak{m}}$. But $N_{\mathfrak{M}}$ is equal to $M[X]_{\mathfrak{M}}/\langle F \rangle M[X]_{\mathfrak{M}}$ by (**12.15**). And F is monic, so a nonzerodivisor. So $M[X]_{\mathfrak{M}}$ is Cohen–Macaulay over $R[X]_{\mathfrak{M}}$ by (**23.32**). Thus $M[X]$ is so over $R[X]$. □

Definition (23.44). — Let R be a ring, M a module. We call M **universally**

catenary if, for every finite set of variables $X_1, \ldots, X_n$, every quotient of the $R[X_1, \ldots, X_n]$-module $M[X_1, \ldots, X_n]$ is catenary.

We call R **universally catenary** if R is so as an R-module.

Theorem (23.45). — *A Cohen–Macaulay module M is universally catenary.*

Proof: Any quotient of a catenary module is catenary by **(15.13)**. So it suffices to prove that $N := M[X_1, \ldots, X_n]$ is catenary over $P := R[X_1, \ldots, X_n]$ for every set of variables $X_1, \ldots, X_n$.

Given nested primes $\mathfrak{q} \subset \mathfrak{p}$ in P containing $\operatorname{Ann}(N)$, the chains of primes from $\mathfrak{q}$ to $\mathfrak{p}$ correspond bijectively to the chain from $\mathfrak{q}P_{\mathfrak{p}}$ to $\mathfrak{p}P_{\mathfrak{p}}$ containing $\operatorname{Ann}(N_{\mathfrak{p}})$ by **(12.17)**(1). But N is Cohen–Macaulay over P by **(23.43)** and induction on n. Thus $N_{\mathfrak{p}}$ is Cohen–Macaulay over $P_{\mathfrak{p}}$ by **(23.41)**.

Given any two maximal chains of primes from $\mathfrak{q}P_{\mathfrak{p}}$ to $\mathfrak{p}P_{\mathfrak{p}}$, extend them by adjoining to each the same maximal chain downard from $\mathfrak{q}P_{\mathfrak{p}}$; we get two maximal chains in $N_{\mathfrak{p}}$. These two have the same length by **(23.37)**. Hence the two given chains have the same length. Thus M is universally catenary. □

Example (23.46). — Trivially, a field is Cohen–Macaulay. Plainly, a domain of dimension 1 is Cohen–Macaulay. By **(23.15)**, a normal domain of dimension 2 is Cohen–Macaulay. Thus these rings are all universally catenary by **(23.45)**. In particular, we recover **(15.14)**.

Proposition (23.47). — *Let A be a regular local ring of dimension n, and M a finitely generated module. Assume M is Cohen–Macaulay of dimension n. Then M is free.*

Proof: Induct on n. If $n = 0$, then A is a field by **(21.14)**, and so M is free.

Assume $n \geq 1$. Let $t \in A$ be an element of a regular system of parameters. Then $A/\langle t\rangle$ is regular of dimension $n-1$ by **(21.16)**. As M is Cohen–Macaulay of dimension n, any associated prime $\mathfrak{q}$ is minimal in A by **(23.37)**; so $\mathfrak{q} = \langle 0\rangle$ as A is a domain by **(21.17)**. Hence t is a nonzerodivisor on M by **(17.12)**. So M/tM is Cohen–Macaulay of dimension $n-1$ by **(23.32)** and **(21.5)**. Hence by induction, M/tM is free, say of rank r.

Let k be the residue field of A. Then $M \otimes_A k = (M/tM) \otimes_{A/\langle t\rangle} k$ by **(8.27)**(1). So $r = \operatorname{rank}(M \otimes_A k)$.

Set $\mathfrak{p} := \langle t\rangle$. Then $A_{\mathfrak{p}}$ is a DVR by **(23.6)**. Moreover, $M_{\mathfrak{p}}$ is Cohen–Macaulay of dimension 1 by **(23.39)** as $\operatorname{depth}(\langle t\rangle, M) = 1$. So $M_{\mathfrak{p}}$ is torsionfree by **(23.11)**. Therefore $M_{\mathfrak{p}}$ is flat by **(9.35)**, so free by **(10.12)**. Set $s := \operatorname{rank}(M_{\mathfrak{p}})$.

Let $k(\mathfrak{p})$ be the residue field of $A_{\mathfrak{p}}$. Then $M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} k(\mathfrak{p}) = M_{\mathfrak{p}}/tM_{\mathfrak{p}}$ by **(8.27)**(1). Moreover, $M_{\mathfrak{p}}/tM_{\mathfrak{p}} = (M/tM)_{\mathfrak{p}}$ by **(12.15)**. So $r = s$.

Set $K := \operatorname{Frac}(A)$. Then $A - \mathfrak{p} \subset K^{\times}$; so $K = K_{\mathfrak{p}}$ by **(11.4)**. So **(12.30)** yields $K \otimes M = K \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$. So $M \otimes_A K$ has rank r. Thus M is free by **(14.23)**. □

Proposition (23.48). — *Let R be a ring, M a module, and $x_1, \ldots, x_s \in R$ an M-sequence. Then $x_1, \ldots, x_s$ is M-quasi-regular.*

Proof: Form the surjection $\phi_s \colon (M/\mathfrak{q}M)[X_1, \ldots, X_s] \twoheadrightarrow G_{\mathfrak{q}}(M)$ of **(21.11.1)**, where $\mathfrak{q} := \langle x_1, \ldots, x_s\rangle$ and the X_i are variables. We have to prove that ϕ_s is bijective. So given a homogeneous polynomial $F \in M[X_1, \ldots, X_s]$ of degree r with $F(x_1, \ldots, x_s) \in \mathfrak{q}^{r+1}M$, we have to show that the coefficients of F lie in $\mathfrak{q}M$.

As $F(x_1, \ldots, x_s) \in \mathfrak{q}^{r+1}M$, there are homogeneous $F_i \in M[X_1, \ldots, X_d]$ of degree

r with $F(x_1, \ldots, x_s) = \sum_i x_i F_i(x_1, \ldots, x_s)$. Set $F' := \sum_i x_i F_i(X_1, \ldots, X_s)$. Then F' has coefficients in $\mathfrak{q}M$. Set $F'' := F - F'$. If F'' has coefficients in $\mathfrak{q}M$, so does F. Also $F''(x_1, \ldots, x_s) = 0$. So replace F by F''.

Induct on s. For $s = 1$, say $F = mX_1^r$. Then $x_1^r m = 0$. But x_1 is M-regular. So $x_1^{r-1} m = 0$. Thus, by recursion, $m = 0$.

Assume $s > 1$. Set $\mathfrak{r} := \langle x_1, \ldots, x_{s-1} \rangle$. By induction, $x_1, \ldots, x_{s-1}$ is M-quasi-regular; that is, $\phi_{s-1} \colon (M/\mathfrak{r}M)[X_1, \ldots, X_{s-1}] \to G_{\mathfrak{r}}(M)$ is bijective. So $G_{\mathfrak{r},k}(M)$ is a direct sum of copies of $M/\mathfrak{r}M$ for all k. But x_s is $M/\mathfrak{r}M$-regular. So x_s is $G_{\mathfrak{r},k}(M)$-regular. Consider the exact sequence

$$0 \to G_{\mathfrak{r},k}(M) \to M/\mathfrak{r}^{k+1}M \to M/\mathfrak{r}^k M \to 0.$$

Induct on k and apply **(23.17)** to conclude that x_s is $M/\mathfrak{r}^k M$-regular for all k.

To see that the coefficients of F lie in $\mathfrak{q}M$, induct on r. The case $r = 0$ is trivial. So assume $r > 0$. Say

$$F(X_1, \ldots, X_s) = G(X_1, \ldots, X_{s-1}) + X_s H(X_1, \ldots, X_s),$$

where G is homogeneous of degree r and H is homogeneous of degree $r - 1$. Recall $F(x_1, \ldots, x_s) = 0$. Hence $x_s H(x_1, \ldots, x_s) \in \mathfrak{r}^r M$. But x_s is $M/\mathfrak{r}^r M$-regular. Hence $H(x_1, \ldots, x_s) \in \mathfrak{r}^r M \subset \mathfrak{q}^r M$. So by induction on r, the coefficients of H lie in $\mathfrak{q}M$. Thus it suffices to see that the coefficients of G lie in $\mathfrak{q}M$.

Since $H(x_1, \ldots, x_s) \in \mathfrak{r}^r M$, there is a homogeneous polynomial $H'(X_1, \ldots, X_{s-1})$ of degree r with $H'(x_1, \ldots, x_{s-1}) = H(x_1, \ldots, x_s)$. Set

$$G'(X_1, \ldots, X_{s-1}) := G(X_1, \ldots, X_{s-1}) + x_s H'(X_1, \ldots, X_{s-1}).$$

Then G' has degree r, and $G'(x_1, \ldots, x_{s-1}) = 0$. So the coefficients of G' lie in $\mathfrak{r}M$ by induction on s. So the coefficients of G lie in $\mathfrak{q}M$. So the coefficients of F lie in $\mathfrak{q}M$. Thus $x_1, \ldots, x_s$ is M-quasi-regular. □

Proposition (23.49). — *Let R be a ring, M a module, and $x_1, \ldots, x_s \in R$. Set $M_i := M/\langle x_1, \ldots, x_i \rangle M$, and set $\mathfrak{q} := \langle x_1, \ldots, x_s \rangle$. Assume that $x_1, \ldots, x_s$ is M-quasi-regular and that M_i is separated for the $\mathfrak{q}$-adic topology for $0 \le i \le s - 1$. Then $x_1, \ldots, x_s$ is M-regular.*

Proof: First, let's see that x_1 is M-regular. Given $m \in M$ with $x_1 m = 0$, we have to show $m = 0$. But $\bigcap_{r \ge 0} \mathfrak{q}^r M = 0$ as M is separated. So we have to show $m \in \mathfrak{q}^r M$ for all $r \ge 0$. Induct on r. Note $m \in M = \mathfrak{q}^0 M$. So assume $m \in \mathfrak{q}^r M$. We have to show $m \in \mathfrak{q}^{r+1} M$.

As $m \in \mathfrak{q}^r M$, there's a homogeneous polynomial $F \in M[X_1, \ldots, X_s]$ of degree r with $F(x_1, \ldots, x_s) = m$. Consider the map $\phi_s \colon (M/\mathfrak{q}M)[X_1, \ldots, X_s] \to G_{\mathfrak{q}}(M)$ of **(21.11.1)**, where the X_i are variables. As $x_1, \ldots, x_s$ is M-quasi-regular, ϕ_s is bijective. But $x_1 m = 0$. Hence $X_1 F$ has coefficients in $\mathfrak{q}M$. But $X_1 F$ and F have the same coefficients. Thus $m \in \mathfrak{q}^{r+1} M$. Thus x_1 is M-regular.

Suppose $s \ge 2$. Induct on s. Set $\mathfrak{q}_1 := \langle x_2, \ldots, x_s \rangle$. Then **(4.21)** yields $M_1/\mathfrak{q}_1 M_1 = M/\mathfrak{q}M$. Thus $M_1/\mathfrak{q}_1 M_1 \ne 0$. Next, form this commutative diagram:

$$\begin{tikzcd} (M/\mathfrak{q}M)[X_1, \ldots, X_s] \arrow[r, "\phi_s"] & G_{\mathfrak{q}}(M) \\ (M_1/\mathfrak{q}_1 M_1)[X_2, \ldots, X_s] \arrow[u, "\iota"] \arrow[r, "\phi_{s-1}"] & G_{\mathfrak{q}_1}(M_1) \arrow[u, "\psi"'] \end{tikzcd}$$

where ι is the inclusion and ψ is induced by the inclusions $\mathfrak{q}_1^r \subset \mathfrak{q}^r$ for $r \ge 0$. As ι

and ϕ_s are injective, so is ϕ_{s-1}. Thus $x_2, \dots, x_s$ is M_1-quasi-regular.

Set $M_{1,i} := M_1/\langle x_2, \dots, x_i\rangle M_1$ for $1 \le i \le s$. Then $M_{1,i} = M_i$ by **(4.21)** again. Also $\mathfrak{q}_1 M_{1,i} = \mathfrak{q} M_i$. So $M_{1,i}$ is separated for the $\mathfrak{q}_1$-adic topology for $1 \le i \le s-1$. Hence $x_2, \dots, x_s$ is M_1-regular by induction on s. Thus $x_1, \dots, x_s$ is M-regular. □

Theorem (23.50). — *Let R be a ring, M a Noetherian semilocal module, and $x_1, \dots, x_s$ a sop for M. Set $\mathfrak{q} := \langle x_1, \dots, x_s\rangle$. Then these conditions are equivalent:*

(1) $e(\mathfrak{q}, M) = \ell(M/\mathfrak{q}M)$. (2) *$x_1, \dots, x_s$ is M-quasi-regular.*
(3) *$x_1, \dots, x_s$ is M-regular.* (4) *M is Cohen–Macaulay.*

Proof: First, (1) and (2) are equivalent by **(21.12)**.

Second, (3) implies (2) by **(23.48)**. Conversely, fix i. Set $N := \langle x_1, \dots, x_i\rangle M$. Set $M' := M/N$ and $R' := R/\operatorname{Ann}(M')$. Then $\operatorname{rad}(R') = \operatorname{rad}(M')/\operatorname{Ann}(M')$ by **(4.1.1)**. But $\operatorname{Ann}(M') \supset \operatorname{Ann}(M)$; so $\operatorname{rad}(M') \supset \operatorname{rad}(M)$. But $\operatorname{rad}(M) \supset \mathfrak{q}$. Hence $\mathfrak{q}R' \subset \operatorname{rad}(R')$. Hence M' is separated for the $\mathfrak{q}$-adic topology by **(18.35)**. Thus owing to **(23.49)**, (2) implies (3). Thus (2) and (3) are equivalent.

Third, (4) implies (3) by **(23.38)**. Conversely, assume (3). Then $s \le \operatorname{depth}(M)$. But $\operatorname{depth}(M) \le \dim(M)$ by **(23.5)**(3). Also, as $x_1, \dots, x_s$ is a sop, $\dim(M) = s$ by **(21.4)**. Thus (4) holds. Thus (3) and (4) are equivalent. □

D. Appendix: Exercises

Exercise (23.51) . — Let R be a ring, M a module, and $x_1, \dots, x_n \in R$. Set $\mathfrak{a} := \langle x_1, \dots, x_n\rangle$ and assume $M/\mathfrak{a}M \ne 0$. For all $\mathfrak{p} \in \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{a})$, assume $x_1/1, \dots, x_n/1$ is $M_\mathfrak{p}$-regular. Prove $x_1, \dots, x_n$ is M-regular.

Exercise (23.52) . — Let R be a ring, M a Noetherian module, $x_1, \dots, x_n$ an M-sequence in $\operatorname{rad}(M)$, and σ a permutation of $1, \dots, n$. Prove that $x_{\sigma 1}, \dots, x_{\sigma n}$ is an M-sequence too; first, say σ just transposes i and $i+1$.

Exercise (23.53) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a Noetherian module. Let $x_1, \dots, x_r$ be an M-sequence, and $n_1, \dots, n_r \ge 1$. Prove these two assertions:
(1) $x_1^{n_1}, \dots, x_r^{n_r}$ is an M-sequence. (2) $\operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(\sqrt{\mathfrak{a}}, M)$.

Exercise (23.54) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a nonzero Noetherian module, $x \in R$. Assume $\mathfrak{a} \subset \operatorname{z.div}(M)$ and $\mathfrak{a} + \langle x\rangle \subset \operatorname{rad}(M)$. Show $\operatorname{depth}(\mathfrak{a} + \langle x\rangle, M) \le 1$.

Exercise (23.55) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a nonzero Noetherian module, $x \in R$. Set $\mathfrak{b} := \mathfrak{a} + \langle x\rangle$. Assume $\mathfrak{b} \subset \operatorname{rad}(M)$. Show $\operatorname{depth}(\mathfrak{b}, M) \le \operatorname{depth}(\mathfrak{a}, M) + 1$.

Exercise (23.56) . — Let R be a ring, M a nonzero Noetherian module. Given any proper ideal $\mathfrak{a}$, set $c(\mathfrak{a}, M) := \min\{\dim M_\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Supp}(M/\mathfrak{a}M)\}$. Prove M is Cohen–Macaulay if and only if $\operatorname{depth}(\mathfrak{a}, M) = c(\mathfrak{a}, M)$ for all proper ideals $\mathfrak{a}$.

Exercise (23.57) . — Prove that a Noetherian local ring A of dimension $r \ge 1$ is regular if and only if its maximal ideal $\mathfrak{m}$ is generated by an A-sequence. Prove that, if A is regular, then A is Cohen–Macaulay and universally catenary.

Exercise (23.58) . — Let R be a ring, and M a nonzero Noetherian semilocal module. Set $\mathfrak{m} := \operatorname{rad}(M)$. Prove: (1) $\widehat{M}$ is a nonzero Noetherian semilocal $\widehat{R}$-module, and $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{M})$; and (2) $\operatorname{depth}_R(M) = \operatorname{depth}_R(\widehat{M}) = \operatorname{depth}_{\widehat{R}}(\widehat{M})$.

Exercise (23.59) . — Let A be a DVR, t a uniformizing parameter, X a variable. Set $P := A[X]$. Set $\mathfrak{m}_1 := \langle 1 - tX\rangle$ and $\mathfrak{m}_2 := \langle t, X\rangle$. Prove P is Cohen–Macaulay, and each $\mathfrak{m}_i$ is maximal with $\mathrm{ht}(\mathfrak{m}_i) = i$.

Set $S_i := P - \mathfrak{m}_i$ and $T := S_1 \cap S_2$. Set $B := T^{-1}P$ and $\mathfrak{n}_i := \mathfrak{m}_i B$. Prove B is semilocal and Cohen–Macaulay, $\mathfrak{n}_i$ is maximal, and $\dim(B_{\mathfrak{n}_i}) = i$.

Exercise (23.60) . — Let R be a ring, M a nonzero Noetherian semilocal module, and $x_1, \dots, x_m \in \mathrm{rad}(M)$. For all i, set $M_i := M/\langle x_1, \dots, x_i\rangle M$. Assume that $\mathrm{depth}(M) = \dim(M)$ and $\dim(M_m) = \dim(M) - m$. For all i, show $x_1, \dots, x_i$ form an M-sequence, and $\mathrm{depth}(M_i) = \dim(M_i) = \dim(M) - i$.

Exercise (23.61) . — Let k be an algebraically closed field, $P := k[X_1, \dots, X_n]$ a polynomial ring, and $F_1, \dots, F_m \in P$. Set $\mathfrak{A} := \langle F_1, \dots, F_m\rangle$. For all i, j, define $\partial F_i/\partial X_j \in P$ formally as in (1.18.1). Let $\mathfrak{A}'$ be the ideal generated by $\mathfrak{A}$ and all the maximal minors of the m by n matrix $(\partial F_i/\partial X_j)$. Set $R := P/\mathfrak{A}$ and $R' := P/\mathfrak{A}'$. Assume $\dim R = n - m$. Show that R is Cohen–Macaulay, and that R is normal if and only if either $R' = 0$ or $\dim R' \le n - m - 2$.

24. Dedekind Domains

Dedekind domains are defined as the 1-dimensional normal Noetherian domains. We prove they are the Noetherian domains whose localizations at nonzero primes are discrete valuation rings. Next we prove the Main Theorem of Classical Ideal Theory: in a Dedekind domain, every nonzero ideal factors uniquely into primes. Then we prove that a normal domain has a module-finite integral closure in any finite separable extension of its fraction field by means of the trace pairing of the extension; in Chapter 26, we do without separability by means of the Krull–Akizuki Theorem. We conclude that a ring of algebraic integers is a Dedekind domain and that, if a domain is algebra finite over a field of characteristic 0, then in the fraction field or in any algebraic extension of it, the integral closure is module finite over the domain and is algebra finite over the field.

A. Text

Definition (24.1). — A domain R is said to be **Dedekind** if it is Noetherian, normal, and of dimension 1.

Example (24.2). — Examples of Dedekind domains include the integers $\mathbb{Z}$, the Gaussian integers $\mathbb{Z}\big[\sqrt{-1}\,\big]$, the polynomial ring $k[X]$ in one variable over a field, and any DVR. Indeed, those rings are PIDs, and every PID R is a Dedekind domain: namely, R is of dimension 1 as every nonzero prime is maximal by **(2.17)**; and R is a UFD, so normal by Gauss's Theorem, **(10.21)**; and R is plainly Noetherian.

On the other hand, any local Dedekind domain is a DVR by **(23.6)**.

Example (24.3). — Let $d \in \mathbb{Z}$ be a square-free integer. Set $R := \mathbb{Z} + \mathbb{Z}\eta$ where

$$\eta := \begin{cases} (1+\sqrt{d})/2 & \text{if } d \equiv 1 \pmod 4; \\ \sqrt{d} & \text{if not.} \end{cases}$$

Then R is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ by [**3**, Prp. (6.14), p. 412]; so R is normal by **(10.20)**. Also, $\dim(R) = \dim(\mathbb{Z})$ by **(15.26)**; so $\dim(R) = 1$. Finally, R is Noetherian by **(16.10)** as $\mathbb{Z}$ is so and as $R := \mathbb{Z} + \mathbb{Z}\eta$. Thus R is Dedekind.

Exercise (24.4) . — Let R be a domain, S a multiplicative subset.

(1) Assume $\dim(R) = 1$. Prove $\dim(S^{-1}R) = 1$ if and only if there is a nonzero prime $\mathfrak{p}$ of R with $\mathfrak{p} \cap S = \emptyset$.

(2) Assume $\dim(R) \geq 1$. Prove $\dim(R) = 1$ if and only if $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero prime $\mathfrak{p}$ of R.

Exercise (24.5) . — Let R be a Dedekind domain, and S a multiplicative subset. Assume $0 \notin S$. Show that $S^{-1}R$ is Dedekind if there's a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$, and that $S^{-1}R = \mathrm{Frac}(R)$ if not.

Proposition (24.6). — *Let R be a Noetherian domain, not a field. Then R is a Dedekind domain if and only if $R_{\mathfrak{p}}$ is a DVR for every nonzero prime $\mathfrak{p}$.*

Proof: If R is Dedekind, then $R_{\mathfrak{p}}$ is too by **(24.5)**; so $R_{\mathfrak{p}}$ is a DVR by **(23.6)**.

Conversely, suppose $R_{\mathfrak{p}}$ is a DVR for every nonzero prime $\mathfrak{p}$. Then, trivially, R

satisfies (R_1) and (S_2); so R is normal by Serre's Criterion **(23.15)**. As R is not a field, $\dim(R) \ge 1$; hence, $\dim(R) = 1$ by **(24.4)**(2). Thus R is Dedekind. □

Proposition (24.7). — *In a Noetherian domain R of dimension 1, every ideal $\mathfrak{a} \neq 0$ has a unique factorization $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_r$ with the $\mathfrak{q}_i$ primary and their primes $\mathfrak{p}_i$ distinct; further, $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \mathrm{Ass}(R/\mathfrak{a})$ and $\mathfrak{q}_i = \mathfrak{a}R_{\mathfrak{p}_i} \cap R$ for each i.*

Proof: The Lasker–Noether Theorem, **(18.19)**, yields an irredundant primary decomposition $\mathfrak{a} = \bigcap \mathfrak{q}_i$. Say $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary. Then by **(18.17)** the $\mathfrak{p}_i$ are distinct and $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \mathrm{Ass}(R/\mathfrak{a})$.

The $\mathfrak{q}_i$ are pairwise comaximal for the following reason. Suppose $\mathfrak{q}_i + \mathfrak{q}_j$ lies in a maximal ideal $\mathfrak{m}$. Now, $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$ by **(18.3)**(5); so $\mathfrak{p}_i^{n_i} \subset \mathfrak{q}_i$ for some n_i by **(3.38)**. Hence $\mathfrak{p}_i^{n_i} \subset \mathfrak{m}$. So $\mathfrak{p}_i \subset \mathfrak{m}$ by **(2.25)**(1).

But $0 \neq \mathfrak{a} \subset \mathfrak{p}_i$; hence, $\mathfrak{p}_i$ is maximal since $\dim(R) = 1$. Therefore, $\mathfrak{p}_i = \mathfrak{m}$. Similarly, $\mathfrak{p}_j = \mathfrak{m}$. Hence $i = j$. Thus the $\mathfrak{q}_i$ are pairwise comaximal. So the Chinese Remainder Theorem, **(1.21)**(4)(b), yields $\mathfrak{a} = \prod_i \mathfrak{q}_i$.

As to uniqueness, let $\mathfrak{a} = \prod \mathfrak{q}_i$ be any factorization with the $\mathfrak{q}_i$ primary and their primes $\mathfrak{p}_i$ distinct. The $\mathfrak{p}_i$ are minimal containing $\mathfrak{a}$ as $\dim(R) = 1$; so the $\mathfrak{p}_i$ lie in $\mathrm{Ass}(R/\mathfrak{a})$ by **(17.14)**. Conversely, given $\mathfrak{p} \in \mathrm{Ass}(A/\mathfrak{a})$, note $\mathfrak{p} \supset \mathfrak{a}$. So $\mathfrak{p} \supset \mathfrak{p}_i$ for some i again by **(3.38)** and **(2.25)**(1). So $\mathfrak{p} = \mathfrak{p}_i$. Thus $\mathrm{Ass}(A/\mathfrak{a}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$.

By the above reasoning, the $\mathfrak{q}_i$ are pairwise comaximal; so $\prod \mathfrak{q}_i = \bigcap \mathfrak{q}_i$. Hence $\mathfrak{a} = \bigcap \mathfrak{q}_i$ is an irredundant primary decomposition by **(18.17)**. Thus the Second Uniqueness Theorem, **(18.22)**, plus **(12.12)**(3) give $\mathfrak{q}_i = \mathfrak{a}R_{\mathfrak{p}_i} \cap R$. □

Theorem (24.8) (Main Theorem of Classical Ideal Theory). — *Let R be a domain. Assume R is Dedekind. Then every nonzero ideal $\mathfrak{a}$ has a unique factorization into primes $\mathfrak{p}$. In fact, if $v_{\mathfrak{p}}$ denotes the valuation of $R_{\mathfrak{p}}$, then*

$$\mathfrak{a} = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})} \quad \textit{where} \quad v_{\mathfrak{p}}(\mathfrak{a}) := \min\{\, v_{\mathfrak{p}}(a) \mid a \in \mathfrak{a} \,\}.$$

Proof: Using **(24.7)**, write $\mathfrak{a} = \prod \mathfrak{q}_i$ with the $\mathfrak{q}_i$ primary, their primes $\mathfrak{p}_i$ distinct and unique, and $\mathfrak{q}_i = \mathfrak{a}R_{\mathfrak{p}_i} \cap R$. Then $R_{\mathfrak{p}_i}$ is a DVR by **(24.6)**. So **(23.1.3)** yields $\mathfrak{a}R_{\mathfrak{p}_i} = \mathfrak{p}_i^{m_i} R_{\mathfrak{p}_i}$ with $m_i := \min\{\, v_{\mathfrak{p}_i}(a/s) \mid a \in \mathfrak{a} \text{ and } s \in R - \mathfrak{p}_i \,\}$. But $v_{\mathfrak{p}_i}(1/s) = 0$. So $v_{\mathfrak{p}_i}(a/s) = v_{\mathfrak{p}_i}(a)$. Hence $m_i := v_{\mathfrak{p}_i}(\mathfrak{a})$. Now, $\mathfrak{p}_i^{m_i}$ is primary by **(18.11)** as $\mathfrak{p}_i$ is maximal; so $\mathfrak{p}_i^{m_i} R_{\mathfrak{p}_i} \cap R = \mathfrak{p}_i^{m_i}$ by **(18.20)**. Thus $\mathfrak{q}_i = \mathfrak{p}_i^{m_i}$. □

Corollary (24.9). — *A Noetherian domain R of dimension 1 is Dedekind if and only if every primary ideal is a power of its radical.*

Proof: If R is Dedekind, every primary ideal is a power of its radical by **(24.8)**.

Conversely, given a nonzero prime $\mathfrak{p}$, set $\mathfrak{m} := \mathfrak{p}R_{\mathfrak{p}}$. Then $\mathfrak{m} \neq 0$. So $\mathfrak{m} \neq \mathfrak{m}^2$ by Nakayama's Lemma **(10.6)**. Take $t \in \mathfrak{m} - \mathfrak{m}^2$. Then $\mathfrak{m}$ is the only prime containing t, as $\dim(R_{\mathfrak{p}}) = 1$ by **(24.4)**(2). So $\mathfrak{m} = \sqrt{tR_{\mathfrak{p}}}$ by the Scheinnullstellensatz **(3.14)**. Thus **(18.11)** implies $tR_{\mathfrak{p}}$ is $\mathfrak{m}$-primary.

Set $\mathfrak{q} := tR_{\mathfrak{p}} \cap R$. Then $\mathfrak{q}$ is $\mathfrak{p}$-primary by **(18.20)**. So $\mathfrak{q} = \mathfrak{p}^n$ for some n by hypothesis. But $\mathfrak{q}R_{\mathfrak{p}} = tR_{\mathfrak{p}}$ by **(11.11)**(1)(b). So $tR_{\mathfrak{p}} = \mathfrak{m}^n$. But $t \notin \mathfrak{m}^2$. So $n = 1$. So $R_{\mathfrak{p}}$ is a DVR by **(23.6)**. Thus **(24.6)** implies R is Dedekind . □

Lemma (24.10) (Artin Character). — *Let L be a field, G a group, $\sigma_i \colon G \to L^{\times}$ distinct homomorphisms. Then the σ_i are linearly independent over L in the vector space of set maps $\sigma \colon G \to L$ under valuewise addition and scalar multiplication.*

Proof: Suppose there's an equation $\sum_{i=1}^{m} a_i\sigma_i = 0$ with nonzero $a_i \in L$. Take $m \geq 1$ minimal. Now, $\sigma_i \neq 0$ as $\sigma_i\colon = G \to L^\times$; so $m \geq 2$. Since $\sigma_1 \neq \sigma_2$, there's an $x \in G$ with $\sigma_1(x) \neq \sigma_2(x)$. Then $\sum_{i=1}^{m} a_i\sigma_i(x)\sigma_i(y) = \sum_{i=1}^{m} a_i\sigma_i(xy) = 0$ for every $y \in G$ since σ_i is a homomorphism.

Set $b_i := a_i\big(1 - \sigma_i(x)/\sigma_1(x)\big)$. Then

$$\textstyle\sum_{i=1}^{m} b_i\sigma_i = \sum_{i=1}^{m} a_i\sigma_i - \frac{1}{\sigma_1(x)}\sum_{i=1}^{m} a_i\sigma_i(x)\sigma_i = 0.$$

But $b_1 = 0$ and $b_2 \neq 0$, contradicting the minimality of m. □

(24.11) (Trace). — Let L/K be a finite Galois field extension. Its **trace** is this:

$$\mathrm{tr}\colon L \to K \quad \text{by} \quad \mathrm{tr}(x) := \textstyle\sum_{\sigma\in\mathrm{Gal}(L/K)} \sigma(x).$$

Indeed, $\mathrm{tr}(x) \in K$ as $\tau(\mathrm{tr}(x)) = \mathrm{tr}(x)$ for all $\tau \in \mathrm{Gal}(L/K)$.

Plainly, tr is K-linear. It is nonzero by **(24.10)** applied with $G := L^\times$.

Consider the symmetric K-bilinear **Trace Pairing**:

$$L \times L \to K \quad \text{by} \quad (x, y) \mapsto \mathrm{tr}(xy). \tag{24.11.1}$$

It is nondegenerate for this reason. As tr is nonzero, there is $z \in L$ with $\mathrm{tr}(z) \neq 0$. Now, given $x \in L^\times$, set $y := z/x$. Then $\mathrm{tr}(xy) \neq 0$, as desired.

Lemma (24.12). — *Let R be a normal domain, K its fraction field, L/K a finite Galois field extension, and $x \in L$ integral over R. Then $\mathrm{tr}(x) \in R$.*

Proof: Let $x^n + a_1x^{n-1} + \cdots + a_n = 0$ be an equation of integral dependence for x over R. Let $\sigma \in \mathrm{Gal}(L/K)$. Then

$$(\sigma x)^n + a_1(\sigma x)^{n-1} + \cdots + a_n = 0;$$

so σx is integral over R. Hence $\mathrm{tr}(x)$ is integral over R, and lies in K. Thus $\mathrm{tr}(x) \in R$ since R is normal. □

Theorem (24.13) (Finiteness of integral closure). — *Let R be a normal Noetherian domain, K its fraction field, L/K a finite separable field extension, and R' the integral closure of R in L. Then R' is module finite over R, and is Noetherian.*

Proof: Let L_1 be the Galois closure of L/K, and R_1' the integral closure of R in L_1. Let $z_1, \ldots, z_n \in L_1$ form a K-basis. Using **(11.30)**, write $z_i = y_i/a_i$ with $y_i \in R_1'$ and $a_i \in R$. Clearly, $y_1, \ldots, y_n$ form a basis of L_1/K contained in R_1'.

Let $x_1, \ldots, x_n$ form the dual basis with respect to the Trace Pairing, **(24.11.1)**, so that $\mathrm{tr}(x_iy_j) = \delta_{ij}$. Given $b \in R'$, write $b = \sum c_ix_i$ with $c_i \in K$. Fix j. Then

$$\mathrm{tr}(by_j) = \mathrm{tr}\Big(\textstyle\sum_i c_ix_iy_j\Big) = \sum_i c_i\,\mathrm{tr}(x_iy_j) = c_j \quad \text{for each } j.$$

But $by_j \in R_1'$. So $c_j \in R$ by **(24.12)**. Thus $R' \subset \sum Rx_i$. Since R is Noetherian, R' is module finite over R by definition, and so is Noetherian owing to **(16.15)**. □

Corollary (24.14). — *Let R be a Dedekind domain, K its fraction field, L/K a finite separable field extension. Then the integral closure R' of R in L is Dedekind.*

Proof: First, R' is module finite over R by **(24.13)**; so R' is Noetherian by **(16.15)**. Second, R' is normal by **(10.20)**. Finally, $\dim(R') = \dim(R)$ by **(15.26)**, and $\dim(R) = 1$ as R is Dedekind. Thus R' is Dedekind. □

Theorem (24.15). — *The ring of all algebraic integers in any finite field extension of $\mathbb{Q}$ is a Dedekind domain.*

Proof: By (**24.2**), $\mathbb{Z}$ is a Dedekind domain; whence, so is its integral closure in any field that is a finite extension of $\mathbb{Q}$ by (**24.14**). □

Example (24.16). — The ring R of all algebraic integers in $\mathbb{C}$ is non-Noetherian, as the ascending chain $\langle\sqrt{2}\rangle \subsetneqq \langle\sqrt[4]{2}\rangle \subsetneqq \langle\sqrt[8]{2}\rangle \subsetneqq \cdots$ doesn't stabilize. So R isn't Dedekind, although R is normal, and $\dim(R) = 1$ by (**15.26**) as $R/\mathbb{Z}$ is integral.

Theorem (24.17) (Noether's Finiteness of Integral Closure). — *Let k be a field of characteristic* 0*, and R an algebra-finite domain over k. Set $K := \mathrm{Frac}(R)$. Let L/K be a finite field extension (possibly $L = K$), and R' the integral closure of R in L. Then R' is module finite over R and is algebra finite over k.*

Proof: By the Noether Normalization Lemma, (**15.1**), R is module finite over a polynomial subring P. Then P is normal by Gauss's Theorem, (**10.21**), and Noetherian by the Hilbert Basis Theorem, (**16.10**); also, $L/\mathrm{Frac}(P)$ is a finite field extension, which is separable as k is of characteristic 0. Thus R' is module finite over P by (**24.13**), and so R' is plainly algebra finite over k. □

(24.18) (Other cases). — In (**24.14**), even if L/K is inseparable, the integral closure R' of R in L is still Dedekind; see (**26.14**).

However, Akizuki constructed an example of a DVR R and a finite inseparable extension $L/\mathrm{Frac}(R)$ such that the integral closure of R is a DVR, but is not module finite over R. The construction is nicely explained in [**16**, Secs. 9.4(1) and 9.5]. Thus separability is a necessary hypothesis in (**24.13**).

Noether's Theorem, (**24.17**), remains valid in positive characteristic, but the proof is more involved. See [**6**, (13.13), p. 297].

B. Exercises

Exercise (24.19) . — Let R be a Dedekind domain, and $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ideals. By first reducing to the case that R is local, prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}),$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

Exercise (24.20) . — Let R be a Dedekind domain; $x_1, \ldots, x_n \in R$; and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals. Prove that the system of congruences $x \equiv x_i \bmod \mathfrak{a}_i$ for all i has a solution $x \in R$ if and only if $x_i \equiv x_j \bmod (\mathfrak{a}_i + \mathfrak{a}_j)$ for $i \neq j$. In other words, prove the exactness (in the middle) of the sequence of R-modules

$$R \xrightarrow{\varphi} \bigoplus_{i=1}^n R/\mathfrak{a}_i \xrightarrow{\psi} \bigoplus_{i<j} R/(\mathfrak{a}_i + \mathfrak{a}_j)$$

where $\varphi(y)$ is the vector of residues of y in the $R/\mathfrak{a}_i$ and where $\psi(y_1, \ldots, y_n)$ is the vector of residues of the $y_i - y_j$ in $R/(\mathfrak{a}_i + \mathfrak{a}_j)$.

Exercise (24.21) . — Prove that a semilocal Dedekind domain A is a PID. Begin by proving that each maximal ideal is principal.

Exercise (24.22) . — Let R be a Dedekind domain, and $\mathfrak{a}$ a nonzero ideal. Prove (1) $R/\mathfrak{a}$ is a PIR, and (2) $\mathfrak{a}$ is generated by two elements.

Exercise (24.23) . — Let R be a Dedekind domain, and M a finitely generated module. Assume M is **torsion**; that is, $T(M) = M$. Show $M \simeq \sum_{i,j} R/\mathfrak{p}_i^{n_{ij}}$ for unique nonzero primes $\mathfrak{p}_i$ and unique $n_{ij} > 0$.

Exercise (24.24) . — Let R be a Dedekind domain; X a variable; $F, G \in R[X]$. Show $c(FG) = c(F)c(G)$.

Exercise (24.25) . — Let k be an algebraically closed field, $P := k[X_1, \ldots, X_n]$ a polynomial ring, and $F_1, \ldots, F_m \in P$. Set $\mathfrak{P} := \langle F_1, \ldots, F_m \rangle$. For all i, j, define $\partial F_i/\partial X_j \in P$ formally as in (**1.18.1**). Let $\mathfrak{A}$ be the ideal generated by $\mathfrak{P}$ and all the $n-1$ by $n-1$ minors of the m by n matrix $(\partial F_i/\partial X_j)$. Set $R := P/\mathfrak{P}$. Assume R is a domain of dimension 1. Show R is Dedekind if and only if $1 \in \mathfrak{A}$.

25. Fractional Ideals

A **fractional ideal** is defined to be a submodule of the fraction field of a domain. A fractional ideal is called **invertible** if its product with another fractional ideal is equal to the given domain. We characterize the invertible fractional ideals as those that are nonzero, finitely generated, and principal locally at every maximal ideal. We prove that, in a Dedekind domain, any two nonzero ordinary ideals have an invertible fractional ideal as their quotient.

We characterize Dedekind domains as the domains whose ordinary ideals are, equivalently, all invertible, all projective, or all flat of finite rank. Further, we prove a Noetherian domain is Dedekind if and only if every torsionfree module is flat. Finally, we prove the **ideal class group** is equal to the **Picard group**; the former is the group of invertible fractional ideals modulo those that are principal, and the latter is the group, under tensor product, of isomorphism classes of modules local free of rank 1.

A. Text

Definition (25.1). — Let R be a domain, and set $K := \operatorname{Frac}(R)$. We call an R-submodule M of K a **fractional ideal**. We call M **principal** if there is an $x \in K$ with $M = Rx$.

Given another fractional ideal N, form these two new fractional ideals:

$$MN := \left\{ \sum x_i y_i \;\middle|\; x_i \in M \text{ and } y_i \in N \right\} \quad \text{and} \quad (M : N) := \{ z \in K \mid zN \subset M \}.$$

We call them the **product** of M and N and the **quotient** of M by N.

Exercise (25.2) . — Let R be a domain, M and N nonzero fractional ideals. Prove that M is principal if and only if there exists some isomorphism $M \simeq R$. Construct the following canonical surjection and canonical isomorphism:

$$\pi\colon M \otimes N \twoheadrightarrow MN \quad \text{and} \quad \alpha\colon (M : N) \xrightarrow{\sim} \operatorname{Hom}(N, M).$$

Proposition (25.3). — *Let R be a domain, and $K := \operatorname{Frac}(R)$. Consider these finiteness conditions on a fractional ideal M:*

(1) *There exist ordinary ideals $\mathfrak{a}$ and $\mathfrak{b}$ with $\mathfrak{b} \neq 0$ and $(\mathfrak{a} : \mathfrak{b}) = M$.*
(2) *There exists an $x \in K^\times$ with $xM \subset R$.*
(3) *There exists a nonzero $x \in R$ with $xM \subset R$.*
(4) *M is finitely generated.*

Then (1), (2)*, and* (3) *are equivalent, and they are implied by* (4)*. Further, all four conditions are equivalent for every M if and only if R is Noetherian.*

Proof: Assume (1) holds. Take any nonzero $x \in \mathfrak{b}$. Given $m \in M$, clearly $xm \in \mathfrak{a} \subset R$; so $xM \subset R$. Thus (2) holds.

Assume (2) holds. Write $x = a/b$ with $a, b \in R$ and $a, b \neq 0$. Then $aM \subset bR \subset R$. Thus (3) holds.

If (3) holds, then xM and xR are ordinary, and $M = (xM : xR)$; thus (1) holds.

Assume (4) holds. Say $y_1/x_1, \ldots, y_n/x_n \in K^\times$ generate M with $x_i, y_i \in R$. Set $x := \prod x_i$. Then $x \neq 0$ and $xM \subset R$. Thus (3) holds.

Assume (3) holds and R is Noetherian. Then $xM \subset R$. So xM is finitely generated, say by $y_1, \ldots, y_n$. Then $y_1/x, \ldots, y_n/x$ generate M. Thus (4) holds.

Finally, assume all four conditions are equivalent for every M. If M is ordinary, then (3) holds with $x := 1$, and so (4) holds. Thus R is Noetherian. □

Lemma (25.4). — *Let R be a domain, M and N fractional ideals. Let S be a multiplicative subset. Then*

$$S^{-1}(MN) = (S^{-1}M)(S^{-1}N) \quad \text{and} \quad S^{-1}(M : N) \subset (S^{-1}M : S^{-1}N),$$

with equality if N is finitely generated.

Proof: Given $x \in S^{-1}(MN)$, write $x = (\sum m_i n_i)/s$ with $m_i \in M$, with $n_i \in N$, and with $s \in S$. Then $x = \sum(m_i/s)(n_i/1)$, and so $x \in (S^{-1}M)(S^{-1}N)$. Thus $S^{-1}(MN) \subset (S^{-1}M)(S^{-1}N)$.

Conversely, given $x \in (S^{-1}M)(S^{-1}N)$, say $x = \sum(m_i/s_i)(n_i/t_i)$ with $m_i \in M$ and $n_i \in N$ and $s_i, t_i \in S$. Set $s := \prod s_i$ and $t := \prod t_i$. Then

$$x = \sum(m_i n_i / s_i t_i) = \sum m_i' n_i'/st \in S^{-1}(MN)$$

with $m_i' \in M$ and $n_i' \in N$. Thus $S^{-1}(MN) \supset (S^{-1}M)(S^{-1}N)$, so equality holds.

Given $z \in S^{-1}(M : N)$, write $z = x/s$ with $x \in (M : N)$ and $s \in S$. Given $y \in S^{-1}N$, write $y = n/t$ with $n \in N$ and $t \in S$. Then $z \cdot n/t = xn/st$ and $xn \in M$ and $st \in S$. So $z \in (S^{-1}M : S^{-1}N)$. Thus $S^{-1}(M : N) \subset (S^{-1}M : S^{-1}N)$.

Conversely, say N is generated by $n_1, \ldots, n_r$. Given $z \in (S^{-1}M : S^{-1}N)$, write $zn_i/1 = m_i/s_i$ with $m_i \in M$ and $s_i \in S$. Set $s := \prod s_i$. Then $sz \cdot n_i \in M$. So $sz \in (M : N)$. Hence $z \in S^{-1}(M : N)$, as desired. □

Definition (25.5). — Let R be a domain. We call a fractional ideal M **locally principal** if, for every maximal ideal $\mathfrak{m}$, the localization $M_\mathfrak{m}$ is principal over $R_\mathfrak{m}$.

Exercise (25.6) . — Let R be a domain, M and N fractional ideals. Prove that the map $\pi\colon M \otimes N \to MN$ of (25.2) is an isomorphism if M is locally principal.

(25.7) (Invertible fractional ideals). — Let R be a domain. A fractional ideal M is said to be **invertible** if there is some fractional ideal M^{-1} with $MM^{-1} = R$.

For example, a nonzero principal ideal Rx is invertible, as $(Rx)(R \cdot 1/x) = R$.

Proposition (25.8). — *Let R be a domain, M an invertible fractional ideal. Then M^{-1} is unique; in fact, $M^{-1} = (R : M)$.*

Proof: Clearly $M^{-1} \subset (R : M)$ as $MM^{-1} = R$. But, if $x \in (R : M)$, then $x \cdot 1 \in (R : M)MM^{-1} \subset M^{-1}$, so $x \in M^{-1}$. Thus $(R : M) \subset M^{-1}$, as desired. □

Exercise (25.9) . — Let R be a domain, M and N fractional ideals. Prove this:

(1) Assume N is invertible. Then $(M : N) = M \cdot N^{-1}$.

(2) Both M and N are invertible if and only if their product MN is. If so, then $(MN)^{-1} = N^{-1}M^{-1}$.

Lemma (25.10). — *An invertible ideal is finitely generated and nonzero.*

Proof: Let R be the domain, M the ideal. Say $1 = \sum m_i n_i$ with $m_i \in M$ and $n_i \in M^{-1}$. Let $m \in M$. Then $m = \sum m_i m n_i$. But $mn_i \in R$ as $m \in M$ and $n_i \in M^{-1}$. So the m_i generate M. Trivially, $M \neq 0$. □

Lemma (25.11). — *Let A be a local domain, M a fractional ideal. Then M is invertible if and only if M is principal and nonzero.*

Proof: Assume M is invertible. Say $1 = \sum m_i n_i$ with $m_i \in M$ and $n_i \in M^{-1}$. As A is local, $A - A^\times$ is an ideal. So there's a j with $m_j n_j \in A^\times$. Let $m \in M$. Then $mn_j \in A$. Set $a := (mn_j)(m_j n_j)^{-1} \in A$. Then $m = am_j$. Thus $M = Am_j$.

Conversely, if M is principal and nonzero, then it's invertible by **(25.7)**. □

Exercise (25.12) . — Let R be a UFD. Show that a fractional ideal M is invertible if and only if M is principal and nonzero.

Theorem (25.13). — *Let R be a domain, M a fractional ideal. Then M is invertible if and only if M is finitely generated, nonzero, and locally principal.*

Proof: Say $MN = R$. Then M is finitely generated and nonzero by **(25.10)**. Let S be a multiplicative subset. Then $(S^{-1}M)(S^{-1}N) = S^{-1}R$ by **(25.4)**. Let $\mathfrak{m}$ be a maximal ideal. Then, therefore, $M_\mathfrak{m}$ is an invertible fractional ideal over $R_\mathfrak{m}$. Thus $M_\mathfrak{m}$ is principal by **(25.11)**, as desired.

Conversely, set $\mathfrak{a} := M(R : M) \subset R$. Assume M is finitely generated. Then **(25.4)** yields $\mathfrak{a}_\mathfrak{m} = M_\mathfrak{m}(R_\mathfrak{m} : M_\mathfrak{m})$. In addition, assume $M_\mathfrak{m}$ is principal and nonzero. Then **(25.7)** implies $M_\mathfrak{m}$ is invertible. Hence **(25.8)** yields $\mathfrak{a}_\mathfrak{m} = R_\mathfrak{m}$. Thus **(13.53)** yields $\mathfrak{a} = R$, as desired. □

Theorem (25.14). — *Let R be a Dedekind domain, $\mathfrak{a}$, $\mathfrak{b}$ nonzero ordinary ideals, $M := (\mathfrak{a} : \mathfrak{b})$. Then M is invertible, and has a unique factorization into powers of primes $\mathfrak{p}$: if $v_\mathfrak{p}$ denotes the valuation of $R_\mathfrak{p}$ and if $\mathfrak{p}^v := (\mathfrak{p}^{-1})^{-v}$ when $v < 0$, then*

$$M = \prod \mathfrak{p}^{v_\mathfrak{p}(M)} \quad \textit{where} \quad v_\mathfrak{p}(M) := \min\{\, v_\mathfrak{p}(x) \mid x \in M \,\}.$$

Further, $v_\mathfrak{p}(M) = \min\{v_\mathfrak{p}(x_i)\}$ if the x_i generate M.

Proof: First, R is Noetherian. So **(25.3)**(1)⇒(4) yields that M is finitely generated and that there is a nonzero $x \in R$ with $xM \subset R$. Also, each $R_\mathfrak{p}$ is a DVR by **(24.6)**. So $xM_\mathfrak{p}$ is principal by **(23.1.3)**. Thus M is invertible by **(25.13)**.

The Main Theorem of Classical Ideal Theory, **(24.8)**, yields $xM = \prod \mathfrak{p}^{v_\mathfrak{p}(xM)}$ and $xR = \prod \mathfrak{p}^{v_\mathfrak{p}(x)}$. But $v_\mathfrak{p}(xM) = v_\mathfrak{p}(x) + v_\mathfrak{p}(M)$. Thus **(25.9)** yields

$$M = (xM : xR) = \prod \mathfrak{p}^{v_\mathfrak{p}(x)+v_\mathfrak{p}(M)} \cdot \prod \mathfrak{p}^{-v_\mathfrak{p}(x)} = \prod \mathfrak{p}^{v_\mathfrak{p}(M)}.$$

Further, given $x \in M$, say $x = \sum_{i=1}^n a_i x_i$ with $a_i \in R$. Then **(23.1.1)** yields

$$v_\mathfrak{p}(x) \ge \min\{v_\mathfrak{p}(a_i x_i)\} \ge \min\{v_\mathfrak{p}(x_i)\}$$

by induction on n. Thus $v_\mathfrak{p}(M) = \min\{v_\mathfrak{p}(x_i)\}$. □

Exercise (25.15) . — Show that it is equivalent for a ring R to be either a PID, a 1-dimensional UFD, or a Dedekind domain and a UFD.

(25.16) (Invertible modules). — Let R be an arbitrary ring. We call a module M **invertible** if there is another module N with $M \otimes N \simeq R$.

Up to (noncanonical) isomorphism, N is unique if it exists: if $N' \otimes M \simeq R$, then

$$N = R \otimes N \simeq (N' \otimes M) \otimes N = N' \otimes (M \otimes N) \simeq N' \otimes R = N'.$$

Exercise (25.17) . — Let R be a ring, M an invertible module. Prove that M is finitely generated, and that, if R is local, then M is free of rank 1.

Exercise (25.18) . — Show these conditions on an R-module M are equivalent:

(1) M is invertible.

(2) M is finitely generated, and $M_\mathfrak{m} \simeq R_\mathfrak{m}$ at each maximal ideal $\mathfrak{m}$.

(3) M is locally free of rank 1.

Assuming these conditions hold, show that $M \otimes \mathrm{Hom}(M, R) = R$.

Proposition (25.19). — *Let R be a domain, M a fractional ideal. Then the following conditions are equivalent:*

(1) *M is an invertible fractional ideal.*
(2) *M is an invertible abstract module.*
(3) *M is a nonzero projective abstract module.*

Proof: Assume (1). Then there's N with $MN = R$. But M is locally principal by (**25.13**). So (**25.6**) yields $M \otimes N = MN$. So $M \otimes N = R$. Thus (2) holds.

If (2) holds, then M is locally free of rank 1 by (**25.18**); so (**13.15**) yields (3).

Finally, assume (3). By (**5.16**), there's an M' with $M \oplus M' \simeq R^{\oplus\Lambda}$. Let $\rho\colon R^{\oplus\Lambda} \to M$ be the projection, and set $x_\lambda := \rho(e_\lambda)$ where $\{e_\lambda\}_{\lambda\in\Lambda}$ is the standard basis. Define $\alpha_\lambda\colon M \hookrightarrow R^{\oplus\Lambda} \to R$ to be the composition of the injection with the projection α_λ on the λth factor. Then given $x \in M$, we have $\alpha_\lambda(x) = 0$ for almost all λ and $x = \sum_{\lambda\in\Lambda} \alpha_\lambda(x)x_\lambda$.

Fix a nonzero $y \in M$. For $\lambda \in \Lambda$, set $q_\lambda := \frac{1}{y}\alpha_\lambda(y) \in \mathrm{Frac}(R)$. Set $N := \sum Rq_\lambda$. Given any nonzero $x \in M$, say $x = a/b$ and $y = c/d$ with $a, b, c, d \in R$. Then $a, c \in M$; so $ad\alpha_\lambda(y) = \alpha_\lambda(ac) = bc\alpha_\lambda(x)$. So $xq_\lambda = \alpha_\lambda(x) \in R$. Thus $M \cdot N \subset R$. But $y = \sum \alpha_\lambda(y)y_\lambda$; so $1 = \sum y_\lambda q_\lambda$. Thus $M \cdot N = R$. Thus (1) holds. □

Theorem (25.20). — *Let R be a domain. Then the following are equivalent:*

(1) *R is a Dedekind domain or a field.*
(2) *Every nonzero ordinary ideal $\mathfrak{a}$ is invertible.*
(3) *Every nonzero ordinary ideal $\mathfrak{a}$ is projective.*
(4) *Every nonzero ordinary ideal $\mathfrak{a}$ is finitely generated and flat.*

Proof: Assume R is not a field; otherwise, (1)–(4) hold trivially.

If R is Dedekind, then (**25.14**) yields (2) since $\mathfrak{a} = (\mathfrak{a} : R)$.

Assume (2). Then $\mathfrak{a}$ is finitely generated by (**25.10**). Thus R is Noetherian. Let $\mathfrak{p}$ be any nonzero prime of R. Then by hypothesis, $\mathfrak{p}$ is invertible. So by (**25.13**), $\mathfrak{p}$ is locally principal. So $R_\mathfrak{p}$ is a DVR by (**23.6**). Hence R is Dedekind by (**24.6**). Thus (1) holds. Thus (1) and (2) are equivalent.

By (**25.19**), (2) and (3) are equivalent. But (2) implies that R is Noetherian by (**25.10**). Thus (3) and (4) are equivalent by (**16.15**) and (**13.15**). □

Theorem (25.21). — *Let R be a Noetherian domain, but not a field. Then R is Dedekind if and only if every torsionfree module is flat.*

Proof: (Of course, as R is a domain, every flat module is torsionfree by (**9.35**).)

Assume R is Dedekind. Let M be a torsionfree module, $\mathfrak{m}$ a maximal ideal. Let's see that $M_\mathfrak{m}$ is torsionfree over $R_\mathfrak{m}$. Let $z \in R_\mathfrak{m}$ be nonzero, and say $z = x/s$ with $x, s \in R$ and $s \notin \mathfrak{m}$. Then $\mu_x\colon M \to M$ is injective as M is torsionfree. So $\mu_x\colon M_\mathfrak{m} \to M_\mathfrak{m}$ is injective by the Exactness of Localization. But $\mu_{x/s} = \mu_x\mu_{1/s}$ and $\mu_{1/s}$ is invertible. So $\mu_{x/s}$ is injective. Thus $M_\mathfrak{m}$ is torsionfree.

Since R is Dedekind, $R_\mathfrak{m}$ is a DVR by (**24.6**), so a PID by (**24.1**). Hence $M_\mathfrak{m}$ is flat over $R_\mathfrak{m}$ by (**9.35**). But $\mathfrak{m}$ is arbitrary. Thus by (**13.12**), M is flat over R.

Conversely, assume every torsionfree module is flat. In particular, every nonzero ordinary ideal is flat. But R is Noetherian. Thus R is Dedekind by (**25.20**). □

(25.22) (The Picard Group). — Let R be a ring. We denote the collection of isomorphism classes of invertible modules by $\mathrm{Pic}(R)$. By **(25.17)**, every invertible module is finitely generated, so isomorphic to a quotient of R^n for some integer n. Hence, $\mathrm{Pic}(R)$ is a set. Further, $\mathrm{Pic}(R)$ is, clearly, a group under tensor product with the class of R as identity. We call $\mathrm{Pic}(R)$ the **Picard Group** of R.

Assume R is a domain, not a field. Set $K := \mathrm{Frac}(R)$. Given an invertible abstract module M, we can embed M into K as follows. Recall $S_0 := R - 0$. Form the canonical map $M \to S_0^{-1}M$. It is injective owing to **(12.12)**(3)(a) if the multiplication map $\mu_x\colon M \to M$ is injective for all $x \in S_0$. Let's prove it is.

Given a maximal ideal $\mathfrak{m}$, note $M_\mathfrak{m} \simeq R_\mathfrak{m}$ by **(25.18)**(1)⇒(2). So $\mu_x\colon M_\mathfrak{m} \to M_\mathfrak{m}$ is injective. Therefore, $\mu_x\colon M \to M$ is injective by **(13.9)**. Thus M embeds canonically into $S_0^{-1}M$. Now, $S_0^{-1}M$ is a localization of $M_\mathfrak{m}$, so is a 1-dimensional K-vector space, again as $M_\mathfrak{m} \simeq R_\mathfrak{m}$. Choose an isomorphism $S_0^{-1}M \simeq K$. It yields the desired embedding of M into K.

Hence, **(25.19)** implies M is also invertible as a fractional ideal.

The invertible fractional ideals N, clearly, form a group $\mathcal{F}(R)$. Sending an N to its isomorphism class yields a map $\kappa\colon \mathcal{F}(R) \to \mathrm{Pic}(R)$ by **(25.19)**(1)⇒(2). By the above, κ is surjective. The invertible fractional ideals N, clearly, form a group $\mathcal{F}(R)$. Sending an N to its isomorphism class yields a map $\kappa\colon \mathcal{F}(R) \to \mathrm{Pic}(R)$ by **(25.19)**(1)⇒(2). By the above, κ is surjective.

Further, κ is a group homomorphism by **(25.6)**. Its kernel is the group $\mathcal{P}(R)$ of principal (fractional) ideals by **(25.2)** and, plainly, $\mathcal{P}(R) = K^\times/R^\times$. We call $\mathcal{F}(R)/\mathcal{P}(R)$ the **Ideal Class Group** of R. Thus $\mathcal{F}(R)/\mathcal{P}(R) = \mathrm{Pic}(R)$; in other words, the Ideal Class Group is canonically isomorphic to the Picard Group.

Every invertible fractional ideal is, by **(25.13)**, finitely generated and nonzero, so of the form $(\mathfrak{a} : \mathfrak{b})$ where $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ordinary ideals by **(25.3)**. Conversely, by **(25.14)** and **(25.20)**, every fractional ideal of this form is invertible if and only if R is Dedekind. In fact, then $\mathcal{F}(R)$ is the free abelian group on the prime ideals. Further, then $\mathrm{Pic}(R) = 0$ if and only if R is UFD by **(21.33)** and **(21.34)**, or equivalently by **(25.15)**, a PID. See [**3**, Ch. 11, Sects. 10–11, pp. 424–437] for a discussion of the case in which R is a ring of quadratic integers, including many examples where $\mathrm{Pic}(R) \neq 0$.

B. Exercises

Exercise (25.23) . — Let R be a Dedekind domain, S a multiplicative subset. Prove $M \mapsto S^{-1}M$ induces a surjective group map $\mathrm{Pic}(R) \twoheadrightarrow \mathrm{Pic}(S^{-1}R)$.

26. Arbitrary Valuation Rings

A **valuation ring** is a subring of a field such that the reciprocal of any element outside the subring lies in it. We prove valuation rings are normal local domains. They are maximal under **domination of local rings**; that is, one contains the other, and the inclusion map is a local homomorphism. Given any domain, its normalization is equal to the intersection of all the valuation rings containing it. Given a 1-dimensional Noetherian domain and a finite extension of its fraction field with a proper subring containing the domain, that subring too is 1-dimensional and Noetherian; this is the Krull–Akizuki Theorem. So normalizing a Dedekind domain in any finite extension of its fraction field yields another Dededind domain.

A. Text

Definition (26.1). — A proper subring V of a field K is said to be a **valuation ring** of K if, whenever $z \in K - V$, then $1/z \in V$.

Proposition (26.2). — *Let V be a valuation ring of a field K, and set*

$$\mathfrak{m} := \{1/z \mid z \in K - V\} \cup \{0\}.$$

Then V is local, $\mathfrak{m}$ is its maximal ideal, and K is its fraction field.

Proof: Plainly $\mathfrak{m} = V - V^\times$. Let's show $\mathfrak{m}$ is an ideal. Take a nonzero $a \in V$ and nonzero $x, y \in \mathfrak{m}$. Suppose $ax \notin \mathfrak{m}$. Then $ax \in V^\times$. So $a(1/ax) \in V$. So $1/x \in V$. So $x \in V^\times$, a contradiction. Thus $ax \in \mathfrak{m}$. Now, by hypothesis, either $x/y \in V$ or $y/x \in V$. Say $y/x \in V$. Then $1 + (y/x) \in V$. So $x + y = (1 + (y/x))x \in \mathfrak{m}$. Thus $\mathfrak{m}$ is an ideal. Hence V is local and $\mathfrak{m}$ is its maximal ideal by **(3.5)**. Finally, K is its fraction field, because whenever $z \in K - V$, then $1/z \in V$. □

Exercise (26.3) . — Prove that a valuation ring V is normal.

Lemma (26.4). — *Let R be a domain, $\mathfrak{a}$ an ideal, $K := \operatorname{Frac}(R)$, and $x \in K^\times$. Then either $1 \notin \mathfrak{a}R[x]$ or $1 \notin \mathfrak{a}R[1/x]$.*

Proof: Assume $1 \in \mathfrak{a}R[x]$ and $1 \in \mathfrak{a}R[1/x]$. Then there are equations

$$1 = a_0 + \cdots + a_n x^n \quad \text{and} \quad 1 = b_0 + \cdots + b_m/x^m \quad \text{with all} \quad a_i, b_j \in \mathfrak{a}.$$

Assume n, m minimal and $m \le n$. Multiply through by $1 - b_0$ and $a_n x^n$, getting

$$1 - b_0 = (1 - b_0)a_0 + \cdots + (1 - b_0)a_n x^n \quad \text{and}$$
$$(1 - b_0)a_n x^n = a_n b_1 x^{n-1} + \cdots + a_n b_m x^{n-m}.$$

Combine the latter equations, getting

$$1 - b_0 = (1 - b_0)a_0 + \cdots + (1 - b_0)a_{n-1}x^{n-1} + a_n b_1 x^{n-1} + \cdots + a_n b_m x^{n-m}.$$

Simplify, getting an equation of the form $1 = c_0 + \cdots + c_{n-1}x^{n-1}$ with $c_i \in \mathfrak{a}$, which contradicts the minimality of n. □

(26.5) (Domination). — Let A, B be local rings, and $\mathfrak{m}$, $\mathfrak{n}$ their maximal ideals. We say B **dominates** A if $B \supset A$ and $\mathfrak{n} \cap A = \mathfrak{m}$; in other words, the inclusion map $\varphi\colon A \hookrightarrow B$ is a local homomorphism.

Proposition (26.6). — *Let K be a field, A a local subring. Then A is dominated by a valuation ring V of K with algebraic residue field extension.*

Proof: Let $\mathfrak{m}$ be the maximal ideal of A. There is an algebraic closure Ω of $A/\mathfrak{m}$ by (**14.13**). Form the set $\mathcal{S}$ of pairs (R, σ) with $A \subset R \subset K$ and $\sigma\colon R \to \Omega$ an extension of the quotient map $A \to A/\mathfrak{m}$. Order $\mathcal{S}$ as follows: $(R, \sigma) \le (R', \sigma')$ if $R \subset R'$ and $\sigma'|R = \sigma$. Given a totally ordered subset $\{(R_\lambda, \sigma_\lambda)\}$, set $B := \bigcup R_\lambda$ and define $\tau\colon B \to \Omega$ by $\tau(x) := \sigma_\lambda(x)$ if $x \in R_\lambda$. Plainly τ is well defined, and $(B, \tau) \in \mathcal{S}$. Thus by Zorn's Lemma, $\mathcal{S}$ has a maximal element, say (V, ρ).

Set $\mathfrak{M} := \mathrm{Ker}(\rho)$. Let's see that V is local with $\mathfrak{M}$ as maximal ideal. Indeed, $V \subset V_\mathfrak{M}$ and ρ extends to $V_\mathfrak{M}$ as $\rho(V - \mathfrak{M}) \subset \Omega^\times$. Thus maximality yields $V = V_\mathfrak{M}$.

Let's see that V is a valuation ring of K. Given $x \in K$, set $V' := V[x]$. First, suppose $1 \notin \mathfrak{M}V'$. Let's see $x \in V$. Indeed, $\mathfrak{M}V'$ lies in a maximal ideal $\mathfrak{M}'$ of V'. So $\mathfrak{M}' \cap V \supset \mathfrak{M}$, but $1 \notin \mathfrak{M}'$. So $\mathfrak{M}' \cap V = \mathfrak{M}$. Set $k := V/\mathfrak{M}$ and $k' := V'/\mathfrak{M}'$. Then $k' = k[x']$ where x' is the residue of x. But k' is a field, not a polynomial ring. So x' is algebraic over k. Thus (**10.18**)(2)⇒(1) yields k'/k is algebraic.

Let $\overline{\rho}\colon k \hookrightarrow \Omega$ be the embedding induced by ρ. Then $\overline{\rho}$ extends to an embedding $\overline{\rho}'\colon k' \hookrightarrow \Omega$ by (**14.12**). Composing with the quotient map $V' \to k'$ yields a map $\rho'\colon V' \to \Omega$ that extends ρ. Thus $(V', \rho') \in \mathcal{S}$, and $(V', \rho') \ge (V, \rho)$. By maximality, $V = V'$. Thus $x \in V$.

Similarly, set $V'' := V[1/x]$. Then $1 \notin \mathfrak{M}V''$ implies $1/x \in V$. But by (**26.4**), either $1 \notin \mathfrak{M}V'$ or $1 \notin \mathfrak{M}V''$. Thus either $x \in V$ or $1/x \in V$. Thus V is a valuation ring of K. But $(V, \rho) \in \mathcal{S}$. Thus V dominates A.

Finally, $k \hookrightarrow \Omega$. But Ω is an algebraic closure of $A/\mathfrak{m}$, so algebraic over $A/\mathfrak{m}$. Hence k is algebraic over $A/\mathfrak{m}$ too. Thus V is as desired. □

Theorem (26.7). — *Let R be any subring of a field K. Then the integral closure $\overline{R}$ of R in K is the intersection of all valuation rings V of K containing R. Further, if R is local, then the V dominating R with algebraic residue field extension suffice.*

Proof: Every valuation ring V is normal by (**26.3**). So if $V \supset R$, then $V \supset \overline{R}$. Thus $\left(\bigcap_{V \supset R} V\right) \supset \overline{R}$.

To prove the opposite inclusion, take any $x \in K - \overline{R}$. To find a valuation ring V with $V \supset R$ and $x \notin V$, set $y := 1/x$. If $1/y \in R[y]$, then for some n,

$$1/y = a_0 y^n + a_1 y^{n-1} + \cdots + a_n \quad \text{with} \quad a_\lambda \in R.$$

Multiplying by x^n yields $x^{n+1} - a_n x^n - \cdots - a_0 = 0$. So $x \in \overline{R}$, a contradiction.

Thus $1 \notin yR[y]$. So there is a maximal ideal $\mathfrak{m}$ of $R[y]$ containing y. Then the composition $R \to R[y] \to R[y]/\mathfrak{m}$ is surjective as $y \in \mathfrak{m}$. Its kernel is $\mathfrak{m} \cap R$, so $\mathfrak{m} \cap R$ is a maximal ideal of R. By (**26.6**), there is a valuation ring V that dominates $R[y]_\mathfrak{m}$ with algebraic residue field extension; whence, if R is local, then V also dominates R, and the residue field of $R[y]_\mathfrak{m}$ is equal to that of R. But $y \in \mathfrak{m}$; so $x = 1/y \notin V$, as desired. □

(26.8) (Valuations). — We call an additive abelian group Γ **totally ordered** if Γ has a subset Γ_+ that is closed under addition and satisfies $\Gamma_+ \sqcup \{0\} \sqcup -\Gamma_+ = \Gamma$.

Given $x, y \in \Gamma$, write $x > y$ if $x - y \in \Gamma_+$. Note that either $x > y$ or $x = y$ or $y > x$. Note that, if $x > y$, then $x + z > y + z$ for any $z \in \Gamma$.

Let V be a domain, and set $K := \mathrm{Frac}(V)$ and $\Gamma := K^\times/V^\times$. Write the group Γ

additively, and let $v\colon K^\times \to \Gamma$ be the quotient map. It is a homomorphism:

$$v(xy) = v(x) + v(y). \tag{26.8.1}$$

Set $\Gamma_+ := v\big(V - 0\big) - 0$. Then Γ_+ is closed under addition. Plainly, V is a valuation ring if and only if $-\Gamma_+ \sqcup \{0\} \sqcup \Gamma_+ = \Gamma$, so if and only if Γ is totally ordered.

As a convention, set $v(0) := \infty$. Note that **(26.8.1)** remains valid.

Assume V is a valuation ring. Let's prove that, for all $x, y \in K$,

$$v(x+y) \ge \min\{v(x),\, v(y)\}. \tag{26.8.2}$$

Indeed, say $v(x) \ge v(y)$ and $y \ne 0$. Then $z := x/y \in V$. So $z + 1 \in V$. So $v(z+1) \ge 0$. But $x + y = (z+1)y$. Thus

$$v(x+y) = v(z+1) + v(y) \ge v(y) = \min\{v(x), v(y)\}.$$

Note that **(26.8.1)** and **(26.8.2)** are the same as (1) and (2) of **(23.1)**.

Conversely, start with a field K, with a totally ordered additive abelian group Γ, and with a surjective homomorphism $v\colon K^\times \to \Gamma$ satisfying **(26.8.2)**. Set

$$V := \{x \in K^\times \mid v(x) \ge 0\} \cup \{0\}.$$

Then V is a valuation ring, and $\Gamma = K^\times/V^\times$. We call such a v a **valuation** of K, and Γ the **value group** of v or of V.

For example, a DVR V of K is just a valuation ring with value group $\mathbb{Z}$, since any $x \in K^\times$ has the form $x = ut^n$ with $u \in V^\times$, with t a uniformizing parameter, and with $n \in \mathbb{Z}$.

Example (26.9). — Fix a totally ordered additive abelian group Γ, and a field k. Form the k-vector space R on the symbols X^a for $a \in \Gamma$ as basis. Define $X^a X^b := X^{a+b}$, and extend this product to R by linearity. Then R is a k-algebra with $X^0 = 1$. We call R the **group algebra** of Γ.

Given $x = \sum r_a X^a \in (R - 0)$, set

$$v(x) := \min\{a \mid r_a \ne 0\} \in \Gamma \quad\text{and}\quad \mathrm{IT}(x) := r_{v(x)} X^{v(x)} \in (R - 0).$$

Given $y \in (R - 0)$, note that $\mathrm{IT}(x)\,\mathrm{IT}(y) \ne 0$ since R is a domain. Therefore, $\mathrm{IT}(xy) = \mathrm{IT}(x)\,\mathrm{IT}(y)$. Thus R is a domain, and $v(xy) = v(x) + v(y)$. Further, if $v(x+y) = a$, then either $v(x) \le a$ or $v(y) \le a$. Thus $v(x+y) \ge \min\{v(x),\, v(y)\}$.

Set $K := \mathrm{Frac}(R)$. Extend v to $v\colon K^\times \to \Gamma$ by $v(x/y) := v(x) - v(y)$. Plainly v is well defined, surjective, and a group homomorphism. Further, for $x, y \in K^\times$, plainly $v(x+y) \ge \min\{v(x),\, v(y)\}$. Thus v is a valuation with group Γ.

Set $v(0) := \infty$ and $R' := \{x \in R \mid v(x) \ge 0\}$ and $\mathfrak{p} := \{x \in R \mid v(x) > 0\}$. Plainly, R' is a ring, and $\mathfrak{p}$ is a prime of R'. Further, $R'_{\mathfrak{p}}$ is the valuation ring of v.

There are many choices for Γ other than $\mathbb{Z}$. Examples include the additive rationals, the additive reals, its subgroup generated by two incommensurate reals, and the lexicographically ordered product of any two totally ordered abelian groups.

Proposition (26.10). — *Let v be a valuation of a field K, and $x_1, \dots, x_n \in K$ with $n \ge 2$. Set $v(0) := \infty$ and $m := \min\{v(x_i)\}$.*

(1) *If $n = 2$ and if $v(x_1) \ne v(x_2)$, then $v(x_1 + x_2) = m$.*

(2) *If $x_1 + \cdots + x_n = 0$, then $m = v(x_i) = v(x_j)$ for some $i \ne j$.*

Proof: For (1), say $v(x_1) > v(x_2)$; so $v(x_2) = m$. Set $z := x_1/x_2$. Then $v(z) > 0$. Also $v(z+1) \ge \min\{v(z),\, v(1)\} \ge 0$ and $v(-z) = v(z) + v(-1) > 0$. Now,

$$0 = v(1) = v(z+1-z) \ge \min\{v(z+1),\ v(-z)\} \ge 0.$$

Hence $v(z+1) = 0$. But $x_1 + x_2 = (z+1)x_2$. Thus $v(x_1+x_2) = v(x_2) = m$.

For (2), suppose $m = v(x_1)$ but $v(x_i) > m$ for $i \ge 2$. Set $x := x_2 + \cdots + x_n$. By induction, **(26.8.2)** yields $v(x) \ge \min_{i\ge 2}\{v(x_i)\} > m$. So $v(x_1 + x) = m$ by (1). So $v(0) = m < \infty$, a contradiction. Thus (2) holds. □

Exercise (26.11) . — Let V be a valuation ring. Prove these statements:

(1) Every finitely generated ideal $\mathfrak{a}$ is principal.

(2) V is Noetherian if and only if V is a DVR.

Lemma (26.12). — *Let R be a 1-dimensional Noetherian domain, K its fraction field, M a torsionfree module, and $x \in R$ nonzero. Then $\ell(R/xR) < \infty$. Further,*

$$\ell(M/xM) \le \dim_K(M \otimes_R K)\, \ell(R/xR), \tag{26.12.1}$$

with equality if M is finitely generated.

Proof: Set $r := \dim_K(M \otimes_R K)$. If $r = \infty$, then **(26.12.1)** is trivial; so we may assume $r < \infty$.

Given any module N, set $N_K := S_0^{-1}N$ with $S_0 := R - 0$. Recall $N_K = N \otimes_R K$.

First, assume M is finitely generated. Choose any K-basis $m_1/s_1, \ldots, m_r/s_r$ of M_K with $m_i \in M$ and $s_i \in S_0$. Then $m_1/1, \ldots, m_r/1$ is also a basis. Define an R-map $\alpha\colon R^r \to M$ by sending the standard basis elements to the m_i. Then its localization α_K is an K-isomorphism. But $\mathrm{Ker}(\alpha)$ is a submodule of R^r, so torsionfree. And $S_0^{-1}\,\mathrm{Ker}(\alpha) = \mathrm{Ker}(\alpha_K) = 0$. So $\mathrm{Ker}(\alpha) = 0$. Thus α is injective.

Set $N := \mathrm{Coker}(\alpha)$. Then $N_K = 0$, and N is finitely generated. Hence, $\mathrm{Supp}(N)$ is a proper closed subset of $\mathrm{Spec}(R)$ by **(13.4)**(3). But $\dim(R) = 1$ by hypothesis. Hence, $\mathrm{Supp}(N)$ consists entirely of maximal ideals. So $\ell(N) < \infty$ by **(19.4)**.

Similarly, $\mathrm{Supp}(R/xR)$ is closed and proper in $\mathrm{Spec}(R)$. So $\ell(R/xR) < \infty$.

Consider the standard exact sequence:

$$0 \to N' \to N \xrightarrow{\mu_x} N \to N/xN \to 0 \quad \text{where} \quad N' := \mathrm{Ker}(\mu_x).$$

Apply Additivity of Length, **(19.7)**; it yields $\ell\big(N'\big) = \ell(N/xN)$.

Since M is torsionfree, $\mu_x\colon M \to M$ is injective. Consider this commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & R^r \arrow[r, "\alpha"] \arrow[d, "\mu_x"'] & M \arrow[r] \arrow[d, "\mu_x"'] & N \arrow[r] \arrow[d, "\mu_x"'] & 0 \\
0 \arrow[r] & R^r \arrow[r, "\alpha"] & M \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

Apply the Snake Lemma **(5.10)**. It yields this exact sequence:

$$0 \to N' \to (R/xR)^r \to M/xM \to N/xN \to 0.$$

Hence $\ell(M/xM) = \ell\big((R/xR)^r\big)$ by additivity. But $\ell\big((R/xR)^r\big) = r\,\ell(R/xR)$ also by additivity. Thus equality holds in **(26.12.1)** when M is finitely generated.

Second, assume M is arbitrary, but **(26.12.1)** fails. Then M possesses a finitely generated submodule M' whose image H in M/xM satisfies $\ell(H) > r\ell(R/xR)$. Now, $M_K \supset M'_K$; so $r \ge \dim_K(M'_K)$. Therefore,

$$\ell(M'/xM') \ge \ell(H) > r\,\ell(R/xR) \ge \dim_K(M'_K)\,\ell\big(R/xR\big).$$

However, together these inequalities contradict the first case with M' for M. □

Theorem (26.13) (Krull–Akizuki). — *Let R be a 1-dimensional Noetherian domain, K its fraction field, K' a finite extension field, and R' a proper subring of K' containing R. Then R' is, like R, a 1-dimensional Noetherian domain.*

Proof: Given a nonzero ideal $\mathfrak{a}'$ of R', take any nonzero $x \in \mathfrak{a}'$. Since K'/K is finite, there is an equation $a_n x^n + \cdots + a_0 = 0$ with $a_i \in R$ and $a_0 \neq 0$. Then $a_0 \in \mathfrak{a}' \cap R$. Further, (26.12) yields $\ell(R/a_0R) < \infty$.

Plainly, R' is a domain, so a torsionfree R-module. Also $R' \otimes_R K = S_0^{-1}R' \subset K'$; hence, $\dim_K(R' \otimes_R K) < \infty$. Therefore, (26.12) yields $\ell_R(R'/a_0R') < \infty$.

But $\mathfrak{a}'/a_0R' \subset R'/a_0R'$. So $\ell_R(\mathfrak{a}'/a_0R') < \infty$. So $\mathfrak{a}'/a_0R'$ is finitely generated over R by (19.2)(3). Hence $\mathfrak{a}'$ is finitely generated over R'. Thus R' is Noetherian.

Set $R'' := R'/a_0R'$. Plainly, $\ell_{R''}R'' \le \ell_R R''$. So $\ell_{R''}R'' < \infty$. So, in R'', every prime is maximal by (19.4). So if $\mathfrak{a}'$ is prime, then $\mathfrak{a}'/a_0R'$ is maximal, whence $\mathfrak{a}'$ maximal. So in R, every nonzero prime is maximal. Thus R' is 1-dimensional. □

Corollary (26.14). — *Let R be a 1-dimensional Noetherian domain, such as a Dedekind domain. Let K be its fraction field, K' a finite extension field, and R' the normalization of R in K'. Then R' is Dedekind.*

Proof: Since R is 1-dimensional, it's not a field. But R' is the normalization of R. So R' is not a field by (14.1). Hence, R' is Noetherian and 1-dimensional by (26.13). Thus R' is Dedekind by (24.1). □

Corollary (26.15). — *Let K'/K be a field extension, V' a valuation ring of K' not containing K. Set $V := V' \cap K$. Then V is a DVR if V' is, and the converse holds if K'/K is finite.*

Proof: It follows easily from (26.1) that V is a valuation ring, and from (26.8) that its value group is a subgroup of that of V'. Now, a nonzero subgroup of $\mathbb{Z}$ is a copy of $\mathbb{Z}$. Thus V is a DVR if V' is.

Conversely, assume V is a DVR, so Noetherian and 1-dimensional. Now, $V' \not\supset K$, so $V' \subsetneq K'$. Hence, V' is Noetherian by (26.13), so a DVR by (26.11)(2). □

B. Exercises

Exercise (26.16) . — Let V be a domain. Show that V is a valuation ring if and only if, given any two ideals $\mathfrak{a}$ and $\mathfrak{b}$, either $\mathfrak{a}$ lies in $\mathfrak{b}$ or $\mathfrak{b}$ lies in $\mathfrak{a}$.

Exercise (26.17) . — Let V be a valuation ring of K, and $V \subset W \subset K$ a subring. Prove that W is also a valuation ring of K, that its maximal ideal $\mathfrak{p}$ lies in V, that $V/\mathfrak{p}$ is a valuation ring of the field $W/\mathfrak{p}$, and that $W = V_{\mathfrak{p}}$.

Exercise (26.18) . — Let K be a field, $\mathcal{S}$ the set of local subrings ordered by domination. Show that the valuation rings of K are the maximal elements of $\mathcal{S}$.

Exercise (26.19) . — Let V be a valuation ring of a field K. Let $\varphi\colon V \to R$ and $\psi\colon R \to K$ be ring maps. Assume $\operatorname{Spec}(\varphi)$ is closed and $\psi\varphi\colon V \to K$ is the inclusion. Set $W := \psi(R)$. Show $W = V$.

Exercise (26.20) . — Let $\varphi\colon R \to R'$ be a map of rings. Prove that, if R' is integral over R, then for any R-algebra C, the map $\operatorname{Spec}(\varphi \otimes_R C)$ is closed; further, the converse holds if also R' has only finitely many minimal primes. To prove the converse, start with the case where R' is a domain, take C to be an arbitrary valuation ring of $\operatorname{Frac}(R')$ containing $\varphi(R)$, and apply **(26.19)**.

Exercise (26.21) . — Let V be a valuation ring with valuation $v\colon K^\times \to \Gamma$, and $\mathfrak{p}$ a prime of V. Set $\Delta := v(V_\mathfrak{p}^\times)$. Prove the following statements:

(1) Δ and Γ/Δ are the valuation groups of the valuation rings $V/\mathfrak{p}$ and $V_\mathfrak{p}$.
(2) $v(V - \mathfrak{p})$ is the set of nonnegative elements $\Delta_{\geq 0}$ of Δ, and $\mathfrak{p} = V - v^{-1}\Delta_{\geq 0}$.
(3) Δ is **isolated** in Γ; that is, given $\alpha \in \Delta$ and $0 \leq \beta \leq \alpha$, also $\beta \in \Delta$.

Exercise (26.22) . — Let V be a valuation ring with valuation $v\colon K^\times \to \Gamma$. Prove that $\mathfrak{p} \mapsto v(V_\mathfrak{p}^\times)$ is a bijection γ from the primes $\mathfrak{p}$ of V onto the isolated subgroups Δ of Γ and that its inverse is $\Delta \mapsto V - v^{-1}\Delta_{\geq 0}$.

Exercise (26.23) . — Let V be a valuation ring, such as a DVR, whose value group Γ is **Archimedean**; that is, given any nonzero $\alpha, \beta \in \Gamma$, there's $n \in \mathbb{Z}$ such that $n\alpha > \beta$. Show that V is a maximal proper subring of its fraction field K.

Exercise (26.24) . — Let R be a Noetherian domain, $K := \operatorname{Frac}(R)$, and L a finite extension field (possibly $L = K$). Prove the integral closure $\overline{R}$ of R in L is the intersection of all DVRs V of L containing R by modifying the proof of **(26.7)**: show y is contained in a height-1 prime $\mathfrak{p}$ of $R[y]$ and apply **(26.14)** to $R[y]_\mathfrak{p}$.

A Term of Commutative Algebra
Solutions

By Allen ALTMAN
and Steven KLEIMAN

$$\begin{tikzcd}
 & & R/\mathfrak{a} \arrow[dl, "\psi"] \arrow[dd, "1"] \\
R \arrow[urr, "\kappa"] \arrow[r, "\varphi"] \arrow[drr, "\kappa"'] & R' \arrow[dr, "\psi'"] & \\
 & & R/\mathfrak{a}
\end{tikzcd}$$

Worldwide Center of Mathematics

Part II

Solutions

1. Rings and Ideals

Exercise (1.13) . — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$, $\mathfrak{a}_1$, $\mathfrak{a}_2$ ideals of R, and $\mathfrak{b}$, $\mathfrak{b}_1$, $\mathfrak{b}_2$ ideals of R'. Prove the following statements:

(1a)	$(\mathfrak{a}_1+\mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$.	(1b)	$(\mathfrak{b}_1+\mathfrak{b}_2)^c \supset \mathfrak{b}_1^c + \mathfrak{b}_2^c$.
(2a)	$(\mathfrak{a}_1\cap\mathfrak{a}_2)^e \subset \mathfrak{a}^e \cap \mathfrak{a}_2^e$.	(2b)	$(\mathfrak{b}_1\cap\mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.
(3a)	$(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$.	(3b)	$(\mathfrak{b}_1\mathfrak{b}_2)^c \supset \mathfrak{b}_1^c\mathfrak{b}_2^c$.
(4a)	$(\mathfrak{a}_1:\mathfrak{a}_2)^e \subset (\mathfrak{a}_1^e:\mathfrak{a}_2^e)$.	(4b)	$(\mathfrak{b}_1:\mathfrak{b}_2)^c \subset (\mathfrak{b}_1^c:\mathfrak{b}_2^c)$.

Solution: For (1a), note $\mathfrak{a}_i^e \subset (\mathfrak{a}_1+\mathfrak{a}_2)^e$. So $\mathfrak{a}_1^e+\mathfrak{a}_2^e \subset (\mathfrak{a}_1+\mathfrak{a}_2)^e$. Conversely, given $z \in (\mathfrak{a}_1+\mathfrak{a}_2)^e$, there are $a_{ij} \in \mathfrak{a}_i$ and $y_j \in R'$ with $z = \sum(a_{1j}+a_{2j})y_j$. Then $z = \sum a_{1j}y_j + \sum a_{2j}y_j$. So $z \in \mathfrak{a}_1^e+\mathfrak{a}_2^e$. Thus $(\mathfrak{a}_1+\mathfrak{a}_2)^e \subset \mathfrak{a}_1^e+\mathfrak{a}_2^e$. Thus (1a) holds.

For (1b), given $b_i \in \mathfrak{b}_i^c$ for $i=1,2$, note $\varphi(b_i) \in \mathfrak{b}_i$. But $\varphi(b_1+b_2) = \varphi(b_1)+\varphi(b_2)$. Hence $\varphi(b_1+b_2) \in \mathfrak{b}_1+\mathfrak{b}_2$. So $b_1+b_2 \in (\mathfrak{b}_1+\mathfrak{b}_2)^c$. Thus (1b) holds.

For (2a), note $\mathfrak{a}_1\cap\mathfrak{a}_2 \subset \mathfrak{a}_i$. So $(\mathfrak{a}_1\cap\mathfrak{a}_2)^e \subset \mathfrak{a}_i^e$, Thus (2a) holds.

For (2b), note similarly $(\mathfrak{b}_1\cap\mathfrak{b}_2)^c \subset \mathfrak{b}_1^c\cap\mathfrak{b}_2^c$. Conversely, given $b \in \mathfrak{b}_1^c\cap\mathfrak{b}_2^c$, note $\varphi(b) \in \mathfrak{b}_1\cap\mathfrak{b}_2$. Thus $b \in (\mathfrak{b}_1\cap\mathfrak{b}_2)^c$. Thus (2b) holds.

For (3a), note both $(\mathfrak{a}_1\mathfrak{a}_2)^e$ and $\mathfrak{a}_1^e\mathfrak{a}_2^e$ are generated by the products a_1a_2 with $a_i \in \mathfrak{a}_i$. Thus (3a) holds.

For (3b), given $b_i \in \mathfrak{b}_i^c$ for $i=1,2$, note $\varphi(b_1b_2) = \varphi(b_1)\varphi(b_2) \in \mathfrak{b}_1\mathfrak{b}_2$. Hence $b_1b_2 \in (\mathfrak{b}_1\mathfrak{b}_2)^c$. Thus (3b) holds.

For (4a), given $x \in (\mathfrak{a}_1:\mathfrak{a}_2)$ and $a_2 \in \mathfrak{a}_2$, note $xa_2 \in \mathfrak{a}_1$. So $\varphi(xa_2) \in \mathfrak{a}_1^e$. But $\varphi(xa_2) = \varphi(x)\varphi(a_2)$. So $\varphi(x)\varphi(a_2) \in \mathfrak{a}_1^e$. But the $\varphi(a_2)$ generate $\mathfrak{a}_2^e$. So $\varphi(x)\mathfrak{a}_2^e \subset \mathfrak{a}_1^e$. So $\varphi(x) \in (\mathfrak{a}_1^e:\mathfrak{a}_2^e)$. But the $\varphi(x)$ generate $(\mathfrak{a}_1:\mathfrak{a}_2)^e$. So (4a) holds.

For (4b), given $x \in (\mathfrak{b}_1:\mathfrak{b}_2)^c$ and $b_2 \in \mathfrak{b}_2^c$, note $\varphi(xb_2) = \varphi(x)\varphi(b_2) \in \mathfrak{b}_1$. So $xb_2 \in \mathfrak{b}_1^c$. Thus (4b) holds. □

Exercise (1.14) . — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Prove the following statements:

(1) Then $\mathfrak{a}^{ec} \supset \mathfrak{a}$ and $\mathfrak{b}^{ce} \subset \mathfrak{b}$. (2) Then $\mathfrak{a}^{ece} = \mathfrak{a}^e$ and $\mathfrak{b}^{cec} = \mathfrak{b}^c$.

(3) If $\mathfrak{b}$ is an extension, then $\mathfrak{b}^c$ is the largest ideal of R with extension $\mathfrak{b}$.

(4) If two extensions have the same contraction, then they are equal.

Solution: For (1), given $x \in \mathfrak{a}$, note $\varphi(x) = x\cdot 1 \in \mathfrak{a}R'$. So $x \in \varphi^{-1}(\mathfrak{a}R')$, or $x \in \mathfrak{a}^{ec}$. Thus $\mathfrak{a} \subset \mathfrak{a}^{ec}$. Next, $\varphi(\varphi^{-1}\mathfrak{b}) \subset \mathfrak{b}$. But $\mathfrak{b}$ is an ideal of R'. So $\varphi(\varphi^{-1}\mathfrak{b})R' \subset \mathfrak{b}$, or $\mathfrak{b}^{ce} \subset \mathfrak{b}$. Thus (1) holds.

For (2), note $\mathfrak{a}^{ece} \subset \mathfrak{a}^e$ by (1) applied with $\mathfrak{b} := \mathfrak{a}^e$. But $\mathfrak{a} \subset \mathfrak{a}^{ec}$ by (1); so $\mathfrak{a}^e \subset \mathfrak{a}^{ece}$. Thus $\mathfrak{a}^e = \mathfrak{a}^{ece}$. Similarly, $\mathfrak{b}^{cec} \supset \mathfrak{b}^c$ by (1) applied with $\mathfrak{a} := \mathfrak{b}^c$. But $\mathfrak{b}^{ce} \subset \mathfrak{b}$ by (1); so $\mathfrak{b}^{cec} \subset \mathfrak{b}^c$. Thus $\mathfrak{b}^{cec} = \mathfrak{b}^c$. Thus (2) holds.

For (3), say $\mathfrak{b} = \mathfrak{a}^e$. Then $\mathfrak{b}^{ce} = \mathfrak{a}^{ece}$. But $\mathfrak{a}^{ece} = \mathfrak{a}^e$ by (2). Hence $\mathfrak{b}^c$ has extension $\mathfrak{b}$. Further, it's the largest such ideal, as $\mathfrak{a}^{ec} \supset \mathfrak{a}$ by (1). Thus (3) holds.

For (4), say $\mathfrak{b}_1^c = \mathfrak{b}_2^c$ for extensions $\mathfrak{b}_i$. Then $\mathfrak{b}_i^{ce} = \mathfrak{b}_i$ by (3). Thus (4) holds. □

Exercise (1.15) . — Let R be a ring, $\mathfrak{a}$ an ideal, $\mathcal{X}$ a set of variables. Prove:

(1) The extension $\mathfrak{a}\big(R[\mathcal{X}]\big)$ is the set $\mathfrak{a}[\mathcal{X}]$ of polynomials with coefficients in $\mathfrak{a}$.

(2) $\mathfrak{a}\big(R[\mathcal{X}]\big) \cap R = \mathfrak{a}$.

Solution: For (1), use double inclusion. Given $F \in \mathfrak{a}\big(R[\mathcal{X}]\big)$, say $F = \sum_i a_iF_i$ where $a_i \in \mathfrak{a}$ and where $F_i = \sum_j a_{ij}\mathbf{M}_j$ with $a_{ij} \in R$ and with $\mathbf{M}_j$ a monomial in the variables. Then $F = \sum_j(\sum_i a_ia_{ij})\mathbf{M}_j \in \mathfrak{a}[\mathcal{X}]$.

Conversely, given $F \in \mathfrak{a}[\mathcal{X}]$, say $F = \sum a_j\mathbf{M}_j$ with $a_j \in \mathfrak{a}$ and $\mathbf{M}_j$ a monomial in the variables. Then $a_j\mathbf{M}_j \in \mathfrak{a}\big(R[\mathcal{X}]\big)$. Thus $F \in \mathfrak{a}\big(R[\mathcal{X}]\big)$. Thus (1) holds.

For (2), note that plainly $\mathfrak{a}[\mathcal{X}] \cap R = \mathfrak{a}$. Thus (1) implies (2). □

Exercise (1.16) . — Let R be a ring, $\mathfrak{a}$ an ideal, and $\mathcal{X}$ a set of variables. Set $P := R[\mathcal{X}]$. Prove $P/\mathfrak{a}P = (R/\mathfrak{a})[\mathcal{X}]$.

Solution: Say $\mathcal{X} =: \{X_\lambda\}$. Let $\kappa\colon R \to R/\mathfrak{a}$ be the quotient map. By **(1.3)**, there is a unique ring map $\varphi\colon P \to (R/\mathfrak{a})[\mathcal{X}]$ with $\varphi|R = \kappa$ and $\varphi(X_\lambda) = X_\lambda$ for all λ. As κ is surjective, so is φ. But $\operatorname{Ker}(\varphi)$ consists of the polynomials whose coeffients map to 0 under κ, that is, lie in $\mathfrak{a}$. Hence $\operatorname{Ker}(\varphi) = \mathfrak{a}P$ by **(1.15)**. Thus φ induces an isomorphism $P/\mathfrak{a}P \xrightarrow{\sim} (R/\mathfrak{a})[\mathcal{X}]$ by **(1.5.1)**, as desired.

Alternatively, the two R-algebras are equal, as they have the same UMP: each is universal among R-algebras R' with distinguished elements x_λ and with $\mathfrak{a}R' = 0$. Namely, the structure map $\varphi\colon R \to R'$ factors through a unique map $\pi\colon P \to R'$ such that $\pi(X_\lambda) = x_\lambda$ for all λ by **(1.3)**; then π factors through a unique map $P/\mathfrak{a}P \to R'$ as $\mathfrak{a}R' = 0$ by **(1.5)**. On the other hand, φ factors through a unique map $\psi\colon R/\mathfrak{a} \to R'$ as $\mathfrak{a}R' = 0$ by **(1.5)**; then ψ factors through a unique map $(R/\mathfrak{a})[\mathcal{X}] \to R'$ such that $\pi(X_\lambda) = x_\lambda$ for all λ by **(1.3)**. □

Exercise (1.17) . — Let R be a ring, $P := R[\{X_\lambda\}]$ the polynomial ring in variables X_λ for $\lambda \in \Lambda$, and $(x_\lambda) \in R^\Lambda$ a vector. Let $\pi_{(x_\lambda)}\colon P \to R$ denote the R-algebra map defined by $\pi_{(x_\lambda)}X_\mu := x_\mu$ for all $\mu \in \Lambda$. Show:

(1) Any $F \in P$ has the form $F = \sum a_{(i_1,\dots,i_n)}(X_{\lambda_1} - x_{\lambda_1})^{i_1} \cdots (X_{\lambda_n} - x_{\lambda_n})^{i_n}$ for unique $a_{(i_1,\dots,i_n)} \in R$.
(2) Then $\operatorname{Ker}(\pi_{(x_\lambda)}) = \{F \in P \mid F\big((x_\lambda)\big) = 0\} = \langle\{X_\lambda - x_\lambda\}\rangle$.
(3) Then π induces an isomorphism $P/\langle\{X_\lambda - x_\lambda\}\rangle \xrightarrow{\sim} R$.
(4) Given $F \in P$, its residue in $P/\langle\{X_\lambda - x_\lambda\}\rangle$ is equal to $F\big((x_\lambda)\big)$.
(5) Let $\mathcal{Y}$ be a second set of variables. Then $P[\mathcal{Y}]/\langle\{X_\lambda - x_\lambda\}\rangle \xrightarrow{\sim} R[\mathcal{Y}]$.

Solution: For (1), as in **(1.8)**, let $\varphi_{(x_\lambda)}$ be the R-automorphism of P defined by $\varphi_{(x_\lambda)}X_\mu := X_\mu + x_\mu$ for all $\mu \in \Lambda$. Say $\varphi_{(x_\lambda)}F = \sum a_{(i_1,\dots,i_n)}X_{\lambda_1}^{i_1}\cdots X_{\lambda_n}^{i_n}$. Note the $a_{(i_1,\dots,i_n)} \in R$ are unique. Also $\varphi_{(x_\lambda)}^{-1}\varphi_{(x_\lambda)}F = F$. Recall $\varphi_{(x_\lambda)}^{-1} = \varphi_{(-x_\lambda)}$. Thus **(1.3.1)** with $\pi := \varphi_{(x_\lambda)}^{-1}$ yields (1).

For (2), given $F \in P$, note $\pi_{(x_\lambda)}F = F\big((x_\lambda)\big)$ by **(1.3.1)**. Thus $F \in \operatorname{Ker}(\pi_{(x_\lambda)})$ if and only if $F\big((x_\lambda)\big) = 0$. Now, if $F = \sum(X_\lambda - x_\lambda)F_\lambda$ with $F_\lambda \in P$, then $F\big((x_\lambda)\big) = \sum 0 \cdot F_\lambda\big((x_\lambda)\big) = 0$. Conversely, if $F\big((x_\lambda)\big) = 0$, then $a_{(0,\dots,0)} = 0$ in (1), and so $F \in \langle\{X_\lambda - x_\lambda\}\rangle$ by (1) again. Thus (2) holds.

For (3), note $\pi_{(x_\lambda)}$ is surjective as it's an R-map. Thus (2) and **(1.5.1)** yield (3).

For (4), again note $\pi_{(x_\lambda)}F = F\big((x_\lambda)\big)$ by **(1.3.1)**. Thus (3) yields (4).

For (5), set $R' := R[\mathcal{Y}]$. So $P[\mathcal{Y}] = R'[\{X_\lambda\}]$. So (3) with R' for R yields (4). □

Exercise (1.18) . — Let R be a ring, $P := R[X_1,\dots,X_n]$ the polynomial ring in variables X_i. Given $F = \sum a_{(i_1,\dots,i_n)}X_1^{i_1}\cdots X_n^{i_n} \in P$, formally set

$$\partial F/\partial X_j := \sum i_j a_{(i_1,\dots,i_n)}X_1^{i_1}\cdots X_n^{i_n}/X_j \in P \quad \text{for } j = 1,\dots,n. \qquad \textbf{(1.18.1)}$$

Given $(x_1,\dots,x_n) \in R^n$, set $\mathbf{x} := (x_1,\dots,x_n)$, set $a_j := (\partial F/\partial X_j)(\mathbf{x})$, and set $\mathfrak{M} := \langle X_1 - x_1,\dots,X_n - x_n\rangle$. Show $F = F(\mathbf{x}) + \sum a_j(X_j - x_j) + G$ with $G \in \mathfrak{M}^2$. First show that, if $F = (X_1 - x_1)^{i_1}\cdots(X_n - x_n)^{i_n}$, then $\partial F/\partial X_j = i_jF/(X_j - x_j)$.

Solution: For any i, note $(X_j - x_j)^i = \sum_{p=0}^{i} \binom{i}{p} X_j^p x_j^{i-p}$ and

$$\sum_p \binom{i}{p} p X_j^{p-1} x_j^{i-p} = \sum_p i \binom{i-1}{p-1} X_j^{p-1} x_j^{i-p} = i(X_j - x_j)^{i-1}.$$

Thus, if $F = (X_1 - x_1)^{i_1} \cdots (X_n - x_n)^{i_n}$, then $\partial F/\partial X_j = i_j F/(X_j - x_j)$.

In general, by (**1.17**)(1), there are (unique) $b_{(i_1,\dots,i_n)} \in R$ such that

$$F = \sum b_{(i_1,\dots,i_n)} (X_1 - x_1)^{i_1} \cdots (X_n - x_n)^{i_n}$$

Plainly, $b_{(0,\dots,0)} = F(\mathbf{x})$. Moreover, by linearity, the first case yields

$$\partial F/\partial X_j = \sum i_j b_{(i_1,\dots,i_n)} (X_1 - x_1)^{i_1} \cdots (X_n - x_n)^{i_n}/(X_j - x_j).$$

Thus $(\partial F/\partial X_j)(\mathbf{x}) = b_{(\delta_{1j},\dots,\delta_{nj})}$ where δ_{ij} is the Kronecker delta, as desired. □

Exercise (1.19) . — Let R be a ring, X a variable, $F \in P := R[X]$, and $a \in R$. Set $F' := \partial F/\partial X$; see (**1.18.1**). We call a a **root** of F if $F(a) = 0$, a **simple root** if also $F'(a) \neq 0$, and a **supersimple root** if also $F'(a)$ is a unit.

Show that a is a root of F if and only if $F = (X - a)G$ for some $G \in P$, and if so, then G is unique: that a is a simple root if and only if also $G(a) \neq 0$; and that a is a supersimple root if and only if also $G(a)$ is a unit.

Solution: By (**1.17**)(1), there are $a_i \in R$ such that $F = \sum_{i=0}^{n} a_i (X - a)^i$. Set $G(X) := \sum_{i=1}^{n} a_i (X - a)^{i-1}$. Then $F(a) = a_0$. So a is a root if and only if $a_0 = 0$; thus (if and) only if $F = (X - a)G(X)$.

Suppose $F = (X - a)H$. Then $F(a) = 0$, or a is a root. So $(X - a)(G - H) = 0$. But $X - a$ is monic. So $G - H = 0$. Thus G is unique.

Assume a is a root. Then $F = F'(a)(X - a) + H$ with $H \in \langle X - a\rangle^2$ by (**1.18**). But $F = a_1(X - a) + (X - a)^2 \sum_{i=2}^{n} a_i (X - a)^{i-2}$. So $(F'(a) - a_1)(X - a) \in \langle X - a\rangle^2$. But $F'(a) - a_1 \in R$. So $F'(a) - a_1 = 0$. But also $G(a) = a_1$. Thus a is simple if and only if $G(a) \neq 0$, and a is supersimple if and only if $G(a)$ is a unit. □

Exercise (1.20) . — Let R be a ring, $P := R[X_1, \dots, X_n]$ the polynomial ring, $F \in P$ of degree d, and $F_i := X_i^{d_i} + a_1 X_i^{d_i - 1} + \cdots$ a monic polynomial in X_i alone for all i. Find $G, G_i \in P$ such that $F = \sum_{i=1}^{n} F_i G_i + G$ where $G_i = 0$ or $\deg(G_i) \leq d - d_i$ and where the highest power of X_i in G is less than d_i.

Solution: By linearity, we may assume $F := X_1^{m_1} \cdots X_n^{m_n}$. If $m_i < d_i$ for all i, set $G_i := 0$ and $G := F$, and we're done. Else, fix i with $m_i \geq d_i$, and set $G_i := F/X_i^{d_i}$ and $G := (-a_1 X_i^{d_i - 1} - \cdots)G_i$. Plainly, $F = F_i G_i + G$ and $\deg(G_i) d - d_i$. Replace F by G, and repeat from the top. The algorithm terminates because on each iteration, $\deg(G) < \deg(F)$. □

Exercise (1.21) (*Chinese Remainder Theorem*) . — Let R be a ring.

(1) Let $\mathfrak{a}$ and $\mathfrak{b}$ be **comaximal** ideals; that is, $\mathfrak{a} + \mathfrak{b} = R$. Show

$$\text{(a)}\ \ \mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b} \quad \text{and} \quad \text{(b)}\ \ R/\mathfrak{a}\mathfrak{b} = (R/\mathfrak{a}) \times (R/\mathfrak{b}).$$

(2) Let $\mathfrak{a}$ be comaximal to both $\mathfrak{b}$ and $\mathfrak{b}'$. Show $\mathfrak{a}$ is also comaximal to $\mathfrak{b}\mathfrak{b}'$.

(3) Given $m, n \geq 1$, show $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal if and only if $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are.

(4) Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be pairwise comaximal. Show:

(a) $\mathfrak{a}_1$ and $\mathfrak{a}_2 \cdots \mathfrak{a}_n$ are comaximal;
(b) $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdots \mathfrak{a}_n$;
(c) $R/(\mathfrak{a}_1 \cdots \mathfrak{a}_n) \xrightarrow{\sim} \prod (R/\mathfrak{a}_i)$.

(5) Find an example where $\mathfrak{a}$ and $\mathfrak{b}$ satisfy (1)(a), but aren't comaximal.

Solution: For (1)(a), note that always $\mathfrak{ab} \subseteqq \mathfrak{a}\cap\mathfrak{b}$. Conversely, $\mathfrak{a}+\mathfrak{b}=R$ implies $x+y=1$ with $x\in\mathfrak{a}$ and $y\in\mathfrak{b}$. So given $z\in\mathfrak{a}\cap\mathfrak{b}$, we have $z=xz+yz\in\mathfrak{ab}$.

For (1)(b), form the map $R\to R/\mathfrak{a}\times R/\mathfrak{b}$ that carries an element to its pair of residues. The kernel is $\mathfrak{a}\cap\mathfrak{b}$, which is $\mathfrak{ab}$ by (1)(a). So we have an injection

$$\varphi\colon R/\mathfrak{ab}\hookrightarrow R/\mathfrak{a}\times R/\mathfrak{b}.$$

To show that φ is surjective, take any element $(\bar{x},\bar{y})$ in $R/\mathfrak{a}\times R/\mathfrak{b}$. Say $\bar{x}$ and $\bar{y}$ are the residues of x and y. Since $\mathfrak{a}+\mathfrak{b}=R$, we can find $a\in\mathfrak{a}$ and $b\in\mathfrak{b}$ such that $a+b=y-x$. Then $\varphi(x+a)=(\bar{x},\bar{y})$, as desired. Thus φ is surjective, so bijective.

For (2), note $R=(\mathfrak{a}+\mathfrak{b})(\mathfrak{a}+\mathfrak{b}')=(\mathfrak{a}^2+\mathfrak{ba}+\mathfrak{ab}')+\mathfrak{bb}'\subseteqq\mathfrak{a}+\mathfrak{bb}'\subseteqq R$.

For (3), first assume $\mathfrak{a}$ and $\mathfrak{b}$ are comaximal. Then (2) implies $\mathfrak{a}$ and $\mathfrak{b}^n$ are comaximal by induction on n. Thus $\mathfrak{b}^n$ and $\mathfrak{a}^m$ are comaximal.

Alternatively, there are $x\in\mathfrak{a}$ and $y\in\mathfrak{b}$ with $1=x+y$. Thus the binomial theorem yields $1=(x+y)^{m+n-1}=x'+y'$ with $x'\in\mathfrak{a}^m$ and $y'\in\mathfrak{b}^n$, as desired.

Conversely, if $\mathfrak{a}^m$ and $\mathfrak{b}^n$ are comaximal, then $\mathfrak{a}$ and $\mathfrak{b}$ are, as $\mathfrak{a}^m\subset\mathfrak{a}$ and $\mathfrak{b}^n\subset\mathfrak{b}$.

For (4)(a), assume $\mathfrak{a}_1$ and $\mathfrak{a}_2\cdots\mathfrak{a}_{n-1}$ are comaximal by induction on n. By hypothesis, $\mathfrak{a}_1$ and $\mathfrak{a}_n$ are comaximal. Thus (2) yields (a).

For (4)(b) and (4)(c), again proceed by induction on n. Thus (1) yields

$$\mathfrak{a}_1\cap(\mathfrak{a}_2\cap\cdots\cap\mathfrak{a}_n)=\mathfrak{a}_1\cap(\mathfrak{a}_2\cdots\mathfrak{a}_n)=\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_n;$$
$$R/(\mathfrak{a}_1\cdots\mathfrak{a}_n)\xrightarrow{\sim}R/\mathfrak{a}_1\times R/(\mathfrak{a}_2\cdots\mathfrak{a}_n)\xrightarrow{\sim}\prod(R/\mathfrak{a}_i). \qquad \square$$

For (5), let k be a field, and X, Y variables. Take $R:=k[X,Y]$ and $\mathfrak{a}:=\langle X\rangle$ and $\mathfrak{b}:=\langle Y\rangle$. Given $f\in\langle X\rangle\cap\langle Y\rangle$, note that every monomial of f contains both X and Y, and so $f\in\langle X\rangle\langle Y\rangle$. Thus (1)(a) holds. But $\langle X\rangle$ and $\langle Y\rangle$ are not comaximal, as both are contained in $\langle X, Y\rangle$.

Exercise (1.22) . — First, given a prime number p and a $k\ge 1$, find the idempotents in $\mathbb{Z}/\langle p^k\rangle$. Second, find the idempotents in $\mathbb{Z}/\langle 12\rangle$. Third, find the number of idempotents in $\mathbb{Z}/\langle n\rangle$ where $n=\prod_{i=1}^N p_i^{n_i}$ with p_i distinct prime numbers.

Solution: First, let $m\in\mathbb{Z}$ be idempotent modulo p^k. Then $m(m-1)$ is divisible by p^k. So either m or $m-1$ is divisible by p^k, as m and $m-1$ have no common prime divisor. Hence 0 and 1 are the only idempotents in $\mathbb{Z}/\langle p^k\rangle$.

Second, since $-3+4=1$, the Chinese Remainder Theorem **(1.21)**(1)(b) yields

$$\mathbb{Z}/\langle 12\rangle=\mathbb{Z}/\langle 3\rangle\times\mathbb{Z}/\langle 4\rangle.$$

Hence m is idempotent modulo 12 if and only if m is idempotent modulo 3 and modulo 4. By the previous case, we have the following possibilities:

$$\begin{aligned}
m&\equiv 0 \pmod 3 &&\text{and}&& m\equiv 0 \pmod 4;\\
m&\equiv 1 \pmod 3 &&\text{and}&& m\equiv 1 \pmod 4;\\
m&\equiv 1 \pmod 3 &&\text{and}&& m\equiv 0 \pmod 4;\\
m&\equiv 0 \pmod 3 &&\text{and}&& m\equiv 1 \pmod 4.
\end{aligned}$$

Therefore, $m\equiv 0,\,1,\,4,\,9 \pmod{12}$.

Third, for each i, the two numbers $p_1^{n_1}\cdots p_{i-1}^{n_{i-1}}$ and $p_i^{n_i}$ have no common prime divisor. Hence some linear combination is equal to 1 by the Euclidean Algorithm. So the principal ideals they generate are comaximal. Hence by induction on N, the

Chinese Remainder Theorem yields

$$\mathbb{Z}/\langle n\rangle = \prod_{i=1}^{N} \mathbb{Z}/\langle p_i^{n_i}\rangle.$$

So m is idempotent modulo n if and only if m is idempotent modulo p^{n_i} for all i; hence, if and only if m is 0 or 1 modulo p^{n_i} for all i by the first case. Thus there are 2^N idempotents in $\mathbb{Z}/\langle n\rangle$. □

Exercise (1.23) . — Let $R := R' \times R''$ be a product of rings, $\mathfrak{a} \subset R$ an ideal. Show $\mathfrak{a} = \mathfrak{a}' \times \mathfrak{a}''$ with $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ ideals. Show $R/\mathfrak{a} = (R'/\mathfrak{a}') \times (R''/\mathfrak{a}'')$.

Solution: Set $\mathfrak{a}' := \{x' \mid (x', 0) \in \mathfrak{a}\}$ and $\mathfrak{a}'' := \{x'' \mid (0, x'') \in \mathfrak{a}\}$. Clearly, $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ are ideals. Clearly,

$$\mathfrak{a} \supset \mathfrak{a}' \times 0 + 0 \times \mathfrak{a}'' = \mathfrak{a}' \times \mathfrak{a}''.$$

The opposite inclusion holds, because if $\mathfrak{a} \ni (x', x'')$, then

$$\mathfrak{a} \ni (x', x'') \cdot (1, 0) = (x', 0) \quad \text{and} \quad \mathfrak{a} \ni (x', x'') \cdot (0, 1) = (0, x'').$$

Finally, the equation $R/\mathfrak{a} = (R/\mathfrak{a}') \times (R/\mathfrak{a}'')$ is now clear from the construction of the residue class ring. □

Exercise (1.24) . — Let R be a ring; e, e' idempotents (see **(10.23)** also). Show:

(1) Set $\mathfrak{a} := \langle e\rangle$. Then $\mathfrak{a}$ is **idempotent**; that is, $\mathfrak{a}^2 = \mathfrak{a}$.
(2) Let $\mathfrak{a}$ be a principal idempotent ideal. Then $\mathfrak{a} = \langle f\rangle$ with f idempotent.
(3) Set $e'' := e + e' - ee'$. Then $\langle e, e'\rangle = \langle e''\rangle$, and e'' is idempotent.
(4) Let $e_1, \ldots, e_r$ be idempotents. Then $\langle e_1, \ldots, e_r\rangle = \langle f\rangle$ with f idempotent.
(5) Assume R is Boolean. Then every finitely generated ideal is principal.

Solution: For (1), note $\mathfrak{a}^2 = \langle e^2\rangle$ since $\mathfrak{a} = \langle e\rangle$. But $e^2 = e$. Thus (1) holds.

For (2), say $\mathfrak{a} = \langle g\rangle$. Then $\mathfrak{a}^2 = \langle g^2\rangle$. But $\mathfrak{a}^2 = \mathfrak{a}$. So $g = xg^2$ for some x. Set $f := xg$. Then $f = x(xg^2) = f^2$. Thus f is idempotent. Furthermore, $f \in \mathfrak{a}$; so $\langle f\rangle \subset \mathfrak{a}$. And $g = fg$. So $\mathfrak{a} \subset \langle f\rangle$. So $\mathfrak{a} = \langle f\rangle$. Thus (2) holds.

For (3), note $\langle e''\rangle \subset \langle e, e'\rangle$. Conversely, $ee'' = e^2 + ee' - e^2e' = e + ee' - ee' = e$. By symmetry, $e'e'' = e'$. So $\langle e, e'\rangle \subset \langle e''\rangle$ and $e''^2 = ee'' + e'e'' - ee'e'' = e''$. So $\langle e, e'\rangle = \langle e''\rangle$ and e'' is idempotent, as desired. Thus (3) holds.

For (4), if $r = 2$, appeal to (3). If $r \geq 3$, induct on r. Thus (4) holds.

For (5), recall that every element of R is idempotent. Thus (4) implies (5). □

Exercise (1.25) . — Let L be a **lattice**, that is, a partially ordered set in which every pair x, $y \in L$ has a sup $x \vee y$ and an inf $x \wedge y$. Assume L is **Boolean**; that is:

(1) L has a least element 0 and a greatest element 1.
(2) The operations $\wedge$ and $\vee$ **distribute** over each other; that is,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \text{and} \quad x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

(3) Each $x \in L$ has a unique **complement** x'; that is, $x \wedge x' = 0$ and $x \vee x' = 1$.

Show that the following six laws are obeyed:

$$x \wedge x = x \quad \text{and} \quad x \vee x = x. \qquad \textbf{(idempotent)}$$

$$x \wedge 0 = 0,\ \ x \wedge 1 = x \quad \text{and} \quad x \vee 1 = 1,\ \ x \vee 0 = x. \qquad \textbf{(unitary)}$$

$$x \wedge y = y \wedge x \quad \text{and} \quad x \vee y = y \vee x. \qquad \textbf{(commutative)}$$

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z \quad \text{and} \quad x \vee (y \vee z) = (x \vee y) \vee z. \qquad \textbf{(associative)}$$

$$x'' = x \quad \text{and} \quad 0' = 1,\ \ 1' = 0. \qquad \textbf{(involutory)}$$

$$(x \wedge y)' = x' \vee y' \quad \text{and} \quad (x \vee y)' = x' \wedge y'. \qquad \textbf{(De Morgan's)}$$

Moreover, show that $x \le y$ if and only if $x = x \wedge y$.

Solution: By definition, $x \wedge y$ is the greatest element smaller than both x and y, and $x \vee y$ is the least element larger than both x and y. It follows easily that the first four laws are obeyed and that $x \le y$ if and only if $x = x \wedge y$.

For the involutory law, note by commutativity $x' \wedge x = 0$ and $x' \vee x = 1$; thus by uniqueness $x'' = x$. Moreover, by the unitary law, $0 \wedge 1 = 0$ and $0 \vee 1 = 1$; thus by uniqueness $0' = 1$. Thus $1' = 0'' = 0$.

For De Morgan's laws, note $(x \wedge y) \wedge (x' \vee y') = ((x \wedge y) \wedge x') \vee ((x \wedge y) \wedge y')$ by distributivity. Now, $(x \wedge y) \wedge x' = (y \wedge x) \wedge x' = y \wedge (x \wedge x') = y \wedge 0 = 0$ by the commutative, associative, complementary, and unitary laws. Similarly, $(x\wedge y)\wedge y'$ is 0. But $0 \vee 0 = 0$. Thus $(x\wedge y)\wedge(x'\vee y') = 0$. Similarly, $(x\wedge y)\vee(x'\vee y') = 1$. Thus, by uniqueness, De Morgan's first law holds. The second can be proved similarly; alternatively, it follows directly and formally from the first by symmetry. □

Exercise (1.26) . — Let L be a Boolean lattice; see **(1.25)**. For all $x, y \in L$, set

$$x + y := (x \wedge y') \vee (x' \wedge y) \quad \text{and} \quad xy := x \wedge y.$$

Show: (1) $x + y = (x \vee y)(x' \vee y')$ and (2) $(x + y)' = (x'y') \vee (xy)$. Furthermore, show L is a Boolean ring.

Solution: For (1), note $x + y = ((x \wedge y') \vee x') \wedge ((x \wedge y') \vee y)$ by distributivity. Now, $(x \wedge y') \vee x' = (x \vee x') \wedge (y' \vee x')$ by distributivity. But $x \vee x' = 1$ and $1 \wedge (y' \vee x') = y' \vee x'$. Similarly, $(x \wedge y') \vee y = x \vee y$. Thus commutativity gives (1).

For (2), note $(x+y)' = ((x\vee y)(x'\vee y'))'$ by (1). So $(x+y)' = (x\vee y)' \vee (x'\vee y')'$ by De Morgan's first law. So $(x+y)' = (x'y') \vee (x''y'')$ by De Morgan's second law applied twice. Thus the involutory law yields (2).

Furthermore, $x(yz) = (xy)z$ and $x{\cdot}1 = x$ and $x^2 = x$ and $xy = yx$ and $x\vee y = y\vee x$ by **(1.25)**. And so $x + y := (xy') \vee (x'y) = (y'x) \vee (yx') = (yx') \vee (y'x) =: y + x$.

Let's check $+$ is associative. Set $w := x + y$. Then $w + z := (wz') \vee (w'z)$. But $wz' = ((xy')z') \vee ((x'y)z')$ by distributivity. Now, $(xy')z'$ and $(x'y)z'$ may be written as $xy'z'$ and $x'yz'$ by associativity. Thus $wz' = (xy'z') \vee (x'yz')$.

Similarly, $w'z = (x'y'z) \vee (xyz)$ by (2), distributivity, and associativity. Thus $(x+y)+z = (xy'z') \vee (x'yz') \vee (x'y'z) \vee (xyz)$ by associativity of $\vee$. But the right-hand side is invariant under permutation of x, y, z by commutativity of $\cdot$ and $\vee$. So, $(x+y)+z = (y+z)+x$. Thus commutativity of $+$ yields $(x+y)+z = x+(y+z)$.

Finally, let's check distributivity of $\cdot$ over $+$. Recall $y+z := (yz') \vee (y'z)$. Hence, distributivity of $\cdot$ over $\vee$ yields $x(y+z) = (x(yz')) \vee (x(y'z))$.

However, $xy + xz := ((xy)(xz)') \vee ((xy)'(xz))$. Now, $(xy)(xz)' = (xy)x' \vee (xy)z'$ by De Morgan's first law and distributivity of $\cdot$ over $\vee$. And $(xy)x' = (xx')y$ by associativity and commutativity But $xx' = 0$ and $0 \cdot y = 0$ and $0 \vee u = u$ for any u.

Thus $(xy)(xz)' = (xy)z'$. Similarly, $(xy)'(xz) = y'(xz)$. Thus, by associativity and commutativity, $x(y+z) = xy + xz$, as desired. In sum, L is a Boolean ring. □

Exercise (1.27) . — Given a Boolean ring R, order R by $x \le y$ if $x = xy$. Show R is thus a Boolean lattice. Viewing this construction as a map ρ from the set of Boolean-ring structures on the set R to the set of Boolean-lattice structures on R, show ρ is bijective with inverse the map λ associated to the construction in **(1.26)**.

Solution: Let's check R is partially ordered. First, $x \le x$ as $x = x^2$ since R is Boolean. Second, if $x \le y$ and $y \le z$, then $x = xy$ and $y = yz$, and so $x = xy = x(yz) = (xy)z = xz$; thus, $x \le z$. Third, if $x \le y$ and $y \le x$, then $x = xy$ and $y = yx$; however, $xy = yx$, and thus $x = y$. Thus R is partially ordered.

Given $x, y \in R$, set $x \vee y := x + y + xy$ and $x \wedge y := xy$. Then $x \le x \vee y$ as $x(x + y + xy) = x^2 + xy + x^2y = x + 2xy = x$ since $x^2 = x$ and $2xy = 0$. By symmetry, $y \le x \vee y$. Also, if $z \le x$ and $z \le y$, then $z = zx$ and $z = zy$, and so $z(x \vee y) = zx + zy + zxy = z + z + z = z$ as $2z = 0$; thus $z \le x \vee y$. Thus $x \vee y = \sup\{x, y\}$. Similarly, $x \wedge y = \inf\{x, y\}$. Moreover, $0 \le x$ and $x \le 1$ as $0 = 0 \cdot x$ and $x = x \cdot 1$. Thus R is a lattice with a least element and a greatest.

Let's check the distributive laws. First, $(x + y + xy)z = xz + yz + (xz)(yz)$ as $z = z^2$; thus, $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$. Second, $(x+z+xz)(y+z+yz) = xy+z+xyz$ as $z = z^2$ and $2w = 0$ for all w; thus, $(x \vee z) \wedge (y \vee z) = (x \wedge y) \vee z$, as desired.

Finally, given $x \in R$, if there's $y \in R$ with $x \wedge y = 0$ and $x \vee y = 1$, then $1 = x + y + xy = x + y$, and so $y = 1 - x$; thus, y is unique if it exists. Now, set $x' := 1 - x$. Then $x \wedge x' := xx' = x - x^2 = 0$ and $x \vee x' := x + x' + xx' = 1$. Thus x' is a complement of x. In sum, R is a Boolean lattice.

To show $\lambda\rho = 1$, given $x, y \in R$, let $x +_1 y$ and $x \cdot_1 y$ be the sum and product in the ring structure on R constructed in **(1.26)** with the above lattice as L. Then $x \cdot_1 y := x \wedge y$. But $x \wedge y := xy$. Thus $x \cdot_1 y = xy$. Now, $2xy = 0$ and $x(1-x) = 0$ imply $x(1-y) + (1-x)y + x(1-y)(1-x)y = x + y$. So $x + y = (x \wedge y') \vee (x' \wedge y)$. But $x +_1 y := (x \wedge y') \vee (x' \wedge y)$. Thus $x +_1 y = x + y$. Thus $\lambda\rho = 1$.

To show $\rho\lambda = 1$, assume the ring structure on R is constructed as in **(1.26)** from a given Boolean lattice structure on R, whose order and inf are denoted by $\le_0$ and $\wedge_0$. Given $x, y \in R$, we just have to show that $x \le y$ if and only if $x \le_0 y$.

By definition, $x \le y$ if and only if $x = xy$. But $xy := x \wedge_0 y$. Also, $x = x \wedge_0 y$ if and only if $x \le_0 y$ by **(1.25)**. Thus $x \le y$ if and only if $x \le_0 y$. Thus $\rho\lambda = 1$. In sum, ρ is bijective with inverse λ. □

Exercise (1.28) . — Let X be a set, and L the set of all subsets of X, partially ordered by inclusion. Show that L is a Boolean lattice and that the ring structure on L constructed in **(1.2)** coincides with that constructed in **(1.26)**.

Assume X is a topological space, and let M be the set of all its open and closed subsets. Show that M is a sublattice of L, and that the subring structure on M of **(1.2)** coincides with the ring structure of **(1.26)** with M for L.

Solution: Given $S, T \in L$, plainly $S \cap T$ is the largest set contained in both S and T, and $S \cup T$ is the smallest set containing both S and T. Also, every subset of X contains $\emptyset$, and is contained in X. And, given $U \in L$, the distributive laws

$$S \cap (T \cup U) = (S \cap T) \cup (S \cap U), \quad \text{and} \quad S \cup (T \cap U) = (S \cup T) \cap (S \cup U)$$

are easy to check by double inclusion.

Finally, $(X - S)$ is a complement of S, as $(X - S) \cap S = \emptyset$ and $(X - S) \cup S = X$.

Moreover, $X - S$ is the only complement, because, if $S \cap T = \emptyset$, then $T \subset (X - S)$, and if $T \cup S = X$, then $T \supset (X - S)$. Thus L is a Boolean lattice.

The product of S and T is equal to $S \cap T$ in both (**1.2**) and (**1.26**). Their sum is equal to $(S - T) \cup (T - S)$ in (**1.2**) and to $(S \cap (X - T)) \cup ((X - S) \cap T)$ in (**1.26**). But $S - T = S \cap (X - T)$. So the two sums are also the same. Thus the two ring structures on L coincide.

Assume $S, T \in M$. Then also $S \cap T$, $S \cup T$, $\emptyset$, $X \in M$. It follows that M is a Boolean sublattice of L. Lastly, the construction in (**1.26**) plainly turns a Boolean sublattice into a subring. But we just showed that, the two ring strucures on L coincide. Thus the two induced ring structures on M also coincide, □

Exercise (1.29) . — Let R be a ring, $P := R[X_1, \dots, X_m]$ the polynomial ring in variables X_i, and $V \subset R^m$ the set of common zeros of a set of polynomials $F_\lambda \in P$.

(1) Let $I(V)$ be the ideal of all $F \in P$ vanishing on V, and $P(V)$ the R-algebra of all functions $\gamma\colon V \to R$ given by evaluating some $G \in P$. Show $I(V)$ is the largest set of polynomials with V as set of common zeros. Show $P/I(V) = P(V)$. And show $1 \in I(V)$ (or $P(V) = 0$) if and only if $V = \emptyset$.

(2) Let $W \subset R^n$ be like V, and $\rho\colon V \to W$ any map. Call ρ **regular** if there are $G_i \in P$ with $\rho(v) = (G_1(v), \dots, G_n(v))$ for all $v \in V$. If ρ is regular, define $\rho^*\colon P(W) \to P(V)$ by $\rho^*(\delta) := \delta \circ \rho$, and show ρ^* is a well-defined algebra map.

(3) Let $Q := R[Y_1, \dots, Y_n]$ be the polynomial ring, and $\zeta_i \in P(W)$ the function given by evaluating the variable Y_i. Let $\varphi\colon P(W) \to P(V)$ be an algebra map. Define $\varphi^*\colon V \to W$ by $\varphi^*(v) := (w_1, \dots, w_n)$ where $w_i := (\varphi\zeta_i)(v)$, and show φ^* is a well-defined regular map.

(4) Show $\rho \mapsto \rho^*$ and $\varphi \mapsto \varphi^*$ define inverse bijective correspondences between the regular maps $\rho\colon V \to W$ and the algebra maps $\varphi\colon P(W) \to P(V)$.

Solution: For (1), recall V is the set of zeros of the F_λ. So $F_\lambda \in I(V)$ for all λ. So V contains the zero set V' of all the $F \in I(V)$. Conversely, $V \subset V'$ as every $F \in I(V)$ vanishes on V. Thus $V = V'$. Trivially, $I(V)$ contains every set I of polynomials with V as set of common zeros. Thus $I(V)$ is the largest I.

Next, form the evaluation map ev_V from P to the R-algebra R^V of all $\gamma\colon V \to R$. Note $P(V) := \mathrm{Im}(\mathrm{ev}_V)$ and $I(V) := \mathrm{Ker}(\mathrm{ev}_V)$. So (**1.5.1**) gives $P/I(V) = P(V)$.

Finally, if $V = \emptyset$, then 1 vanishes on every point in V, and so $1 \in I(V)$. Conversely, if $V \neq \emptyset$, then 1 doesn't vanish on V, and so $1 \notin I(V)$. Thus (1) holds.

For (2), define $R^W \to R^V$ by $\delta \mapsto \delta \circ \rho$; plainly, it's an algebra map. Suppose ρ is regular and $\delta \in P(W)$. Say $\rho(v) := (G_1(v), \dots, G_n(v))$ with $G_i \in P$. Say δ is given by evaluating a polynomial $D(Y_1, \dots, Y_n)$. Set $G := D(G_1, \cdots, G_n)$. Then $G \in P$, and $\rho^*(\delta)$ is given by evaluating G; so $\rho^*(\delta) \in P(V)$. Thus (2) holds.

For (3), let $H \in Q$. In general, an algebra map, plainly, carries a polynomial combination of elements to the same combination of their images. Thus

$$\varphi(H(\zeta_1, \dots, \zeta_n)) = H(\varphi\zeta_1, \dots, \varphi\zeta_n). \tag{1.29.1}$$

Let $v \in V$. Evaluation at v gives an algebra map $P(V) \to R$. Hence

$$\big(H(\varphi\zeta_1, \dots, \varphi\zeta_n)\big)(v) = H(\varphi\zeta_1(v), \dots, \varphi\zeta_n(v)) =: H(\varphi^*(v)). \tag{1.29.2}$$

Together, (**1.29.1**) and (**1.29.2**) yield

$$\big(\varphi(H(\zeta_1, \dots, \zeta_n))\big)(v) = H(\varphi^*(v)). \tag{1.29.3}$$

Let $w \in W$. Evaluation at w gives an algebra map $P(W) \to R$. Hence

$$\big(H(\zeta_1, \ldots, \zeta_n)\big)(w) = H(\zeta_1(w), \ldots, \zeta_n(w)) = H(w). \qquad \textbf{(1.29.4)}$$

Suppose $H \in I(W)$; so $H(w) = 0$ for all $w \in W$. Hence $H(\zeta_1, \ldots, \zeta_n) = 0$ in $P(W)$ by **(1.29.4)**. But $\varphi(0) = 0$. So $\varphi(H(\zeta_1, \ldots, \zeta_n)) = 0$ in $P(V)$. So **(1.29.3)** implies $H(\varphi^*(v)) = 0$ for all $v \in V$. But $H \in I(W)$ is arbitrary. Hence (1) implies $\varphi^*(v) \in W$ for all $v \in V$. Thus $\varphi^*(V) \subset W$. Thus φ^* is well-defined.

For all i, since $\varphi\zeta_i \in P(V)$, there's $G_i \in P$ with $(\varphi\zeta_i)(v) = G_i(v)$ for all $v \in V$. Thus φ^* is regular. Thus (3) holds.

For (4), first, given an algebra map $\varphi\colon P(W) \to P(V)$, let's check $\varphi^{**} = \varphi$.

Given $\delta \in P(W)$, we must check $\varphi^{**}(\delta) = \varphi(\delta)$. Say δ is given by evaluating $D \in Q$; so $\delta(w) = D(w)$ for all $w \in W$. Hence $\delta = D(\zeta_1, \ldots, \zeta_n)$ in $P(W)$ by **(1.29.4)**. Therefore, **(1.29.3)** implies $(\varphi(\delta))(v) = \delta(\varphi^*(v))$ for all $v \in V$.

On the other hand, $\varphi^{**}(\delta) := \delta \circ \varphi^*$. So $\big(\varphi^{**}(\delta)\big)(v) = \delta(\varphi^*(v))$ for all $v \in V$. Hence $(\varphi^{**}(\delta))(v) = (\varphi(\delta))(v)$ for all $v \in V$. Thus $\varphi^{**}(\delta) = \varphi(\delta)$, as desired.

Lastly, given a regular map $\rho\colon V \to W$, let's check $\rho^{**} = \rho$. Let $v \in V$. Then $\rho^{**}(v) := \big((\rho^*\zeta_1)(v), \ldots, (\rho^*\zeta_n)(v)\big)$. However, $\rho^*\zeta_i(v) := \zeta_i(\rho(v))$. Therefore, $\rho^{**}(v) = \rho(v)$. But $v \in V$ is arbitrary. Thus $\rho^{**} = \rho$. Thus (4) holds. □

2. Prime Ideals

Exercise (2.9) . — Let R be a ring, $P := R[\mathcal{X}, \mathcal{Y}]$ the polynomial ring in two sets of variables $\mathcal{X}$ and $\mathcal{Y}$. Set $\mathfrak{p} := \langle \mathcal{X} \rangle$. Show $\mathfrak{p}$ is prime if and only if R is a domain.

Solution: Note that $\mathfrak{p}$ is prime if and only if $P/\mathfrak{p}$ is a domain by **(2.8)**. But $P/\mathfrak{p} = R[\mathcal{Y}]$ by **(1.17)**(5). Finally, $R[\mathcal{Y}]$ is a domain if R is by **(2.4)**, and the converse is trivial, as desired. □

Exercise (2.18) . — Show that, in a PID, nonzero elements x and y are **relatively prime** (share no prime factor) if and only if they're coprime.

Solution: Say $\langle x \rangle + \langle y \rangle = \langle d \rangle$. Then $d = \gcd(x, y)$, as is easy to check. The assertion is now obvious. □

Exercise (2.23) . — Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals, and $\mathfrak{p}$ a prime ideal. Prove that these conditions are equivalent: (1) $\mathfrak{a} \subset \mathfrak{p}$ or $\mathfrak{b} \subset \mathfrak{p}$; and (2) $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{p}$; and (3) $\mathfrak{a}\mathfrak{b} \subset \mathfrak{p}$.

Solution: Trivially, (1) implies (2). If (2) holds, then (3) follows as $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Finally, assume $\mathfrak{a} \not\subset \mathfrak{p}$ and $\mathfrak{b} \not\subset \mathfrak{p}$. Then there are $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$ with $x, y \notin \mathfrak{p}$. Hence, since $\mathfrak{p}$ is prime, $xy \notin \mathfrak{p}$. However, $xy \in \mathfrak{a}\mathfrak{b}$. Thus (3) implies (1). □

Exercise (2.24) . — Let R be a ring, $\mathfrak{p}$ a prime ideal, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ maximal ideals. Assume $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Show $\mathfrak{p} = \mathfrak{m}_i$ for some i.

Solution: Note $\mathfrak{p} \supset 0 = \mathfrak{m}_1 \cdots \mathfrak{m}_n$. So $\mathfrak{p} \supset \mathfrak{m}_1$ or $\mathfrak{p} \supset \mathfrak{m}_2 \cdots \mathfrak{m}_n$ by **(2.23)**. So $\mathfrak{p} \supset \mathfrak{m}_i$ for some i by induction on n. But $\mathfrak{m}_i$ is maximal. Thus $\mathfrak{p} = \mathfrak{m}_i$. □

Exercise (2.25) . — Let R be a ring, and $\mathfrak{p}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals with $\mathfrak{p}$ prime.

(1) Assume $\mathfrak{p} \supset \bigcap_{i=1}^n \mathfrak{a}_i$. Show $\mathfrak{p} \supset \mathfrak{a}_j$ for some j,

(2) Assume $\mathfrak{p} = \bigcap_{i=1}^n \mathfrak{a}_i$. Show $\mathfrak{p} = \mathfrak{a}_j$ for some j,

Solution: For (1), note $\mathfrak{p} \supset \mathfrak{a}_1$ or $\mathfrak{p} \supset \bigcap_{i=2}^n \mathfrak{a}_i$ by (**2.23**). So $\mathfrak{p} \supset \mathfrak{a}_j$ for some j by induction on n. Thus (1) holds.

For (2), note $\mathfrak{p} \supset \mathfrak{a}_j$ for some j by (1). But $\mathfrak{p} \subset \mathfrak{a}_j$ now. Thus (2) holds. □

Exercise (2.26) . — Let R be a ring, $\mathcal{S}$ the set of all ideals that consist entirely of zerodivisors. Show that $\mathcal{S}$ has maximal elements and they're prime. Conclude that $\mathrm{z.div}(R)$ is a union of primes.

Solution: Given a totally ordered subset $\{\mathfrak{a}_\lambda\}$ of $\mathcal{S}$, set $\mathfrak{a} := \bigcup \mathfrak{a}_\lambda$. Plainly $\mathfrak{a}$ is an upper bound of $\{\mathfrak{a}_\lambda\}$ in $\mathcal{S}$. Thus by Zorn's Lemma, $\mathcal{S}$ has maximal elements $\mathfrak{p}$.

Given $x, x' \in R$ with $xx' \in \mathfrak{p}$, but $x, x' \notin \mathfrak{p}$, note $\langle x\rangle + \mathfrak{p}$, $\langle x'\rangle + \mathfrak{p} \notin \mathcal{S}$. So there are $a, a' \in R$ and $p, p' \in \mathfrak{p}$ such that $y := ax + p$ and $y' := a'x' + p'$ are nonzerodivisors. Then $yy' \in \mathfrak{p}$. So $yy' \in \mathrm{z.div}(R)$, a contradiction. Thus $\mathfrak{p}$ is prime.

Finally, given $x \in \mathrm{z.div}(R)$, note $\langle x\rangle \in \mathcal{S}$. So $\langle x\rangle$ lies in a maximal element $\mathfrak{p}$ of $\mathcal{S}$. Thus $x \in \mathfrak{p}$ and $\mathfrak{p}$ is prime, as desired. (For an alternative proof, see (**3.24**).) □

Exercise (2.27) . — Given a prime number p and an integer $n \geq 2$, prove that the residue ring $\mathbb{Z}/\langle p^n\rangle$ does not contain a domain as a subring.

Solution: Any subring of $\mathbb{Z}/\langle p^n\rangle$ must contain 1, and 1 generates $\mathbb{Z}/\langle p^n\rangle$ as an abelian group. So $\mathbb{Z}/\langle p^n\rangle$ contains no proper subrings. However, $\mathbb{Z}/\langle p^n\rangle$ is not a domain, because in it, $p \cdot p^{n-1} = 0$ but neither p nor p^{n-1} is 0. □

Exercise (2.28) . — Let $R := R' \times R''$ be a **product** of two rings. Show that R is a domain if and only if either R' or R'' is a domain and the other is 0.

Solution: Assume R is a domain. As $(1,0)\cdot(0,1) = (0,0)$, either $(1,0) = (0,0)$ or $(0,1) = (0,0)$. Correspondingly, either $R' = 0$ and $R = R''$, or $R'' = 0$ and $R = R''$. The assertion is now obvious. □

Exercise (2.29) . — Let $R := R' \times R''$ be a product of rings, $\mathfrak{p} \subset R$ an ideal. Prove $\mathfrak{p}$ is prime if and only if either $\mathfrak{p} = \mathfrak{p}' \times R''$ with $\mathfrak{p}' \subset R'$ prime or $\mathfrak{p} = R' \times \mathfrak{p}''$ with $\mathfrak{p}'' \subset R''$ prime. What if *prime* is replaced by *maximal*?

Solution: Note $\mathfrak{p} = \mathfrak{p}' \times \mathfrak{p}''$ and $R/\mathfrak{p} = R'/\mathfrak{p}' \times R''/\mathfrak{p}''$ by (**1.23**). And $R/\mathfrak{p}$ is a domain if and only if either $R'/\mathfrak{p}'$ or $R''/\mathfrak{p}''$ is a domain and the other is 0 by (**2.28**). Thus (**2.8**) yields the original statement.

Replace *prime* by *maximal*. Note every maximal ideal is prime by (**2.15**). So the preceding paragraph yields $\mathfrak{p} = \mathfrak{p}' \times \mathfrak{p}''$ and either $R/\mathfrak{p} = R'/\mathfrak{p}'$ and $\mathfrak{p}'' = R''$ or $R/\mathfrak{p} = R''/\mathfrak{p}''$ and $\mathfrak{p}' = R'$. Thus (**2.13**) yields the new statement. □

Exercise (2.30) . — Let R be a domain, and $x, y \in R$. Assume $\langle x\rangle = \langle y\rangle$. Show $x = uy$ for some unit u.

Solution: By hypothesis, $x = uy$ and $y = vx$ for some $u, v \in R$. So $x = 0$ if and only if $y = 0$; if so, take $u := 1$. Assume $x \neq 0$. Now, $x = uvx$, or $x(1 - uv) = 0$. But R is a domain. So $1 - uv = 0$. Thus u is a unit. □

Exercise (2.31) . — Let k be a field, R a nonzero ring, $\varphi\colon k \to R$ a ring map. Prove φ is injective.

Solution: By (**1.1**), $1 \neq 0$ in R. So $\mathrm{Ker}(\varphi) \neq k$. So $\mathrm{Ker}(\varphi) = 0$ by (**2.12**). Thus φ is injective. □

Exercise (2.32) . — Let R be a ring, $\mathfrak{p}$ a prime, $\mathcal{X}$ a set of variables. Let $\mathfrak{p}[\mathcal{X}]$ denote the set of polynomials with coefficients in $\mathfrak{p}$. Prove these statements:

(1) $\mathfrak{p}R[\mathcal{X}]$ and $\mathfrak{p}[\mathcal{X}]$ and $\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle$ are primes of $R[\mathcal{X}]$, which contract to $\mathfrak{p}$.
(2) Assume $\mathfrak{p}$ is maximal. Then $\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle$ is maximal.

Solution: For (1), note that $R[\mathcal{X}]/\mathfrak{p}R[\mathcal{X}] = (R/\mathfrak{p})[\mathcal{X}]$ by **(1.16)**. But $R/\mathfrak{p}$ is a domain by **(2.8)**. So $R[\mathcal{X}]/\mathfrak{p}R[\mathcal{X}]$ is a domain by **(2.4)**. Thus, by **(2.8)** again, $\mathfrak{p}R[\mathcal{X}]$ is prime.

Moreover, $\mathfrak{p}R[\mathcal{X}] = \mathfrak{p}[\mathcal{X}]$ by **(1.15)** (1). Thus $\mathfrak{p}[\mathcal{X}]$ is prime. Plainly, $\mathfrak{p}[\mathcal{X}]$ contracts to $\mathfrak{p}$; so $\mathfrak{p}R[\mathcal{X}]$ does too.

Note $\big(\mathfrak{p}R[\mathcal{X}]+\langle\mathcal{X}\rangle\big)/\mathfrak{p}R[\mathcal{X}]$ is equal to $\langle\mathcal{X}\rangle \subset (R/\mathfrak{p})[\mathcal{X}]$. But $(R/\mathfrak{p})[\mathcal{X}]/\langle\mathcal{X}\rangle$ is equal to $R/\mathfrak{p}$ by **(1.17)**(3). So $R[\mathcal{X}]/\big(\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle\big)$ is equal to $R/\mathfrak{p}$ by **(1.9)**. But as noted above, $R/\mathfrak{p}$ is a domain by **(2.8)**. Thus $\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle$ is prime again by **(2.8)**.

Since the canonical map $R/\mathfrak{p} \to R[\mathcal{X}]/\big(\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle\big)$ is bijective, it's injective. Thus $\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle$ contracts to $\mathfrak{p}$. Thus (1) holds.

In (2), $R/\mathfrak{p}$ is a field by **(2.13)**. But, as just noted, $R/\mathfrak{p} \xrightarrow{\sim} R[\mathcal{X}]/(\mathfrak{p}R[\mathcal{X}]+\langle\mathcal{X}\rangle)$. Thus $\mathfrak{p}R[\mathcal{X}] + \langle\mathcal{X}\rangle$ is maximal again by **(2.13)**. □

Exercise (2.33) . — Let R be a ring, X a variable, $H \in P := R[X]$, and $a \in R$. Given $n \ge 1$, show $(X-a)^n$ and H are coprime if and only if $H(a)$ is a unit.

Solution: By **(2.16)**, $(X-a)^n$ and H are coprime if and only if $X-a$ and H are, if and only if, modulo $X-a$, the residue of H is a unit. But by **(1.17)**(4), that residue is equal to $H(a)$. Thus the desired equivalence holds, □

Exercise (2.34) . — Let R be a ring, X a variable, $F \in P := R[X]$, and $a \in R$. Set $F' := \partial F/\partial X$; see **(1.18.1)**. Show the following statements are equivalent:

(1) a is a supersimple root of F.
(2) a is a root of F, and $X-a$ and F' are coprime.
(3) $F = (X-a)G$ for some G in P coprime to $X-a$.

Show that, if (3) holds, then G is unique.

Solution: Owing to **(2.33)** with $n = 1$, the definition and the assertion in **(1.19)** yield (1)⇔(2) and (1)⇔(3) and the uniqueness of G. □

Exercise (2.35) . — Let R be a ring, X a variable, $F(X)$ a polynomial of degree d. Show: (1) Assume R is a domain. Then F has at most d (distict) zeros in R.
(2) Take $R := \mathbb{Z}/\langle 6\rangle$ and $F := X^2 + X$. Then F has more than d zeros in R.

Solution: In (1), if $d = 0$, then $F \ne 0$ and $F \in R$, and so F has no zeros in R. Assume $d \ge 1$. Given (distinct) roots $a, b \in R$ of F, note $F = (X-a)G$, by **(1.19)**, and $\deg(G) = d-1$ by **(2.4.1)**. Moreover, $F(b) = (b-a)G(b)$. As R is a domain, $G(b) = 0$. But, G has at most $d-1$ roots by induction on d. Thus (1) holds.

To show (2), note 0, 2, 3, 5 are (all the) zeros of F in R. □

Exercise (2.36) . — Let R be a ring, $\mathfrak{p}$ a prime; $\mathcal{X}$ a set of variables; $F, G \in R[\mathcal{X}]$. Let $c(F)$, $c(G)$, $c(FG)$ be the ideals of R generated by the coefficients of F, G, FG.

(1) Assume $\mathfrak{p} \not\supset c(F)$ and $\mathfrak{p} \not\supset c(G)$. Show $\mathfrak{p} \not\supset c(FG)$.
(2) Show $c(F) = R$ and $c(G) = R$ if and only if $c(FG) = R$.

Solution: For (1), denote the residues of F, G, FG in $(R/\mathfrak{p})[\mathcal{X}]$ by $\bar{F}$, $\bar{G}$, $\overline{FG}$. Now, $\mathfrak{p} \not\supset c(F)$; so $\bar{F} \neq 0$. Similarly, $\bar{G} \neq 0$. But $R/\mathfrak{p}$ is a domain by **(2.8)**. So $(R/\mathfrak{p})[X]$ is too by **(2.4)**. So $\bar{F}\bar{G} \neq 0$. But $\bar{F}\bar{G} = \overline{FG}$. Thus $\mathfrak{p} \not\supset c(FG)$.

For (2), first assume $c(F) = R$ and $c(G) = R$. Then $\mathfrak{p} \not\supset c(F)$ and $\mathfrak{p} \not\supset c(G)$. So $\mathfrak{p} \not\supset c(FG)$ by (1). But $\mathfrak{p}$ is arbitrary. Thus **(2.21)** and **(2.15)** imply $c(FG) = R$.

Conversely, assume $c(FG) = R$. Plainly, in general, $c(FG) \subset c(F)$. So $c(F) = R$. Similarly, $c(G) = R$, as desired. □

Exercise (2.37) . — Let B be a Boolean ring. Show that every prime $\mathfrak{p}$ is maximal, and that $B/\mathfrak{p} = \mathbb{F}_2$.

Solution: Given $x \in B/\mathfrak{p}$, plainly $x(x-1) = 0$. But $B/\mathfrak{p}$ is a domain by **(2.8)**. So $x = 0, 1$. Thus $B/\mathfrak{p} = \mathbb{F}_2$. Plainly, $\mathbb{F}_2$ is a field. So $\mathfrak{p}$ is maximal by **(2.13)**. □

Exercise (2.38) . — Let R be a ring. Assume that, given any $x \in R$, there is an $n \geq 2$ with $x^n = x$. Show that every prime $\mathfrak{p}$ is maximal.

Solution: Given $y \in R/\mathfrak{p}$, say $y(y^{n-1} - 1) = 0$ with $n \geq 2$. By **(2.8)**, $R/\mathfrak{p}$ is a domain. So $y = 0$ or $yy^{n-2} = 1$. So $R/\mathfrak{p}$ is a field. So by **(2.13)**, $\mathfrak{p}$ is maximal. □

Exercise (2.39) . — Prove the following statements, or give a counterexample.

(1) The complement of a multiplicative subset is a prime ideal.
(2) Given two prime ideals, their intersection is prime.
(3) Given two prime ideals, their sum is prime.
(4) Given a ring map $\varphi\colon R \to R'$, the operation φ^{-1} carries maximal ideals of R' to maximal ideals of R.
(5) In **(1.9)**, an ideal $\mathfrak{n}' \subset R/\mathfrak{a}$ is maximal if and only if $\kappa^{-1}\mathfrak{n}' \subset R$ is maximal.

Solution: (1) False. In the ring $\mathbb{Z}$, consider the set S of powers of 2. The complement T of S contains 3 and 5, but not 8; so T is not an ideal.

(2) False. In the ring $\mathbb{Z}$, consider the prime ideals $\langle 2\rangle$ and $\langle 3\rangle$; their intersection $\langle 2\rangle \cap \langle 3\rangle$ is equal to $\langle 6\rangle$, which is not prime.

(3) False. Since $2 \cdot 3 - 5 = 1$, we have $\langle 3\rangle + \langle 5\rangle = \mathbb{Z}$.

(4) False. Let $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. Then $\varphi^{-1}\langle 0\rangle = \langle 0\rangle$.

(5) True. By **(1.9)**, the operation $\mathfrak{b}' \mapsto \kappa^{-1}\mathfrak{b}'$ sets up an inclusion-preserving bijective correspondence between the ideals $\mathfrak{b}' \supset \mathfrak{n}'$ and the ideals $\mathfrak{b} \supset \kappa^{-1}\mathfrak{n}'$. □

Exercise (2.40) . — Preserve the setup of **(2.20)**. Let $F := a_0X^n + \cdots + a_n$ be a polynomial of positive degree n. Assume that R has infinitely many prime elements p, or simply that there is a p such that $p \nmid a_0$. Show that $\langle F\rangle$ is not maximal.

Solution: Set $\mathfrak{a} := \langle p, F\rangle$. Then $\mathfrak{a} \supsetneqq \langle F\rangle$, because p is not a multiple of F. Set $k := R/\langle p\rangle$. Since p is irreducible, k is a domain by **(2.5)** and **(2.7)**. Let $F' \in k[X]$ denote the image of F. By hypothesis, $\deg(F') = n \geq 1$. Hence F' is not a unit by **(2.4.1)** since k is a domain. Therefore, $\langle F'\rangle$ is proper. But $P/\mathfrak{a} \xrightarrow{\sim} k[X]/\langle F'\rangle$ by **(1.16)** and **(1.9)**. So $\mathfrak{a}$ is proper. Thus $\langle F\rangle$ is not maximal. □

Exercise (2.41) . — Preserve the setup of **(2.20)**. Let $\langle 0\rangle \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ be a chain of primes in P. Show $n \leq 2$, with equality if the chain is **maximal**—or, not a proper subchain of a longer chain—and if R has infinitely many primes.

Solution: Recall that R is a UFD, and so P is one too, and that, in any UFD, an element is irreducible if and only if it generates a prime ideal; see **(2.17)** and**(2.5)**. Now, in any domain, consider nested principal ideals $\langle p_1\rangle \subset \langle p_2\rangle$ with p_1 and p_2 irreducible. Then $p_1 = xp_2$ for some x. So x is a unit. Thus $\langle p_1\rangle = \langle p_2\rangle$.

Suppose $n \ge 2$. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$ aren't maximal. So they're all principal by **(2.20)**(1). They're nonzero, so equal by the above. So $1 = n-1$. Thus $n \le 2$.

Assume the chain is maximal. Then $\mathfrak{p}_n$ is maximal. Indeed, $\mathfrak{p}_n$ lies in a maximal ideal $\mathfrak{m}$ by **(2.21)**, and $\mathfrak{m}$ is prime by **(2.15)**. So adjoining $\mathfrak{m}$ results in a longer chain unless $\mathfrak{p}_n = \mathfrak{m}$.

Assume R has infinitely many primes. Then $\mathfrak{p}_n$ isn't principal by **(2.40)**. So $\mathfrak{p}_n = \langle p, G\rangle$ with $p \in R$ prime and $G \in P$ prime by **(2.20)**. So $\langle 0\rangle \subsetneqq \langle p\rangle \subsetneqq \mathfrak{p}_n$ and $\langle 0\rangle \subsetneqq \langle G\rangle \subsetneqq \mathfrak{p}_n$ are both longer chains than $\langle 0\rangle \subsetneqq \mathfrak{p}_n$. But the given chain is maximal. So $n \ne 1$. Thus $n = 2$. □

Exercise (2.42) (*Schwartz–Zippel Theorem with multiplicities*) **.** — Let R be a domain, $T \subset R$ a subset of q elements, $P := R[X_1, \ldots, X_n]$ the polynomial ring in n variables, and $F \in P$ a nonzero polynomial of degree d.

(1) Show by induction on n that $\sum_{x_i\in T} \mathrm{ord}_{(x_1,\ldots,x_n)} F \le dq^{n-1}$.

(2) Show that at most dq^{n-1} points $(x_1, \ldots, x_n) \in T^n$ satisfy $F(x_1, \ldots, x_n) = 0$.

(3) Assume $d < q$. Show that $F(x_1, \ldots, x_n) \ne 0$ for some $x_i \in T_i$.

Solution: In (1), if $F(x, X_2, \ldots, X_n) = 0$ for some $x \in T$, then $F = (X_1 - x)G$ for some $G \in P$ by **(1.6)**(1) with $R[X_2, \cdots, X_n]$ for R. Repeating, we obtain $F = G\prod_{x\in T}(X_1 - x)^{r_x}$ for some $G \in P$ with $G(x, X_2, \cdots, X_n) \ne 0$ for all $x \in T$, and for some $r_x \ge 0$. Then **(2.4.1)** yields

$$\deg(G) = d - \sum_{x\in T} r_x. \tag{2.42.1}$$

Given $x_1, \ldots, x_n \in T$, set $H := \prod_{x\in(T-x_1)}(X_1 - x)^{r_x}$. Then $H(x_1, \ldots, x_n) \ne 0$. So $\mathrm{ord}_{(x_1,\ldots,x_n)} H = 0$ by **(1.8)**. Also $\mathrm{ord}_{(x_1,\ldots,x_n)}(X_1 - x)^{r_x} = r_x$ by **(1.8)**. Hence **(2.4.2)** yields

$$\mathrm{ord}_{(x_1,\ldots,x_n)} F = r_{x_1} + \mathrm{ord}_{(x_1,\ldots,x_n)} G. \tag{2.42.2}$$

Assume $n = 1$. Then $G(x) \ne 0$ for all $x \in T$. So $\mathrm{ord}_{(x)} G = 0$ by **(1.8)**. So **(2.42.2)** yields $\mathrm{ord}_{(x)} F = r_x$. Thus **(2.42.1)** yields $\sum_{x\in T} \mathrm{ord}_{(x)} F \le d$, as desired.

Assume $n > 1$. Summing **(2.42.2)** over all $x_1, \ldots, x_n \in T$ yields

$$\sum_{\text{all } x_i\in T} \mathrm{ord}_{(x_1,\ldots,x_n)} F = q^{n-1}\sum_{x_1\in T} r_{x_1} + \sum_{\text{all } x_i\in T} \mathrm{ord}_{(x_1,\ldots,x_n)} G. \tag{2.42.3}$$

Note $\mathrm{ord}_{(x_1,\ldots,x_n)} G \le \mathrm{ord}_{(x_1,\ldots,x_n)} G_{1,x_1}$ with $G_{1,x_1} := G(x_1, X_2, \ldots, X_n)$ by **(1.8.1)**. But $G_{1,x_1} \in R[X_2, \ldots, X_n]$; so by induction on n and **(2.42.1)**,

$$\sum_{\text{all } x_i\in T} \mathrm{ord}_{(x_2,\ldots,x_n)} G_{1,x_1} \le \Big(d - \sum_{x_1\in T} r_{x_1}\Big)q^{n-2}. \tag{2.42.4}$$

But $\mathrm{ord}_{(x_2,\ldots,x_n)} G_{1,x_1} = \mathrm{ord}_{(x_1,\ldots,x_n)} G_{1,x_1}$ by **(1.8.2)**. Hence, summing **(2.42.4)** over $x_1 \in T$ yields

$$\sum_{\text{all } x_i\in T} \mathrm{ord}_{(x_1,\ldots,x_n)} G \le \sum_{\text{all } x_i\in T} \mathrm{ord}_{(x_1,\ldots,x_n)} G_{1,x_1} \le \Big(d - \sum_{x_1\in T} r_{x_1}\Big)q^{n-1}. \tag{2.42.5}$$

Finally, **(2.42.3)** and **(2.42.5)** yield the desired bound.

For (2), note $\operatorname{ord}_{(x_1,\dots,x_n)}F \geq 0$ with equality (if and) only if $F(x_1,\dots,x_n) \neq 0$ by (**1.8**). Thus (1) yields the desired bound.

In (3), note $dq^{n-1} < q^n$. Thus (2) yields the desired x_i. □

Exercise (2.43) . — Let R be a domain, $P := R[X_1,\dots,X_n]$ the polynomial ring, $F \in P$ nonzero, and $T_i \subset R$ subsets with t_i elements for $i = 1,\dots,n$. For all i, assume that the highest power of X_i in F is at most $t_i - 1$. Show by induction on n that $F(x_1,\dots,x_n) \neq 0$ for some $x_i \in T_i$.

Solution: Say $F = \sum_{j=0}^{t_n-1} F_j X_n^j$ with $F_j \in R[X_1,\dots,X_{n-1}]$. As $F \neq 0$, there's j with $F_j \neq 0$. For all i, the largest exponent of X_i in F_j is at most $t_i - 1$. If $n = 1$, then $F_j \in R$; else, by induction, $F_j(x_1,\dots,x_{n-1}) \neq 0$ for some $x_i \in T_i$. So $F(x_1,\dots,x_{n-1},X_n) \neq 0$. So (**2.42**)(3) yields $x_n \in T_n$ with $F(x_1,\dots,x_n) \neq 0$. □

Exercise (2.44) (*Alon's Combinatorial Nullstellensatz* [1]) . — Let R be a domain, $P := R[X_1,\dots,X_n]$ the polynomial ring, $F \in P$ nonzero of degree d, and $T_i \subset R$ a subset with t_i elements for $i = 1,\dots,n$. Let $\mathbf{M} := \prod_{i=1}^n X_i^{m_i}$ be a monomial with $m_i < t_i$ for all i. Assume F vanishes on $T_1 \times \cdots \times T_n$. Set $F_i(X_i) := \prod_{x\in T_i}(X_i - x)$.

(1) Find $G_i \in P$ with $\deg(G_i) \leq d - t_i$ such that $F = \sum_{i=1}^n F_i G_i$.

(2) Assume $\mathbf{M}$ appears in F. Show $\deg(\mathbf{M}) < d$.

(3) Assume R is a field K. Set $\mathfrak{a} := \langle F_1,\dots,F_n\rangle$ and $t := \prod_{i=1}^n t_i$. Define the evaluation map $\operatorname{ev}\colon P \to K^t$ by $\operatorname{ev}(G) := \big(G(x_1,\dots,x_n)\big)$ where $(x_1,\dots,x_n)$ runs over $T_1 \times \cdots \times T_n$. Show that ev induces a K-algebra isomorphism $\varphi\colon P/\mathfrak{a} \xrightarrow{\sim} K^t$.

Solution: By (**1.20**), there are $G, G_i \in P$ such that $F = \sum_{i=1}^n F_i G_i + G$ where $G_i = 0$ or $\deg(G_i) \leq d - t_i$ and where the highest power of X_i in G is less than t_i.

For (1), note that F and all F_i vanish on $T_1 \times \cdots \times T_n$, so G does too. Hence (**2.43**) implies $G = 0$, as desired.

For (2), note (1) implies $\mathbf{M}$ appears in some $F_i G_i$. But $\deg(G_i) \leq d - t_i$; so $X_i^{t_i}$ divides every monomial in $F_i G_i$ of degree d. Thus $\deg(\mathbf{M}) < d$, as desired.

For (3), note ev is a K-algebra map; also, $\operatorname{ev}(F_i) = 0$ for all i. So ev induces a K-algebra map $\varphi\colon P/\mathfrak{a} \to K^t$. Further, (1) implies $\operatorname{Ker}(\varphi) = 0$, so φ is injective.

Finally, (**1.20**) implies that $P/\mathfrak{a}$ is generated by the residues $a_1^{k_1}\cdots a_n^{k_n}$ of the monomials $X_1^{k_1}\cdots X_n^{k_n}$ with $0 \leq k_i < t_i$. If some linear combination H of those monomials has residue 0, then $\operatorname{ev}(H) = 0$, and so $H = 0$ by (**2.43**). Hence the $a_1^{k_1}\cdots a_n^{k_n}$ are linearly independent. Thus $\dim_K(P/\mathfrak{a}) = t$. But K is a field, φ is injective, and $\dim_K(K^t) = t$. Thus φ is bijective, as desired. □

Exercise (2.45) (*Cauchy–Davenport Theorem*) . — Let $A, B \subset \mathbb{F}_p$ be nonempty subsets. Set $C := \{a + b \mid a \in A \text{ and } b \in B\}$. Say A, B, C have α, β, γ elements.

(1) Assume $C \subsetneq \mathbb{F}_p$. Use $F(X,Y) := \prod_{c\in C}(X + Y - c)$ to show $\gamma \geq \alpha + \beta - 1$.

(2) Show $\gamma \geq \min\{\alpha + \beta - 1,\ p\}$.

Solution (*Alon* [1, Thm. 3.2]): For (1), note that F vanishes on $A \times B$ and has degree γ. Set $m_1 := \alpha - 1$ and $m_2 := \gamma - \alpha + 1$. Then $X^{m_1}Y^{m_2}$ has degree γ, and appears in F with coefficient $\binom{\gamma}{m_1}$, which is nonzero as $\gamma < p$. So $m_2 < \beta$ would contradict (**2.44**)(2). Thus $m_2 \geq \beta$, as desired.

For (2), notice that if $C = \mathbb{F}_p$, then $\gamma = p$ (and conversely), and that if $C \subsetneq \mathbb{F}_p$, then $\gamma \geq \alpha + \beta - 1$ by (1). □

Exercise (2.46) (*Chevalley–Warning Theorem*) . — Let $P := \mathbb{F}_q[X_1, \ldots, X_n]$ be the polynomial ring, $F_1, \ldots, F_m \in P$, and $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ a common zero of the F_j. Assume $n > \sum_{i=1}^m \deg(F_i)$. Set

$$G_1 := \prod_{i=1}^{m}(1 - F_i^{q-1}), \quad G_2 := \delta \prod_{j=1}^{n} \prod_{c \in \mathbb{F}_q,\, c \neq c_j} (X_j - c), \quad \text{and} \quad F := G_1 - G_2,$$

and choose δ so that $F(c_1, \ldots, c_n) = 0$.

(1) Show that $X_1^{q-1} \cdots X_n^{q-1}$ has coefficient $-\delta$ in F and that $\delta \neq 0$.

(2) Use (1) and (2.44)(2) to show that the F_j have another common zero.

Solution (*Alon* [1, Thm. 3.2]): For (1), note $\deg(G_1) = (q-1)\sum \deg(F_i)$. So $\deg(G_1) < (q-1)n$. So $X_1^{q-1} \cdots X_n^{q-1}$ doesn't appear in G_1, but does in $-G_2$, with coefficient $-\delta$, as desired. But $G_1(c_1, \ldots, c_n) = 1$. Thus $\delta \neq 0$, as desired.

For (2), note $\deg(F) = (q-1)n$. So (1) and (2.44)(2) yield $x_j \in \mathbb{F}_q$ with $F(x_1, \ldots, x_n) \neq 0$. But $G_2(x_1, \ldots, x_n) = 0$. So $G_1(x_1, \ldots, x_n) \neq 0$. Given i, then $F_i(x_1, \ldots, x_n)^{q-1} \neq 1$. But $\mathbb{F}_q^\times$ has order $q-1$. So $F_i(x_1, \ldots, x_n) = 0$, as desired. □

3. Radicals

Exercise (3.10) . — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{p}$ an ideal of R. Show:

(1) there is an ideal $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$ if and only if $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$.

(2) if $\mathfrak{p}$ is prime with $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$, then there's a prime $\mathfrak{q}$ of R' with $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$.

Solution: In (1), given $\mathfrak{q}$, note $\varphi(\mathfrak{p}) \subset \mathfrak{q}$, as always $\varphi(\varphi^{-1}(\mathfrak{q})) \subset \mathfrak{q}$. So $\mathfrak{p}R' \subset \mathfrak{q}$. Hence $\varphi^{-1}(\mathfrak{p}R') \subset \varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. But, always $\mathfrak{p} \subset \varphi^{-1}(\mathfrak{p}R')$. Thus $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$. The converse is trivial: take $\mathfrak{q} := \mathfrak{p}R'$.

In (2), set $S := \varphi(R - \mathfrak{p})$. Then $S \cap \mathfrak{p}R' = \emptyset$, as $\varphi(x) \in \mathfrak{p}R'$ implies $x \in \varphi^{-1}(\mathfrak{p}R')$ and $\varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$. So there's a prime $\mathfrak{q}$ of R' containing $\mathfrak{p}R'$ and disjoint from S by (3.9). So $\varphi^{-1}(\mathfrak{q}) \supset \varphi^{-1}(\mathfrak{p}R') = \mathfrak{p}$ and $\varphi^{-1}(\mathfrak{q}) \cap (R - \mathfrak{p}) = \emptyset$. Thus $\varphi^{-1}(\mathfrak{q}) = \mathfrak{p}$. □

Exercise (3.16) . — Use Zorn's lemma to prove that any prime ideal $\mathfrak{p}$ contains a prime ideal $\mathfrak{q}$ that is minimal containing any given subset $\mathfrak{s} \subset \mathfrak{p}$.

Solution: Let $\mathcal{S}$ be the set of all prime ideals $\mathfrak{q}$ such that $\mathfrak{s} \subset \mathfrak{q} \subset \mathfrak{p}$. Then $\mathfrak{p} \in \mathcal{S}$, so $\mathcal{S} \neq \emptyset$. Order $\mathcal{S}$ by reverse inclusion. To apply Zorn's Lemma, we must show that, for any decreasing chain $\{\mathfrak{q}_\lambda\}$ of prime ideals, the intersection $\mathfrak{q} := \bigcap \mathfrak{q}_\lambda$ is a prime ideal. Plainly $\mathfrak{q}$ is always an ideal. So take $x, y \notin \mathfrak{q}$. Then there exists λ such that $x, y \notin \mathfrak{q}_\lambda$. Since $\mathfrak{q}_\lambda$ is prime, $xy \notin \mathfrak{q}_\lambda$. So $xy \notin \mathfrak{q}$. Thus $\mathfrak{q}$ is prime. □

Exercise (3.19) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $R[[X]]$ the formal power series ring, $\mathfrak{M} \subset R[[X]]$ an ideal, $F := \sum a_n X^n \in R[[X]]$. Set $\mathfrak{m} := \mathfrak{M} \cap R$ and $\mathfrak{A} := \{\sum b_n X^n \mid b_n \in \mathfrak{a}\}$. Prove the following statements:

(1) If F is nilpotent, then a_n is nilpotent for all n. The converse is false.

(2) Then $F \in \operatorname{rad}(R[[X]])$ if and only if $a_0 \in \operatorname{rad}(R)$.

(3) Assume $X \in \mathfrak{M}$. Then X and $\mathfrak{m}$ generate $\mathfrak{M}$.

(4) Assume $\mathfrak{M}$ is maximal. Then $X \in \mathfrak{M}$ and $\mathfrak{m}$ is maximal.

(5) If $\mathfrak{a}$ is finitely generated, then $\mathfrak{a}R[[X]] = \mathfrak{A}$. However, there's an example of an R with a prime ideal $\mathfrak{a}$ such that $\mathfrak{a}R[[X]] \neq \mathfrak{A}$.

Solution: For (1), assume F and a_i for $i < n$ nilpotent. Set $G := \sum_{i\geq n} a_iX^i$. Then $G = F - \sum_{i<n} a_iX^i$. So G is nilpotent by (**3.15**); say $G^m = 0$ with $m \geq 1$. Then $a_n^m = 0$. Thus a_n is nilpotent, and by induction on n, all a_n are too.

For a counterexample to the converse, set $P := \mathbb{Z}[X_2, X_3, \dots]$ for variables X_n. Set $R := P/\langle X_2^2, X_3^3, \dots\rangle$. Let a_n be the residue of X_n. Then $a_n^n = 0$, but $\sum a_nX^n$ is not nilpotent. Thus (1) holds.

For (2), given $G = \sum b_nX^n \in \mathrm{rad}(R[[X]])$, note that $1 + FG$ is a unit if and only if $1 + a_0b_0$ is a unit by (**3.7**). Thus (**3.2**) yields (2).

For (3), note $\mathfrak{M}$ contains X and $\mathfrak{m}$, so the ideal they generate. But $F = a_0 + XG$ for some $G \in R[[X]]$. So if $F \in \mathfrak{M}$, then $a_0 \in \mathfrak{M} \cap R = \mathfrak{m}$. Thus (3) holds.

For (4), note that $X \in \mathrm{rad}(R[[X]])$ by (2). But $\mathfrak{M}$ is maximal. So $X \in \mathfrak{M}$. So X and $\mathfrak{m}$ generate $\mathfrak{M}$ by (3). So $R[X]/\mathfrak{M} = R/\mathfrak{m}$ by (**3.7**). Thus (**2.13**) yields (4).

In (5), plainly $\mathfrak{a}R[[X]] \subset \mathfrak{A}$. Now, assume $F := \sum a_nX^n \in \mathfrak{A}$, so all $a_n \in \mathfrak{a}$. Say $b_1, \dots, b_m \in \mathfrak{a}$ generate. Then $a_n = \sum_{i=1}^m c_{ni}b_i$ for some $c_{ni} \in R$. Thus, as desired,

$$F = \sum_{n\geq 0}\Big(\sum_{i=1}^m c_{ni}b_i\Big)X^n = \sum_{i=1}^m b_i\Big(\sum_{n\geq 0} c_{ni}X^n\Big) \in \mathfrak{a}R[[X]].$$

For the desired example, take $a_1, a_2, \dots$ to be variables. Take $R := \mathbb{Z}[a_1, a_2, \dots]$ and $\mathfrak{a} := \langle a_1, a_2, \dots\rangle$. Then $R/\mathfrak{a} = \mathbb{Z}$ by (**1.17**)(3). Thus (**2.8**) implies $\mathfrak{a}$ is prime.

Given $G \in \mathfrak{a}R[[X]]$, say $G = \sum_{i=1}^m b_iG_i$ with $b_i \in \mathfrak{a}$ and $G_i = \sum_{n\geq 0} b_{in}X^n$. Choose p greater than the maximum n such that a_n occurs in any b_i. Then $\sum_{i=1}^m b_ib_{in} \in \langle a_1, \dots, a_{p-1}\rangle$, but $a_p \notin \langle a_1, \dots, a_{p-1}\rangle$. Set $F := \sum a_nX^n$. Then $F \neq G$ for any $G \in \mathfrak{a}R[[X]]$. Thus $F \notin \mathfrak{a}R[[X]]$, but $F \in \mathfrak{A}$. □

Exercise (3.21) . — Let R be a ring, $\mathfrak{a} \subset \mathrm{rad}(R)$ an ideal, $w \in R$, and $w' \in R/\mathfrak{a}$ its residue. Prove that $w \in R^\times$ if and only if $w' \in (R/\mathfrak{a})^\times$. What if $\mathfrak{a} \not\subset \mathrm{rad}(R)$?

Solution: Plainly, $w \in R^\times$ implies $w' \in (R/\mathfrak{a})^\times$, whether $\mathfrak{a} \subset \mathrm{rad}(R)$ or not.

Assume $\mathfrak{a} \subset \mathrm{rad}(R)$. As every maximal ideal of R contains $\mathrm{rad}(R)$, the operation $\mathfrak{m} \mapsto \mathfrak{m}/\mathfrak{a}$ establishes a bijective correspondence between the maximal ideals of R and those of $R/\mathfrak{a}$ owing to (**1.9**). So w belongs to a maximal ideal of R if and only if w' belongs to one of $R/\mathfrak{a}$. Thus $w \in R^\times$ if and only if $w' \in (R/\mathfrak{a})^\times$ by (**2.22**).

Assume $\mathfrak{a} \not\subset \mathrm{rad}(R)$. Then there is a maximal ideal $\mathfrak{m} \subset R$ with $\mathfrak{a} \not\subset \mathfrak{m}$. So $\mathfrak{a} + \mathfrak{m} = R$. So there are $a \in \mathfrak{a}$ and $v \in \mathfrak{m}$ with $a + v = w$. Then $v \notin R^\times$, but the residue of v is w', even if $w' \in (R/\mathfrak{a})^\times$. For example, take $R := \mathbb{Z}$ and $\mathfrak{a} := \langle 2\rangle$ and $w := 3$. Then $w \notin R^\times$, but the residue of w is $1 \in (R/\mathfrak{a})^\times$. □

Exercise (3.22) . — Let A be a local ring, e an idempotent. Show $e = 1$ or $e = 0$.

Solution: Let $\mathfrak{m}$ be the maximal ideal. Then $1 \notin \mathfrak{m}$, so either $e \notin \mathfrak{m}$ or $1-e \notin \mathfrak{m}$. Say $e \notin \mathfrak{m}$. Then e is a unit by (**3.5**). But $e(1-e) = 0$. Thus $e = 1$. Similarly, if $1 - e \notin \mathfrak{m}$, then $e = 0$.

Alternatvely, (**3.6**) implies that A is not the product of two nonzero rings. So (**1.12**) implies that either $e = 0$ or $e = 1$. □

Exercise (3.23) . — Let A be a ring, $\mathfrak{m}$ a maximal ideal such that $1 + m$ is a unit for every $m \in \mathfrak{m}$. Prove A is local. Is this assertion still true if $\mathfrak{m}$ is not maximal?

Solution: Take $y \in A - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, $\langle y\rangle + \mathfrak{m} = A$. Hence there exist $x \in R$ and $m \in \mathfrak{m}$ such that $xy + m = 1$, or in other words, $xy = 1 - m$. So xy is a unit by hypothesis; whence, y is a unit. Thus A is local by (**3.5**).

No, the assertion is not true if $\mathfrak{m}$ is not maximal. Indeed, take any ring that is not local, for example $\mathbb{Z}$, and take $\mathfrak{m} := \langle 0\rangle$. □

Exercise (3.24) . — Let R be a ring, S a subset. Show that S is saturated multiplicative if and only if $R - S$ is a union of primes.

Solution: First, assume S is saturated multiplicative. Take $x \in R - S$. Then $xy \notin S$ for all $y \in R$; in other words, $\langle x\rangle \cap S = \emptyset$. Then (3.9) gives a prime $\mathfrak{p} \supset \langle x\rangle$ with $\mathfrak{p} \cap S = \emptyset$. Thus $R - S$ is a union of primes.

Conversely, assume $R - S$ is a union of primes $\mathfrak{p}$. Then $1 \in S$ as 1 lies in no $\mathfrak{p}$. Take $x, y \in R$. Then $x, y \in S$ if and only if x, y lie in no $\mathfrak{p}$; if and only if xy lies in no $\mathfrak{p}$, as every $\mathfrak{p}$ is prime; if and only if $xy \in S$. Thus S is saturated multiplicative. □

Exercise (3.25) . — Let R be a ring, and S a multiplicative subset. Define its **saturation** to be the subset

$$\overline{S} := \{\, x \in R \mid \text{there is } y \in R \text{ with } xy \in S \,\}.$$

(1) Show (a) that $\overline{S} \supset S$, and (b) that $\overline{S}$ is saturated multiplicative, and (c) that any saturated multiplicative subset T containing S also contains $\overline{S}$.

(2) Set $U := \bigcup_{\mathfrak{p}\cap S=\emptyset} \mathfrak{p}$. Show that $R - \overline{S} = U$.

(3) Let $\mathfrak{a}$ be an ideal; assume $S = 1 + \mathfrak{a}$; set $W := \bigcup_{\mathfrak{p}\supset\mathfrak{a}} \mathfrak{p}$. Show $R - \overline{S} = W$.

(4) Given $f, g \in R$, show that $\overline{S_f} \subset \overline{S_g}$ if and only if $\sqrt{\langle f\rangle} \supset \sqrt{\langle g\rangle}$.

Solution: Consider (1). Trivially, if $x \in S$, then $x \cdot 1 \in S$. Thus (a) holds.

Hence $1 \in \overline{S}$ as $1 \in S$. Now, take $x, x' \in \overline{S}$. Then there are $y, y' \in R$ with xy, $x'y' \in S$. But S is multiplicative. So $(xx'')(yy') \in S$. Hence $xx' \in \overline{S}$. Thus $\overline{S}$ is multiplicative. Further, take $x, x' \in R$ with $xx' \in \overline{S}$. Then there is $y \in R$ with $xx'y \in S$. So $x, x' \in \overline{S}$. Thus S is saturated. Thus (b) holds

Finally, consider (c). Given $x \in \overline{S}$, there is $y \in R$ with $xy \in S$. So $xy \in T$. But T is saturated multiplicative. So $x \in T$. Thus $T \supset \overline{S}$. Thus (c) holds.

In (2), plainly, $R - U \supset S$. Further, $R - U$ is saturated multiplicative by (3.24). So $R - U \supset \overline{S}$ by (1)(c). Thus $U \subset R - \overline{S}$. Conversely, $R - \overline{S}$ is a union of primes $\mathfrak{p}$ by (3.24). Plainly, $\mathfrak{p} \cap S = \emptyset$ for all $\mathfrak{p}$. So $U \supset R - \overline{S}$. Thus $R - \overline{S} = U$, as desired.

For (3), first take a prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $1 \notin \mathfrak{p} + \mathfrak{a}$; else, $1 = p + a$ with $p \in \mathfrak{p}$ and $a \in \mathfrak{a}$, and so $1 - p = a \in \mathfrak{p} \cap S$. So $\mathfrak{p} + \mathfrak{a}$ lies in a maximal ideal $\mathfrak{m}$ by (2.21). Then $\mathfrak{a} \subset \mathfrak{m}$; so $\mathfrak{m} \subset W$. But also $\mathfrak{p} \subset \mathfrak{m}$. Thus $U \subset W$.

Conversely, take $\mathfrak{p} \supset \mathfrak{a}$. Then $1 + \mathfrak{p} \supset 1 + \mathfrak{a} = S$. But $\mathfrak{p} \cap (1 + \mathfrak{p}) = \emptyset$. So $\mathfrak{p} \cap S = \emptyset$. Thus $U \supset W$. Thus $U = W$. Thus (2) implies (3).

Consider (4). By (1)(a), $\overline{S_f} \subset \overline{S_g}$ if and only if $f \in \overline{S_g}$. By definition of saturation, $f \in \overline{S_g}$ if and only if $hf = g^n$ for some h and n. By definition of radical, $hf = g^n$ for some h and n if and only if $g \in \sqrt{\langle f\rangle}$. Plainly, $g \in \sqrt{\langle f\rangle}$ if and only if $\sqrt{\langle g\rangle} \subset \sqrt{\langle f\rangle}$. Thus $\overline{S_f} \subset \overline{S_g}$ if and only if $\sqrt{\langle f\rangle} \supset \sqrt{\langle g\rangle}$, as desired. □

Exercise (3.26) . — Let R be a nonzero ring, S a subset. Show S is maximal in the set $\mathfrak{S}$ of multiplicative subsets T of R with $0 \notin T$ if and only if $R - S$ is a minimal prime of R .

Solution: First, assume S is maximal in $\mathfrak{S}$. Then S is equal to its saturation $\overline{S}$, as $S \subset \overline{S}$ and $\overline{S}$ is multiplicative by (3.25) (1) (a), (b) and as $0 \in \overline{S}$ would imply $0 = 0 \cdot y \in S$ for some y. So $R - S$ is a union of primes $\mathfrak{p}$ by (3.24). Fix a $\mathfrak{p}$. Then (3.16) yields in $\mathfrak{p}$ a minimal prime $\mathfrak{q}$. Then $S \subset R - \mathfrak{q}$. But $R - \mathfrak{q} \in \mathfrak{S}$ by (2.2).

As S is maximal, $S = R - \mathfrak{q}$, or $R - S = \mathfrak{q}$. Thus $R - S$ is a minimal prime.

Conversely, assume $R - S$ is a minimal prime $\mathfrak{q}$. Then $S \in \mathfrak{S}$ by **(2.2)**. Given $T \in \mathfrak{S}$ with $S \subset T$, note $R - \overline{T} = \bigcup \mathfrak{p}$ with $\mathfrak{p}$ prime by **(3.24)**. Fix a $\mathfrak{p}$. Now, $S \subset T \subset \overline{T}$. So $\mathfrak{q} \supset \mathfrak{p}$. But $\mathfrak{q}$ is minimal. So $\mathfrak{q} = \mathfrak{p}$. But $\mathfrak{p}$ is arbitrary, and $\bigcup \mathfrak{p} = R - \overline{T}$. Hence $\mathfrak{q} = R - \overline{T}$. So $S = \overline{T}$. Hence $S = T$. Thus S is maximal. □

Exercise (3.27) . — Let k be a field, X_λ for $\lambda \in \Lambda$ variables, and Λ_π for $\pi \in \Pi$ disjoint subsets of Λ. Set $P := k[\{X_\lambda\}_{\lambda\in\Lambda}]$ and $\mathfrak{p}_\pi := \langle \{X_\lambda\}_{\lambda\in\Lambda_\pi}\rangle$ for all $\pi \in \Pi$. Let $F, G \in P$ be nonzero, and $\mathfrak{a} \subset P$ a nonzero ideal. Set $U := \bigcup_{\pi\in\Pi} \mathfrak{p}_\pi$. Show:

(1) Assume $F \in \mathfrak{p}_\pi$ for some $\pi \in \Pi$, Then every monomial of F is in $\mathfrak{p}_\pi$.

(2) Assume there are $\pi, \rho \in \Pi$ such that $F + G \in \mathfrak{p}_\pi$ and $G \in \mathfrak{p}_\rho$ but $\mathfrak{p}_\rho$ contains no monomial of F. Then $\mathfrak{p}_\pi$ contains every monomial of F and of G.

(3) Assume $\mathfrak{a} \subset U$. Then $\mathfrak{a} \subset \mathfrak{p}_\pi$ for some $\pi \in \Pi$.

Solution: In (1), $F = \sum_{\lambda\in\Lambda_\pi} F_\lambda X_\lambda$ for some $F_\lambda \in P$. So every monomial of F is a multiple of X_λ for some $\lambda \in \Lambda_\pi$. Thus (1) holds.

In (2), every monomial of G is in $\mathfrak{p}_\rho$ by (1). So F and G have distinct monomials. So there's no cancellation in $F + G$. But $F + G \in \mathfrak{p}_\pi$. Thus (1) implies (2).

For (3), fix a nonzero $F \in \mathfrak{a}$. Then for any $G \in \mathfrak{a}$, also $F + G \in \mathfrak{a}$. But $\mathfrak{a} \subset U$. So there are $\pi, \rho \in \Pi$ such that $F + G \in \mathfrak{p}_\pi$ and $G \in \mathfrak{p}_\rho$. So (2) implies that either $\mathfrak{p}_\pi$ or $\mathfrak{p}_\rho$ contains G and some monomial of F. So $\mathfrak{a}$ lies in the union of all $\mathfrak{p}_\rho$ that contain some monomial of F. But the Λ_ρ are disjoint. So this union is finite. Thus Prime Avoidance **(3.12)** yields (3). □

Exercise (3.28) . — Let k be a field, $\mathcal{S} \subset k$ a subset of cardinality d at least 2.

(1) Let $P := k[X_1, \ldots, X_n]$ be the polynomial ring, $F \in P$ nonzero. Assume the highest power of any X_i in F is less than d. Proceeding by induction on n, show that there are $a_1, \ldots, a_n \in \mathcal{S}$ with $F(a_1, \ldots, a_n) \neq 0$.

(2) Let V be a k-vector space, and $W_1, \ldots, W_r$ proper subspaces. Assume $r < d$. Show $\bigcup_i W_i \neq V$.

(3) In (2), let $W \subset \bigcup_i W_i$ be a subspace. Show $W \subset W_i$ for some i.

(4) Let R a k-algebra, $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ideals with $\mathfrak{a} \subset \bigcup_i \mathfrak{a}_i$. Show $\mathfrak{a} \subset \mathfrak{a}_i$ for some i.

Solution: For (1), first assume $n = 1$. Then F has degree at most $d - 1$, so at most $d - 1$ zeros by **(2.35)**(1) or by **(2.42)**(2). So there's $a_1 \in \mathcal{S}$ with $F(a_1) \neq 0$.

Assume $n > 1$. Say $F = \sum_j G_j X_1^j$ with $G_j \in k[X_2, \ldots, X_n]$. But $F \neq 0$. So $G_i \neq 0$ for some i. By induction, there are $a_2, \ldots, a_n \in \mathcal{S}$ with $G_i(a_2, \ldots, a_n) \neq 0$. So there's $a_1 \in \mathcal{S}$ with $F(a_1, \ldots, a_n) = \sum_j G_j(a_2, \ldots, a_n)a_1^j \neq 0$, as desired.

For (2), for all i, take $v_i \in V - W_i$. Form their span $V' \subset V$. Set $n := \dim V'$ and $W_i' := W_i \cap V'$. Then $n < \infty$, and it suffices to show $\bigcup_i W_i' \neq V'$.

Identify V' with k^n. Form the polynomial ring $P := k[X_1, \ldots, X_n]$. For each i, take a linear form $L_i \in P$ that vanishes on W_i'. Set $F := L_1 \cdots L_r$. Then r is the highest power of any variable in F. But $r < d$. So (1) yields $a_1, \ldots, a_n \in \mathcal{S}$ with $F(a_1, \ldots, a_n) \neq 0$. Then $(a_1, \ldots, a_n) \in V' - \bigcup_i W_i'$, as desired.

For (3), for all i, set $U_i := W \cap W_i$. Then $\bigcup_i U_i = W$. So (2) implies $U_i = W$ for some i. Thus $W \subset W_i$ as desired.

Finally, (4) is a special case of (3), as every ideal is a k-vector space. □

Exercise (3.29) . — Let k be a field, $R := k[X, Y]$ the polynomial ring in two variables, $\mathfrak{m} := \langle X, Y\rangle$. Show $\mathfrak{m}$ is a union of strictly smaller primes.

Solution: Since R is a UFD, and $\mathfrak{m}$ is maximal, so prime, any nonzero $F \in \mathfrak{m}$ has a prime factor $P \in \mathfrak{m}$. Thus $\mathfrak{m} = \bigcup_P \langle P \rangle$, but $\mathfrak{m} \neq \langle P \rangle$ as $\mathfrak{m}$ is not principal. □

Exercise (3.30) . — Find the nilpotents in $\mathbb{Z}/\langle n \rangle$. In particular, take $n = 12$.

Solution: An integer m is nilpotent modulo n if and only if some power m^k is divisible by n. The latter holds if and only if every prime factor of n occurs in m. In particular, in $\mathbb{Z}/\langle 12 \rangle$, the nilpotents are 0 and 6. □

Exercise (3.31) (*Nakayama's Lemma for a nilpotent ideal*) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Assume $\mathfrak{a}M = M$ and $\mathfrak{a}$ is nilpotent. Show $M = 0$.

Solution: Since $M = \mathfrak{a}M$, also $\mathfrak{a}^{n-1}M = \mathfrak{a}^n M$ for all $n \geq 1$. So $M = \mathfrak{a}^n M$ for all $n \geq 1$. But $\mathfrak{a}^n = \langle 0 \rangle$ for some $n \geq 1$ by hypothesis. Thus $M = 0$. □

Exercise (3.32) . — Let R be a ring; $\mathfrak{a}$, $\mathfrak{b}$ ideals; $\mathfrak{p}$ a prime. Prove the following:

(1) $\sqrt{\mathfrak{ab}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$. (2) $\sqrt{\mathfrak{a}} = R$ if and only if $\mathfrak{a} = R$.

(3) $\sqrt{\mathfrak{a} + \mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$. (4) $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n > 0$.

Solution: For (1), note $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}, \mathfrak{b}$. So $\sqrt{\mathfrak{ab}} \subset \sqrt{\mathfrak{a} \cap \mathfrak{b}} \subset \sqrt{\mathfrak{a}}, \sqrt{\mathfrak{b}}$ by **(3.13)**. But, given $x \in \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$, note $x^n \in \mathfrak{a}$ and $x^m \in \mathfrak{b}$ for some n, m. So $x^{n+m} \in \mathfrak{ab}$. Thus (1) holds.

For (2), note $1 \in \sqrt{\mathfrak{a}}$ if and only if $1 \in \mathfrak{a}$, as $1^n = 1$ for all n. So **(1.4)** yields (2).

For (3), note $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$ and $\mathfrak{b} \subset \sqrt{\mathfrak{b}}$. So $\mathfrak{a} + \mathfrak{b} \subset \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$. So **(3.13)** yields $\sqrt{\mathfrak{a} + \mathfrak{b}} \subset \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$. Conversely, say $x^n \in \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$ with $n > 0$. Then $x^n = a + b$ with $a^p \in \mathfrak{a}$ and $b^q \in \mathfrak{b}$ with $p, q > 0$. Hence $x^{n(p+q-1)} \in \mathfrak{a} + \mathfrak{b}$; see **(3.15.1)** and the two lines after it. So $x \in \sqrt{\mathfrak{a} + \mathfrak{b}}$. Thus (3) holds.

For (4), note $\mathfrak{p}^n \subset \mathfrak{p}$. So $\sqrt{\mathfrak{p}^n} \subset \sqrt{\mathfrak{p}}$. But $\mathfrak{p}$ is prime; so $\sqrt{\mathfrak{p}} \subset \mathfrak{p}$. Conversely, given $x \in \mathfrak{p}$, note $x^n \in \mathfrak{p}^n$. So $x \in \sqrt{\mathfrak{p}^n}$. Thus (4) holds. □

Exercise (3.33) . — Let R be a ring. Prove these statements: (1) Assume every ideal not contained in $\operatorname{nil}(R)$ contains a nonzero idempotent. Then $\operatorname{nil}(R) = \operatorname{rad}(R)$.
(2) Assume R is Boolean. Then $\operatorname{nil}(R) = \operatorname{rad}(R) = \langle 0 \rangle$.

Solution: For (1), recall **(3.13.1)**, that $\operatorname{nil}(R) \subset \operatorname{rad}(R)$. To prove the opposite inclusion, set $R' := R/\operatorname{nil}(R)$. Assume $\operatorname{rad}(R') \neq \langle 0 \rangle$. Then there is a nonzero idempotent $e \in \operatorname{rad}(R')$. Then $e(1-e) = 0$. But $1 - e$ is a unit by **(3.2)**. So $e = 0$, a contradiction. Hence $\operatorname{rad}(R') = \langle 0 \rangle$. Thus **(1.9)** yields (1).

For (2), recall from **(1.2)** that every element of R is idempotent. So $\operatorname{nil}(R) = \langle 0 \rangle$, and every nonzero ideal contains a nonzero idempotent. Thus (1) yields (2). □

Exercise (3.34) . — Let $e, e' \in \operatorname{Idem}(R)$. Assume $\sqrt{\langle e \rangle} = \sqrt{\langle e' \rangle}$. Show $e = e'$.

Solution: By hypothesis, $e^n \in \langle e' \rangle$ for some $n \geq 1$. But $e^2 = e$, so $e^n = e$. So $e = xe'$ for some x. So $e = xe'^2 = ee'$. By symmetry, $e' = e'e$. Thus $e = e'$. □

Exercise (3.35) . — Let R be a ring, $\mathfrak{a}_1$, $\mathfrak{a}_2$ comaximal ideals with $\mathfrak{a}_1\mathfrak{a}_2 \subset \operatorname{nil}(R)$. Show there are complementary idempotents e_1 and e_2 with $e_i \in \mathfrak{a}_i$.

Solution: Since $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are comaximal, there are $x_i \in \mathfrak{a}_i$ with $x_1 + x_2 = 1$. Given $n \geq 1$, expanding $(x_1 + x_2)^{2n-1}$ and collecting terms yields $a_1 x_1^n + a_2 x_2^n = 1$ for suitable $a_i \in R$. Now, $x_1 x_2 \in \operatorname{nil}(R)$; take $n \geq 1$ so that $(x_1 x_2)^n = 0$. Set $e_i := a_i x_i^n \in \mathfrak{a}_i$. Then $e_1 + e_2 = 1$ and $e_1 e_2 = 0$. Thus e_1 and e_2 are complementary idempotents by **(1.10)**. □

Exercise (3.36) . — Let R be a ring, $\mathfrak{a}$ an ideal, $\kappa\colon R \to R/\mathfrak{a}$ the quotient map. Assume $\mathfrak{a} \subset \operatorname{nil}(R)$. Prove that $\operatorname{Idem}(\kappa)$ is bijective.

Solution: Note that $\operatorname{Idem}(\kappa)$ is injective by **(3.13.1)** and **(3.3)**.

As to surjectivity, given $e' \in \operatorname{Idem}(R/\mathfrak{a})$, take $z \in R$ with residue e'. Then $\langle z \rangle$ and $\langle 1 - z \rangle$ are trivially comaximal. And $\langle z \rangle \langle 1 - z \rangle \subset \mathfrak{a} \subset \operatorname{nil}(R)$ as $\kappa(z - z^2) = 0$. So **(3.35)** yields complementary idempotents $e_1 \in \langle z \rangle$ and $e_2 \in \langle 1 - z \rangle$.

Say $e_1 = xz$ with $x \in R$. Then $\kappa(e_1) = xe'$. So $\kappa(e_1) = xe'^2 = \kappa(e_1)e'$. Similarly, $\kappa(e_2) = \kappa(e_2)(1 - e')$. So $\kappa(e_2)e' = 0$. But $\kappa(e_2) = 1 - \kappa(e_1)$. So $(1 - \kappa(e_1))e' = 0$, or $e' = \kappa(e_1)e'$. But $\kappa(e_1) = \kappa(e_1)e'$. So $\kappa(e_1) = e'$. Thus $\operatorname{Idem}(\kappa)$ is surjective. □

Exercise (3.37) . — Let R be a ring. Prove the following statements equivalent:

(1) R has exactly one prime $\mathfrak{p}$;
(2) every element of R is either nilpotent or a unit;
(3) $R/\operatorname{nil}(R)$ is a field.

Solution: Assume (1). Let $x \in R$ be a nonunit. Then $x \in \mathfrak{p}$. So x is nilpotent by the Scheinnullstellensatz **(3.14)**. Thus (2) holds.

Assume (2). Then every $x \notin \operatorname{nil}(R)$ has an inverse. Thus (3) holds.

Assume (3). Then $\operatorname{nil}(R)$ is maximal by **(2.12)**. But any prime of R contains $\operatorname{nil}(R)$ by **(3.14)**. Thus (1) holds. □

Exercise (3.38) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Assume that $\mathfrak{b}$ is finitely generated modulo $\mathfrak{a}$ and that $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$. Show there's $n \geq 1$ with $\mathfrak{b}^n \subset \mathfrak{a}$.

Solution: Say $x_1, \ldots, x_m$ generate $\mathfrak{b}$ modulo $\mathfrak{a}$. For each i, there's $n_i \geq 1$ with $x_i^{n_i} \in \mathfrak{a}$. Set $n := \sum (n_i - 1)$. Given $x \in \mathfrak{b}$, say $x = \sum_{i=1}^m y_i x_i + a$ with $y_i \in R$ and $a \in \mathfrak{a}$. Then x^n is, modulo $\mathfrak{a}$, a linear combination of terms of the form $x_1^{j_1} \cdots x_m^{j_m}$ with $\sum_{i=1}^m j_i = n$. But $j_i \geq n_i$ for some i, because if $j_i \leq n_i - 1$ for all i, then $\sum j_i \leq \sum (n_i - 1)$. Thus $x^n \in \mathfrak{a}$. □

Exercise (3.39) . — Let $\varphi\colon R \to R'$ be a ring map, $\mathfrak{a} \subset R$ and $\mathfrak{b} \subset R'$ subsets. Prove these two relations: (1) $(\varphi\sqrt{\mathfrak{a}})R' \subset \sqrt{(\varphi\mathfrak{a})R'}$ and (2) $\varphi^{-1}\sqrt{\mathfrak{b}} = \sqrt{\varphi^{-1}\mathfrak{b}}$.

Solution: For (1), given $y \in (\varphi\sqrt{\mathfrak{a}})R'$, say $y = \sum_{i=1}^r (\varphi x_i) y_i$ with $x_i \in \sqrt{\mathfrak{a}}$ and $y_i \in R'$. Then $x_i^{n_i} \in \mathfrak{a}$ for some $n_i > 0$. Hence $y^n \in (\varphi\mathfrak{a})R'$ for any $n > \sum (n_i - 1)$, see the solution of **(3.38)**. So $y \in \sqrt{(\varphi\mathfrak{a})R'}$. Thus (1) holds.

For (2), note that below, (a) is plainly equivalent to (b); and (b), to (c); etc.:

(a) $x \in \varphi^{-1}\sqrt{\mathfrak{b}}$;	(b) $\varphi x \in \sqrt{\mathfrak{b}}$;
(c) $(\varphi x)^n \in \mathfrak{b}$ for some n;	(d) $\varphi(x^n) \in \mathfrak{b}$ for some n;
(e) $x^n \in \varphi^{-1}\mathfrak{b}$ for some n;	(f) $x \in \sqrt{\varphi^{-1}\mathfrak{b}}$.

□

Exercise (3.40) . — Let R be a ring, $\mathfrak{q}$ an ideal, $\mathfrak{p}$ a prime. Assume $\mathfrak{p}$ is finitely generated modulo $\mathfrak{q}$. Show $\mathfrak{p} = \sqrt{\mathfrak{q}}$ if and only if there's $n \geq 1$ with $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$.

Solution: If $\mathfrak{p} = \sqrt{\mathfrak{q}}$, then $\mathfrak{p} \supset \mathfrak{q} \supset \mathfrak{p}^n$ by (**3.38**). Conversely, if $\mathfrak{q} \supset \mathfrak{p}^n$, then clearly $\sqrt{\mathfrak{q}} \supset \mathfrak{p}$. Further, since $\mathfrak{p}$ is prime, if $\mathfrak{p} \supset \mathfrak{q}$, then $\mathfrak{p} \supset \sqrt{\mathfrak{q}}$. □

Exercise (3.41) . — Let R be a ring. Assume R is reduced and has finitely many minimal prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$. Prove that $\varphi\colon R \to \prod(R/\mathfrak{p}_i)$ is injective, and for each i, there is some $(x_1, \dots, x_n) \in \operatorname{Im}(\varphi)$ with $x_i \neq 0$ but $x_j = 0$ for $j \neq i$.

Solution: Clearly $\operatorname{Ker}(\varphi) = \bigcap \mathfrak{p}_i$. Now, R is reduced and the $\mathfrak{p}_i$ are its minimal primes; hence, (**3.14**) and (**3.16**) yield

$$\langle 0\rangle = \sqrt{\langle 0\rangle} = \bigcap \mathfrak{p}_i.$$

Thus $\operatorname{Ker}(\varphi) = \langle 0\rangle$, and so φ is injective.

Finally, fix i. Since $\mathfrak{p}_i$ is minimal, $\mathfrak{p}_i \not\supset \mathfrak{p}_j$ for $j \neq i$; say $a_j \in \mathfrak{p}_j - \mathfrak{p}_i$. Set $a := \prod_{j\neq i} a_j$. Then $a \in \mathfrak{p}_j - \mathfrak{p}_i$ for all $j \neq i$. So take $(x_1, \dots, x_n) := \varphi(a)$. □

Exercise (3.42) . — Let R be a ring, X a variable, $F := a_0 + a_1X + \cdots + a_nX^n$.

(1) Prove F is nilpotent if and only if $a_0, \dots, a_n$ are nilpotent.

(2) Prove F is a unit if and only if a_0 is a unit and $a_1, \dots, a_n$ are nilpotent.

Solution: In (1), if $a_0, \dots, a_n$ are nilpotent, so is F owing to (**3.15**).

Conversely, say $a_i \notin \operatorname{nil}(R)$. Then (**3.14**) yields a prime $\mathfrak{p} \subset R$ with $a_i \notin \mathfrak{p}$. So $F \notin \mathfrak{p}R[X]$. But $\mathfrak{p}R[X]$ is prime by (**2.32**). Thus plainly $F \notin \operatorname{nil}(R[X])$.

Alternatively, say $F^k = 0$. Then $(a_nX^n)^k = 0$. So $F - a_nX^n$ is nilpotent owing to (**3.15**). So $a_0, \dots, a_{n-1}$ are nilpotent by induction on n. Thus (1) is proved.

For (2), suppose a_0 is a unit and $a_1, \dots, a_n$ are nilpotent. Then $a_1X + \cdots + a_nX^n$ is nilpotent by (1), so belongs to $\operatorname{rad}(R)$ by (**3.13.1**). Thus F is a unit by (**3.2**).

Conversely, say $FG = 1$ and $G = b_0 + \cdots + b_mX^m$. So $a_0b_0 = 1$. Thus $a_0 \in R^\times$.

Further, given a prime $\mathfrak{p} \subset R$, let $\kappa\colon R[X] \to (R/\mathfrak{p})[X]$ be the canonical map. Then $\kappa(F)\kappa(G) = 1$. But $R/\mathfrak{p}$ is a domain by (**2.8**). So $\deg \kappa(F) = 0$ owing to (**2.4.1**). So $a_1, \dots, a_n \in \mathfrak{p}$. But $\mathfrak{p}$ is arbitrary. Thus $a_1, \dots, a_n \in \operatorname{nil}(R)$ by (**3.14**).

Alternatively, let's prove $a_n^{r+1}b_{m-r} = 0$ by induction on r. Set $c_i := \sum_{j+k=i} a_jb_k$. Then $\sum c_iX^i = FG$. But $FG = 1$. So $c_i = 0$ for $i > 0$. Taking $i := m + n$ yields $a_nb_m = 0$. But $c_{m+n-r} = 0$. So $a_nb_{m-r} + a_{n-1}b_{m-(r-1)} + \cdots = 0$. Multiply by a_n^r; then $a_n^{r+1}b_{m-r} = 0$ by induction. So $a_n^{m+1}b_0 = 0$. But b_0 is a unit. So $a_n^{m+1} = 0$. So $a_nX^n \in \operatorname{rad}(R[X])$ by (**3.13.1**). But F is a unit. So $F - a_nX^n$ is too by (**3.21**). So $a_1, \dots, a_{n-1}$ are nilpotent by induction on n. Thus (2) is proved. □

Exercise (3.43) . — Generalize (**3.42**) to the polynomial ring $P := R[X_1, \dots, X_r]$.

Solution: Let $F \in P$. Say $F = \sum a_{(i)}X^{(i)}$ where $(i) := (i_1, \dots, i_r)$ and where $X^{(i)} := X_1^{i_1} \cdots X_r^{i_r}$. Set $(0) := (0, \dots, 0)$. Then (1) and (2) generalize as follows:

(1′) Then F is nilpotent if and only if $a_{(i)}$ is nilpotent for all (i).

(2′) Then F is a unit if and only if $a_{(0)}$ is a unit and $a_{(i)}$ is nilpotent for $(i) \neq (0)$.

To prove them, set $R' := R[X_2, \dots, X_r]$, and say $F = \sum F_iX_1^i$ with $F_i \in R'$.

In (1′), if F is nilpotent, so are all F_i by (**3.42**)(1); hence by induction on r, so are all $a_{(i)}$. Conversely, if all $a_{(i)}$ are nilpotent, so is F by (**3.15**). Thus (1′) holds.

In (2′), if $a_{(0)}$ is a unit and $a_{(i)}$ is nilpotent for $(i) \neq (0)$, then $\sum_{(i)\neq(0)} a_{(i)}X^{(i)}$ is nilpotent by (1), so belongs to $\operatorname{rad}(R)$ by (**3.13.1**). Then F is a unit by (**3.2**).

Conversely, suppose F is a unit. Then F_0 is a unit, and F_i is nilpotent for $i > 0$ by (**3.42**)(2). So $a_{(0)}$ is a unit, and $a_{(i)}$ is nilpotent if $i_1 = 0$ and $(i) \neq (0)$, by induction on r. Also, $a_{(i)}$ is nilpotent if $i_1 > 0$ by (1′). Thus (2′) holds. □

Exercise (3.44) . — Let R be a ring, R' an algebra, X a variable. Show:

$$(1)\ \ \mathrm{nil}(R)R' \subset \mathrm{nil}(R') \quad \text{and} \quad (2)\ \ \mathrm{rad}(R[X]) = \mathrm{nil}(R[X]) = \mathrm{nil}(R)R[X].$$

Solution: For (1), given any $y \in \mathrm{nil}(R)R'$, say $y = \sum x_i y_i$ with $x_i \in \mathrm{nil}(R)$ and $y_i \in R'$. Then $x_i y_i \in \mathrm{nil}(R')$. So **(3.15)** yields $y \in \mathrm{nil}(R')$. Thus (1) holds.

For (2), note $\mathrm{rad}(R[X]) \supset \mathrm{nil}(R[X])$ by **(3.13.1)**. And $\mathrm{nil}(R[X]) \supset \mathrm{nil}(R)R[X]$ by (1) or by **(3.42)**(1). Now, given $F := a_0 + \cdots + a_n X^n$ in $\mathrm{rad}(R[X])$, note that $1 + XF$ is a unit by **(3.2)**. So $a_0, \ldots, a_n$ are nilpotent by **(3.42)**(2). So $F \in \mathrm{nil}(R)R[X]$. Thus $\mathrm{nil}(R)R[X] \supset \mathrm{rad}(R[X])$. Thus (2) holds. □

4. Modules

Exercise (4.3) . — Let R be a ring, M a module. Consider the set map

$$\rho\colon \mathrm{Hom}(R, M) \to M \quad \text{defined by} \quad \rho(\theta) := \theta(1).$$

Show that ρ is an isomorphism, and describe its inverse.

Solution: First off, ρ is R-linear, because

$$\rho(x\theta + x'\theta') = (x\theta + x'\theta')(1) = x\theta(1) + x'\theta'(1) = x\rho(\theta) + x'\rho(\theta').$$

Set $H := \mathrm{Hom}(R, M)$. Define $\alpha\colon M \to H$ by $\alpha(m)(x) := xm$. It is easy to check that $\alpha\rho = 1_H$ and $\rho\alpha = 1_M$. Thus ρ and α are inverse isomorphisms by **(4.2)**. □

Exercise (4.14) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, M and N modules. Set

$$\Gamma_{\mathfrak{a}}(M) := \Big\{ m \in M \ \Big|\ \mathfrak{a} \subset \sqrt{\mathrm{Ann}(m)} \Big\}.$$

Show: (1) Assume $\mathfrak{a} \supset \mathfrak{b}$. Then $\Gamma_{\mathfrak{a}}(M) \subset \Gamma_{\mathfrak{b}}(M)$.
(2) Assume $M \subset N$. Then $\Gamma_{\mathfrak{a}}(M) = \Gamma_{\mathfrak{a}}(N) \cap M$.
(3) Then $\Gamma_{\mathfrak{a}}(\Gamma_{\mathfrak{b}}(M)) = \Gamma_{\mathfrak{a}+\mathfrak{b}}(M) = \Gamma_{\mathfrak{a}}(M) \cap \Gamma_{\mathfrak{b}}(M)$.
(4) Then $\Gamma_{\mathfrak{a}}(M) = \Gamma_{\sqrt{\mathfrak{a}}}(M)$.
(5) Assume $\mathfrak{a}$ is finitely generated. Then $\Gamma_{\mathfrak{a}}(M) = \bigcup_{n \ge 1} \{ m \in M \mid \mathfrak{a}^n m = 0 \}$.

Solution: For (1), given $m \in \Gamma_{\mathfrak{a}}(M)$, note $\mathfrak{b} \subset \mathfrak{a} \subset \sqrt{\mathrm{Ann}(m)}$. So $m \in \Gamma_{\mathfrak{b}}(M)$. Thus (1) holds.

For (2), given $m \in \Gamma_{\mathfrak{a}}(M)$, note $\sqrt{\mathrm{Ann}(m)}$ is the same ideal whether m is viewed in M or in N. Thus (2) holds.

For (3), given $m \in M$, note $\mathfrak{a} \subset \sqrt{\mathrm{Ann}(m)}$ and $\mathfrak{b} \subset \sqrt{\mathrm{Ann}(m)}$ if and only if $\mathfrak{a} + \mathfrak{b} \subset \sqrt{\mathrm{Ann}(m)}$. Thus (3) holds.

For (4), given $m \in M$, note $\mathfrak{a} \subset \sqrt{\mathrm{Ann}(m)}$ if and only if $\sqrt{\mathfrak{a}} \subset \sqrt{\mathrm{Ann}(m)}$. Thus (4) holds.

For (5), given $m \in M$ and $n \ge 1$ with $\mathfrak{a}^n m = 0$, note $\mathfrak{a} \subset \sqrt{\mathrm{Ann}(m)}$. Conversely, given $m \in \Gamma_{\mathfrak{a}}(M)$, note $\mathfrak{a} \subset \sqrt{\mathrm{Ann}(m)}$. But $\mathfrak{a}$ is finitely generated. So **(3.38)** gives $n \ge 1$ with $\mathfrak{a}^n \subset \mathrm{Ann}(m)$. So $\mathfrak{a}^n m = 0$. Thus (5) holds. □

Exercise (4.15) . — Let R be a ring, M a module, $x \in \mathrm{rad}(M)$, and $m \in M$. Assume $(1 + x)m = 0$. Show $m = 0$.

Solution: Set $\mathfrak{a} := \mathrm{Ann}(M)$ and $R' := R/\mathfrak{a}$. Then $\mathrm{rad}(R') = \mathrm{rad}(M)/\mathfrak{a}$ by **(4.1.1)**. Let x' be the residue of x. Then $x' \in \mathrm{rad}(R')$. So $1 + x'$ is a unit in R' by **(3.2)**. But $x'm = xm$. Thus $m = (1 + x')^{-1}(1 + x')m = 0$. □

Exercise (4.16) . — Let R be a ring, M a module, N and N_λ submodules for $\lambda \in \Lambda$, and $\mathfrak{a}$, $\mathfrak{a}_\lambda$, $\mathfrak{b}$ ideals for $\lambda \in \Lambda$. Set $(N : \mathfrak{a}) := \{m \in M \mid \mathfrak{a}m \subset N\}$. Show:

(1) $(N : \mathfrak{a})$ is a submodule. (2) $N \subset (N : \mathfrak{a})$.
(3) $(N : \mathfrak{a})\mathfrak{a} \subset N$. (4) $((N : \mathfrak{a}) : \mathfrak{b}) = (N : \mathfrak{ab}) = ((N : \mathfrak{b}) : \mathfrak{a})$.
(5) $\big(\bigcap N_\lambda : \mathfrak{a}\big) = \bigcap (N_\lambda : \mathfrak{a})$. (6) $\big(N : \sum \mathfrak{a}_\lambda\big) = \bigcap (N : \mathfrak{a}_\lambda)$.

Solution: For (1), given $m, n \in (N : \mathfrak{a})$ and $x \in R$, $a \in \mathfrak{a}$, note $am, xan \in N$. So $a(m + xn) \in N$. So $m + xn \in (N : \mathfrak{a})$. Thus (1) holds.

For (2), given $n \in N$, note $\mathfrak{a}n \subset N$. So $n \in (N : \mathfrak{a})$. Thus (2) holds.

For (3), given $m \in (N : \mathfrak{a})$ and $a \in \mathfrak{a}$, note $am \in N$. Thus (3) holds.

For (4), fix $m \in M$. Given $b \in \mathfrak{b}$, note $bm \in (N : \mathfrak{a})$ if and only if $a(bm) \in N$ for all $a \in \mathfrak{a}$. Also, $m \in (N : \mathfrak{ab})$ if and only if $(ab)m \in N$ for all $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$. But $a(bm) = (ab)m$. Thus $((N : \mathfrak{a}) : \mathfrak{b}) = (N : \mathfrak{ab})$. Similarly, $(N : \mathfrak{ab}) = ((N : \mathfrak{b}) : \mathfrak{a})$. Thus (4) holds.

For (5), given $m \in M$, note $\mathfrak{a}m \subset \bigcap N_\lambda$ if and only if $\mathfrak{a}m \subset N_\lambda$ for all λ. Thus (5) holds.

For (6), given $m \in M$, note $\big(\sum \mathfrak{a}_\lambda\big)m \subset N$ if and only if $\mathfrak{a}_\lambda m \subset N$ for all λ. Thus (6) holds. □

Exercise (4.17) . — Let R be a ring, M a module, N, N_λ, L, L_λ submodules for $\lambda \in \Lambda$. Set $(N : L) := \{x \in R \mid xL \subset N\}$. Show:

(1) $(N : L)$ is an ideal. (2) $(N : L) = \mathrm{Ann}((L + N)/N)$.
(3) $(0 : L) = \mathrm{Ann}(L)$. (4) $(N : L) = R$ if $L \subset N$
(5) $(\bigcap N_\lambda : L) = \bigcap (N_\lambda : L)$. (6) $\big(N : \sum L_\lambda\big) = \bigcap (N : L_\lambda)$.

Solution: Assertions (1), (5), (6) can be proved like **(4.16)**(1), (5), (6).

For (2), given $x \in R$, note $xL \subset N$ if and only if $x(L + N) \subset N$. Thus (2) holds.

As to (3), it's the special case of (2) where $N = 0$. Finally, (4) is trivial. □

Exercise (4.18) . — Let R be a ring, $\mathcal{X} := \{X_\lambda\}$ a set of variables, M a module, N a submodule. Set $P := R[\mathcal{X}]$. Prove these statements:

(1) $M[\mathcal{X}]$ is universal among P-modules Q with a given R-map $\alpha\colon M \to Q$; namely, there's a unique P-map $\beta\colon M[\mathcal{X}] \to Q$ with $\beta|M = \alpha$.

(2) $M[\mathcal{X}]$ has this UMP: given a P-module Q and R-maps $\alpha\colon M \to Q$ and $\chi_\lambda\colon Q \to Q$ for all λ, there's a unique R-map $\beta\colon M[\mathcal{X}] \to Q$ with $\beta|M = \alpha$ and $\beta\mu_{X_\lambda} = \chi_\lambda\beta$ for all λ.

(3) $M[\mathcal{X}]/N[\mathcal{X}] = (M/N)[\mathcal{X}]$.

Solution: For (1), given a P-map $\beta\colon M[\mathcal{X}] \to Q$, note $\beta(\sum m_i\mathbf{M}_i)$ is equal to $\sum \beta(m_i)\mathbf{M}_i$ with $m_i \in M$ and $\mathbf{M}_i$ a monomial. So β is unique if $\beta|M = \alpha$, as then $\beta(\sum m_i\mathbf{M}_i) = \sum \alpha(m_i)\mathbf{M}_i$. But the latter equation serves to define a map $\beta\colon M[\mathcal{X}] \to Q$ with $\beta|M = \alpha$. Plainly β is an P-map. Thus (1) holds.

For (2), recall that to give the χ_λ is the same as to give a P-module structure on Q compatible with the R-module structure on Q; see **(4.5)**. Furthermore, given an R-map $\beta\colon M[\mathcal{X}] \to Q$, the condition $\beta\mu_{X_\lambda} = \chi_\lambda\beta$ for all λ just means that β is an $R[\mathcal{X}]$-map. Thus (2) is equivalent to (1).

For (3), let $\kappa_M\colon M \to M/N$ be the quotient map. Define $\lambda\colon M[\mathcal{X}] \to (M/N)[\mathcal{X}]$ by $\lambda(\sum m_i\mathbf{M}_i) := \sum \kappa_M(m_i)\mathbf{M}_i$. Plainly λ is a P-map, and $N[\mathcal{X}] \subset \mathrm{Ker}\,\lambda$. Also λ is surjective as κ_M is. Suppose that $\lambda(\sum m_i\mathbf{M}_i) = 0$. Then $\kappa_M(m_i) = 0$. So $m_i \in N$. So $\sum m_i\mathbf{M}_i \in N[\mathcal{X}]$. Thus $\mathrm{Ker}\,\lambda \subset N[\mathcal{X}]$. So λ induces an isomorphism

$M[\mathfrak{X}]/N[\mathfrak{X}] \xrightarrow{\sim} (M/N)[\mathfrak{X}]$ by (**4.6.1**). Thus (3) holds.

Alternatively, in (3) the two P-modules are equal, as each is universal among P-modules Q with a given R-map $\alpha\colon M \to Q$ vanishing on N. Indeed, first, each is, plainly, a P-module with a canonical R-map from M vanishing on N.

Next, (1) yields a unique P-map $\beta\colon M[\mathfrak{X}] \to Q$ with $\beta|M = \alpha$. But α vanishes on N. Hence β vanishes on $N[\mathfrak{X}]$. Thus β induces a P-map $M[\mathfrak{X}]/N[\mathfrak{X}] \to Q$ whose composition with the canonical map $M \to M[\mathfrak{X}]/N[\mathfrak{X}]$ is α.

Lastly, α factors via M/N. So (1) yields a unique P-map $(M/N)[\mathfrak{X}] \to Q$ whose composition with the map $M \to (M/N)[\mathfrak{X}]$ is α. Thus (3) holds. □

Exercise (4.19) . — Let R be a ring, $\mathfrak{X}$ a set of variables, M a module, and $N_1, \ldots, N_r$ submodules. Set $N = \bigcap N_i$. Prove the following equations:

$$(1)\ \ \operatorname{Ann}\big(M[\mathfrak{X}]\big) = \operatorname{Ann}(M)[\mathfrak{X}]. \quad (2)\ \ N[\mathfrak{X}] = \bigcap N_i[\mathfrak{X}].$$

Solution: For (1), use double inclusion. Given $f \in R[\mathfrak{X}]$, say $f = \sum a_i\mathbf{M}_i$ for monomials $\mathbf{M}_i$. First, assume $f \in \operatorname{Ann}\big(M[\mathfrak{X}]\big)$. Given $m \in M$, note that $0 = fm = \sum a_i m\mathbf{M}_i$. So $a_i m = 0$ for all i. Thus $f \in \operatorname{Ann}(M)[\mathfrak{X}]$.

Conversely, assume $f \in \operatorname{Ann}(M)[\mathfrak{X}]$. Then $a_i \in \operatorname{Ann}(M)$ for all i. Given $g \in M[\mathfrak{X}]$, say that $g = \sum m_j\mathbf{M}'_j$ for $m_j \in M$ and monomials $\mathbf{M}'_j$. Then $fg = \sum_{i,j} a_i m_j \mathbf{M}_i\mathbf{M}'_j = 0$. Thus $f \in \operatorname{Ann}\big(M[\mathfrak{X}]\big)$. Thus (1) holds.

For (2), use double inclusion. Given $m \in M[\mathfrak{X}]$, say $m = \sum m_j\mathbf{M}_j$ for $m_j \in M$ and monomials $\mathbf{M}_j$. First, assume $m \in N[\mathfrak{X}]$. Then for all j, note $m_j \in N$, so $m_j \in N_i$ for all i. So $m \in N_i[\mathfrak{X}]$ for all i. Thus $m \in \bigcap N_i[\mathfrak{X}]$.

Conversely, assume $m \in \bigcap N_i[\mathfrak{X}]$. Then, for all i, as $m \in N_i[\mathfrak{X}]$, each $m_j \in N_i$. So each $m_j \in N$. Thus $m \in N[\mathfrak{X}]$. Thus (2) holds. □

Exercise (4.20) . — Let R be a ring, M a module, X a variable, $F \in R[X]$. Assume there's a nonzero $G \in M[X]$ with $FG = 0$. Show there's a nonzero $m \in M$ with $Fm = 0$. Proceed as follows. Say $G = m_0 + m_1X + \cdots + m_sX^s$ with $m_s \neq 0$. Assume s is minimal among all possible G. Show $Fm_s = 0$ (so $s = 0$).

Solution: Suppose $Fm_s \neq 0$. Say $F = a_0 + a_1X + \cdots + a_rX^r$. Then there's $t \geq 0$ with $a_tm_s \neq 0$, but $a_{t+i}m_s = 0$ for $i > 0$. Fix $i > 0$, and set $H := a_{t+i}G$. Then $FH = 0$. But $H = a_{t+i}m_0 + \cdots + a_{t+i}m_{s-1}X^{s-1}$. As s is minimal, $H = 0$. So $a_{t+i}m_{s-i} = 0$. But $i > 0$ is arbitrary. Also $FG = 0$ yields $a_tm_s + a_{t+1}m_{s-1} + \cdots = 0$. So $a_tm_s = 0$, a contradiction. Thus $Fm_s = 0$. □

Exercise (4.21) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module. Set $N := M/\mathfrak{a}M$. Show that $M/(\mathfrak{a}+\mathfrak{b})M \xrightarrow{\sim} N/\mathfrak{b}N$.

Solution: Note $\mathfrak{b}N = (\mathfrak{a}+\mathfrak{b})M/\mathfrak{a}M$. Thus (**4.8.1**) yields the isomorphism. □

Exercise (4.22) . — Show that a finitely generated free module has finite rank.

Solution: Say e_λ for $\lambda \in \Lambda$ form a free basis, and $m_1, \ldots, m_r$ generate. Then $m_i = \sum x_{ij}e_{\lambda_j}$ for some x_{ij}. Consider the e_{λ_j} that occur. Plainly, they are finite in number, and generate. So they form a finite free basis, as desired. □

Exercise (4.23) . — Let R be a domain, and $x \in R$ nonzero. Let M be the submodule of $\operatorname{Frac}(R)$ generated by 1, x^{-1}, $x^{-2}, \ldots.$ Suppose that M is finitely generated. Prove that $x^{-1} \in R$, and conclude that $M = R$.

Solution: Suppose M is generated by $m_1, \ldots, m_k$. Say $m_i = \sum_{j=0}^{n_i} a_{ij} x^{-j}$ for some n_i and $a_{ij} \in R$. Set $n := \max\{n_i\}$. Then $1,\ x^{-1}, \ldots, x^{-n}$ generate M. So

$$x^{-(n+1)} = a_n x^{-n} + \cdots + a_1 x^{-1} + a_0$$

for some $a_i \in R$. Thus

$$x^{-1} = a_n + \cdots + a_1 x^{n-1} + a_0 x^n \in R.$$

Finally, as $x^{-1} \in R$ and R is a ring, also $1, x^{-1}, x^{-2}, \ldots \in R$; so $M \subset R$. Conversely, $M \supset R$ as $1 \in M$. Thus $M = R$. □

Exercise (4.24) . — Let Λ be an infinite set, R_λ a nonzero ring for $\lambda \in \Lambda$. Endow $\prod R_\lambda$ and $\bigoplus R_\lambda$ with componentwise addition and multiplication. Show that $\prod R_\lambda$ has a multiplicative identity (so is a ring), but that $\bigoplus R_\lambda$ does not (so is not a ring).

Solution: Consider the vector (1) whose every component is 1. Obviously, (1) is a multiplicative identity of $\prod R_\lambda$. On the other hand, no restricted vector (x_λ) can be a multiplicative identity in $\bigoplus R_\lambda$; indeed, because Λ is infinite, x_μ must be zero for some μ. So $(x_\lambda) \cdot (y_\lambda) \neq (y_\lambda)$ if $y_\mu \neq 0$. □

Exercise (4.25) . — Let R be a ring, M a module, and M', M'' submodules. Show that $M = M' \oplus M''$ if and only if $M = M' + M''$ and $M' \cap M'' = 0$.

Solution: Assume $M = M' \oplus M''$. Then M is the set of pairs (m', m'') with $m' \in M'$ and $m'' \in M''$ by (4.13); further, M' is the set of $(m', 0)$, and M'' is that of $(0, m'')$. So plainly $M = M' + M''$ and $M' \cap M'' = 0$.

Conversely, consider the map $M' \oplus M'' \to M$ given by $(m', m'') \mapsto m' + m''$. It is surjective if $M = M' + M''$. It is injective if $M' \cap M'' = 0$; indeed, if $m' + m'' = 0$, then $m' = -m'' \in M' \cap M'' = 0$, and so $(m', m'') = 0$ as desired. □

Exercise (4.26) . — Let L, M, and N be modules. Consider a diagram

$$L \underset{\rho}{\overset{\alpha}{\rightleftarrows}} M \underset{\sigma}{\overset{\beta}{\rightleftarrows}} N$$

where α, β, ρ, and σ are homomorphisms. Prove that

$$M = L \oplus N \quad \text{and} \quad \alpha = \iota_L,\ \beta = \pi_N,\ \sigma = \iota_N,\ \rho = \pi_L$$

if and only if the following relations hold:

$$\beta\alpha = 0,\ \beta\sigma = 1,\ \rho\sigma = 0,\ \rho\alpha 1,\ \text{and } \alpha\rho + \sigma\beta = 1.$$

Solution: If $M = L \oplus N$ and $\alpha = \iota_L$, $\beta = \pi_N$, $\sigma\iota_N$, $\rho = \pi_L$, then the definitions immediately yield $\alpha\rho + \sigma\beta = 1$ and $\beta\alpha = 0$, $\beta\sigma = 1$, $\rho\sigma = 0$, $\rho\alpha = 1$.

Conversely, assume $\alpha\rho + \sigma\beta = 1$ and $\beta\alpha = 0$, $\beta\sigma = 1$, $\rho\sigma = 0$, $\rho\alpha = 1$. Consider the maps $\varphi \colon M \to L \oplus N$ and $\theta \colon L \oplus N \to M$ given by $\varphi m := (\rho m,\ \beta m)$ and $\theta(l, n) := \alpha l + \sigma n$. They are inverse isomorphisms, because

$$\varphi\theta(l, n) = (\rho\alpha l + \rho\sigma n,\ \beta\alpha l + \beta\sigma n) = (l, n) \quad \text{and} \quad \theta\varphi m = \alpha\rho m + \sigma\beta m = m.$$

Lastly, $\beta = \pi_N \varphi$ and $\rho = \pi_L \varphi$ by definition of φ, and $\alpha = \theta\iota_L$ and $\sigma = \theta\iota_N$ by definition of θ. □

Exercise (4.27) . — Let L be a module, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove that the injections $\iota_\kappa \colon M_\kappa \to \bigoplus M_\lambda$ induce an injection

$$\bigoplus \operatorname{Hom}(L,\ M_\lambda) \hookrightarrow \operatorname{Hom}(L,\ \bigoplus M_\lambda),$$

and that it is an isomorphism if L is finitely generated.

Solution: For $\lambda \in \Lambda$, let $\alpha_\lambda\colon L \to M_\lambda$ be maps, almost all 0. Then

$$\bigl(\sum \iota_\lambda \alpha_\lambda\bigr)(l) = \bigl(\alpha_\lambda(l)\bigr) \in \bigoplus M_\lambda.$$

So if $\sum \iota_\lambda \alpha_\lambda = 0$, then $\alpha_\lambda = 0$ for all λ. Thus the ι_κ induce an injection.

Assume L is finitely generated, say by $l_1, \dots, l_k$. Let $\alpha\colon L \to \bigoplus M_\lambda$ be a map. Then each $\alpha(l_i)$ lies in a finite direct subsum of $\bigoplus M_\lambda$. So $\alpha(L)$ lies in one too. Set $\alpha_\kappa := \pi_\kappa \alpha$ for all $\kappa \in \Lambda$. Then almost all α_κ vanish. So (α_κ) lies in $\bigoplus \operatorname{Hom}(L, M_\lambda)$, and $\sum \iota_\kappa \alpha_\kappa = \alpha$. Thus the ι_κ induce a surjection, so an isomorphism. □

Exercise (4.28) . — Let $\mathfrak{a}$ be an ideal, Λ a nonempty set, M_λ a module for $\lambda \in \Lambda$. Prove $\mathfrak{a}\bigl(\bigoplus M_\lambda\bigr) = \bigoplus \mathfrak{a}M_\lambda$. Prove $\mathfrak{a}(\prod M_\lambda) = \prod \mathfrak{a}M_\lambda$ if $\mathfrak{a}$ is finitely generated.

Solution: First, $\mathfrak{a}\bigl(\bigoplus M_\lambda\bigr) \subset \bigoplus \mathfrak{a}M_\lambda$ because $a \cdot (m_\lambda) = (am_\lambda)$. Conversely, $\mathfrak{a}\bigl(\bigoplus M_\lambda\bigr) \supset \bigoplus \mathfrak{a}M_\lambda$ because $(a_\lambda m_\lambda) = \sum a_\lambda \iota_\lambda m_\lambda$ since the sum is finite.

Second, $\mathfrak{a}\bigl(\prod M_\lambda\bigr) \subset \prod \mathfrak{a}M_\lambda$ as $a(m_\lambda) = (am_\lambda)$. Conversely, say $\mathfrak{a}$ is generated by $f_1, \dots, f_n$. Then $\mathfrak{a}\bigl(\prod M_\lambda\bigr) \supset \prod \mathfrak{a}M_\lambda$. Indeed, take $(m'_\lambda) \in \prod \mathfrak{a}M_\lambda$. Then for each λ, there is n_λ such that $m'_\lambda = \sum_{j=1}^{n_\lambda} a_{\lambda j} m_{\lambda j}$ with $a_{\lambda j} \in \mathfrak{a}$ and $m_{\lambda j} \in M_\lambda$. Write $a_{\lambda j} = \sum_{i=1}^{n} x_{\lambda j i} f_i$ with the $x_{\lambda j i}$ scalars. Then

$$(m'_\lambda) = \Bigl(\sum_{j=1}^{n_\lambda} \sum_{i=1}^{n} f_i x_{\lambda j i} m_{\lambda j}\Bigr) = \sum_{i=1}^{n} f_i \Bigl(\sum_{j=1}^{n_\lambda} x_{\lambda j i} m_{\lambda j}\Bigr) \in \mathfrak{a}\Bigl(\prod M_\lambda\Bigr). \qquad \square$$

Exercise (4.29) . — Let R be a ring, Λ a set, M_λ a module for $\lambda \in \Lambda$, and $N_\lambda \subset M_\lambda$ a submodule. Set $M := \bigoplus M_\lambda$ and $N := \bigoplus N_\lambda$ and $Q := \bigoplus M_\lambda/N_\lambda$. Show $M/N = Q$.

Solution: For each λ, let $\kappa_\lambda\colon M_\lambda \twoheadrightarrow M_\lambda/N_\lambda$ be the quotient map. Define $\kappa\colon M \to Q$ by $\kappa\bigl((m_\lambda)\bigr) = \bigl(\kappa_\lambda(m_\lambda)\bigr)$.

Given $(q_\lambda) \in Q$, say $q_\lambda = \kappa_\lambda(m_\lambda)$. Then $\kappa\bigl((m_\lambda)\bigr) = (q_\lambda)$. Thus κ is surjective.

Given $(m_\lambda) \in M$, note $\kappa\bigl((m_\lambda)\bigr) = 0$ if and only if $\kappa_\lambda(m_\lambda) = 0$ for all λ, so if and only if $m_\lambda \in N_\lambda$ for all λ. Thus $\operatorname{Ker}(\kappa) = N$. Thus (4.6) yields $Q = M/N$. □

5. Exact Sequences

Exercise (5.5) . — Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence. Prove that, if M' and M'' are finitely generated, then so is M.

Solution: Let $m''_1, \dots, m''_n \in M$ map to elements generating M''. Let $m \in M$, and write its image in M'' as a linear combination of the images of the m''_i. Let $m'' \in M$ be the same combination of the m''_i. Set $m' := m - m''$. Then m' maps to 0 in M''; so m' is the image of an element of M'.

Let $m'_1, \dots, m'_l \in M$ be the images of elements generating M'. Then m' is a linear combination of the m'_j. So m is a linear combination of the m''_i and m'_j. Thus the m'_i and m''_j together generate M. □

Exercise (5.15) . — Show that a free module $R^{\oplus\Lambda}$ is projective.

Solution: Given $\beta\colon M \twoheadrightarrow N$ and $\alpha\colon R^{\oplus\Lambda} \to N$, use the UMP of (4.10) to define $\gamma\colon R^{\oplus\Lambda} \to M$ by sending the standard basis vector e_λ to any **lift** of $\alpha(e_\lambda)$, that is, any $m_\lambda \in M$ with $\beta(m_\lambda) = \alpha(e_\lambda)$. (The Axiom of Choice permits a simultaneous choice of all m_λ if Λ is infinite.) Clearly $\alpha = \beta\gamma$. Thus $R^{\oplus\Lambda}$ is projective. □

Exercise (5.18) . — Let R be a ring, and $0 \to L \to R^n \to M \to 0$ an exact sequence. Prove M is finitely presented if and only if L is finitely generated.

Solution: Assume M is finitely presented; say $R^l \to R^m \to M \to 0$ is a finite presentation. Let L' be the image of R^l. Then $L' \oplus R^n \simeq L \oplus R^m$ by Schanuel's Lemma (5.17). Hence L is a quotient of $R^l \oplus R^n$. Thus L is finitely generated.

Conversely, assume L is generated by ℓ elements. They yield a surjection $R^\ell \twoheadrightarrow L$ by (4.10)(1). It yields a sequence $R^\ell \to R^n \to M \to 0$. The latter is, plainly, exact. Thus M is finitely presented. □

Exercise (5.21) . — Let M' and M'' be modules, $N \subset M'$ a submodule. Set $M := M' \oplus M''$. Using (5.2)(1) and (5.3) and (5.4), prove $M/N = M'/N \oplus M''$.

Solution: By (5.2)(1) and (5.3), the two sequences $0 \to M'' \to M'' \to 0$ and $0 \to N \to M' \to M'/N \to 0$ are exact. So by (5.4), the sequence

$$0 \to N \to M' \oplus M'' \to (M'/N) \oplus M'' \to 0$$

is exact. Thus (5.3) yields the assertion. □

Exercise (5.22) . — Let M', M'' be modules, and set $M := M' \oplus M''$. Let N be a submodule of M containing M', and set $N'' := N \cap M''$. Prove $N = M' \oplus N''$.

Solution: Form the sequence $0 \to M' \to N \to \pi_{M''} N \to 0$. It splits by (5.8) as $(\pi_{M'}|N) \circ \iota_{M'} = 1_{M'}$. Finally, if $(m', m'') \in N$, then $(0, m'') \in N$ as $M' \subset N$; hence, $\pi_{M''} N = N''$. □

Exercise (5.23) (*Five Lemma*) . — Consider this commutative diagram:

$$\begin{array}{ccccccccc}
M_4 & \xrightarrow{\alpha_4} & M_3 & \xrightarrow{\alpha_3} & M_2 & \xrightarrow{\alpha_2} & M_1 & \xrightarrow{\alpha_1} & M_0 \\
\gamma_4 \downarrow & & \gamma_3 \downarrow & & \gamma_2 \downarrow & & \gamma_1 \downarrow & & \gamma_0 \downarrow \\
N_4 & \xrightarrow{\beta_4} & N_3 & \xrightarrow{\beta_3} & N_2 & \xrightarrow{\beta_2} & N_1 & \xrightarrow{\beta_1} & N_0
\end{array}$$

Assume it has exact rows. Via a chase, prove these two statements:

(1) If γ_3 and γ_1 are surjective and if γ_0 is injective, then γ_2 is surjective.
(2) If γ_3 and γ_1 are injective and if γ_4 is surjective, then γ_2 is injective.

Solution: Let's prove (1). Take $n_2 \in N_2$. Since γ_1 is surjective, there is $m_1 \in M_1$ such that $\gamma_1(m_1) = \beta_2(n_2)$. Then $\gamma_0\alpha_1(m_1) = \beta_1\gamma_1(m_1) = \beta_1\beta_2(n_2) = 0$ by commutativity and exactness. Since γ_0 is injective, $\alpha_1(m_1) = 0$. Hence exactness yields $m_2 \in M_2$ with $\alpha_2(m_2) = m_1$. So $\beta_2(\gamma_2(m_2) - n_2) = \gamma_1\alpha_2(m_2) - \beta_2(n_2) = 0$.

Hence exactness yields $n_3 \in N_3$ with $\beta_3(n_3) = \gamma_2(m_2) - n_2$. Since γ_3 is surjective, there is $m_3 \in M_3$ with $\gamma_3(m_3) = n_3$. Then $\gamma_2\alpha_3(m_3) = \beta_3\gamma_3(m_3) = \gamma_2(m_2) - n_2$. Hence $\gamma_2(m_2 - \alpha_3(m_3)) = n_2$. Thus γ_2 is surjective.

The proof of (2) is similar. □

Exercise (5.24) (*Nine Lemma*) . — Consider this commutative diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & L' \arrow[r] \arrow[d] & L \arrow[r] \arrow[d] & L'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & N' \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & N'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Assume all the columns are exact and the middle row is exact. Applying the Snake Lemma (5.10), show that the first row is exact if and only if the third is.

Solution: The first row is exact if the third is owing to the Snake Lemma (5.10) applied to the bottom two rows. The converse is proved similarly. □

Exercise (5.25) . — Referring to (4.8), give an alternative proof that β is an isomorphism by applying the Snake Lemma (5.10) to the diagram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d, "\kappa"'] & N/M \arrow[r] \arrow[d, "\beta"'] & 0 \\
0 \arrow[r] & M/L \arrow[r] & N/L \arrow[r, "\lambda"] & (N/L)\big/(M/L) \arrow[r] & 0
\end{tikzcd}$$

Solution: The Snake Lemma yields an exact sequence,

$$L \xrightarrow{1} L \to \operatorname{Ker}(\beta) \to 0;$$

hence, $\operatorname{Ker}(\beta) = 0$. Moreover, β is surjective because κ and λ are. □

Exercise (5.26) . — Consider this commutative diagram with exact rows:

$$\begin{tikzcd}
M' \arrow[r, "\beta"] \arrow[d, "\alpha'"'] & M \arrow[r, "\gamma"] \arrow[d, "\alpha"'] & M'' \arrow[d, "\alpha''"'] \\
N' \arrow[r, "\beta'"] & N \arrow[r, "\gamma'"] & N''
\end{tikzcd}$$

Assume α' and γ are surjective. Given $n \in N$ and $m'' \in M''$ with $\alpha''(m'') = \gamma'(n)$, show that there is $m \in M$ such that $\alpha(m) = n$ and $\gamma(m) = m''$.

Solution: Since γ is surjective, there is $m_1 \in M$ with $\gamma(m_1) = m''$. Then $\gamma'\big(n - \alpha(m_1)\big) = 0$ as $\alpha''(m'') = \gamma'(n)$ and as the right-hand square is commutative. So by exactness of the bottom row, there is $n' \in N'$ with $\beta'(n') = n - \alpha(m_1)$. Since α' is surjective, there is $m' \in M'$ with $\alpha'(m') = n'$. Set $m := m_1 + \beta(m')$. Then $\gamma(m) = m''$ as $\gamma\beta = 0$. Further, $\alpha(m) = \alpha(m_1) + \beta'(n') = n$ as the left-hand square is commutative. Thus m works. □

Exercise (5.27) . — Let R be a ring. Show that a module P is finitely generated and projective if and only if it's a direct summand of a free module of finite rank.

Solution: Assume P is generated by n elements. Then **(5.13)** yields an exact sequence $0 \to K \to R^n \to P \to 0$. Assume P is projective too, Then this sequence splits by **(5.16)**, as desired.

Conversely, assume $P \oplus K \simeq R^n$ for some K and n. Then P is projective by **(5.16)**. Also, the projection $R^n \to P$ is surjective; so P is finitely generated. □

Exercise (5.28) . — Let R be a ring, P and N finitely generated modules with P projective. Prove $\operatorname{Hom}(P, N)$ is finitely generated, and is finitely presented if N is.

Solution: Say P is generated by n elements. Then **(5.13)** yields an exact sequence $0 \to K \to R^n \to P \to 0$. It splits by **(5.16)**. So **(4.13.2)** yields

$$\operatorname{Hom}(P, N) \oplus \operatorname{Hom}(K, N) = \operatorname{Hom}(R^{\oplus m}, N).$$

But $\operatorname{Hom}(R^{\oplus n}, N) = \operatorname{Hom}(R, N)^{\oplus n} = N^{\oplus n}$ by **(4.13.2)** and **(4.3)**. Also N is finitely generated. Hence $\operatorname{Hom}(R^{\oplus n}, N)$ is too. But $\operatorname{Hom}(P, N)$ and $\operatorname{Hom}(K, N)$ are quotients of $\operatorname{Hom}(R^{\oplus n}, N)$ by **(5.8)**. Thus they're finitely generated too.

Suppose now there is a finite presentation $F_2 \to F_1 \to N \to 0$. Then **(5.15)** and **(5.16)** yield the exact sequence

$$\operatorname{Hom}(R^{\oplus n}, F_2) \to \operatorname{Hom}(R^{\oplus n}, F_1) \to \operatorname{Hom}(R^{\oplus n}, N) \to 0.$$

But the $\operatorname{Hom}(R^{\oplus n}, F_i)$ are free of finite rank by **(4.13.1)** and **(4.13.2)**. Thus $\operatorname{Hom}(R^{\oplus n}, N)$ is finitely presented.

As in **(5.2)**, form the (split) exact sequence

$$0 \to \operatorname{Hom}(K, N) \to \operatorname{Hom}(R^{\oplus n}, N) \to \operatorname{Hom}(P, N) \to 0.$$

Apply **(5.19)**. Thus $\operatorname{Hom}(P, N)$ is finitely presented. □

Exercise (5.29) . — Let R be a ring, $X_1, X_2, \ldots$ infinitely many variables. Set $P := R[X_1, X_2, \ldots]$ and $M := P/\langle X_1, X_2, \ldots \rangle$. Is M finitely presented? Explain.

Solution: No, otherwise by **(5.18)**, the ideal $\langle X_1, X_2, \ldots \rangle$ would be generated by some $f_1, \ldots, f_n \in P$, so also by $X_1, \ldots, X_m$ for some m, but plainly it isn't. □

Exercise (5.30) . — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence with M finitely generated and N finitely presented. Prove L is finitely generated.

Solution: Let R be the ground ring. Say M is generated by m elements. They yield a surjection $\mu\colon R^m \twoheadrightarrow M$ by **(4.10)**(1). As in **(5.19)**, μ induces the following commutative diagram, with λ surjective:

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, "\lambda"'] & R^m \arrow[r] \arrow[d, "\mu"'] & N \arrow[r] \arrow[d, "1_N"'] & 0 \\
0 \arrow[r] & L \arrow[r, "\alpha"] & M \arrow[r, "\beta"] & N \arrow[r] & 0
\end{tikzcd}$$

By **(5.18)**, K is finitely generated. Thus L is too, as λ is surjective. □

5. Appendix: Fitting Ideals

Exercise (5.36) . — Let R be a ring, and $a_1, \dots, a_m \in R$ with $\langle a_1 \rangle \supset \cdots \supset \langle a_m \rangle$. Set $M := R/\langle a_1 \rangle \oplus \cdots \oplus R/\langle a_m \rangle$. Show that $F_r(M) = \langle a_1 \cdots a_{m-r} \rangle$.

Solution: Form the presentation $R^m \xrightarrow{\alpha} R^m \to M \to 0$ where α has matrix

$$\mathbf{A} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_m \end{pmatrix}$$

Set $s := m - r$. Now, $a_i \in \langle a_{i-1} \rangle$ for all $i > 1$. Hence $a_{i_1} \cdots a_{i_s} \in \langle a_1 \cdots a_s \rangle$ for all $1 \le i_1 < \cdots < i_s \le m$. Thus $I_s(\mathbf{A}) = \langle a_1 \cdots a_s \rangle$, as desired. □

Exercise (5.37) . — In the setup of (5.36), assume a_1 is a nonunit. Show:

(1) Then m is the smallest integer such that $F_m(M) = R$.

(2) Let n be the largest integer with $F_n(M) = \langle 0 \rangle$; set $k := m - n$. Assume R is a domain. Then (a) $a_i \neq 0$ for $i < k$ and $a_i = 0$ for $i \ge k$, and (b) each a_i is unique up to unit multiple.

Solution: For (1), note there's a presentation $R^m \to R^m \to M \to 0$; see the solution to (5.36). So $F_m(M) = R$ by (5.35). On the other hand, $F_{m-1}(M) = \langle a_1 \rangle$ by (5.36). So $F_{m-1}(M) \neq R$ as a_1 is a nonunit. Thus (1) holds.

For (2)(a), note $F_{n+1}(M) \neq \langle 0 \rangle$ and $F_n(M) = \langle 0 \rangle$. Hence $a_1 \cdots a_{k-1} \neq 0$ and $a_1 \cdots a_k = 0$ by (5.36). But R is a domain. Hence $a_1, \dots, a_i \neq 0$ for $i < k$ and $a_k = 0$. But $\langle a_k \rangle \supset \cdots \supset \langle a_m \rangle$. Hence $a_i = 0$ for $i \ge k$. Thus (2)(a) holds.

For (2)(b), given $b_1, \dots, b_p \in R$ with b_1 a nonunit, with $\langle b_1 \rangle \supset \cdots \supset \langle b_p \rangle$ and $M = (R/\langle b_1 \rangle) \oplus \cdots \oplus (R/\langle b_p \rangle)$, note that (1) yields $p = m$ and that (2)(a) yields $b_i \neq 0$ for $i < k$ and $b_i = 0$ for $i \ge k$.

Given i, (5.36) yields $\langle a_1 \cdots a_i \rangle = \langle b_1 \cdots b_i \rangle$. But R is a domain. So (2.30) yields a unit u_i such that $a_1 \cdots a_i = u_i b_1 \cdots b_i$. So

$$u_{i-1} b_1 \cdots b_{i-1} a_i = u_r b_1 \cdots b_i.$$

If $i < k$, then $b_1 \cdots b_{i-1} \neq 0$; whence, $u_{i-1} a_i = u_i b_i$. Thus (2)(b) holds. □

Exercise (5.41) (*Structure Theorem*) . — Let R be a PID, M a finitely generated module. Set $T := \{m \in M \mid xm = 0 \text{ for some nonzero } x \in R\}$. Show:

(1) Then M has a free submodule F of finite rank with $M = T \oplus F$.

(2) Then $T \simeq \bigoplus_{j=1}^{n} R/\langle d_j \rangle$ with the d_j nonzero nonunits in R, unique up to unit multiple, and $d_j \mid d_{j+1}$ for $1 \le j < n$.

(3) Then $T \simeq \bigoplus_{i=1}^{m} M(p_i)$ with $M(p_i) := \bigoplus_{j=1}^{n} R/\langle p_i^{e_{ij}} \rangle$, the p_i primes in R, unique up to unit multiple, and the e_{ij} unique with $0 \le e_{ij} \le e_{i\,j+1}$ and $1 \le e_{in}$.

(4) If M isn't finitely generated, there may be no free F with $M = T \oplus F$.

Solution: Note (4.10)(1) yields a free module E of finite rank and a surjection $E \twoheadrightarrow M$. Let N be the kernel. Then N is free of finite rank by (4.12). So (5.38) yields a decomposition $E = E' \oplus F$, a basis $e_1, \dots, e_n$ of E', and essentially unique $d_1, \dots, d_n \in R$ with $N = Rd_1e_1 \oplus \cdots \oplus Rd_ne_n$ and $\langle d_1 \rangle \supset \cdots \supset \langle d_n \rangle \neq 0$. Moreover, $E' = \{m \in M \mid xm \in N \text{ for some nonzero } x \in R\}$; so $E'/N = T \subset M$.

Note (1) holds as $M = T \oplus F$ by (5.21), and F is free of finite rank by (4.12).

Note (2) holds as $E'/N = R/\langle d_1 \rangle \oplus \cdots \oplus R/\langle d_n \rangle$ by (4.29).

For (3), recall R is a UFD; see (2.17). Say $d_n = p_1^{e_{1n}} \cdots p_m^{e_{mn}}$ with the p_i primes in R, unique up to unit multiple, and the e_{in} unique with $1 \le e_{in}$. Now, $d_j \mid d_{j+1}$ for $1 \le j < n$; so $d_j = p_1^{e_{1j}} \cdots p_m^{e_{mj}}$ for unique e_{ij} and $0 \le e_{ij} \le e_{i\,j+1}$. Finally, $R\big/\langle d_j\rangle = R\big/\langle p_1^{e_{1j}}\rangle \oplus \cdots \oplus R\big/\langle p_m^{e_{mj}}\rangle$ by **(1.21)**(4)(c). Thus (3) holds.

For (4), take $R := \mathbb{Z}$ and $M := \mathbb{Q}$. Then $T = 0$, but $\mathbb{Q}$ isn't free by **(4.11)**. $\square$

Exercise (5.42) . — Criticize the following misstatement of **(5.8)**: given a 3-term exact sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$, there is an isomorphism $M \simeq M' \oplus M''$ if and only if there is a section $\sigma\colon M'' \to M$ of β and α is injective.

Moreover, show that this construction (due to B. Noohi) yields a counterexample: For each integer $n \ge 2$, let M_n be the direct sum of countably many copies of $\mathbb{Z}/\langle n\rangle$. Set $M := \bigoplus M_n$. Then let p be a prime number, and take M' to be a cyclic subgroup of order p of one of the components of M isomorphic to $\mathbb{Z}/\langle p^2\rangle$.

Solution: We have $\alpha\colon M' \to M$, and $\iota_{M'}\colon M' \to M' \oplus M''$, but **(5.8)** requires that they be compatible with the isomorphism $M \simeq M' \oplus M''$, and similarly for $\beta\colon M \to M''$ and $\pi_{M''}\colon M' \oplus M'' \to M''$.

Moreover, for the counterexample, let's first check these two statements:

(1) For any finite abelian group G, we have $G \oplus M \simeq M$.

(2) For any finite subgroup $G \subset M$, we have $M/G \simeq M$.

Statement (1) holds since G is isomorphic to a direct sum of copies of $\mathbb{Z}/\langle n\rangle$ for various n by the structure theorem for finite abelian groups **(5.41)**.

To prove (2), write $M = B \bigoplus M'$, where B contains G and involves only finitely many components of M. Then $M' \simeq M$. Therefore, **(5.22)** and (1) yield

$$M/G \simeq (B/G) \oplus M' \simeq M.$$

Finally, there's no retraction $\mathbb{Z}/\langle p^2\rangle \to M'$; so there is no retraction $M \to M'$ either, since the latter would induce the former. Finally, take $M'' := M/M'$. Then (1) and (2) yield $M \simeq M' \oplus M''$. $\square$

6. Direct Limits

Exercise (6.13) . — (1) Show that the condition **(6.2)**(1) is equivalent to the commutativity of the corresponding diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B, C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B), F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A, C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A), F(C)\big) \end{array} \qquad \textbf{(6.13.1)}$$

(2) Given $\gamma\colon C \to D$, show **(6.2)**(1) yields the commutativity of this diagram:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathcal{C}}(B, C) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(B), F(C)\big) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathcal{C}}(A, D) & \to & \mathrm{Hom}_{\mathcal{C}'}\big(F(A), F(D)\big) \end{array}$$

Solution: In **(6.13.1)**, the left-hand vertical map is given by composition with α, and the right-hand vertical map is given by composition with $F(\alpha)$. So the composition of the top map and the right-hand map sends β to $F(\beta)F(\alpha)$, whereas the composition of the left-hand map with the bottom map sends β to $F(\beta\alpha)$. These two images are always equal if and only if **(6.13.1)** commutes. Thus **(6.2)**(1) is equivalent to the commutativity of (**6.13.1**).

As to (2), the argument is similar. □

Exercise (6.14) . — Let $\mathcal{C}$ and $\mathcal{C}'$ be categories, $F\colon \mathcal{C} \to \mathcal{C}'$ and $F'\colon \mathcal{C}' \to \mathcal{C}$ an adjoint pair. Let $\varphi_{A,A'}\colon \operatorname{Hom}_{\mathcal{C}'}(FA,\, A') \xrightarrow{\sim} \operatorname{Hom}_{\mathcal{C}}(A,\, F'A')$ denote the natural bijection, and set $\eta_A := \varphi_{A,FA}(1_{FA})$. Do the following:

(1) Prove η_A is natural in A; that is, given $g\colon A \to B$, the induced square

$$\begin{array}{ccc} A & \xrightarrow{\eta_A} & F'FA \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle F'Fg} \\ B & \xrightarrow{\eta_B} & F'FB \end{array}$$

is commutative. We call the natural transformation $A \mapsto \eta_A$ the **unit** of $(F,\, F')$.

(2) Given $f'\colon FA \to A'$, prove $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

(3) Prove the canonical map $\eta_A\colon A \to F'FA$ is **universal** from A to F'; that is, given $f\colon A \to F'A'$, there is a unique map $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$.

(4) Conversely, instead of assuming $(F,\, F')$ is an adjoint pair, assume given a natural transformation $\eta\colon 1_{\mathcal{C}} \to F'F$ satisfying (1) and (3). Prove the equation in (2) defines a natural bijection making $(F,\, F')$ an adjoint pair, whose unit is η.

(5) Identify the units in the two examples in (**6.3**): the "free module" functor and the "polynomial ring" functor.

(Dually, we can define a **counit** $\varepsilon\colon FF' \to 1_{\mathcal{C}'}$, and prove similar statements.)

Solution: For (1), form this canonical diagram, with horizontal induced maps:

$$\begin{array}{ccccc} \operatorname{Hom}_{\mathcal{C}'}(FA,\, FA) & \xrightarrow{(Fg)_*} & \operatorname{Hom}_{\mathcal{C}'}(FA,\, FB) & \xleftarrow{(Fg)^*} & \operatorname{Hom}_{\mathcal{C}'}(FB,\, FB) \\ {\scriptstyle \varphi_{A,\,FA}}\downarrow & & {\scriptstyle \varphi_{A,\,FB}}\downarrow & & {\scriptstyle \varphi_{B,\,FB}}\downarrow \\ \operatorname{Hom}_{\mathcal{C}}(A,\, F'FA) & \xrightarrow{(F'Fg)_*} & \operatorname{Hom}_{\mathcal{C}}(A,\, F'FB) & \xleftarrow{g^*} & \operatorname{Hom}_{\mathcal{C}}(B,\, F'FB) \end{array}$$

It commutes since φ is natural. Follow 1_{FA} out of the upper left corner to find $F'Fg \circ \eta_A = \varphi_{A,\,FB}(Fg)$ in $\operatorname{Hom}_{\mathcal{C}}(A,\, F'FB)$. Follow 1_{FB} out of the upper right corner to find $\varphi_{A,\,FB}(Fg) = \eta_B \circ g$ in $\operatorname{Hom}_{\mathcal{C}}(A,\, F'FB)$. Thus $(F'Fg) \circ \eta_A = \eta_B \circ g$.

For (2), form this canonical commutative diagram:

$$\begin{array}{ccc} \operatorname{Hom}_{\mathcal{C}'}(FA,\, FA) & \xrightarrow{f'_*} & \operatorname{Hom}_{\mathcal{C}'}(FA, A') \\ {\scriptstyle \varphi_{A,\,FA}}\downarrow & & {\scriptstyle \varphi_{A,A'}}\downarrow \\ \operatorname{Hom}_{\mathcal{C}}(A,\, F'FA) & \xrightarrow{(F'f')_*} & \operatorname{Hom}_{\mathcal{C}}(A,\, F'A') \end{array}$$

Follow 1_{FA} out of the upper left-hand corner to find $\varphi_{A,A'}(f') = F'f' \circ \eta_A$.

For (3), given an f, note that (2) yields $\varphi_{A,A'}(f') = f$; whence, $f' = \varphi^{-1}_{A,A'}(f)$. Thus f' is unique. Further, an f' exists: just set $f' := \varphi^{-1}_{A,A'}(f)$.

For (4), set $\psi_{A,A'}(f') := F'f' \circ \eta_A$. As η_A is universal, given $f\colon A \to F'A'$, there is a unique $f'\colon FA \to A'$ with $F'f' \circ \eta_A = f$. Thus $\psi_{A,A'}$ is a bijection:

$$\psi_{A,A'}\colon \operatorname{Hom}_{\mathcal{C}'}(FA, A') \xrightarrow{\sim} \operatorname{Hom}_{\mathcal{C}}(A,\, F'A').$$

Also, $\psi_{A,A'}$ is natural in A, as η_A is natural in A and F' is a functor. And, $\psi_{A,A'}$ is natural in A', as F' is a functor. Clearly, $\psi_{A,\,FA}(1_{FA}) = \eta_A$. Thus (4) is done.

For (5), use the notation of (**6.3**). Clearly, if F is the "free module" functor, then $\eta_\Lambda\colon \Lambda \to R^{\oplus\Lambda}$ carries an element of Λ to the corresponding standard basis vector.

Further, if F is the "polynomial ring" functor and if A is the set of variables $\{X_\lambda\}_{\lambda\in\Lambda}$, then $\eta_A(X_\lambda)$ is just X_λ viewed in $R[A]$. □

Exercise (6.15) . — Show that the canonical map $\varphi_F\colon \varinjlim F(M_\lambda) \to F(\varinjlim M_\lambda)$ of (6.4.1) is compatible with any natural transformation $\theta\colon F \to G$.

Solution: Form this diagram, whose left horizontal maps are the insertions:

$$\begin{array}{ccccc} F(M_\kappa) & \to & \varinjlim F(M_\lambda) & \xrightarrow{\varphi_F} & F(\varinjlim M_\lambda) \\ {\scriptstyle \theta(M_\kappa)}\big\downarrow & & {\scriptstyle \varinjlim \theta(M_\lambda)}\big\downarrow & & {\scriptstyle \theta(\varinjlim M_\lambda)}\big\downarrow \\ G(M_\kappa) & \to & \varinjlim G(M_\lambda) & \xrightarrow{\varphi_G} & G(\varinjlim M_\lambda) \end{array}$$

By the construction of φ_F and φ_G in (6.4), the horizontal compositions are equal to the images under F and G of the insertions $M_\kappa \to \varinjlim M_\lambda$. But θ is a natural transformation. So the outer rectangle is commutative. So the left square remains commutative when $\varinjlim \theta(M_\lambda)$ is replaced by $\varphi_G^{-1}\theta(\varinjlim M_\lambda)\varphi_F$. Hence, those two maps are equal by uniqueness. Thus the right square is commutative, as desired. □

Exercise (6.16) . — Let $\alpha\colon L \to M$ and $\beta\colon L \to N$ be two maps in a category $\mathcal{C}$. Their **pushout** is defined as the object of $\mathcal{C}$ universal among objects P equipped with a pair of maps $\gamma\colon M \to P$ and $\delta\colon N \to P$ such that $\gamma\alpha = \delta\beta$. Express the pushout as a direct limit. Show that, in ((Sets)), the pushout is the disjoint union $M \sqcup N$ modulo the smallest equivalence relation $\sim$ with $m \sim n$ if there is $\ell \in L$ with $\alpha(\ell) = m$ and $\beta(\ell) = n$. Show that, in ((R-mod)), the pushout is equal to the direct sum $M \oplus N$ modulo the image of L under the map $(\alpha, -\beta)$.

Solution: Let Λ be the category with three objects λ, μ, and ν and two nonidentity maps $\lambda \to \mu$ and $\lambda \to \nu$. Define a functor $\lambda \mapsto M_\lambda$ by $M_\lambda := L$, $M_\mu := M$, $M_\nu := N$, $\alpha^\lambda_\mu := \alpha$, and $\alpha^\lambda_\nu := \beta$. Set $Q := \varinjlim M_\lambda$. Then writing

$$\begin{array}{ccccc} N & \xleftarrow{\beta} & L & \xrightarrow{\alpha} & M \\ {\scriptstyle \eta_\nu}\big\downarrow & & {\scriptstyle \eta_\lambda}\big\downarrow & & {\scriptstyle \eta_\mu}\big\downarrow \\ Q & \xleftarrow{1_R} & Q & \xrightarrow{1_R} & Q \end{array} \qquad \text{as} \qquad \begin{array}{ccc} L & \xrightarrow{\alpha} & M \\ {\scriptstyle \beta}\big\downarrow & & {\scriptstyle \eta_\mu}\big\downarrow \\ N & \xrightarrow{\eta_\nu} & Q \end{array}$$

we see that Q is equal to the pushout of α and β; here $\gamma = \eta_\mu$ and $\delta = \eta_\nu$.

In ((Sets)), take γ and δ to be the inclusions followed by the quotient map. Clearly $\gamma\alpha = \delta\beta$. Further, given P and maps $\gamma'\colon M \to P$ and $\delta'\colon N \to P$, they define a unique map $M \sqcup N \to P$, and it factors through the quotient if and only if $\gamma'\alpha = \delta'\beta$. Thus $(M \sqcup N)/\sim$ is the pushout.

In ((R-mod)), take γ and δ to be the inclusions followed by the quotient map. Then for all $\ell \in L$, clearly $\iota_M\alpha(\ell) - \iota_N\beta(\ell) = (\alpha(\ell), -\beta(\ell))$. Hence $\iota_M\alpha(\ell) - \iota_N\beta(\ell)$ is in $\mathrm{Im}(L)$. Hence, $\iota_M\alpha(\ell)$ and $\iota_N\beta(\ell)$ have the same image in the quotient. Thus $\gamma\alpha = \delta\beta$. Given $\gamma'\colon M \to P$ and $\delta'\colon N \to P$, they define a unique map $M \oplus N \to P$, and it factors through the quotient if and only if $\gamma'\alpha = \delta'\beta$. Thus $(M \oplus N)/\,\mathrm{Im}(L)$ is the pushout. □

Exercise (6.17) . — Let R be a ring, M a module, N a submodule, $\mathcal{X}$ a set of variables. Prove $M \mapsto M[X]$ is the left adjoint of the restriction of scalars from $R[\mathcal{X}]$ to R. As a consequence, reprove the equation $(M/N)[\mathcal{X}] = M[\mathcal{X}]/N[\mathcal{X}]$.

Solution: First, (**4.18**)(1) yields, for any $R[\mathcal{X}]$-module P, a bijection

$$\varphi_{M,P}\colon \operatorname{Hom}_{R[\mathcal{X}]}(M[\mathcal{X}],\, P) \xrightarrow{\sim} \operatorname{Hom}_R(M,P) \quad \text{with} \quad \varphi_{M,P}(\beta) := \beta|M.$$

Plainly, $\varphi_{M,P}$ is natural in M and P. Thus the first assertion holds.

Next, recall a quotient is a direct limit; see (**6.6**). But every left adjoint preseves direct limits by (**6.9**). Thus the first assertion yields the desired equation. $\square$

Exercise (6.18) . — Let $\mathcal{C}$ be a category, Σ and Λ small categories. Prove:

(1) Then $\mathcal{C}^{\Sigma\times\Lambda} = (\mathcal{C}^{\Lambda})^{\Sigma}$ with $(\sigma,\lambda) \mapsto M_{\sigma,\lambda}$ corresponding to $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$.

(2) Assume $\mathcal{C}$ has direct limits indexed by Σ and by Λ. Then $\mathcal{C}$ has direct limits indexed by $\Sigma \times \Lambda$, and $\varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma} = \varinjlim_{(\sigma,\lambda)\in\Sigma\times\Lambda}$.

Solution: Consider (1). In $\Sigma\times\Lambda$, a map $(\sigma,\lambda) \to (\tau,\mu)$ factors in two ways:

$$(\sigma,\lambda) \to (\tau,\lambda) \to (\tau,\mu) \quad \text{and} \quad (\sigma,\lambda) \to (\sigma,\mu) \to (\tau,\mu).$$

So, given a functor $(\sigma,\lambda) \mapsto M_{\sigma,\lambda}$, there is a commutative diagram like (**6.10.1**). It shows that the map $\sigma \to \tau$ in Σ induces a natural transformation from $\lambda \mapsto M_{\sigma,\lambda}$ to $\lambda \mapsto M_{\tau,\lambda}$. Thus the rule $\sigma \mapsto (\lambda \mapsto M_{\sigma\lambda})$ is a functor from Σ to $\mathcal{C}^{\Lambda}$.

A map from $(\sigma,\lambda) \mapsto M_{\sigma,\lambda}$ to a second functor $(\sigma,\lambda) \mapsto N_{\sigma,\lambda}$ is a collection of maps $\theta_{\sigma,\lambda}\colon M_{\sigma,\lambda} \to N_{\sigma,\lambda}$ such that, for every map $(\sigma,\lambda) \to (\tau,\mu)$, the square

$$\begin{array}{ccc} M_{\sigma\lambda} & \longrightarrow & M_{\tau\mu} \\ {\scriptstyle \theta_{\sigma,\lambda}}\big\downarrow & & \big\downarrow{\scriptstyle \theta_{\tau,\mu}} \\ N_{\sigma\lambda} & \longrightarrow & N_{\tau\mu} \end{array}$$

is commutative. Factoring $(\sigma,\lambda) \to (\tau,\mu)$ in two ways as above, we get a commutative cube. It shows that the $\theta_{\sigma,\lambda}$ define a map in $(\mathcal{C}^{\Lambda})^{\Sigma}$.

This passage from $\mathcal{C}^{\Sigma\times\Lambda}$ to $(\mathcal{C}^{\Lambda})^{\Sigma}$ is reversible. Thus (1) holdes.

As to (2), assume $\mathcal{C}$ has direct limits indexed by Σ and Λ. Then $\mathcal{C}^{\Lambda}$ has direct limits indexed by Σ by (**6.10**). So the functors $\varinjlim_{\lambda\in\Lambda}\colon \mathcal{C}^{\Lambda} \to \mathcal{C}$ and $\varinjlim_{\sigma\in\Sigma}\colon (\mathcal{C}^{\Lambda})^{\Sigma} \to \mathcal{C}^{\Lambda}$ exist, and they are the left adjoints of the diagonal functors $\mathcal{C} \to \mathcal{C}^{\Lambda}$ and $\mathcal{C}^{\Lambda} \to (\mathcal{C}^{\Lambda})^{\Sigma}$ by (**6.4**). Hence the composition $\varinjlim_{\lambda\in\Lambda} \varinjlim_{\sigma\in\Sigma}$ is the left adjoint of the composition of the two diagonal functors. But the latter is just the diagonal $\mathcal{C} \to \mathcal{C}^{\Sigma\times\Lambda}$ owing to (1). So this diagonal has a left adjoint, which is necessarily $\varinjlim_{(\sigma,\lambda)\in\Sigma\times\Lambda}$ by the uniqueness of adjoints. Thus (2) holds. $\square$

Exercise (6.19) . — Let $\lambda \mapsto M_\lambda$ and $\lambda \mapsto N_\lambda$ be two functors from a small category Λ to $((R\text{-mod}))$, and $\{\theta_\lambda\colon M_\lambda \to N_\lambda\}$ a natural transformation. Show

$$\varinjlim \operatorname{Coker}(\theta_\lambda) = \operatorname{Coker}(\varinjlim M_\lambda \to \varinjlim N_\lambda).$$

Show that the analogous statement for kernels can be false by constructing a counterexample using the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} \mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/\langle 2\rangle & \longrightarrow & 0 \\ \big\downarrow{\scriptstyle \mu_2} & & \big\downarrow{\scriptstyle \mu_2} & & \big\downarrow{\scriptstyle \mu_2} & & \\ \mathbb{Z} & \xrightarrow{\mu_2} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/\langle 2\rangle & \longrightarrow & 0 \end{array}$$

Solution: By (**6.6**), the cokernel is a direct limit, and by (**6.11**), direct limits commute; thus, the asserted equation holds.

To construct the desired counterexample using the given diagram, view its rows as expressing the cokernel $\mathbb{Z}/\langle 2\rangle$ as a direct limit over the category Λ of (**6.6**). View the left two columns as expressing a natural transformation $\{\theta_\lambda\}$, and view the third column as expressing the induced map between the two limits. The latter map is 0; so its kernel is $\mathbb{Z}/\langle 2\rangle$. However, $\mathrm{Ker}(\theta_\lambda) = 0$ for $\lambda \in \Lambda$; so $\varinjlim \mathrm{Ker}(\theta_\lambda) = 0$. □

Exercise (6.20) . — Let R be a ring, M a module. Define the map

$$D(M)\colon M \to \mathrm{Hom}\big(\mathrm{Hom}(M,\, R),\, R\big) \quad \text{by} \quad \big(D(M)(m)\big)(\alpha) := \alpha(m).$$

If $D(M)$ is an isomorphism, call M **reflexive**. Show:

(1) $D : 1_{((R\text{-mod}))} \to \mathrm{Hom}\big(\mathrm{Hom}(\bullet,\, R),\, R\big)$ is a natural transformation.
(2) Let M_i for $1 \le i \le n$ be modules. Then $D(\bigoplus_{i=1}^n M_i) = \bigoplus_{i=1}^n D(M_i)$.
(3) Assume M is finitely generated and projective. Then M is reflexive.

Solution: For (1), given an R-map $\beta\colon M \to N$, note that the induced diagram

$$\begin{tikzcd} M \arrow[r, "D(M)"] \arrow[d, "\beta"'] & \mathrm{Hom}\big(\mathrm{Hom}(M,\, R),\, R\big) \arrow[d, "\beta_*"] \\ N \arrow[r, "D(N)"] & \mathrm{Hom}\big(\mathrm{Hom}(N,\, R),\, R\big) \end{tikzcd}$$

commutes, as $\big(D(N)\beta(m)\big)(\gamma) = \gamma(\beta(m)) = \big(\beta_*(D(M)(m))\big)(\gamma)$ where $m \in M$ and $\gamma \in \mathrm{Hom}(N,\, R)$. Thus (1) holds.

For (2), form the following diagram:

$$\begin{tikzcd} \bigoplus_{i=1}^n M_i \arrow[r, equal] \arrow[d, "\bigoplus_{i=1}^n D(M_i)"] & \bigoplus_{i=1}^n M_i \arrow[d, "D(\bigoplus_{i=1}^n M_i)"] \\ \bigoplus_{i=1}^n \mathrm{Hom}\big(\mathrm{Hom}(M_i,\, R),\, R\big) \arrow[r] & \mathrm{Hom}\big(\mathrm{Hom}(\bigoplus_{i=1}^n M_i,\, R),\, R\big) \end{tikzcd}$$

The bottom map is an isomorphism by (**4.13.2**) applied twice. Thus (1) and (**6.15**), applied with $\theta := D$ and $\varinjlim := \bigoplus$, yield (2).

For (3), note $D(R)$ is an isomorphism owing to (**4.3**). But plainly, a direct sum of isomorphisms is an isomorphism (and conversely). Thus (2) implies that $D(F)$ is an isomorphism for any free module F of finite rank.

By (**4.10**), there is a surjection $\rho\colon F \to M$ where F is free of finite rank. Set $K := \mathrm{Ker}(\rho)$. Then $F = K \oplus M$ by (**5.16**)(1)⇒(2). Since $D(F)$ is an isomorphism, $D(M)$ is an isomorphism, again owing to (2). Thus (3) holds. □

7. Filtered direct limits

Exercise (7.2) . — Let R be a ring, M a module, Λ a set, M_λ a submodule for each $\lambda \in \Lambda$. Assume $\bigcup M_\lambda = M$. Assume, given λ, $\mu \in \Lambda$, there is $\nu \in \Lambda$ such that M_λ, $M_\mu \subset M_\nu$. Order Λ by inclusion: $\lambda \le \mu$ if $M_\lambda \subset M_\mu$. Prove $M = \varinjlim M_\lambda$.

Solution: Let us prove that M has the UMP characterizing $\varinjlim M_\lambda$. Given homomorphisms $\beta_\lambda \colon M_\lambda \to P$ with $\beta_\lambda = \beta_\nu|M_\lambda$ when $\lambda \le \nu$, define $\beta\colon M \to P$ by $\beta(m) := \beta_\lambda(m)$ if $m \in M_\lambda$. Such a λ exists as $\bigcup M_\lambda = M$. If also $m \in M_\mu$ and M_λ, $M_\mu \subset M_\nu$, then $\beta_\lambda(m) = \beta_\nu(m) = \beta_\mu(m)$; so β is well defined. Clearly, $\beta\colon M \to P$ is the unique set map such that $\beta|M_\lambda = \beta_\lambda$. Further, given $m, n \in M$ and $x \in R$, there is ν such that $m, n \in M_\nu$. So $\beta(m+n) = \beta_\nu(m+n) = \beta(m)+\beta(n)$ and $\beta(xm) = \beta_\nu(xm) = x\beta(m)$. Thus β is R-linear. Thus $M = \varinjlim M_\lambda$. □

Exercise (7.11) . — Show that every module M is the filtered direct limit of its finitely generated submodules.

Solution: Every element $m \in M$ belongs to the submodule generated by m; hence, M is the union of all its finitely generated submodules. Any two finitely generated submodules are contained in a third, for example, their sum. So the assertion results from (7.2) with Λ the set of all finite subsets of M. □

Exercise (7.12) . — Show that every direct sum of modules is the filtered direct limit of its finite direct subsums.

Solution: Consider an element of the direct sum. It has only finitely many nonzero components. So it lies in the corresponding finite direct subsum. Thus the union of the subsums is the whole direct sum. Now, given any two finite direct subsums, their sum is a third. Thus the finite subsets of indices form a directed partially ordered set Λ. So the assertion results from (7.2). □

Exercise (7.13) . — Keep the setup of (7.3). For each $n \in \Lambda$, set $N_n := \mathbb{Z}/\langle n\rangle$; if $n = ms$, define $\alpha_n^m \colon N_m \to N_n$ by $\alpha_n^m(x) := xs \pmod{n}$. Show $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$.

Solution: For each $n \in \Lambda$, set $Q_n := M_n/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$. If $n = ms$, then clearly Diagram (7.3.1) induces this one:

$$\begin{tikzcd} N_m \arrow[r, "\alpha_n^m"] \arrow[d, "\gamma_m"', "\simeq"] & N_n \arrow[d, "\gamma_n"', "\simeq"] \\ Q_m \arrow[r, hook, "\eta_n^m"] & Q_n \end{tikzcd}$$

where η_n^m is the inclusion. Now, $\bigcup Q_n = \mathbb{Q}/\mathbb{Z}$ and Q_n, $Q_{n'} \subset Q_{nn'}$. So (7.2) yields $\mathbb{Q}/\mathbb{Z} = \varinjlim Q_n$. Thus $\varinjlim N_n = \mathbb{Q}/\mathbb{Z}$. □

Exercise (7.14) . — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha_\mu^\lambda \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$.

(1) Prove that all α_λ are injective if and only if all α_μ^λ are. What if $\varinjlim M_\lambda$ isn't filtered?
(2) Assume that all α_λ are injective. Prove $M = \bigcup \alpha_\lambda M_\lambda$.

Solution: For (1), recall that $\alpha_\mu\alpha^\lambda_\mu = \alpha_\lambda$. So if α_λ is injective, then so is α^λ_μ, whether $\varinjlim M_\lambda$ is filtered, or not.

Conversely, suppose all α^λ_μ are injective. Given $m_\lambda \in M_\lambda$ with $\alpha_\lambda m_\lambda = 0$, there's α^λ_μ with $\alpha^\lambda_\mu m_\lambda = 0$ by **(7.5)**(3). So $m_\lambda = 0$. Thus α_λ is injective.

However, if $M := \varinjlim M_\lambda$ isn't filtered, then all α_λ aren't necessarily injective. For example, take any module M_1 with $2M_1 \neq 0$, and set $M_2 := M_1 \oplus M_1$. Define $\alpha,\ \alpha' \colon M_1 \rightrightarrows M_2$ by $\alpha(m) := (m, m)$ and $\alpha'(m) := (m, -m)$. Then α and α' are injective. But $M = \operatorname{Coker}(\alpha - \alpha')$, and $\alpha_2 \colon M_2 \to M$ is the quotient map by **(6.6)**. Also, $\operatorname{Im}(\alpha - \alpha') = 0 \oplus 2M_1 \neq 0$. Thus α_2 isn't injective.

For (2), note each $\alpha^\lambda_\mu \colon M_\lambda \to M_\mu$ corresponds to an inclusion $\alpha_\lambda M_\lambda \hookrightarrow \alpha_\mu M_\mu$. So $M = \varinjlim \alpha_\lambda M_\lambda$. Moreover, given λ, μ, there's ν with $\alpha_\lambda M_\lambda,\ \alpha_\mu M_\mu \subset \alpha_\nu M_\nu$ owing to **(7.1)**(1). Thus **(7.2)** yields $M = \bigcup \alpha_\lambda M_\lambda$. □

Exercise (7.15) . — Let R be a ring, $\mathfrak{a}$ a finitely generated ideal, M a module. Show $\Gamma_{\mathfrak{a}}(M) = \varinjlim \operatorname{Hom}(R/\mathfrak{a}^n,\ M)$.

Solution: Define a map $\operatorname{Hom}(R/\mathfrak{a}^n,\ M) \to \{\, m \in M \mid \mathfrak{a}^n m = 0 \,\}$ by sending α to $\alpha(1)$. Plainly it's a (canonical) isomorphism. Thus **(7.2)** and **(4.14)**(5) yield

$$\varinjlim \operatorname{Hom}(R/\mathfrak{a}^n,\ M) = \textstyle\bigcup_{n\geq 1}\{\, m \in M \mid \mathfrak{a}^n m = 0 \,\} = \Gamma_{\mathfrak{a}}(M). \qquad \square$$

Exercise (7.16) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Show:

(1) Then $R = 0$ if and only if $R_\lambda = 0$ for some λ.
(2) Assune each R_λ is a domain. Then R is a domain.
(3) Assume each R_λ is a field. Then each insertion $\alpha_\lambda \colon R_\lambda \to R$ is injective, $R = \bigcup \alpha_\lambda R_\lambda$, and R is a field.

Solution: For (1), first assume $R = 0$. Fix any κ. Then $1 \in R_\kappa$ maps to $0 \in R$. So **(7.5)**(3) with $\mathbb{Z}$ for R yields some transition map $\alpha^\kappa_\lambda \colon R_\kappa \to R_\lambda$ with $\alpha^\kappa_\lambda 1 = 0$. But $\alpha^\kappa_\lambda 1 = 1$. Thus $1 = 0$ in R_λ. Thus $R_\lambda = 0$ by **(1.1)**.

Conversely, assume $R_\lambda = 0$. Then $1 = 0$ in R_λ. So $1 = 0$ in R, as the transition map $\alpha_\lambda \colon R_\lambda \to R$ carries 1 to 1 and 0 to 0. Thus $R = 0$ by **(1.1)**. Thus (1) holds.

In (2), given $x,\ y \in R$ with $xy = 0$, we can lift $x,\ y$ back to some $x_\lambda,\ y_\lambda \in R_\lambda$ for some λ by **(7.5)**(1) and **(7.1)**(1). Then $x_\lambda y_\lambda$ maps to $0 \in R$. So **(7.5)**(3) yields a transition map α^λ_μ with $\alpha^\lambda_\mu(x_\lambda y_\lambda) = 0$ in R_μ. But $\alpha^\lambda_\mu(x_\lambda y_\lambda) = \alpha^\lambda_\mu(x_\lambda)\alpha^\lambda_\mu(y_\lambda)$, and R_μ is a domain. So either $\alpha^\lambda_\mu(x_\lambda) = 0$ or $\alpha^\lambda_\mu(y_\lambda) = 0$. Hence, either $x = 0$ or $y = 0$. Thus R is a domain. Thus (2) holds.

In (3), each $\alpha_\lambda \colon R_\lambda \to R$ is injective as each R_λ is a field. So $R = \bigcup \alpha_\lambda R_\lambda$ by **(7.14)**. Finally, given $x \in R - 0$, say $x \in \alpha_\lambda R_\lambda$. As R_λ is a field, there's $y \in \alpha_\lambda R_\lambda$ with $xy = 1$. So R is a field. Thus (3) holds. □

Exercise (7.17) . — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha^\lambda_\mu \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$. For each λ, let $N_\lambda \subset M_\lambda$ be a submodule, and let $N \subset M$ be a submodule. Prove that $N_\lambda = \alpha_\lambda^{-1} N$ for all λ if and only if (a) $N_\lambda = (\alpha^\lambda_\mu)^{-1} N_\mu$ for all α^λ_μ and (b) $\bigcup \alpha_\lambda N_\lambda = N$.

Solution: First, assume $N_\lambda = \alpha_\lambda^{-1} N$ for all λ. Recall $\alpha_\lambda = \alpha_\mu \alpha^\lambda_\mu$ for all α^λ_μ. So $\alpha_\lambda^{-1} N (\alpha^\lambda_\mu)^{-1} \alpha_\mu^{-1} N$. Thus (a) holds.

Further, $N_\lambda = \alpha_\lambda^{-1} N$ implies $\alpha_\lambda N_\lambda \subset N$. So $\bigcup \alpha_\lambda N_\lambda \subset N$. Finally, for any $m \in M$, there is λ and $m_\lambda \in M_\lambda$ with $m = \alpha_\lambda m_\lambda$ by **(7.5)**(1). But $N_\lambda := \alpha_\lambda^{-1} N$; hence, if $m \in N$, then $m_\lambda \in N_\lambda$, so $m \in \alpha_\lambda N_\lambda$. Thus (b) holds too.

Conversely, assume (b). Then $\alpha_\lambda N_\lambda \subset N$, or $N_\lambda \subset \alpha_\lambda^{-1} N$, for all λ.

Assume (a) too. Given λ and $m_\lambda \in \alpha_\lambda^{-1} N$, note $\alpha_\lambda m_\lambda \in N = \bigcup \alpha_\mu N_\mu$. So there is μ and $n_\mu \in N_\mu$ with $\alpha_\mu n_\mu = \alpha_\lambda m_\lambda$. So (**7.5**)(2) yields ν and α^μ_ν and α^λ_ν with $\alpha^\mu_\nu n_\mu = \alpha^\lambda_\nu m_\lambda$. But $\alpha^\mu_\nu N_\mu \subset N_\nu$ and $(\alpha^\lambda_\nu)^{-1} N_\nu = N_\lambda$ by (a). Hence $m_\lambda \in N_\lambda$. Thus $N_\lambda \supset \alpha_\lambda^{-1} N$. Thus $N_\lambda \alpha_\lambda^{-1} N$, as desired. □

Exercise (7.18) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings, $\mathfrak{a}_\lambda \subset R_\lambda$ an ideal for each λ. Assume $\alpha^\lambda_\mu \mathfrak{a}_\lambda \subset \mathfrak{a}_\mu$ for each transition map α^λ_μ. Set $\mathfrak{a} := \varinjlim \mathfrak{a}_\lambda$. If each $\mathfrak{a}_\lambda$ is prime, show $\mathfrak{a}$ is prime. If each $\mathfrak{a}_\lambda$ is maximal, show $\mathfrak{a}$ is maximal.

Solution: The functor $\lambda \mapsto \mathfrak{a}_\lambda$ induces functors $\lambda \mapsto \mathfrak{a}_\lambda$ and $\lambda \mapsto (R_\lambda/\mathfrak{a}_\lambda)$. So (**7.4**) implies that $\mathfrak{a} := \varinjlim \mathfrak{a}_\lambda$ and $\varinjlim (R_\lambda/\mathfrak{a}_\lambda)$ exist, and (**7.9**) implies that $\varinjlim (R_\lambda/\mathfrak{a}_\lambda) = R/\mathfrak{a}$. Thus (**7.16**) yields the assertions. □

Exercise (7.19) . — Let $M := \varinjlim M_\lambda$ be a filtered direct limit of modules, with transition maps $\alpha^\lambda_\mu \colon M_\lambda \to M_\mu$ and insertions $\alpha_\lambda \colon M_\lambda \to M$. Let $N_\lambda \subset M_\lambda$ be a be a submodule for all λ. Assume $\alpha^\lambda_\mu N_\lambda \subset N_\mu$ for all α^λ_μ. Prove $\varinjlim N_\lambda = \bigcup \alpha_\lambda N_\lambda$.

Solution: The functor $\lambda \mapsto M_\lambda$ induces a functor $\lambda \mapsto N_\lambda$. So $\varinjlim N_\lambda$ exists by (**7.4**). Also, by (**7.9**), the inclusions $N_\lambda \hookrightarrow M_\lambda$ induce an injection $\varinjlim N_\lambda \hookrightarrow M$ such that the insertions $\alpha_\lambda \colon M_\lambda \to M$ restrict to the insertions $N_\lambda \to \varinjlim N_\lambda$. Hence $\varinjlim N_\lambda \supset \bigcup \alpha_\lambda N_\lambda$. Finally, let $n \in \varinjlim N_\lambda$. Then (**7.5**)(1) yields a λ and a $m_\lambda \in N_\lambda$ with $n = \alpha_\lambda m_\lambda \in \alpha_\lambda N_\lambda$. Thus $\varinjlim N_\lambda = \bigcup \alpha_\lambda N_\lambda$. □

Exercise (7.20) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Prove that

$$\varinjlim \operatorname{nil}(R_\lambda) = \operatorname{nil}(R).$$

Solution: Set $\mathfrak{n}_\lambda := \operatorname{nil}(R_\lambda)$ and $\mathfrak{n} := \operatorname{nil}(R)$. As usual, denote the transition maps by $\alpha^\lambda_\mu \colon R_\lambda \to R_\mu$ and the insertions by $\alpha_\lambda \colon R_\lambda \to R$. Then $\alpha^\lambda_\mu \mathfrak{n}_\lambda \subset \mathfrak{n}_\mu$ for all α^λ_μ. So (**7.19**) yields $\varinjlim \mathfrak{n}_\lambda = \bigcup \alpha_\lambda \mathfrak{n}_\lambda$. Now, $\alpha_\lambda \mathfrak{n}_\lambda \subset \mathfrak{n}$ for all λ. So $\bigcup \alpha_\lambda \mathfrak{n}_\lambda \subset \mathfrak{n}$.

Conversely, given $x \in \mathfrak{n}$, say $x^n = 0$. Then (**7.5**)(1) yields λ and $x_\lambda \in R_\lambda$ with $\alpha_\lambda x_\lambda = x$. So $\alpha_\lambda x_\lambda^n = 0$. So (**7.5**)(3) yields α^λ_μ with $\alpha^\lambda_\mu x_\lambda^n = 0$. Set $x_\mu := \alpha^\lambda_\mu x_\lambda$. Then $x_\mu^n = 0$. So $x_\mu \in \mathfrak{n}_\mu$. Thus $x \in \alpha_\mu \mathfrak{n}_\mu$. Thus $\bigcup \alpha_\lambda \mathfrak{n}_\lambda = \mathfrak{n}$, as desired. □

Exercise (7.21) . — Let $R := \varinjlim R_\lambda$ be a filtered direct limit of rings. Assume each ring R_λ is local, say with maximal ideal $\mathfrak{m}_\lambda$, and assume each transition map $\alpha^\lambda_\mu \colon R_\lambda \to R_\mu$ is local. Set $\mathfrak{m} := \varinjlim \mathfrak{m}_\lambda$. Prove that R is local with maximal ideal $\mathfrak{m}$ and that each insertion $\alpha_\lambda \colon R_\lambda \to R$ is local.

Solution: As each α^λ_μ is local, $(\alpha^\lambda_\mu)^{-1}\mathfrak{m}_\lambda = \mathfrak{m}_\mu$. So $\alpha^\lambda_\mu \mathfrak{m}_\lambda \subset \mathfrak{m}_\mu$. So (**7.19**) yields $\mathfrak{m} = \bigcup \alpha_\lambda \mathfrak{m}_\lambda$. Now, given $x \in R - \mathfrak{m}$, there is λ and $x_\lambda \in R_\lambda$ with $\alpha_\lambda x_\lambda = x$ by (**7.5**)(1). Then $x_\lambda \notin \mathfrak{m}_\lambda$ as $x \notin \mathfrak{m} = \bigcup \alpha_\lambda \mathfrak{m}_\lambda$. So x_λ is invertible as R_λ is local with maximal ideal $\mathfrak{m}_\lambda$. Hence x is invertible. Thus R is local with maximal ideal $\mathfrak{m}$ by (**3.4**). Finally, (**7.17**) yields $\alpha_\lambda^{-1}\mathfrak{m} = \mathfrak{m}_\lambda$; that is, α_λ is local. □

Exercise (7.22) . — Let Λ and Λ' be small categories, $C \colon \Lambda' \to \Lambda$ a functor. Assume Λ' is filtered. Assume C is **cofinal**; that is,

(1) given $\lambda \in \Lambda$, there is a map $\lambda \to C\lambda'$ for some $\lambda' \in \Lambda'$, and
(2) given $\psi, \varphi \colon \lambda \rightrightarrows C\lambda'$, there is $\chi \colon \lambda' \to \lambda'_1$ with $(C\chi)\psi = (C\chi)\varphi$.

Let $\lambda \mapsto M_\lambda$ be a functor from Λ to $\mathcal{C}$ whose direct limit exists. Show that

$$\varinjlim_{\lambda' \in \Lambda'} M_{C\lambda'} = \varinjlim_{\lambda \in \Lambda} M_\lambda;$$

more precisely, show that the right side has the UMP characterizing the left.

Solution: Let P be an object of $\mathcal{C}$. For $\lambda' \in \Lambda'$, take maps $\gamma_{\lambda'}\colon M_{C\lambda'} \to P$ compatible with the transition maps $M_{C\lambda'} \to M_{C\mu'}$. Given $\lambda \in \Lambda$, choose a map $\lambda \to C\lambda'$, and define $\beta_\lambda\colon M_\lambda \to P$ to be the composition

$$\beta_\lambda\colon M_\lambda \longrightarrow M_{C\lambda'} \xrightarrow{\gamma_{\lambda'}} P.$$

Let's check that β_λ is independent of the choice of $\lambda \to C\lambda'$.

Given a second choice $\lambda \to C\lambda''$, there are maps $\lambda'' \to \mu'$ and $\lambda' \to \mu'$ for some $\mu' \in \Lambda'$ since Λ' is filtered. So there is a map $\mu' \to \mu'_1$ such that the compositions $\lambda \to C\lambda' \to C\mu' \to C\mu'_1$ and $\lambda \to C\lambda'' \to C\mu' \to C\mu'_1$ are equal since C is cofinal. Therefore, $\lambda \to C\lambda''$ gives rise to the same β_λ, as desired.

Clearly, the β_λ are compatible with the transition maps $M_\kappa \to M_\lambda$. So the β_λ induce a map $\beta\colon \varinjlim M_\lambda \to P$ with $\beta\alpha_\lambda = \beta_\lambda$ for every insertion $\alpha_\lambda\colon M_\lambda \to \varinjlim M_\lambda$. In particular, this equation holds when $\lambda = C\lambda'$ for any $\lambda' \in \Lambda'$, as required. □

Exercise (7.23) . — Show that every R-module M is the filtered direct limit over a directed set of finitely presented modules.

Solution: By (5.13), there is a presentation $R^{\oplus\Phi_1} \xrightarrow{\alpha} R^{\oplus\Phi_2} \to M \to 0$. For $i = 1, 2$, let Λ_i be the set of finite subsets Ψ_i of Φ_i, and order Λ_i by inclusion. Clearly, an inclusion $\Psi_i \hookrightarrow \Phi_i$ yields an injection $R^{\oplus\Psi_i} \hookrightarrow R^{\oplus\Phi_i}$, which is given by extending vectors by 0. Hence (7.2) yields $\varinjlim R^{\oplus\Psi_i} = R^{\oplus\Phi_i}$.

Let $\Lambda \subset \Lambda_1 \times \Lambda_2$ be the set of pairs $\lambda := (\Psi_1, \Psi_2)$ such that α induces a map $\alpha_\lambda\colon R^{\oplus\Psi_1} \to R^{\oplus\Psi_2}$. Order Λ by componentwise inclusion. Clearly, Λ is directed. For $\lambda \in \Lambda$, set $M_\lambda := \operatorname{Coker}(\alpha_\lambda)$. Then M_λ is finitely presented.

For $i = 1, 2$, the projection $C_i\colon \Lambda \to \Lambda_i$ is surjective, so cofinal. Hence, (7.22) yields $\varinjlim_{\lambda \in \Lambda} R^{\oplus C_i\lambda} = \varinjlim_{\Psi_i \in \Lambda_i} R^{\oplus\Psi_i}$. Thus (6.19) yields $\varinjlim M_\lambda = M$. □

8. Tensor Products

Exercise (8.7) . — Let R be a ring, R' an R-algebra, and M, N two R'-modules.

(1) Show that there is a canonical R-linear map $\tau\colon M \otimes_R N \to M \otimes_{R'} N$.

(2) Let $K \subset M \otimes_R N$ denote the R-submodule generated by all the differences $(x'm) \otimes n - m \otimes (x'n)$ for $x' \in R'$ and $m \in M$ and $n \in N$. Show that $K = \operatorname{Ker}(\tau)$ and that τ is surjective.

(3) Suppose that R' is a quotient of R. Show that τ is an isomorphism.

(4) Let $\{t_\tau\}$ be a set of algebra generators of R' over R. Let $\{m_\mu\}$ and $\{n_\nu\}$ be sets of generators of M and N over R'. Regard $M \otimes_R N$ as an $(R' \otimes_R R')$-module. Let K' denote the $(R' \otimes_R R')$-submodule generated by all differences $(t_\tau m_\mu) \otimes n_\nu - m_\mu \otimes (t_\tau n_\nu)$. Show that $K' = K$.

Solution: For (1), form the canonical map $\beta'\colon M \times N \to M \otimes_{R'} N$. It is R'-bilinear, so R-bilinear. Hence, (8.3) yields $\beta' = \tau\beta$ where $\beta\colon M \times N \to M \otimes_R N$ is the canonical map and τ is the desired map, as desired.

For (2), note that each generator $(x'm) \otimes n - m \otimes (x'n)$ of K maps to 0 in $M \otimes_{R'} N$. Set $Q := (M \otimes_R N)/K$. Then τ factors through a map $\tau'\colon Q \to M \otimes_{R'} N$.

By (**8.6**), there is an R'-structure on $M \otimes_R N$ with $y'(m \otimes n) = m \otimes (y'n)$, and so by (**8.5**)(1), another one with $y'(m \otimes n) = (y'm) \otimes n$. Clearly, K is a submodule for each structure, so Q is too. But on Q the two structures coincide. Further, the canonical map $M \times N \to Q$ is R'-bilinear. Hence the latter factors through $M \otimes_{R'} N$, furnishing an inverse to τ'. So $\tau' \colon Q \xrightarrow{\sim} M \otimes_{R'} N$. Hence $\mathrm{Ker}(\tau)$ is equal to K, and τ is surjective, as desired.

In (3), each $x' \in R'$ is the residue of some $x \in R$. So each $(x'm) \otimes n - m \otimes (x'n)$ is 0 in $M \otimes_R N$, as $x'm = xm$ and $x'n = xn$. Thus $\mathrm{Ker}(\tau) = 0$, so (2) yields (3).

In (4), trivially $K' \subset K$. Given any t_τ, $t_{i'}$ and m_μ, n_ν, note that

$$(t_\tau t_{i'} m_\mu) \otimes n_\nu - m_\mu \otimes (t_\tau t_{i'} n_\nu) = (t_\tau \otimes 1)\big((t_{i'} m_\mu) \otimes n_\nu - m_\mu \otimes (t_{i'} n_\nu)\big) \\ + (1 \otimes t_{i'})\big((t_\tau m_\mu) \otimes n_\nu - m_\mu \otimes (t_\tau n_\nu)\big) \in K'.$$

Hence given any monomial $\mathbf{M}_\alpha$ in the t_τ, it follows via induction on $\deg(\mathbf{M}_\alpha)$ that $(\mathbf{M}_\alpha m_\mu) \otimes n_\nu - m_\mu \otimes (\mathbf{M}_\alpha n_\nu) \in K'$.

Given any $x' = \sum x_\alpha \mathbf{M}_\alpha \in R'$ with $x_\alpha \in R$ and $\mathbf{M}_\alpha$ a monomial in the t_τ, note

$$(x'm_\mu) \otimes n_\nu - m_\mu \otimes (x'n_\nu) = \sum x_\alpha\big((\mathbf{M}_\alpha m_\mu) \otimes n_\nu - m_\mu \otimes (\mathbf{M}_\alpha n_\nu)\big) \in K'.$$

Finally, given any $m = \sum y_\mu m_\mu$ and $n = \sum z_\nu n_\nu$ with y_μ, $z_\nu \in R'$, note that

$$(x'm) \otimes n - m \otimes (x'n) = \sum (y_\mu \otimes 1)(1 \otimes z_\nu)\big((x'm_\mu) \otimes n_\nu - m_\mu \otimes (x'n_\nu)\big) \in K',$$

as desired. □

Exercise (8.14) . — Let $F \colon ((R\text{-mod})) \to ((R\text{-mod}))$ be a linear functor, and $\mathcal{C}$ the category of finitely generated modules. Show that F always preserves finite direct sums. Show that $\theta(M) \colon M \otimes F(R) \to F(M)$ is surjective if F preserves surjections in $\mathcal{C}$ and M is finitely generated, and that $\theta(M)$ is an isomorphism if F preserves cokernels in $\mathcal{C}$ and M is finitely presented.

Solution: The first assertion follows from the characterization of the direct sum of two modules in terms of maps (**4.26**), since F preserves the relations there.

The second assertion follows from the first via the second part of the proof of Watt's Theorem (**8.13**), but with Λ, then Σ and Λ finite. □

Exercise (8.20) . — Let R be a ring, R' and R'' algebras, M' an R'-module and M'' an R''-module. Say $\{m'_\lambda\}$ generates M' over R' and $\{m''_\mu\}$ generates M'' over R''. Show $\{m'_\lambda \otimes m''_\mu\}$ generates $M' \otimes_R M''$ over $R' \otimes_R R''$.

Solution: Owing to (**8.2**), $M' \otimes M''$ is generated by all the $m' \otimes m''$ with $m' \in M'$ and $m'' \in M''$. But $m' = \sum_\lambda x'_\lambda m'_\lambda$ and $m'' = \sum_\mu x''_\mu m''_\mu$ with $x'_\lambda \in R'$ and $x''_\mu \in R''$. Thus $m' \otimes m'' = \sum_{\lambda,\mu} (x'_\lambda \otimes x''_\mu)(m'_\lambda \otimes m''_\mu)$, as desired. □

Exercise (8.21) . — Let R be a ring, R' an R- algebra, and M an R'-module. Set $M' := R' \otimes_R M$. Define $\alpha \colon M \to M'$ by $\alpha m := 1 \otimes m$. Prove M is a direct summand of M' with $\alpha = \iota_M$, and find the retraction (projection) $\pi_M \colon M' \to M$.

Solution: As the canonical map $R' \times M \to M'$ is bilinear, α is linear. Define $\mu \colon M \times R' \to M$ by $\mu(x, m) := xm$. Plainly μ is R-bilinear. So μ induces an R-linear map $\rho : M' \to M$, given by $\rho(x \otimes m) = xm$. Then ρ is a retraction of α, as $\rho(\alpha(m)) = 1 \cdot m$. Let $\beta \colon M' \to \mathrm{Coker}(\alpha)$ be the quotient map. Then (**5.8**) implies that M is a direct summand of M' with $\alpha = \iota_M$ and $\rho = \pi_M$. □

Exercise (8.22) . — Let R be a domain, $\mathfrak{a}$ a nonzero ideal. Set $K := \operatorname{Frac}(R)$. Show that $\mathfrak{a} \otimes_R K = K$.

Solution: Define a map $\beta\colon \mathfrak{a} \times K \to K$ by $\beta(x, y) := xy$. It is clearly R-bilinear. Given any R-bilinear map $\alpha\colon \mathfrak{a} \times K \to P$, fix a nonzero $z \in \mathfrak{a}$, and define an R-linear map $\gamma\colon K \to P$ by $\gamma(y) := \alpha(z, y/z)$. Then $\alpha = \gamma\beta$ as

$$\alpha(x, y) = \alpha(xz, y/z) = \alpha(z, xy/z) = \gamma(xy) = \gamma\beta(x, y).$$

Clearly, β is surjective. So γ is unique with this property. Thus the UMP implies that $K = \mathfrak{a} \otimes_R K$. (Also, as γ is unique, γ is independent of the choice of z.)

Alternatively, form the linear map $\varphi\colon \mathfrak{a} \otimes K \to K$ induced by the bilinear map β. Since β is surjective, so is φ. Now, given any $w \in \mathfrak{a} \otimes K$, say $w = \sum a_i \otimes x_i/x$ with all x_i and x in R. Set $a := \sum a_i x_i \in \mathfrak{a}$. Then $w = a \otimes (1/x)$. Hence, if $\varphi(w) = 0$, then $a/x = 0$; so $a = 0$ and so $w = 0$. Thus φ is injective, so bijective. □

Exercise (8.23) . — In the setup of (8.9), find the unit η_M of each adjunction.

Solution: Consider the left adjoint $FM := M \otimes_R R'$ of restriction of scalars. A map $\theta\colon FM \to P$ corresponds to the map $M \to P$ carrying m to $\theta(m \otimes 1_{R'})$. Take $P := FM$ and $\theta := 1_{FM}$. Thus $\eta_M\colon M \to FM$ is given by $\eta_M m = m \otimes 1_{R'}$.

Consider the right adjoint $F'P := \operatorname{Hom}_R(R',\, P)$ of restriction of scalars. A map $\mu\colon M \to P$ corresponds to the map $M \to F'P$ carrying m to the map $\nu : R' \to P$ defined by $\nu x := x(\mu m)$. Take $P := M$ and $\mu := 1_M$. Thus $\eta_M\colon M \to F'M$ is given by $(\eta_M m)(x) = xm$. □

Exercise (8.24) . — Let M and N be nonzero k-vector spaces. Prove $M \otimes N \neq 0$.

Solution: Vector spaces are free modules; say $M = k^{\oplus\Phi}$ and $N = k^{\oplus\Psi}$. Then (8.10) yields $M \otimes N = k^{\oplus(\Phi\times\Psi)}$ as $k \otimes k = k$ by (8.5)(2). Thus $M \otimes N \neq 0$. □

Exercise (8.25) . — Let R be a nonzero ring. Show:

(1) Assume there is a surjective map $\alpha\colon R^n \twoheadrightarrow R^m$. Then $n \geq m$.

(2) Assume $R^n \simeq R^m$. Then $n = m$.

Solution: For (1), let $\mathfrak{m}$ be a maximal ideal. Set $k := R/\mathfrak{m}$. Then k is a field. Now, $\alpha \otimes 1_k\colon R^n \otimes k \twoheadrightarrow R^m \otimes k$ is surjective by (8.10). But (8.10) and (8.5)(2) yield $R^r \otimes k = (R \otimes k)^r = k^r$ for any $r \geq 0$. Thus $\alpha \otimes 1_k$ is a surjective map of vector spaces. So $n \geq m$. Thus (1) holds.

Note (2) holds as (1) implies both $n \geq m$ and $m \geq n$. □

Exercise (8.26) . — Under the conditions of (5.41)(1), set$K := \operatorname{Frac}(R)$. Show

$$\operatorname{rank}(F) = \dim_K(M \otimes K).$$

Solution: Recall $M = T \oplus F$. So $M \otimes K = (T \otimes K) \oplus (F \otimes K)$ by (8.10).

Given $m \in T$, say $xm = 0$ with $x \in R$ nonzero. Given $y \in K$, note that $m \otimes y = xm \otimes (y/x) = 0$. Thus $T \otimes K = 0$. Thus $M \otimes K = F \otimes K$.

Set $r = \operatorname{rank}(F)$; so $F \simeq R^r$. Then $F \otimes K \simeq K^r$ again by (8.10) as $R \otimes K = K$ by (8.5)(1)–(2). But $\dim_K(K^r) = r$. Thus $\dim_K(F \otimes K) = r$, as desired. □

Exercise (8.27) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals, and M a module.

(1) Use (8.10) to show that $(R/\mathfrak{a}) \otimes M = M/\mathfrak{a}M$.

(2) Use (1) and (4.21) to show that $(R/\mathfrak{a}) \otimes (M/\mathfrak{b}M) = M/(\mathfrak{a} + \mathfrak{b})M$.

Solution: For (1), view $R/\mathfrak{a}$ as the cokernel of the inclusion $\mathfrak{a} \to R$. Then **(8.10)** implies that $(R/\mathfrak{a}) \otimes M$ is the cokernel of $\mathfrak{a} \otimes M \to R \otimes M$. Now, $R \otimes M = M$ and $x \otimes m = xm$ by **(8.5)**(2). Correspondingly, $\mathfrak{a} \otimes M \to M$ has $\mathfrak{a}M$ as image. The assertion follows. (Caution: $\mathfrak{a} \otimes M \to M$ needn't be injective; if it's not, then $\mathfrak{a} \otimes M \neq \mathfrak{a}M$. For example, take $R := \mathbb{Z}$, take $\mathfrak{a} := \langle 2\rangle$, and take $M := \mathbb{Z}/\langle 2\rangle$; then $\mathfrak{a} \otimes M \to M$ is just multiplication by 2 on $\mathbb{Z}/\langle 2\rangle$, and so $\mathfrak{a}M = 0$.)

For (2), set $N := M/\mathfrak{b}M$. Then (1) yields $(R/\mathfrak{a}) \otimes N = N/\mathfrak{a}N$. But **(4.21)** yields $N/\mathfrak{a}N = M/(\mathfrak{a} + \mathfrak{b})M$, as desired. □

Exercise (8.28) . — Let R be a ring, B an algebra, B' and B'' algebras over B. Regard B as an $(B \otimes_R B)$-algebra via the multiplication map. Set $C := B' \otimes_R B''$. Prove these formulas: (1) $B' \otimes_B B'' = C/\mathfrak{d}_B C$ and (2) $B' \otimes_B B'' = B \otimes_{B\otimes_R B} C$.

Solution: Consider the natural map $C \to B' \otimes_B B''$. It's surjective, and its kernel is generated by all differences $xx' \otimes x'' - x' \otimes xx''$ for $x \in B$ and $x' \in B'$ and $x'' \in B''$ by **(8.7)**(2). But $xx' \otimes x'' - x' \otimes xx'' = (x' \otimes x'')(x \otimes 1 - 1 \otimes x)$. Thus the kernel is equal to $\mathfrak{d}_B C$. So **(1.5.1)** yields (1).

Finally, $C/\mathfrak{d}_B C = \big((B \otimes_R B)/\mathfrak{d}_B\big) \otimes_{B\otimes_R B} C$ by **(8.27)**(1). But $(B \otimes_R B)/\mathfrak{d}_B = B$ by **(1.5.1)**. Thus (1) yields (2). □

Exercise (8.29) . — Show $\mathbb{Z}/\langle m\rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle n\rangle = 0$ if m and n are relatively prime.

Solution: Note $\langle m\rangle + \langle n\rangle = \mathbb{Z}$ by **(2.18)**. Thus **(8.27)**(2) yields

$$\mathbb{Z}/\langle m\rangle \otimes_{\mathbb{Z}} \mathbb{Z}/\langle n\rangle = \mathbb{Z}/\big\langle \langle m\rangle + \langle n\rangle \big\rangle = 0.$$ □

Exercise (8.30) . — Let R be a ring, R' and R'' algebras, $\mathfrak{a}' \subset R'$ and $\mathfrak{a}'' \subset R''$ ideals. Let $\mathfrak{b} \subset R' \otimes_R R''$ denote the ideal generated by $\mathfrak{a}'$ and $\mathfrak{a}''$. Show that

$$(R' \otimes_R R'')/\mathfrak{b} = (R'/\mathfrak{a}') \otimes_R (R''/\mathfrak{a}'').$$

Solution: Set $C := R' \otimes_R R''$. Then $C/\mathfrak{a}'C = (R'/\mathfrak{a}') \otimes_{R'} C$ by **(8.27)**(1). But $(R'/\mathfrak{a}') \otimes_{R'} C = (R'/\mathfrak{a}') \otimes_R R''$ by **(8.9)**(1) and **(8.5)**(2). Similar reasoning yields

$$\big((R'/\mathfrak{a}') \otimes_R R''\big)/\big((R'/\mathfrak{a}') \otimes_R R''\big)\mathfrak{a}'' = (R'/\mathfrak{a}') \otimes_R (R''/\mathfrak{a}'').$$

But plainly the canonical map $C \to (R'/\mathfrak{a}') \otimes_R R''$ takes $\mathfrak{b}$ onto $\big((R'/\mathfrak{a}') \otimes_R R''\big)\mathfrak{a}''$. So **(1.9)** yields the desired result. □

Exercise (8.31) . — Let R be a ring, M a module, $\mathcal{X}$ a set of variables. Prove the equation $M \otimes_R R[\mathcal{X}] = M[\mathcal{X}]$.

Solution: Both sides are "the" left adjoint of the Restriction of Scalars from P to R owing to **(8.9)**(2) and **(6.17)**. Thus by **(6.3)**, they are equal.

Alternatively, define $b\colon M \times R[\mathcal{X}] \to M[\mathcal{X}]$ by $b\big(m, \sum a_i\mathbf{M}_i\big) := \sum a_i m\mathbf{M}_i$ for monomials $\mathbf{M}_i$. Then b is bilinear, so induces a linear map $\beta\colon M \otimes_R R[\mathcal{X}] \to M[\mathcal{X}]$.

Note β is surjective: given $u := \sum m_i\mathbf{M}_i$ in $M[\mathcal{X}]$, set $t := \sum m_i \otimes \mathbf{M}_i$; then $\beta t = u$. Finally, β is injective: by **(8.16)**, any $t \in M \otimes_R R[\mathcal{X}]$ is of the form $t = \sum m_i \otimes \mathbf{M}_i$, so $\beta t = \sum m_i\mathbf{M}_i$; if $\beta t = 0$, then $m_i = 0$ for all i, so $t = 0$. □

Exercise (8.32) . — Generalize **(4.20)** to several variables $X_1, \ldots, X_r$ via this standard device: reduce to the case of one variable Y by taking a suitably large d and defining $\varphi\colon R[X_1, \ldots, X_r] \to R[Y]$ by $\varphi(X_i) := Y^{d^i}$ and setting $\alpha := 1_M \otimes \varphi$.

Solution: Let $F \in R[X_1, \dots]$. Assume there's a nonzero $G \in M[X_1, \dots]$ with $FG = 0$. Let's show there's a nonzero $m \in M$ with $Fm = 0$.

Recall $M[X_1, \dots] = M \otimes_R R[X_1, \dots]$ by (**8.31**), so $\alpha\colon M[X_1, \dots] \to M[Y]$. Moreover, $\varphi(F)\alpha(G) = \alpha(FG)$ Thus $\varphi(F)\alpha(G) = 0$.

Take d larger than any exponent in F or G. Note $\varphi(X_1^{i_1} \cdots X_r^{i_r}) = Y^{\sum i_j d^j}$. So φ carries distinct monomials of F to distinct monomials of $\varphi(F)$, and α carries distinct monomials of G to distinct monomials of $\alpha(G)$. So $\varphi(F)$ has the same coefficients as F, and $\alpha(G)$ has the same coefficients as G. Thus $\alpha(G) \neq 0$.

So (**4.20**) yields a nonzero $m \in M$ with $\varphi(F)m = 0$. Thus $Fm = 0$. □

Exercise (8.33) . — Let R be a ring, R_σ for $\sigma \in \Sigma$ algebras. For each finite subset J of Σ, let R_J be the tensor product of the R_σ for $\sigma \in J$. Prove that the assignment $J \mapsto R_J$ extends to a filtered direct system and that $\varinjlim R_J$ exists and is the coproduct $\coprod R_\sigma$.

Solution: Let Λ be the set of subsets of Σ, partially ordered by inclusion. Then Λ is a filtered small category by (**7.1**). Further, the assignment $J \mapsto R_J$ extends to a functor from Λ to $((R\text{-alg}))$ as follows: by induction, (**8.17**) implies that R_J is the coproduct of the family $(R_\sigma)_{\sigma \in J}$, so that, first, for each $\sigma \in J$, there is a canonical algebra map $\iota_\sigma\colon R_\sigma \to R_J$, and second, given $J \subset K$, the ι_σ for $\sigma \in K$ induce an algebra map $\alpha_K^J\colon R_J \to R_K$. So $\varinjlim R_J$ exists in $((R\text{-alg}))$ by (**7.4**).

Given a family of algebra maps $\varphi_\sigma\colon R_\sigma \to R'$, for each J, there is a compatible map $\varphi_J\colon R_J \to R'$, since R_J is the coproduct of the R_σ. Further, the various φ_J are compatible, so they induce a compatible map $\varphi\colon \varinjlim R_J \to R'$. Thus $\varinjlim R_J$ is the coproduct of the R_σ. □

Exercise (8.34) . — Let X be a variable, ω a complex cube root of 1, and $\sqrt[3]{2}$ the real cube root of 2. Set $k := \mathbb{Q}(\omega)$ and $K := k[\sqrt[3]{2}]$. Show $K = k[X]/\langle X^3 - 2\rangle$ and then $K \otimes_k K = K \times K \times K$.

Solution: Note ω is a root of $X^2 + X + 1$, which is irreducible over $\mathbb{Q}$; hence, $[k : \mathbb{Q}] = 2$. But the three roots of $X^3 - 2$ are $\sqrt[3]{2}$ and $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. Therefore, $X^3 - 2$ has no root in k. So $X^3 - 2$ is irreducible over k. Thus $k[X]/\langle X^3 - 2\rangle \xrightarrow{\sim} K$.

Note $K[X] = K \otimes_k k[X]$ as k-algebras by (**8.18**). So (**8.5**)(2) and (**8.9**)(1) and (**8.27**)(1) yield

$$\begin{aligned} k[X]/\langle X^3 - 2\rangle \otimes_k K &= k[X]/\langle X^3 - 2\rangle \otimes_{k[X]} (k[X] \otimes_k K) \\ &= k[X]/\langle X^3 - 2\rangle \otimes_{k[X]} K[X] = K[X]/\langle X^3 - 2\rangle. \end{aligned}$$

However, $X^3 - 2$ factors in K as follows:

$$X^3 - 2 = \big(X - \sqrt[3]{2}\big)\big(X - \omega\sqrt[3]{2}\big)\big(X - \omega^2\sqrt[3]{2}\big).$$

So the Chinese Remainder Theorem, (**1.21**), yields

$$K[X]/\langle X^3 - 2\rangle = K \times K \times K,$$

because $K[X]/\langle X - \omega^i\sqrt[3]{2}\rangle \xrightarrow{\sim} K$ for any i by (**1.6**)(2). □

9. Flatness

Exercise (9.17) . — Let R be a ring, $\mathfrak{a}$ an ideal. Show $\Gamma_{\mathfrak{a}}(\bullet)$ is a left exact functor.

Solution: Given an R-map $\alpha\colon M \to N$, note that $\mathrm{Ann}(m) \subset \mathrm{Ann}(\alpha(m))$ for all $m \in M$. Assume that $m \in \Gamma_{\mathfrak{a}}(M)$; that is, $\mathfrak{a} \subset \sqrt{\mathrm{Ann}(m)}$. It follows that $\alpha(m) \in \Gamma_{\mathfrak{a}}(N)$. Thus $\Gamma_{\mathfrak{a}}(\bullet)$ is a functor.

Given an exact sequence of R-modules $0 \to M \xrightarrow{\alpha} N \xrightarrow{\beta} P$. form the sequence $0 \to \Gamma_{\mathfrak{a}}(M) \xrightarrow{\alpha} \Gamma_{\mathfrak{a}}(N) \xrightarrow{\beta} \Gamma_{\mathfrak{a}}(P)$. Trivially, it is exact at $\Gamma_{\mathfrak{a}}(M)$. Owing to **(4.14)**(2), it is exact at $\Gamma_{\mathfrak{a}}(N)$. Thus $\Gamma_{\mathfrak{a}}(\bullet)$ is left exact. □

Exercise (9.18) . — Let R be a ring, N a module, N_1 and N_2 submodules, R' an algebra, F an exact R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Prove:

$$F(N_1 \cap N_2) = F(N_1) \cap F(N_2) \quad \text{and} \quad F(N_1 + N_2) = F(N_1) + F(N_2).$$

Solution: Define $\sigma_N\colon N_1 \oplus N_2 \to N$ by $\sigma_N(n_1, n_2) := n_1 + n_2$. Identifying its kernel and image yields the following exact sequence, where $\alpha(n) := (n, -n)$:

$$0 \to N_1 \cap N_2 \xrightarrow{\alpha} N_1 \oplus N_2 \to N_1 + N_2 \to 0.$$

As F is exact, applying F yields the following exact sequence:

$$0 \to F(N_1 \cap N_2) \to F(N_1 \oplus N_2) \to F(N_1 + N_2) \to 0.$$

But $F(\sigma_N) = \sigma_{F(N)}$ owing to **(8.15)**. So the above sequence is equal to this one

$$0 \to F(N_1) \cap F(N_2) \to F(N_1) \oplus F(N_2) \to F(N_1) + F(N_2) \to 0,$$

which identifies the kernel and image of $\sigma_{F(N)}$, as desired. □

Exercise (9.14) (*Equational Criterion for Flatness*) . — Prove that Condition **(9.13)**(4) can be reformulated as follows: Given any relation $\sum_i x_i m_i = 0$ with $x_i \in R$ and $m_i \in M$, there are $x_{ij} \in R$ and $m'_j \in M$ such that

$$\textstyle\sum_j x_{ij} m'_j = m_i \text{ for all } i \text{ and } \sum_i x_{ij} x_i = 0 \text{ for all } j. \tag{9.14.1}$$

Solution: Assume **(9.13)**(4) holds. Let $e_1, \dots, e_m$ be the standard basis of R^m. Given a relation $\sum_1^m x_i m_i = 0$, define $\alpha\colon R^m \to M$ by $\alpha(e_i) := m_i$ for each i. Set $k := \sum x_i e_i$. Then $\alpha(k) = 0$. So **(9.13)**(4) yields a factorization $\alpha\colon R^m \xrightarrow{\varphi} R^n \xrightarrow{\beta} M$ with $\varphi(k) = 0$. Let $e'_1, \dots, e'_n$ be the standard basis of R^n, and set $m'_j := \beta(e'_j)$ for each j. Let (x_{ij}) be the $n \times m$ matrix of φ; that is, $\varphi(e_i) = \sum x_{ji} e'_j$. Then $m_i = \sum x_{ji} m'_j$. Now, $\varphi(k) = 0$; hence, $\sum_{i,j} x_{ji} x_i e'_j = 0$. Thus **(9.14.1)** holds.

Conversely, given $\alpha\colon R^m \to M$ and $k \in \mathrm{Ker}(\alpha)$, say $k = \sum x_i e_i$. Assume **(9.14.1)**. Define $\varphi\colon R^m \to R^n$ via the matrix (x_{ij}); that is, $\varphi(e_i) = \sum x_{ji} e'_j$. Then $\varphi(k) = \sum x_i x_{ji} e'_j = 0$. Define $\beta\colon R^n \to M$ by $\beta(e'_j) := m'_j$. Then $\beta\varphi(e_i) = m_i$; hence, $\beta\varphi = \alpha$. Thus **(9.13)**(4) holds. □

Exercise (9.19) . — Let R be a ring, R' an algebra, F an R-linear functor from $((R\text{-mod}))$ to $((R'\text{-mod}))$. Assume F is exact. Prove the following equivalent:

(1) F is faithful.
(2) An R-module M vanishes if FM does.
(3) $F(R/\mathfrak{m}) \neq 0$ for every maximal ideal $\mathfrak{m}$ of R.
(4) A sequence $M' \xrightarrow{\alpha} M \xrightarrow{\beta} M''$ is exact if $FM' \xrightarrow{F\alpha} FM \xrightarrow{F\beta} FM''$ is.

Solution: To prove (1) implies (2), suppose $FM = 0$. Then $1_{FM} = 0$. But always $1_{FM} = F(1_M)$. Hence (1) yields $1_M = 0$. So $M = 0$. Thus (2) holds.

Conversely, assume (2). Given $\alpha\colon M \to N$ with $F\alpha = 0$, set $I := \mathrm{Im}(\alpha)$. As F is exact, **(9.3)** yields $FI = \mathrm{Im}(F\alpha)$. Hence $FI = 0$. So (2) yields $I = 0$. Thus $\alpha = 0$. Thus (1) holds. Thus (1) and (2) are equivalent.

To prove (2) implies (3), take $M := R/\mathfrak{m}$.

Conversely, assume (3). Given $0 \neq m \in M$, form $\alpha\colon R \to M$ by $\alpha(x) := xm$. Set $\mathfrak{a} := \mathrm{Ker}(\alpha)$. Let $\mathfrak{m} \supset \mathfrak{a}$ be a maximal ideal. We get a surjection $R/\mathfrak{a} \twoheadrightarrow R/\mathfrak{m}$ and an injection $R/\mathfrak{a} \hookrightarrow M$. They induce a surjection $F(R/\mathfrak{a}) \twoheadrightarrow F(R/\mathfrak{m})$ and an injection $F(R/\mathfrak{a}) \hookrightarrow FM$ as F is exact. But $F(R/\mathfrak{m}) \neq 0$ by (3). So $F(R/\mathfrak{a}) \neq 0$. So $FM \neq 0$. Thus (2) holds. Thus (1) and (2) and (3) are equivalent.

To prove (1) implies (4), set $I := \mathrm{Im}(\alpha)$ and $K := \mathrm{Ker}(\beta)$. Now, $F(\beta\alpha) = 0$. So (1) yields $\beta\alpha = 0$. Hence $I \subset K$. But F is exact; so $F(K/I) = FK/FI$, and **(9.3)** yields $FI = \mathrm{Im}(F\alpha)$ and $FK = \mathrm{Ker}(F\beta)$. Hence $F(K/I) = 0$. But (1) implies (2). So $K/I = 0$. Thus (4) holds.

Conversely, assume (4). Given $\alpha\colon M \to N$ with $F\alpha = 0$, set $K := \mathrm{Ker}(\alpha)$. As F is exact, **(9.3)** yields $FK = \mathrm{Ker}(F\alpha)$. Hence $FK \to FM \to 0$ is exact. So (4) implies $K \to M \to 0$ is exact. So $\alpha = 0$. Thus (1) holds, as desired. □

Exercise (9.20) . — Show that a ring of polynomials P is faithfully flat.

Solution: The monomials form a free basis, so P is faithfully flat by **(9.6)**. □

Exercise (9.21) . — Let R be a ring, M and N flat modules. Show that $M \otimes N$ is flat. What if "flat" is replaced everywhere by "faithfully flat"?

Solution: Associativity **(8.8)**(1) yields $(M \otimes N) \otimes \bullet = M \otimes (N \otimes \bullet)$; in other words, $(M \otimes N) \otimes \bullet = (M \otimes \bullet) \circ (N \otimes \bullet)$. So $(M \otimes N) \otimes \bullet$ is the composition of two exact functors. Hence it is exact. Thus $M \otimes N$ is flat.

Similarly if M and N are faithfully flat, then $M \otimes N \otimes \bullet$ is faithful and exact. So $M \otimes N$ is faithfully flat. □

Exercise (9.22) . — Let R be a ring, M a flat module, R' an algebra. Show that $M \otimes_R R'$ is flat over R'. What if "flat" is replaced everywhere by "faithfully flat"?

Solution: Cancellation **(8.9)**(1) yields $(M \otimes_R R') \otimes_{R'} \bullet = M \otimes_R \bullet$. But $M \otimes_R \bullet$ is exact, as M is flat over R. Thus $M \otimes_R R'$ is flat over R'.

Similarly, if M is faithfully flat over R, then $M \otimes_R \bullet$ is faithful too. Thus $M \otimes_R R'$ is faithfully flat over R'. □

Exercise (9.23) . — Let R be a ring, R' a flat algebra, M a flat R'-module. Show that M is flat over R. What if "flat" is replaced everywhere by "faithfully flat"?

Solution: Cancellation **(8.9)**(1) yields $M \otimes_R \bullet = M \otimes_{R'} (R' \otimes_R \bullet)$. But $R' \otimes_R \bullet$ and $M \otimes_{R'} \bullet$ are exact; so their composition $M \otimes_R \bullet$ is too. Thus M is flat over R.

Similarly, as the composition of two faithful functors is, plainly, faithful, the assertion remains true if "flat" is replaced everywhere by "faithfully flat." □

Exercise (9.24) . — Let R be a ring, R' and R'' algebras, M' a flat R'-module, and M'' a flat R''-module. Show that $M' \otimes_R M''$ is a flat $(R' \otimes_R R'')$-module. What if "flat" is replaced everywhere by "faithfully flat"?

Solution: Given an $(R'\otimes_R R'')$-module N, apply Associativity (8.8)(1) liberally, apply Cancellation (8.9)(1) twice, and apply Commutativity (8.5)(1) once to get

$$\begin{aligned} N\otimes_{R''} M'' &= N_{R'\otimes_R R''}(R'\otimes_R R'')\otimes_{R''} M'' = N\otimes_{R'\otimes_R R''}(R'\otimes_R M'') \\ &= (R'\otimes_R M'')\otimes_{R'\otimes_R R''} N. \end{aligned}$$

Hence (8.9)(1) yields $M'\otimes_{R'}(N\otimes_{R''} M'') = (M'\otimes_R M'')\otimes_{R'\otimes_R R''} N$. Therefore, $(M'\otimes_R M')\otimes_{R'\otimes_R R''}\bullet$ is equal to the composition of two exact functors, $M'\otimes_R\bullet$ and $\bullet\otimes_{R''} M''$. Thus $M'\otimes_R M''$ is flat.

Similarly, as the composition of two faithful functors is, plainly, faithful, the assertion remains true if "flat" is replaced everywhere by "faithfully flat." □

Exercise (9.25) . — Let R be a ring, R' an algebra, and M an R'-module. Assume that M is flat over R and faithfully flat over R'. Show that R' is flat over R.

Solution: Cancellation (8.9)(1) yields $\bullet\otimes_R M = (\bullet\otimes_R R')\otimes_{R'} M$. But $\bullet\otimes_R M$ is exact, and $\bullet\otimes_{R'} M$ is faithful. Thus, by (9.19), $\bullet\otimes_R R'$ is exact, as desired. □

Exercise (9.26) . — Let R be a ring, R' an algebra, R'' an R'-algebra, and M an R'-module. Assume that R'' is flat over R' and that M is flat over R. Show that $R''\otimes_{R'} M$ is flat over R. Conversely, assume that $R''\otimes_{R'}\bullet$ is faithful and that $R''\otimes_{R'} M$ is flat over R. Show that M is flat over R.

Solution: Associativity (8.8)(1) yields $(R''\otimes_{R'} M)\otimes_R \bullet R''\otimes_{R'}(M\otimes_R\bullet)$. Thus $(R''\otimes_{R'} M)\otimes_R\bullet$ is exact if $R''\otimes_{R'}\bullet$ and $M\otimes_R\bullet$ are. Conversely, by (9.19), $M\otimes_R\bullet$ is exact if $R''\otimes_{R'}\bullet$ is faithful and $(R''\otimes_{R'} M)\otimes_R\bullet$ is exact. □

Exercise (9.27) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $R/\mathfrak{a}$ is flat. Show $\mathfrak{a}=\mathfrak{a}^2$.

Solution: Since $R/\mathfrak{a}$ is flat, tensoring it with the inclusion $\mathfrak{a}\hookrightarrow R$ yields an injection $\mathfrak{a}\otimes_R(R/\mathfrak{a})\hookrightarrow R\otimes_R(R/\mathfrak{a})$. But the image vanishes: $a\otimes r = 1\otimes ar = 0$. Further, $\mathfrak{a}\otimes_R(R/\mathfrak{a}) = \mathfrak{a}/\mathfrak{a}^2$ by (8.27)(1). Hence $\mathfrak{a}/\mathfrak{a}^2=0$. Thus $\mathfrak{a}=\mathfrak{a}^2$. □

Exercise (9.28) . — Let R be a ring, R' a flat algebra. Prove equivalent:

(1) R' is faithfully flat over R.
(2) For every R-module M, the map $M\xrightarrow{\alpha} M\otimes_R R'$ by $\alpha m = m\otimes 1$ is injective.
(3) Every ideal $\mathfrak{a}$ of R is the contraction of its extension, or $\mathfrak{a}=(\mathfrak{a}R')^c$.
(4) Every prime $\mathfrak{p}$ of R is the contraction of some prime $\mathfrak{q}$ of R', or $\mathfrak{p}=\mathfrak{q}^c$.
(5) Every maximal ideal $\mathfrak{m}$ of R extends to a proper ideal, or $\mathfrak{m}R'\neq R'$.
(6) Every nonzero R-module M extends to a nonzero module, or $M\otimes_R R'\neq 0$.

Solution: Assume (1). In (2), set $K := \operatorname{Ker}\alpha$. Then the canonical sequence

$$0\longrightarrow K\otimes R'\longrightarrow M\otimes R'\xrightarrow{\alpha\otimes 1} M\otimes R'\otimes R'$$

is exact. But $\alpha\otimes 1$ has a retraction, namely $m\otimes x\otimes y\mapsto m\otimes xy$. So $\alpha\otimes 1$ is injective. Hence $K\otimes_R R'=0$. So (1) implies $K=0$ by (9.19). Thus (2) holds.

Assume (2). Then $R/\mathfrak{a}\to(R/\mathfrak{a})\otimes R'$ is injective. But $(R/\mathfrak{a})\otimes R' = R'/\mathfrak{a}R'$ by (8.27)(1). Thus (3) holds.

Assume (3). Then (3.10)(2) yields (4).

Assume (4). Then every maximal ideal $\mathfrak{m}$ of R is the contraction of some prime $\mathfrak{q}$ of R'. So $\mathfrak{m}R'\subset\mathfrak{q}$. Thus (5) holds.

Assume (5). Consider (6). Take a nonzero $m\in M$, and set $M' := Rm$. As R' is flat, the inclusion $M'\hookrightarrow M$ yields an injection $M'\otimes R'\hookrightarrow M\otimes R'$.

Note $M' = R/\mathfrak{a}$ for some $\mathfrak{a}$ by (**4.7**). So $M' \otimes_R R' = R'/\mathfrak{a}R'$ by (**8.27**)(1). Take a maximal ideal $\mathfrak{m} \supset \mathfrak{a}$. Then $\mathfrak{a}R' \subset \mathfrak{m}R'$. But $\mathfrak{m}R' \subsetneqq R'$ by (5). Hence $R'/\mathfrak{a}R' \neq 0$. So $M' \otimes_R R' \neq 0$. Hence $M \otimes R' \neq 0$. Thus (6) holds.

Finally, (6) and (1) are equivalent by (**9.19**). $\square$

Exercise (9.29) . — Let R be a ring, R' a faithfully flat algebra. Assume R' is local. Prove R is local too.

Solution: Let $\mathfrak{m}'$ be the maximal ideal of R'. Given a proper ideal $\mathfrak{a}$ of R, note that $\mathfrak{a} = (\mathfrak{a}R')^c$ by (**9.28**)(3) as R' is faithfully flat. So $1 \notin \mathfrak{a}R'$. Hence $\mathfrak{a}R' \subset \mathfrak{m}'$. So $\mathfrak{a} \subset \mathfrak{m}'^c$. Thus $\mathfrak{m}'^c$ is the only maximal ideal of R. $\square$

Exercise (9.30) . — Let R be a ring, $0 \to M' \xrightarrow{\alpha} M \to M'' \to 0$ an exact sequence with M flat. Assume $N \otimes M' \xrightarrow{N\otimes\alpha} N \otimes M$ is injective for all N. Prove M'' is flat.

Solution: Let $\beta\colon N \to P$ be an injection. It yields the following commutative diagram with exact rows by hypothesis and by (**8.10**):

$$\begin{tikzcd}
0 \arrow[r] & N \otimes M' \arrow[r] \arrow[d, "\beta\otimes M'"'] & N \otimes M \arrow[r] \arrow[d, "\beta\otimes M"'] & N \otimes M'' \arrow[r] \arrow[d, "\beta\otimes M''"] & 0 \\
0 \arrow[r] & P \otimes M' \arrow[r] \arrow[d] & P \otimes M \arrow[r] \arrow[d] & P \otimes M'' \arrow[r] & 0 \\
0 \arrow[r] & P/N \otimes M' \arrow[r] & P/N \otimes M & &
\end{tikzcd}$$

Since M is flat, $\mathrm{Ker}(\beta \otimes M) = 0$. So the Snake Lemma (**5.10**) applied to the top two rows yields $\mathrm{Ker}(\beta \otimes M'') = 0$. Thus M'' is flat. $\square$

Exercise (9.31) . — Prove that an R-algebra R' is faithfully flat if and only if the structure map $\varphi\colon R \to R'$ is injective and the quotient $R'/\varphi R$ is flat over R.

Solution: Assume R' is faithfully flat. Then for every R-module M, the map $M \xrightarrow{\alpha} M \otimes_R R'$ is injective by (**9.28**). Taking $M := R$ shows φ is injective. And, since R' is flat, $R'/\varphi(R)$ is flat by (**9.30**).

Conversely, assume φ is injective and $R'/\varphi(R)$ is flat. Then $M \to M \otimes_R R'$ is injective for every module M by (**9.8**)(1), and R' is flat by (**9.8**)(2). Thus R' is faithfully flat by (**9.28**). $\square$

Exercise (9.32) . — Let R be a ring, $0 \to M_n \to \cdots \to M_1 \to 0$ an exact sequence of flat modules, and N any module. Then the following sequence is exact:

$$0 \to M_n \otimes N \to \cdots - \to M_1 \otimes N \to 0. \qquad (\mathbf{9.32.1})$$

Solution: Set $K := \mathrm{Ker}(M_2 \to M_1)$. Then the following sequences are exact:

$$0 \to M_n \to \cdots \to M_3 \to K \to 0 \quad \text{and} \quad 0 \to K \to M_2 \to M_1 \to 0.$$

Since M_1 is flat, the sequence

$$0 \to K \otimes N \to M_2 \otimes N \to M_1 \otimes N \to 0$$

is exact by (**9.8**)(1). Since M_1 and M_2 are flat, K is flat by (**9.8**)(2). So

$$0 \to M_n \otimes N \to \cdots \to M_3 \otimes N \to K \otimes N \to 0$$

is exact by induction on n. Thus (**9.32.1**) is exact. $\square$

Exercise (9.33) . — Let R be a ring, R' an algebra, M and N modules.

(1) Show that there is a canonical R'-homomorphism

$$\sigma_M\colon \operatorname{Hom}_R(M,\,N)\otimes_R R' \to \operatorname{Hom}_{R'}(M\otimes_R R',\,N\otimes_R R').$$

(2) Assume M is finitely generated and projective. Show that σ_M is bijective.

(3) Assume R' is flat over R. Show that if M is finitely generated, then σ_M is injective, and that if M is finitely presented, then σ_M is bijective.

Solution: For (1) and (3), set $R' := R$ and $P := R'$ in **(9.10)**, set $P := N\otimes_R R'$ in **(8.9)**(2), and combine the two results.

For (2), note that **(5.27)** yields K, n and $M\oplus K \xrightarrow{\sim} R^n$. Form the functors

$$F(\bullet) := \operatorname{Hom}_R(\bullet, N)\otimes_R R' \quad\text{and}\quad F'(\bullet) := \operatorname{Hom}_{R'}(\bullet\otimes_R R', N\otimes_R R').$$

Plainly, F and F' are linear. So they preserve finite direct sums by **(8.14)**. Plainly, $\sigma_\bullet\colon F\to F'$ is a natural transformation. Also, $\bullet\otimes R'$ preserves direct sums by **(8.10)**. Putting it all together yields this diagram, with horizontal isomorphisms:

$$\begin{tikzcd}
\big(F(M)\otimes_R R'\big)\oplus\big(F(M')\otimes_R R'\big) \arrow[r, "\sim"] \arrow[d, "\sigma_M\oplus\sigma_{M'}"'] & F(R^n)\otimes_R R' \arrow[d, "\sigma_{R^n}"'] \\
F'(M)\oplus F'(M') \arrow[r, "\sim"] & F'(R^n)
\end{tikzcd}$$

Direct sum is a special case of direct limit by **(6.5)**. So the above diagram is commutative by **(6.15)**. By **(5.4)**, therefore, σ_M is an isomorphism if σ_{R^n} is. Similarly, σ_{R^n} is an isomorphism if σ_R is. Thus we must show σ_R is an isomorphism.

It is not hard to check that the following diagram is commutative:

$$\begin{tikzcd}
\operatorname{Hom}_R(R,\,N)\otimes_R R' \arrow[r, "\sim"] \arrow[d, "\sigma_R"'] & N\otimes_R R' \arrow[d, "1_{N\otimes_R R'}"'] \\
\operatorname{Hom}_{R'}(R\otimes_R R',\ N\otimes_R R') \arrow[r, "\sim"] & N\otimes_R R'
\end{tikzcd}$$

where the horizontal maps are the isomorphisms arising from **(4.3)** and **(8.5)**(2). Thus σ_R is an isomorphism, as required. □

Exercise (9.34) . — Let R be a ring, M a module, and R' an algebra. Prove $\operatorname{Ann}(M)R' \subset \operatorname{Ann}(M\otimes_R R')$, with equality if M is finitely generated, R' flat.

Solution: By construction, every element of $M\otimes R'$ is a sum of elements of the form $m\otimes r$ with $m\in M$ and $r\in R'$. But given $x\in\operatorname{Ann}(M)$ and $s\in R'$, note $xs(m\otimes r) = m\otimes xsr = xm\otimes sr = 0$ by **(8.6)**. Thus $\operatorname{Ann}(M)R'\subset\operatorname{Ann}(M\otimes_R R')$.

Assume M is finitely generated, say by $m_1,\dots,m_r$. Set $\mathfrak a := \operatorname{Ann}(M)$. Form $0\to\mathfrak a\to R\xrightarrow{\beta} M^r$ with $\beta(x) := (xm_1,\dots,xm_r)$. Plainly, it is exact. Assume R' is flat. Then $0\to\mathfrak a\otimes R'\to R'\xrightarrow{\beta\otimes 1} M^r\otimes R'$ is exact. And $\mathfrak a\otimes R' = \mathfrak aR'$ by **(9.15)**.

Given $y\in\operatorname{Ann}(M\otimes_R R')$, note $(m_i\otimes 1)y = 0$ for all i. But $M^r\otimes R' = (M\otimes R')^r$ by **(8.10)**; hence $(\beta\otimes 1)y = \big((m_1\otimes 1)y,\dots,(m_r\otimes 1)y\big)$. So $(\beta\otimes 1)y = 0$. Hence $y\in\mathfrak aR'$ by the above. Thus $\operatorname{Ann}(M\otimes_R R')\subset\mathfrak aR'$, and so equality holds. □

Exercise (9.35) . — Let R be a ring, M a module. Prove (1) if M is flat, then for $x\in R$ and $m\in M$ with $xm=0$, necessarily $m\in\operatorname{Ann}(x)M$, and (2) the converse holds if R is a **Principal Ideal Ring** (PIR); that is, every ideal $\mathfrak a$ is principal.

Solution: For (1), assume M is flat and $xm = 0$. Then **(9.14)** yields $x_j \in R$ and $m_j \in M$ with $\sum x_j m_j = m$ and $x_j x = 0$ for all j. Thus $m \in \mathrm{Ann}(x)M$.

Alternatively, $0 \to \mathrm{Ann}(x) \to R \xrightarrow{\mu_x} R$ is always exact. Tensoring with M gives $0 \to \mathrm{Ann}(x) \otimes M \to M \xrightarrow{\mu_x} M$, which is exact as M is flat. So $\mathrm{Im}(\mathrm{Ann}(x) \otimes M)$ is $\mathrm{Ker}(\mu_x)$. But always $\mathrm{Im}(\mathrm{Ann}(x) \otimes M)$ is $\mathrm{Ann}(x)M$. Thus (1) holds.

For (2), it suffices, by **(9.15)**, to show $\alpha\colon \mathfrak{a} \otimes M \to \mathfrak{a}M$ is injective. Since R is a PIR, $\mathfrak{a} = \langle x \rangle$ for some $x \in R$. So, given $z \in \mathfrak{a} \otimes M$, there are $y_i \in R$ and $m_i \in M$ such that $z = \sum_i y_i x \otimes m_i$. Set $m := \sum_i y_i m_i$. Then

$$z = \textstyle\sum_i x \otimes y_i m_i = x \otimes \sum_i y_i m_i = x \otimes m.$$

Suppose $z \in \mathrm{Ker}(\alpha)$. Then $xm = 0$. Hence $m \in \mathrm{Ann}(x)M$ by hypothesis. So $m = \sum_j z_j n_j$ for some $z_j \in \mathrm{Ann}(x)$ and $n_j \in M$. Hence

$$z = x \otimes \textstyle\sum_j z_j n_j = \sum_j z_j x \otimes n_j = 0.$$

Thus α is injective. Thus (2) holds. □

10. Cayley–Hamilton Theorem

Exercise (10.9) . — Let A be a local ring, $\mathfrak{m}$ the maximal ideal, M a finitely generated A-module, and $m_1, \ldots, m_n \in M$. Set $k := A/\mathfrak{m}$ and $M' := M/\mathfrak{m}M$, and write m'_i for the image of m_i in M'. Prove that $m'_1, \ldots, m'_n \in M'$ form a basis of the k-vector space M' if and only if $m_1, \ldots, m_n$ form a **minimal generating set** of M (that is, no proper subset generates M), and prove that every minimal generating set of M has the same number of elements.

Solution: By **(10.8)**, reduction mod $\mathfrak{m}$ gives a bijective correspondence between generating sets of M as an A-module, and generating sets of M' as an A-module, or equivalently by **(4.5)**, as an k-vector space. This correspondence preserves inclusion. Hence, a minimal generating set of M corresponds to a minimal generating set of M', that is, to a basis. But any two bases have the same number of elements. □

Exercise (10.10) . — Let A be a local ring, k its residue field, M and N finitely generated modules. Show: (1) $M = 0$ if and only if $M \otimes_A k = 0$.

(2) $M \otimes_A N \neq 0$ if $M \neq 0$ and $N \neq 0$.

Solution: For (1), let $\mathfrak{m}$ be the maximal ideal. Then $M \otimes k = M/\mathfrak{m}M$ by **(8.27)**(1). Thus (1) is nothing but a form of Nakayama's Lemma **(10.6)**.

In (2), $M \otimes k \neq 0$ and $N \otimes k \neq 0$ by (1). So $(M \otimes k) \otimes (N \otimes k) \neq 0$ by **(8.24)** and **(8.7)**(3). But $(M \otimes k) \otimes (N \otimes k) = (M \otimes N) \otimes (k \otimes k)$ by the Associative and Commutative Laws, **(8.8)**(1) and **(8.5)**(1). Finally, $k \otimes k = k$ by **(8.27)**(1). □

Exercise (10.23) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a}$ is finitely generated and idempotent (or $\mathfrak{a} = \mathfrak{a}^2$). Prove there is a unique idempotent e with $\langle e \rangle = \mathfrak{a}$.

Solution: By **(10.3)** with $\mathfrak{a}$ for M, there is $e \in \mathfrak{a}$ such that $(1-e)\mathfrak{a} = 0$. So for all $x \in \mathfrak{a}$, we have $(1-e)x = 0$, or $x = ex$. Thus $\mathfrak{a} = \langle e \rangle$ and $e = e^2$.

Finally, e is unique by **(3.34)**. □

Exercise (10.24) . — Let R be a ring, $\mathfrak{a}$ an ideal. Prove the following conditions are equivalent:

(1) $R/\mathfrak{a}$ is projective over R.

(2) $R/\mathfrak{a}$ is flat over R, and $\mathfrak{a}$ is finitely generated.
(3) $\mathfrak{a}$ is finitely generated and idempotent.
(4) $\mathfrak{a}$ is generated by an idempotent.
(5) $\mathfrak{a}$ is a direct summand of R.

Solution: Suppose (1) holds. Then $R/\mathfrak{a}$ is flat by **(9.6)**. Further, the sequence $0 \to \mathfrak{a} \to R \to R/\mathfrak{a} \to 0$ splits by **(5.16)**. So **(5.8)** yields a surjection $\rho\colon R \to \mathfrak{a}$. Hence $\mathfrak{a}$ is principal. Thus (2) holds.

If (2) holds, then (3) holds by **(9.27)**. If (3) holds, then (4) holds by **(10.23)**. If (4) holds, then (5) holds by **(1.12)**. If (5) holds, then $R \simeq \mathfrak{a} \bigoplus R/\mathfrak{a}$, and so (1) holds by **(5.16)**. □

Exercise (10.25) . — Prove the following conditions on a ring R are equivalent:

(1) R is **absolutely flat**; that is, every module is flat.
(2) Every finitely generated ideal is a direct summand of R.
(3) Every finitely generated ideal is idempotent.
(4) Every principal ideal is idempotent.

Solution: Assume (1). Let $\mathfrak{a}$ be a finitely generated ideal. Then $R/\mathfrak{a}$ is flat by hypotheses. So $\mathfrak{a}$ is a direct summand of R by **(10.24)**. Thus (2) holds.

Conditions (2) and (3) are equivalent by **(10.24)**.

Trivially, if (3) holds, then (4) does. Conversely, assume (4). Given a finitely generated ideal $\mathfrak{a}$, say $\mathfrak{a} = \langle x_1, \ldots, x_n\rangle$. Then each $\langle x_i\rangle$ is idempotent by hypothesis. So $\langle x_i\rangle = \langle f_i\rangle$ for some idempotent f_i by **(1.24)**(2). Then $\mathfrak{a} = \langle f_1, \ldots, f_n\rangle$. Hence $\mathfrak{a}$ is idempotent by **(1.24)**(4), (1). Thus (3) holds.

Assume (2). Let M be a module, and $\mathfrak{a}$ a finitely generated ideal. Then $\mathfrak{a}$ is a direct summand of R by hypothesis. So $R/\mathfrak{a}$ is flat by **(9.5)**. Hence $\mathfrak{a}\otimes M \xrightarrow{\sim} \mathfrak{a}M$ by **(9.8)**(1); cf. the proof of **(8.27)**(1). So M is flat by **(9.15)**. Thus (1) holds. □

Exercise (10.26) . — Let R be a ring. Prove the following statements:

(1) Assume R is Boolean. Then R is absolutely flat.
(2) Assume R is absolutely flat. Then any quotient ring R' is absolutely flat.
(3) Assume R is absolutely flat. Then every nonunit x is a zerodivisor.
(4) Assume R is absolutely flat and local. Then R is a field.

Solution: In (1), as R is Boolean, every element is idempotent. Hence every principal ideal is idempotent by **(1.24)**(1). Thus **(10.25)** yields (1).

For (2), let $\mathfrak{b} \subset R'$ be principal, say $\mathfrak{b} = \langle \overline{x}\rangle$. Let $x \in R$ lift $\overline{x}$. Then $\langle x\rangle$ is idempotent by **(10.25)**. Hence $\mathfrak{b}$ is also idempotent. Thus **(10.25)** yields (2).

For (3) and (4), take a nonunit x. Then $\langle x\rangle$ is idempotent by **(10.25)**. So $x = ax^2$ for some a. Then $x(ax-1) = 0$. But x is a nonunit. So $ax - 1 \neq 0$. Thus (3) holds.

Suppose R is local, say with maximal ideal $\mathfrak{m}$. Since x is a nonunit, $x \in \mathfrak{m}$. So $ax \in \mathfrak{m}$. So $ax - 1 \notin \mathfrak{m}$. So $ax - 1$ is a unit. But $x(ax-1) = 0$. So $x = 0$. Thus 0 is the only nonunit. Thus (4) holds. □

Exercise (10.27) . — Let R be a ring, $\alpha\colon M \to N$ a map of modules, $\mathfrak{m}$ an ideal. Assume that $\mathfrak{m} \subset \operatorname{rad}(N)$, that N is finitely generated, and that the induced map $\overline{\alpha}\colon M/\mathfrak{m}M \to N/\mathfrak{m}N$ is surjective. Show that α is surjective too.

Solution: As $\overline{\alpha}$ is surjective, $\alpha(M) + \mathfrak{m}N = N$. As N is finitely generated, so is $N/\alpha(M)$. But $\mathfrak{m} \subset \operatorname{rad}(N)$. So $\alpha(M) = N$ by **(10.8)**(1). Thus α is surjective. □

Exercise (10.28) . — Let R be a ring, $\mathfrak{m}$ an ideal, E a module, M, N submodules. Assume N is finitely generated, $\mathfrak{m} \subset \operatorname{rad}(N)$, and $N \subset M + \mathfrak{m}N$. Show $N \subset M$.

Solution: Set $L := M + N$. Then $M + \mathfrak{m}N \supset L$ as $N \subset \mathfrak{m}N + M$. Hence $M + \mathfrak{m}N = L$. So $M + \mathfrak{m}L = L$. So $M = L$ by (10.8)(1). Thus $N \subset M$. □

Exercise (10.29) . — Let R be a ring, $\mathfrak{m}$ an ideal, and $\alpha, \beta\colon M \rightrightarrows N$ two maps of finitely generated modules. Assume α is an isomorphism, $\mathfrak{m} \subset \operatorname{rad}(N)$, and $\beta(M) \subset \mathfrak{m}N$. Set $\gamma := \alpha + \beta$. Show γ is an isomorphism.

Solution: As α is surjective, given $n \in N$, there is $m \in M$ with $\alpha(m) = n$. So

$$n = \alpha(m) + \beta(m) - \beta(m) \in \gamma(M) + \mathfrak{m}N.$$

But $N/\gamma(M)$ is finitely generated as N is. Hence $\gamma(M) = N$ by (10.8)(1). So $\alpha^{-1}\gamma$ is surjective, and therefore an isomorphism by (10.4). Thus γ is an isomorphism. □

Exercise (10.30) . — Let $A \to B$ be a local homomorphism, M a finitely generated B-module. Prove that M is faithfully flat over A if and only if M is flat over A and nonzero. Conclude that, if B is flat over A, then B is faithfully flat over A.

Solution: Plainly, to prove the first assertion, it suffices to show that $M \otimes_A \bullet$ is faithful if and only if $M \neq 0$. Now, if $M \otimes_A \bullet$ is faithful, then $M \otimes N \neq 0$ whenever $N \neq 0$ by (9.19). But $M \otimes A = M$ by (8.5)(2), and $A \neq 0$. Thus $M \neq 0$.

Conversely, suppose $M \neq 0$. Denote the maximal ideals of A and B by $\mathfrak{m}$ and $\mathfrak{n}$. Then $\mathfrak{n}M \neq M$ by Nakayama's Lemma (10.6). But $\mathfrak{m}B \subset \mathfrak{n}$ as $A \to B$ is a local homomorphism. So $M/\mathfrak{m}M \neq 0$. But $M/\mathfrak{m}M = M \otimes (A/\mathfrak{m})$ by (8.27)(1). Thus (9.19) implies $M \otimes_A \bullet$ is faithful.

Finally, the second assertion is the special case with $M := B$. □

Exercise (10.31) . — Let $A \to B$ be a flat local homomorphism, M a finitely generated A-module. Set $N := M \otimes B$. Assume N is cyclic. Show M is cyclic too. Conclude that an ideal $\mathfrak{a}$ of A is principal if its extension $\mathfrak{a}B$ is so.

Solution: Let $\mathfrak{n}$ be the maximal ideal of B. Set $V := N/\mathfrak{n}N$. Suppose $V = 0$. Then $N = 0$ by Nakayama's Lemma (10.6). But B is faithfully flat over A by (10.30). So $M = 0$ by (9.28)(6). In particular, M is cyclic.

Suppose $V \neq 0$. Then, as the $m \otimes 1$ for $m \in M$ generate N over B, there's an m such that $m \otimes 1$ has nonzero image $v \in V$. But N is cyclic. So V is 1-dimensional. So v generates V. So $m \otimes 1$ generates N by (10.8)(2). Set $M' := mA$.

Form the standard short exact sequence $0 \to M' \xrightarrow{\iota} M \to M/M' \to 0$ where ι is the inclusion. As B is flat, tensoring with B yields the following exact sequence:

$$0 \to M' \otimes B \xrightarrow{\iota \otimes B} N \to (M/M') \otimes B \to 0.$$

But $\iota \otimes B$ is surjective, as N is generated by $m \otimes 1$. Hence $(M/M') \otimes B = 0$. But B is faithfully flat. So $M/M' = 0$ by (9.28)(6). Thus M is cyclic.

The second assertion follows from the first, as $\mathfrak{a} \otimes B = \mathfrak{a}B$ by (9.15). □

Exercise (10.32) . — Let R be a ring, X a variable, R' an algebra, $n \geq 0$. Assume R' is a free R-module of rank n. Set $\mathfrak{m} := \operatorname{rad}(R)$ and $k := R/\mathfrak{m}$. Given a k-isomorphism $\widetilde{\varphi}\colon k[X]/\langle \widetilde{F} \rangle \xrightarrow{\sim} R'/\mathfrak{m}R'$ with $\widetilde{F}$ monic, show we can lift $\widetilde{\varphi}$ to an R-isomorphism $\varphi\colon R[X]/\langle F \rangle \xrightarrow{\sim} R'$ with F monic. Show F must then lift $\widetilde{F}$.

Solution: As R' is free of rank n over R, so is $R'/\mathfrak{m}R'$ over k. Let $\widetilde{x} \in R'/\mathfrak{m}R'$ be the image of X, and $x \in R$ a lift of $\widetilde{x}$. Then $1, \widetilde{x}, \ldots, \widetilde{x}^{n-1}$ generate $R'/\mathfrak{m}R'$ over k by **(10.15)**(1)⇒(4). So $1, x, \ldots, x^{n-1}$ generate R' over R by **(10.8)**(2). Thus **(10.5)** implies $1, x, \ldots, x^{n-1}$ form a free basis of R' over R.

Form the R-algebra map $\kappa\colon R[X] \to R'$ with $\kappa(X) = x$. As the x^i generate, κ is surjective. So $\operatorname{Ker}(\kappa)$ is generated by a monic polynomial F of degree n by **(10.15)**(4)⇒(1). Thus κ induces an R-isomorphism $\varphi\colon R[X]/\langle F\rangle \xrightarrow{\sim} R'$ lifting $\widetilde{\varphi}$.

Finally, let $\overline{F} \in k[X]$ be the residue of F. Then $\overline{F}$ is monic of degree n. Also, $k[X]/\langle\overline{F}\rangle = k[X]/\langle\widetilde{F}\rangle$. So $\langle\overline{F}\rangle = \langle\widetilde{F}\rangle$. So $\overline{F} = \widetilde{F}$. Thus F lifts $\widetilde{F}$. □

Exercise (10.33) . — Let R be a ring, $\mathfrak{a}$ an ideal, $P := R[X]$ the polynomial ring in one variable X, and $G_1, G_2, H \in P$ with G_1 monic of degree n. Show:

(1) Assume G_1 and G_2 are coprime. Then there are unique $H_1, H_2 \in P$ with $H = H_1G_1 + H_2G_2$ and $\deg(H_2) < n$.

(2) Assume the images of G_1 and G_2 are coprime in $(R/\mathfrak{a})[X]$ and $\mathfrak{a} \subset \operatorname{rad}(R)$. Then G_1 and G_2 are coprime.

Solution: Set $M := \sum_{i=0}^{n-1} RX^i \subset P$ and $R' := P/\langle G_1\rangle$. Let $\kappa\colon P \twoheadrightarrow R'$ be the canonical map. By (1)⇒(2) of **(10.15)**, κ induces an R-linear bijection $M \xrightarrow{\sim} R'$.

In (1), $\kappa(G_2) \in R'^{\times}$ by **(2.16)**. Hence $\kappa(H) = \kappa(H_2)\kappa(G_2)$ for a unique $H_2 \in M$. Hence there's $H_1 \in P$ with $H = H_1G_1 + H_2G_2$. If $H = H_1'G_1 + H_2G_2$ too, then $0 = (H_1 - H_1')G_1$. But G_1 is monic. So $H_1 - H_1' = 0$. Thus (1) holds.

In (2), the residue of G_2 is a unit in $R'/\mathfrak{a}R'$ by **(2.16)**. Hence $G_2R' + \mathfrak{a}R' = R'$. But R' is R-module finite as $M \xrightarrow{\sim} R'$. Also $\mathfrak{a} \subset \operatorname{rad}(R) \subset \operatorname{rad}_R(R')$. So $G_2R' = R'$ by **(10.8)**(1). So $\kappa(G_2) \in R'^{\times}$. Thus **(2.16)** yields (2). □

Exercise (10.34) . — Let R be a ring, $\mathfrak{a} \subset \operatorname{rad}(R)$ an ideal, $P := R[X]$ the polynomial ring in one variable X, and $F, G, H \in P$. Assume that $F \equiv GH \pmod{\mathfrak{a}P}$, that G and H are coprime, and that G is monic, say of degree n. Show that there are coprime polynomials $G', H' \in P$ with G' monic of degree n, with $\deg(H') \le \max\{\deg(H), \deg(F) - n\}$, and with

$$G \equiv G' \text{ and } H \equiv H' \pmod{\mathfrak{a}P} \quad\text{and}\quad F \equiv G'H' \pmod{\mathfrak{a}^2P}.$$

Solution: Note **(10.33)**(1) yields (unique) $A, B \in P$ with $F - GH = AG + BH$ and $\deg(B) < n$. Then $AG + BH \equiv 0 \pmod{\mathfrak{a}P}$. But the residues of G and H in $P/\mathfrak{a}P$ are coprime; see **(2.16)**. Also, the residue of G is monic of degree n. Thus the uniqueness statement in **(10.33)**(1) yields $A, B \equiv 0 \pmod{\mathfrak{a}P}$.

Set $G' := G + B$ and $H' := H + A$. Then $F - G'H' = -AB$. Thus $F \equiv G'H' \pmod{\mathfrak{a}^2P}$. Also, G' is monic of degree n, as G is so and $\deg(B) < n$.

The residues of G' and H' in $P/\mathfrak{a}P$ are the same as those of G and H. But G and H are coprime, and $\mathfrak{a} \subset \operatorname{rad}(R)$. Thus **(10.33)**(2) implies G' and H' are coprime.

Finally, assume $\deg(H') > \deg(H)$. Then $\deg(H') = \deg(A)$ as $H' := H + A$. But $F - G'H' = -AB$. Also $\deg(AB) \le \deg(A) + \deg(B) < \deg(H') + n$, and $\deg(G'H') = n + \deg(H')$ as G' is monic of degree n. Hence $\deg(F) = \deg(G'H')$. Thus $\deg(H') \le \max\{\deg(H), \deg(F) - n\}$. □

Exercise (10.35) . — Let G be a finite group acting on a ring R. Show that every $x \in R$ is integral over R^G, in fact, over its subring R' generated by the elementary symmetric functions in the conjugates gx for $g \in G$.

Solution: Given an $x \in R$, form $F(X) := \prod_{g\in G}(X - gx)$. The coefficients of $F(X)$ are the elementary symmetric functions in the conjugates gx for $g \in G$. Thus $F(x) = 0$ is an equation of integral dependence for x over R', so also over R^G. □

Exercise (10.36) . — Let R be a ring, R' an algebra, G a group that acts on R'/R, and $\overline{R}$ the integral closure of R in R'. Show that G acts canonically on $\overline{R}/R$.

Solution: Given $x \in \overline{R}$, say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in R$. Given $g \in G$, then $ga_i = a_i$. So $gx^n + a_1gx^{n-1} + \cdots + a_n = 0$. So $gx \in \overline{R}$. Thus $g\overline{R} \subset \overline{R}$. Similarly, $g^{-1}\overline{R} \subset \overline{R}$. So $\overline{R} \subset g\overline{R}$. So $g\overline{R} = \overline{R}$. Thus G acts on $\overline{R}/R$. □

Exercise (10.37) . — Let R be a normal domain, K its fraction field, L/K a **Galois extension** with group G, and $\overline{R}$ the integral closure of R in L. (By definition, G is the group of automorphisms of L/K and $K = L^G$.) Show $R = \overline{R}^G$.

Solution: As G is the group of automorphisms of L/K, it acts on L/R. So G acts canonically on $\overline{R}/R$ by (10.36). So $\overline{R}^G$ is an R-algebra. Thus $R \subset \overline{R}^G$.

Conversely, given $x \in \overline{R}^G$, also $x \in K$, as $K = L^G$ by definition of Galois extension with group G. But x is in $\overline{R}$; so x is integral over R. But R is normal. So $x \in R$. Thus $R \supset \overline{R}^G$. Thus $R = R'^G$. □

Exercise (10.38) . — Let R'/R be an extension of rings. Assume $R' - R$ is closed under multiplication. Show that R is integrally closed in R'.

Solution: By way of contradiction, suppose there's $x \in R' - R$ integral over R. Say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in R$ and n minimal. Then $n > 1$ as $x \notin R$. Set $y := x^{n-1} + \cdots + a_{n-1}$. Then $y \notin R$; else, $x^{n-1} + \cdots + (a_{n-1} - y) = 0$, contradicting minimality. But $xy = -a_n \in R$. Thus $R' - R$ is not closed under multiplication, a contradiction. □

Exercise (10.39) . — Let R be a ring; C, R' two R-algebras; R'' an R'-algebra. If R'' is either (1) integral over R', or (2) module finite over R', or (3) algebra finite over R', show $R'' \otimes_R C$ is so over $R' \otimes_R C$.

Solution: For (1), given $x \in R''$, say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in R'$. Further, given $c \in C$, note $x \otimes c$ is integral over $R' \otimes C$, because

$$\begin{aligned}(x\otimes c)^n + (a_1\otimes c)(x\otimes c)^{n-1} + \cdots + (a_n\otimes c^n)\\ = (x^n + a_1x^{n-1} + \cdots + a_n)\otimes c^n = 0.\end{aligned}$$

But every element of $R'' \otimes C$ is a sum of elements of the form $x \otimes c$. Thus (10.20) implies that $R'' \otimes C$ is integral over $R' \otimes C$.

For (2), say $x_1, \ldots, x_n$ generate R'' as an R'-module. Given $x \in R''$, write $x = \sum a_ix_i$ with $a_i \in R'$. Then $x \otimes c = \sum (a_i \otimes c)(x_i \otimes 1)$. But every element of $R'' \otimes C$ is a sum of elements of the form $x \otimes c$. Thus the $x_i \otimes 1$ generate $R'' \otimes C$ as an $R' \otimes C$-module.

For (3), argue as for (2), but use algebra generators and polynomials in them. □

Exercise (10.40) . — Let k be a field, $P := k[X]$ the polynomial ring in one variable, $F \in P$. Set $R := k[X^2] \subset P$. Using the free basis $1, X$ of P over R, find an explicit equation of integral dependence of degree 2 on R for F.

Solution: Write $F = F_e + F_o$, where F_e and F_o are the polynomials formed by the terms of F of even and odd degrees. Say $F_o = Gx$. Then the matrix of μ_F is $\left(\begin{smallmatrix} F_e & Gx^2 \\ G & F_e \end{smallmatrix}\right)$. Its characteristic polynomial is $T^2 - 2F_eT + F_e^2 - F_o^2$. So the Cayley–Hamilton Theorem (**10.1**) yields $F^2 - 2F_eF + F_e^2 - F_o^2 = 0$. □

Exercise (10.41) . — Let $R_1, \ldots, R_n$ be R-algebras that are integral over R. Show that their product $\prod R_i$ is integral over R.

Solution: Let $y = (y_1, \ldots, y_n) \in \prod_{i=1}^n R_i$. Since R_i/R is integral, each $y_i \in R_i$ satisfies an equation of integral dependence on R. Plainly, the image of y_i in $\prod_{i=1}^n R_i$ satisfies the same equation. Hence $\prod_{i=1}^n R[y_i]$ is module-finite by (**10.14**). Now, $y \in \prod_{i=1}^n R[y_i]$. Therefore, y is integral over R by (**10.18**). Thus $\prod_{i=1}^n R_i$ is integral over R. □

Exercise (10.42) . — For $1 \le i \le r$, let R_i be a ring, R_i' an extension of R_i, and $x_i \in R_i'$. Set $R := \prod R_i$, set $R' := \prod R_i'$, and set $x := (x_1, \ldots, x_r)$. Prove

(1) x is integral over R if and only if x_i is integral over R_i for each i;

(2) R is integrally closed in R' if and only if each R_i is integrally closed in R_i'.

Solution: Assume x is integral over R. Say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_j \in R$. Say $a_j =: (a_{1j}, \ldots, a_{rj})$. Fix i. Then $x_i^n + a_{i1}x^{n-1} + \cdots + a_{in} = 0$. So x_i is integral over R_i.

Conversely, assume each x_i is integral over R_i. Say $x_i^{n_i} + a_{i1}x_i^{n_i-1} + \cdots + a_{in_i} = 0$. Set $n := \max n_i$, set $a_{ij} := 0$ for $j > n_i$, and set $a_j := (a_{1j}, \ldots, a_{rj}) \in R$ for each j. Then $x^n + a_1x^{n-1} + \cdots + a_n = 0$. Thus x is integral over R. Thus (1) holds.

Assertion (2) is an immediate consequence of (1). □

Exercise (10.43) . — Let k be a field, X and Y variables. Set

$$R := k[X, Y]/\langle Y^2 - X^2 - X^3\rangle,$$

and let $x, y \in R$ be the residues of X, Y. Prove that R is a domain, but not a field. Set $t := y/x \in \operatorname{Frac}(R)$. Prove that $k[t]$ is the integral closure of R in $\operatorname{Frac}(R)$.

Solution: As $k[X, Y]$ is a UFD and $Y^2 - X^2 - X^3$ is irreducible, $\langle Y^2 - X^2 - X^3\rangle$ is prime by (**2.5**); however, it is not maximal by (**2.40**). Hence R is a domain by (**2.8**), but not a field by (**2.13**).

Note $y^2 - x^2 - x^3 = 0$. Hence $x = t^2 - 1$ and $y = t^3 - t$. So $k[t] \supset k[x, y] = R$. Further, t is integral over R; so $k[t]$ is integral over R by (2)⇒(1) of (**10.18**).

Finally, $k[t]$ has $\operatorname{Frac}(R)$ as fraction field. Further, $\operatorname{Frac}(R) \ne R$, so x and y cannot be algebraic over k; hence, t must be transcendental. So $k[t]$ is normal by (**10.22**)(1). Thus $k[t]$ is the integral closure of R in $\operatorname{Frac}(R)$. □

11. Localization of Rings

Exercise (11.5) . — Let R' and R'' be rings. Consider $R := R' \times R''$ and set $S := \{ (1,1),\ (1,0) \}$. Prove $R' = S^{-1}R$.

Solution: Let's show that the projection map $\pi\colon R' \times R'' \to R'$ has the UMP of (11.3). First, note that $\pi S = \{1\} \subset R'^{\times}$. Let $\psi\colon R' \times R'' \to B$ be a ring map such that $\psi(1,0) \in B^{\times}$. Then in B,

$$\psi(1,0) \cdot \psi(0,x) = \psi\big((1,0)\cdot(0,x)\big) = \psi(0,0) = 0 \text{ in } B.$$

Hence $\psi(0,x) = 0$ for all $x \in R''$. So ψ factors uniquely through π by (1.5). □

Exercise (11.19) . — Let R be a ring, S a multiplicative subset. Prove $S^{-1}R = 0$ if and only if S contains a nilpotent element.

Solution: By (1.1), $S^{-1}R = 0$ if and only if $1/1 = 0/1$. But by construction, $1/1 = 0/1$ if and only if $0 \in S$. Finally, since S is multiplicative, $0 \in S$ if and only if S contains a nilpotent element. □

Exercise (11.20) . — Find all intermediate rings $\mathbb{Z} \subset R \subset \mathbb{Q}$, and describe each R as a localization of $\mathbb{Z}$. As a starter, prove $\mathbb{Z}[2/3] = S_3^{-1}\mathbb{Z}$ where $S_3 := \{3^i \mid i \ge 0\}$.

Solution: Clearly $\mathbb{Z}[2/3] \subset \mathbb{Z}[1/3]$ as $2/3 = 2\cdot(1/3)$. But the opposite inclusion holds as $1/3 = 1-(2/3)$. Clearly $S_3^{-1}\mathbb{Z} = \mathbb{Z}[1/3]$.

Let $P \subset \mathbb{Z}$ be the set of all prime numbers that appear as factors of the denominators of elements of R in lowest terms; recall that $x = r/s \in \mathbb{Q}$ is in **lowest terms** if r and s have no common prime divisor. Let S denote the multiplicative subset **generated by** P, that is, the smallest multiplicative subset containing P. Clearly, S is equal to the set of all products of elements of P.

First note that, if $p \in P$, then $1/p \in R$. Indeed, take an element $x = r/ps \in R$ in lowest terms. Then $sx = r/p \in R$. Also the Euclidean algorithm yields $m, n \in \mathbb{Z}$ such that $mp + nr = 1$. Then $1/p = m + nsx \in R$, as desired. Hence $S^{-1}\mathbb{Z} \subset R$. But the opposite inclusion holds because, by the very definition of S, every element of R is of the form r/s for some $s \in S$. Thus $S^{-1}\mathbb{Z} = R$. □

Exercise (11.21) . — Take R and S as in (11.5). On $R \times S$, impose this relation:

$$(x,s) \sim (y,t) \quad \text{if} \quad xt = ys.$$

Prove that it is not an equivalence relation.

Solution: Observe that, for any $z \in R''$, we have

$$\big((1,z),\ (1,1)\big) \sim \big((1,0),\ (1,0)\big).$$

However, if $z \ne 0$, then

$$\big((1,z),\ (1,1)\big) \not\sim \big((1,0),\ (1,1)\big).$$

Thus although $\sim$ is reflexive and symmetric, it is *not* transitive if $R'' \ne 0$. □

Exercise (11.22) . — Let R be a ring, S a multiplicative subset, G be a group acting on R, Assume $g(S) \subset S$ for all $g \in G$. Set $S^G := S \cap R^G$. Show:

(1) The group G acts canonically on $S^{-1}R$.

(2) If G is finite, there's a canonical isomorphism $\rho\colon (S^G)^{-1}R^G \xrightarrow{\sim} (S^{-1}R)^G$.

Solution: For (1), given $g \in G$, note $\varphi_S g(S) \subset (S^{-1}R)^\times$ as $g(S) \subset S$. So g induces a map $S^{-1}(g)\colon S^{-1}R \to S^{-1}R$ by (**11.3**). By naturality, $S^{-1}(g^{-1})$ is an inverse. Thus (1) holds.

For (2), note $\varphi_S(S^G) \subset (S^{-1}R)^\times$ as $S^G \subset S$. So $(\varphi_S|R^G)\colon R^G \to S^{-1}R$ induces a map $\rho\colon (S^G)^{-1}R^G \to S^{-1}R$ by (**11.3**). Assume G is finite. Let's show ρ works.

First, given $x \in R^G$ and $s \in S^G$, suppose $\rho(x/s) = 0$. Then there's $t \in S$ with $tx = 0$ in R. Set $t' := \prod_{g\in G} g(t)$. Then $t'x = 0$. And $t' \in R^G$, so $t' \in S^G$. So $x/s = 0$ in $(S^G)^{-1}R^G$. Thus ρ is injective.

Second, given $x \in R^G$ and $s \in S^G$ and $g \in G$, note $g\rho(x/s) = \rho\big(g(x)/g(s)\big)$. But $g(x) = x$ and $g(s) = s$. So $g\rho(x/s) = \rho(x/s)$. Thus $\mathrm{Im}(\rho) \subset (S^{-1}R)^G$.

Conversely, given $y/t \in (S^{-1}R)^G$, set $t' := \prod_{g\neq 1} g(t)$. Then $tt' \in S^G$ and $y/t = yt'/tt'$. Fix $g \in G$. Then $g(y/t) = g(yt')/g(tt')$. But $g(tt'') = tt'$. Also $g(y/t) = y/t$. So $g(yt')/tt' = yt'/tt'$. So there is $u_g \in S$ with $u_g(g(yt') - yt') = 0$.

Set $u := \prod_{g\in G} u_g$. Then $u(g(yt') - yt') = 0$ for all g. Set $u' := \prod_{g\in G} g(u)$. Then $u' \in S^G$, and $u'(g(yt') - yt') = 0$ for all g. So $u'yt' \in R^G$ and $\rho(u'yt'/u'tt') = y/t$. Thus $\mathrm{Im}(\rho) \supset (S^{-1}R)^G$. Thus $\mathrm{Im}(\rho) = (S^{-1}R)^G$. Thus (2) holds. □

Exercise (11.23) . — Let R be a ring, $S \subset T$ a multiplicative subsets, $\overline{S}$ and $\overline{T}$ their saturations; see (**3.25**). Set $U := (S^{-1}R)^\times$. Show the following:

(1) $U = \{\, x/s \mid x \in \overline{S} \text{ and } s \in S \,\}$. (2) $\varphi_S^{-1}U = \overline{S}$.
(3) $S^{-1}R = T^{-1}R$ if and only if $\overline{S} = \overline{T}$. (4) $\overline{S}^{-1}R = S^{-1}R$.

Solution: In (1), given $x \in \overline{S}$ and $s \in S$, take $y \in R$ such that $xy \in S$. Then $x/s \cdot sy/xy = 1$ in $S^{-1}R$. Thus $x/s \in U$. Conversely, say $x/s \cdot y/t = 1$ in $S^{-1}R$ with $x, y \in R$ and $s, t \in S$. Then there's $u \in S$ with $xyu = stu$ in R. But $stu \in S$. Thus $x \in \overline{S}$. Thus (1) holds.

For (2), set $V := \varphi_S^{-1}U$. Then V is saturated multiplicative by (**3.11**). Further, $V \supset S$ by (**11.1**). Thus (1)(c) of (**3.25**) yields $V \supset \overline{S}$. Conversely, take $x \in V$. Then $x/1 \in U$. So (1) yields $x/1 = y/s$ with $y \in \overline{S}$ and $s \in S$. So there's $t \in S$ with $xst = yt$ in R. But $\overline{S} \supset S$ by (1)(a) of (**3.25**), and $\overline{S}$ is multiplicative by (1)(b) of (**3.25**); so $yt \in \overline{S}$. But $\overline{S}$ is saturated again by (1)(b). Thus $x \in \overline{S}$. Thus $V = \overline{S}$.

In (3), if $S^{-1}R = T^{-1}R$, then (2) implies $\overline{S} = \overline{T}$. Conversely, if $\overline{S} = \overline{T}$, then (4) implies $S^{-1}R = T^{-1}R$.

As to (4), note that, in any ring, a product is a unit if and only if each factor is. So a ring map $\varphi\colon R \to R'$ carries $\overline{S}$ into $R'^\times$ if and only if φ carries S into $R'^\times$. Thus $\overline{S}^{-1}R$ and $S^{-1}R$ are characterized by equivalent UMPs. Thus (4) holds. □

Exercise (11.24) . — Let R be a ring, $S \subset T \subset U$ and W multiplicative subsets.

(1) Show there's a unique R-algebra map $\varphi_T^S\colon S^{-1}R \to T^{-1}R$ and $\varphi_U^T\varphi_T^S = \varphi_U^S$.

(2) Given a map $\varphi\colon S^{-1}R \to W^{-1}R$, show $S \subset \overline{S} \subset \overline{W}$ and $\varphi = \varphi_{\overline{W}}^S$.

Solution: For (1), note $\varphi_T S \subset \varphi_T T \subset (T^{-1}R)^\times$. So (**11.3**) yields a unique R-algebra map $\varphi_T^S\colon S^{-1}R \to T^{-1}R$. By uniqueness, $\varphi_U^T\varphi_T^S = \varphi_U^S$, as desired.

For (2), note $\varphi(S^{-1}R)^\times \subset (W^{-1}R)^\times$. So $\varphi_S^{-1}(S^{-1}R)^\times \subset \varphi_W^{-1}(W^{-1}R)^\times$. But $\varphi_S^{-1}(S^{-1}R)^\times = \overline{S}$ and $\varphi_W^{-1}(W^{-1}R)^\times = \overline{W}$ by (**11.23**)(2). Also $S \subset \overline{S}$ by (**3.25**)(1)(a), as desired. □

Exercise (11.25) . — Let $R = \varinjlim R_\lambda$ be a filtered direct limit of rings with transitions maps $\varphi^\lambda_\mu\colon R_\lambda \to R_\mu$ and insertions $\varphi_\mu\colon R_\mu \to R$. For all λ, let $S_\lambda \subset R_\lambda$ be a multiplicative subset. For all φ^λ_μ, assume $\varphi^\lambda_\mu(S_\lambda) \subset S_\mu$. Set $S := \bigcup \varphi_\lambda S_\lambda$. Then $\varinjlim S_\lambda^{-1}R_\lambda = S^{-1}R$.

Solution: Owing to the UMP of localization (11.3), the maps φ^λ_μ and φ_μ induce unique maps ψ^λ_μ and ψ_μ such that the following two squares are commutative:

$$\begin{tikzcd}
R_\lambda \arrow[r, "\varphi^\lambda_\mu"] \arrow[d, "\varphi_{S_\lambda}"'] & R_\mu \arrow[r, "\varphi_\mu"] \arrow[d, "\varphi_{S_\mu}"] & R \arrow[d, "\varphi_S"] \\
S_\lambda^{-1}R_\lambda \arrow[r, "\psi^\lambda_\mu"] & S_\mu^{-1}R_\mu \arrow[r, "\psi_\mu"] & S^{-1}R
\end{tikzcd}$$

Owing to uniquenss, $\psi_\mu\psi^\lambda_\mu = \psi_\lambda$ as $\varphi_\mu\varphi^\lambda_\mu = \varphi_\lambda$. Similarly, $\psi^\mu_\nu\psi^\lambda_\mu = \psi^\lambda_\nu$ for all ψ^μ_ν.

Let's show that $S^{-1}R$ has the UMP characterizing $\varinjlim S_\lambda^{-1}R_\lambda$. Fix a ring R' and ring maps $\theta_\mu\colon S_\mu^{-1}R_\mu \to R'$ with $\theta_\mu\psi^\lambda_\mu = \theta_\lambda$ for all ψ^λ_μ. Set $\rho_\mu := \theta_\mu\varphi_{S_\mu}$ for all μ.

The $\rho_\mu\colon R_\mu \to R'$ induce a unique ring map $\rho\colon R \to R'$ with $\rho\varphi_\mu = \rho_\mu$. Now, given $s \in S$, say $s = \varphi_\mu(s_\mu)$ with $s_\mu \in S_\mu$. Then $\varphi_{S_\mu}(s_\mu)$ is a unit. So $\theta_\mu\varphi_{S_\mu}(s_\mu)$ is a unit. But $\rho_\mu := \theta_\mu\varphi_{S_\mu}$ and $\rho_\mu(s_\mu) = \rho(s)$. Thus the UMP of localization (11.3) yields a unique map $\theta\colon S^{-1}R \to R'$ with $\theta\varphi_S = \rho$.

So $\theta\varphi_S\varphi_\mu = \rho_\mu$. But $\varphi_S\varphi_\mu = \psi_\mu\varphi_{S_\mu}$. So $\theta\psi_\mu\varphi_{S_\mu} = \rho_\mu$. But $\theta_\mu\varphi_{S_\mu} =: \rho_\mu$ and ρ_μ factors uniquely via φ_{S_μ}. Thus $\theta\psi_\mu = \theta_\mu$, as desired. □

Exercise (11.26) . — Let R be a ring, S_0 the set of nonzerodivisors. Show:

(1) Then S_0 is the largest multiplicative subset S with $\varphi_S\colon R \to S^{-1}R$ injective.
(2) Every element x/s of $S_0^{-1}R$ is either a zerodivisor or a unit.
(3) Suppose every element of R is either a zerodivisor or a unit. Then $R = S_0^{-1}R$.

Solution: For (1), recall φ_{S_0} is injective by (11.2). Conversely, let $s \in S$ and $x \in R$ with $sx = 0$. Then $\varphi_S(sx) = 0$. So $\varphi_S(s)\varphi_S(x) = 0$. But $\varphi_S(s)$ is a unit. So $\varphi_S(x) = 0$. But φ_S is injective. So $x = 0$. Thus $S \subset S_0$. Thus (1) holds.

For (2), take $x/s \in S_0^{-1}R$, and suppose it is a nonzerodivisor. Then $x/1$ is also a nonzerodivisor. Hence $x \in S_0$, for if $xy = 0$, then $x/1 \cdot y/1 = 0$, so $\varphi_{S_0}(y) = y/1 = 0$, so $y = 0$ as φ_{S_0} is injective. Hence x/s is a unit, as desired. Thus (2) holds.

In (3), by hypothesis, $S_0 \subset R^\times$. So $R \xrightarrow{\sim} S_0^{-1}R$ by (11.4). Thus (3) holds. □

Exercise (11.27) . — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Show: (1) if $\mathfrak{a} \subset \mathfrak{b}$, then $\mathfrak{a}^S \subset \mathfrak{b}^S$; (2) $(\mathfrak{a}^S)^S = \mathfrak{a}^S$; and (3) $(\mathfrak{a}^S\mathfrak{b}^S)^S = (\mathfrak{a}\mathfrak{b})^S$.

Solution: For (1), take $x \in \mathfrak{a}^S$. Then there is $s \in S$ with $sx \in \mathfrak{a}$. If $\mathfrak{a} \subset \mathfrak{b}$, then $sx \in \mathfrak{b}$, and so $x \in \mathfrak{b}^S$. Thus (1) holds.

To show (2), proceed by double inclusion. First, note $\mathfrak{a}^S \supset \mathfrak{a}$ by (11.10)(2). So $(\mathfrak{a}^S)^S \supset \mathfrak{a}^S$ again by (11.10)(2). Conversely, given $x \in (\mathfrak{a}^S)^S$, there is $s \in S$ with $sx \in \mathfrak{a}^S$. So there is $t \in S$ with $tsx \in a$. But $ts \in S$. So $x \in \mathfrak{a}^S$. Thus (2) holds.

To show (3), proceed by double inclusion. First, note $\mathfrak{a} \subset \mathfrak{a}^S$ and $\mathfrak{b} \subset \mathfrak{b}^S$ by (11.10)(2). So $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}^S\mathfrak{b}^S$. Thus (1) yields $(\mathfrak{a}\mathfrak{b})^S \subset (\mathfrak{a}^S\mathfrak{b}^S)^S$.

Conversely, given $x \in \mathfrak{a}^S\mathfrak{b}^S$, say $x := \sum y_iz_i$ with $y_i \in \mathfrak{a}^S$ and $z_i \in \mathfrak{b}^S$. Then there are $s_i, t_i \in S$ such that $s_iy_i \in \mathfrak{a}$ and $t_iz_i \in \mathfrak{b}$. Set $u := \prod s_it_i$. Then $u \in S$ and $ux \in \mathfrak{a}\mathfrak{b}$. So $x \in (\mathfrak{a}\mathfrak{b})^S$. Thus $\mathfrak{a}^S\mathfrak{b}^S \subset (\mathfrak{a}\mathfrak{b})^S$. So $(\mathfrak{a}^S\mathfrak{b}^S)^S \subset ((\mathfrak{a}\mathfrak{b})^S)^S$ by (1). But $((\mathfrak{a}\mathfrak{b})^S)^S = (\mathfrak{a}\mathfrak{b})^S$ by (2). Thus (3) holds. □

Exercise (11.28) . — Let R be a ring, S a multiplicative subset. Prove that

$$\mathrm{nil}(R)(S^{-1}R) = \mathrm{nil}(S^{-1}R).$$

Solution: Proceed by double inclusion. Given an element of $\mathrm{nil}(R)(S^{-1}R)$, put it in the form x/s with $x \in \mathrm{nil}(R)$ and $s \in S$ using **(11.8)**(1). Then $x^n = 0$ for some $n \geq 1$. So $(x/s)^n = 0$. So $x/s \in \mathrm{nil}(S^{-1}R)$. Thus $\mathrm{nil}(R)(S^{-1}R) \subset \mathrm{nil}(S^{-1}R)$.

Conversely, take $x/s \in \mathrm{nil}(S^{-1}R)$. Then $(x/s)^m = 0$ with $m \geq 1$. So there's $t \in S$ with $tx^m = 0$ by **(11.10)**(1). Then $(tx)^m = 0$. So $tx \in \mathrm{nil}(R)$. But $tx/ts = x/s$. So $x/s \in \mathrm{nil}(R)(S^{-1}R)$ by **(11.8)**(1). Thus $\mathrm{nil}(R)(S^{-1}R) \supset \mathrm{nil}(S^{-1}R)$. □

Exercise (11.29) . — Let R be a ring, S a multiplicative subset, R' an algebra. Assume R' is integral over R. Show $S^{-1}R'$ is integral over $S^{-1}R$.

Solution: Given $x/s \in S^{-1}R'$, let $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ be an equation of integral dependence of x on R. Then

$$(x/s)^n + (a_{n-1}/1)(1/s)(x/s)^{n-1} + \cdots + a_0(1/s)^n = 0$$

is an equation of integral dependence of x/s on $S^{-1}R$, as required. □

Exercise (11.30) . — Let R be a domain, K its fraction field, L a finite extension field, and $\overline{R}$ the integral closure of R in L. Show that L is the fraction field of $\overline{R}$. Show that, in fact, every element of L can be expressed as a fraction b/a where b is in $\overline{R}$ and a is in R.

Solution: Let $x \in L$. Then x is algebraic (integral) over K, say

$$x^n + y_1x^{n-1} + \cdots + y_n = 0$$

with $y_i \in K$. Write $y_i = a_i/a$ with $a_1, \ldots, a_n, a \in R$. Then

$$(ax)^n + a_1(ax)^{n-1} + \cdots + a^{n-1}a_0 = 0.$$

Set $b := ax$. Then $b \in \overline{R}$ and $x = b/a$. □

Exercise (11.31) . — Let $R \subset R'$ be domains, K and L their fraction fields. Assume that R' is a finitely generated R-algebra, and that L is a finite dimensional K-vector space. Find an $f \in R$ such that R'_f is module finite over R_f.

Solution: Let $x_1, \ldots, x_n$ generate R' over R. Using **(11.30)**, write $x_i = b_i/a_i$ with b_i integral over R and a_i in R. Set $f := \prod a_i$. The x_i generate R'_f as an R_f-algebra; so the b_i do too. Thus R'_f is module finite over R_f by **(10.18)**. □

Exercise (11.32) (*Localization and normalization commute*) . — Given a domain R and a multiplicative subset S with $0 \notin S$. Show that the localization of the normalization $S^{-1}\overline{R}$ is equal to the normalization of the localization $\overline{S^{-1}R}$.

Solution: Since $0 \notin S$, clearly $\mathrm{Frac}(S^{-1}R) = \mathrm{Frac}(R)$ owing to **(11.2)**. Now, $S^{-1}\overline{R}$ is integral over $S^{-1}R$ by **(11.29)**. Thus $S^{-1}\overline{R} \subset \overline{S^{-1}R}$.

Conversely, given $x \in \overline{S^{-1}R}$, consider an equation of integral dependence:

$$x^n + a_1x^{n-1} + \cdots + a_n = 0.$$

Say $a_i = b_i/s_i$ with $b_i \in R$ and $s_i \in S$; set $s := \prod s_i$. Multiplying by s^n yields

$$(sx)^n + sa_1(sx)^{n-1} + \cdots + s^na_n = 0.$$

Hence $sx \in \overline{R}$. So $x \in S^{-1}\overline{R}$. Thus $S^{-1}\overline{R} \supset \overline{S^{-1}R}$, as desired. □

Exercise (11.33) . — Let k be a field, A a local k-algebra with maximal ideal $\mathfrak{m}$. Assume that A is a localization of a k-algebra R and that $A/\mathfrak{m} = k$. Find a maximal ideal $\mathfrak{n}$ of R with $R_{\mathfrak{n}} = A$.

Solution: By hypothesis, $A = T^{-1}R$ for some multiplicative subset T of R. Take $\mathfrak{n} := \varphi_T^{-1}\mathfrak{m}$. Then $k \hookrightarrow R/\mathfrak{n} \hookrightarrow A/\mathfrak{m} = k$. Hence $R/\mathfrak{n} = A/\mathfrak{m}$. So $\mathfrak{n}$ is maximal. But, given any $t \in T$, note $\varphi_T(t) \in A^\times$ by (**11.1**). So $\varphi_T(t) \notin \mathfrak{m}$ by (**3.5**). Hence $T \subset R - \mathfrak{n}$. Thus (**11.16**) yields $R_{\mathfrak{n}} = A$, as desired. □

Exercise (11.34) . — Let R be a ring, S a multiplicative subset, $\mathcal{X} := \{X_\lambda\}$ a set of variables. Show $(S^{-1}R)[\mathcal{X}] = S^{-1}\big(R[\mathcal{X}]\big)$.

Solution: In spirit, the proof is like that of (**1.16**): the two rings are equal, as each is universal among R-algebras with distinguished elements x_λ and in which all $s \in S$ become units. □

Exercise (11.35) . — Let R be a ring, S a multiplicative subset, $\mathcal{X}$ a set of variables, $\mathfrak{p}$ an ideal of $R[\mathcal{X}]$. Set $R' := S^{-1}R$, and let $\varphi\colon R[\mathcal{X}] \to R'[\mathcal{X}]$ be the canonical map. Show $\mathfrak{p}$ is prime and $\mathfrak{p} \cap S = \emptyset$ if and only if $\mathfrak{p}R'[\mathcal{X}]$ is prime and $\mathfrak{p} = \varphi^{-1}\big(\mathfrak{p}R'[\mathcal{X}]\big)$.

Solution: The assertion results directly from (**11.34**) and (**11.12**)(2). □

12. Localization of Modules

Exercise (12.4) . — Let R be a ring, S a multiplicative subset, and M, N modules. Show: (1) If M, N are $S^{-1}R$-modules, then $\operatorname{Hom}_{S^{-1}R}(M,N) = \operatorname{Hom}_R(M,N)$.
(2) M is an $S^{-1}R$-module if and only if $M = S^{-1}M$.

Solution: In (1), note $\operatorname{Hom}_{S^{-1}R}(M,N) \subset \operatorname{Hom}_R(M,N)$. Let $\varphi \in \operatorname{Hom}_R(M,N)$, $s \in S$, $a \in R$, $m \in M$. Then $s\varphi((a/s)m) = \varphi(s(a/s)m) = \varphi(am) = a\varphi(m)$. Multiply by $1/s$; so $\varphi((a/s)m) = (a/s)\varphi(m)$. So φ is an $S^{-1}R$-map. So (1) holds.

For (2), first suppose M is an $S^{-1}R$-module. Every R-map $\varphi\colon M \to N$ is an $S^{-1}R$-map by (1). So M, equipped with 1_M, has the UMP that characterizes $S^{-1}M$; see (**12.3**). Thus $M = S^{-1}M$.

Conversely, if $M = S^{-1}M$, then M is an $S^{-1}R$-module as $S^{-1}M$ is by (**12.2**). Thus (2) holds. □

Exercise (12.5) . — Let R be a ring, $S \subset T$ multiplicative subsets, M a module. Set $T' := \varphi_S(T) \subset S^{-1}R$. Show $T^{-1}M = T'^{-1}(S^{-1}M)$.

Solution: Set $\varphi := \varphi_{T'}\varphi_S$; so $\varphi\colon M \to T'^{-1}(S^{-1}M)$. Let's check $T'^{-1}(S^{-1}M)$, equipped with φ, has the UMP characterizing $T^{-1}M$; see (**12.3**).

Let P be an $S^{-1}R$-module. Given $t \in T$, set $t' := \varphi_S(t)$. Then $\mu_t = \mu_{t'}$ on P. So (**12.1**) implies P is a $T^{-1}R$-module if and only if P is a $T'^{-1}R$-module. In particular, $T'^{-1}(S^{-1}M)$ is a $T^{-1}R$-module.

Let N be a $T^{-1}R$-module, $\psi\colon M \to N$ an R-map. Then μ_s is bijective on N for all $s \in S \subset T$ by (**12.1**). So N is an $S^{-1}R$-module by (**12.1**) again. So by (**12.3**), there's $\sigma\colon S^{-1}M \to N$ with $\sigma\varphi_S = \psi$, and σ is unique among R-maps. Similarly, there's $\tau\colon T'^{-1}(S^{-1}M) \to N$ with $\tau\varphi_{T'} = \sigma$, and τ is unique among R-maps. Then (**12.4**)(1) implies τ is a $T^{-1}R$-map. Moreover, $\tau\varphi = \psi$.

Given an R-map $\tau'\colon T'^{-1}(S^{-1}M) \to N$ with $\tau'\varphi = \psi$, it remains to show $\tau' = \tau$. Set $\sigma' := \tau'\varphi_T$. Then $\sigma'\varphi_S = \psi$. So the above uniqueness of σ gives $\sigma' = \sigma$. So $\sigma = \tau'\varphi_T$. So the above uniqueness of τ gives $\tau' = \tau$, as desired. □

Exercise (12.6) . — Let R be a ring, S a multiplicative subset. Show that S becomes a filtered category when equipped as follows: given $s, t \in S$, set

$$\operatorname{Hom}(s,t) := \{x \in R \mid xs = t\}.$$

Given a module M, define a functor $S \to ((R\text{-mod}))$ as follows: for $s \in S$, set $M_s := M$; to each $x \in \operatorname{Hom}(s,t)$, associate $\mu_x \colon M_s \to M_t$. Define $\beta_s \colon M_s \to S^{-1}M$ by $\beta_s(m) := m/s$. Show the β_s induce an isomorphism $\varinjlim M_s \xrightarrow{\sim} S^{-1}M$.

Solution: Clearly, S is a category. Now, given $s, t \in S$, set $u := st$. Then $u \in S$; also $t \in \operatorname{Hom}(s,u)$ and $s \in \operatorname{Hom}(t,u)$. Given $x, y \in \operatorname{Hom}(s,t)$, we have $xs = t$ and $ys = t$. So $s \in \operatorname{Hom}(t,u)$ and $xs = ys$ in $\operatorname{Hom}(s,u)$. Thus S is filtered.

Further, given $x \in \operatorname{Hom}(s,t)$, we have $\beta_t\mu_x = \beta_s$ since $m/s = xm/t$ as $xs = t$. So the β_s induce a homomorphism $\beta \colon \varinjlim M_s \to S^{-1}M$. Now, every element of $S^{-1}M$ is of the form m/s, and $m/s =: \beta_s(m)$; hence, β is surjective.

Each $m \in \varinjlim M_s$ lifts to an $m' \in M_s$ for some $s \in S$ by (7.5)(1). Assume $\beta m = 0$. Then $\beta_s m' = 0$ as the β_s induce β. But $\beta_s m' = m'/s$. So there is $t \in S$ with $tm' = 0$. So $\mu_t m' = 0$ in M_{st}, and $\mu_t m' \mapsto m$. So $m = 0$. Thus β is injective, so an isomorphism. □

Exercise (12.17) . — Let R be a ring, S a multiplicative subset, M a module. Show: (1) $S^{-1}\operatorname{Ann}(M) \subset \operatorname{Ann}(S^{-1}M)$, with equality if M is finitely generated;
(2) $S^{-1}M = 0$ if $\operatorname{Ann}(M) \cap S \neq \emptyset$, and conversely if M is finitely generated.

Solution: First off, (1) results from (9.34) owing to (12.10) and (12.13).

Alternatively, here's a direct proof of (1). Given $x \in \operatorname{Ann}(M)$ and $m \in M$ and $s, t \in S$, note $x/s \cdot m/t$ is 0. Thus $S^{-1}\operatorname{Ann}(M) \subset \operatorname{Ann}(S^{-1}M)$.

Conversely, say $m_1, \dots m_n$ generate M. Given $x \in R$ and $s \in S$ such that $x/s \in \operatorname{Ann}(S^{-1}M)$, note $x/s \cdot m_i/1 = 0$ for all i. So there's $t_i \in S$ with $t_i x m_i = 0$. Set $t = \prod t_i$. Then $txM = 0$. So $tx \in \operatorname{Ann}(M)$. But $tx/ts = x/s$. Thus $x/s \in S^{-1}\operatorname{Ann}(M)$. Thus $\operatorname{Ann}(S^{-1}M) \subset S^{-1}\operatorname{Ann}(M)$. Thus (1) holds.

For (2), note $\operatorname{Ann}(M) \cap S \neq \emptyset$ if and only if $S^{-1}\operatorname{Ann}(M) = S^{-1}R$ by (11.8)(2). But $\operatorname{Ann}(S^{-1}M) = S^{-1}R$ if and only if $S^{-1}M = 0$. Thus (1) yields (2). □

Exercise (12.24) . — Let R be a ring, M a module, and S, T multiplicative subsets.
(1) Set $U := ST := \{st \in R \mid s \in S \text{ and } t \in T\}$. Show $U^{-1}M = T^{-1}(S^{-1}M)$.
(2) Assume $S \subset T$. Show $T^{-1}M = T^{-1}(S^{-1}M)$.

Solution: Do (1) much like (12.5). Set $\varphi := \varphi_T\varphi_S$; so $\varphi \colon M \to T^{-1}(S^{-1}M)$. Let's check $T^{-1}(S^{-1}M)$, with φ, has the UMP characterizing $U^{-1}M$; see (12.3).

Given $s \in S$ and $t \in T$, note $\mu_{st} = \mu_s\mu_t$ on $T^{-1}(S^{-1}M)$. Hence μ_{st} is bijective. Thus (12.1) implies $T^{-1}(S^{-1}M)$ is a $U^{-1}R$-module. Trivially, φ is an R-map.

Let N be a $U^{-1}R$-module, and $\psi \colon M \to N$ an R-map. Now, $1 \in T$ and $1 \in S$; so $s, t \in U$. So μ_s and μ_t are both bijective on N by (12.1). Thus by (12.1) again, N is both an $S^{-1}R$-module and a $T^{-1}R$-module.

Hence by (12.3), there's $\sigma \colon S^{-1}M \to N$ with $\sigma\varphi_S = \psi$, and σ is unique among R-maps. Similarly, there's $\tau \colon T^{-1}(S^{-1}M) \to N$ with $\tau\varphi_T = \sigma$, and τ is unique among R-maps. Then τ is a $U^{-1}R$-map by (12.4)(1). Moreover, $\tau\varphi = \psi$.

Given an R-map $\tau' \colon T^{-1}(S^{-1}M) \to N$ with $\tau'\varphi = \psi$, it remains to show $\tau' = \tau$. Set $\sigma' := \tau'\varphi_{T'}$. Then $\sigma'\varphi_S = \psi$. So the above uniqueness of σ gives $\sigma' = \sigma$. So $\sigma = \tau'\varphi_{T'}$. So the above uniqueness of τ gives $\tau' = \tau$, as desired.

Note (2) is a special case of (1), because $T = ST$ as $1 \in S$. □

Exercise (12.25) . — Let R be a ring, S a multiplicative subset, M a module. Show: (1) Let T' be a multiplicative subset of $S^{-1}R$; set $T := \varphi_S^{-1}(T')$; and assume $S \subset T$. Then $T^{-1}M = T'^{-1}(S^{-1}M)$.

(2) Let $\mathfrak{p}$ be a prime of R; assume $\mathfrak{p} \cap S = \emptyset$; and set $\mathfrak{P} := \mathfrak{p}S^{-1}R$. Then $M_{\mathfrak{p}} = (S^{-1}M)_{\mathfrak{p}} = (S^{-1}M)_{\mathfrak{P}}$.

(3) Let $\mathfrak{p} \subset \mathfrak{q}$ be primes of R. Set $\mathfrak{P} := \mathfrak{p}R_{\mathfrak{q}}$. Then $M_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{P}}$.

Solution: Do (1) much like (12.5). Set $\varphi := \varphi_{T'}\varphi_S$; so $\varphi\colon M \to T'^{-1}(S^{-1}M)$. Let's check $T'^{-1}(S^{-1}M)$, with φ, has the UMP characterizing $T^{-1}M$; see (12.3).

Given $t \in T$, set $t' := \varphi_S(t) \subset T'$. Then $\mu_t = \mu_{t'}$ on $T'^{-1}(S^{-1}M)$. So μ_t is bijective by (12.1). Thus by (12.1) again, $T'^{-1}(S^{-1}M)$ is a $T^{-1}R$-module.

Let N be a $T^{-1}R$-module, $\psi\colon M \to N$ an R-map. Then μ_s is bijective on N for all $s \in S \subset T$ by (12.1). So N is an $S^{-1}R$-module by (12.1) again. So by (12.3), there's $\sigma\colon S^{-1}M \to N$ with $\sigma\varphi_S = \psi$, and σ is unique among R-maps.

Given $t' \in T'$, say $t' = t/s$ with $t \in R$ and $s \in S \subset T$. Then $s/1 \in T'$. So $t/1 = (s/1)t' \in T'$. So $t \in T$. So μ_t and μ_s are both bijective on N by (12.1). But $\mu_{t'} = \mu_t\mu_{1/s}$. So $\mu_{t'}$ is bijective too. So N is an $T'^{-1}R$-module by (12.1) again. So by (12.3), there's $\tau\colon T'^{-1}(S^{-1}M) \to N$ with $\tau\varphi_{T'} = \sigma$, and τ is unique among R-maps. Then (12.4)(1) implies τ is a $T^{-1}R$-map. Moreover, $\tau\varphi = \psi$.

Given an R-map $\tau'\colon T'^{-1}(S^{-1}M) \to N$ with $\tau'\varphi = \psi$, it remains to show $\tau' = \tau$. Set $\sigma' := \tau'\varphi_T$. Then $\sigma'\varphi_S = \psi$. So the above uniqueness of σ gives $\sigma' = \sigma$. So $\sigma = \tau'\varphi_T$. So the above uniqueness of τ gives $\tau' = \tau$, as desired. Thus (1) holds.

For (2), note $\mathfrak{P}$ is prime by (11.12)(2); so $(S^{-1}M)_{\mathfrak{P}}$ makes sense. Next, take $T' := S^{-1}R - \mathfrak{P}$ in (1). Then $\mathfrak{p} = \varphi_S^{-1}\mathfrak{P}$ by (11.12)(2) again. So $T = R - \mathfrak{p}$. But $\mathfrak{p} \cap S = \emptyset$. So $S \subset T$. Thus (12.24)(2) and (1) imply (2).

To get (3) from (2), take $S := R - \mathfrak{q}$, and note $S^{-1}M = M_{\mathfrak{q}}$ and $S \cap \mathfrak{p} = \emptyset$. □

Exercise (12.26) . — Let R be a ring, S a multiplicative subset, $\varphi\colon R \to R'$ a map of rings, M' an R'-module. Set $S' := \varphi(S)$. Show $S'^{-1}M' = S^{-1}M'$ as R'-modules.

Solution: Recall that φ induces an R'-algebra isomrphism $S^{-1}R' \xrightarrow{\sim} S'^{-1}R'$; see (11.15.1). So $S^{-1}M'$ and $S'^{-1}M'$ have the same UMP, established in (12.3): both are universal among the modules over these two algebras equipped with an R-map from M. Thus $S'^{-1}M' = S^{-1}M'$ as R'-modules. □

Exercise (12.27) . — Let R be a ring, M a finitely generated module, $\mathfrak{a}$ an ideal.

(1) Set $S := 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ lies in the radical of $S^{-1}R$.

(2) Use (1), Nakayama's Lemma (10.6), and (12.17)(2), but not the determinant trick (10.2), to prove this part of (10.3): if $M = \mathfrak{a}M$, then $sM = 0$ for an $s \in S$.

Solution: For (1), use (3.2) as follows. Take $a/(1+b) \in S^{-1}\mathfrak{a}$ with $a, b \in \mathfrak{a}$. Then for $x \in R$ and $c \in \mathfrak{a}$, we have

$$1 + \big(a/(1+b)\big)\big(x/(1+c)\big) = \big(1 + (b + c + bc + ax)\big)/(1+b)(1+c).$$

The latter is a unit in $S^{-1}R$, as $b + c + bc + ax \in \mathfrak{a}$. So $a/(1+b) \in \operatorname{rad}(S^{-1}R)$ by (3.2), as desired.

For (2), assume $M = \mathfrak{a}M$. Then $S^{-1}M = S^{-1}\mathfrak{a}S^{-1}M$ by (12.2). So $S^{-1}M = 0$ by (1) and (10.6). So (12.17)(2) yields an $s \in S$ with $sM = 0$, as desired. □

Exercise (12.28) . — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal, M a module, N a submodule. Prove $(\mathfrak{a}N)^S = (\mathfrak{a}^S N^S)^S$.

Solution: Use double inclusion. First, trivially, $\mathfrak{a} \subset \mathfrak{a}^S$ and $N \subset N^S$. Hence, $\mathfrak{a}N \subset \mathfrak{a}^S N^S$. Thus (**12.12**)(5)(a) yields $(\mathfrak{a}N)^S \subset (\mathfrak{a}^S N^S)^S$.

Conversely, given $m \in \mathfrak{a}^S N^S$, say $m := \sum x_i m_i$ with $x_i \in \mathfrak{a}^S$ and $m_i \in N^S$. Say $s_i x_i \in \mathfrak{a}$ and $t_i m_i \in N$ for s_i, $t_i \in S$. Set $u := \prod s_i t_i$. Then $u \in S$ and $um \in \mathfrak{a}N$. So $m \in (\mathfrak{a}N)^S$. Thus $\mathfrak{a}^S N^S \subset (\mathfrak{a}N)^S$. So $(\mathfrak{a}^S N^S)^S \subset ((\mathfrak{a}N)^S)^S$ by (**12.12**)(5)(a). But $((\mathfrak{a}N)^S)^S = (\mathfrak{a}N)^S$ by (**12.12**)(4)(a) as $SS = S$. Thus $(\mathfrak{a}N)^S \supset (\mathfrak{a}^S N^S)^S$. □

Exercise (12.29) . — Let R be a ring, S a multiplicative subset, P a projective module. Then $S^{-1}P$ is a projective $S^{-1}R$-module.

Solution: By (**5.16**), there is a module K such that $F := K \oplus P$ is free. So (**12.9**) yields that $S^{-1}F = S^{-1}P \oplus S^{-1}K$ and that $S^{-1}F$ is free over $S^{-1}R$. Thus $S^{-1}P$ is a projective $S^{-1}R$-module again by (**5.16**). □

Exercise (12.30) . — Let R be a ring, S a multiplicative subset, M, N modules. Show $S^{-1}(M \otimes_R N) = S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} S^{-1}N = S^{-1}M \otimes_R S^{-1}N$.

Solution: By (**12.10**), $S^{-1}(M \otimes_R N) = S^{-1}R \otimes_R (M \otimes_R N)$. The latter is equal to $(S^{-1}R \otimes_R M) \otimes_R N$ by Associativity (**8.8**)(1). Again by (**12.10**), the latter is equal to $S^{-1}M \otimes_R N$. Thus the first equality holds.

By Cancellation (**8.9**)(1), $S^{-1}M \otimes_R N = S^{-1}M \otimes_{S^{-1}R} (S^{-1}R \otimes_R N)$, and the latter is equal to $S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ by (**12.10**). Thus the second equality holds.

Lastly by (**8.7**)(2), map $S^{-1}M \otimes_R S^{-1}N \to S^{-1}M \otimes_{S^{-1}R} S^{-1}N$ is surjective, and its kernel is generated by the elements $p := (xm/s) \otimes (n/1) - (m/1) \otimes (xn/s)$ with $m \in M$, $n \in N$, $x \in R$, and $s \in S$. But $p = 0$, because $sp = 0$, and μ_s is an isomorphism on the R-module $S^{-1}M \otimes_R S^{-1}N$. Thus the third equality holds. □

Exercise (12.31) . — Let R be a ring, S a multiplicative subset, $\mathcal{X}$ a set of variables, and M a module. Prove $(S^{-1}M)[\mathcal{X}] = S^{-1}(M[\mathcal{X}])$.

Solution: In spirit, the proof is like that of (**11.34**): the left side is a module over $(S^{-1}R)[\mathcal{X}]$, and the right side, over $S^{-1}\big(R[\mathcal{X}]\big)$, but the two rings are equal by (**11.34**); the two sides are equal, as each is universal among $(S^{-1}R)[\mathcal{X}]$-modules Q with a given R-map $M \to Q$, owing to (**12.3**) and (**4.18**)(1). □

Exercise (12.32) . — Let R be a ring, $\mathfrak{a}$ an ideal, S a multiplicative subset, $\mathcal{X}$ a set of variables. Set $R' := R/\mathfrak{a}$ and $P := R[\mathcal{X}]$. Let $T \subset P$ be a multiplicative subset, and assume $S \subset T$. Prove $T^{-1}P\big/\mathfrak{a}T^{-1}P = T^{-1}\big((S^{-1}R')[\mathcal{X}]\big)$.

Solution: Note $T^{-1}P\big/\mathfrak{a}T^{-1}P = T^{-1}(P/\mathfrak{a}P)$ by (**12.15**). But $P/\mathfrak{a}P = P'$ with $P' := R'[\mathcal{X}]$ by (**1.16**). Now, $T^{-1}P' = T^{-1}(S^{-1}P')$ by (**12.24**)(2). Furthermore, $S^{-1}P' = (S^{-1}R')[\mathcal{X}]$ by (**12.31**). Thus $T^{-1}P\big/\mathfrak{a}T^{-1}P = T^{-1}\big((S^{-1}R')[\mathcal{X}]\big)$. □

Exercise (12.33) . — Let R be a ring, S a multiplicative subset. For $i = 1, 2$, let $\varphi_i\colon R \to R_i$ be a ring map, $S_i \subset R_i$ a multiplicative subset with $\varphi_i S \subset S_i$, and M_i an R_i-module. Set $T := \{s_1 \otimes s_2 \mid s_i \in S_i\} \subset R_1 \otimes_R R_2$. Prove

$$S_1^{-1}M_1 \otimes_{S^{-1}R} S_2^{-1}M_2 = S_1^{-1}M_1 \otimes_R S_2^{-1}M_2 = T^{-1}(M_1 \otimes_R M_2).$$

Solution: Note that $S^{-1}S_i^{-1}M' = S_i^{-1}M'$ by (**12.4**)(2) since $\varphi_i S \subset S_i$. Thus (**12.30**) yields the first equality.

In $R_1 \otimes_R R_2$, form $T_1 := \{s_1 \otimes 1 \mid s_1 \in S_1\}$ and $T_2 := \{1 \otimes s_2 \mid s_2 \in S_2\}$. Then

(**12.26**)(2) and (**12.10**) and (**8.8**)(1) and again (**12.10**) yield

$$T_1^{-1}(M_1 \otimes_R M_2) = S_1^{-1}(M_1 \otimes_R M_2) = (S_1^{-1}R_1) \otimes_{R_1} (M_1 \otimes_R M_2)$$
$$= (S_1^{-1}R_1 \otimes_{R_1} M_1) \otimes_R M_2 = (S_1^{-1}M_1) \otimes_R M_2.$$

Similarly, $T_2^{-1}((S_1^{-1}M_1) \otimes_R M_2) = S_1^{-1}M_1 \otimes_R S_2^{-1}M_2$. Those two results yield

$$S_1^{-1}M_1 \otimes_R S_2^{-1}M_2 = T_2^{-1}(T_1^{-1}(M_1 \otimes_R M_2)). \tag{12.33.1}$$

Apply (**12.26**)(1), (2) to (**12.33.1**) to get the second desired equation:

$$S_1^{-1}M_1 \otimes_R S_2^{-1}M_2 = (T_2T_1)^{-1}(M_1 \otimes_R M_2) = T^{-1}(M_1 \otimes_R M_2). \qquad \square$$

Exercise (12.34) . — Let R be a ring, $\mathfrak{m}$ a maximal ideal, $n \ge 1$, and M a module. Show $M/\mathfrak{m}^n M = M_\mathfrak{m}/\mathfrak{m}^n M_\mathfrak{m}$.

Solution: Note that $R/\mathfrak{m}^n$ is a local ring with maximal ideal $\mathfrak{m}/\mathfrak{m}^n$. So the elements of $R - \mathfrak{m}$ become units in $R/\mathfrak{m}^n$. But $M/\mathfrak{m}^n M$ is an $R/\mathfrak{m}^n$-module. So any $s \in R - \mathfrak{m}$ induces a bijection μ_s on $M/\mathfrak{m}^n M$. Hence $M/\mathfrak{m}^n M$ has a compatible $R_\mathfrak{m}$-structure by (**12.1**). So $M/\mathfrak{m}^n M = (M/\mathfrak{m}^n M)_\mathfrak{m}$ by (**12.4**)(2). Moreover, (**12.15**) yields $(M/\mathfrak{m}^n M)_\mathfrak{m} = M_\mathfrak{m}/\mathfrak{m}^n M_\mathfrak{m}$. Thus $M/\mathfrak{m}^n M = M_\mathfrak{m}/\mathfrak{m}^n M_\mathfrak{m}$. $\square$

Exercise (12.35) . — Let k be a field. For $i = 1, 2$, let R_i be an algebra, and $\mathfrak{n}_i \subset R_i$ a maximal ideal with $R_i/\mathfrak{n}_i = k$. Let $\mathfrak{n} \subset R_1 \otimes_k R_2$ denote the ideal generated by $\mathfrak{n}_1$ and $\mathfrak{n}_2$. Set $A_i := (R_i)_{\mathfrak{n}_i}$ and $\mathfrak{m} := \mathfrak{n}(A_1 \otimes_k A_2)$. Prove that both $\mathfrak{n}$ and $\mathfrak{m}$ are maximal with k as residue field and that $(A_1 \otimes_k A_2)_\mathfrak{m} = (R_1 \otimes_k R_2)_\mathfrak{n}$.

Solution: First off, note that (**8.30**), the hypotheses, and (**8.5**)(2) yield

$$(R_1 \otimes_k R_2)/\mathfrak{n} = (R_1/\mathfrak{n}_1) \otimes_k (R_2/\mathfrak{n}_2) = k \otimes_k k = k.$$

But k is a field. Thus $\mathfrak{n}$ is maximal, as desired.

Second, set $\mathfrak{m}_i := \mathfrak{n}_i A_i$. Plainly, the $\mathfrak{m}_i$ generate $\mathfrak{m}$. Also, $A_i/\mathfrak{m}_i = R_i/\mathfrak{n}_i$ by (**12.16**). So as above, $\mathfrak{m}$ is maximal, and $A_1 \otimes A_2/\mathfrak{m} = k$, as desired.

Third, set $S_i := S_{\mathfrak{n}_i} := R_i - \mathfrak{n}_i$. Then $A_i := S_i^{-1}R_i$. So (**12.33**) yields

$$A_1 \otimes A_2 = (S_1 \otimes S_2)^{-1}(R_1 \otimes_k R_2). \tag{12.35.1}$$

Set $\varphi := \varphi_{S_1 \otimes S_2}$ and $T' := (A_1 \otimes_k A_2) - \mathfrak{m}$ and $T := (R_1 \otimes_k R_2) - \mathfrak{n}$. Then (**11.16**) yields $(A_1 \otimes_k A_2)_\mathfrak{m} = (R_1 \otimes_k R_2)_\mathfrak{n}$ provided (a) $T = \varphi^{-1}T'$ and (b) $\varphi(S_1 \otimes S_2) \subset T'$.

To check (a), note $\mathfrak{n} \subset \varphi^{-1}\mathfrak{m}$. But $\mathfrak{n}$ is maximal. So $\mathfrak{n} = \varphi^{-1}\mathfrak{m}$. Thus (a) holds.

To check (b), note that $\varphi(S_1 \otimes S_2)$ consists of units by (**11.1**). But $\mathfrak{m}$ is a proper ideal. Thus (**12.35.1**) yields (b), as desired. $\square$

Exercise (12.36) . — Let R be a ring, R' an algebra, S a multiplicative subset, M a finitely presented module. Prove these properties of the rth Fitting ideal:

$$F_r(M \otimes_R R') = F_r(M)R' \quad \text{and} \quad F_r(S^{-1}M) = F_r(M)S^{-1}R = S^{-1}F_r(M).$$

Solution: Let $R^n \xrightarrow{\alpha} R^m \to M \to 0$ be a presentation. Then, by (**8.10**),

$$(R')^n \xrightarrow{\alpha \otimes 1} (R')^m \to M \otimes_R R' \to 0$$

is a presentation. Further, the matrix $\mathbf{A}$ of α induces the matrix of $\alpha \otimes 1$. Thus

$$F_r(M \otimes_R R') = I_{m-r}(\mathbf{A})R' = F_r(M)R'.$$

For the last equalities, take $R' := S^{-1}R$. Then $F_r(S^{-1}M) = F_r(M)S^{-1}R$ by (**12.10**). Finally, $F_r(M)S^{-1}R = S^{-1}F_r(M)$ by (**12.2**). $\square$

Exercise (12.37) . — Let R be a ring, S a multiplicative subset. Prove this:

(1) Let $M_1 \xrightarrow{\alpha} M_2$ be a map of modules, which restricts to a map $N_1 \to N_2$ of submodules. Then $\alpha(N_1^S) \subset N_2^S$; that is, there is an induced map $N_1^S \to N_2^S$.

(2) Let $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3$ be a left exact sequence, which restricts to a left exact sequence $0 \to N_1 \to N_2 \to N_3$ of submodules. Then there is an induced left exact sequence of saturations: $0 \to N_1^S \to N_2^S \to N_3^S$.

Solution: For (1), take $m \in N_1^S$. Then there is $s \in S$ with $sm \in N_1$. So $\alpha(sm) \in N_2$. But $\alpha(sm) = s\alpha(m)$. Thus (1) holds.

In (2), $\alpha(N_1^S) \subset N_2^S$ and $\beta(N_2^S) \subset N_3^S$ by (1). Trivially, $\alpha|N_1^S$ is injective, and $\beta\alpha|N_1^S = 0$. Finally, given $m_2 \in \operatorname{Ker}(\beta|N_2^S)$, there is $s \in S$ with $sm_2 \in N_2$, and exactness yields $m_1 \in M_1$ with $\alpha(m_1) = m_2$. Then $\beta(sm_2) = s\beta(m_2) = 0$. So exactness yields $n_1 \in N_1$ with $\alpha(n_1) = sm_2$. Also $\alpha(sm_1) = s\alpha(m_1) = sm_2$. But α is injective. Hence $sm_1 = n_1$. So $m_1 \in N_1^S$, and $\alpha(m_1) = m_2$. Thus (2) holds. □

Exercise (12.38) . — Let R be a ring, M a module, and S a multiplicative subset. Set $T^S M := \langle 0 \rangle^S$. We call it the ***S*-torsion submodule of** M. Prove the following:

(1) $T^S(M/T^S M) = 0$. (2) $T^S M = \operatorname{Ker}(\varphi_S)$.

(3) Let $\alpha\colon M \to N$ be a map. Then $\alpha(T^S M) \subset T^S N$.

(4) Let $0 \to M' \to M \to M''$ be exact. Then so is $0 \to T^S M' \to T^S M \to T^S M''$.

(5) Let $S_1 \subset S$ be a multiplicative subset. Then $T^S(S_1^{-1}M) = S_1^{-1}(T^S M)$.

Solution: For (1), given an element of $T^S(M/T^S(M))$, let $m \in M$ represent it. Then there is $s \in S$ with $sm \in T^S(M)$. So there is $t \in S$ with $tsm = 0$. So $m \in T^S(M)$. Thus (1) holds. Assertion (2) holds by **(12.12)**(3)(a).

Assertions (3) and (4) follow from **(12.37)**(1) and (2).

For (5), given $m/s_1 \in S_1^{-1}T^S(M)$ with $s_1 \in S_1$ and $m \in T^S(M)$, take $s \in S$ with $sm = 0$. Then $sm/s_1 = 0$. So $m/s_1 \in T^S(S_1^{-1}M)$. Thus $S_1^{-1}T^S(M) \subset T^S(S_1^{-1}M)$.

For the opposite inclusion, given $m/s_1 \in T^S(S_1^{-1}M)$ with $m \in M$ and $s_1 \in S_1$, take t/t_1 with $t \in S$ and $t_1 \in S_1$ and $t/t_1 \cdot m/s_1 = 0$. Then $tm/1 = 0$. So there's $s' \in S_1$ with $s'tm = 0$ by **(12.12)**(3)(a). But $s't \in S$ as $S_1 \subset S$. So $m \in T^S(M)$. Thus $m/s_1 \in S_1^{-1}T^S(M)$. Thus (5) holds. □

Exercise (12.39) . — Set $R := \mathbb{Z}$ and $S := S_0 := Z - \langle 0 \rangle$. Set $M := \bigoplus_{n \ge 2} \mathbb{Z}/\langle n \rangle$ and $N := M$. Show that the map σ of **(12.19)** is not injective.

Solution: Given $m > 0$, set $e_n := (\delta_{in})$, and fix e_n for some $n > m$. Then $m \cdot e_n \neq 0$. Hence $\mu_R\colon R \to \operatorname{Hom}_R(M, M)$ is injective. But $S^{-1}M = 0$, as any $x \in M$ has only finitely many nonzero components; so $kx = 0$ for some nonzero integer k. So $\operatorname{Hom}(S^{-1}M, S^{-1}M) = 0$. Thus σ is not injective. □

Exercise (12.40) . — Let R be a ring, S a multiplicative subset, M a module. Show that $S^{-1}\operatorname{nil}(M) \subset \operatorname{nil}(S^{-1}M)$, with equality if M is finitely generated.

Solution: Given an element x/s of $S^{-1}\operatorname{nil}(M)$ with $x \in \operatorname{nil}(M)$ and $s \in S$, there's $n \ge 1$ with $x^n \in \operatorname{Ann}(M)$. So $x^n M = 0$. So $(x/s)^n S^{-1}M = 0$. So $x/s \in \operatorname{nil}(S^{-1}M)$. Thus $S^{-1}\operatorname{nil}(M) \subset \operatorname{nil}(S^{-1}M)$.

Assume M is finitely generated, say by $m_1, \dots, m_r$. Given $x/s \in \operatorname{nil}(S^{-1}M)$, there's $n \ge 1$ with $(x/s)^n \in \operatorname{Ann}(S^{-1}M)$. So $(x^n m_i)/s = 0$ for all i. So there's $t_i \in S$ with $t_i x^n m_i = 0$. Set $t := \prod t_i$. Then $(tx)^n m_i = 0$. So $tx \in \operatorname{nil}(M)$. Hence $x/s \in S^{-1}\operatorname{nil}(M)$. Thus $S^{-1}\operatorname{nil}(M) \supset \operatorname{nil}(S^{-1}M)$, as desired. □

Exercise (12.41) . — Let R be a ring, S a multiplicative subset, $\mathfrak{a}$ an ideal, M a module, and N a submodule. Set $\mathfrak{n} := \mathrm{nil}(M/N)$. Show:

(1) Then $\mathfrak{n} \cap S \neq \emptyset$ if and only if $\mathfrak{n}^S = R$.
(2) Assume $\mathfrak{n} \cap S \neq \emptyset$. Then $S^{-1}N = S^{-1}M$ and $N^S = M$.
(3) Then $\mathfrak{n}^S \subset \mathrm{nil}(M/N^S)$, with equality if M is finitely generated.

Solution: In (1), there's $s \in \mathfrak{n} \cap S$ if and only if there are $s \in S$ and $n \geq 1$ with $s^n M \subset N$, so if and only if $1 \in \mathfrak{n}^S$. Thus (1) holds.

In (2), given $s \in S \cap \mathfrak{n}$, there's $n \geq 1$ with $s^n M \subset N$. So $S^{-1}M \subset S^{-1}N$. Thus $S^{-1}M = S^{-1}N$. So $N^S = M$ by **(12.12)**(2)(a). Thus (2) holds.

In (3), given $x \in \mathfrak{n}^S$, there is $s \in S$ such that $sx \in \mathfrak{n}$. So there is $n \geq 1$ such that $(sx)^n M \subset N$. So $x^n M \subset N^S$. Hence $x \in \mathrm{nil}(M/N^S)$. Thus $\mathfrak{n}^S \subset \mathrm{nil}(M/N^S)$.

Assume $m_1, \ldots, m_r \in M$ generate. Given $x \in \mathrm{nil}(M/N^S)$, there is $n \geq 1$ such that $x^n M \subset N^S$. So there are $s_i \in S$ with $s_i x^n m_i \in N$. Set $s := \prod s_i$. Then $(sx)^n M \subset N$. So $sx \in \mathfrak{n}$. So $x \in \mathfrak{n}^S$. Thus $\mathfrak{n}^S \supset \mathrm{nil}(M/N^S)$. Thus (3) holds. □

Exercise (12.42) . — Let R be a ring, M a module, N, N' submodules. Show:

(1) $\sqrt{\mathrm{nil}(M)} = \mathrm{nil}(M)$.
(2) $\mathrm{nil}\big(M/(N \cap N')\big) = \mathrm{nil}(M/N) \bigcap \mathrm{nil}(M/N')$.
(3) $\mathrm{nil}(M/N) = R$ if and only if $N = M$.
(4) $\mathrm{nil}\big(M/(N + N')\big) \supset \sqrt{\mathrm{nil}(M/N) + \mathrm{nil}(M/N')}$.

Find an example where equality fails in (4), yet R is a field k.

Solution: For (1), recall $\mathrm{nil}(M) = \sqrt{\mathrm{Ann}(M)}$. Thus **(3.13)** yields (1).

For (2), given $x \in \mathrm{nil}\big(M/(N \cap N')\big)$, say $x^n M \subset N \cap N'$. So $x^n M \subset N$ and $x^n M \subset N'$. Thus $x \in \mathrm{nil}(M/N) \bigcap \mathrm{nil}(M/N')$.

Conversely, given $x \in \mathrm{nil}(M/N) \bigcap \mathrm{nil}(M/N')$, say $x^n M \subset N$ and $x^m M \subset N'$. Then $x^{n+m} M \subset N \cap N'$. Thus $x \in \mathrm{nil}\big(M/(N \cap N')\big)$. Thus (2) holds.

For (3), note $\mathrm{nil}(M/N) = R$ if and only if $1 \in \mathrm{Ann}(M/N)$, so if and only if $N = M$. Thus (3) holds.

For (4), given $x \in \sqrt{\mathrm{nil}(M/N) + \mathrm{nil}(M/N')}$, say $x^m = y + z$ where $y^n M \subset N$ and $z^p M \subset N'$. Then $x^{m(n+p-1)} M \subset N + N'$; see **(3.15.1)** and the two lines after it. So $x \in \mathrm{nil}(M/(N + N'))$. Thus (4) holds.

For an example, take $N := N' := k$ and $M := N \oplus N'$. Then $M/(N+N') = 0$, so $\mathrm{nil}(M/(N + N')) = k$. But $M/N = k$, so $\mathrm{nil}(M/N) = 0$. Similarly, $\mathrm{nil}(M/N') = 0$. Thus equality fails in (4). □

13. Support

Exercise (13.10) . — Let R be a ring, M a module, and $m_\lambda \in M$ elements. Prove the m_λ generate M if and only if, at every maximal ideal $\mathfrak{m}$, the fractions $m_\lambda/1$ generate $M_\mathfrak{m}$ over $R_\mathfrak{m}$.

Solution: The m_λ define a map $\alpha \colon R^{\oplus\{\lambda\}} \to M$. By **(13.9)**, it is surjective if and only if $\alpha_\mathfrak{m} \colon \big(R^{\oplus\{\lambda\}}\big)_\mathfrak{m} \to M_\mathfrak{m}$ is surjective for all $\mathfrak{m}$. But $\big(R^{\oplus\{\lambda\}}\big)_\mathfrak{m} = R_\mathfrak{m}^{\oplus\{\lambda\}}$ by **(12.9)**. Hence **(4.10)**(1) yields the assertion. □

Exercise (13.16) . — Let R be a ring, $X := \mathrm{Spec}(R)$, and $\mathfrak{p}, \mathfrak{q} \in X$. Show:

(1) The closure $\overline{\{\mathfrak{p}\}}$ of $\mathfrak{p}$ is equal to $\mathbf{V}(\mathfrak{p})$; that is, $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$ if and only if $\mathfrak{p} \subset \mathfrak{q}$.

(2) Then $\mathfrak{p}$ is a closed point, that is, $\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}}$, if and only if $\mathfrak{p}$ is maximal.
(3) Then X is T_0; that is, if $\mathfrak{p} \neq \mathfrak{q}$ but every neighborhood of $\mathfrak{q}$ contains $\mathfrak{p}$, then some neighborhood of $\mathfrak{p}$ doesn't contain $\mathfrak{q}$.

Solution: For (1) first assume $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$. Given $f \in R - \mathfrak{p}$, note $\mathfrak{q} \in D(f)$. But $D(f)$ is open. So $\mathfrak{p} \in D(f)$. So $f \notin \mathfrak{p}$. Thus $\mathfrak{p} \subset \mathfrak{q}$.

Conversely, assume $\mathfrak{p} \subset \mathfrak{q}$. Given $f \in R$ with $\mathfrak{q} \in D(f)$, note $f \notin \mathfrak{q}$. So $f \notin \mathfrak{p}$. So $\mathfrak{p} \in D(f)$. Thus $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$. Thus (1) holds.

For (2), note $\{\mathfrak{p}\} = \overline{\{\mathfrak{p}\}}$ means, owing to (1), that if $\mathfrak{p} \subset \mathfrak{q}$, then $\mathfrak{p} = \mathfrak{q}$; that is, $\mathfrak{p}$ is maximal. Thus (2) holds.

For (3), assume every neighborhood of $\mathfrak{q}$ contains $\mathfrak{p}$. Then $\mathfrak{q} \in \overline{\{\mathfrak{p}\}}$. So $\mathfrak{p} \subset \mathfrak{q}$ by (1). If also $\mathfrak{p} \neq \mathfrak{q}$, then $\mathfrak{p} \in X - \mathbf{V}(\mathfrak{q})$. But $\mathfrak{q} \notin X - \mathbf{V}(\mathfrak{q})$. Thus (3) holds. □

Exercise (13.17) . — Describe $\operatorname{Spec}(\mathbb{R})$, $\operatorname{Spec}(\mathbb{Z})$, $\operatorname{Spec}(\mathbb{C}[X])$, and $\operatorname{Spec}(\mathbb{R}[X])$.

Solution: First, $\mathbb{R}$ is a field, so has only one prime, $\langle 0\rangle$. Thus $\operatorname{Spec}(\mathbb{R})$ is the unique topological space with only one point.

The rings $\mathbb{Z}$, $\mathbb{C}[X]$, and $\mathbb{R}[X]$ are PIDs. For any PID R, the points x_p of $\operatorname{Spec}(R)$ represent the ideals $\langle p\rangle$ with p a prime or 0. By **(13.1)**, the closed sets are the $\mathbf{V}(\langle a\rangle)$ with $a \in R$; moreover, $\mathbf{V}(\langle a\rangle) = \emptyset$ if a is a unit, $\mathbf{V}(\langle 0\rangle) = \operatorname{Spec}(R)$, and $\mathbf{V}(\langle a\rangle) = x_{p_1} \cup \cdots \cup x_{p_s}$ if $a = p_1^{n_1} \cdots p_s^{n_s}$ with p_i a prime and $n_i \geq 1$. □

Exercise (13.18) . — Let R be a ring, and set $X := \operatorname{Spec}(R)$. Let $X_1, X_2 \subset X$ be closed subsets. Show that the following four statements are equivalent:

(1) Then $X_1 \sqcup X_2 = X$; that is, $X_1 \cup X_2 = X$ and $X_1 \cap X_2 = \emptyset$.
(2) There are complementary idempotents $e_1, e_2 \in R$ with $\mathbf{V}(\langle e_i\rangle) = X_i$.
(3) There are comaximal ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1\mathfrak{a}_2 = 0$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.
(4) There are ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subset R$ with $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = R$ and $\mathbf{V}(\mathfrak{a}_i) = X_i$.

Finally, given any e_i and $\mathfrak{a}_i$ satisfying (2) and either (3) or (4), necessarily $e_i \in \mathfrak{a}_i$.

Solution: Assume (1). Take ideals $\mathfrak{a}_1, \mathfrak{a}_2$ with $\mathbf{V}(\mathfrak{a}_i) = X_i$. Then **(13.1)** yields

$$\mathbf{V}(\mathfrak{a}_1\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1) \cup \mathbf{V}(\mathfrak{a}_2) = X = \mathbf{V}(0) \quad \text{and}$$
$$\mathbf{V}(\mathfrak{a}_1 + \mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1) \cap \mathbf{V}(\mathfrak{a}_2) = \emptyset = \mathbf{V}(R).$$

So $\sqrt{\mathfrak{a}_1\mathfrak{a}_2} = \sqrt{\langle 0\rangle}$ and $\sqrt{\mathfrak{a}_1 + \mathfrak{a}_2} = \sqrt{R}$ again by **(13.1)**. Hence **(3.35)** yields (2).

Assume (2). Set $\mathfrak{a}_i := \langle e_i\rangle$. As $e_1 + e_2 = 1$ and $e_1 e_2 = 0$, plainly (3) holds.

Assume (3). As the $\mathfrak{a}_i$ are comaximal, the Chinese Remainder Theorem **(1.21)**(1) yields $\mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{a}_2$. But $\mathfrak{a}_1\mathfrak{a}_2 = 0$. So $\mathfrak{a}_1 \oplus \mathfrak{a}_2 = R$ by **(4.25)**. Thus (4) holds.

Assume (4). Then **(13.1)** yields (1) as follows:

$$X_1 \cup X_2 = \mathbf{V}(\mathfrak{a}_1) \cup \mathbf{V}(\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1\mathfrak{a}_2) = \mathbf{V}(0) = X \quad \text{and}$$
$$X_1 \cap X_2 = \mathbf{V}(\mathfrak{a}_1) \cap \mathbf{V}(\mathfrak{a}_2) = \mathbf{V}(\mathfrak{a}_1 + \mathfrak{a}_2) = \mathbf{V}(R) = \emptyset.$$

Finally, say e_i and $\mathfrak{a}_i$ satisfy (2) and either (3) or (4). Then $\sqrt{\langle e_i\rangle} = \sqrt{\mathfrak{a}_i}$ by **(13.1)**. So $e_i^n \in \mathfrak{a}_i$ for some $n \geq 1$. But $e_i^2 = e_i$, so $e_i^n = e_1$. Thus $e_i \in \mathfrak{a}_i$. □

Exercise (13.19) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Show:

(1) Then $\Gamma_{\mathfrak{a}}(M) = \{\, m \in M \mid \operatorname{Supp}(Rm) \subset \mathbf{V}(\mathfrak{a}) \,\}$.
(2) Then $\Gamma_{\mathfrak{a}}(M) = \{\, m \in M \mid m/1 = 0 \text{ in } M_{\mathfrak{p}} \text{ for all primes } \mathfrak{p} \not\supset \mathfrak{a} \,\}$.
(3) Then $\Gamma_{\mathfrak{a}}(M) = M$ if and only if $\operatorname{Supp}(M) \subset \mathbf{V}(\mathfrak{a})$.

Solution: For (1), note that $\operatorname{Supp}(Rm) = \mathbf{V}(\operatorname{Ann}(m))$ by **(13.4)**(3). However, $\mathbf{V}(\operatorname{Ann}(m)) \subset \mathbf{V}(\mathfrak{a})$ if and only if $\mathfrak{a} \subset \sqrt{\operatorname{Ann}(m)}$ by **(13.1)**. Thus (1) holds.

For (2), note $(Rm)_{\mathfrak{p}} = R_{\mathfrak{p}}(m/1)$. So $\mathfrak{p} \notin \operatorname{Supp}(Rm)$ if and only if $m/1 = 0$ in $M_{\mathfrak{p}}$. Thus (2) holds.

For (3), note $\operatorname{Supp}(M) = \bigcup_{m \in M} \operatorname{Supp}(Rm)$ by **(13.4)**(2). Thus (1) gives (3). □

Exercise (13.20) . — Let R be a ring, $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ a short exact sequence of finitely generated modules, and $\mathfrak{a}$ a finitely generated ideal. Assume $\operatorname{Supp}(M') \subset \mathbf{V}(\mathfrak{a})$. Show $0 \to \Gamma_{\mathfrak{a}}(M') \xrightarrow{\Gamma_{\mathfrak{a}}(\alpha)} \Gamma_{\mathfrak{a}}(M) \xrightarrow{\Gamma_{\mathfrak{a}}(\beta)} \Gamma_{\mathfrak{a}}(M'') \to 0$ is exact.

Solution: Recall $\Gamma_{\mathfrak{a}}(M) = \varinjlim \operatorname{Hom}(R/\mathfrak{a}^n, M)$ for all modules M by **(7.15)**. But $0 \to \operatorname{Hom}(R/\mathfrak{a}^n, M') \to \operatorname{Hom}(R/\mathfrak{a}^n, M) \to \operatorname{Hom}(R/\mathfrak{a}^n, M'')$ is exact for each n by **(5.11)**(2). Thus by **(7.9)** the desired exactness holds at $\Gamma_{\mathfrak{a}}(M')$ and $\Gamma_{\mathfrak{a}}(M)$.

It remains to show exactness at $\Gamma_{\mathfrak{a}}(M'')$. Given $m'' \in \Gamma_{\mathfrak{a}}(M'')$ and $x \in \mathfrak{a}$, say $x^n m'' = 0$. As β is surjective, there's $m \in M$ with $\beta(m) = m''$. Then $\beta(x^n m) = 0$. So by exactness, there's $m' \in M'$ with $\alpha(m') = x^n m$. But $M' = \Gamma_{\mathfrak{a}}(M')$ by **(13.19)**(3). So there's r with $x^r m' = 0$. So $x^{n+r} m = 0$. But $\mathfrak{a}$ is finitely generated. So there's s with $\mathfrak{a}^s m = 0$. So $m \in \Gamma_{\mathfrak{a}}(M)$. Thus $\Gamma_{\mathfrak{a}}(\beta)$ is surjective, as desired. □

Exercise (13.21) . — Let R be a ring, S a multiplicative subset. Prove this:

(1) Assume R is absolutely flat. Then $S^{-1}R$ is absolutely flat.

(2) Then R is absolutely flat if and only if $R_{\mathfrak{m}}$ is a field for each maximal $\mathfrak{m}$.

Solution: In (1), given $x \in R$, note that $\langle x \rangle$ is idempotent by **(10.25)**. Hence $\langle x \rangle = \langle x \rangle^2 = \langle x^2 \rangle$. So there is $y \in R$ with $x = x^2 y$.

Given $a/s \in S^{-1}R$, there are, therefore, $b, t \in R$ with $a = a^2 b$ and $s = s^2 t$. So $s(st - 1) = 0$. So $(st-1)/1 \cdot s/1 = 0$. But $s/1$ is a unit. Hence $s/1 \cdot t/1 - 1 = 0$. So $a/s = (a/s)^2 \cdot b/t$. So $a/s \in \langle a/s \rangle^2$. Thus $\langle a/s \rangle$ is idempotent. Hence $S^{-1}R$ is absolutely flat by **(10.25)**. Thus (1) holds.

Alternatively, given an $S^{-1}R$-module M, note M is also an R-module, so R-flat. Hence $M \otimes S^{-1}R$ is $S^{-1}R$-flat by **(9.22)**. But $M \otimes S^{-1}R = S^{-1}M$ by **(12.10)**, and $S^{-1}M = M$ by **(12.4)**(2). Thus M is $S^{-1}R$-flat. Thus again (1) holds.

For (2), first assume R is absolutely flat. By (1), each $R_{\mathfrak{m}}$ is absolutely flat. So by **(10.26)**(4), each $R_{\mathfrak{m}}$ is a field.

Conversely, assume each $R_{\mathfrak{m}}$ is a field. Then, given an R-module M, each $M_{\mathfrak{m}}$ is $R_{\mathfrak{m}}$-flat. So M is R-flat by **(13.12)**. Thus (2) holds. □

Exercise (13.22) . — Let R be a ring; set $X := \operatorname{Spec}(R)$. Prove that the four following conditions are equivalent:

(1) $R/\operatorname{nil}(R)$ is absolutely flat.

(2) X is Hausdorff.

(3) X is T_1; that is, every point is closed.

(4) Every prime $\mathfrak{p}$ of R is maximal.

Assume (1) holds. Prove that X is **totally disconnected**; namely, no two distinct points lie in the same connected component.

Solution: Note $X = \operatorname{Spec}(R/\operatorname{nil}(R))$ as $X = \mathbf{V}(0) = \mathbf{V}(\sqrt{0}) = \operatorname{Spec}(R/\sqrt{0})$ by **(13.1)**. Hence we may replace R by $R/\operatorname{nil}(R)$, and thus assume $\operatorname{nil}(R) = 0$.

Assume (1). Given distinct primes $\mathfrak{p}, \mathfrak{q} \in X$, take $x \in \mathfrak{p} - \mathfrak{q}$. Then $x \in \langle x^2 \rangle$ by **(10.25)**(4). So there is $y \in R$ with $x = x^2 y$. Set $\mathfrak{a}_1 := \langle x \rangle$ and $\mathfrak{a}_2 := \langle 1 - xy \rangle$.

Set $X_i := \mathbf{V}(\mathfrak{a}_i)$. Then $\mathfrak{p} \in X_1$ as $x \in \mathfrak{p}$. Further, $\mathfrak{q} \in X_2$ as $1 - xy \in \mathfrak{q}$ since $x(1-xy) = 0 \in \mathfrak{q}$, but $x \notin \mathfrak{q}$.

The $\mathfrak{a}_i$ are comaximal as $xy + (1-xy) = 1$. Further $\mathfrak{a}_1\mathfrak{a}_2 = 0$ as $x(1-xy) = 0$. So $X_1 \cup X_2 = X$ and $X_1 \cap X_2 = \emptyset$ by **(13.18)**. Hence the X_i are disjoint open and closed sets. Thus (2) holds, and X is totally disconnected.

In general, a Hausdorff space is T_1. Thus (2) implies (3).

Conditions (3) and (4) are equivalent by **(13.16)**(2).

Assume (4). Then every prime $\mathfrak{m}$ is both maximal and minimal. So $R_\mathfrak{m}$ is a local ring with $\mathfrak{m}R_\mathfrak{m}$ as its only prime by **(11.12)**(2). Hence $\mathfrak{m}R_\mathfrak{m} = \mathrm{nil}(R_\mathfrak{m})$ by the Scheinnullstellensatz **(3.14)**. But $\mathrm{nil}(R_\mathfrak{m}) = \mathrm{nil}(R)_\mathfrak{m}$ by **(11.28)**. And $\mathrm{nil}(R) = 0$. Thus $R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m} = R_\mathfrak{m}$. So $R_\mathfrak{m}$ is a field. Hence R is absolutely flat by **(13.21)**(2). Thus (1) holds. □

Exercise (13.23) . — Let R be a ring, and $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} \subset \mathrm{nil}(R)$. Set $X := \mathrm{Spec}(R)$. Show that the following three statements are equivalent:

(1) Then R is decomposable. (2) Then $R/\mathfrak{a}$ is decomposable.

(3) Then $X = \bigsqcup_{i=1}^n X_i$ where $X_i \subset X$ is closed and has a unique closed point.

Solution: Assume (1), say $R = \prod_{i=1}^n R_i$ with R_i local. Set $X_i := \mathrm{Spec}(R_i)$. Then the projection $R \twoheadrightarrow R_i$ induces the inclusion $X_i \hookrightarrow X$ as a closed subset by **(13.1.7)**. Moreover, X_i has a unique closed point by **(13.16)**(2). Let's show $X = \bigsqcup_{i=1}^n X_i$; so (3) holds. If $n = 1$, then trivially $X = X_1$. So suppose $n \ge 2$.

Set $R' := \prod_{i=2}^n R_i$. Then $R = R_1 \times R'$. Set $e_1 := (1,0)$ and $e' := (0,1)$. Then $R/\langle e_1\rangle = R'$ and $R/\langle e'\rangle = R_1$. So $\mathbf{V}(\langle e_1\rangle) = \mathrm{Spec}(R')$ and $\mathbf{V}(\langle e'\rangle) = X_1$ by **(13.1.7)**. So $X = X_1 \bigsqcup \mathrm{Spec}(R')$ by **(13.18)**(2)⇒(1). But $\mathrm{Spec}(R') = \bigsqcup_{i=2}^n X_i$ by induction. Thus (3) holds.

Assume (3). Let's prove (1) by induction on n. Suppose $n = 1$. Then X has a unique closed point. So R is local by **(13.16)**(2). Thus (1) holds. So assume $n \ge 2$.

Set $X' = \bigsqcup_{i=2}^n X_i$. Then $X = X_1 \sqcup X'$. So **(13.18)**(1)⇒(2) yields complementary idempotents e_1, $e' \in R$ with $\mathbf{V}(\langle e_1\rangle) = X'$ and $\mathbf{V}(\langle e'\rangle) = X_1$. Set $R_1 := R/\langle e'\rangle$ and $R' := R/\langle e_1\rangle$. Then **(13.1.7)** yields $X' = \mathrm{Spec}(R')$ and $X_1 = \mathrm{Spec}(R_1)$.

By induction, R' is decomposable. But $R = R_1 \times R'$ by **(1.12)**. Thus (1) holds.

Note $\mathrm{Spec}(R/\mathfrak{a}) = \mathbf{V}(\mathfrak{a}) = \mathbf{V}(0) = X$ by **(13.1)**. So (1)⇔(3) gives (2)⇔(3). □

Exercise (13.24) . — Let $\varphi\colon R \to R'$ be a map of rings, $\mathfrak{a}$ an ideal of R, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Prove these two statements:

(1) Every prime of R is the contraction of a prime if and only if φ^* is surjective.

(2) If every prime of R' is the extension of a prime, then φ^* is injective.

Is the converse of (2) true?

Solution: Note $\varphi^*(\mathfrak{q}) := \varphi^{-1}(\mathfrak{q})$ by **(13.1.4)**. Hence (1) holds.

Given two primes $\mathfrak{q}_1$ and $\mathfrak{q}_2$ that are extensions, if $\mathfrak{q}_1^c = \mathfrak{q}_2^c$, then $\mathfrak{q}_1 = \mathfrak{q}_2$ by **(1.14)**(3). Thus (2) holds.

The converse of (2) is false. Take R to be a domain. Set $R' := R[X]/\langle X^2\rangle$. Then $R'/\langle X\rangle = R$ by **(1.9)** and **(1.6)**(2). So $\langle X\rangle$ is prime by **(2.8)**. But $\langle X\rangle$ is not an extension, as $X \notin \mathfrak{a}R'$ for any proper ideal $\mathfrak{a}$ of R. Finally, every prime $\mathfrak{q}$ of R' contains the residue x of X, as $x^2 = 0$. Hence $\mathfrak{q}$ is generated by $\mathfrak{q} \cap R$ and x. But $\mathfrak{q} \cap R = \varphi^*(\mathfrak{q})$. Thus φ^* is injective. □

Exercise (13.25) . — Let R be a ring, and S a multiplicative subset of R. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(S^{-1}R)$. Set $\varphi_S^* := \mathrm{Spec}(\varphi_S)$ and $S^{-1}X := \mathrm{Im}\,\varphi_S^*$ in X. Show (1) that $S^{-1}X$ consists of the primes $\mathfrak{p}$ of R with $\mathfrak{p} \cap S = \emptyset$ and (2) that φ_S^* is a homeomorphism of Y onto $S^{-1}X$.

Solution: Note $\varphi_S^*(\mathfrak{q}) := \varphi_S^{-1}(\mathfrak{q})$ by **(13.1.4)**. So **(11.12)**(2) gives (1) and the bijectivity of φ_S^*. But φ_S^* is continuous by **(13.1)**. So we must show $\varphi_S^*\colon Y \to S^{-1}X$ is closed. Given an ideal $\mathfrak{b} \subset S^{-1}R$, set $\mathfrak{a} := \varphi_S^{-1}(\mathfrak{b})$. We must show

$$\varphi_S^*(\mathbf{V}(\mathfrak{b})) = S^{-1}X \bigcap \mathbf{V}(\mathfrak{a}). \tag{13.25.1}$$

Given $\mathfrak{p} \in \varphi_S^*(\mathbf{V}(\mathfrak{b}))$, say $\mathfrak{p} = \varphi_S^*(\mathfrak{q})$ and $\mathfrak{q} \in \mathbf{V}(\mathfrak{b})$. Then $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{q})$ and $\mathfrak{q} \supset \mathfrak{b}$ by **(13.1)**. So $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{q}) \supset \varphi_S^{-1}(\mathfrak{b}) =: \mathfrak{a}$. So $\mathfrak{p} \in \mathbf{V}(\mathfrak{a})$. But $\mathfrak{p} \in \varphi_S^*(\mathbf{V}(\mathfrak{b})) \subset S^{-1}X$. Thus $\varphi_S^*(\mathbf{V}(\mathfrak{b})) \subset S^{-1}X \bigcap \mathbf{V}(\mathfrak{a})$.

Conversely, given $\mathfrak{p} \in S^{-1}X \bigcap \mathbf{V}(\mathfrak{a})$, say that $\mathfrak{p} = \varphi_S^*(\mathfrak{q})$. Then $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{q})$ and $\mathfrak{p} \supset \mathfrak{a} := \varphi_S^{-1}(\mathfrak{b})$. So $\varphi_S^{-1}(\mathfrak{q}) \supset \varphi_S^{-1}(\mathfrak{b})$. So $\varphi_S^{-1}(\mathfrak{q})R \supset \varphi_S^{-1}(\mathfrak{b})R$. So $\mathfrak{q} \supset \mathfrak{b}$ by **(11.11)**(1)(b). So $\mathfrak{q} \in \mathbf{V}(\mathfrak{b})$. So $\mathfrak{p} = \varphi_S^*(\mathfrak{q}) \in \varphi_S^*(\mathbf{V}(\mathfrak{b}))$. Thus **(13.25.1)** holds, as desired. Thus (2) holds. □

Exercise (13.26) . — Let $\theta\colon R \to R'$ be a ring map, $S \subset R$ a multiplicative subset. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$ and $\theta^* := \mathrm{Spec}(\theta)$. Via **(13.25)**(2) and **(11.15)**, identify $\mathrm{Spec}(S^{-1}R)$ and $\mathrm{Spec}(S^{-1}R')$ with their images $S^{-1}X \subset X$ and $S^{-1}Y \subset Y$. Show (1) $S^{-1}Y = \theta^{*-1}(S^{-1}X)$ and (2) $\mathrm{Spec}(S^{-1}\theta) = \theta^*\big|S^{-1}Y$.

Solution: Given $\mathfrak{q} \in Y$, elementary set-theory shows that $\mathfrak{q} \cap \theta(S) = \emptyset$ if and only if $\theta^{-1}(\mathfrak{q}) \cap S = \emptyset$. So $\mathfrak{q} \in S^{-1}Y$ if and only if $\theta^{-1}(\mathfrak{q}) \in S^{-1}X$ by **(13.25)**(1) and **(11.15)**. But $\varphi_S^{-1}(\mathfrak{q}) =: \varphi_S^*(\mathfrak{q})$ by **(13.1.4)**. Thus (1) holds.

Finally, $(S^{-1}\theta)\varphi_S = \varphi_S\theta$ by **(12.7)**. So $\varphi_S^{-1}(S^{-1}\theta)^{-1}(\mathfrak{q}) = (S^{-1}\theta)^{-1}\varphi_S^{-1}(\mathfrak{q})$. Thus **(13.1.4)** yields (2). □

Exercise (13.27) . — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{a} \subset R$ an ideal. Set $\mathfrak{b} := \mathfrak{a}R'$. Let $\overline{\theta}\colon R/\mathfrak{a} \to R'/\mathfrak{b}$ be the induced map. Set $X := \mathrm{Spec}(R)$ and $Y := \mathrm{Spec}(R')$. Set $\theta^* := \mathrm{Spec}(\theta)$ and $\overline{\theta}^* := \mathrm{Spec}(\overline{\theta})$. Via **(13.1)**, identify $\mathrm{Spec}(R/\mathfrak{a})$ and $\mathrm{Spec}(R'/\mathfrak{b})$ with $\mathbf{V}(\mathfrak{a}) \subset X$ and $\mathbf{V}(\mathfrak{b}) \subset Y$. Show (1) $\mathbf{V}(\mathfrak{b}) = \theta^{*-1}(\mathbf{V}(\mathfrak{a}))$ and (2) $\overline{\theta}^* = \theta^*\big|\,\mathbf{V}(\mathfrak{b})$.

Solution: Given $\mathfrak{q} \in Y$, observe that $\mathfrak{q} \supset \mathfrak{b}$ if and only if $\theta^{-1}(\mathfrak{q}) \supset \mathfrak{a}$, as follows. By **(1.14)**(1) in its notation, $\mathfrak{q} \supset \mathfrak{b} := \mathfrak{a}^e$ yields $\mathfrak{q}^c \supset \mathfrak{a}^{ec} \supset \mathfrak{a}$, and $\mathfrak{q}^c \supset \mathfrak{a}$ yields $\mathfrak{q} \supset \mathfrak{q}^{ce} \supset \mathfrak{a}^e$. Thus (1) holds.

Plainly, $\overline{\theta}(\mathfrak{q}/\mathfrak{b}) = (\theta^{-1}\mathfrak{q})/\mathfrak{a}$. Thus **(13.1.4)** yields (2). □

Exercise (13.28) . — Let $\theta\colon R \to R'$ be a ring map, $\mathfrak{p} \subset R$ a prime, k the residue field of $R_\mathfrak{p}$. Set $\theta^* := \mathrm{Spec}(\theta)$. Show (1) $\theta^{*-1}(\mathfrak{p})$ is canonically homeomorphic to $\mathrm{Spec}(R'_\mathfrak{p}/\mathfrak{p}R'_\mathfrak{p})$ and to $\mathrm{Spec}(k \otimes_R R')$ and (2) $\mathfrak{p} \in \mathrm{Im}\,\theta^*$ if and only if $k \otimes_R R' \neq 0$.

Solution: First, take $S := S_\mathfrak{p} := R - \mathfrak{p}$ and apply **(13.26)** to obtain

$$\mathrm{Spec}(R'_\mathfrak{p}) = \theta^{*-1}(\mathrm{Spec}(R_\mathfrak{p})) \quad \text{and} \quad \mathrm{Spec}(\theta_\mathfrak{p}) = \theta^*\big|\,\mathrm{Spec}(R'_\mathfrak{p}).$$

Next, take $\mathfrak{a} := \mathfrak{p}R_\mathfrak{p}$ and apply **(13.27)** to $\theta_\mathfrak{p}\colon R_\mathfrak{p} \to R'_\mathfrak{p}$ to obtain

$$\mathrm{Spec}(R'_\mathfrak{p}/\mathfrak{p}R'_\mathfrak{p}) = \mathrm{Spec}(\theta_\mathfrak{p})^{-1}\,\mathbf{V}(\mathfrak{p}R_\mathfrak{p}).$$

But $\varphi_\mathfrak{p}^{-1}(\mathfrak{p}R_\mathfrak{p}) = \mathfrak{p}$ by **(11.12)**(2); so $\mathbf{V}(\mathfrak{p}R_\mathfrak{p}) = \mathfrak{p}$. Thus,

$$\mathrm{Spec}(R'_\mathfrak{p}/\mathfrak{p}R'_\mathfrak{p}) = \big(\theta^*\big|\,\mathrm{Spec}(R'_\mathfrak{p})\big)^{-1}(\mathfrak{p}) = \theta^{*-1}(\mathfrak{p}).$$

It remains to see $R'_{\mathfrak p}/\mathfrak p R'_{\mathfrak p} = k\otimes_R R'$. Note $k := R_{\mathfrak p}/\mathfrak p R_{\mathfrak p}$. So $R'_{\mathfrak p}/\mathfrak p R'_{\mathfrak p} = k\otimes_{R_{\mathfrak p}} R'_{\mathfrak p}$ by **(8.27)** with $\mathfrak a := \mathfrak p R_{\mathfrak p}$ and $M := R'_{\mathfrak p}$ as $\mathfrak p R'_{\mathfrak p} = (\mathfrak p R_{\mathfrak p})R'_{\mathfrak p}$. But $k\otimes_{R_{\mathfrak p}} R'_{\mathfrak p} = k\otimes_R R'$ by **(12.30)** as $k = k_{\mathfrak p}$ by **(12.4)**(2). Thus $R'_{\mathfrak p}/\mathfrak p R'_{\mathfrak p} = k\otimes_R R'$. Thus (1) holds.

Finally, (1) implies $\mathfrak p \in \operatorname{Im}\theta^*$ if and only if $\operatorname{Spec}(R'\otimes_R k) \neq \emptyset$. Thus (2) holds. □

Exercise (13.29) . — Let R be a ring, $\mathfrak p$ a prime ideal. Show that the image of $\operatorname{Spec}(R_{\mathfrak p})$ in $\operatorname{Spec}(R)$ is the intersection of all open neighborhoods of $\mathfrak p$ in $\operatorname{Spec}(R)$.

Solution: By **(13.25)**, the image $X_{\mathfrak p}$ consists of the primes contained in $\mathfrak p$. Given $f\in R-\mathfrak p$, note that $\mathbf D(f)$ contains every prime contained in $\mathfrak p$, or $X_{\mathfrak p}\subset \mathbf D(f)$. But the principal open sets form a basis of the topology of X by **(13.1)**. Hence $X_{\mathfrak p}$ is contained in the intersection, Z say, of all open neighborhoods of $\mathfrak p$. Conversely, given a prime $\mathfrak q\not\subset\mathfrak p$, there is $g\in\mathfrak q-\mathfrak p$. So $\mathbf D(g)$ is an open neighborhood of $\mathfrak p$, and $\mathfrak q\notin \mathbf D(g)$. Thus $X_{\mathfrak p} = Z$, as desired. □

Exercise (13.30) . — Let $\varphi\colon R\to R'$ and $\psi\colon R\to R''$ be ring maps, and define $\theta\colon R\to R'\otimes_R R''$ by $\theta(x) := \varphi(x)\otimes\psi(x)$. Show

$$\operatorname{Im}\operatorname{Spec}(\theta) = \operatorname{Im}\operatorname{Spec}(\varphi)\bigcap \operatorname{Im}\operatorname{Spec}(\psi).$$

Solution: Given $\mathfrak p\in X$, set $k := R_{\mathfrak p}/\mathfrak p R_{\mathfrak p}$. Then **(8.8)**(1) and **(8.9)**(1) yield

$$(R'\otimes_R R'')\otimes_R k = R'\otimes_R (R''\otimes_R k) = (R'\otimes_R k)\otimes_k (R''\otimes_R k).$$

So $(R'\otimes_R R'')\otimes_R k\neq 0$ if and only if $R'\otimes_R k\neq 0$ and $R''\otimes_R k\neq 0$ by **(8.24)**. Hence **(13.28)**(2) implies that $\mathfrak p\in\operatorname{Im}\operatorname{Spec}(\theta)$ if and only if $\mathfrak p\in\operatorname{Im}\operatorname{Spec}(\varphi)$ and $\mathfrak p\in\operatorname{Im}\operatorname{Spec}(\psi)$, as desired. □

Exercise (13.31) . — Let R be a filtered direct limit of rings R_λ with transition maps α^λ_μ and insertions α_λ. For each λ, let $\varphi_\lambda\colon R'\to R_\lambda$ be a ring map with $\varphi_\mu = \alpha^\lambda_\mu\varphi_\lambda$ for all α^λ_μ, so that $\varphi := \alpha_\lambda\varphi_\lambda$ is independent of λ. Show

$$\operatorname{Im}\operatorname{Spec}(\varphi) = \textstyle\bigcap_\lambda \operatorname{Im}\operatorname{Spec}(\varphi_\lambda).$$

Solution: Given $\mathfrak q\in\operatorname{Spec}(R')$, set $k := R'_{\mathfrak q}/\mathfrak q R'_{\mathfrak q}$. Then **(8.10)** yields

$$R\otimes_{R'} k = \varinjlim(R_\lambda\otimes_{R'} k).$$

So $R\otimes_{R'} k\neq 0$ if and only if $R_\lambda\otimes_{R'} k\neq 0$ for some λ by **(7.16)**(1). So **(13.28)**(2) implies $\mathfrak q\in\operatorname{Im}\operatorname{Spec}(\varphi)$ if and only if $\mathfrak q\in\operatorname{Im}\operatorname{Spec}(\varphi_\lambda)$ for some λ, as desired. □

Exercise (13.32) . — Let R be a ring, $\varphi_\sigma\colon R\to R_\sigma$ for $\sigma\in\Sigma$ ring maps. Let $\gamma_\Sigma\colon R\to\coprod R_\sigma$ and $\pi_\Sigma\colon R\to\prod R_\sigma$ be the induced maps. Set $X := \operatorname{Spec}(R)$. Show:

(1) Then $\operatorname{Im}\operatorname{Spec}(\gamma_\Sigma) = \bigcap\operatorname{Im}\operatorname{Spec}(\varphi_\sigma)$.
(2) Assume Σ is finite. Then $\operatorname{Im}\operatorname{Spec}(\pi_\Sigma) = \bigcup\operatorname{Im}\operatorname{Spec}(\varphi_\sigma)$.
(3) The subsets of X of the form $\operatorname{Im}\operatorname{Spec}(\varphi)$, where $\varphi\colon R\to R'$ is a ring map, are the closed sets of a topology, known as the **constructible topology**. It contains the Zariski topology.
(4) In the constructible topology, X is quasi-compact.

Solution: For (1), recall from **(8.33)** that $\coprod R_\sigma = \varinjlim_J\big(\bigotimes_{\sigma\in J} R_\sigma\big)$ where J runs over the finite subsets of Σ. Then $\operatorname{Im}\operatorname{Spec}(\gamma_\Sigma) = \bigcap_J\operatorname{Im}\operatorname{Spec}(\gamma_J)$ by **(13.31)**. But $\operatorname{Im}\operatorname{Spec}(\gamma_J) = \bigcap_{\sigma\in J}\operatorname{Im}\operatorname{Spec}(\varphi_\sigma)$ by **(13.30)**. Thus (1) holds.

For (2), given $\tau\in\Sigma$, set $e_\tau := (\delta_{\sigma\tau})\in\prod R_\sigma$. As Σ is finite, the primes of $\prod R_\sigma$ are the ideals of the form $\mathfrak p_\sigma e_\sigma$ for some σ, where $\mathfrak p_\sigma\subset R_\sigma$ is prime, by **(2.29)**.

But $\pi_\Sigma^{-1}(\mathfrak{p}_\sigma e_\sigma) = \varphi_\sigma^{-1}\mathfrak{p}_\sigma$. Thus (2) holds.

For (3), note that, by (1) and (2), finite intersections and arbitrary unions of closed sets are closed. Moreover, $\operatorname{Im}\operatorname{Spec}(1_R) = \operatorname{Spec}(R)$ and $\operatorname{Im}\operatorname{Spec}(0_R) = \emptyset$ where $0_R\colon R \to 0$ is the zero map. Thus the closed sets form a topology.

Given an ideal $\mathfrak{a}$, let $\varphi\colon R \to R/\mathfrak{a}$ be the quotient map. Then $\mathbf{V}(\mathfrak{a}) = \operatorname{Im}\operatorname{Spec}(\varphi)$ by **(13.1.7)**. Thus every set closed in the Zariski topology is also closed in the constructible topology. Thus (3) holds.

For (4), set $F_\sigma := \operatorname{Im}\operatorname{Spec}(\varphi_\sigma)$ for $\sigma \in \Sigma$. Assume $\bigcap F_\sigma = \emptyset$. Then (1) implies $\operatorname{Im}\operatorname{Spec}(\coprod R_\sigma) = \emptyset$. So $\coprod R_\sigma = 0$. Since $\coprod R_\sigma = \varinjlim_J R_J$ where J runs over the finite subsets of Σ, there's a J with $R_J = 0$ by **(7.1)** and **(7.16)**. Hence $\bigcap_{\sigma\in J} F_\sigma = \emptyset$ by **(13.30)**. Thus (4) holds. □

Exercise (13.33) . — Let R be a ring, $X := \operatorname{Spec}(R)$. Show:

(1) Given $g \in R$, the set $\mathbf{D}(g)$ is open and closed in the constructible toplogy.
(2) On X, any topology with all $\mathbf{D}(g)$ open and closed is Hausdorff and totally disconnected.
(3) On any set, nested topologies $\mathcal{T} \supset \mathcal{S}$ coincide if $\mathcal{T}$ is quasi-compact and $\mathcal{S}$ is Hausdorff.
(4) On X, the constructible and the Zariski topologies coincide if and only if the Zariski topology is Hausdorff, if and only if $R/\operatorname{nil}(R)$ is absolutely flat.
(5) On X, the construcible topology is smallest with all $\mathbf{D}(g)$ open and closed.
(6) On X, the constructible open sets are the arbitray unions U of the finite intersections of the $\mathbf{D}(g)$ and the $X - \mathbf{D}(g)$.

Solution: For (1), note $\mathbf{D}(g)$ is open in the Zariski topology by **(13.1.2)**, so open in the constructible topology by **(13.32)**(3). But $\mathbf{D}(g) = \operatorname{Im}\operatorname{Spec}(\varphi_g)$, where $\varphi_g\colon R \to R_g$ is the localization map, owing to **(13.1.8)**; so $\mathbf{D}(g)$ is closed in the constructible topology by definition. Thus (1) holds.

In (2), given distinct primes $\mathfrak{p}, \mathfrak{q}$ of R, either $\mathfrak{p} \not\subset \mathfrak{q}$ or $\mathfrak{q} \not\subset \mathfrak{p}$; say $\mathfrak{p} \not\subset \mathfrak{q}$. Then there's $g \in \mathfrak{p} - \mathfrak{q}$. So $\mathfrak{q} \in \mathbf{D}(g)$ and $\mathfrak{p} \in X - \mathbf{D}(g)$. The sets $\mathbf{D}(g)$ and $X - \mathbf{D}(g)$ are disjoint. Both are open and closed by hypothesis. Thus (2) holds.

For (3), we must show any set U open in $\mathcal{T}$ is also open in $\mathcal{S}$. As $\mathcal{S}$ is Hausdorff, given x in U and y in its complement C, there are disjoint open sets U_y, V_y in $\mathcal{S}$ with $x \in U_y$ and $y \in V_y$. But $\mathcal{T} \supset \mathcal{S}$. So U_y and V_y are are also open in $\mathcal{T}$.

Note $\bigcup_{y\in C} V_y \supset C$. But C is closed in $\mathcal{T}$, and $\mathcal{T}$ is quasi-compact. So there's a finite subset F of C with $\bigcup_{y\in F} V_y \supset C$. Then $\bigcap_{y\in F} U_y$ is open in $\mathcal{S}$, lies in U, and contains x. But $x \in U$ is arbitrary. Thus U is open in $\mathcal{S}$. Thus (3) holds.

For (4), note by **(13.1)** the $\mathbf{D}(g)$ form a basis of the Zariski topology. So it lies in the constructible topology by (1). But the latter is quasi-compact by **(13.31)**(4). So by (3) the two topologies coincide if the Zariski topology is Hausdorff. The converse holds by (1) and (2). Finally, the Zariski topology is Hausdorff if and only if $R/\operatorname{nil}(R)$ is absolutely flat by **(13.22)**. Thus (4) holds.

For (5), note that the construcible topology contains the smallest topology $\mathcal{S}$ with all $\mathbf{D}(g)$ open and closed by (1). Moreover, the construcible topology is quasi-compact by **(13.31)**(4), and $\mathcal{S}$ is Hausdorff by (2). Thus (3) implies (5).

In (6), every such U is a constructible open set owing to (1). Conversely, the family $\mathcal{F}$ of all U trivially contains X and $\emptyset$ and is stable under arbitrary union. Moreover, $\mathcal{F}$ is stable under finite intersection since $(\bigcup Y_\lambda) \cap (\bigcup Z_\mu) = \bigcup_{\lambda,\mu} Y_\lambda \cap Z_\mu$ for any families $\{Y_\lambda\}$ and $\{Z_\mu\}$ of subsets of X. Hence, these U are the open sets of a topology, in which all $\mathbf{D}(g)$ are open and closed. Hence $\mathcal{F}$ contains the constructible open sets owing to (5). Thus (6) holds. $\square$

Exercise (13.34) . — Let $\varphi\colon R \to R'$ be a ring map. Show, in the constructible topology, $\operatorname{Spec}(\varphi)\colon \operatorname{Spec}(R') \to \operatorname{Spec}(R)$ is continuous and closed.

Solution: By (**13.33**)(6), the constructible open sets of $\operatorname{Spec}(R)$ are the arbitrary unions of finite intersections of all $\mathbf{D}(g)$ and all $X - D(g)$. But $\operatorname{Spec}(\varphi)^{-1}$ preserves arbitrary unions, arbitrary intersections, and complements. Moreover, $\operatorname{Spec}(\varphi)^{-1}\mathbf{D}(g) = \mathbf{D}(\varphi(g))$ by (**13.1.5**). Thus $\operatorname{Spec}(\varphi)$ is continuous.

Given another ring map $\varphi'\colon R' \to R''$, recall $\operatorname{Spec}(\varphi)\operatorname{Spec}(\varphi') = \operatorname{Spec}(\varphi'\varphi)$ from (**13.1.6**). So $\operatorname{Spec}(\varphi)(\operatorname{Im}\operatorname{Spec}(\varphi')) = \operatorname{Im}\operatorname{Spec}(\varphi'\varphi)$. Thus $\operatorname{Spec}(\varphi)$ is closed. $\square$

Exercise (13.35) . — Let A be a domain with just one nonzero prime $\mathfrak{p}$. Set $K := \operatorname{Frac}(A)$ and $R := (A/\mathfrak{p}) \times K$. Define $\varphi\colon A \to R$ by $\varphi(x) := (x', x)$ with x' the residue of x. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Show φ^* is bijective, but not a homeomorphism.

Solution: Note $\mathfrak{p}$ is maximal; so $A/\mathfrak{p}$ is a field. The primes of R are $(0, K)$ and $(A/\mathfrak{p}, 0)$ by (**2.29**). Plainly, $\varphi^{-1}(0, K) = \mathfrak{p}$ and $\varphi^{-1}(A/\mathfrak{p}, 0) = 0$. So φ^* is bijective. Finally, $\operatorname{Spec}(R)$ is discrete, but $\operatorname{Spec}(A)$ has $\mathfrak{p} \in \mathbf{V}(0)$; so φ^* is not a homeomorphism. $\square$

Exercise (13.36) . — Let $\varphi\colon R \to R'$ be a ring map, and $\mathfrak{b}$ an ideal of R'. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Show (1) that the closure $\overline{\varphi^*(\mathbf{V}(\mathfrak{b}))}$ in $\operatorname{Spec}(R)$ is equal to $\mathbf{V}(\varphi^{-1}\mathfrak{b})$ and (2) that $\varphi^*(\operatorname{Spec}(R'))$ is dense in $\operatorname{Spec}(R)$ if and only if $\operatorname{Ker}(\varphi) \subset \operatorname{nil}(R)$.

Solution: For (1), given $\mathfrak{p} \in \varphi^*(\mathbf{V}(\mathfrak{b}))$, say $\mathfrak{p} = \varphi^{-1}(\mathfrak{P})$ where $\mathfrak{P}$ is a prime of R' with $\mathfrak{P} \supset \mathfrak{b}$. Then $\varphi^{-1}\mathfrak{P} \supset \varphi^{-1}\mathfrak{b}$. So $\mathfrak{p} \supset \varphi^{-1}\mathfrak{b}$, or $\mathfrak{p} \in \mathbf{V}(\varphi^{-1}\mathfrak{b})$. Thus $\varphi^*(\mathbf{V}(\mathfrak{b})) \subset \mathbf{V}(\varphi^{-1}\mathfrak{b})$. But $\mathbf{V}(\varphi^{-1}\mathfrak{b})$ is closed. So $\overline{\varphi^*(\mathbf{V}(\mathfrak{b})} \subset \mathbf{V}(\varphi^{-1}\mathfrak{b})$.

Conversely, given $\mathfrak{p} \in \mathbf{V}(\varphi^{-1}\mathfrak{b})$, note $\mathfrak{p} \supset \sqrt{\varphi^{-1}\mathfrak{b}}$. Take a neighborhood $\mathbf{D}(f)$ of $\mathfrak{p}$; then $f \notin \mathfrak{p}$. Hence $f \notin \sqrt{\varphi^{-1}\mathfrak{b}}$. But $\sqrt{\varphi^{-1}\mathfrak{b}} = \varphi^{-1}(\sqrt{\mathfrak{b}})$ by (**3.39**)(2). Hence $\varphi(f) \notin \sqrt{\mathfrak{b}}$. So there's a prime $\mathfrak{P} \supset \mathfrak{b}$ with $\varphi(f) \notin \mathfrak{P}$ by the Scheinnullstellensatz (**3.14**). So $\varphi^{-1}\mathfrak{P} \in \varphi^*(\mathbf{V}(\mathfrak{b}))$. Further, $f \notin \varphi^{-1}\mathfrak{P}$, or $\varphi^{-1}\mathfrak{P} \in \mathbf{D}(f)$. Therefore, $\varphi^{-1}\mathfrak{P} \in \varphi^*(\mathbf{V}(\mathfrak{b})) \cap \mathbf{D}(f)$. So $\varphi^*(\mathbf{V}(\mathfrak{b})) \cap \mathbf{D}(f) \neq \emptyset$. So $\mathfrak{p} \in \overline{\varphi^*(\mathbf{V}(\mathfrak{b}))}$. Thus (1) holds.

For (2), take $\mathfrak{b} := \langle 0 \rangle$. Then (1) yields $\overline{\varphi^*(\mathbf{V}(\mathfrak{b}))} = \mathbf{V}(\operatorname{Ker}(\varphi))$. But by (**13.1**), $\mathbf{V}(\mathfrak{b}) = \operatorname{Spec}(R')$ and $\operatorname{Spec}(R) = \mathbf{V}(\langle 0 \rangle)$. So $\overline{\varphi^*(\operatorname{Spec}(R'))} = \operatorname{Spec}(R)$ if and only if $\mathbf{V}(\langle 0 \rangle) = \mathbf{V}(\operatorname{Ker}(\varphi))$. The latter holds if and only if $\operatorname{nil}(R) = \sqrt{\operatorname{Ker}(\varphi)}$ by (**13.1**), so plainly if and only if $\operatorname{nil}(R) \supset \operatorname{Ker}(\varphi)$. Thus (2) holds. $\square$

Exercise (13.37) . — Let $\varphi\colon R \to R'$ be a ring map. Consider these statements:

(1) The map φ has the **Going-up Property**: given primes $\mathfrak{q}' \subset R'$ and $\mathfrak{p} \subset R$ with $\mathfrak{p} \supset \varphi^{-1}(\mathfrak{q}')$, there is a prime $\mathfrak{p}' \subset R'$ with $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ and $\mathfrak{p}' \supset \mathfrak{q}'$.

(2) Given a prime $\mathfrak{q}'$ of R', set $\mathfrak{q} := \varphi^{-1}(\mathfrak{q}')$. Then $\operatorname{Spec}(R'/\mathfrak{q}') \to \operatorname{Spec}(R/\mathfrak{q})$ is surjective.

(3) The map $\operatorname{Spec}(\varphi)$ is closed: it maps closed sets to closed sets.

Prove that (1) and (2) are equivalent, and are implied by (3).

Solution: Plainly, (1) holds if and only if the following equality does:

$$\operatorname{Spec}(\varphi)(\mathbf{V}(\mathfrak{q}')) = \mathbf{V}(\varphi^{-1}(\mathfrak{q}')). \qquad \textbf{(13.37.1)}$$

But (**13.37.1**) holds if and only if (2) does owing to (**13.1.7**). Thus (1) and (2) are equivalent.

Finally, $\overline{\operatorname{Spec}(\varphi)(\mathbf{V}(\mathfrak{q}'))} = \mathbf{V}(\varphi^{-1}(\mathfrak{q}'))$ by **(13.36)**(1). So **(13.37.1)** holds if (3) does. Thus (1) and (2) are implied by (3). □

Exercise (13.38) . — Let $\varphi\colon R \to R'$ be a ring map. Consider these statements:

(1) The map φ has the **Going-down Property**: given primes $\mathfrak{q}' \subset R'$ and $\mathfrak{p} \subset R$ with $\mathfrak{p} \subset \varphi^{-1}(\mathfrak{q}')$, there is a prime $\mathfrak{p}' \subset R'$ with $\varphi^{-1}(\mathfrak{p}') = \mathfrak{p}$ and $\mathfrak{p}' \subset \mathfrak{q}'$.

(2) Given a prime $\mathfrak{q}'$ of R', set $\mathfrak{q} := \varphi^{-1}(\mathfrak{q}')$. Then $\operatorname{Spec}(R'_{\mathfrak{q}'}) \to \operatorname{Spec}(R_{\mathfrak{q}})$ is surjective.

(3) The map $\operatorname{Spec}(\varphi)$ is open: it maps open sets to open sets.

Prove (1) and (2) are equivalent; using **(13.31)**, prove they're implied by (3).

Solution: Set $\varphi^* := \operatorname{Spec}(\varphi)$. Identify $\operatorname{Spec}(R_{\mathfrak{q}})$ with the subspace of $\operatorname{Spec}(R)$ of $\mathfrak{p} \subset \mathfrak{q}$ by **(13.25)** with $S := S_{\mathfrak{q}}$; similarly, identify $\operatorname{Spec}(R'_{\mathfrak{q}'})$ in $\operatorname{Spec}(R')$. Then **(13.1.4)** implies the following statement:

$$\varphi^* \operatorname{Spec}(R'_{\mathfrak{q}'}) \subset \operatorname{Spec}(R_{\mathfrak{q}}),\ \text{with equality if and only if (1) holds.} \qquad \textbf{(13.38.1)}$$

Those identifications are made via $\operatorname{Spec}(\varphi^*_{S_{\mathfrak{p}}})$ and $\operatorname{Spec}(\varphi^*_{S_{\mathfrak{p}'}})$. So φ^* induces $\operatorname{Spec}(\rho)$ where $\rho\colon R_{\mathfrak{q}} \to R_{\mathfrak{q}'}$ is the map induced by φ. So $\varphi^* \operatorname{Spec}(R'_{\mathfrak{q}'}) = \operatorname{Spec}(R_{\mathfrak{q}})$ if and only if (2) holds. Thus (1) and (2) are equivalent by **(13.38.1)**.

Lastly, $R'_{\mathfrak{q}'} = \varinjlim_{t \in S_{\mathfrak{q}'}} R'_t$ by **(12.6)**. Hence $\varphi^* \operatorname{Spec}(R'_{\mathfrak{q}'}) = \bigcap \varphi^* \operatorname{Spec}(R'_t)$ by **(13.31)**. Assume (3). Then $\varphi^* \operatorname{Spec}(R'_t)$ is open, as $\operatorname{Spec}(R'_t)$ is by **(13.1)**. But $\mathfrak{q}' \in \operatorname{Spec}(R'_t)$, so $\mathfrak{q} \in \varphi^* \operatorname{Spec}(R'_t)$. So $\operatorname{Spec}(R_{\mathfrak{q}}) \subset \varphi^* \operatorname{Spec}(R'_t)$ by **(13.29)**. Thus $\operatorname{Spec}(R_{\mathfrak{q}}) \subset \varphi^* \operatorname{Spec}(R'_{\mathfrak{q}'})$. Thus **(13.38.1)** yields equality here, and with it (1). □

Exercise (13.39) . — Let R be a ring; $f, g \in R$. Prove (1)–(8) are equivalent:

(1) $\mathbf{D}(g) \subset \mathbf{D}(f)$. (2) $\mathbf{V}(\langle g\rangle) \supset \mathbf{V}(\langle f\rangle)$. (3) $\sqrt{\langle g\rangle} \subset \sqrt{\langle f\rangle}$.
(4) $\overline{S}_f \subset \overline{S}_g$. (5) $g \in \sqrt{\langle f\rangle}$. (6) $f \in \overline{S}_g$.
(7) There is a unique R-algebra map $\varphi^f_g\colon \overline{S}_f^{-1} R \to \overline{S}_g^{-1} R$.
(8) There is an R-algebra map $R_f \to R_g$.

If these conditions hold, prove the map in (8) is equal to φ^f_g.

Solution: First, (1) and (2) are equivalent by **(13.1)**, and (2) and (3) are too. Plainly, (3) and (5) are equivalent. Further, (3) and (4) are equivalent by **(3.25)**(4). Always $f \in \overline{S}_f$; so (4) implies (6). Conversely, (6) implies $S_f \subset \overline{S}_g$; whence, **(3.25)**(1)(c) yields (4). Finally, (8) implies (4) by **(11.24)**(2). And (4) implies (7) by **(11.24)**(1). But $\overline{S}_f^{-1} R = S_f^{-1} R$ and $\overline{S}_g^{-1} R = S_g^{-1} R$ by **(11.23)**; whence, (7) implies both (8) and the last statement. □

Exercise (13.40) . — Let R be a ring. Prove these statements:

(1) $\mathbf{D}(f) \mapsto R_f$ is a well-defined contravariant functor from the category of principal open sets and inclusions to $((R\text{-alg}))$.

(2) Given $\mathfrak{p} \in \operatorname{Spec}(R)$, then $\varinjlim_{\mathbf{D}(f) \ni \mathfrak{p}} R_f = R_{\mathfrak{p}}$.

Solution: Consider (1). By **(13.39)**, if $\mathbf{D}(g) \subset \mathbf{D}(f)$, then there is a unique R-algebra map $\varphi^f_g\colon \overline{S}_f^{-1} R \to \overline{S}_g^{-1} R$. By uniqueness, if $\mathbf{D}(h) \subset \mathbf{D}(g) \subset \mathbf{D}(f)$, then $\varphi^g_h \varphi^f_g = \varphi^f_h$; also $\varphi^f_f = 1$. Further, if $\mathbf{D}(g) = \mathbf{D}(f)$, then $\overline{S}_f \subset \overline{S}_g$ and $\overline{S}_g \subset \overline{S}_f$, so $\overline{S}_f = \overline{S}_g$ and $\varphi^f_g = 1$. Finally, $R_f = \overline{S}_f^{-1} R$ by **(11.23)**(4). Thus (1) holds.

For (2), notice **(13.39)** yields an inclusion-reversing bijective correspondence between the principal open sets $\mathbf{D}(f)$ and the saturated multiplicative subsets $\overline{S}_f$. Further, $\mathbf{D}(f) \ni \mathfrak{p}$ if and only if $f \notin \mathfrak{p}$ by **(13.1)**.

Recall $S_\mathfrak{p} := R - \mathfrak{p}$. By **(3.24)**, $S_\mathfrak{p}$ is saturated. So $S_\mathfrak{p} \supset \overline{S}_f$ if and only if $f \notin \mathfrak{p}$ by **(3.25)**(1)(c). Moreover, $S_\mathfrak{p} = \bigcup_{f\notin\mathfrak{p}} \overline{S}_f$.

Note $\overline{S}_f^{-1}R = R_f$ by **(11.23)**(4). Thus $\varinjlim_{\mathbf{D}(f)\ni\mathfrak{p}} R_f = \varinjlim_{\overline{S}_f\subset S_\mathfrak{p}} \overline{S}_f^{-1}R$.

By the definition of saturation in **(3.25)**, $\overline{S}_{fg} \ni f,\, g$. By **(3.25)**(1)(b), $\overline{S}_{fg}$ is saturated multiplicative. So $\overline{S}_{fg} \supset \overline{S}_f,\, \overline{S}_g$ by **(3.25)**(1)(c). Hence, **(11.25)** with $R_\lambda := R$ implies $\varinjlim \overline{S}_f^{-1}R = S_\mathfrak{p}^{-1}R$. But $S_\mathfrak{p}^{-1}R =: R_\mathfrak{p}$. Thus (2) holds. □

Exercise (13.41) . — Let R be a ring, $X := \operatorname{Spec}(R)$, and U an open subset. Show U is quasi-compact if and only if $X - U = \mathbf{V}(\mathfrak{a})$ where $\mathfrak{a}$ is finitely generated.

Solution: Assume U is quasi-compact. By **(13.1)**, $U = \bigcup_\lambda \mathbf{D}(f_\lambda)$ for some f_λ. So $U = \bigcup_{i=1}^n \mathbf{D}(f_{\lambda_i})$ for some f_{λ_i}. Thus $X - U = \bigcap \mathbf{V}(f_{\lambda_i}) = \mathbf{V}(\langle f_{\lambda_1}, \dots, f_{\lambda_n}\rangle)$.

Conversely, assume $X - U = \mathbf{V}(\langle f_1, \dots, f_n\rangle)$. Then $U = \bigcup_{i=1}^n \mathbf{D}(f_i)$. But $\mathbf{D}(f_i) = \operatorname{Spec}(R_{f_i})$ by **(13.1.8)**. So by **(13.2)** with R_{f_i} for R, each $\mathbf{D}(f_i)$ is quasi-compact. Thus U is quasi-compact. □

Exercise (13.42) . — Let R be a ring, M a module. Set $X := \operatorname{Spec}(R)$. Assume $X = \bigcup_{\lambda\in\Lambda} \mathbf{D}(f_\lambda)$ for some set Λ and some $f_\lambda \in R$. Show:

(1) Given $m \in M$, assume $m/1 = 0$ in M_{f_λ} for all λ. Then $m = 0$.
(2) Given $m_\lambda \in M_{f_\lambda}$ for each λ, assume the images of m_λ and m_μ in $M_{f_\lambda f_\mu}$ are equal. Then there is a unique $m \in M$ whose image in M_{f_λ} is m_λ for all λ. First assume Λ is finite.

Solution: In (1), as $m/1 = 0$ in M_{f_λ}, there's $n_\lambda > 0$ with $f_\lambda^{n_\lambda} m = 0$. But $X = \bigcup \mathbf{D}(f_\lambda)$. Hence each prime excludes an f_λ, so $f_\lambda^{n_\lambda}$ too. So there are $\lambda_1, \dots, \lambda_n$ and $x_1, \dots, x_n$ with $1 = \sum x_i f_{\lambda_i}^{n_{\lambda_i}}$. So $m = \sum x_i f_{\lambda_i}^{n_{\lambda_i}} m = 0$. Thus (1) holds.

For (2), first assume Λ is finite. Given $\lambda \in \Lambda$, there are $l_\lambda \in M$ and $n_\lambda \ge 0$ with $m_\lambda/1 = l_\lambda/f_\lambda^{n_\lambda}$. Set $n := \max\{n_\lambda\}$ and $k_\lambda := f_\lambda^{n-n_\lambda} l_\lambda$. Thus $m_\lambda/1 = k_\lambda/f_\lambda^n$.

Given $\mu \in \Lambda$, by hypothesis $f_\mu^n k_\lambda/(f_\lambda f_\mu)^n = f_\lambda^n k_\mu/(f_\lambda f_\mu)^n$ in $M_{f_\lambda f_\mu}$. So there's $n_{\lambda,\mu} \ge 0$ with $(f_\lambda f_\mu)^{n_{\lambda,\mu}}(f_\mu^n k_\lambda - f_\lambda^n k_\mu) = 0$. So $(f_\lambda f_\mu)^p f_\mu^n k_\lambda = (f_\lambda f_\mu)^p f_\lambda^n k_\mu$ for $p := \max\{n_{\lambda,\mu}\}$. Set $h_\lambda := f_\lambda^p k_\lambda$. Thus $f_\lambda^{n+p} h_\mu = f_\mu^{n+p} h_\lambda$.

By hypothesis, $X = \bigcup \mathbf{D}(f_\lambda)$. So, as in the solution to (1), there are $x_\lambda \in R$ with $1 = \sum x_\lambda f_\lambda^{n+p}$. Set $m := \sum x_\lambda h_\lambda$. Then as $f_\lambda^{n+p} h_\mu = f_\mu^{n+p} h_\lambda$,

$$f_\mu^{n+p} m = \textstyle\sum_\lambda f_\mu^{n+p} x_\lambda h_\lambda = \sum_\lambda f_\lambda^{n+p} x_\lambda h_\mu = h_\mu = f_\mu^p k_\mu.$$

Thus the image of m in M_{f_μ} is $k_\mu/f_\mu^n = m_\mu$, as desired.

If $m' \in M$ also has image m_λ in M_{f_λ} for all λ, then $(m - m')/1 = 0$ in M_{f_λ} for all λ. So $m - m' = 0$ by (1). Thus m is unique.

In general, there's a finite subset Λ' of Λ with $X = \bigcup_{\lambda\in\Lambda'} \mathbf{D}(f_\lambda)$ by **(13.2)**. Apply the first case to Λ' to obtain $m \in M$ with image m_λ in M_{f_λ} for all $\lambda \in \Lambda'$.

Let's see m works. Given $\mu \in \Lambda$, apply the first case to $\Lambda' \cup \{\mu\}$ to obtain $m' \in M$ with image m_{λ_i} in $M_{f_{\lambda_i}}$ for all $\lambda \in \Lambda'$ and image m_μ in M_{f_μ}. By uniqueness $m' = m$. So m has image m_μ in M_{f_μ}. Thus (2) holds. □

Exercise (13.43) . — Let B be a Boolean ring, and set $X := \operatorname{Spec}(B)$. Show a subset $U \subset X$ is both open and closed if and only if $U = \mathbf{D}(f)$ for some $f \in B$. Further, show X is a compact Hausdorff space. (Following Bourbaki, we shorten "quasi-compact" to "compact" when the space is Hausdorff.)

Solution: Let $f \in B$. Then $\mathbf{D}(f) \bigcup \mathbf{D}(1-f) = X$ whether B is Boolean or not; indeed, if $\mathfrak{p} \in X - \mathbf{D}(f)$, then $f \in \mathfrak{p}$, so $1 - f \notin \mathfrak{p}$, so $\mathfrak{p} \in \mathbf{D}(1-f)$. However, $\mathbf{D}(f) \bigcap \mathbf{D}(1-f) = \emptyset$; indeed, if $\mathfrak{p} \in \mathbf{D}(f)$, then $f \notin \mathfrak{p}$, but $f(1-f) = 0$ as B is Boolean, so $1 - f \in \mathfrak{p}$, so $\mathfrak{p} \notin \mathbf{D}(1-f)$. Thus $X - \mathbf{D}(f) = \mathbf{D}(1-f)$. Thus $\mathbf{D}(f)$ is closed as well as open.

Conversely, let $U \subset X$ be open and closed. Then U is quasi-compact, as U is closed and X is quasi-compact by (**13.2**). So $X - U = \mathbf{V}(\mathfrak{a})$ where $\mathfrak{a}$ is finitely generated by (**13.41**). Since B is Boolean, $\mathfrak{a} = \langle f \rangle$ for some $f \in B$ by (**1.24**)(5). Thus $U = \mathbf{D}(f)$.

Finally, let $\mathfrak{p}$, $\mathfrak{q}$ be prime ideals with $\mathfrak{p} \neq \mathfrak{q}$. Then there is $f \in \mathfrak{p} - \mathfrak{q}$. So $\mathfrak{p} \notin \mathbf{D}(f)$, but $\mathfrak{q} \in \mathbf{D}(f)$. By the above, $\mathbf{D}(f)$ is both open and closed. Thus X is Hausdorff. By (**13.2**), X is quasi-compact, so compact as it is Hausdorff. □

Exercise (13.44) (*Stone's Theorem*) . — Show every Boolean ring B is isomorphic to the ring of continuous functions from a compact Hausdorff space X to $\mathbb{F}_2$ with the discrete topology. Equivalently, show B is isomorphic to the ring R of open and closed subsets of X; in fact, $X := \operatorname{Spec}(B)$, and $B \xrightarrow{\sim} R$ is given by $f \mapsto \mathbf{D}(f)$.

Solution: The two statements are equivalent by (**1.2**). Further, $X := \operatorname{Spec}(B)$ is compact Hausdorff, and its open and closed subsets are precisely the $\mathbf{D}(f)$ by (**13.43**). Thus $f \mapsto D(f)$ is a well defined function, and is surjective.

This function preserves multiplication owing to (**13.1.3**). To show it preserves addition, we must show that, for any $f, g \in B$,

$$\mathbf{D}(f+g) = (\mathbf{D}(f) - \mathbf{D}(g)) \bigcup (\mathbf{D}(g) - \mathbf{D}(f)). \tag{13.44.1}$$

Fix a prime $\mathfrak{p}$. There are four cases. First, if $f \notin \mathfrak{p}$ and $g \in \mathfrak{p}$, then $f + g \notin \mathfrak{p}$. Second, if $g \notin \mathfrak{p}$ but $f \in \mathfrak{p}$, then again $f + g \notin \mathfrak{p}$. In both cases, $\mathfrak{p}$ lies in the (open) sets on both sides of (**13.44.1**).

Third, if $f \in \mathfrak{p}$ and $g \in \mathfrak{p}$, then $f + g \in \mathfrak{p}$. The first three cases do not use the hypothesis that B is Boolean. The fourth does. Suppose $f \notin \mathfrak{p}$ and $g \notin \mathfrak{p}$. Now, $B/\mathfrak{p} = \mathbb{F}_2$ by (**2.37**). So the residues of f and g are both equal to 1. But $1 + 1 = 0 \in \mathbb{F}_2$. So again $f + g \in \mathfrak{p}$. Thus in both the third and fourth cases, $\mathfrak{p}$ lies in neither side of (**13.44.1**). Thus (**13.44.1**) holds.

Finally, to show that $f \mapsto \mathbf{D}(f)$ is injective, suppose that $\mathbf{D}(f)$ is empty. Then $f \in \operatorname{nil}(B)$. But $\operatorname{nil}(B) = \langle 0 \rangle$ by (**3.33**). Thus $f = 0$.

Alternatively, if $\mathbf{D}(f) = D(g)$, then $\mathbf{V}(\langle f \rangle) = \mathbf{V}(\langle g \rangle)$, so $\sqrt{\langle f \rangle} = \sqrt{\langle g \rangle}$ by (**13.1**). But $f, g \in \operatorname{Idem}(B)$ as B is Boolean. Thus $f = g$ by (**3.34**). □

Exercise (13.45) . — Let L be a Boolean lattice. Show that L is isomorphic to the lattice of open and closed subsets of a compact Hausdorff space.

Solution: By (**1.26**), L carries a canonical structure of Boolean ring. Set $X := \operatorname{Spec}(L)$. By (**13.43**), X is a compact Hausdorff space, and by (**13.44**), its ring M of open and closed subsets is isomorphic to L. By (**1.28**), M is a Boolean lattice, and its ring structure is produced by the construction of (**1.26**). So the ring structure on L is produced by this construction both from its given lattice structure and that induced by M. Thus by (**1.27**) these two lattice structures coincide. $\square$

Exercise (13.46) . — Let R be a ring, $\mathfrak{q}$ an ideal, M a module. Show:

(1) $\mathrm{Supp}(M/\mathfrak{q}M) \subset \mathrm{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q})$, with equality if M is finitely generated.

(2) Assume M is finitely generated. Then

$$\mathbf{V}(\mathfrak{q} + \mathrm{Ann}(M)) = \mathrm{Supp}(M/\mathfrak{q}M) = \mathbf{V}(\mathrm{Ann}(M/\mathfrak{q}M)).$$

Solution: For (1), note $M/\mathfrak{q}M = M \otimes R/\mathfrak{q}$ by (**8.27**)(1). But $\mathrm{Ann}(R/\mathfrak{q}) = \mathfrak{q}$; hence, (**13.4**)(3) yields $\mathrm{Supp}(R/\mathfrak{a}) = \mathbf{V}(\mathfrak{q})$. Thus (**13.7**) yields (1).

For (2), set $\mathfrak{a} := \mathrm{Ann}(M)$ and $\mathfrak{q}' := \mathrm{Ann}(M/\mathfrak{q}M)$. As M is finitely generated, (**13.1**) and (**13.4**)(3) and (1) and again (**13.4**)(3) yield, respectively,

$$\mathbf{V}(\mathfrak{a} + \mathfrak{q}) = \mathbf{V}(\mathfrak{a}) \bigcap \mathbf{V}(\mathfrak{q}) = \mathrm{Supp}(M) \bigcap \mathbf{V}(\mathfrak{q}) = \mathrm{Supp}(M/\mathfrak{q}M) = \mathbf{V}(\mathfrak{q}').$$

Thus (2) holds. $\square$

Exercise (13.47) . — Let $\varphi\colon R \to R'$ be a ring map, M' a finitely generated R'-module. Set $\varphi^* := \mathrm{Spec}(\varphi)$. Assume M' is flat over R. Then M' is faithfully flat if and only if $\varphi^* \,\mathrm{Supp}(M') = \mathrm{Spec}(R)$.

Solution: Assume M' is faithfully flat over R. Given $\mathfrak{p} \in \mathrm{Spec}(R)$, note that $M' \otimes_R R_\mathfrak{p}$ is faithfully flat over $R_\mathfrak{p}$ by (**9.22**). So replace R by $R_\mathfrak{p}$ and M' by $M' \otimes R_\mathfrak{p}$. Then R is local with maximal ideal $\mathfrak{p}$.

So $M' \otimes_R (R/\mathfrak{p}) \neq 0$ by (**9.19**). But $M' \otimes_R (R/\mathfrak{p}) = M'/\mathfrak{p}M'$ by (**8.27**)(1). So there's $\mathfrak{q} \in \mathrm{Supp}(M'/\mathfrak{p}M')$ by (**13.8**). But $\mathrm{Supp}(M'/\mathfrak{p}M') = \mathrm{Supp}(M') \cap \mathbf{V}(\mathfrak{p}R')$ by (**13.46**). So $\mathfrak{q} \in \mathrm{Supp}(M')$ and $\mathfrak{q} \supset \mathfrak{p}R'$. So $\varphi^{-1}\mathfrak{q} \supset \varphi^{-1}\mathfrak{p}R' \supset \mathfrak{p}$. But $\mathfrak{p}$ is maximal. So $\varphi^{-1}\mathfrak{q} = \mathfrak{p}$. Thus $\varphi^* \,\mathrm{Supp}(M') = \mathrm{Spec}(R)$.

For the converse, reverse the above argument. Assume $\varphi^* \,\mathrm{Supp}(M') = \mathrm{Spec}(R)$. Then given any maximal ideal $\mathfrak{m}$ of R, there is $\mathfrak{m}' \in \mathrm{Supp}(M')$ with $\varphi^{-1}\mathfrak{m}' = \mathfrak{m}$. So $\mathfrak{m}' \in \mathrm{Supp}(M') \cap \mathbf{V}(\mathfrak{m}R') = \mathrm{Supp}(M' \otimes_R (R/\mathfrak{m}))$. So $M' \otimes_R (R/\mathfrak{m}) \neq 0$. Thus (**9.19**) implies M' is faithfully flat. $\square$

Exercise (13.48) . — Let $\varphi\colon R \to R'$ be a ring map, M' a finitely generated R'-module, and $\mathfrak{q} \in \mathrm{Supp}(M')$. Assume that M' is flat over R. Set $\mathfrak{p} := \varphi^{-1}(\mathfrak{q})$. Show that φ induces a surjection $\mathrm{Supp}(M'_\mathfrak{q}) \twoheadrightarrow \mathrm{Spec}(R_\mathfrak{p})$.

Solution: Recall $S_\mathfrak{p} := R - \mathfrak{p}$. So $R'_\mathfrak{p} = R'_{\varphi S_\mathfrak{p}}$ by (**11.15.1**). But $\mathfrak{p} = \varphi^{-1}(\mathfrak{q})$, so $\varphi S_\mathfrak{p} \subset S_\mathfrak{q}$. So $R'_\mathfrak{q}$ and $M'_\mathfrak{q}$ are localizations of $R'_\mathfrak{p}$ and $M'_\mathfrak{p}$ by (**12.25**)(2). Further, owing to (**11.12**)(2), the composition $R_p \xrightarrow{\varphi_\mathfrak{p}} R'_\mathfrak{p} \to R'_\mathfrak{q}$ is a local ring map.

Moreover, $M'_\mathfrak{p} = R_\mathfrak{p} \otimes_R M'$ by (**12.10**), and $R_\mathfrak{p} \otimes_R M'$ is flat over $R_\mathfrak{p}$ by (**9.22**); so $M'_\mathfrak{p}$ is flat over $R_\mathfrak{p}$. Also, $M'_\mathfrak{q} = R'_\mathfrak{q} \otimes_{R'_\mathfrak{p}} M'_\mathfrak{p}$ by (**12.10**), and $R'_\mathfrak{q}$ is flat over $R'_\mathfrak{p}$ by (**12.14**); so $M'_\mathfrak{q}$ is flat over $R_\mathfrak{p}$ by (**9.26**). So $M'_\mathfrak{q}$ is faithfully flat over $R_\mathfrak{p}$ by (**10.30**) as $\mathfrak{q} \in \mathrm{Supp}(M')$. Thus (**13.47**) yields the desired surjectivity. $\square$

Exercise (13.49) . — Let $\varphi\colon R \to R'$ be a map of rings, M an R-module. Prove

$$\mathrm{Supp}(M \otimes_R R') \subset \mathrm{Spec}(\varphi)^{-1}(\mathrm{Supp}(M)), \qquad (\mathbf{13.49.1})$$

with equality if M is finitely generated.

Solution: Fix a prime $\mathfrak{q} \subset R'$. Set $\mathfrak{p} := \varphi^{-1}\mathfrak{q}$, so $\mathrm{Spec}(\varphi)(\mathfrak{p}) = \mathfrak{q}$. Apply, in order, **(12.10)**, twice Cancellation **(8.9)**(1), and again **(12.10)** to obtain

$$\begin{aligned}(M \otimes_R R')_{\mathfrak{q}} &= (M \otimes_R R') \otimes_{R'} R'_{\mathfrak{q}} = M \otimes_R R'_{\mathfrak{q}} \\ &= (M \otimes_R R_{\mathfrak{p}}) \otimes_{R_{\mathfrak{p}}} R'_{\mathfrak{q}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R'_{\mathfrak{q}}.\end{aligned} \tag{13.49.2}$$

First, assume $\mathfrak{q} \in \mathrm{Supp}(M \otimes_R R')$; that is, $(M \otimes_R R')_{\mathfrak{q}} \neq 0$. Then **(13.49.2)** implies $M_{\mathfrak{p}} \neq 0$; that is, $\mathfrak{p} \in \mathrm{Supp}(M)$. Thus **(13.49.1)** holds.

Conversely, assume $\mathfrak{q} \in \mathrm{Spec}(\varphi)^{-1}(\mathrm{Supp}(M))$. Then $\mathfrak{p} \in \mathrm{Supp}(M)$, or $M_{\mathfrak{p}} \neq 0$. Set $k := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. Then $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} k$ and $R'_{\mathfrak{p}}/\mathfrak{p}R'_{\mathfrak{p}} = R'_{\mathfrak{p}} \otimes_A k$ by **(8.27)**(1). Hence Cancellation **(8.9)**(1), the Associative Law **(8.8)**(1), and **(13.49.2)** yield

$$\begin{aligned}(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}) \otimes_k (R'_{\mathfrak{q}}/\mathfrak{p}R'_{\mathfrak{q}}) &= (M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} k) \otimes_k (R'_{\mathfrak{q}} \otimes_{R_{\mathfrak{p}}} k) \\ &= M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} (R'_{\mathfrak{q}} \otimes_{R_{\mathfrak{p}}} k) = (M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} R'_{\mathfrak{q}}) \otimes_{R_{\mathfrak{p}}} k \\ &= (M \otimes_R R')_{\mathfrak{q}} \otimes_{R_{\mathfrak{p}}} k.\end{aligned} \tag{13.49.3}$$

Assume M is finitely generated. Then $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}} \neq 0$ by Nakayama's Lemma **(10.6)** over $R_{\mathfrak{p}}$. And $R'_{\mathfrak{q}}/\mathfrak{p}R'_{\mathfrak{q}} \neq 0$ by Nakayama's Lemma **(10.6)** over $R'_{\mathfrak{q}}$, because $\mathfrak{p}R' \subset \mathfrak{q}$. So $(M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}) \otimes_k (R'_{\mathfrak{q}}/\mathfrak{p}R'_{\mathfrak{q}}) \neq 0$ by **(8.24)**. So **(13.49.3)** implies that $(M \otimes_R R')_{\mathfrak{q}} \neq 0$, or $\mathfrak{q} \in \mathrm{Supp}(M \otimes_R R')$. Thus equality holds in **(13.49.1)**. □

Exercise (13.50) . — Let R be a ring, M a module, $\mathfrak{p} \in \mathrm{Supp}(M)$. Prove

$$\mathbf{V}(\mathfrak{p}) \subset \mathrm{Supp}(M).$$

Solution: Let $\mathfrak{q} \in \mathbf{V}(\mathfrak{p})$. Then $\mathfrak{q} \supset \mathfrak{p}$. So $M_{\mathfrak{p}} = (M_{\mathfrak{q}})_{\mathfrak{p}}$ by **(12.25)**(3). Now, $\mathfrak{p} \in \mathrm{Supp}(M)$. So $M_{\mathfrak{p}} \neq 0$. Hence $M_{\mathfrak{q}} \neq 0$. Thus $\mathfrak{q} \in \mathrm{Supp}(M)$. □

Exercise (13.51) . — Set $M := \mathbb{Q}/\mathbb{Z}$. Find $\mathrm{Supp}(M)$, and show it's not Zariski closed in $\mathrm{Spec}(\mathbb{Z})$. Is $\mathrm{Supp}(M) = \mathbf{V}(\mathrm{Ann}(M))$? What about **(13.4)**(3)?

Solution: Let $\mathfrak{p} \in \mathrm{Spec}(\mathbb{Z})$. Then $M_{\mathfrak{p}} = \mathbb{Q}_{\mathfrak{p}}/\mathbb{Z}_{\mathfrak{p}}$ since localization is exact by **(12.13)**. Now, $\mathbb{Q}_{\mathfrak{p}} = \mathbb{Q}$ by **(12.4)**(2) and **(12.1)** since $\mathbb{Q}$ is a field. If $\mathfrak{p} \neq \langle 0\rangle$, then $\mathbb{Z}_{\mathfrak{p}} \neq \mathbb{Q}_{\mathfrak{p}}$ since $\mathfrak{p}\mathbb{Z}_{\mathfrak{p}} \bigcap \mathbb{Z} = \mathfrak{p}$ by **(11.12)**(2). If $\mathfrak{p} = \langle 0\rangle$, then $\mathbb{Z}_{\mathfrak{p}} = \mathbb{Q}_{\mathfrak{p}}$. Thus $\mathrm{Supp}(M)$ consists of all the nonzero primes of $\mathbb{Z}$.

Finally, suppose $\mathrm{Supp}(M) = \mathbf{V}(\mathfrak{a})$. Then $\mathfrak{a}$ lies in every nonzero prime; so $\mathfrak{a} = \langle 0\rangle$. But $\langle 0\rangle$ is prime. Hence $\langle 0\rangle \in \mathbf{V}(\mathfrak{a}) = \mathrm{Supp}(M)$, contradicting the above. Thus $\mathrm{Supp}(M)$ is not closed. In particular, $\mathrm{Supp}(M) \neq \mathbf{V}(\mathrm{Ann}(M)$. However, M is not finitely generated; so **(13.4)**(3) doesn't apply. □

Exercise (13.52) . — Let R be a domain, M a module. Set $T(M) := T^{S_0}(M)$. Call $T(M)$ the **torsion submodule** of M, and M **torsionfree** if $T(M) = 0$.

Prove M is torsionfree if and only if $M_{\mathfrak{m}}$ is torsionfree for all maximal ideals $\mathfrak{m}$.

Solution: Given an $\mathfrak{m}$, note $R - \mathfrak{m} \subset R - \langle 0\rangle$, or $S_{\mathfrak{m}} \subset S_0$. So **(12.38)**(5) yields

$$T(M_{\mathfrak{m}}) = T(M)_{\mathfrak{m}}. \tag{13.52.1}$$

Assume M is torsionfree. Then $M_{\mathfrak{m}}$ is torsionfree for all $\mathfrak{m}$ by **(13.52.1)**. Conversely, if $M_{\mathfrak{m}}$ is torsionfree for all $\mathfrak{m}$, then $T(M)_{\mathfrak{m}} = 0$ for all $\mathfrak{m}$ by **(13.52.1)**. Hence $T(M) = 0$ by **(13.8)**. Thus M is torsionfree. □

Exercise (13.53) . — Let R be a ring, P a module, M, N submodules. Assume $M_{\mathfrak{m}} = N_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Show $M = N$. First assume $M \subset N$.

Solution: If $M \subset N$, then (**12.13**) yields $(N/M)_{\mathfrak{m}} = N_{\mathfrak{m}}/M_{\mathfrak{m}} = 0$ for each $\mathfrak{m}$; so $N/M = 0$ by (**13.8**). The general case follows by replacing N by $M + N$ owing to (**12.12**)(7)(b). □

Exercise (13.54) . — Let R be a ring, M a module, and $\mathfrak{a}$ an ideal. Suppose $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$ containing $\mathfrak{a}$. Show that $M = \mathfrak{a}M$.

Solution: Given any maximal ideal $\mathfrak{m}$, note that $(\mathfrak{a}M)_{\mathfrak{m}} = \mathfrak{a}_{\mathfrak{m}}M_{\mathfrak{m}}$ by (**12.2**). But $M_{\mathfrak{m}} = 0$ if $\mathfrak{m} \supset \mathfrak{a}$ by hypothesis. And $\mathfrak{a}_{\mathfrak{m}} = R_{\mathfrak{m}}$ if $\mathfrak{m} \not\supset \mathfrak{a}$ by (**11.8**)(2). Hence $M_{\mathfrak{m}} = (\mathfrak{a}M)_{\mathfrak{m}}$ in any case. Thus (**13.53**) yields $M = \mathfrak{a}M$.

Alternatively, form the ring $R/\mathfrak{a}$ and its module $M/\mathfrak{a}M$. Given any maximal ideal $\mathfrak{m}'$ of $R/\mathfrak{a}$, say $\mathfrak{m}' = \mathfrak{m}/\mathfrak{a}$. By hypothesis, $M_{\mathfrak{m}} = 0$. But $M_{\mathfrak{m}}/(\mathfrak{a}M)_{\mathfrak{m}} = (M/\mathfrak{a}M)_{\mathfrak{m}}$ by (**12.15**). Thus $(M/\mathfrak{a}M)_{\mathfrak{m}'} = 0$. So $M/\mathfrak{a}M = 0$ by (**13.8**). Thus $M = \mathfrak{a}M$. □

Exercise (13.55) . — Let R be a ring, P a module, M a submodule, and $p \in P$ an element. Assume $p/1 \in M_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$. Show $p \in M$.

Solution: Set $N := M + Rp$. Then $N_{\mathfrak{m}} = M_{\mathfrak{m}} + R_{\mathfrak{m}} \cdot p/1$ for every $\mathfrak{m}$. But $p/1 \in M_{\mathfrak{m}}$. Hence $N_{\mathfrak{m}} = M_{\mathfrak{m}}$. So $N = M$ by (**13.53**). Thus $p \in M$. □

Exercise (13.56) . — Let R be a domain, $\mathfrak{a}$ an ideal. Show $\mathfrak{a} = \bigcap_{\mathfrak{m}} \mathfrak{a}R_{\mathfrak{m}}$ where $\mathfrak{m}$ runs through the maximal ideals and the intersection takes place in $\mathrm{Frac}(R)$.

Solution: Plainly, $\mathfrak{a} \subset \bigcap \mathfrak{a}R_{\mathfrak{m}}$. Conversely, take $x \in \bigcap \mathfrak{a}R_{\mathfrak{m}}$. Then $x \in \mathfrak{a}R_{\mathfrak{m}}$ for every $\mathfrak{m}$. But $\mathfrak{a}R_{\mathfrak{m}} = \mathfrak{a}_{\mathfrak{m}}$ by (**12.2**). So (**13.55**) yields $x \in \mathfrak{a}$ as desired. □

Exercise (13.57) . — Prove these three conditions on a ring R are equivalent:

(1) R is reduced.
(2) $S^{-1}R$ is reduced for all multiplicative subsets S.
(3) $R_{\mathfrak{m}}$ is reduced for all maximal ideals $\mathfrak{m}$.

Solution: Assume (1) holds. Then $\mathrm{nil}(R) = 0$. But $\mathrm{nil}(R)(S^{-1}R) = \mathrm{nil}(S^{-1}R)$ by (**11.28**). Thus (2) holds. Trivially (2) implies (3).

Assume (3) holds. Then $\mathrm{nil}(R_{\mathfrak{m}}) = 0$. Hence $\mathrm{nil}(R)_{\mathfrak{m}} = 0$ by (**11.28**) and (**12.2**). So $\mathrm{nil}(R) = 0$ by (**13.8**). Thus (1) holds. Thus (1)–(3) are equivalent. □

Exercise (13.58) . — Let R be a ring, Σ the set of minimal primes. Prove this:

(1) If $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$, then the $\mathfrak{p} \in \Sigma$ are pairwise comaximal.
(2) $R_{\mathfrak{p}}$ is a domain for any prime $\mathfrak{p}$ and Σ is finite if and only if $R = \prod_{i=1}^{n} R_i$ where R_i is a domain. If so, then $R_i = R/\mathfrak{p}_i$ with $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \Sigma$.

If $R_{\mathfrak{m}}$ is a domain for all maximal ideals $\mathfrak{m}$, is R necessarily a domain?

Solution: Consider (1). Suppose $\mathfrak{p}, \mathfrak{q} \in \Sigma$ are not comaximal. Then $\mathfrak{p} + \mathfrak{q}$ lies in some maximal ideal $\mathfrak{m}$. Hence $R_{\mathfrak{m}}$ contains two minimal primes, $\mathfrak{p}R_{\mathfrak{m}}$ and $\mathfrak{q}R_{\mathfrak{m}}$, by (**11.12**)(2). However, $R_{\mathfrak{m}}$ is a domain by hypothesis, and so $\langle 0 \rangle$ is its only minimal prime. Hence $\mathfrak{p}R_{\mathfrak{m}} = \mathfrak{q}R_{\mathfrak{m}}$. So $\mathfrak{p} = \mathfrak{q}$. Thus (1) holds.

Consider (2). Assume $R_{\mathfrak{p}}$ is a domain for any $\mathfrak{p}$. Then R is reduced by (**13.57**). Assume, also, Σ is finite. Form the canonical map $\varphi\colon R \to \prod_{\mathfrak{p}\in\Sigma} R/\mathfrak{p}$; it is injective by (**3.41**), and surjective by (1) and the Chinese Remainder Theorem (**1.21**)(4)(c). Thus R is a finite product of domains.

Conversely, assume $R = \prod_{i=1}^{n} R_i$ where R_i is a domain. Let $\mathfrak{p}$ be a prime of R. Then $R_{\mathfrak{p}} = \prod (R_i)_{\mathfrak{p}}$ by (**12.9**). Each $(R_i)_{\mathfrak{p}}$ is a domain by (**11.2**). But $R_{\mathfrak{p}}$ is local. So $R_{\mathfrak{p}} = (R_i)_{\mathfrak{p}}$ for some i by (**3.6**). Thus $R_{\mathfrak{p}}$ is a domain. Further, owing to

(**2.29**), each $\mathfrak{p}_i \in \Sigma$ has the form $\mathfrak{p}_i = \prod \mathfrak{a}_j$ where, after renumbering, $\mathfrak{a}_i = \langle 0 \rangle$ and $\mathfrak{a}_j = R_j$ for $j \neq i$. Thus the ith projection gives $R/\mathfrak{p}_i \xrightarrow{\sim} R_i$. Thus (2) holds.

Finally, the answer is no. For example, take $R := k_1 \times k_2$ with $k_i := \mathbb{Z}/\langle 2 \rangle$. The primes of R are $\mathfrak{p} := \langle (1,0) \rangle$ and $\mathfrak{q} := \langle (0,1) \rangle$ by (**2.29**). Further, $R_\mathfrak{q} = k_1$ by (**11.5**), as $R - \mathfrak{q} = \{(1,1),\, (1,0)\}$. Similarly $R_\mathfrak{p} = k_2$. But R is not a domain, as $(1,0) \cdot (0,1) = (0,0)$, although $R_\mathfrak{m}$ is a domain for all maximal ideals $\mathfrak{m}$.

In fact, take $R := R_1 \times R_2$ for any domains R_i. Then again R is not a domain, but $R_\mathfrak{p}$ is a domain for all primes $\mathfrak{p}$ by (2). □

Exercise (13.59) . — Let R be a ring, M a module. Assume that there are only finitely many maximal ideals $\mathfrak{m}_i$ with $M_{\mathfrak{m}_i} \neq 0$. Show that the canonical map $\alpha\colon M \to \prod M_{\mathfrak{m}_i}$ is bijective if and only if $(M_{\mathfrak{m}_i})_{\mathfrak{m}_j} = 0$ whenever $i \neq j$.

Solution: By (**13.9**), the map α is bijective if and only if each localization $\alpha_{\mathfrak{m}_j}\colon M_{\mathfrak{m}_j} \to (\prod M_{\mathfrak{m}_i})_{\mathfrak{m}_j}$ is bijective. As the product is finite, it commutes with localization by (**12.9**). But $(M_{\mathfrak{m}_j})_{\mathfrak{m}_j} = M_{\mathfrak{m}_j}$ by (**12.4**)(2). Thus $\alpha_{\mathfrak{m}_j}$ is bijective if and only if $(M_{\mathfrak{m}_i})_{\mathfrak{m}_j} = 0$ whenever $i \neq j$. □

Exercise (13.60) . — Let R be a ring, R' a flat algebra, $\mathfrak{p}'$ a prime in R', and $\mathfrak{p}$ its contraction in R. Prove that $R'_{\mathfrak{p}'}$ is a faithfully flat $R_\mathfrak{p}$-algebra.

Solution: Note $R'_\mathfrak{p}$ is flat over $R_\mathfrak{p}$ by (**13.12**). And $R'_{\mathfrak{p}'} = (R'_\mathfrak{p})_{\mathfrak{p}'}$ by (**12.25**)(2) as $R - \mathfrak{p} \subset R' - \mathfrak{p}'$; so $R'_{\mathfrak{p}'}$ is flat over $R'_\mathfrak{p}$ by (**12.14**). Hence $R'_{\mathfrak{p}'}$ is flat over $R_\mathfrak{p}$ by (**9.23**). But a flat local map is faithfully flat by (**10.30**), as desired. □

Exercise (13.61) . — Let R be an absolutely flat ring, $\mathfrak{p}$ a prime. Show $\mathfrak{p}$ is maximal, $R_\mathfrak{p}$ is a field, and R is reduced,

Solution: Note $R/\operatorname{nil}(R)$ is absolutely flat by (**10.26**)(2). Thus $\mathfrak{p}$ is maximal by (**13.22**). Thus $R_\mathfrak{p}$ is a field by (**13.21**)(2). So $R_\mathfrak{p}$ is reduced. Thus (**13.57**) implies R is reduced. □

Exercise (13.62) . — Given n, prove an R-module P is locally free of rank n if and only if P is finitely generated and $P_\mathfrak{m} \simeq R^n_\mathfrak{m}$ holds at each maximal ideal $\mathfrak{m}$.

Solution: If P is locally free of rank n, then P is finitely generated by (**13.15**). But, given $\mathfrak{p} \in \operatorname{Spec}(R)$, there's $f \in R - \mathfrak{p}$ with $P_f \simeq R^n_f$; so $P_\mathfrak{p} \simeq R^n_\mathfrak{p}$ by (**12.25**)(2).

As to the converse, given any prime $\mathfrak{p}$, take a maximal ideal $\mathfrak{m}$ containing it. Assume $P_\mathfrak{m} \simeq R^n_\mathfrak{m}$. Take a free basis $p_1/s_1, \dots, p_n/s_n$ of $P_\mathfrak{m}$ over $R_\mathfrak{m}$ with $p_i \in P$ and $s_i \in R - \mathfrak{m}$ for all i. The p_i define a map $\alpha\colon R^n \to P$, and $\alpha_\mathfrak{m}\colon R^n_\mathfrak{m} \to P_\mathfrak{m}$ is bijective, so surjective.

Assume P is finitely generated. Then (**12.18**)(1) provides $f \in R - \mathfrak{m}$ such that $\alpha_f\colon R^n_f \to P_f$ is surjective. Hence $\alpha_\mathfrak{q}\colon R^n_\mathfrak{q} \to P_\mathfrak{q}$ is surjective for every $\mathfrak{q} \in \mathbf{D}(f)$ by (**12.13**) as $(\alpha_f)_\mathfrak{q} = \alpha_\mathfrak{q}$ owing to (**12.25**)(2).

In addition, assume $P_\mathfrak{q} \simeq R^n_\mathfrak{q}$ if $\mathfrak{q}$ is maximal. Then $\alpha_\mathfrak{q}$ is bijective by (**10.4**). But $\alpha_\mathfrak{q} = (\alpha_f)_{(\mathfrak{q}R_f)}$ owing to (**12.25**)(2). Hence $\alpha_f\colon R^n_f \to P_f$ is bijective by (**13.9**) with R_f for R. But $\mathfrak{p} \in \mathbf{D}(f)$. Thus P is locally free of rank n. □

Exercise (13.63) . — Let A be a semilocal ring, P a locally free module of rank n. Show that P is free of rank n.

Solution: As P is locally free, P is finitely presented by (**13.15**), and $P_\mathfrak{m} \simeq A^n_\mathfrak{m}$ at each maximal $\mathfrak{m}$ by (**13.62**). But A is semilocal. So $P \simeq A^n$ by (**13.11**). □

Exercise (13.64) . — Let R be a ring, M a finitely presented module, $n \ge 0$. Show that M is locally free of rank n if and only if $F_{n-1}(M) = \langle 0 \rangle$ and $F_n(M) = R$.

Solution: Assume M is locally free of rank n. Then $M_{\mathfrak{m}} \simeq R^n_{\mathfrak{m}}$ for any maximal ideal $\mathfrak{m}$ by (13.62). So $F_{n-1}(M_{\mathfrak{m}})\langle 0 \rangle$ and $F_n(M_{\mathfrak{m}}) = R_{\mathfrak{m}}$ by (5.39)(2). But $F_r(M_{\mathfrak{m}}) = F_r(M)_{\mathfrak{m}}$ for all r by (12.36). So $F_{n-1}(M_{\mathfrak{m}}) = \langle 0 \rangle$ and $F_n(M_{\mathfrak{m}}) = R_{\mathfrak{m}}$ by (13.53). The converse follows via reversing the above steps. □

14. Cohen–Seidenberg Theory

Exercise (14.10) . — Let R'/R be an integral extension of rings, $x \in R$. Show (1) if $x \in R'^{\times}$, then $x \in R^{\times}$ and (2) $\mathrm{rad}(R) = \mathrm{rad}(R') \cap R$.

Solution: For (1), say $xy = 1$ with $y \in R'$. Say $y^n + a_{n-1}y^{n-1} + \cdots + a_0 = 0$ with $a_i \in R$. Then $y = -a_{n-1} - a_{n-2}x - \cdots - a_0 x^{n-1}$. So $y \in R$. Thus (1) holds.

For (2), use double inclusion. Given a maximal ideal $\mathfrak{m}' \subset R'$, note $\mathfrak{m}' \cap R$ is maximal by (14.3)(1). So if $x \in \mathrm{rad}(R)$, then $x \in \mathfrak{m}'$. Thus $\mathrm{rad}(R) \subset \mathrm{rad}(R') \cap R$.

Conversely, given a maximal ideal $\mathfrak{m} \subset R$, there is a maximal ideal $\mathfrak{m}' \subset R'$ with $\mathfrak{m}' \cap R = \mathfrak{m}$ by (14.3)(1),(3). So given $y \in \mathrm{rad}(R') \cap R$, then $y \in \mathfrak{m}$. Hence $\mathrm{rad}(R) \supset \mathrm{rad}(R') \cap R$. Thus (2) holds. □

Exercise (14.11) . — Let $\varphi\colon R \to R'$ be a map of rings. Assume R' is integral over R. Show the map $\mathrm{Spec}(\varphi)\colon \mathrm{Spec}(R') \to \mathrm{Spec}(R)$ is closed.

Solution: Given a closed set $\mathbf{V}(\mathfrak{b}) \subset \mathrm{Spec}(R')$, set $\mathfrak{a} := \varphi^{-1}(\mathfrak{b})$. Plainly, $R'/\mathfrak{b}$ is an integral extension of $R/\mathfrak{a}$. So every prime of $R/\mathfrak{a}$ is the contraction of a prime of $R'/\mathfrak{b}$ by (14.3)(3). So $\mathrm{Spec}(R'/\mathfrak{b})$ maps onto $\mathrm{Spec}(R/\mathfrak{a})$ by (13.24)(1). Hence (13.1.7) yields $\mathrm{Spec}(\varphi)(\mathbf{V}(\mathfrak{b})) = \mathbf{V}(\mathfrak{a})$. Thus $\mathrm{Spec}(\varphi)$ is closed. □

Exercise (14.12) . — Let R'/R be an integral extension of rings, $\rho\colon R \to \Omega$ a map to an algebraically closed field. Show ρ extends to a map $\rho'\colon R' \to \Omega$. First, assume R'/R is an algebraic extension of fields K/k, and use Zorn's lemma on the set $\mathcal{S}$ of all extensions $\lambda\colon L \to \Omega$ of ρ where $L \subset K$ is a subfield containing k.

Solution: First, given a totally ordered set of extensions $\lambda_i\colon L_i \to \Omega$ in $\mathcal{S}$, set $L := \bigcup L_i$, and for $x \in L$, set $\lambda(x) := \lambda_i(x)$ if $x \in L_i$. Then λ is an upper bound. So Zorn's Lemma yields a maximal extension $\lambda\colon L \to \Omega$.

Given $x \in K$, take a variable X, and define $\varphi\colon L[X] \to L[x]$ by $\varphi(X) := x$. Then φ is surjective. But L is a field. So $\mathrm{Ker}(\varphi) = \langle F \rangle$ for some $F \in L[X]$. As x is algebraic, $F \neq 0$. As Ω is algebraically closed, $\lambda(F) \in \Omega[X]$ has a root $y \in \Omega$.

Define $\omega\colon L[X] \to \Omega$ by $\omega(X) := y$. Then $\omega(F) = 0$. So ω factors through a map $L[X]/\langle F \rangle \to \Omega$ extending λ. But $L[X]/\langle F \rangle = L[x]$, and λ is maximal. Hence $x \in L$. Thus $L = K$, and λ is the desired extension of ρ.

For the general case, set $\mathfrak{p} := \mathrm{Ker}(\rho)$. Then $\mathfrak{p}$ is prime. Further, given $s \in R - \mathfrak{p}$, note $\rho(s)$ is nonzero, so invertible as Ω is a field. Hence ρ factors through a map $\pi\colon R_{\mathfrak{p}} \to \Omega$ by (11.3). But $\rho(\mathfrak{p}) = 0$, so $\pi(\mathfrak{p}R_{\mathfrak{p}}) = 0$. Set $k := R_{\mathfrak{p}}\big/\mathfrak{p}R_{\mathfrak{p}}$. Then k is a field, and π factors through a map $\kappa\colon k \to \Omega$.

Moreover, $R'_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$ by (11.29). Also, $R_{\mathfrak{p}} \to R'_{\mathfrak{p}}$ is injective by (12.13). So there's a maximal ideal $\mathfrak{M}$ of $R'_{\mathfrak{p}}$ lying over $\mathfrak{p}R_{\mathfrak{p}}$ by (14.3)(1), (3). Set $K := R'_{\mathfrak{p}}/\mathfrak{M}$. Then K is a field, and an algebraic extension of k. Hence κ extends to a map $\kappa'\colon K \to \Omega$ by the first case. Plainly, the composition $R' \to R'_{\mathfrak{p}} \to K \to \Omega$ is the desired map ρ'. □

Exercise (14.13) (*E. Artin*) . — Form the algebraic closure of a field k as follows:

(1) Let X be a variable, $\mathcal{S}$ the set of all monic $F \in k[X]$, and X_F a variable for each $F \in \mathcal{S}$. Set $P := k[\{X_F\}]$ and $\mathfrak{a} := \langle \{F(X_F)\} \rangle$. Show $1 \notin \mathfrak{a}$. Conclude k has an algebraic extension k_1 in which each $F \in \mathcal{S}$ has a root.

(2) Apply (1) repeatedly to obtain a chain $k_0 := k \subset k_1 \subset k_2 \subset \cdots$ such that every monic polynomial with coefficients in k_n has a root in k_{n+1} for all n. Set $K := \varinjlim k_n$. Show K is an algebraic closure of k.

(3) Using **(14.12)**, show any two algebraic closures K_1, K_2 are k-isomorphic.

Solution: For (1), suppose $1 \in \mathfrak{a}$. Say $1 = \sum G_i F_i(X_{F_i})$ with $G_i \in P$ and $F_i \in \mathcal{S}$. By **(14.4)**(1), there's an extension $R \supset k$ with $x_i \in R$ such that $F_i(x_i) = 0$. Define $\varphi\colon P \to R$ by $\varphi(X_{F_i}) = x_i$ and $\varphi(X_F) := 0$ for $F \neq F_i$ for all i. Then $1 = \varphi\big(\sum G_i F_i(X_{F_i})\big) = \sum \varphi(G_i) F_i(x_i) = 0$, a contradiction. Thus $1 \notin \mathfrak{a}$.

So $\mathfrak{a}$ lies in a maximal ideal $\mathfrak{m}$ of P. Set $k_1 := P/\mathfrak{m}$; let x_F be the residue of X_F. Then k_1 is an extension field of k. In k_1, every $F \in \mathcal{S}$ has a root, as $F(x_F) = 0$. But F is monic; so x_F is integral over k. Also, the x_F generate k_1 by construction. So k_1 is the integral closure of k in k_1 by **(10.20)**. Thus (1) holds.

For (2), note **(7.16)**(3) implies that K is a field, that each insertion $k_n \to K$ is injective, and that $K = \bigcup k_n$ after k_n is identified with its image. Hence every monic polynomial with coefficients in K has all its coefficients in some k_n, so it has a root in $k_{n+1} \subset K$. So K is algebraically closed. Thus (2) holds.

For (3), use **(14.12)** to extend $1_k\colon k \to k$ to a ring map $\lambda\colon K_1 \to K_2$. Then λ is injective as K_1 is a field. But K_2 is algebraic over k. So each $x \in K_2$ is a root of a monic polynomial $F \in k[X]$. But λK_1 is algebraically closed. So λK_1 contains a root y of F. Then $F = (X - y)G$ by **(1.19)**. So if $x \neq y$, then $G(x) = 0$ and $x \in \lambda K_1$ by induction on $\deg(G)$. Thus λ is surjective. Thus (3) holds. □

Exercise (14.14) . — Let R be a domain, $\overline{R}$ its integral closure, $K := \mathrm{Frac}(R)$. Let L/K be a field extension, $y \in L$ algebraic with monic minimal polynomial $G(X) \in K[X]$. Show that y is integral over R if and only if $G \in \overline{R}[X]$.

Solution: If $G \in \overline{R}[X]$, then y is integral over $\overline{R}$, so over R by **(10.17)**(1).

Conversely, assume y is integral over R. Then there is a monic polynomial $F \in R[X]$ with $F(y) = 0$. Say $F = GH$ with $H \in K[X]$. Then by **(14.4)**(2), the coefficients of G are integral over R, so in $\overline{R}$, as desired. □

Exercise (14.15) . — Let R'/R be an integral extension of rings, and $\mathfrak{p}$ a prime of R. Assume R' has just one prime $\mathfrak{p}'$ over $\mathfrak{p}$. Show (1) that $\mathfrak{p}'R'_\mathfrak{p}$ is the only maximal ideal of $R'_\mathfrak{p}$, (2) that $R'_{\mathfrak{p}'} = R'_\mathfrak{p}$, and (3) that $R'_{\mathfrak{p}'}$ is integral over $R_\mathfrak{p}$.

Solution: Note $R'_\mathfrak{p}$ is integral over $R_\mathfrak{p}$ by **(11.29)**, as R' is integral over R.

For (1), recall $R_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$ by **(11.14)**. Hence, every maximal ideal of $R'_\mathfrak{p}$ lies over $\mathfrak{p}R_\mathfrak{p}$ by **(14.3)**(1). But every maximal ideal of $R'_\mathfrak{p}$ is the extension of some prime $\mathfrak{q}' \subset R'$ by **(11.12)**(2), and therefore $\mathfrak{q}'$ lies over $\mathfrak{p}$ in R. So, by hypothesis, $\mathfrak{q}' = \mathfrak{p}'$. Thus (1) holds.

For (2), let's check $R'_\mathfrak{p}$ has the UMP of $R'_{\mathfrak{p}'}$. Set $S := R' - \mathfrak{p}'$. First, $R'_\mathfrak{p} - \mathfrak{p}'R'_\mathfrak{p}$ consists of units by (1); so $\varphi_\mathfrak{p} S$ does too. Second, $R - \mathfrak{p} \subset S$; so any ring map $\psi\colon R' \to R''$ with $\psi S \subset (R'')^\times$ factors uniquely through $R'_\mathfrak{p}$. Thus (2) holds.

Finally, (3) follows from (2), since, as noted above, $R'_\mathfrak{p}$ is integral over $R_\mathfrak{p}$. □

Exercise (14.16) . — Let R'/R be an integral extension of rings, $\mathfrak{p} \subset R$ a prime, $\mathfrak{p}'$, $\mathfrak{q}' \subset R'$ two distinct primes lying over $\mathfrak{p}$. Assume R' is a domain, or simply, $R'_{\mathfrak{p}} \subset R'_{\mathfrak{p}'}$. Show that $R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$. Show that, in fact, given $y \in \mathfrak{q}' - \mathfrak{p}'$, then $1/y \in R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$.

Solution: Some $y \in \mathfrak{q}' - \mathfrak{p}'$ exists; else, $\mathfrak{q}' \subset \mathfrak{p}'$, so **(14.3)**(2) implies $\mathfrak{q}' = \mathfrak{p}'$.

By way of contradiction, suppose $1/y$ is integral over $R_{\mathfrak{p}}$. Say that, in $R'_{\mathfrak{p}'}$,

$$(1/y)^n + a_1(1/y)^{n-1} + \cdots + a_n = 0$$

with $n \geq 1$ and $a_i \in R_{\mathfrak{p}}$. Set $y' := -a_1 - \cdots - a_n y^{n-1} \in R'_{\mathfrak{p}}$. Then $yy' - 1 \in R'_{\mathfrak{p}}$ maps to 0 in $R'_{\mathfrak{p}'}$. But $R'_{\mathfrak{p}} \subset R'_{\mathfrak{p}'}$. So $yy' = 1$ in $R'_{\mathfrak{p}}$. But $y \in \mathfrak{q}'$; so $1 \in \mathfrak{q}' R'_{\mathfrak{p}}$. So $\mathfrak{q}' \cap (R - \mathfrak{p}) \neq \emptyset$ by **(11.11)**(3)(b). But $\mathfrak{q}' \cap R = \mathfrak{p}$, a contradiction, as desired. □

Exercise (14.17) . — Let k be a field, and X an indeterminate. Set $R' := k[X]$, and $Y := X^2$, and $R := k[Y]$. Set $\mathfrak{p} := (Y-1)R$ and $\mathfrak{p}' := (X-1)R'$. Is $R'_{\mathfrak{p}'}$ integral over $R_{\mathfrak{p}}$? Treat the case $\mathrm{char}(k) = 2$ separately. Explain.

Solution: Note that R' is a domain, and that the extension R'/R is integral by **(10.18)** as R' is generated by 1 and X as an R-module.

Suppose the characteristic is not 2. Set $\mathfrak{q}' := (X+1)R'$. Then both $\mathfrak{p}'$ and $\mathfrak{q}'$ contain $Y - 1$, so lie over the maximal ideal $\mathfrak{p}$ of R. Further $X + 1$ lies in $\mathfrak{q}'$, but not in $\mathfrak{p}'$. Thus $R'_{\mathfrak{p}'}$ is not integral over $R_{\mathfrak{p}}$ by **(14.16)**.

Suppose the characteristic is 2. Then $(X-1)^2 = Y - 1$. Let $\mathfrak{q}' \subset R'$ be a prime over $\mathfrak{p}$. Then $(X-1)^2 \in \mathfrak{q}'$. So $\mathfrak{p}' \subset \mathfrak{q}'$. But $\mathfrak{p}'$ is maximal. So $\mathfrak{q}' = \mathfrak{p}'$. Thus R' has just one prime $\mathfrak{p}'$ over $\mathfrak{p}$. Thus $R'_{\mathfrak{p}'}$ is integral over $R_{\mathfrak{p}}$ by **(14.15)**(3). □

Exercise (14.18) . — Let R be a ring, G be a finite group acting on R, and $\mathfrak{p}$ a prime of R^G. Let $\mathcal{P}$ denote the set of primes $\mathfrak{P}$ of R whose contraction in R^G is $\mathfrak{p}$. Prove: (1) G acts transitively on $\mathcal{P}$; and (2) $\mathcal{P}$ is nonempty and finite.

Solution: For (1), given $\mathfrak{P} \in \mathcal{P}$, and $g \in G$, note that $g(\mathfrak{P})$ is prime as g is an automorphism. Moreover, $g(\mathfrak{P}) \cap R^G = \mathfrak{P} \cap R^G$ as g leaves R^G fixed. So $g(\mathfrak{P}) \in \mathcal{P}$. Thus G acts on $\mathcal{P}$.

Given $\mathfrak{P}$ and $\mathfrak{P}'$ in $\mathcal{P}$, let's find $g \in G$ with $g(\mathfrak{P}) = \mathfrak{P}'$. Given $x \in \mathfrak{P}'$, set $y := \prod_{g \in G} g(x)$. Then $y \in R^G \cap \mathfrak{P}'$. Hence $y \in \mathfrak{p} \subset \mathfrak{P}$. So there is $g \in G$ with $g(x) \in \mathfrak{P}$. So $x \in g^{-1}(\mathfrak{P})$. Thus $\mathfrak{P}' \subset \bigcup_{g \in G} g(\mathfrak{P})$.

So $\mathfrak{P}' \subset g(\mathfrak{P})$ for some $g \in G$ by **(3.12)**. But R is integral over R^G by **(10.35)**. Hence **(14.3)**(2) yields $\mathfrak{P}' = g(\mathfrak{P})$. Thus (1) holds.

For (2), note R is integral over R^G by **(10.35)**. Thus $\mathcal{P}$ is nonempty by **(14.3)**(3). Finally, G acts transitively on $\mathcal{P}$ by (1). But G is finite. Thus (2) holds. □

Exercise (14.19) . — Let R be a normal domain, K its fraction field, L/K a finite field extension, $\overline{R}$ the integral closure of R in L. Prove that only finitely many primes $\mathfrak{P}$ of $\overline{R}$ lie over a given prime $\mathfrak{p}$ of R as follows.

First, assume L/K is separable, and use **(14.18)**. Next, assume L/K is purely inseparable, and show that $\mathfrak{P}$ is unique; in fact, $\mathfrak{P} = \{x \in \overline{R} \mid x^{p^n} \in \mathfrak{p} \text{ for some } n\}$ where p denotes the characteristic of K. Finally, do the general case.

Solution: First, assume L/K is separable. Then there exists a finite Galois extension L'/K, say with group G, such that $L \subset L'$ by [14, p. 242]. Form the integral closure R' of R in L'. Then $R'^G = R$ by **(10.37)**. So only finitely many primes $\mathfrak{P}'$ of R' lie over $\mathfrak{p}$ by **(14.18)**(2). But R' is integral over $\overline{R}$. So some such $\mathfrak{P}'$ lies over each $\mathfrak{P}$ by **(14.3)**(3). Thus there are only finitely many $\mathfrak{P}$.

Next, assume L/K is purely inseparable. Given any $x \in \mathfrak{P}$, note $x^q \in K$ where $q := p^n$ for some $n > 0$, as L/K is purely inseparable. But $x^q \in \overline{R}$ as $\mathfrak{P} \subset \overline{R}$. So x^q is integral over R. But R is normal. So $x^q \in R$. Thus $x^q \in \mathfrak{P} \cap R = \mathfrak{p}$.

Conversely, given $x \in \overline{R}$ with $x^r \in \mathfrak{p}$ for any $r > 0$, then $x^r \in \mathfrak{P}$. But $\mathfrak{P}$ is prime. So $x \in \mathfrak{P}$. Thus $\mathfrak{P} = \{x \in \overline{R} \mid x^{p^n} \in \mathfrak{p} \text{ for some } n\}$, as desired.

Finally, in the general case, there's an intermediate field K' with K'/K separable and L/K' purely inseparable by [**14**, Prp. 6.6, p. 250]. Form the integral closure R' of R in K'. By the first case, only finitely many primes $\mathfrak{P}'$ of R' lie over $\mathfrak{p}$.

Moreover, R' is normal by **(10.20)**. Let's see $\overline{R}$ is its integral closure in L. First, $\overline{R}$ is integral over R, so over R'. Second, given $x \in L$ integral over R', it is also integral over R by **(10.17)**(1); so $x \in \overline{R}$, as desired. So by the second case, only one prime $\mathfrak{P}$ of $\overline{R}$ lies over each $\mathfrak{P}'$. Thus only finitely many $\mathfrak{P}$ of $\overline{R}$ lie over $\mathfrak{p}$. □

Exercise (14.20) . — Let R be a ring. For $i = 1, 2$, let R_i be an algebra, $P_i \subset R_i$ a subalgebra. Assume P_1, P_2, R_1, R_2 are R-flat domains. Denote their fraction fields by L_1, L_2, K_1, K_2. Form the following diagram, induced by the inclusions:

$$\begin{array}{ccc} L_1 \otimes_R L_2 & \to & K_1 \otimes_R K_2 \\ \uparrow & & \uparrow{\scriptstyle\beta} \\ P_1 \otimes_R P_2 & \xrightarrow{\alpha} & R_1 \otimes_R R_2 \end{array}$$

(1) Show $K_1 \otimes K_2$ is flat over $P_1 \otimes P_2$. (2) Show β is injective.
(3) Given a minimal prime $\mathfrak{p}$ of $R_1 \otimes R_2$, show $\alpha^{-1}\mathfrak{p} = 0$ if $P_1 \otimes P_2$ is a domain.

Solution: For (1), note that L_i is a localization of P_i, so P_i-flat by **(12.14)**. Further, L_i is a field, so K_i is L_i-flat. Hence K_i is P_i-flat by **(9.23)**. Thus $K_1 \otimes K_2$ is $(P_1 \otimes P_2)$-flat by **(9.24)**, as desired.

For (2), note K_i is a localization of R_i, so R_i-flat by **(12.14)**. But R_i is R-flat. Hence K_i is R-flat by **(9.23)**. But β factors: $\beta\colon R_1 \otimes R_2 \to R_1 \otimes K_2 \to K_1 \otimes K_2$. The factors are injective as R_1 and K_2 are R-flat. Thus β is injective, as desired.

For (3), given $x \in \alpha^{-1}\mathfrak{p}$, note **(14.7)** yields a nonzero $y \in R_1 \otimes R_2$ with $\alpha(x)y = 0$. Set $\gamma := \beta\alpha$. Then $\gamma(x)\beta(y) = 0$. But $\beta(y) \neq 0$ by (2). So $\mu_{\gamma(x)}$ is not injective. So μ_x isn't either by (1). But $P_1 \otimes P_2$ is a domain. Thus $x = 0$, as desired. □

Exercise (14.21) . — Let R be a reduced ring, Σ the set of minimal primes. Prove that $\operatorname{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$ and that $R_{\mathfrak{p}} = \operatorname{Frac}(R/\mathfrak{p})$ for any $\mathfrak{p} \in \Sigma$.

Solution: If $\mathfrak{p} \in \Sigma$, then $\mathfrak{p} \subset \operatorname{z.div}(R)$ by **(14.7)**. Thus $\operatorname{z.div}(R) \supset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Conversely, say $xy = 0$. If $x \notin \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $y \in \mathfrak{p}$. So if $x \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, then $y \in \bigcap_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. But $\bigcap_{\mathfrak{p}\in\Sigma} \mathfrak{p} = \langle 0 \rangle$ by the Scheinnullstellensatz **(3.14)** and **(3.16)**. So $y = 0$. Thus, if $x \notin \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$, then $x \notin \operatorname{z.div}(R)$. Thus $\operatorname{z.div}(R) \subset \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Thus $\operatorname{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$.

Fix $\mathfrak{p} \in \Sigma$. Then $R_{\mathfrak{p}}$ is reduced by **(13.57)**. Further, $R_{\mathfrak{p}}$ has only one prime, namely $\mathfrak{p}R_{\mathfrak{p}}$, by **(11.12)**(2). Hence $R_{\mathfrak{p}}$ is a field, and $\mathfrak{p}R_{\mathfrak{p}} = \langle 0 \rangle$. But by **(12.16)**, $R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} = \operatorname{Frac}(R/\mathfrak{p})$. Thus $R_{\mathfrak{p}} = \operatorname{Frac}(R/\mathfrak{p})$. □

Exercise (14.22) . — Let R be a ring, Σ the set of minimal primes, and K the total quotient ring. Assume Σ is finite. Prove these three conditions are equivalent:

(1) R is reduced.

(2) $\mathrm{z.div}(R) = \bigcup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$, and $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p}\in\Sigma$.
(3) $K/\mathfrak{p}K = \mathrm{Frac}(R/\mathfrak{p})$ for each $\mathfrak{p}\in\Sigma$, and $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$.

Solution: Assume (1) holds. Then **(14.21)** yields (2).

Assume (2) holds. Set $S := R - \mathrm{z.div}(R)$. Let $\mathfrak{q}$ be a prime of R with $\mathfrak{q}\cap S = \emptyset$. Then $\mathfrak{q}\subset \mathrm{z.div}(R)$. So (2) yields $\mathfrak{q}\subset\bigcup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$. But Σ is finite. So $\mathfrak{q}\subset\mathfrak{p}$ for some $\mathfrak{p}\in\Sigma$ by Prime Avoidance **(3.12)**. Hence $\mathfrak{q}=\mathfrak{p}$ since $\mathfrak{p}$ is minimal. But $K = S^{-1}R$. Therefore, by **(11.12)**(2), for $\mathfrak{p}\in\Sigma$, the extensions $\mathfrak{p}K$ are the only primes of K, and they all are both maximal and minimal.

Fix $\mathfrak{p}\in\Sigma$. Then $K/\mathfrak{p}K = S^{-1}(R/\mathfrak{p})$ by **(12.15)**. So $S^{-1}(R/\mathfrak{p})$ is a field. But clearly $S^{-1}(R/\mathfrak{p})\subset\mathrm{Frac}(R/\mathfrak{p})$. Therefore, $K/\mathfrak{p}K = \mathrm{Frac}(R/\mathfrak{p})$ by **(2.3)**. Further, $S\subset R-\mathfrak{p}$. Hence **(11.12)**(2) yields $\mathfrak{p} = \varphi_S^{-1}(\mathfrak{p}K)$. Therefore, $\varphi_S^{-1}(K-\mathfrak{p}K) = R-\mathfrak{p}$. So $K_{\mathfrak{p}K} = R_{\mathfrak{p}}$ by **(11.16)**. But $R_{\mathfrak{p}} = \mathrm{Frac}(R/\mathfrak{p})$ by hypothesis. Thus K has only finitely many primes, the $\mathfrak{p}K$; each $\mathfrak{p}K$ is minimal, and each $K_{\mathfrak{p}K}$ is a domain. Therefore, **(13.58)**(2) yields $K = \prod_{\mathfrak{p}\in\Sigma} K/\mathfrak{p}K$. Thus (3) holds.

Assume (3) holds. Then K is a finite product of fields, and fields are reduced. But clearly, a product of reduced ring is reduced. Further, $R\subset K$, and trivially, a subring of a reduced ring is reduced. Thus (1) holds. □

Exercise (14.23) . — Let A be a reduced local ring with residue field k and a finite set Σ of minimal primes. For each $\mathfrak{p}\in\Sigma$, set $K(\mathfrak{p}) := \mathrm{Frac}(A/\mathfrak{p})$. Let P be a finitely generated module. Show that P is free of rank r if and only if $\dim_k(P\otimes_A k) = r$ and $\dim_{K(\mathfrak{p})}(P\otimes_A K(\mathfrak{p})) = r$ for each $\mathfrak{p}\in\Sigma$.

Solution: If P is free of rank r, then $\dim(P\otimes k) = r$ and $\dim(P\otimes K(\mathfrak{p})) = r$ owing to **(8.10)**.

Conversely, suppose $\dim(P\otimes k) = r$. As P is finitely generated, **(10.9)** implies P is generated by r elements. So **(5.13)** yields an exact sequence

$$0\to M\xrightarrow{\alpha} A^r\to P\to 0.$$

Momentarily, fix a $\mathfrak{p}\in\Sigma$. Since A is reduced, $K(\mathfrak{p}) = A_{\mathfrak{p}}$ by **(14.21)**. So $K(\mathfrak{p})$ is flat by **(12.14)**. So the induced sequence is exact:

$$0\to M\otimes K(\mathfrak{p})\to K(\mathfrak{p})^r\to P\otimes K(\mathfrak{p})\to 0.$$

Suppose $\dim(P\otimes K(\mathfrak{p})) = r$ too. It then follows that $M\otimes_A K(\mathfrak{p}) = 0$.

Let K be the total quotient ring of A, and form this commutative square:

$$\begin{tikzcd} M \arrow[r, "\alpha"] \arrow[d, "\varphi_M"] & A^r \arrow[d, "\varphi_{A^r}"] \\ M\otimes K \arrow[r] & K^r \end{tikzcd}$$

Here α is injective. And φ_{A^r} is injective as $\varphi_A\colon A\to K$ is. Hence, φ_M is injective.

By hypothesis, A is reduced and Σ is finite; so $K = \prod_{\mathfrak{p}\in\Sigma} K(\mathfrak{p})$ by **(14.22)**. So $M\otimes K = \prod(M\otimes K(\mathfrak{p}))$. But $M\otimes_A K(\mathfrak{p}) = 0$ for each $\mathfrak{p}\in\Sigma$. So $M\otimes K = 0$. But $\varphi_M\colon M\to M\otimes K$ is injective. So $M = 0$. Thus $A^r \xrightarrow{\sim} P$, as desired. □

Exercise (14.24) . — Let A be a reduced semilocal ring with a finite set of minimal primes. Let P be a finitely generated A-module, and B an A-algebra such that $\mathrm{Spec}(B)\to\mathrm{Spec}(A)$ is surjective. For each prime $\mathfrak{q}\subset B$, set $L(\mathfrak{q}) := \mathrm{Frac}(B/\mathfrak{q})$. Given r, assume $\dim((P\otimes_A B)\otimes_B L(\mathfrak{q})) = r$ whenever $\mathfrak{q}$ is either maximal or minimal. Show that P is a free A-module of rank r.

Solution: Let $\mathfrak{p} \subset A$ be a prime; set $K := \mathrm{Frac}(A/\mathfrak{p})$. As $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective, there's a prime $\mathfrak{q} \subset B$ whose contraction is $\mathfrak{p}$. Then **(8.9)**(1) yields

$$(P \otimes_A K) \otimes_K L(\mathfrak{q}) = (P \otimes_A B) \otimes_B L(\mathfrak{q}). \tag{14.24.1}$$

If $\mathfrak{p}$ is minimal, take a minimal prime $\mathfrak{q}' \subset \mathfrak{q}$. Then the contraction of $\mathfrak{q}'$ is contained in $\mathfrak{p}$, so equal to $\mathfrak{p}$. Replace $\mathfrak{q}$ by $\mathfrak{q}'$. If $\mathfrak{p}$ is maximal, take a maximal ideal $\mathfrak{q}' \supset \mathfrak{q}$. Then the contraction of $\mathfrak{q}'$ contains $\mathfrak{p}$, so is equal to $\mathfrak{p}$. Again, replace $\mathfrak{q}$ by $\mathfrak{q}'$. Either way, $\dim((P \otimes_A B) \otimes_B L(\mathfrak{q})) = r$ by hypothesis. So **(14.24.1)** yields $\dim\big((P \otimes_A K) \otimes_K L(\mathfrak{q})\big) = r$. Hence $\dim(P \otimes_A K) = r$.

If A is local, then P is free of rank r by **(14.23)**. In general, by **(13.63)** it suffices to show that $P_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module of rank r for every maximal ideal $\mathfrak{m}$ of A. So by the preceding case, it suffices to show that $\mathrm{Spec}(B_\mathfrak{m}) \to \mathrm{Spec}(A_\mathfrak{m})$ is surjective.

For reference, form the following commutative diagram:

$$\begin{array}{ccc} B & \longrightarrow & B_\mathfrak{m} \\ \uparrow & & \uparrow \\ A & \longrightarrow & A_\mathfrak{m} \end{array}$$

Given a prime $\mathfrak{P} \subset A_\mathfrak{m}$, let $\mathfrak{p}$ be its contraction. Since $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective, there's a prime $\mathfrak{q} \subset B$ that contracts to $\mathfrak{p}$. Set $\mathfrak{Q} := \mathfrak{q}B_\mathfrak{m}$. Then $\mathfrak{Q}$ contracts to $\mathfrak{q}$ by **(11.12)**(2). Hence $\mathfrak{Q}$ contracts to $\mathfrak{p}$. But $\mathfrak{P}$ does too. Hence $\mathfrak{Q}$ contracts to $\mathfrak{P}$ by **(11.12)**(2). Thus $\mathrm{Spec}(B_\mathfrak{m}) \to \mathrm{Spec}(A_\mathfrak{m})$ is surjective. □

Exercise (14.25) . — Let R be a ring, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ all its minimal primes, and K the total quotient ring. Prove that these three conditions are equivalent:

(1) R is normal.
(2) R is reduced and integrally closed in K.
(3) R is a finite product of normal domains R_i.

Assume the conditions hold. Prove the R_i are equal to the $R/\mathfrak{p}_j$ in some order.

Solution: Assume (1). Let $\mathfrak{m}$ any maximal ideal. Then $R_\mathfrak{m}$ is a normal domain. So R is reduced by **(13.57)**.

Recall S_0 is the set of nonzerodivisors of R, so $K := S_0^{-1}R$. Recall $S_\mathfrak{m} := R - \mathfrak{m}$, so $R_\mathfrak{m} := S_\mathfrak{m}^{-1}R$. But $S_\mathfrak{m}^{-1}S_0^{-1}R = S_0^{-1}S_\mathfrak{m}^{-1}R$ by **(12.26)**(1). So $S_\mathfrak{m}^{-1}K = S_0^{-1}R_\mathfrak{m}$.

Let $t \in S_0$. Then $t/1 \neq 0$ in $R_\mathfrak{m}$; else, there's $s \in S_\mathfrak{m}$ with $st = 0$, a contradiction as $s \neq 0$ and $t \in S_0$. Thus **(11.15)** and **(11.2)** yield $S_0^{-1}R_\mathfrak{m} \subset \mathrm{Frac}(R_\mathfrak{m})$.

Let $x \in K$ be integral over R. Then $x/1 \in S_\mathfrak{m}^{-1}K$ is integral over $S_\mathfrak{m}^{-1}R$ by **(11.29)**. But $S_\mathfrak{m}^{-1}R = R_\mathfrak{m}$, and $R_\mathfrak{m}$ is a normal domain. So $x/1 \in R_\mathfrak{m}$. Hence $x \in R$ by **(13.55)**. Thus (2) holds.

Assume (2). Set $R_i := R/\mathfrak{p}_i$ and $K_i := \mathrm{Frac}(R_i)$. Then $K = \prod K_i$ by **(14.22)**. Let R_i' be the normalization of R_i. Then $R \hookrightarrow \prod R_i \hookrightarrow \prod R_i'$. Further, the first extension is integral by **(10.41)**, and the second, by **(10.42)**; whence, $R \hookrightarrow \prod R_i'$ is integral by the tower property **(10.17)**. However, R is integrally closed in K by hypothesis. Hence $R = \prod R_i = \prod R_i'$. Thus (3) holds.

Assume (3). Let $\mathfrak{p}$ be any prime of R. Then $R_\mathfrak{p} = \prod (R_i)_\mathfrak{p}$ by **(12.9)**, and each $(R_i)_\mathfrak{p}$ is normal by **(11.32)**. But $R_\mathfrak{p}$ is local. So $R_\mathfrak{p} = (R_i)_\mathfrak{p}$ for some i by **(3.6)**. Hence $R_\mathfrak{p}$ is a normal domain. Thus (1) holds.

Finally, the last assertion results from **(13.58)**(2). □

Exercise (14.26) . — Let X be a nonempty compact Hausdorff space, R the ring of $\mathbb{R}$-valued continuous functions on X, and $\widetilde{X} \subset \operatorname{Spec}(R)$ the set of maximal ideals. Give $\widetilde{X}$ the induced topology. For all $x \in X$, set $\mathfrak{m}_x := \{f \in R \mid f(x) = 0\}$. Show:

(1) Given a maximal ideal $\mathfrak{m}$, set $V := \{x \in X \mid f(x) = 0 \text{ for all } f \in \mathfrak{m}\}$. Then $V \neq \emptyset$; otherwise, there's a contradiction. Moreover, $\mathfrak{m} = \mathfrak{m}_x$ for any $x \in V$.

(2) Urysohn's Lemma [15, Thm. 3.1, p. 207] implies $\mathfrak{m}_x \neq \mathfrak{m}_y$ if $x \neq y$.

(3) For any $f \in R$, set $U_f = \{x \in X \mid f(x) \neq 0\}$ and $\overline{U}_f = \{\mathfrak{m} \in \widetilde{X} \mid f \notin \mathfrak{m}\}$. Then $\mathfrak{m}_x \in \widetilde{X}$ for any $x \in X$, and $x \in U_f$ if and only if $\mathfrak{m}_x \in \overline{U}_f$; moreover, the $\overline{U}_f$ and, by Urysohn's Lemma, the U_f form bases of the topologies.

(4) Define $\varphi\colon X \to \widetilde{X}$ by $\varphi(x) := \mathfrak{m}_x$. Then φ is a well-defined homeomorphism.

Solution: For (1), suppose $V = \emptyset$. Then for each $x \in X$, there's $f_x \in \mathfrak{m}$ with $f_x(x) \neq 0$. As f_x is continuous, there's a neighborhood U_x of x on which f_x has no zero. By compactness, finitely many U_x cover X, say U_{x_i} for $1 \leq i \leq n$. Set $f := \sum f_{x_i}^2$. Then $f(y) \neq 0$ for all $y \in X$. So $f \in R^\times$. But $f \in \mathfrak{m}$, a contradiction.

Moreover, given $x \in V$, note $\mathfrak{m} \subset \mathfrak{m}_x$. But $\mathfrak{m}$ is maximal, and $1 \notin \mathfrak{m}_x$. Thus $\mathfrak{m} = \mathfrak{m}_x$. Thus (1) holds.

For (2), note $\{x\}$ and $\{y\}$ are closed as X is Hausdorff. As X is compact too, it's normal by[15, Thm. 2.4, p. 198]. So Urysohn's Lemma gives $f \in R$ with $f(x) = 0$ and $f(y) = 1$. So $f \in \mathfrak{m}_x - \mathfrak{m}_y$. Thus (2) holds.

For (3), note $\mathfrak{m}_x = \operatorname{Ker}(\theta_x)$ where $\theta_x\colon R \twoheadrightarrow \mathbb{R}$ by $\theta_x(f) := f(x)$. Thus $\mathfrak{m}_x \in \widetilde{X}$.

Note $x \in U_f$ if and only if $f(x) \neq 0$, if and only if $f \notin \mathfrak{m}_x$, if and only if $x \in \overline{U}_f$.

Moreover, the $\mathbf{D}(f)$ form a basis of the topology of $\operatorname{Spec}(R)$ by **(13.1)**. But $\overline{U}_f = \mathbf{D}(f) \cap \widetilde{X}$. Thus the $\overline{U}_f$ form a basis of the topoology of $\widetilde{X}$.

Given $x \in W \subset X$ with W open, Urysohn's Lemma provides $f \in R$ with $f(x) = 1$ and $f(X - W) = 0$. So $x \in U_f \subset W$. Thus the U_f form a basis. Thus (3) holds.

For (4), note φ is a well defined as $\mathfrak{m}_x \in \widetilde{X}$ for any $x \in X$ by (3). Moreover, φ is injective by (2), and surjective by (1). Finally, φ is a homeomorphism as it preserves bases of the topologies by (3). Thus (4) holds. □

15. Noether Normalization

Exercise (15.15) . — Let $k := \mathbb{F}_q$ be the finite field with q elements, and $k[X, Y]$ the polynomial ring. Set $F := X^qY - XY^q$ and $R := k[X, Y]/\langle F \rangle$. Let $x, y \in R$ be the residues of X, Y. For every $a \in k$, show that R is not module finite over $P := k[y - ax]$. (Thus, in **(15.1)**, no k-linear combination works.) First, take $a = 0$.

Solution: Take $a = 0$. Then $P = k[y]$. Any algebraic relation over P satisfied by x is given by a polynomial in $k[X, Y]$, which is a multiple of F. However, no multiple of F is monic in X. So x is not integral over P. By **(10.14)**, R is not module finite over P.

Consider an arbitrary a. Since $a^q = a$, after the change of variable $Y' := Y - aX$, our F still has the same form. Thus, we have reduced to the previous case. □

Exercise (15.16) . — Let k be a field, and X, Y, Z variables. Set

$$R := k[X, Y, Z]/\langle X^2 - Y^3 - 1,\ XZ - 1\rangle,$$

and let $x, y, z \in R$ be the residues of X, Y, Z. Fix $a, b \in k$, and set $t := x + ay + bz$ and $P := k[t]$. Show that x and y are integral over P for any a, b and that z is integral over P if and only if $b \neq 0$.

Solution: To see x is integral, notice $xz = 1$, so $x^2 - tx + b = -axy$. Raising both sides of the latter equation to the third power, and using the equation $y^3 = x^2 - 1$, we obtain an equation of integral dependence of degree 6 for x over P. So $P[x]$ is integral over k by **(10.18)**. Now, $y^3 - x^2 + 1 = 0$; so y is integral over $P[x]$. Hence, the Tower Property, **(10.17)**(1), implies that y too is integral over P.

If $b \neq 0$, then $z = b^{-1}(t - x - ay) \in P[x, y]$, and so z is integral over P by **(10.18)**.

Assume $b = 0$ and z is integral over P. Now, $P \subset k[x, y]$. So z is integral over $k[x, y]$ as well. But $y^3 - x^2 + 1 = 0$. So y is integral over $k[x]$. Hence z is too. However, $k[x]$ is a polynomial ring, so integrally closed in its fraction field $k(x)$ by **(10.22)**(1). Moreover, $z = 1/x \in k(x)$. Hence, $1/x \in k[x]$, which is absurd. Thus z is not integral over P if $b = 0$. □

Exercise (15.17) . — Let R'/R be an extension of rings, $\overline{R}$ the integral closure of R, and X a variable. Prove $\overline{R}[X]$ is the integral closure of $R[X]$ in $R'[X]$.

Solution: Note $\overline{R}[X] = \overline{R} \otimes_R R[X]$ by **(8.18)**. So $\overline{R}[X]$ is integral over $R[X]$ by **(10.39)**. So let's show $\overline{R}[X]$ contains every $f \in R'[X]$ that's integral over $R[X]$.

Say $f^n + g_1 f^{n-1} + \cdots + g_n = 0$ with $g_i \in R[X]$. Set $f_1 := f - X^r$ with $r \gg 0$. Then $(f_1 + X^r)^n + \cdots + g_n = 0$. So $f_1^n + h_1 f_1^{n-1} + \cdots + h_n = 0$ with $h_i \in R[X]$.

Then $h_n = (X^r)^n + (X^r)^{n-1} g_1 + \cdots + g_n$. So h_n is monic as $ri > \deg(g_i)$ for all i. Set $f_2 := f_1^{n-1} + h_1 f_1^{n-2} + \cdots + h_{n-1}$. Then $h_n = -f_1 f_2$. But f_1 is monic as $r > \deg(f)$. Hence the coefficients of f_1 are integral over R by **(14.4)**(2). But the coefficients of f_1 include those of f. Thus $f \in \overline{R}[X]$, as desired. □

Exercise (15.18) . — Let R be a domain, $\varphi\colon R \hookrightarrow R'$ an algebra-finite extension. Set $\varphi^* := \operatorname{Spec}(\varphi)$. Find a nonzero $f \in R$ such that $\varphi^* \operatorname{Spec}(R') \supset \mathbf{D}(f)$.

Solution: By **(15.3)**, there are a nonzero $f \in R$ and algebraically independent $x_1, \ldots, x_n \in R'$ such that R'_f is an integral extension of $R[x_1, \ldots, x_n]_f$. Given $\mathfrak{p} \in \mathbf{D}(f)$, its extension $\mathfrak{p}R[x_1, \ldots, x_n]$ is a prime lying over $\mathfrak{p}$ by **(2.32)**. So $\mathfrak{p}R[x_1, \ldots, x_n]_f$ is a prime lying over $\mathfrak{p}R[x_1, \ldots, x_n]$ by **(11.12)**(2). So there's a prime $\mathfrak{P}'$ of R'_f lying over $\mathfrak{p}R[x_1, \ldots, x_n]_f$ by **(14.3)**(3). Note that $\mathfrak{P}'$ lies over $\mathfrak{p}$. Let $\mathfrak{P}$ be the contraction of $\mathfrak{P}'$ in R'. Then $\mathfrak{P}$ lies over $\mathfrak{p}$. Thus $\mathfrak{p} \in \varphi^* \operatorname{Spec}(R')$. □

Exercise (15.19) . — Let R be a domain, R' an algebra-finite extension. Find a nonzero $f \in R$ such that, given an algebraically closed field Ω and a ring map $\varphi\colon R \to \Omega$ with $\varphi(f) \neq 0$, there's an extension of φ to R'.

Solution: By **(15.3)**, there are a nonzero $f \in R$ and algebraically independent $x_1, \ldots, x_n$ in R' such that R'_f is integral over $R[x_1, \ldots, x_n]_f$. Given a map $\varphi\colon R \to \Omega$ with Ω algebraically closed and $\varphi(f) \neq 0$, we can extend φ to $R[x_1, \ldots, x_n]$ by **(1.3)**. Then we can extend φ further to $R[x_1, \ldots, x_n]_f$ by **(11.3)**. Finally, we can extend φ to $\varphi'\colon R'_f \to \Omega$ by **(14.12)**. Thus $\varphi'|R'$ is the desired extension of φ to R'. □

Exercise (15.20) . — Let R be a domain, R' an algebra-finite extension. Assume $\operatorname{rad}(R) = \langle 0 \rangle$. Prove $\operatorname{rad}(R') = \operatorname{nil}(R')$. First do the case where R' is a domain by applying **(15.19)** with $R' := R'_g$ for any given nonzero $g \in R'$.

Solution: First assume R' is a domain. Then $\mathrm{nil}(R') = \langle 0\rangle$. So we have to prove $\mathrm{rad}(R') = \langle 0\rangle$. So given a nonzero $g \in R'$, we must find a maximal ideal $\mathfrak{m}'$ of R' with $g \notin \mathfrak{m}'$. Note that, as R'/R is algebra finite, so is R'_g/R.

Applying (**15.19**) with $R' := R'_g$ yields an $f \in R$. As $\mathrm{rad}(R) = \langle 0\rangle$, there's a maximal ideal $\mathfrak{m}$ of R with $f \notin \mathfrak{m}$. Set $k := R/\mathfrak{m}$. Let $\varphi\colon R \to k$ be the quotient map. Then $\varphi(f) \neq 0$.

There is an algebraic closure Ω of k by (**14.13**). So (**15.19**) yields an extension $\varphi'\colon R'_g \to \Omega$ of φ. Let $\mathfrak{m}'$ be the contraction of $\mathrm{Ker}(\varphi')$ to R'. Note that g is a unit in R'_g; so $\varphi'(g) \neq 0$. Thus $g \notin \mathfrak{m}'$.

Say $R' = R[y_1, \ldots, y_n]$. The $\varphi'(y_i)$ are algebraic over k as Ω/k is algebraic. But k is a field. So the $\varphi'(y_i)$ are integral over k. So $\varphi'(R')$ is integral over k by (**10.18**). So $\varphi'(R')$ is a field by (**14.1**). But $R'/\mathfrak{m}' \xrightarrow{\sim} \varphi'(R')$. So $R'/\mathfrak{m}'$ is a field. So $\mathfrak{m}'$ is maximal. But $g \notin \mathfrak{m}'$, as desired. Thus we've done the case where R is a domain.

For the general case, note $\mathrm{nil}(R') = \bigcap \mathfrak{p}'$, where $\mathfrak{p}'$ runs over the minimal primes of R', by (**3.14**) and (**3.16**). So it suffices to prove that each $\mathfrak{p}'$ is the intersection, $\mathfrak{a}'_{\mathfrak{p}'}$ say, of the maximal ideals of R' containing $\mathfrak{p}'$.

Fix $\mathfrak{p}'$. Set $R'_1 := R'/\mathfrak{p}'$. Let R_1 be the image in R'_1 of R. Then $\mathfrak{a}'_{\mathfrak{p}'}/\mathfrak{p}' = \mathrm{rad}(R'_1)$. So it remains to show $\mathrm{rad}(R'_1) = \langle 0\rangle$.

Note R'_1 is a domain; so R_1 is too. Plainly, R'_1 is an algebra-finite extension of R_1. So $\mathrm{rad}(R'_1) = \langle 0\rangle$ by the preceding case. Thus the general case holds. □

Exercise (15.21) . — Let k be a field, K an algebraically closed extension field. Let $P := k[X_1, \ldots, X_n]$ be the polynomial ring, and $F, F_1, \ldots, F_r \in P$. Assume F vanishes at every zero in K^n of $F_1, \ldots, F_r$; that is, if $(\mathbf{a}) := (a_1, \ldots, a_n) \in K^n$ and $F_1(\mathbf{a}) = 0, \ldots, F_r(\mathbf{a}) = 0$, then $F(\mathbf{a}) = 0$ too. Prove that there are polynomials $G_1, \ldots, G_r \in P$ and an integer N such that $F^N = G_1F_1 + \cdots + G_rF_r$.

Solution: Set $\mathfrak{a} := \langle F_1, \ldots, F_r\rangle$. We have to show $F \in \sqrt{\mathfrak{a}}$. But, by the Hilbert Nullstellensatz (**15.7**), $\sqrt{\mathfrak{a}}$ is equal to the intersection of all the maximal ideals $\mathfrak{m}$ containing $\mathfrak{a}$. So given an $\mathfrak{m}$, we have to show that $F \in \mathfrak{m}$.

Set $L := P/\mathfrak{m}$. By the Zariski Nullstellensatz (**15.4**), L is a finite extension field of k. So we may embed L/k as a subextension of K/k. Let $a_i \in K$ be the image of the variable $X_i \in P$, and set $(\mathbf{a}) := (a_1, \ldots, a_n) \in K^n$. Then plainly $F_1(\mathbf{a}) = 0, \ldots, F_r(\mathbf{a}) = 0$. So $F(\mathbf{a}) = 0$ by hypothesis. Thus $F \in \mathfrak{m}$, as desired. □

Exercise (15.22) . — (1) Find an example where (**15.21**) fails if K isn't required to be algebraically closed, say with $K := k := \mathbb{R}$ and $n := 1$ and $r := 1$.

(2) Find an example where (**15.21**) fails if the G_i are all required to be in k, say with $K := k := \mathbb{C}$ and $n := 1$ and $r := 2$.

Solution: For (1), take $F := 1$ and $F_1 := X_1^2 + 1$. Then F has no zero, and F_1 has no zero, but no power of F is equal to any multiple of F_1.

For (2), take $F := 1$ and $F_1 := X_1$ and $F_2 := X_1^2 + 1$. Then F has no zero, and F_1 and F_2 have no common zero, but no power of F is equal to $G_1F_1 + G_2F_2$ for any $G_i \in k$. □

Exercise (15.23) . — Let k be an algebraically closed field, $P := k[X_1, \ldots, X_n]$ the polynomial ring in n variables X_i, and $V \subset k^n$ the set of common zeroes of a set of polynomials F_μ. Assume $V \neq \emptyset$. Show there exist a linear subspace $L \subset k^n$ and a linear map $\lambda\colon k^n \twoheadrightarrow L$ such that $\lambda(V) = L$.

Solution: Let $P(V)$ be the algebra of all $\gamma\colon V \to R$ given by evaluating some $G \in P$. Note $P(V)$ is a quotient of P by **(1.29)**(1), so generated by the residues ξ_i of the X_i. Note $P(V) \neq 0$ as $V \neq \emptyset$. Note k is infinite. So **(15.2)** yields algebraically independent k-linear combinations $\rho_j := \sum_{i=1}^n a_{ij}\xi_i$ for $1 \le j \le m$ where $m \le n$ such that $P(V)$ is module finite over $R := k[\rho_1, \dots, \rho_m]$.

Let L be the subspace of $(v_1, \dots, v_n) \in k^n$ with $v_i = 0$ for $i > m$. Define $\lambda\colon k^n \to L$ by $\lambda(v_1, \dots, v_n) := (w_1, \dots, w_n)$ where $w_j := \sum_{i=1}^n a_{ij}v_i$ for $j \le m$ and $w_j = 0$ for $j > m$. It remains to show $\lambda(V) = L$.

Given $(w_1, \dots, w_n) \in L$, define an algebra map $\varphi\colon R \to k$ by $\varphi(\rho_j) := w_j$. But k is algebraically closed. So φ extends to an algebra map $\pi\colon P(V) \to k$ by **(14.12)**. Then $\varphi(\rho_j) = \pi(\rho_j)$, and $\pi(\rho_j) = \sum_{i=1}^n a_{ij}\pi(\xi_i)$. Set $v_i := \pi(\xi_i)$. Then $w_j = \sum_{i=1}^n a_{ij}v_i$ for $j \le m$. Thus $\lambda(v_1, \dots, v_n) = (w_1, \dots, w_n)$.

Finally, let's adapt the reasoning used to prove **(1.29)**(3). First, for each μ, we get $F_\mu(\xi_1, \dots, \xi_n) = 0$ in $P(V)$. So $\pi(F_\mu(\xi_1, \dots, \xi_n)) = 0$ in k. Second, we get $\pi(F_\mu(\xi_1, \dots, \xi_n)) = F_\mu(\pi(\xi_1), \dots, \pi(\xi_n))$. But $v_i := \pi(\xi_i)$. So $F_\mu(v_1, \dots, v_n) = 0$. Thus $(v_1, \dots, v_n) \in V$. Thus $\lambda(V) = L$. □

Exercise (15.24) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} \subset \operatorname{nil}(R)$. Show

$$\dim(R/\mathfrak{a}) = \dim(R). \tag{15.24.1}$$

Solution: Plainly, every prime $\mathfrak{p}$ of R contains $\mathfrak{a}$. So $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ sets up a bijection from the chains of primes of R onto those of $R/\mathfrak{a}$. Thus $\dim(R/\mathfrak{a}) = \dim(R)$. □

Exercise (15.25) . — Let R be a domain of (finite) dimension r, and $\mathfrak{p}$ a nonzero prime. Show $\dim(R/\mathfrak{p}) < r$.

Solution: Every chain of primes of $R/\mathfrak{p}$ is of the form $\mathfrak{p}_0/\mathfrak{p} \subsetneqq \cdots \subsetneqq \mathfrak{p}_s/\mathfrak{p}$ where $0 \subsetneqq \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_s$ is a chain of primes of R. So $s < r$. Thus $\dim(R/\mathfrak{p}) < r$. □

Exercise (15.26) . — Given an integral extension of rings R'/R, show

$$\dim(R) = \dim(R'). \tag{15.26.1}$$

Solution: Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes of R. Set $\mathfrak{p}'_{-1} := 0$. Given $\mathfrak{p}'_{i-1}$ for $0 \le i \le r$, Going-up, **(14.3)**(4), yields a prime $\mathfrak{p}'_i$ of R' with $\mathfrak{p}'_{i-1} \subset \mathfrak{p}'_i$ and ${\mathfrak{p}'}_i \cap R = \mathfrak{p}_i$. Then $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ as $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$. Thus $\dim(R) \le \dim(R')$.

Conversely, let ${\mathfrak{p}'}_0 \subsetneqq \cdots \subsetneqq {\mathfrak{p}'}_r$ be a chain of primes of R'. Set $\mathfrak{p}_i := {\mathfrak{p}'}_i \cap R$. Then $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ by Incomparability, **(14.3)**(2). Thus $\dim(R) \ge \dim(R')$. □

Exercise (15.27) . — Let R'/R be an integral extension of domains with R normal, $\mathfrak{m}$ a maximal ideal of R'. Show $\mathfrak{n} := \mathfrak{m} \cap R$ is maximal and $\dim(R'_\mathfrak{m}) = \dim(R_\mathfrak{n})$.

Solution: First, $\mathfrak{n}$ is maximal by **(14.3)**(1).

Next, let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes of R with $\mathfrak{p}_r = \mathfrak{n}$. Set $\mathfrak{p}'_r := \mathfrak{m}$, and proceed by descending induction. Given $\mathfrak{p}'_i$ with $\mathfrak{p}'_i \cap R = \mathfrak{p}_i$ where $1 \le i \le r$, there's a prime $\mathfrak{p}'_{i-1}$ of R' with $\mathfrak{p}'_{i-1} \cap R = \mathfrak{p}_{i-1}$ by **(14.6)** as R is normal. Then $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ is a chain of primes of R' with $\mathfrak{p}'_r = \mathfrak{m}$. Thus $\dim(R_\mathfrak{n}) \le \dim(R'_\mathfrak{m})$.

Lastly, let $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ be a chain of primes of R' with $\mathfrak{p}'_r \subset \mathfrak{m}$. Set $\mathfrak{p}_i := \mathfrak{p}'_i \cap R$. Then $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ by **(14.3)**(2), and $\mathfrak{p}_r \subset \mathfrak{n}$. Thus $\dim(R_\mathfrak{n}) \ge \dim(R'_\mathfrak{m})$. □

Exercise (15.28) . — (1) Given a product of rings $R := R' \times R''$, show

$$\dim(R) = \max\{\dim(R'), \dim(R'')\}. \tag{15.28.1}$$

(2) Find a ring R with a maximal chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$, yet $r < \dim(R)$.

Solution: For (1), by (**2.29**), recall that a prime in R either has the form $\mathfrak{p}' \times R''$ where $\mathfrak{p}'$ is a prime of R' or $R' \times \mathfrak{p}''$ where $\mathfrak{p}''$ is a prime of R''. So any chain of primes of R arises from either a chain of primes of R' or a chain of primes of R''. Thus (**15.28.1**) holds.

For (2), let k be a field and set $R := k[X] \times k$. Then $\dim(R) = 1$ by (1). Set $\mathfrak{p}_0 := k[X] \times \langle 0 \rangle$. Then $\mathfrak{p}_0$ forms a maximal chain by the proof of (1), as desired. □

Exercise (15.29) . — Let k be a field, R_1 and R_2 algebra-finite domains, and $\mathfrak{p}$ a minimal prime of $R_1 \otimes_k R_2$. Use Noether Normalization and (**14.20**) to prove this:

$$\dim\big((R_1 \otimes_k R_2)/\mathfrak{p}\big) = \dim(R_1) + \dim(R_2). \qquad (\mathbf{15.29.1})$$

Solution: Noether Normalization (**15.1**) yields a polynomial subalgebra P_i of R_i such that R_i is module finite over P_i. Then P_i and R_i are domains, and they are k-flat as k is a field. Moreover, $P_1 \otimes P_2$ is a domain by (**8.18**) and (**2.4**).

Say $\{x_i\}$ and $\{y_j\}$ are sets of module generators of R_1 over P_1 and of R_2 over P_2. Then, plainly, the $x_i \otimes y_j \in R_1 \otimes R_2$ form a set of module generators over $P_1 \otimes P_2$; so their residues in $(R_1 \otimes R_2)/\mathfrak{p}$ form one too. Thus (**10.18**) implies $(R_1 \otimes R_2)/\mathfrak{p}$ is integral over $P_1 \otimes P_2$.

Further, $P_1 \otimes P_2 \to (R_1 \otimes R_2)/\mathfrak{p}$ is injective by (**14.20**)(3). So (**15.26**) yields

$$\dim\big((R_1 \otimes R_2)/\mathfrak{p}\big) = \dim(P_1 \otimes P_2).$$

Similarly, $\dim(R_1) = \dim(P_1)$ and $\dim(R_2) = \dim(P_2)$. Finally, (**15.11**) yields

$$\dim(P_1 \otimes P_2) = \dim(P_1) + \dim(P_2).$$

Thus (**15.29.1**) holds, as desired. □

Exercise (15.30) . — Let k be a field, R a finitely generated k-algebra, $f \in R$ nonzero. Assume R is a domain. Prove that $\dim(R) = \dim(R_f)$.

Solution: Note that R_f is a finitely generated R-algebra as R_f is, by (**11.7**), obtained by adjoining $1/f$. So since R is a finitely generated k-algebra, R_f is one too. Moreover, R and R_f have the same fraction field K. Hence both $\dim(R)$ and $\dim(R_f)$ are equal to $\operatorname{tr.deg}_k(K)$ by (**15.10**). □

Exercise (15.31) . — Let k be a field, $P := k[f]$ the polynomial ring in one variable f. Set $\mathfrak{p} := \langle f \rangle$ and $R := P_{\mathfrak{p}}$. Find $\dim(R)$ and $\dim(R_f)$.

Solution: In P, the chain of primes $0 \subsetneqq \mathfrak{p}$ is maximal by (**2.17**). So $\langle 0 \rangle$ and $\mathfrak{p}R$ are the only primes in R by (**11.12**)(2). Thus $\dim(R) = 1$.

Set $K := \operatorname{Frac}(P)$. Then $R_f = K$ since, if $a/(bf^n) \in K$ with $a, b \in P$ and $f \nmid b$, then $a/b \in R$ and so $(a/b)/f^n \in R_f$. Thus $\dim(R_f) = 0$. □

Exercise (15.32) . — Let R be a ring, $R[X]$ the polynomial ring. Prove

$$1 + \dim(R) \le \dim(R[X]) \le 1 + 2\dim(R).$$

(In particular, $\dim(R[X]) = \infty$ if and only if $\dim(R) = \infty$.)

Solution: Let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ be a chain of primes in R. Then

$$\mathfrak{p}_0 R[X] \subsetneqq \cdots \subsetneqq \mathfrak{p}_n R[X] \subsetneqq \mathfrak{p}_n R[X] + \langle X \rangle$$

is a chain of primes in $R[X]$ by (**2.32**). Thus $1 + \dim(R) \le \dim(R[X])$.

Let $\mathfrak{p}$ be a prime of R, and $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r$ be a chain of primes of $R[X]$ with $\mathfrak{q}_i \cap R = \mathfrak{p}$ for each i. Then (**1.9**) and (**2.7**) yield a chain of primes of length r in

$R[X]/\mathfrak{p}R[X]$. Further, as $\mathfrak{q}_i \cap R = \mathfrak{p}$ for each i, the latter chain gives rise to a chain of primes of length r in $k(\mathfrak{p})[X]$ where $k(\mathfrak{p}) = (R/\mathfrak{p})_{\mathfrak{p}}$ by **(1.16)** and **(11.34)** and **(11.12)**(2). But $\dim\big(k(\mathfrak{p})[X]\big) = 1$ by **(15.9)** as $k(\mathfrak{p})[X]$ is a PID. Thus $r \le 1$.

Take any chain $\mathfrak{P}_0 \subsetneqq \cdots \subsetneqq \mathfrak{P}_m$ of primes in $R[X]$. It contracts to a chain $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ in R. At most two $\mathfrak{P}_j$ contract to a given $\mathfrak{p}_i$ by the above discussion. So $m + 1 \le 2(n+1)$, or $m \le 2n+1$. Thus $\dim(R[X]) \le 1 + 2\dim(R)$. □

15. Appendix: Jacobson Rings

Exercise (15.39) . — Let X be a topological space. We say a subset Y is **locally closed** if Y is the intersection of an open set and a closed set; equivalently, Y is open in its closure $\overline{Y}$; equivalently, Y is closed in an open set containing it.

We say a subset X_0 of X is **very dense** if X_0 meets every nonempty locally closed subset Y. We say X is **Jacobson** if its set of closed points is very dense.

Show that the following conditions on a subset X_0 of X are equivalent:

(1) X_0 is very dense.
(2) Every closed set F of X satisfies $\overline{F \cap X_0} = F$.
(3) The map $U \mapsto U \cap X_0$ from the open sets of X to those of X_0 is bijective.

Solution: Assume (1). Given a closed set F, take any $x \in F$, and let U be an open neighborhood of x in X. Then $F \cap U$ is locally closed, so meets X_0. Hence $x \in \overline{F \cap X_0}$. Thus $F \subset \overline{F \cap X_0}$. The opposite inclusion is trivial. Thus (2) holds.

Assume (2). In (3), the map is trivially surjective. To check it's injective, suppose $U \cap X_0 = V \cap X_0$. Then $(X-U) \cap X_0 = (X-V) \cap X_0$. So (2) yields $X - U = X - V$. So $U = V$. Thus (3) holds.

Assume (3). Then the map $F \mapsto F \cap X_0$ of closed sets is bijective too; whence, so is the map $Y \mapsto Y \cap X_0$ of locally closed sets. In particular, if a locally closed set Y is nonempty, then so is $Y \cap X_0$. Thus (1) holds. □

Exercise (15.40) . — Let R be a ring, $X := \operatorname{Spec}(R)$, and X_0 the set of closed points of X. Show that the following conditions are equivalent:

(1) R is a Jacobson ring.
(2) X is a Jacobson space.
(3) If $y \in X$ is a point such that $\{y\}$ is locally closed, then $y \in X_0$.

Solution: Assume (1). Let $F \subset X$ be closed. Trivially, $F \supset \overline{F \cap X_0}$. To prove $F \subset \overline{F \cap X_0}$, say $F = \mathbf{V}(\mathfrak{a})$ and $\overline{F \cap X_0} = \mathbf{V}(\mathfrak{b})$. Then $F \cap X_0$ is the set of maximal ideals $\mathfrak{m}$ containing $\mathfrak{a}$ by **(13.16)**(2), and every such $\mathfrak{m}$ contains $\mathfrak{b}$. So (1) implies $\mathfrak{b} \subset \sqrt{\mathfrak{a}}$. But $\mathbf{V}(\sqrt{\mathfrak{a}}) = F$. Thus $F \subset \overline{F \cap X_0}$. Thus **(15.39)** yields (2).

Assume (2). Let $y \in X$ be a point such that $\{y\}$ is locally closed. Then $\{y\} \bigcap X_0$ is nonempty by (2). So $\big(\{y\} \bigcap X_0\big) \ni y$. Thus (3) holds.

Assume (3). Let $\mathfrak{p}$ be a prime ideal of R such that $\mathfrak{p}R_f$ is maximal for some $f \notin \mathfrak{p}$. Then $\{\mathfrak{p}\}$ is closed in $\mathbf{D}(f)$ by **(13.1.8)**. So $\{\mathfrak{p}\}$ is locally closed in X. Hence $\{\mathfrak{p}\}$ is closed in X by (3). Thus $\mathfrak{p}$ is maximal. Thus **(15.35)** yields (1). □

Exercise (15.41) . — Why is a field K finite if it's an algebra-finite $\mathbb{Z}$-algebra?

Solution: First off, $\mathbb{Z}$ is Jacobson by **(15.33)**. So **(15.37)**(1) applies with $\mathbb{Z}$ for R, with K for R', and with $\langle 0\rangle$ for $\mathfrak{m}'$. Thus $\langle 0\rangle^c = \langle p\rangle$ for some prime $p \in \mathbb{Z}$, and K is finite over $\mathbb{Z}/\langle p\rangle$. Thus K is finite. □

Exercise (15.42) . — Let $P := \mathbb{Z}[X_1, \ldots, X_n]$ be the polynomial ring. Assume $F \in P$ vanishes at every zero in K^n of $F_1, \ldots, F_r \in P$ for every finite field K; that is, if $(a) := (a_1, \ldots, a_n) \in K^n$ and $F_1(a) = 0, \ldots, F_r(a) = 0$ in K, then $F(a) = 0$ too. Prove there are $G_1, \ldots, G_r \in P$ and $N \geq 1$ with $F^N = G_1F_1 + \cdots + G_rF_r$.

Solution: Set $\mathfrak{a} := \langle F_1, \ldots, F_r \rangle$. Suppose $F \notin \sqrt{\mathfrak{a}}$. Then F lies outside some maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$ by **(15.37)**(2) and **(15.33)**. Set $K := P/\mathfrak{m}$. Then K is a finite extension of $\mathbb{F}_p$ for some prime p by **(15.37)**(1). So K is finite. Let a_i be the residue of X_i, set $(a) := (a_1, \ldots, a_n) \in K^n$. Then $F_1(a) = 0, \ldots, F_r(a) = 0$. So $F(a) = 0$ by hypothesis. Thus $F \in \mathfrak{m}$, a contradiction. Thus $F \in \sqrt{\mathfrak{a}}$. □

Exercise (15.43) . — Prove that a ring R is Jacobson if and only if each algebra-finite algebra R' that is a field is module finite over it.

Solution: Assume that R is Jacobson. Given an algebra-finite algebra R', set $\mathfrak{m}' := \langle 0 \rangle \subset R'$ and $\mathfrak{m} := \mathfrak{m}'^c$. Assume R' is a field. Then $\mathfrak{m}'$ is maximal. So $\mathfrak{m}$ is maximal and R' is finite over $R/\mathfrak{m}$ by **(15.37)**(1). Thus R' is module finite over R.

Conversely, assume that R is not Jacobson. Then **(15.35)** yields a nonmaximal prime $\mathfrak{p}$ of R and an $f \notin \mathfrak{p}$ such that $\mathfrak{p}R_f$ is maximal. Set $R' := R/\mathfrak{p}$. Then R'_f is algebra finite over R. But $R'_f = R_f/\mathfrak{p}R_f$. So R'_f is a field.

Suppose R'_f is module finite over R, so over R'. Then R'_f is integral over R' by **(10.18)**. So R' is a field by **(14.1)**. So $\mathfrak{p}$ is maximal, a contradiction. □

Exercise (15.44) . — Prove a ring R is Jacobson if and only if each nonmaximal prime $\mathfrak{p}$ is the intersection of the primes that properly contain $\mathfrak{p}$.

Solution: Assume R is Jacobson. By **(15.33)**, every prime $\mathfrak{p}$ is the intersection of maximal ideals. Thus if $\mathfrak{p}$ is not maximal, then it is the intersection of the primes that properly contain it.

Conversely, assume R is not Jacobson. By **(15.33)**, there is a prime $\mathfrak{q}$ that is not the intersection of maximal ideals. If $R/\mathfrak{q}$ has a prime $\mathfrak{p}$ that is not maximal and is not the intersection of primes properly containing it, then its preimage in R is similar. Replace R by $R/\mathfrak{q}$. Thus we may assume R is a domain with $\operatorname{rad}(R) \neq \langle 0 \rangle$.

Say $f \in \operatorname{rad}(R)$ and $f \neq 0$. Then $0 \notin S_f$. So **(3.9)** yields a prime $\mathfrak{p}$ that is maximal among ideals not meeting S_f. Hence any prime properly containing $\mathfrak{p}$ also contains f. Thus $\mathfrak{p}$ is not the intersection of primes properly containing it. But $f \in \operatorname{rad}(R)$ and $f \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is not maximal. Thus $\mathfrak{p}$ is as desired. □

Exercise (15.45) . — Let R be a Jacobson ring, $\mathfrak{p}$ a prime, $f \in R - \mathfrak{p}$. Prove that $\mathfrak{p}$ is the intersection of all the maximal ideals containing $\mathfrak{p}$ but not f.

Solution: Set $\mathfrak{a} := \bigcap \mathfrak{m}$ where $\mathfrak{m}$ runs through the maximal ideals that contain $\mathfrak{p}$ but not f. Let's use double inclusion to prove $\mathfrak{p} = \mathfrak{a}$. Plainly $\mathfrak{p} \subset \mathfrak{a}$.

For the opposite inclusion, given $g \in R - \mathfrak{p}$, let's prove $g \in R - \mathfrak{a}$. If $\mathfrak{p}$ is maximal, then $\mathfrak{p} = \mathfrak{a}$, so $g \in R - \mathfrak{a}$. Assume $\mathfrak{p}$ is not maximal. Since R is Jacobson, $\mathfrak{p}R_{fg}$ is not maximal in R_{fg} by **(15.35)**. So there is a maximal ideal $\mathfrak{M}$ of R_{fg} containing $\mathfrak{p}R_{fg}$. Let $\mathfrak{m}$ be the contraction of $\mathfrak{M}$ in R. Plainly $f, g \notin \mathfrak{m}$ and $\mathfrak{m} \supset \mathfrak{p}$. But $\mathfrak{m}$ is maximal by **(15.37)**(1) applied with $R' := R_{fg}$. Thus $\mathfrak{p} \supset \mathfrak{a}$, as desired. □

Exercise (15.46) . — Let R be a ring, R' an algebra. Prove that if R' is integral over R and R is Jacobson, then R' is Jacobson.

Solution: Given an ideal $\mathfrak{a}' \subset R'$ and an f outside $\sqrt{\mathfrak{a}'}$, set $R'' := R[f]$. Then R'' is Jacobson by **(15.37)**(2). So R'' has a maximal ideal $\mathfrak{m}''$ that avoids f and contains $\mathfrak{a}' \cap R''$. But R' is integral over R''. So R' contains a prime $\mathfrak{m}'$ that contains $\mathfrak{a}'$ and that contracts to $\mathfrak{m}''$ by Going-up **(14.3)**(4). Then $\mathfrak{m}'$ avoids f as $\mathfrak{m}''$ does, and $\mathfrak{m}'$ is maximal by Maximality, **(14.3)**(1). Thus R' is Jacobson. □

Exercise (15.47) . — Let R be a Jacobson ring, S a multiplicative subset, $f \in R$. True or false: prove or give a counterexample to each of the following statements.

(1) The localized ring R_f is Jacobson.
(2) The localized ring $S^{-1}R$ is Jacobson.
(3) The filtered direct limit $\varinjlim R_\lambda$ of Jacobson rings is Jacobson.
(4) In a filtered direct limit of rings R_λ, necessarily $\varinjlim \operatorname{rad}(R_\lambda) = \operatorname{rad}(\varinjlim R_\lambda)$.

Solution: (1) True: $R_f = R[1/f]$ by **(11.7)**; so R_f is Jacobson by **(15.37)**(2).
(2) False: by **(15.34)**, $\mathbb{Z}$ is Jacobson, but $\mathbb{Z}_{\langle p\rangle}$ isn't for any prime number p.
(3) False: $Z_{\langle p\rangle}$ isn't Jacobson by **(15.34)**, but $Z_{\langle p\rangle} = \varinjlim \mathbb{Z}$ by **(12.6)**.
(4) False: $\operatorname{rad}(\mathbb{Z}_{\langle p\rangle}) = p\mathbb{Z}_{\langle p\rangle}$; but $\operatorname{rad}(\mathbb{Z}) = \langle 0\rangle$, so $\varinjlim \operatorname{rad}(\mathbb{Z}) = \langle 0\rangle$. □

Exercise (15.48) . — Let R be a reduced Jacobson ring with a finite set Σ of minimal primes, and P a finitely presented module. Show that P is locally free of rank r if and only if $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$ for any maximal ideal $\mathfrak{m}$.

Solution: Suppose P is locally free of rank r. Then given any maximal ideal $\mathfrak{m}$, there is an $f \in R - \mathfrak{m}$ such that P_f is a free R_f-module of rank r by **(13.13)**. But $P_\mathfrak{m}$ is a localization of P_f by **(12.25)**(2). So $P_\mathfrak{m}$ is a free $R_\mathfrak{m}$-module of rank r by **(12.9)**. But $P_\mathfrak{m}/\mathfrak{m}P_\mathfrak{m} = (P/\mathfrak{m}P)_\mathfrak{m}$ by **(12.15)**. Also $R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m} = R/\mathfrak{m}$ by **(12.16)**. Thus $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$.

Consider the converse. Given a $\mathfrak{p} \in \Sigma$, set $K := \operatorname{Frac}(R/\mathfrak{p})$. Then $P \otimes_R K$ is a K-vector space, say of dimension n. Since R is reduced, $K = R_\mathfrak{p}$ by **(14.21)**. But P is finitely presented. So by **(12.18)**(2), there's an $h \in R - \mathfrak{p}$ with P_h free of rank n. As R is Jacobson, there's a maximal ideal $\mathfrak{m}$ avoiding h, by **(15.33)**. Hence, as above, $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = n$. But, by hypothesis, $\dim_{R/\mathfrak{m}}(P/\mathfrak{m}P) = r$. Thus $n = r$.

Given a maximal ideal $\mathfrak{m}$, set $A := R_\mathfrak{m}$. Then A is reduced by **(13.57)**. Each minimal prime of A is of the form $\mathfrak{p}A$ where $\mathfrak{p} \in \Sigma$ by **(11.12)**(2). Further, it's not hard to see, essentially as above, that $P_\mathfrak{m} \otimes \operatorname{Frac}(A/\mathfrak{p}A) = P \otimes \operatorname{Frac}(R/\mathfrak{p})$. Hence **(14.23)** implies $P_\mathfrak{m}$ is a free A-module of rank r. Finally, **(13.62)** implies P is locally free of rank r. □

16. Chain Conditions

Exercise (16.2) . — Let M be a finitely generated module over an arbitrary ring. Show every set that generates M contains a finite subset that generates.

Solution: Say M is generated by $x_1, \ldots, x_n$ and also by the y_λ for $\lambda \in \Lambda$. Say $x_i = \sum_j z_j y_{\lambda_{ij}}$. Then the $y_{\lambda_{ij}}$ generate M. □

Exercise (16.23) . — Let M be a module. Assume that every nonempty set of finitely generated submodules has a maximal element. Show M is Noetherian.

Solution: Given a submodule N, form the set $\mathcal{S}$ of all its finitely generated submodules. By hypothesis, $\mathcal{S}$ has a maximal element N_0. Suppose $N_0 \neq N$, and take any $x \in N - N_9$. Then the submodule of N generated by N_0 and x is finitely generated, and it properly contains N_0, a contradiction. Thus $N = N_0$. So N is finitely generated. Thus M is Noetherian. □

Exercise (16.24) . — Let R be a Noetherian ring, $\{F_\lambda\}_{\lambda\in\Lambda}$ a set of polynomials in variables $X_1, \ldots, X_n$. Show there's a finite subset $\Lambda_0 \subset \Lambda$ such that the set V_0 of zeros in R^n of the F_λ for $\lambda \in \Lambda_0$ is precisely that V of the F_λ for $\lambda \in \Lambda$.

Solution: Set $P := R[X_1, \ldots, X_n]$ and $\mathfrak{a} := \langle \{F_\lambda\}_{\lambda\in\Lambda} \rangle$. Then P is Noetherian by (**16.10**). So $\mathfrak{a}$ is finitely generated. So by (**16.2**) there's a finite subset $\Lambda_0 \subset \Lambda$ such that the F_λ for $\lambda \in \Lambda_0$ generate $\mathfrak{a}$.

Trivially, $V_0 \supset V$. Conversely, $V_0 \subset V$ because, $F_\lambda \in \mathfrak{a}$ for each $\lambda \in \Lambda$, and so there are $G_{\lambda\mu} \in P$ with $F_\lambda = \sum G_{\lambda\mu} F_\mu$. Thus $V_0 = V$. □

Exercise (16.25) . — Let R be a Noetherian ring, $F := \sum a_n X^n \in R[[X]]$ a power series in one variable. Show that F is nilpotent if and only if each a_n is too.

Solution: By (**3.19**)(1), if F is nilpotent, then each a_n is too for any ring R.

Conversely, assume each a_n is nilpotent. Set $\mathfrak{N} := \mathrm{nil}(R)$. Since R is Noetherian, $\mathfrak{N}$ is finitely generated. So there is $m \geq 1$ with $\mathfrak{N}^m = 0$ by (**3.38**) with $\mathfrak{a} := 0$. Since each a_n lies in $\mathfrak{N}$, each coefficient of F^r lies in $\mathfrak{N}^r$ for all $r \geq 1$. Thus each coefficient of F^m is 0; that is, F is nilpotent. □

Exercise (16.26) . — Let R be a ring, X a variable, $R[X]$ the polynomial ring. Prove this statement or find a counterexample: if $R[X]$ is Noetherian, then so is R.

Solution: It's true. Since $R[X]$ is Noetherian, so is $R[X]/\langle X \rangle$ by (**16.7**). But the latter ring is isomorphic to R by (**1.6**)(2); so R is Noetherian. □

Exercise (16.27) . — Let R'/R be a ring extension with an R-linear retraction $\rho\colon R' \to R$. If R' is Noetherian, show R is too. What if R' is Artinian?

Solution: Assume R' is Noetherian. Let $\mathfrak{a} \subset R$ be an ideal. Then $\mathfrak{a}R'$ is finitely generated. But $\mathfrak{a}$ generates $\mathfrak{a}R'$. So (**16.2**) yields $a_1, \ldots, a_n \in \mathfrak{a}$ that generate $\mathfrak{a}R'$. Hence, given any $a \in \mathfrak{a}$, there are $x'_i \in R'$ such that $a = a_1x'_1 + \cdots + a'_nx'_n$. Applying ρ yields $a = a_1x_1 + \cdots + a_nx_n$ with $x_i := \rho(x'_i) \in R$. Thus $\mathfrak{a}$ is finitely generated. Thus R is Noetherian.

Alternatively, let $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ be an ascending chain of ideals of R. Then $\mathfrak{a}_1R' \subset \mathfrak{a}_2R' \subset \cdots$ stabilizes as R' is Noetherian. So $\rho(\mathfrak{a}_1R') \subset \rho(\mathfrak{a}_2R') \subset \cdots$ stabilizes too. But $\rho(\mathfrak{a}_iR') = \mathfrak{a}_i\rho(R') = \mathfrak{a}_i$. Thus by (**16.5**), R is Noetherian.

Finally, if R' is, instead, Artinian, then R is too, owing to an argument like the alternative argument above, but applied to a descending chain. □

Exercise (16.28) . — Let R be a ring, M a module, R' a faithfully flat algebra. If $M \otimes_R R'$ is Noetherian over R', show M is Noetherian over R. What if $M \otimes_R R'$ is Artinian over R'?

Solution: Assume $M \otimes R'$ is Noetherian over R'. Since R' is flat, given a submodule N of M, the R'-module $N \otimes R'$ may be regarded as a submodule of $M \otimes R'$. So $N \otimes R'$ is finitely generated. But it's also generated over R' by the elements $n \otimes 1$ for $n \in N$. Hence (**16.2**) yields $n_1, \ldots, n_r \in N$ such that the $n_i \otimes 1$ generate $N \otimes R'$ over R'. The n_i define an R-map $\alpha\colon R^r \to N$. It induces an R'-map

$\alpha\otimes R'\colon R'^r \to N\otimes R'$, which is surjective. But R' is faithfully flat. So α is surjective by (**9.19**). So N is finitely generated. Thus M is Noetherian.

Alternatively, let $N_1 \subset N_2 \subset \cdots$ be a chain of submodules in M. Since $M \otimes R'$ is Noetherian, the induced chain $N_1 \otimes R' \subset N_2 \otimes R' \subset \cdots$ stabilizes. Since R' is faithfully flat, an inclusion $N_i \hookrightarrow N_{i+1}$ is surjective if $N_i \otimes R' \hookrightarrow N_{i+1} \otimes R'$ is by (**9.19**). Hence the original chain stabilizes. Thus M is Noetherian.

Finally, if $M \otimes R$ is, instead, Artinian, then M is too, owing to an argument like the alternative argument above, but applied to a descending chain. □

Exercise (16.29) . — Let R be a ring. Assume that, for each maximal ideal $\mathfrak{m}$, the local ring $R_{\mathfrak{m}}$ is Noetherian and that each nonzero $x \in R$ lies in only finitely many maximal ideals. Show R is Noetherian: use (**13.10**) to show any ideal is finitely generated; alternatively, use (**13.9**) to show any ascending chain stabilizes.

Solution: Given a nonzero ideal $\mathfrak{a}$, take a nonzero $x \in \mathfrak{a}$. Then x lies in only finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. As each $R_{\mathfrak{m}_i}$ is Noetherian, $\mathfrak{a}R_{\mathfrak{m}_i}$ is finitely generated, say by $x_{i,j}/s_{i,j}$ with $x_{i,j} \in \mathfrak{a}$ and $s_{i,j} \in R - \mathfrak{m}_i$ for $j = 1, \ldots, n_i$. Let see that together x and all the $x_{i,j}$ generate $\mathfrak{a}$.

Given a maximal ideal $\mathfrak{m}$, let's see that the fractions $x/1$ and $x_{i,j}/1$ generate $\mathfrak{a}R_{\mathfrak{m}}$. If $x \notin \mathfrak{m}$, then $x/1$ is a unit, hence generates $\mathfrak{a}R_{\mathfrak{m}}$. If $x \in \mathfrak{m}$, then $\mathfrak{m} = \mathfrak{m}_i$ for some i, and so the $x_{i,j}/1$ generate $\mathfrak{a}R_{\mathfrak{m}}$, as desired.

Hence x and the $x_{i,j}$ generate $\mathfrak{a}$ by (**13.10**). Thus R is Noetherian.

Alternatively, let $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ be an ascending chain of ideals of R. It is trivially stable if $\mathfrak{a}_i = 0$ for all i. So assume some $\mathfrak{a}_{n_0}$ contains a nonzero x. Then x lies in only finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$. Since each $R_{\mathfrak{m}_j}$ is Noetherian, there's n_j such that $\mathfrak{a}_{n_j}R_{\mathfrak{m}} = \mathfrak{a}_{n_j+1}R_{\mathfrak{m}} = \cdots$. Set $n := \max\{n_0, \ldots, n_m\}$.

Let $\mathfrak{m}$ be a maximal ideal. Suppose $x \notin \mathfrak{m}$. Then $x/1 \in R_{\mathfrak{m}}$ is a unit. So $\mathfrak{a}_{n_0}R_{\mathfrak{m}} = R_{\mathfrak{m}}$. So $\mathfrak{a}_nR_{\mathfrak{m}} = \mathfrak{a}_{n+1}R_{\mathfrak{m}} = \cdots$. Suppose $x \in \mathfrak{m}$. Then $\mathfrak{m} = \mathfrak{m}_j$ for some j. So again $\mathfrak{a}_nR_{\mathfrak{m}} = \mathfrak{a}_{n+1}R_{\mathfrak{m}} = \cdots$.

Given $k \ge n$, set $N_k := \mathfrak{a}_{k+1}/\mathfrak{a}_k$. Then $(N_k)_{\mathfrak{m}} = \mathfrak{a}_{k+1}R_{\mathfrak{m}}\big/\mathfrak{a}_kR_{\mathfrak{m}} = 0$. So $N_k = 0$ by (**13.8**). So the inclusion $\mathfrak{a}_k \hookrightarrow \mathfrak{a}_{k+1}$ is surjective by (**13.9**). So $\mathfrak{a}_k = \mathfrak{a}_{k+1}$. Thus $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$. Thus again R is Noetherian. □

Exercise (16.30) (*Nagata*) . — Let k be a field, $P := k[X_1, X_2, \ldots]$ a polynomial ring, $m_1 < m_2 < \cdots$ positive integers with $m_{i+1} - m_i > m_i - m_{i-1}$ for $i > 1$. Set $\mathfrak{p}_i := \langle X_{m_i+1}, \ldots, X_{m_{i+1}}\rangle$ and $S := P - \bigcup_{i\ge1}\mathfrak{p}_i$. Show S is multiplicative, $S^{-1}P$ is Noetherian of infinite dimension, and the $S^{-1}\mathfrak{p}_i$ are the maximal ideals of $S^{-1}P$.

Solution: Each $P/\mathfrak{p}_i$ is a polynomial ring over k by (**1.17**)(5). So $\mathfrak{p}_i$ is prime. So $P - \mathfrak{p}_i$ is multiplicative. But $S = \bigcap_{i\ge1}(P - \mathfrak{p}_i)$. Thus S is multiplicative.

Similarly, for all $i \ge 1$, all ideals are prime in the following chain:

$$\langle 0\rangle \subsetneqq \langle X_{m_i+1}\rangle \subsetneqq \cdots \subsetneqq \langle X_{m_i+1}, \ldots, X_{m_{i+1}}\rangle = \mathfrak{p}_i.$$

But $\mathfrak{p}_i \cap S = \emptyset$. So by (**11.12**)(2), this chain induces a chain of the same length $m_{i+1} - m_i$ in $S^{-1}P$. But $m_{i+1} - m_i > m_i - m_{i-1}$. Thus $S^{-1}P$ is of infinite dimension.

Given any prime ideal $\mathfrak{P}$ of $S^{-1}P$, let $\mathfrak{p}$ be its contraction in P. Then $\mathfrak{p} \cap S = \emptyset$ by (**11.12**)(2). But $S = P - \bigcup \mathfrak{p}_i$. So $\mathfrak{p} \subset \bigcup \mathfrak{p}_i$. So (**3.27**)(3) yields $\mathfrak{p} \subset \mathfrak{p}_i$ for some i. Thus (**11.11**)(1)(b) yields $\mathfrak{P} \subset S^{-1}\mathfrak{p}_i$ for some i.

If $\mathfrak{P}$ is maximal, then $\mathfrak{P} = S^{-1}\mathfrak{p}_i$. Thus every maximal ideal of $S^{-1}P$ has the form $S^{-1}\mathfrak{p}_i$. Conversely, given j, note $S^{-1}\mathfrak{p}_j$ lies in some maximal ideal of $S^{-1}P$;

say it's $\mathfrak{P}$. Then $\mathfrak{p}_j \subset \mathfrak{p}$ by (**11.12**)(2). But $\mathfrak{p} \subset \mathfrak{p}_i$. So $i = j$, and $\mathfrak{P} = S^{-1}\mathfrak{p}_i$. So $S^{-1}\mathfrak{p}_i$ is maximal. Thus the $S^{-1}\mathfrak{p}_i$ are all the maximal ideals of $S^{-1}P$.

Given i, note $S \cap \mathfrak{p}_i = \emptyset$. So $P_{\mathfrak{p}_i}$ is the localization of $S^{-1}P$ at the prime $S^{-1}\mathfrak{p}_i$ by (**12.25**)(2). Let P' be the polynomial subring over k in the variables X_j for $j \le m_i$ and $j > m_{i+1}$, and set $T := P' - 0$ and $K := \mathrm{Frac}(P') = T^{-1}P'$. Then (**11.34**) yields $T^{-1}P = K[X_{m_i+1}, \dots, X_{m_{i+1}}]$. But $T \cap \mathfrak{p}_i = \emptyset$. Thus (**12.25**)(2) yields

$$P_{\mathfrak{p}_i} = K[X_{m_i+1}, \dots, X_{m_{i+1}}]_{T^{-1}\mathfrak{p}_i}.$$

Note $K[X_{m_i+1}, \dots, X_{m_{i+1}}]$ is Noetherian by the Hilbert Basis Theorem (**16.10**). So $P_{\mathfrak{p}_i}$ is Noetherian by (**16.7**). But $(S^{-1}P)_{S^{-1}\mathfrak{p}_i} = P_{\mathfrak{p}_i}$. Thus it's Noetherian.

Finally, for $f/s \in S^{-1}P$, the polynomial f involves only finitely many variables X_i. Hence f/s lies in only finitely many ideals of the form $S^{-1}\mathfrak{p}_i$. But these are all the maximal ideals of $S^{-1}P$. Thus $S^{-1}P$ is Noetherian by (**16.29**). □

Exercise (16.31) . — Let z be a complex variable. Determine which of these rings R are Noetherian:

(1) the ring R of rational functions of z having no pole on the circle $|z| = 1$,
(2) the ring R of power series in z having a positive radius of convergence,
(3) the ring R of power series in z with an infinite radius of convergence,
(4) the ring R of polynomials in z whose first k derivatives, $k \ge 1$, vanish at 0,
(5) the ring R of polynomials in two complex variables z, w all of whose partial derivatives with respect to w vanish for $z = 0$.

Solution: For (1), let $S \subset \mathbb{C}[z]$ be the subset of polynomials with no zero on $|z| = 1$. Then S is a multiplicative subset. Moreover, $R = S^{-1}\mathbb{C}[z]$. But $\mathbb{C}[z]$ is Noetherian by (**16.9**). Thus (**16.7**) implies R is Noetherian.

For (2), given a nonzero $F \in R$, say $F = \sum_{i=n}^{\infty} a_i z^i$ with $a_n \ne 0$. Then $F = z^n G$ with $G := \sum_{i=0}^{\infty} a_{i+n} z^i$. Plainly G has the same radius of convergence as F; so $G \in R$. Also, $G^{-1} \in R$; see [**12**, Thm. 3.3, p. 65]. So an argument like that in (**3.8**) shows that every nonzero ideal has the form $\langle z^n \rangle$ for some $n \ge 0$. Thus R is Noetherian (in fact, a PID).

For (3), note that a convergent power series is holomorphic inside its disc of convergence; see [**12**, Thm. 5.1, p. 72]. So a function is **entire** — that is, holomorphic on all of $\mathbb{C}$ — if and only if it is in R; see [**12**, Ch. III, (S_7), pp. 129, 130].

For any $n \ge 0$, there is an entire function F_n with zeros at $n, n+1, \dots$ and nowhere else; see [**12**, Thm. 2.3, p. 362]. Let $\mathfrak{a}_n$ be the ideal of all $F \in R$ with zeros at $n, n+1, \dots$. Then $F_n \in \mathfrak{a}_n - \mathfrak{a}_{n-1}$. So $\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \cdots$. Thus R is not Noetherian.

For (4), note R is just the ring of polynomials of the form $c + z^{k+1}F$ where $c \in \mathbb{C}$ and $F \in \mathbb{C}[z]$. So $\mathbb{C} \subset R \subset \mathbb{C}[z]$. Moreover, $\mathbb{C}[z]$ is generated as a module over R by $1, z, z^2, \dots, z^k$. So R is algebra finite over $\mathbb{C}$ owing to (**16.17**). Thus (**16.10**) implies R is Noetherian.

For (5), set $R' := \{c + zG(z,w) \mid c \in \mathbb{C} \text{ and } G \in \mathbb{C}[z,w]\}$, and let R'' be the ring R of polynomials in z, w whose first partial derivative with respect to w vanishes for $z = 0$. Let's show $R' = R = R''$.

Plainly $R' \subset R \subset R''$. Conversely, given $F \in R''$, say $F = \sum F_i w^i$, where the $F_i \in \mathbb{C}[z]$. By hypothesis, $(\partial F/\partial w)(0, w) = 0$. Hence $\sum iF_i(0)w^{i-1} = 0$. Hence $F_i(0) = 0$ for all $i \ge 1$. So $z \mid F_i$. So $F \in R'$. Thus $R' = R = R''$. Thus R is just the case $k := \mathbb{C}$ of the second example in (**16.1**) of a non-Noetherian ring. □

Exercise (16.32) . — Let R be a ring, M a Noetherian module. Adapt the proof of the Hilbert Basis Theorem(**16.9**) to prove $M[X]$ is a Noetherian $R[X]$-module.

Solution: By way of contradiction, assume there is a submodule N of $M[X]$ that is not finitely generated. Set $N_0 := 0$. For $i \geq 1$, choose inductively F_i in $N - N_{i-1}$ of least degree d_i, and let N_i be the submodule generated by $F_1, \ldots, F_i$. Let m_i be the leading coefficient of F_i, and L the submodule of M generated by all the m_i. As M is Noetherian, L is finitely generated. So there's $n \geq 1$ such that $m_1, \ldots, m_n$ generate L by (**16.2**). Thus $m_{n+1} = x_1 m_1 + \cdots + x_n m_n$ with $x_i \in R$.

By construction, $d_i \leq d_{i+1}$ for all i. Set

$$F := F_{n+1} - \big(x_1 F_1 X^{d_{n+1}-d_1} + \cdots + x_n F_n X^{d_{n+1}-d_n}\big).$$

Then $\deg(F) < d_{n+1}$, so $F \in N_n$. Therefore, $F_{n+1} \in N_n$, a contradiction. □

Exercise (16.33) . — Let R be a ring, S a multiplicative subset, M a Noetherian module. Show that $S^{-1}M$ is a Noetherian $S^{-1}R$-module.

Solution: Let K be a submodule of $S^{-1}M$. As M is Noetherian, $\varphi_S^{-1}K \subset M$ is finitely generated. Say $m_1, \ldots, m_k$ generate it. Plainly $m_1/1, \ldots, m_k/1$ generate $S^{-1}\varphi_S^{-1}K$ over $S^{-1}R$. But $S^{-1}\varphi_S^{-1}K = K$ by (**12.12**)(2)(b). Thus $S^{-1}M$ is a Noetherian $S^{-1}R$-module.

Alternatively, let $K_1 \subset K_2 \subset \cdots$ be an ascending chain of $S^{-1}R$-submodues of $S^{-1}M$. Then $\varphi_S^{-1}K_1 \subset \varphi_S^{-1}K_2 \subset \cdots$ is an ascending chain of R-submodules of M. Since M is Noetherian, there is $n \geq 1$ with $\varphi_S^{-1}K_n = \varphi_S^{-1}K_{n+1} = \cdots$. But $S^{-1}\varphi_S^{-1}K_i = K_i$ for all i by (**12.12**)(2)(b). Hence $K_n = K_{n+1} = \cdots$. Thus $S^{-1}M$ is a Noetherian $S^{-1}R$-module. □

Exercise (16.34) . — For $i = 1, 2$, let R_i be a ring, M_i a Noetherian R_i-module. Set $R := R_1 \times R_2$ and $M := M_1 \times M_2$. Show that M is a Noetherian R-module.

Solution: Any submodule N of M is of the form $N = N_1 \times N_2$ where N_i is an R_i-submodule of M_i by a simple generalization of (**1.23**). But M_i is Noetherian; so N_i is finitely generated, say by $n_{i,1}, \ldots, n_{i,h_i}$. Then plainly the $(n_{1,j},\, 0)$ and $(0,\, n_{2,k})$ generate N. Thus M is a Noetherian R-module.

Alternatively, let $N_1 \subset N_2 \subset \cdots$ be an ascending chain of R-submodues of M. Then $N_j = N_{1,j} \times N_{2,j}$ where where $N_{i,j}$ is an R_i-submodule of M_i by a simple generalization of (**1.23**). In fact, the proof shows that, for each i, the $N_{i,j}$ form an ascending chain. But M_i is Noetherian; so this chain stabilizes. Hence the original chain stabilizes too. Thus M is a Noetherian R-module. □

Exercise (16.35) . — Let $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ be a short exact sequence of R-modules, and M_1, M_2 two submodules of M. Prove or give a counterexample to this statement: if $\beta(M_1) = \beta(M_2)$ and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2)$, then $M_1 = M_2$.

Solution: The statement is false: form the exact sequence

$$0 \to \mathbb{R} \xrightarrow{\alpha} \mathbb{R} \oplus \mathbb{R} \xrightarrow{\beta} \mathbb{R} \to 0$$

with $\alpha(r) := (r, 0)$ and $\beta(r, s) := s$, and take

$$M_1 := \{(t, 2t) \mid t \in \mathbb{R}\} \quad \text{and} \quad M_2 := \{(2t, t) \mid t \in \mathbb{R}\}.$$

(Geometrically, we can view M_1 as the line determined by the origin and the point $(1, 2)$, and M_2 as the line determined by the origin and the point $(2, 1)$. Then $\beta(M_1) = \beta(M_2) = \mathbb{R}$, and $\alpha^{-1}(M_1) = \alpha^{-1}(M_2) = 0$, but $M_1 \neq M_2$ in $\mathbb{R} \oplus \mathbb{R}$.) □

Exercise (16.36) . — Let R be a ring, $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ideals such that each $R/\mathfrak{a}_i$ is a Noetherian ring. Prove (1) that $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module, and (2) that, if $\bigcap \mathfrak{a}_i = 0$, then R too is a Noetherian ring.

Solution: Any R-submodule of $R/\mathfrak{a}_i$ is an ideal of $R/\mathfrak{a}_i$. As $R/\mathfrak{a}_i$ is a Noetherian ring, such an ideal is finitely generated as an $(R/\mathfrak{a}_i)$-module, so as an R-module as well. Thus $R/\mathfrak{a}_i$ is a Noetherian R-module. So $\bigoplus R/\mathfrak{a}_i$ is a Noetherian R-module by **(16.14)**. Thus (1) holds.

To prove (2), note that the kernel of the natural map $R \to \prod R/\mathfrak{a}_i = \bigoplus R/\mathfrak{a}_i$ is $\bigcap \mathfrak{a}_i$, which is 0 by hypothesis. Hence R can be identified with a submodule of the Noetherian R-module $\bigoplus R/\mathfrak{a}_i$. So R itself is a Noetherian R-module by **(16.13)**(2). So R is a Noetherian ring by **(16.11)**. Thus (2) holds. □

Exercise (16.37) . — Let R be a ring, and M and N modules. Assume that N is Noetherian and that M is finitely generated. Show that $\operatorname{Hom}(M, N)$ is Noetherian.

Solution: Say M is generated m elements. Then **(4.10)**(1) yields a surjection $R^{\oplus m} \twoheadrightarrow M$. It yields an inclusion $\operatorname{Hom}(M, N) \hookrightarrow \operatorname{Hom}(R^m, N)$ by **(5.11)**(1). But $\operatorname{Hom}(R^{\oplus m}, N) = \operatorname{Hom}(R, N)^{\oplus m} = N^{\oplus m}$ by **(4.13.2)** and **(4.3)**. Further, $N^{\oplus m}$ is Noetherian by **(16.14)**. Thus **(16.13)**(2) implies $\operatorname{Hom}(M, N)$ is Noetherian. □

Exercise (16.38) . — Let R be a ring, M a module. If R is Noetherian, and M finitely generated, show $S^{-1}D(M) = D(S^{-1}M)$.

Solution: Use the map σ in **(12.19)** twice to form this diagram:

$$\begin{CD}
M @>{D(M)}>> \operatorname{Hom}(\operatorname{Hom}(M,\,R),\,R) @>{\mu_S}>> S^{-1}\operatorname{Hom}(\operatorname{Hom}(M,\,R),\,R)\\
@V{\mu_S}VV @. @VV{\sigma}V\\
S^{-1}M @>{D(S^{-1}M)}>> \operatorname{Hom}(\operatorname{Hom}(S^{-1}M,\,S^{-1}R),\,S^{-1}R) @>{\sigma^*}>> \operatorname{Hom}(S^{-1}\operatorname{Hom}(M,\,R),\,S^{-1}R)
\end{CD}$$

It commutes, as $\big((\sigma\mu_S D(M))(m)\big)(\alpha/s) = \alpha(m)/s = \big((\sigma^* D(S^{-1}M)\mu_S)(m)\big)(\alpha/s)$ where $m \in M$ and $\alpha \in \operatorname{Hom}(M,\,R)$ and $s \in S$.

Assume R is Noetherian, and M finitely generated. Then $\operatorname{Hom}(M, R)$ is finitely presented by **(16.37)** and **(16.15)**. So **(12.19)** implies that, in the diagram, σ and σ^* are isomorphisms. Hence $S^{-1}D(M) = \sigma^{-1}\sigma^* D(S^{-1}M)$, as desired. □

Exercise (16.39) . — Let R be a domain, R' an algebra, and set $K := \operatorname{Frac}(R)$. Assume R is Noetherian. Prove the following statements.

(1) [**2**, Thm. 3] Assume R' is a field containing R. Then R'/R is algebra finite if and only if K/R is algebra finite and R'/K is (module) finite.

(2) [**2**, bot. p. 77] Let $K' \supset R$ be a field that embeds in R'. Assume R'/R is algebra finite. Then K/R is algebra finite and K'/K is finite.

Solution: For (1), first assume R'/R is algebra finite. Now, $R \subset K \subset R'$. So R'/K is algebra finite. Thus R'/K is (module) finite by **(15.4)** or **(16.19)**, and so K/R is algebra finite by **(16.17)**.

Conversely, say $x_1, \ldots, x_m$ are algebra generators for K/R, and say $y_1, \ldots, y_n$ are module generators for R'/K. Then clearly $x_1, \ldots, x_m, y_1, \ldots, y_n$ are algebra generators for R'/R. Thus (1) holds.

For (2), let $\mathfrak{m}$ be any maximal ideal of R', and set $L := R'/\mathfrak{m}$. Then L is a field, $R \subset K \subset K' \subset L$, and L/R is algebra finite. So K/R is algebra finite and L/K is finite by (1); whence, K'/K is finite too. Thus (2) holds. □

Exercise (16.40) . — Let R be a domain, $K := \mathrm{Frac}(R)$, and $x \in K$. If x is integral over R, show there is a nonzero $d \in R$ such that $dx^n \in R$ for all $n \ge 0$. Conversely, if such a d exists and if R is Noetherian, show x is integral over R.

Solution: Set $R' := R[x]$. Assume x is integral. Then **(10.14)** implies R' is module finite, say generated by $y_i = x_i/d_i$ for $i = 1, \ldots, n$ with $x_i, d_i \in R - \langle 0 \rangle$. Set $d := \prod_{i=1}^n d_i$. Then $dy_i \in R$ for all i, so $dR' \subset R$. Thus $dx^n \in R$ for all $n \ge 0$.

Conversely, assume R is Noetherian. Given d with $dR' \subset R$, note $R' \subset (1/d)R$. But $(1/d)R$ is a finitely generated module, so Noetherian by **(16.11)**. Hence R' is module finite. Thus x is integral by **(10.14)**. □

Exercise (16.41) . — Let k be a field, V a vector space. Show these statements are equivalent: (1) V is finite dimensional; (2) V is Noetherian; (3) V is Artinian.

Solution: Assume (1). Then any ascending or descending chain of subspaces V_i of V stabilizes, as $\dim(V_1), \dim(V_2), \dim(V_3), \ldots$ stabilizes. Thus (2) and (3) hold.

Conversely, assume (1) doesn't hold. Construct a chain $V_0 \subsetneqq V_1 \subsetneqq V_2 \subsetneqq \cdots$ of subspaces with $\dim(V_i) = i$: set $V_0 = 0$; given V_i, there's $v_{i+1} \in V - V_i$ as $\dim(V) = \infty$; let V_{i+1} be the subspace generated by V_i and v_{i+1}. Obviously, $\dim(V_{i+1}) = i + 1$. Now, by **(16.11)**, the chain shows (2) doesn't hold.

Note the v_i are linearly independent. For $j \ge 1$, let W_j be the subspace generated by $v_j, v_{j+1}, \ldots$. Then $W_1 \supsetneqq W_2 \supsetneqq \cdots$. Thus by **(16.21)**, (3) doesn't hold too. □

Exercise (16.42) . — Let k be a field, R an algebra, M an R-module. Assume M is finite dimensional as a k-vector space. Prove M is Noetherian and Artinian.

Solution: Plainly, if M is Noetherian or Artinian as a k-vector space, then it is so as an R-module. Thus **(16.41)** yields the assertion. □

Exercise (16.43) . — Let R be a ring, and $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ maximal ideals. Assume $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Set $\mathfrak{a}_0 := R$, and for $1 \le i \le n$, set $\mathfrak{a}_i := \mathfrak{m}_1 \cdots \mathfrak{m}_i$ and $V_i := \mathfrak{a}_{i-1}/\mathfrak{a}_i$. Using the $\mathfrak{a}_i$ and V_i, show that R is Artinian if and only if R is Noetherian.

Solution: Note that each V_i is also a vector space over $R/\mathfrak{m}_i$.

Assume R is Noetherian. Fix $i \ge 1$. Then $\mathfrak{a}_i$ is finitely generated. So V_i is finitely generated. So $\dim_{(R/\mathfrak{m}_i)}(V_i) < \infty$. Hence V_i is Artinian over R by **(16.42)**. But $V_i := \mathfrak{a}_{i-1}/\mathfrak{a}_i$. Hence, if $\mathfrak{a}_i$ is Artinian, so is $\mathfrak{a}_{i-1}$ by **(16.22)**(2). But $\mathfrak{a}_n = 0$. Thus $\mathfrak{a}_i$ is Artinian for all i. But $\mathfrak{a}_0 = R$. Thus R is Artinian.

Conversely, assume R is Artinian. Fix $i \ge 1$. Then $\mathfrak{a}_i$ and V_i are Artinian by **(16.22)**(2). So V_i is Noetherian owing to **(16.42)**. But $V_i := \mathfrak{a}_{i-1}/\mathfrak{a}_i$. Hence, if $\mathfrak{a}_i$ is Noetherian, so is $\mathfrak{a}_{i-1}$ by **(16.13)**(2). But $\mathfrak{a}_n = 0$. Thus $\mathfrak{a}_i$ is Noetherian for all i. But $\mathfrak{a}_0 = R$. Thus R is Noetherian. □

Exercise (16.44) . — Fix a prime number p. Set $M_n := \{\, q \in \mathbb{Q}/\mathbb{Z} \mid p^n q = 0 \,\}$ for $n \ge 0$. Set $M := \bigcup M_n$. Find a canonical isomorphism $\mathbb{Z}/\langle p^n \rangle \xrightarrow{\sim} M_n$. Given a proper $\mathbb{Z}$-submodule N of M, show $N = M_n$ for some n. Deduce M is Artinian, but not Noetherian. Find $\mathrm{Ann}(M)$, and deduce $\mathbb{Z}/\mathrm{Ann}(M)$ is not Artinian.

Solution: Let $\kappa\colon \mathbb{Q} \twoheadrightarrow \mathbb{Q}/\mathbb{Z}$ be the quotient map. Given $x \in \mathbb{Q}$, note that $x \in \kappa^{-1}M_n$ if and only if $p^n x \in \mathbb{Z}$. Define $\alpha\colon \mathbb{Z} \to \mathbb{Q}$ by $\alpha(m) := m/p^n$. Then $\alpha(\mathbb{Z}) = \kappa^{-1}M_n$. So $\kappa\alpha\colon \mathbb{Z} \to M_n$ is surjective. But $(\kappa\alpha)^{-1}0 = \kappa^{-1}\mathbb{Z} = \langle p^n \rangle$. Thus $\kappa\alpha$ induces the desired isomorphism $\mathbb{Z}/\langle p^n \rangle \xrightarrow{\sim} M_n$.

Given $q \in N$, write $q = \kappa(n/p^e)$ where n is relatively prime to p. Then there's

$m \in \mathbb{Z}$ with $nm \equiv 1 \pmod{p^e}$. So $N \ni m\kappa(n/p^e) = \kappa(1/p^e)$. Hence $N \supset M_e$. Since $N \neq M$, there's a largest such e; denote it by n. Thus $N = M_n$.

Let $M \supsetneq N_1 \supset N_2 \supset \cdots$ be a descending chain of submodules. Then $N_i = M_{n_i}$ for some n_i. Moreover, the sequence $n_1 \geq n_2 \geq \cdots$ stabilizes; say $n_i = n_{i+1} = \cdots$. So $N_i = N_{i+1} = \cdots$. Thus M is Artinian.

The ascending chain $M_0 \subset M_1 \subset \cdots$ doesn't stabilize, Thus M isn't Noetherian.

Given $m \in \operatorname{Ann}(M)$, note $m/p^n \in \mathbb{Z}$ for all n. So $m = 0$. Thus $\operatorname{Ann}(M) = 0$.

So $\mathbb{Z}/\operatorname{Ann}(M) = \mathbb{Z}$. But the descending chain $\mathbb{Z} \supset \langle p \rangle \supset \langle p^2 \rangle \supset \cdots$ doesn't stabilize. Thus $\mathbb{Z}$ isn't Artinian. □

Exercise (16.45) . — Let R be an Artinian ring. Prove that R is a field if it is a domain. Deduce that in general every prime ideal $\mathfrak{p}$ of R is maximal.

Solution: Take any nonzero element $x \in R$, and consider the chain of ideals $\langle x \rangle \supset \langle x^2 \rangle \supset \cdots$. Since R is Artinian, the chain stabilizes; so $\langle x^e \rangle = \langle x^{e+1} \rangle$ for some e. Hence $x^e = ax^{e+1}$ for some $a \in R$. If R is a domain, then we can cancel to get $1 = ax$; thus R is then a field.

In general, $R/\mathfrak{p}$ is Artinian by **(16.22)**(2). Now, $R/\mathfrak{p}$ is also a domain by **(2.8)**. Hence, by what we just proved, $R/\mathfrak{p}$ is a field. Thus $\mathfrak{p}$ is maximal by **(2.13)**. □

Exercise (16.46) . — Let R be a ring, M an Artinian module, $\alpha\colon M \to M$ an endomorphism. Assume α is injective. Show that α is an isomorphism.

Solution: Consider the chain $M \supset \alpha(M) \supset \cdots \supset \alpha^n(M) \supset \cdots$. It stabilizes: say $\alpha^n(M) = \alpha^{n+1}(M)$. So given $m \in M$, there is $m' \in M$ with $\alpha^{n+1}(m') = \alpha^n(m)$. But α is injective. So $\alpha(m') = m$. Thus α is surjective, so an isomorphism. □

Exercise (16.47) . — Let R be a ring; M a module; N_1, N_2 submodules. If the M/N_i are Noetherian, show $M/(N_1 \cap N_2)$ is too. What if the M/N_i are Artinian?

Solution: The canonical map $M/(N_1 \cap N_2) \to M/N_1 \oplus M/N_2$ is injective. If the M/N_i are Noetherian, so is its target by **(16.14)**; whence, by **(16.13)**(2), its source is Noetherian too.

Similarly, if the M/N_i are Artinian, so is $M/(N_1 \cap N_2)$ by **(16.22)**(3), (2). □

16. Appendix: Noetherian Spaces

Exercise (16.51) . — Let R be a ring. Prove the following statements:

(1) $\mathbf{V}\colon \mathfrak{a} \mapsto \mathbf{V}(\mathfrak{a}) = \operatorname{Spec}(R/\mathfrak{a})$ is an inclusion-reversing bijection from the radical ideals $\mathfrak{a}$ of R onto the closed subspaces of $\operatorname{Spec}(R)$.

(2) $\mathbf{V}$ gives a bijection from the primes onto the irreducible closed subspaces.

(3) $\mathbf{V}$ gives a bijection from the minimal primes onto the irreducible components.

Solution: Assertion (1) follows immediately from the first part of **(13.1)**.

For (2), note that $\operatorname{Spec}(R/\mathfrak{a})$ is irreducible if and only if $\operatorname{nil}(R/\mathfrak{a})$ is prime by **(16.49)**. Plainly, $\operatorname{nil}(R/\mathfrak{a})$ is prime if and only if $\mathfrak{a}$ is. Thus (2) holds.

Finally, (2) implies (3), as the irreducible components are closed by **(16.50)**(5), so are just the maximal irreducible closed subspaces, but $\mathbf{V}$ is lattice-inverting. □

Exercise (16.56) . — Let R be a ring. Prove the following statements:

(1) $\operatorname{Spec}(R)$ is Noetherian if and only if the radical ideals satisfy the acc.

(2) If $\operatorname{Spec}(R)$ is Noetherian, then the primes satisfy the acc.

(3) If R is Noetherian, then $\mathrm{Spec}(R)$ is too.

Solution: For (1), note that, owing to **(16.51)**(1), the radical ideals satisfy the acc if and only if the closed sets satisfy the dcc, that is, $\mathrm{Spec}(R)$ is Noetherian. Thus (1) holds. Plainly, (1) immediately implies (2) and (3). □

Exercise (16.61) . — Let X be a topological space, Y and Z constructible subsets, $\varphi\colon X' \to X$ a continuous map, $A \subset Z$ an arbitrary subset. Prove the following:

(1) Open and closed sets are constructible.
(2) $Y \cup Z$ and $Y \cap Z$ are constructible.
(3) $\varphi^{-1}Y$ is constructible in X'.
(4) A is constructible in Z if and only if A is constructible in X.

Solution: For (1), given an open set U and a closed set C, note $U = U \cap X$ and $C = X \cap C$. But X is both closed and open. Thus (1) holds.

For (2), say $Y = \bigcup(U_i \cap C_i)$ and $Z = \bigcup(V_j \cap D_j)$ with U_i open and C_i closed. Plainly $Y \cup Z$ is constructible. And $Y \cap Z = \bigcup_{i,\,j}(U_i \cap C_i) \cap (V_j \cap D_j)$. But $U_i \cap V_i$ is open, and $C_i \cap D_j$ is closed. Thus $Y \cap Z$ is constructible. Thus (2) holds.

For (3), say $Y = \bigcup(U_i \cap C_i)$ with U_i open in X and C_i closed in X. Then $\varphi^{-1}Y = \bigcup(\varphi^{-1}U_i \cap \varphi^{-1}C_i)$. But $\varphi^{-1}U_i$ is open in X', and $\varphi^{-1}V_i$ is closed in X'. Thus (3) holds.

For (4), first assume A is constructible in Z. Say $A = \bigcup(W_i \cap E_i)$ with W_i open in Z and E_i closed in Z. Say $W_i = U_i \cap Z$ and $E_i = C_i \cap Z$ with U_i open in X and C_i closed in X. Set $B := \bigcup(U_i \cap C_i)$. Then B is constructible in X, and $A = B \cap Z$. So A is constructible in X by (2).

Conversely, assume A is constructible in X. Let $\varphi\colon Z \to X$ be the inclusion. Then $\varphi^{-1}A = A$. So A is constructible in Z by (3). Thus (4) holds. □

Exercise (16.67) . — Find a non-Noetherian ring R with $R_{\mathfrak p}$ Noetherian for every prime $\mathfrak p$.

Solution: Take R to be any non-Noetherian, absolutely flat ring, such as $\mathbb{F}_2^{\mathbb N}$; see **(16.57)**. By **(13.61)**, every $R_{\mathfrak p}$ is a field, so Noetherian. □

Exercise (16.68) . — Describe $\mathrm{Spec}(\mathbb{Z}[X])$.

Solution: The points of $\mathrm{Spec}(\mathbb{Z}[X])$ represent the prime ideals $\mathfrak p$ of $\mathbb{Z}[X]$. By **(2.20)** and **(2.40)**, the $\mathfrak p$ are of three distict types: either $\mathfrak p = \langle 0\rangle$; or $\mathfrak p = \langle F\rangle$ with $F \in \mathbb{Z}[X]$ prime; or $\mathfrak p$ is maximal and not principal.

As to the topology, note $\mathbb{Z}[X]$ is Noetherian by **(16.1)** and **(16.9)**. Now, for any Noetherian ring R, the space $\mathrm{Spec}(R)$ is Noetherian by **(16.56)**(3). So every subspace is also Noetherian by **(16.53)**. Hence, by **(16.54)**, the closed sets V are the finite unions of irreducible closed subsets W of V. But plainly, these W are the irreducible closed subsets of $\mathrm{Spec}(R)$ that lie in V. Thus by **(16.51)**(2), the closed sets V of $\mathrm{Spec}(R)$ are the finite unions of the sets $\mathbf{V}(\mathfrak p)$ with $\mathfrak p \subset R$ prime.

Fix a prime $\mathfrak p \subset \mathbb{Z}[X]$. If $\mathfrak p = \langle 0\rangle$, then $\mathbf{V}(\mathfrak p) = \mathrm{Spec}(\mathbb{Z}[X])$. Suppose $\mathfrak p = \langle F\rangle$ with F prime. Let $\varphi\colon \mathbb{Z} \to \mathbb{Z}[X]$ be the inclusion, and set $\varphi^* := \mathrm{Spec}(\varphi)$. If F is a prime p of $\mathbb{Z}$, then $\mathbf{V}(\mathfrak p)$ is the fiber of φ^* over the point of $\mathrm{Spec}(\mathbb{Z})$ representing $\langle p\rangle$, as $\mathfrak p \cap \mathbb{Z} = \langle p\rangle$. Otherwise, given a prime $p \in \mathbb{Z}$, the corresponding fiber of φ^* is $\mathbf{V}(\langle p\rangle)$, and it intersects $\mathbf{V}(\mathfrak p)$ in $\mathbf{V}(\langle p, F\rangle)$ by **(13.1.1)**. Plainly, the points of this intersection, which represent the maximal ideals containing $\langle p, F\rangle$, correspond bijectively to the prime factors of the image of F in $(\mathbb{Z}/p\mathbb{Z})[X]$.

Finally, suppose $\mathfrak{p}$ is maximal and not principal. Then $\mathfrak{p} = \langle p, G\rangle$ with $p \in \mathbb{Z}$ prime and $G \in P$ prime by **(2.20)**(2). Hence, by the preceding case, $\mathbf{V}(\mathfrak{p})$ is the intersection of $\mathbf{V}(G)$ with the fiber of φ^* over the point representing $\langle p\rangle$. □

Exercise (16.69) . — What are the irreducible components of a Hausdorff space?

Solution: In a Hausdorff space, any pair of distinct points have disjoint open neighborhoods. Thus every irreducible subspace consists of a single point. □

Exercise (16.70) . — Are these conditions on a topological space X equivalent?

(1) X is Noetherian.
(2) Every subspace Y is quasi-compact.
(3) Every open subspace V is quasi-compact.

Solution: Yes, they're equivalent; here's why. If (1) holds, **(16.53)** implies Y is Noetherian, and so quasi-compact; thus (2) holds. Trivially (2) implies (3).

Assume (3). Let $U_0 \subset U_1 \subset \cdots$ be an ascending chain of open subsets of X. Set $V := \bigcup U_n$. Then V is open, so quasi-compact by (3). But the U_n form an open covering of V. So finitely many cover. Hence $U_m = V$ for some m. So $U_0 \subset U_1 \subset \cdots$ stabilizes. Thus (1) holds. □

Exercise (16.71) . — Let $\varphi\colon R \to R'$ a map of rings. Assume R' is algebra finite over R. Show that the fibers of $\operatorname{Spec}(\varphi)$ are Noetherian subspaces of $\operatorname{Spec}(R')$.

Solution: Given $\mathfrak{p} \in \operatorname{Spec}(R)$, set $k := \operatorname{Frac}(R/\mathfrak{p})$. Then the fiber over $\mathfrak{p}$ is equal to $\operatorname{Spec}(R' \otimes_R k)$ by **(13.28)**(1). Since R'/R is algebra finite, $R' \otimes k$ is algebra finite over k by **(10.39)**(3). Hence $R' \otimes k$ is Noetherian by **(16.10)**. So $\operatorname{Spec}(R' \otimes k)$ is Noetherian by **(16.56)**(3). □

Exercise (16.72) . — Let M be a Noetherian module over a ring R. Show that $\operatorname{Supp}(M)$ is a closed Noetherian subspace of $\operatorname{Spec}(R)$.

Solution: Since M is finitely generated, $\operatorname{Supp}(M) = \mathbf{V}(\operatorname{Ann}(M))$ by **(13.4)**(3). Thus $\operatorname{Supp}(M)$ is, by **(13.1)**, a closed subspace of $\operatorname{Spec}(R)$.

Set $R' := R/\operatorname{Ann}(M)$. Then $\mathbf{V}(\operatorname{Ann}(M)) = \operatorname{Spec}(R')$ by **(13.1.7)**. But R' is Noetherian by **(16.16)**. So $\operatorname{Spec}(R')$ is by **(16.56)**(3). Thus $\operatorname{Supp}(M)$ is. □

Exercise (16.73) . — Let X be a Noetherian topological space. Then a subset U is open if and only if this condition holds: given a closed irreducible subset Z of X, either $U \cap Z$ is empty or it contains a nonempty subset that's open in Z.

Solution: Assume U is open. Given a closed irreducible subset Z of X, note $U \cap Z$ is open in Z, whether empty or not. Thus the condition holds.

Conversely, assume the condition holds. Use Noetherian induction: form the set $\mathcal{S}$ of closed subsets C of X with $U \cap C$ not open in C. Assume $\mathcal{S} \neq \emptyset$. As X is Noetherian, an adaptation of **(16.4)** yields a minimal element $Z \in \mathcal{S}$.

Note that $Z \neq \emptyset$ as $U \cap Z$ is not open.

Suppose $Z = Z_1 \cup Z_2$ with each Z_i closed and $Z_i \subsetneqq Z$. By minimality, $Z_i \notin \mathcal{S}$. So $U \cap Z_i$ is open in Z_i. So $Z_i - (U \cap Z_i)$ is closed in Z_i, so closed in X.

Set $A := Z - (U \cap Z)$. Then $A \cap Z_i = Z_i - (U \cap Z_i)$. So $A \cap Z_i$ is closed. But $A = (A \cap Z_1) \cup (A \cap Z_2)$. So A is closed. But $U \cap Z = Z - A$. So $U \cap Z$ is open in Z, a contradiction. Thus Z is irreducible.

Assume $U \cap Z$ isn't empty. By the condition, $U \cap Z$ contains a nonempty set V

that's open in Z. Set $B := Z - V$. Then B is closed in Z, so closed in X. Also $B \subsetneqq Z$. So $B \notin \mathcal{S}$. So $U \cap B$ is open in B.

Set $C := Z - (U \cap Z)$. Then $C \cap B = B - (U \cap B)$ as $B \subset Z$. But $C \cap B = C$ as $U \cap Z \supset V$. Hence C is closed in B, so closed in X. But $U \cap Z = Z - C$. So $U \cap Z$ is open in Z, a contradiction. Thus $\mathcal{S} = \emptyset$. Thus U is open in X, as desired. □

Exercise (16.74) . — Let $\varphi\colon R \to R'$ a map of rings. Assume R is Noetherian and R' is algebra finite over R. Set $X := \operatorname{Spec}(R)$, set $X' := \operatorname{Spec}(R')$, and set $\varphi^* := \operatorname{Spec}(\varphi)$. Prove that φ^* is open if and only if φ has the Going-down Property.

Solution: If φ^* is an open mapping, then φ has the Going-down Property by **(13.38)**, whether or not R is Noetherian and R' is algebra finite over R.

Conversely, assume φ has the Going-down Property. Given an open subset U' of X', set $U := \varphi^* U' \subset X$. We have to see that U is open.

Since R is Noetherian, X is too by **(16.56)**(3). So let's use **(16.73)**: given a closed irreducible subset Z of X with $U \cap Z$ nonempty, we have to see that $U \cap Z$ contains a nonempty subset that's open in Z.

Since R is Noetherian and R' is algebra finite, U is constructible by **(16.66)**. But $U \cap Z \neq \emptyset$. So owing to **(16.64)**, we just have to see that $U \cap Z$ is dense in Z.

Say $\mathfrak{p} \in U \cap Z$ and $\mathfrak{p} = \varphi^{-1}\mathfrak{p}'$ with $\mathfrak{p}' \in U'$. By **(16.51)**(2), $Z = \mathbf{V}(\mathfrak{q})$ for some prime $\mathfrak{q}$ of R. Then $\mathfrak{q} \subset \mathfrak{p}$. But φ has the Going-down Property. So there's a prime $\mathfrak{q}' \subset \mathfrak{p}'$ with $\varphi^{-1}\mathfrak{q}' = \mathfrak{q}$. But U' is open. So $\mathfrak{q}' \in U'$ by **(13.16)**(1). Thus $\mathfrak{q} \in U$.

Finally, given any open set V of X with $V \cap Z \neq \emptyset$, say $\mathfrak{r} \in V \cap Z$. Then $\mathfrak{q} \subset \mathfrak{r}$. So $\mathfrak{q} \in V$ by **(13.16)**(1). So $V \cap U \neq \emptyset$. Thus $U \cap Z$ is dense in Z, as desired. □

Exercise (16.75) . — Let $\varphi\colon R \to R'$ a map of rings, M' a finitely generated R'-module. Assume R is Noetherian, R' is algebra finite, and M' is flat over R. Show $\operatorname{Spec}(\varphi)$ is open.

Solution: Set $\mathfrak{a}' := \operatorname{Ann}(M')$. Then $\operatorname{Supp}(M') = \mathbf{V}(\mathfrak{a}')$ by **(13.4)**(3) as M' is finitely generated. Also $\mathbf{V}(\mathfrak{a}') = \operatorname{Spec}(R'/\mathfrak{a}')$ by **(13.1.7)**. Let $\kappa\colon R' \to R'/\mathfrak{a}'$ be the quotient map, and set $\psi := \kappa\varphi$. Then ψ has the Going-down Property by **(14.8)**. Thus by **(16.74)**, $\operatorname{Spec}(\psi)$ is open.

Given an open set $U \subset \operatorname{Spec}(R')$, set $U' := U \cap \mathbf{V}(\mathfrak{a}')$. Then $\operatorname{Spec}(\psi)(U')$ is open in $\operatorname{Spec}(R)$. But $\operatorname{Spec}(\psi)(U') = \operatorname{Spec}(\varphi)(U)$. Thus $\operatorname{Spec}(\varphi)$ is open. □

17. Associated Primes

Exercise (17.4) . — Let R be a ring, M a module, $\mathfrak{a} \subset \operatorname{Ann}(M)$ an ideal. Set $R' := R/\mathfrak{a}$. Let $\kappa\colon R \twoheadrightarrow R'$ be the quotient map. Show that $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{a}$ is a bijection from $\operatorname{Ass}_R(M)$ to $\operatorname{Ass}_{R'}(M)$ with inverse $\mathfrak{p}' \mapsto \kappa^{-1}(\mathfrak{p}')$.

Solution: Given $\mathfrak{p} \in \operatorname{Ass}_R(M)$, say $\mathfrak{p} = \operatorname{Ann}_R(m)$. Then $\mathfrak{p} \supset \mathfrak{a}$. Set $\mathfrak{p}' := \mathfrak{p}/\mathfrak{a}$. Then $\mathfrak{p}' \subset R'$ is prime, and $\mathfrak{p}' = \operatorname{Ann}_{R'}(m)$. Thus $\mathfrak{p}' \in \operatorname{Ass}_{R'}(M)$; also $\kappa^{-1}\mathfrak{p}' = \mathfrak{p}$.

Conversely, given $\mathfrak{p}' \in \operatorname{Ass}_{R'}(M)$, say $\mathfrak{p}' = \operatorname{Ann}_{R'}(m)$. Set $\mathfrak{p} := \kappa^{-1}\mathfrak{p}'$. Then $\mathfrak{p} \subset R$ is prime, and $\mathfrak{p} = \operatorname{Ann}_R(m)$. Thus $\mathfrak{p} \in \operatorname{Ass}_R(M)$; also $\mathfrak{p}/\mathfrak{a} = \mathfrak{p}'$. □

Exercise (17.21) . — Given modules $M_1, \ldots, M_r$, set $M := M_1 \oplus \cdots \oplus M_r$. Prove

$$\operatorname{Ass}(M) = \operatorname{Ass}(M_1) \cup \cdots \cup \operatorname{Ass}(M_r).$$

Solution: Set $N := M_2 \oplus \cdots \oplus M_r$. Then $N,\, M_1 \subset M$. Also, $M/N = M_1$. So (**17.6**) yields

$$\mathrm{Ass}(N),\, \mathrm{Ass}(M_1) \subset \mathrm{Ass}(M) \subset \mathrm{Ass}(N) \cup \mathrm{Ass}(M_1).$$

So $\mathrm{Ass}(M) = \mathrm{Ass}(N) \cup \mathrm{Ass}(M_1)$. The assertion follows by induction on r. □

Exercise (17.22) . — Let R be a ring, M a module, M_λ for $\lambda \in \Lambda$ submodules. Assume $M = \bigcup M_\lambda$. Show $\mathrm{Ass}(M) = \bigcup \mathrm{Ass}(M_\lambda)$.

Solution: Note $\mathrm{Ass}(M_\lambda) \subset \mathrm{Ass}(M)$ by (**17.6**). Thus $\mathrm{Ass}(M) \supset \bigcup \mathrm{Ass}(M_\lambda)$.

Conversely, given $\mathfrak{p} \in \mathrm{Ass}(M)$, say $\mathfrak{p} = \mathrm{Ann}(m)$ for $m \in M$. Say $m \in M_\lambda$. Note $\mathrm{Ann}_{M_\lambda}(m) = \mathrm{Ann}_M(m)$. So $\mathfrak{p} \in \mathrm{Ass}(M_\lambda)$. Thus $\mathrm{Ass}(M) \subset \bigcup \mathrm{Ass}(M_\lambda)$. □

Exercise (17.23) . — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}/\langle 2\rangle \oplus \mathbb{Z}$. Find $\mathrm{Ass}(M)$ and find two submodules $L,\, N \subset M$ with $L + N = M$ but $\mathrm{Ass}(L) \cup \mathrm{Ass}(N) \subsetneqq \mathrm{Ass}(M)$.

Solution: First, we have $\mathrm{Ass}(M) = \{\langle 0\rangle,\, \langle 2\rangle\}$ by (**17.21**) and (**17.5**)(2). Next, take $L := R \cdot (1,1)$ and $N := R \cdot (0,1)$. Then the canonical maps $R \to L$ and $R \to N$ are isomorphisms. Hence both $\mathrm{Ass}(L)$ and $\mathrm{Ass}(N)$ are $\{\langle 0\rangle\}$ by (**17.5**)(2). Finally, $L + N = M$ because $(a,b) = a \cdot (1,1) + (b-a) \cdot (0,1)$. □

Exercise (17.24) . — If a prime $\mathfrak{p}$ is sandwiched between two primes in $\mathrm{Ass}(M)$, is $\mathfrak{p}$ necessarily in $\mathrm{Ass}(M)$ too?

Solution: No, for example, let $R := k[X,Y]$ be the polynomial ring over a field. Set $M := R \oplus (R/\langle X,Y\rangle)$ and $\mathfrak{p} := \langle X\rangle$. Then $\mathrm{Ass}(M) = \mathrm{Ass}(R) \cup \mathrm{Ass}(R/\langle X,Y\rangle)$ by (**17.21**). Further, $\mathrm{Ass}(R) = \langle 0\rangle$ and $\mathrm{Ass}(R/\langle X,Y\rangle) = \langle X,Y\rangle$ by (**17.5**)(2). □

Exercise (17.25) . — Let R be a ring, S a multiplicative subset, M a module, N a submodule. Prove $\mathrm{Ass}(M/N^S) \supset \{\mathfrak{p} \in \mathrm{Ass}(M/N) \mid \mathfrak{p} \cap S = \emptyset\}$, with equality if either R is Noetherian or M/N is Noetherian.

Solution: First, given $\mathfrak{p} \in \mathrm{Ass}(M/N)$ with $\mathfrak{p} \cap S = \emptyset$, say $\mathfrak{p} = \mathrm{Ann}(m)$ with $m \in M/N$. Let $m' \in M/N^S$ be its residue. Then $m' \neq 0$; else, there's $s \in S$ with $sm = 0$, so $s \in \mathfrak{p}$, a contradiction. Finally, $\mathfrak{p}m = 0$, so $\mathfrak{p}m' = 0$; thus $\mathfrak{p} \subset \mathrm{Ann}(m')$.

Conversely, given $x \in \mathrm{Ann}(m')$, note $xm \in N^S/N$. So there's $s \in S$ with $sxm = 0$. So $sx \in \mathfrak{p}$. But $s \notin \mathfrak{p}$. So $x \in \mathfrak{p}$. Thus $\mathfrak{p} \supset \mathrm{Ann}(m')$. Thus $\mathfrak{p} = \mathrm{Ann}(m')$. Thus $\mathfrak{p} \in \mathrm{Ass}(M/N^S)$.

Second, given $\mathfrak{p} \in \mathrm{Ass}(M/N^S)$, say $\mathfrak{p} = \mathrm{Ann}(m')$ with $m' \in M/N^S$. Lift m' to $m \in M/N$. Let's show there's no $s \in \mathfrak{p} \cap S$. Else, $sm \in N^S/N$. So there's $t \in S$ with $tsm = 0$. So $m \in N^S/N$. So $m' = 0$, a contradiction. Thus $\mathfrak{p} \cap S = \emptyset$.

It remains to show $\mathfrak{p} \in \mathrm{Ass}(M/N)$ if R is Noetherian or M/N is. Either way, $R/\mathrm{Ann}(M/N)$ is Noetherian by (**16.7**) or by (**16.16**). So there are finitely many $x_i \in \mathfrak{p}$ that generate modulo $\mathrm{Ann}(M/N)$. Then $x_i m \in N^S/N$. So there's $s_i \in S$ with $s_i x_i m = 0$. Set $s := \prod s_i \in S$. Then $x_i(sm) = 0$. Given $x \in \mathfrak{p}$, say $x = a + \sum a_i x_i$ with $a \in \mathrm{Ann}(M/N)$ and $a_i \in R$. Then $a,\, x_i \in \mathrm{Ann}(sm)$. So $x \in \mathrm{Ann}(sm)$. Thus $\mathfrak{p} \subset \mathrm{Ann}(sm)$.

Conversely, given $x \in \mathrm{Ann}(sm)$, note $xsm' = 0$. So $xs \in \mathfrak{p}$. But $s \notin \mathfrak{p}$. So $x \in \mathfrak{p}$. Thus $\mathfrak{p} \supset \mathrm{Ann}(sm)$. Thus $\mathfrak{p} = \mathrm{Ann}(sm)$. Thus $\mathfrak{p} \in \mathrm{Ass}(M/N)$, as desired. □

Exercise (17.26) . — Let R be a ring, and suppose $R_\mathfrak{p}$ is a domain for every prime $\mathfrak{p}$. Prove every associated prime of R is minimal.

Solution: Let $\mathfrak{p} \in \mathrm{Ass}(R)$. Then $\mathfrak{p}R_{\mathfrak{p}} \in \mathrm{Ass}(R_{\mathfrak{p}})$ by **(17.8)**. But $R_{\mathfrak{p}}$ is a domain. So $\mathfrak{p}R_{\mathfrak{p}} = \langle 0 \rangle$ by **(17.5)**(2). Thus $\mathfrak{p}$ is a minimal prime of R by **(11.12)**(2).

Alternatively, say $\mathfrak{p} = \mathrm{Ann}(x)$ with $x \in R$. Then $x/1 \neq 0$ in $R_{\mathfrak{p}}$; otherwise, there would be some $s \in S_{\mathfrak{p}} := R - \mathfrak{p}$ with $sx = 0$, contradicting $\mathfrak{p} = \mathrm{Ann}(x)$. However, for any $y \in \mathfrak{p}$, we have $xy/1 = 0$ in $R_{\mathfrak{p}}$. Since $R_{\mathfrak{p}}$ is a domain and since $x/1 \neq 0$, we must have $y/1 = 0$ in $R_{\mathfrak{p}}$. So there exists some $t \in S_{\mathfrak{p}}$ such that $ty = 0$. But, $\mathfrak{p} \supset \mathfrak{q}$ for some minimal prime $\mathfrak{q}$ by **(3.16)**. Suppose $\mathfrak{p} \neq \mathfrak{q}$. Then there is some $y \in \mathfrak{p} - \mathfrak{q}$. So there exists some $t \in R - \mathfrak{p}$ with $ty = 0 \in \mathfrak{q}$, contradicting the primeness of $\mathfrak{q}$. Thus $\mathfrak{p} = \mathfrak{q}$; that is, $\mathfrak{p}$ is minimal. □

Exercise (17.27) . — Let R be a ring, M a module, N a submodule, $x \in R$. Assume that R is Noetherian or M/N is and that $x \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}(M/N)$. Show $xM \cap N = xN$.

Solution: Trivially, $xN \subset xM \bigcap N$. Conversely, take $m \in M$ with $xm \in N$. Let m' be the residue of m in M/N. Then $xm' = 0$. By **(17.12)**, $x \notin \mathrm{z.div}(M/N)$. So $m' = 0$. So $m \in N$. So $xm \in xN$. Thus $xM \bigcap N \subset xN$, as desired. □

Exercise (17.28) . — Let R be a ring, M a module, $\mathfrak{p}$ a prime. Show (1)–(3) are equivalent if R is Noetherian, and (1)–(4) are equivalent if M is Noetherian:

(1) $\mathfrak{p}$ is a minimal prime of M. (2) $\mathfrak{p}$ is minimal in $\mathrm{Supp}(M)$.
(3) $\mathfrak{p}$ is minimal in $\mathrm{Ass}(M)$. (4) $\mathfrak{p}$ is a minimal prime of $\mathrm{Ann}(M)$.

Solution: First off, (1) and (2) are equivalent by definition, **(13.5)**, which has no Noetherian hypotheses.

Assume (2). Then under either Noetherian hypothesis, $\mathfrak{p} \in \mathrm{Ass}(M)$ by **(17.14)**. Say $\mathfrak{p} \supset \mathfrak{q}$ with $\mathfrak{q} \in \mathrm{Ass}(M)$. Then $\mathfrak{q} \in \mathrm{Supp}(M)$ by **(17.13)**, which has no Noetherian hypothesis. So $\mathfrak{p} = \mathfrak{q}$ by (2). Thus under either hypothesis, (3) holds.

Assume (3). Then $\mathfrak{p} \in \mathrm{Supp}(M)$ by **(17.13)** with no Noetherian hypotheses. Say $\mathfrak{p} \supset \mathfrak{p}'$ with $\mathfrak{p}' \in \mathrm{Supp}(M)$. Then under either Noetherian hypothesis, $\mathfrak{p}' \supset \mathfrak{q}$ with $\mathfrak{q} \in \mathrm{Ass}(M)$ by **(17.14)**. So $\mathfrak{p} = \mathfrak{p}' = \mathfrak{q}$ by (3). Thus under either Noetherian hypothesis, (2) holds.

Finally, if M is finitely generated, then (1) and (4) are equivalent by **(13.5)**. Thus, if M is Noetherian, then (1)–(4) are equivalent. □

Exercise (17.29) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $R/\mathfrak{a}$ is Noetherian. Show the minimal primes of $\mathfrak{a}$ are associated to $\mathfrak{a}$, and they are finite in number.

Solution: Set $M := R/\mathfrak{a}$. Then $\mathfrak{a} = \mathrm{Ann}(M)$. Thus the minimal primes of $\mathfrak{a}$ are associated to $\mathfrak{a}$ by **(17.28)**, and they are finite in number by **(17.17)**. □

Exercise (17.30) . — Let M a Noetherian module. Show that $\mathrm{Supp}(M)$ has only finitely many irreducible components Y.

Solution: By **(16.51)**(3), these Y are the $\mathbf{V}(\mathfrak{p})$ where $\mathfrak{p}$ is a minimal prime of $\mathrm{Ann}(M)$. So they're finite in number by **(17.29)**. □

Exercise (17.31) . — Take $R := \mathbb{Z}$ and $M := \mathbb{Z}$ in **(17.16)**. Determine when a chain $0 \subset M_1 \subsetneqq M$ is **acceptable** — that is, it's like the chain in **(17.16)** — and show that then $\mathfrak{p}_2 \notin \mathrm{Ass}(M)$.

Solution: If the chain is acceptable, then $M_1 \neq 0$ as $M_1/0 \simeq R/\mathfrak{p}_1$, and M_1 is a prime ideal as $M_1 = \mathrm{Ann}(M/M_1) = \mathfrak{p}_2$. Conversely, the chain is acceptable if M_1 is a nonzero prime ideal $\mathfrak{p}$, as then $M_1/0 \simeq R/0$ and $M/M_1 \simeq R/\mathfrak{p}$.

Finally, $\mathrm{Ass}(M) = 0$ by **(17.5)**(2). Further, as just observed, given any acceptable chain, $\mathfrak{p}_2 = M_1 \neq 0$. Thus $\mathfrak{p}_2 \notin \mathrm{Ass}(M)$. □

Exercise (17.32) . — Take $R := \mathbb{Z}$ and $M := Z/\langle 12\rangle$ in **(17.16)**. Find all three acceptable chains, and show that, in each case, $\{\mathfrak{p}_i\} = \mathrm{Ass}(M)$.

Solution: An acceptable chain in M corresponds to a chain

$$\langle 12\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle = \mathbb{Z}.$$

Here $\langle a_1\rangle/\langle 12\rangle \simeq \mathbb{Z}/\langle p_1\rangle$ with p_1 prime. So $a_1p_1 = 12$. Hence the possibilities are $p_1 = 2$, $a_1 = 6$ and $p_1 = 3$, $a_1 = 4$. Further, $\langle a_2\rangle/\langle a_1\rangle \simeq \mathbb{Z}/\langle p_2\rangle$ with p_2 prime. So $a_2p_2 = a_1$. Hence, if $a_1 = 6$, then the possibilities are $p_2 = 2$, $a_2 = 3$ and $p_2 = 3$, $a_2 = 2$; if $a_1 = 4$, then the only possibility is $p_2 = 2$ and $a_2 = 2$. In each case, a_2 is prime; hence, $n = 3$, and these three chains are the only possibilities. Conversely, each of these three possibilities, clearly, does arise.

In each case, $\{\mathfrak{p}_i\} = \{\langle 2\rangle, \langle 3\rangle\}$. Hence **(17.16.1)** yields $\mathrm{Ass}(M) \subset \{\langle 2\rangle, \langle 3\rangle\}$. For any M, if $0 \subset M_1 \subset \cdots \subset M$ is an acceptable chain, then **(17.6)** and **(17.5)**(2) yield $\mathrm{Ass}(M) \supset \mathrm{Ass}(M_1) = \{\mathfrak{p}_1\}$. Here, there's one chain with $\mathfrak{p}_1 = \langle 2\rangle$ and another with $\mathfrak{p}_1 = \langle 3\rangle$; hence, $\mathrm{Ass}(M) \supset \{\langle 2\rangle, \langle 3\rangle\}$. Thus $\mathrm{Ass}(M) = \{\langle 2\rangle, \langle 3\rangle\}$. □

Exercise (17.33) . — Let R be a ring, M a nonzero Noetherian module, $x, y \in R$ and $a \in \mathrm{rad}(M)$. Assume $a^r + x \in \mathrm{z.div}(M)$ for all $r \geq 1$. Show $a + xy \in \mathrm{z.div}(M)$.

Solution: Recall $\mathrm{z.div}(M) = \bigcup_{\mathfrak{p}\in\mathrm{Ass}(M)} \mathfrak{p}$ by **(17.12)**, and $\mathrm{Ass}(M)$ is finite by **(17.17)**. So the Pigeonhole Principle yields $r > s > 0$ and $\mathfrak{p} \in \mathrm{Ass}(M)$ with $a^r + x,\ a^s + x \in \mathfrak{p}$. Say $\mathfrak{p} = \mathrm{Ann}(m)$. Then $(a^{r-s} - 1)a^s m = 0$. So $a^s m = 0$ by **(4.15)**. So $a^s \in \mathfrak{p}$. Hence $a,\ x \in \mathfrak{p}$. Thus $a + xy \in \mathfrak{p} \subset \mathrm{z.div}(M)$. □

Exercise (17.34) (*Grothendieck Group* $K_0(R)$) . — Let R be a ring, $\mathcal{C}$ a subcategory of $((R\text{-mod}))$ such that the isomorphism classes of its objects form a set Λ. Let C be the free Abelian group $\mathbb{Z}^{\oplus\Lambda}$. Given M in $\mathcal{C}$, let $(M) \in \Lambda$ be its class. To each short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ in $\mathcal{C}$, associate the element $(M_2) - (M_1) - (M_3)$ of C. Let $D \subset C$ be the subgroup generated by all these elements. Set $K(\mathcal{C}) := C/D$, and let $\gamma_{\mathcal{C}}\colon C \to K(\mathcal{C})$ be the quotient map.

In particular, let $\mathcal{N}$ be the subcategory of all Noetherian modules and all linear maps between them; set $K_0(R) := K(\mathcal{N})$ and $\gamma_0 := \gamma_{\mathcal{N}}$. Show:

(1) Then $K(\mathcal{C})$ has this UMP: for each Abelian group G and function $\lambda\colon \Lambda \to G$ with $\lambda(M_2) = \lambda(M_1) + \lambda(M_3)$ for all exact sequences as above, there's an induced $\mathbb{Z}$-map $\lambda_0\colon K(\mathcal{C}) \to G$ with $\lambda(M) = \lambda_0(\gamma_{\mathcal{C}}(M))$ for all $M \in \mathcal{C}$.
(2) Then $K_0(R)$ is generated by the various elements $\gamma_0(R/\mathfrak{p})$ with $\mathfrak{p}$ prime.
(3) Assume R is a Noetherian domain. Find a surjective $\mathbb{Z}$-map $\kappa : K_0(R) \twoheadrightarrow \mathbb{Z}$.
(4) Assume R is a field or a PID. Then $K_0(R) = \mathbb{Z}$.
(5) Assume R is Noetherian. Let $\varphi\colon R \to R'$ and $\psi\colon R' \to R''$ be module-finite maps of rings. Then (a) restriction of scalars gives rise to a $\mathbb{Z}$-map $\varphi_!\colon K_0(R') \to K_0(R)$, and (b) we have $(\psi\varphi)_! = \varphi_!\psi_!$.

Solution: In (1), λ induces a $\mathbb{Z}$-map $\lambda'\colon C \to G$ by **(4.10)**. But by hypothesis, $\lambda(M_2) = \lambda(M_1) + \lambda(M_3)$; so $D \subset \mathrm{Ker}(\lambda')$. Thus **(4.6)** yields (1).

For (2), note **(17.16)** provides a chain $0 = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$

where $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ with $\mathfrak{p}_i$ prime. Then $\gamma_0(M_i) - \gamma_0(M_{i-1}) = \gamma_0(R/\mathfrak{p}_i)$. So $\gamma_0(M) = \sum \gamma_0(R/\mathfrak{p}_i)$. Thus (2) holds.

For (3), set $K := \operatorname{Frac}(R)$, and define $\lambda\colon \Lambda \to \mathbb{Z}$ by $\lambda(M) := \dim_K(K \otimes M)$. Given a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$, note that the sequence $0 \to K \otimes M_1 \to K \otimes M_2 \to K \otimes M_3 \to 0$ is also exact by **(11.2)**, **(12.10)**, and **(12.13)**; so $\lambda(M_2) = \lambda(M_1) + \lambda(M_3)$. So λ induces a $\mathbb{Z}$-map $\lambda_0\colon K_0(R) \to \mathbb{Z}$ by (1). But $\lambda_0(R^n) = n$ and $R^n \in \mathcal{N}$ by **(16.14)**; so λ_0 is surjective. Thus (3) holds.

In (4), given a prime $\mathfrak{p}$, say $\mathfrak{p} = \langle p\rangle$. If $p \neq 0$, then $\mu_p : R \to \mathfrak{p}$ is injective, so an isomorphism. But $0 \to \mathfrak{p} \to R \to R/\mathfrak{p} \to 0$ is exact. Hence $\gamma_0(R/\mathfrak{p}) = 0$ if $\mathfrak{p} \neq 0$, and $\gamma_0(R/\mathfrak{p}) = (R)$ if $\mathfrak{p} = 0$. So $\gamma_0(R)$ generates $K_0(R)$ by (2). Thus (3) yields (4).

In (5), as R is Noetherian, R' and R'' are too by **(16.10)**. But, over a Noetherian ring, a module is Noetherian if and only if it is finitely generated by **(16.15)**. Thus we need consider only the finitely generated modules over R, R', and R''.

Via restriction of scalars, each finitely generated R'-module is a finitely generated R-module too by **(10.16)**. So restriction of scalars induces a function from the isomorphism classes of finitely generated R'-modules to $K_0(R)$. Plainly, restriction of scalars preserves exactness. Thus (1) yields (a).

For (b), recall that R'' is module finite over R by **(10.17)**(3). So $(\psi\varphi)_!$ is defined. Plainly, restriction of scalars respects composition. Thus (b) holds. □

Exercise (17.35) (*Grothendieck Group* $K^0(R)$**) .** — Keep the setup of **(17.34)**. Assume R is Noetherian. Let $\mathcal{F}$ be the subcategory of $((R\text{-mod}))$ of all finitely generated *flat* R-modules M and all linear maps between them; set $K^0(R) := K(\mathcal{F})$ and $\gamma^0 := \gamma_{\mathcal{F}}$. Let $\varphi\colon R \to R'$ and $\psi\colon R' \to R''$ be maps of Noetherian rings. Show:

(1) Setting $\gamma^0(M)\gamma^0(N) := \gamma^0(M \otimes N)$ makes $K^0(R)$ a $\mathbb{Z}$-algebra with $\gamma^0(R) = 1$.
(2) Setting $\gamma^0(M)\gamma_0(L) := \gamma_0(M \otimes L)$ makes $K_0(R)$ a $K^0(R)$-module.
(3) Assume R is local. Then $K^0(R) = \mathbb{Z}$.
(4) Setting $\varphi^!\gamma^0(M) := \gamma^0(M \otimes_R R')$ defines a ring map $\varphi^!\colon K^0(R) \to K^0(R')$. Moreover, $(\varphi\psi)^! = \varphi^!\psi^!$.
(5) If $\varphi\colon R \to R'$ is module finite, then $\varphi_!\colon K_0(R') \to K_0(R)$ is linear over $K^0(R)$.

Solution: In (1), by construction $K^0(R)$ is a $\mathbb{Z}$-module. Given two finitely generated, flat R-modules M and N, note that $M \otimes N$ is finitely generated owing to **(8.16)**, and is flat owing to **(9.24)** and **(8.5)**(2). As M is flat, $M \otimes \bullet$ is exact. So by **(17.34)**(1) with $G := K^0(R)$, the function $N \mapsto M \otimes N$ induces a $\mathbb{Z}$-map $K^0(R) \to K^0(R)$; in other words, $\gamma^0(M \otimes N)$ depends only on $\gamma^0(N)$.

Similarly, as N is flat, $M \mapsto M \otimes N$ induces a $\mathbb{Z}$-map $K^0(R) \to K^0(R)$; in other words,, $\gamma^0(M \otimes N)$ depends only on $\gamma^0(M)$. Setting $\gamma^0(M)\gamma^0(N) := \gamma^0(M \otimes N)$ thus gives $K^0(R)$ a well-defined two-sided distributive product. It's associative by **(8.8)**(1). It's commutative by **(8.5)**(1). And $\gamma^0(R) = 1$ by **(8.5)**(2). So (1) holds.

To prove (2), argue as in (1) with one major difference: since L needn't be flat, given a short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ where M_3 is flat, note that $0 \to M_1 \otimes L \to M_2 \otimes L \to M_3 \otimes L \to 0$ is also exact by **(9.8)**(1).

For (3), recall that, as R is Noetherian, any finitely generated module is finitely presented by **(16.15)**. Hence any finitely generated, flat M is free by **(10.12)**, so $M \simeq R^n$ for some $n \geq 0$. Thus $\gamma^0(R)$ generates $K^0(R)$ as a $\mathbb{Z}$-algebra.

Consider the function $R^n \mapsto n$; it passes to the isomorphism classes of the R^n by **(10.5)**(2) or **(5.32)**(2). Given a short exact sequence $0 \to R^{n_1} \to R^{n_2} \to R^{n_3} \to 0$, note $R^{n_2} \simeq R^{n_1} \oplus R^{n_3}$ by **(5.16)**(2) and **(5.15)**; so $n_2 = n_1 + n_3$. Hence arguing as in (**17.34**)(1) shows that this function induces a $\mathbb{Z}$-map $\lambda^0 \colon K^0(R) \to \mathbb{Z}$. But $\lambda^0(\gamma^0(R)) = 1$, and $\gamma^0(R)$ generates $K^0(R)$. Thus (3) holds.

For (4), given a finitely generated, flat R-module M, note that $M \otimes_R R'$ is finitely generated and flat over R' by (**8.14**) and (**9.22**). Arguing as in (2), but with R' for N, shows that $M \mapsto M \otimes_R R'$ induces a $\mathbb{Z}$-map $\varphi^! \colon K^0(R) \to K^0(R')$. It's a ring map as $(M \otimes_R N) \otimes_R R' = M \otimes_R (N \otimes_R R') = (M \otimes_R R') \otimes_{R'} (N \otimes_R R')$ by (**8.8**)(1) and (**8.9**)(1). Finally, $(\varphi\psi)^! = \varphi^! \psi^!$ as $(M \otimes_R R') \otimes_{R'} R'' = M \otimes_R R''$ again by (**8.9**)(1). Thus (4) holds.

For (5), note $(M \otimes_R R') \otimes_{R'} L = M \otimes_R L$ by (**8.9**)(1). So $\varphi_!\big(\varphi^!(\gamma^0(M))\gamma_0(L)\big)$ is equal to $\gamma^0(M)\varphi_!(\gamma_0(L))$. Thus, by $\mathbb{Z}$-linearity, (5) holds. □

18. Primary Decomposition

Exercise (18.6) . — Let $\varphi \colon R \twoheadrightarrow R'$ be a surjective ring map, M an R-module, $Q' \subsetneqq M'$ two R'-modules, $\alpha \colon M \twoheadrightarrow M'$ a surjective R-map, $\mathfrak{p}'$ a prime of R'. Set $\mathfrak{p} := \varphi^{-1}(\mathfrak{p}')$ and $Q := \alpha^{-1}Q'$. Show Q is $\mathfrak{p}$-primary if and only if Q' is $\mathfrak{p}'$-primary.

Solution: Note $M/Q = M'/Q'$ and $\operatorname{Ker}(\varphi) \subset \operatorname{Ann}(M/Q)$. Thus (**17.4**) implies that $\operatorname{Ass}_R(M/Q) = \{\mathfrak{p}\}$ if and only if $\operatorname{Ass}_{R'}(M'/'Q) = \{\mathfrak{p}'\}$, as desired. □

Exercise (18.7) . — Let R be a ring, and $\mathfrak{p} = \langle p \rangle$ a principal prime generated by a nonzerodivisor p. Show every positive power $\mathfrak{p}^n$ is old-primary and $\mathfrak{p}$-primary. Show conversely, an ideal $\mathfrak{q}$ is equal to some $\mathfrak{p}^n$ if either (1) $\mathfrak{q}$ is old-primary and $\sqrt{\mathfrak{q}} = \mathfrak{p}$ or (2) R is Noetherian and $\mathfrak{q}$ is $\mathfrak{p}$-primary.

Solution: First, note that $\operatorname{Ann}(R/\mathfrak{p}^n) = \mathfrak{p}^n$. Thus $\operatorname{nil}(R/\mathfrak{p}^n) = \mathfrak{p}$ by (**3.32**)(4). Now, given $x, y \in R$ with $xy \in \mathfrak{p}^n$ but $y \notin \mathfrak{p}$, note $p \mid xy$, but $p \nmid y$. But p is prime. So $p \mid x$. So $x^n \in \mathfrak{p}^n$. Thus $\mathfrak{p}^n$ is old-primary.

Let's now proceed by induction to show $\mathfrak{p}^n$ is $\mathfrak{p}$-primary. Form the exact sequence

$$0 \to \mathfrak{p}^n/\mathfrak{p}^{n+1} \to R/\mathfrak{p}^{n+1} \to R/\mathfrak{p}^n \to 0.$$

Consider the map $R \to \mathfrak{p}^n/\mathfrak{p}^{n+1}$ given by $x \mapsto xp^n$. It is surjective, and its kernel is $\mathfrak{p}$ as p is a nonzerodivisor. Hence $R/\mathfrak{p} \xrightarrow{\sim} \mathfrak{p}^n/\mathfrak{p}^{n+1}$. But $\operatorname{Ass}(R/\mathfrak{p}) = \{\mathfrak{p}\}$ by (**17.5**)(2). Thus (**17.6**) yields $\operatorname{Ass}(R/\mathfrak{p}^n) = \{\mathfrak{p}\}$ for every $n \ge 1$, as desired.

Conversely, assume (1). Then $\mathfrak{p} = \sqrt{\mathfrak{q}}$. So $p^n \in \mathfrak{q}$ for some n; take n minimal. Then $\mathfrak{p}^n \subset \mathfrak{q}$. Suppose there's $x \in \mathfrak{q} - \mathfrak{p}^n$. Say $x = yp^m$ for some y and $m \ge 0$. Then $m < n$ as $x \notin \mathfrak{p}^n$. Take m maximal. Now, $p^m \notin \mathfrak{q}$ as n is minimal. But $\mathfrak{q}$ is old-primary. So $y \in \mathfrak{q} \subset \mathfrak{p}$. So $y = zp$ for some z. Then $x = zp^{m+1}$, contradicting the maximality of m. Thus $\mathfrak{q} = \mathfrak{p}^n$, as desired.

Finally, assume (2). Then $\operatorname{Ass}(R/\mathfrak{q}) = \{\mathfrak{p}\}$. So $\mathfrak{q}$ is old primary and $\sqrt{\mathfrak{q}} = \mathfrak{p}$ by (**18.3**)(5). So (1) holds. Thus by the above, $\mathfrak{q}$ is equal to some $\mathfrak{p}^n$. □

Exercise (18.25) . — Fix a prime $p \in \mathbb{Z}$. Set $M := \bigoplus_{n=1}^{\infty} \mathbb{Z}/\langle p^n \rangle$ and $Q := 0$ in M. Show Q is $\langle p \rangle$-primary, but not old-primary (even though $\mathbb{Z}$ is Noetherian).

Solution: Set $M_k := \bigoplus_{n=1}^{k} \mathbb{Z}/\langle p^n \rangle$. Then $M = \bigcup_{k=1}^{\infty} M_k$. So (**17.22**) yields $\operatorname{Ass}(M) = \bigcup_{k=1}^{\infty} \operatorname{Ass}(M_k)$. But $\operatorname{Ass}(M_k) = \bigcup_{h=1}^{k} \operatorname{Ass}(M_h)$ by (**17.21**). Moreover, $\operatorname{Ass}(M_h) = \{\langle p \rangle\}$ by (**18.7**). Thus $\operatorname{Ass}(M/Q) = \{\langle p \rangle\}$. Thus Q is $\langle p \rangle$-primary.

Set $m := (1, p, p^2, \ldots)$. Then $pm = 0 \in Q$, but $m \notin Q$. And $\operatorname{Ann}(M) = \langle 0 \rangle$. So $p \notin \operatorname{nil}(M/Q)$. Thus Q is not old-primary. □

Exercise (18.26) . — Let k be a field, and $k[X,Y]$ the polynomial ring. Let $\mathfrak{a}$ be the ideal $\langle X^2,\, XY\rangle$. Show $\mathfrak{a}$ is not primary, but $\sqrt{\mathfrak{a}}$ is prime. Show $\mathfrak{a}$ satisfies this condition: $FG \in \mathfrak{a}$ implies $F^2 \in \mathfrak{a}$ or $G^2 \in \mathfrak{a}$.

Solution: First, $\langle X\rangle$ is prime by **(2.9)**. But $\langle X^2\rangle \subset \mathfrak{a} \subset \langle X\rangle$. So $\sqrt{\mathfrak{a}} = \langle X\rangle$ by **(3.40)**. On the other hand, $XY \in \mathfrak{a}$, but $X \notin \mathfrak{a}$ and $Y \notin \sqrt{\mathfrak{a}}$; thus $\mathfrak{a}$ is not primary by **(18.3)**(5). If $FG \in \mathfrak{a}$, then $X \mid F$ or $X \mid G$, so $F^2 \in \mathfrak{a}$ or $G^2 \in \mathfrak{a}$. □

Exercise (18.27) . — Let R be PIR, $\mathfrak{q}$ a primary ideal, and $\mathfrak{p}$, $\mathfrak{r}$ prime ideals.

(1) Assume $\mathfrak{q} \subset \mathfrak{p}$ and $\mathfrak{r} \subsetneqq \mathfrak{p}$. Show $\mathfrak{r} \subset \mathfrak{q}$. (2) Assume $\mathfrak{r} = \sqrt{\mathfrak{q}} \subsetneqq \mathfrak{p}$. Show $\mathfrak{r} = \mathfrak{q}$.
(3) Assume $\mathfrak{r} \subsetneqq \mathfrak{p}$. Show $\mathfrak{r}$ is the intersection of all primary ideals contained in $\mathfrak{p}$.
(4) Assume $\mathfrak{p}$ and $\mathfrak{r}$ are not comaximal. Show one contains the other.

Solution: As R is a PIR, there are $p,\, r \in R$ with $\mathfrak{p} = \langle p\rangle$ and $\mathfrak{r} = \langle r\rangle$.

For (1), note $\mathfrak{r} \subsetneqq \mathfrak{p}$ implies $r = xp$ for some $x \in R$, but $p \notin \mathfrak{r}$. So as $\mathfrak{r}$ is prime, $x \in \mathfrak{r}$. So $x = yr$ for some $y \in R$. Thus $(1 - yp)r = 0 \in \mathfrak{q}$.

Note $1 - yp \notin \mathfrak{p}$. But $\mathfrak{q} \subset \mathfrak{p}$ and $\mathfrak{p}$ is prime, so $\sqrt{\mathfrak{q}} \subset \mathfrak{p}$. Hence $1 - yp \notin \sqrt{\mathfrak{q}}$. So $r \in \mathfrak{q}$ by **(18.3)**(5). Thus $\mathfrak{r} \subset \mathfrak{q}$, as desired.

For (2), note $\mathfrak{r} = \sqrt{\mathfrak{q}} \supset \mathfrak{q}$. But (1) yields $\mathfrak{r} \subset \mathfrak{q}$. Thus $\mathfrak{r} = \mathfrak{q}$, as desired.

For (3), note $\mathfrak{r}$ is itself a primary ideal by **(18.2)**. Thus (1) yields what's desired.

For (4), note some prime $\mathfrak{m}$ contains both $\mathfrak{p}$ and $\mathfrak{r}$. But (3) implies $\mathfrak{m}$ can properly contain at most one prime. So if $\mathfrak{p}$ and $\mathfrak{r}$ are distinct, then one is equal to $\mathfrak{m}$, and so contains the other, as desired. □

Exercise (18.28) . — Let $\mathbb{Z}[X]$ be the polynomial ring, and set $\mathfrak{m} := \langle 2, X\rangle$ and $\mathfrak{q} := \langle 4, X\rangle$. Show $\mathfrak{m}$ is maximal, $\mathfrak{q}$ is $\mathfrak{m}$-primary, and $\mathfrak{q}$ is not a power of $\mathfrak{m}$.

Solution: For any $z \in \mathbb{Z}$, form the map $\varphi_z\colon \mathbb{Z}[X] \to \mathbb{Z}/\langle z\rangle$ restricting to the quotient map $\mathbb{Z} \to \mathbb{Z}/\langle z\rangle$ and sending X to 0. Then $\mathrm{Ker}(\varphi_z) = \langle z, X\rangle$. Therefore,

$$\mathbb{Z}[X]/\langle z, X\rangle \xrightarrow{\sim} \mathbb{Z}/\langle z\rangle.$$

Take $z := 2$. Then $\mathbb{Z}[X]/\mathfrak{m} \xrightarrow{\sim} \mathbb{Z}/\langle 2\rangle$. But $\mathbb{Z}/\langle 2\rangle$ is a field. Thus $\mathfrak{m}$ is maximal.

Take $z := 4$. Then $\mathbb{Z}[X]/\mathfrak{q} \xrightarrow{\sim} \mathbb{Z}/\langle 4\rangle$. But 2 is the only nilpotent of $\mathbb{Z}/\langle 4\rangle$. So $\mathfrak{m} = \mathrm{nil}(\mathbb{Z}[X]/\mathfrak{q})$; moreover, $\mathfrak{m}^2(\mathbb{Z}[X]/\mathfrak{q}) = 0$. Thus $\mathfrak{q}$ is $\mathfrak{m}$-primary by **(18.8)**(2).

Finally, $X \notin \mathfrak{m}^k$ for $k > 1$. But $X \in \mathfrak{q}$. Thus $\mathfrak{q}$ is not a power of $\mathfrak{m}$. □

Exercise (18.29) . — Let k be a field, $R := k[X,Y,Z]$ the polynomial ring in three variables. Set $\mathfrak{p}_1 := \langle X, Y\rangle$, set $\mathfrak{p}_2 := \langle X, Z\rangle$, set $\mathfrak{m} := \langle X, Y, Z\rangle$, and set $\mathfrak{a} := \mathfrak{p}_1\mathfrak{p}_2$. Show that $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is an irredundant primary decomposition. Which associated primes are minimal, and which are embedded?

Solution: Clearly $\mathfrak{a} \subset \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$. Conversely, given $F \in \mathfrak{m}^2$, write

$$F = G_1X^2 + G_2Y^2 + G_3Z^2 + G_4XY + G_5XZ + G_6YZ.$$

If $F \in \mathfrak{p}_1$, then $G_3Z^2 \in \mathfrak{p}_1$, so $G_3 \in \mathfrak{p}_1$, so $G_3Z^2 \in \mathfrak{a}$. Similarly, if $F \in \mathfrak{p}_2$, then $G_2Y^2 \in \mathfrak{a}$. Thus $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$.

The $\mathfrak{p}_i$ are prime, so primary by **(18.2)**, and $\mathfrak{m}^2$ is primary by **(18.11)**. Thus $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a primary decomposition.

The three primes $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{m}$ are clearly distinct. Moreover, $X \in (\mathfrak{p}_1 \cap \mathfrak{p}_2) - \mathfrak{m}^2$ and $Y^2 \in (\mathfrak{m}^2 \cap \mathfrak{p}_1) - \mathfrak{p}_2$ and $Z^2 \in (\mathfrak{m}^2 \cap \mathfrak{p}_2) - \mathfrak{p}_1$. Thus $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is irredundant.

Plainly, the $\mathfrak{p}_i$ are minimal, and $\mathfrak{m}$ is embedded. □

Exercise (18.30) . — Let k be a field, $R := k[X, Y, Z]$ be the polynomial ring. Set $\mathfrak{a} := \langle XY,\, X - YZ\rangle$, set $\mathfrak{q}_1 := \langle X,\, Z\rangle$ and set $\mathfrak{q}_2 := \langle Y^2,\, X - YZ\rangle$. Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ holds and that this expression is an irredundant primary decomposition.

Solution: First, $XY = Y(X - YZ) + Y^2Z \in \mathfrak{q}_2$. Hence $\mathfrak{a} \subset \mathfrak{q}_1 \cap \mathfrak{q}_2$. Conversely, take $F \in \mathfrak{q}_1 \cap \mathfrak{q}_2$. Then $F \in \mathfrak{q}_2$, so $F = GY^2 + H(X - YZ)$ with $G, H \in R$. But $F \in \mathfrak{q}_1$, so $G \in \mathfrak{q}_1$; say $G = AX + BZ$ with $A, B \in R$. Then

$$F = (AY + B)XY + (H - BY)(X - ZY) \in \mathfrak{a}.$$

Thus $\mathfrak{a} \supset \mathfrak{q}_1 \cap \mathfrak{q}_2$. Thus $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ holds.

Finally, $\mathfrak{q}_1$ is prime by (2.9). Let's see $\mathfrak{q}_2$ is primary. Form the $k[Y, Z]$-map $\varphi\colon R \twoheadrightarrow k[Y, Z]$ with $\varphi(X) := YZ$. So $\operatorname{Ker}(\varphi) = \langle X - YZ\rangle$ by (1.17)(2). But $\varphi^{-1}\langle Y^2\rangle = Y^2 + \operatorname{Ker}(\varphi)$. Thus, $\mathfrak{q}_2 = \varphi^{-1}\langle Y^2\rangle$. Similarly, $\langle X,\, Y\rangle = \varphi^{-1}\langle Y\rangle$. But $\langle Y^2\rangle$ is $\langle Y\rangle$-primary in $k[Y, Z]$ by (18.7). Thus $\mathfrak{q}_2$ is $\langle X, Y\rangle$-primary in R by (18.6). Thus $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ is a primary decomposition. It is irredundant as $\mathfrak{q}_1 \neq \langle X, Y\rangle$. □

Exercise (18.31) . — For $i = 1, 2$, let R_i be a ring, M_i a R_i-module with $0 \subset M_i$ primary. Find an irredundant primary decomposition for $0 \subset M_1 \times M_2$ over $R_1 \times R_2$.

Solution: Set $Q_1 := 0 \times M_2$ and $Q_2 := M_1 \times 0$. Then $0 = Q_1 \cap Q_2$.

Say $\operatorname{Ass}_{R_1}(M_1) = \{\mathfrak{p}_1\}$. Set $\mathfrak{P}_1 := \mathfrak{p}_1 \times R_2$. Let's show Q_1 is $\mathfrak{P}_1$-primary.

Set $R := R_1 \times R_2$ and $M := M_1 \times M_2$. Note $M/Q_1 = M_1$ where M_1 is viewed as an R-module by $(x, y)m = xm$. Say $\mathfrak{p}_i = \operatorname{Ann}_{R_1}(m_1)$ with $m_1 \in M_1$. Then $\mathfrak{P}_1 = \operatorname{Ann}_R(m_1)$. But $\mathfrak{P}_1$ is prime by (2.29). Thus $\mathfrak{P}_1 \in \operatorname{Ass}_R(M/Q_1)$.

Given any $\mathfrak{P} \in \operatorname{Ass}_R(M/Q_1)$, note $\mathfrak{P} = \mathfrak{p} \times R_2$ with $\mathfrak{p} \subset R_1$ prime by (2.29). But $\mathfrak{P} = \operatorname{Ann}_R(m)$ with $m \in M_1$. So $\mathfrak{p} = \operatorname{Ann}_{R_1}(m)$. So $\mathfrak{p} \in \operatorname{Ass}_{R_1}(M_1)$. But $0 \subset M_1$ is $\mathfrak{p}_1$-primary. So $\mathfrak{p} = \mathfrak{p}_1$. So $\operatorname{Ass}_R(M/Q_1) = \{\mathfrak{P}_1\}$. Thus Q_1 is primary.

Similarly, Q_2 is primary. Thus $0 = Q_1 \cap Q_2$ is a primary decomposition; plainly it's irredundant. □

Exercise (18.32) . — Let R be a ring, $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} = \sqrt{\mathfrak{a}}$. Prove (1) every prime $\mathfrak{p}$ associated to $\mathfrak{a}$ is minimal over $\mathfrak{a}$ and (2) if R is Noetherian, then the converse holds, and $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(R/\mathfrak{a})} \mathfrak{p}$ is an irredundant primary decomposition. Find a simple example showing (1) doesn't generalize to modules.

Solution: By (3.17), $\sqrt{\mathfrak{a}} = \bigcap_\lambda \mathfrak{p}_\lambda$ where the $\mathfrak{p}_\lambda$ are the minimal primes over $\mathfrak{a}$.

For (1), say $\mathfrak{p} = \operatorname{Ann}(x)$ with $x \in R/\mathfrak{a}$ and $x \neq 0$. So $x \notin \mathfrak{p}_\lambda/\mathfrak{a}$ for some λ. Lift x to $x' \in R$. Then $x' \notin \mathfrak{p}_\lambda$. Given $y \in \mathfrak{p}$, note $x'y \in \mathfrak{p}_\lambda$. So $y \in \mathfrak{p}_\lambda$. Thus $\mathfrak{p} \subset \mathfrak{p}_\lambda$. But $\mathfrak{p}_\lambda$ is minimal. So $\mathfrak{p} = \mathfrak{p}_\lambda$. Thus (1) holds.

For (2), assume R is Noetherian. Then the $\mathfrak{p}_\lambda$ are associated to $\mathfrak{a}$ and are finite in number by (17.29). But primes are primary by (18.2). So $\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\in\operatorname{Ass}(R/\mathfrak{a})} \mathfrak{p}$ is a primary decomposition. It is irredundant, as $\mathfrak{p}_\lambda \supset \bigcap_{\mu\neq\lambda} \mathfrak{p}_\mu$ would imply $\mathfrak{p}_\lambda \supset \mathfrak{p}_\mu$ for some μ by (2.25)(1). Thus (2) holds.

Finally, for an example, take R to be any domain not a field, and $\mathfrak{m}$ a maximal ideal. Set $k := R/\mathfrak{m}$ and $M := R \oplus k$. Then $\operatorname{Ass}(M) = \operatorname{Ass}(R) \cup \operatorname{Ass}(k)$ by (17.21). Further, $\operatorname{Ass}(R) = \{\langle 0\rangle\}$ and $\operatorname{Ass}(k) = \{\mathfrak{m}\}$ by (17.5)(2). Thus $\mathfrak{m}$ is embedded. But plainly $\operatorname{Ann}(M) = 0$. Also, R is a domain. Thus $\operatorname{Ann}(M) = \operatorname{nil}(M)$. □

Exercise (18.33) . — Let R be a ring, M a module. We call a proper submodule Q **irreducible** if $Q = N_1 \cap N_2$ implies $Q = N_1$ or $Q = N_2$. Prove: (1) an irreducible submodule Q is primary if M/Q is Noetherian; and (2) a proper submodule N is the intersection of finitely many irreducible submodules if M/N is Noetherian.

Solution: For (1), note that Q has an irredundant primary decomposition by (**18.19**), say $Q = Q_1 \cap \cdots \cap Q_n$. As Q is irreducible, $Q = Q_1$ or $Q = Q_2 \cap \cdots \cap Q_n$. If the latter, then $Q = Q_i$ for some $i \geq 2$ by recursion. Thus (1) holds.

Alternatively, here's a proof not using the existence of primary decompositions. As Q is irreducible in M, plainly 0 is irreducible in M/Q. And, if 0 is primary in M/Q, then Q is primary in M by definition (**18.1**). Thus we may assume $Q = 0$.

Given $x \in R$ and a nonzero $m \in M$ such that $xm = 0$, let's show $x \in \mathrm{nil}(M)$. Set $M_n := \{m' \in M \mid x^n m' = 0\}$. Then $M_1 \subset M_2 \subset \cdots$ is a chain of submodules of M. But M is Noetherian as $Q = 0$. So $M_n = M_{n+1} = \cdots$ for some $n \geq 1$.

Given $m' \in x^n M \cap Rm$, say $m' = x^n m''$ with $m'' \in M$. But $m' \in Rm$ and $xm = 0$, so $xm' = 0$. Hence $x^{n+1}m'' = 0$, so $m'' \in M_{n+1}$. But $M_{n+1} = M_n$. So $x^n m'' = 0$. Thus $m' = 0$.

Hence $x^n M \cap Rm = 0$. But $Rm \neq 0$ and 0 is irreducible. So $x^n M = 0$. Thus $x \in \mathrm{nil}(M)$. So 0 is old-primary, so primary by (**18.3**)(4). Thus again (1) holds.

For (2), form the set $\mathcal{S}$ of all submodules of M that contain N and are not an intersection of finitely many irreducible submodules. As M/N is Noetherian, $\mathcal{S}$ has a maximal element K. As $K \in \mathcal{S}$, it's not irreducible. So $K = K_1 \cap K_2$ with $K \subsetneqq K_i$. So $K_i \notin \mathcal{S}$. So K_i is an intersection of finitely many irreducible submodules; hence, K is too. So $K \notin \mathcal{S}$, a contradiction. Thus (2) holds. □

Exercise (18.34) . — Let R be a ring, M a module, N a submodule. Consider:

(1) The submodule N is old-primary.
(2) Given any multiplicative subset S, there is $s \in S$ with $N^S = (N : \langle s \rangle)$.
(3) Given any $x \in R$, the sequence $(N : \langle x \rangle) \subset (N : \langle x^2 \rangle) \subset \cdots$ stabilizes.

Prove (1) implies (2), and (2) implies (3). Prove (3) implies (1) if N is irreducible.

Solution: Assume (1). To prove (2), note $N^S \supset (N : \langle s \rangle)$ for all $s \in S$.

First, suppose there's $s \in \mathrm{nil}(M/N) \cap S$. Then there is $k \geq 0$ with $s^k M \subset N$. So $(N : \langle s^k \rangle) = M$. But $s^k \in S$. Hence $N^S \supset (N : \langle s^k \rangle) = M$. Thus $N^S = (N : \langle s^k \rangle)$.

Next, suppose $\mathrm{nil}(M/N) \cap S = \emptyset$. Given $m \in N^S$, there is $s \in S$ with $sm \in N$. So $m \in N$ by (1). Thus $N^S = N$. So $N^S = (N : \langle 1 \rangle)$. But $1 \in S$. Thus (2) holds.

Assume (2). To prove (3), note $N^{S_x} \supset (N : \langle x^\ell \rangle)$ for all ℓ. But (2) yields k with $N^{S_x} = (N : \langle x^k \rangle)$. Hence $(N : \langle x^k \rangle) = (N : \langle x^{k+1} \rangle) = \cdots = N^{S_x}$. Thus (3) holds.

Assume (3). To prove (1), given $x \in R$ and $m \in M - N$ with $xm \in N$, we must prove $x \in \mathrm{nil}(M/N)$. Note (3) gives k with $(N : \langle x^k \rangle) = (N : \langle x^{k+1} \rangle)$. Let's show

$$N = N' \cap N'' \text{ with } N' := N + Rm \text{ and } N'' := N + x^k M. \qquad \textbf{(18.34.1)}$$

Trivially, $N \subset N' \cap N''$. Conversely, given $m' \in N' \cap N''$, note $xm' \in N + Rxm$. But $xm \in N$. So $xm' \in N$. But $m' = n + x^k m''$ with $n \in N$ and $m'' \in M$. So $xm' = xn + x^{k+1}m''$. So $x^{k+1}m'' \in N$. Hence $m'' \in (N : \langle x^{k+1} \rangle) = (N : \langle x^k \rangle)$. Thus $m' \in N$. Thus (**18.34.1**) holds.

Also assume N is irreducible. Recall $m \notin N$. Hence $N + x^k M = N$ owing to (**18.34.1**). So $x^k M \subset N$. So $x \in \mathrm{nil}(M/N)$. Thus (1) holds. □

Exercise (18.35) . — Let R be a ring, M a Noetherian module, N a submodule, $\mathfrak{m} \subset \mathrm{rad}(M)$ an ideal. Show $N = \bigcap_{n \geq 0}(\mathfrak{m}^n M + N)$.

Solution: Set $M' := M/N$ and $N' := \bigcap \mathfrak{m}^n M'$. Then by (**18.23**), there's $x \in \mathfrak{m}$ with $(1 + x)N' = 0$. But $\mathfrak{m} \subset \mathrm{rad}(M) \subset \mathrm{rad}(M')$. So $N' = 0$ by (**4.15**). But $\mathfrak{m}^n M' = (\mathfrak{m}^n M + N)/N$. Thus $\big(\bigcap(\mathfrak{m}^n M + N)\big)/N = 0$, as desired. □

18. Appendix: Old-primary Submodules

Exercise (18.45) . — Let $\varphi\colon R \to R'$ be a ring map, M an R-module, $Q' \subsetneqq M'$ R'-modules, $\alpha\colon M \to M'$ an R-map. Set $Q := \alpha^{-1}Q'$, and assume $Q \subsetneqq M$. Set $\mathfrak{p} := \operatorname{nil}(M/Q)$ and $\mathfrak{p}' := \operatorname{nil}(M'/Q')$. If Q' is old-primary, show Q is and $\varphi^{-1}\mathfrak{p}' = \mathfrak{p}$. Conversely, when φ and α are surjective, show Q' is old-primary if Q is.

Solution: Assume Q' old-primary. Given $x \in \operatorname{z.div}(M/Q)$, there's $m \in M - Q$ with $xm \in Q$. Then $\alpha(m) \in M' - Q'$ with $\alpha(xm) \in Q'$. But $\alpha(xm) = \varphi(x)\alpha(m)$. As Q' is old-primary, $\varphi(x) \in \mathfrak{p}'$. So $x \in \varphi^{-1}\mathfrak{p}$. Thus $\operatorname{z.div}(M/Q) \subset \varphi^{-1}\mathfrak{p}'$.

Given $x \in \varphi^{-1}\mathfrak{p}'$, there's n with $\varphi(x)^n \in \operatorname{Ann}(M'/Q')$. So $\varphi(x)^n\alpha(m) \in Q'$ for all $m \in M$. But $\varphi(x)^n\alpha(m) = \alpha(x^n m)$. So $x^n m \in Q$. So $x \in \mathfrak{p}$. Thus $\varphi^{-1}\mathfrak{p}' \subset \mathfrak{p}$.

Note $\mathfrak{p} \subset \operatorname{z.div}(M/Q)$ by (17.11.1). Thus $\mathfrak{p} \subset \operatorname{z.div}(M/Q) \subset \varphi^{-1}\mathfrak{p}' \subset \mathfrak{p}$. Thus $\operatorname{z.div}(M/Q) = \varphi^{-1}\mathfrak{p}' = \mathfrak{p}$, and so (18.3)(1) implies Q is old-primary.

Conversely, assume φ and α are surjective and Q is old-primary. Given $x' \in R'$ and $m' \in M'$ with $x'm' \in Q'$, but $m' \notin Q'$, take $x \in R$ with $\varphi(x) = x'$ and $m \in M$ with $\alpha(m) = m'$. Then $\alpha(xm) = x'm'$. So $xm \in Q$, but $m \notin Q$. As Q is old-primary, $x \in \mathfrak{p}$. So there's n with $x^n \in \operatorname{Ann}(M/Q)$, or $x^n M \subset Q$. Hence $x'^n M' \subset Q'$, or $x'^n \in \operatorname{Ann}(M'/Q')$. Thus $x' \in \mathfrak{p}'$. Thus Q' is old-primary. □

Exercise (18.50) . — Let $\mathfrak{q} \subset \mathfrak{p}$ be primes, M a module, and Q an old-primary submodule with $\operatorname{nil}(M/Q) = \mathfrak{q}$. Then $0^{S_\mathfrak{p}} \subset Q$.

Solution: Given $m \in 0^{S_\mathfrak{p}}$, there's $s \in S_\mathfrak{p}$ with $sm = 0$. Then $sm \in Q$, but $s \notin \mathfrak{q}$. So $m \in Q$. Thus $0^{S_\mathfrak{p}} \subset Q$. □

Exercise (18.51) . — Let R be an absolutely flat ring, $\mathfrak{q}$ an old-primary ideal. Show that $\mathfrak{q}$ is maximal.

Solution: Set $\mathfrak{p} := \sqrt{\mathfrak{q}}$. Then $\mathfrak{p}$ is prime by (18.3)(2). So (13.61) yields that $\mathfrak{p}$ is maximal and that $R_\mathfrak{p}$ is a field. So $\mathfrak{p}R_\mathfrak{p} = 0$. Thus $\mathfrak{q}R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$.

Set $S := S_\mathfrak{p} := R - \mathfrak{p}$. Then $\mathfrak{q}^S = \mathfrak{p}^S$ by (11.11)(2)(b). But $\mathfrak{p} = \mathfrak{p}^S$ by (11.11)(3)(a). Thus $\mathfrak{q}^S = \mathfrak{p}$. So given $x \in \mathfrak{p}$, there's $s \in S$ with $sx \in \mathfrak{q}$. But $s \notin \mathfrak{p}$. So $x \in \mathfrak{q}$ by hypothesis. Thus $\mathfrak{p} \subset \mathfrak{q}$. But $\mathfrak{p}$ is maximal. So $\mathfrak{p} = \mathfrak{q}$. Thus $\mathfrak{q}$ is maximal. □

Exercise (18.52) . — Let X be an infinite compact Hausdorff space, R the ring of continuous $\mathbb{R}$-valued functions on X. Using (14.26), show that $\langle 0\rangle$ is not a finite intersection of old-primary ideals.

Solution: Every maximal ideal has the form $\mathfrak{m}_x := \{f \in R \mid f(x) = 0)\}$ for some $x \in X$ by (14.26)(1). Given an ideal $\mathfrak{q}$ with $\mathfrak{q} \subset \mathfrak{m}_x \cap \mathfrak{m}_y$ but $x \neq y$, let's now see that $\mathfrak{q}$ isn't old-primary.

Given $f \in R$, set $U_f = \{x \in X \mid f(x) \neq 0\}$. By (14.26)(3), the U_f form a basis of the topology. But X is Hausdorff, and $x \neq y$. So there are f, g with $x \in U_f$ and $y \in U_g$, but $U_f \cap U_g = \emptyset$. Then $f \notin \mathfrak{m}_x$ and $g^n \notin \mathfrak{m}_y$ for all n. So $f, g^n \notin \mathfrak{q}$. But $fg = 0 \in \mathfrak{q}$. Thus $\mathfrak{q}$ isn't old-primary.

Given finitely many old-primary ideals $\mathfrak{q}_i$, say $\mathfrak{q}_i \subset \mathfrak{m}_{x_i}$. As X is infinite, there's $x \in X$ with $x \neq x_i$ for all i. By the above, there's $f_i \in \mathfrak{q}_i - \mathfrak{m}_x$. Set $f = \prod f_i$. Then $f \in \bigcap \mathfrak{q}_i$, but $f(x) \neq 0$. Thus $\langle 0\rangle \neq \bigcap \mathfrak{q}_i$. □

Exercise (18.53) . — Let R be a ring, X a variable, $N, Q \subset M$ modules, and $N = \bigcap_{i=1}^r Q_i$ a decomposition. Assume Q is old-primary. Assume $N = \bigcap_{i=1}^r Q_i$ is irredundant; that is, **(18.13)**(1)–(2) hold. Show:

(1) Assume M is finitely generated. Let $\mathfrak{p}$ be a minimal prime of M. Then $\mathfrak{p}[X]$ is a minimal prime of $M[X]$.
(2) Then $\operatorname{nil}\big(M[X]/N[X]\big) = \operatorname{nil}(M/N)[X]$.
(3) Then $Q[X]$ is old-primary in $M[X]$.
(4) Then $N[X] = \bigcap_{i=1}^r Q_i[X]$ is irredundant in $M[X]$.

Solution: For (1), note $\mathfrak{p}$ is, by **(13.5)**, a minimal prime of $\operatorname{Ann}(M)$ as M is finitely generated. Thus $\mathfrak{p}[X] \supset \operatorname{Ann}(M)[X]$. Now, given $\mathfrak{p}[X] \supset \mathfrak{P} \supset \operatorname{Ann}(M)[X]$ with $\mathfrak{P}$ prime, set $\mathfrak{p}' := \mathfrak{P} \cap R$. Intersecting with R plainly gives $\mathfrak{p} \supset \mathfrak{p}' \supset \operatorname{Ann}(M)$. But $\mathfrak{p}'$ is prime. So $\mathfrak{p}' = \mathfrak{p}$.

So $\mathfrak{p}[X] \supset \mathfrak{P} \supset \mathfrak{p}'[X] = \mathfrak{p}[X]$. So $\mathfrak{P} = \mathfrak{p}[X]$. Thus $\mathfrak{p}[X]$ is a minimal prime of $\operatorname{Ann}(M[X])$. But $M[X]$ is finitely generated over $R[X]$. Thus **(13.5)** yields (1).

For (2), note $M[X]/N[X] = (M/N)[X]$ by **(4.18)**(3). Set $\mathfrak{a} := \operatorname{Ann}(M/N)$. Then $\operatorname{Ann}\big(M[X]/N[X]\big) = \mathfrak{a}[X]$ by **(4.19)**(1). So $\operatorname{nil}\big(M[X]/N[X]\big) = \sqrt{\mathfrak{a}[X]}$. But $\sqrt{\mathfrak{a}[X]} = \sqrt{\mathfrak{a}}[X]$ by **(3.44)**(2) with $R/\mathfrak{a}$ for R, as $R[X]/\mathfrak{a}[X] = (R/\mathfrak{a})[X]$ by **(1.16)**. Thus (2) holds.

For (3), set $\mathfrak{p} := \operatorname{nil}(M/Q)$. Then $\operatorname{nil}\big(M[X]/Q[X]\big) = \mathfrak{p}[X]$ by (2). Thus given $f \in R[X]$ and $m \in M[X]$ with $fm \in Q[X]$ but $m \notin Q[X]$, we must see $f \in \mathfrak{p}[X]$.

Say $f = a_0 + \cdots + a_n X^n$ and $m = m_0 + \cdots + m_d X^d$ with d minimal among all m with $fm \in Q[X]$ but $m \notin Q[X]$. Suppose $fm_d \notin Q[X]$. Let's find a contradiction.

Say $a_r m_d \notin Q$, but $a_{r+i} m_d \in Q$ for $i > 0$. Fix $i > 0$. Set $m' := a_{r+i}(m - m_d X^d)$. Then $fm' \in Q[X]$, as $fm \in Q[X]$ and $a_{r+i} m_d \in Q$. Also $\deg(m') < d$. Hence the minimality of d yields $m' \in Q[X]$. So $a_{r+i} m_{d-i} \in Q$. But i is arbitrary with $i > 0$. Also $fm \in Q[X]$, so $a_r m_d + a_{r+1} m_{d-1} + \cdots \in Q$. So $a_r m_d \in Q$, a contradiction. Thus $fm_d \in Q[X]$.

Thus $a_i m_d \in Q$ for all $i \geq 0$. But $m_d \notin Q$. So all $a_i \in \mathfrak{p}$ as Q is old-primary. Thus $f \in \mathfrak{p}[X]$, as desired. Thus (3) holds.

For (4), suppose $N[X] = \bigcap_{j \neq i} Q_i[X]$. Intersecting with M yields $N = \bigcap_{j \neq i} Q_i$, a contradiction as $N = \bigcap_i Q_i$ is irredundant. Thus $N[X] \neq \bigcap_{j \neq i} Q_i[X]$.

Lastly, set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$. The $\mathfrak{p}_i$ are distinct as $N = \bigcap Q_i$ is irredundant. So the $\mathfrak{p}_i[X]$ are distinct. But $\operatorname{nil}(M[X]/Q_i[X]) = \mathfrak{p}_i[X]$ by (2). Thus (4) holds. □

Exercise (18.54) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring. Given i, set $\mathfrak{p}_i := \langle X_1, \ldots, X_i \rangle$. Show $\mathfrak{p}_i$ is prime, and all its powers are $\mathfrak{p}_i$ -primary.

Solution: First, $\mathfrak{p}_i$ is prime by **(2.9)**. Now, set $P_i := k[X_1, \ldots, X_i]$. Let $\mathfrak{m}_i$ be its ideal generated by $X_1, \ldots, X_i$. Then $\mathfrak{m}_i$ is maximal in P_i by **(2.14)**. So each $\mathfrak{m}_i^m$ is old-primary by **(18.9)**. Hence $\mathfrak{m}_i^m R$ is old-primary by repeated use of **(18.53)**(3). Plainly, $\mathfrak{m}_i^m R = \mathfrak{p}_i^m$ and $\sqrt{\mathfrak{p}_i^m} = \mathfrak{p}_i$. But P is Noetherian by **(16.10)**. Thus **(18.3)**(4) implies $\mathfrak{p}_i^m$ is $\mathfrak{p}_i$ -primary. □

Exercise (18.55) . — Let R be a ring, $\mathfrak{p}$ a prime, M a finitely generated module. Set $Q := 0^{S_\mathfrak{p}} \subset M$. Show (1) and (2) below are equivalent, and imply (3):

(1) $\operatorname{nil}(M/Q) = \mathfrak{p}$. (2) $\mathfrak{p}$ is minimal over $\operatorname{Ann}(M)$. (3) Q is old-primary.

Also, if M/Q is Noetherian, show (1) and (2) above and (3′) below are equivalent:

(3′) Q is $\mathfrak{p}$-primary.

Solution: Assume (1). Then $\mathfrak{p} \supset \mathrm{Ann}(M/Q) \supset \mathrm{Ann}(M)$. Let $\mathfrak{q}$ be a prime with $\mathfrak{p} \supset \mathfrak{q} \supset \mathrm{Ann}(M)$. Given $x \in \mathfrak{p}$, there's $n \geq 0$ with $x^n M \subset Q$. Say $m_1, \ldots, m_r$ generate M. Then there's $s_i \in S_{\mathfrak{p}}$ with $s_i x^n m_i = 0$. Set $s := \prod s_i$. Then $s x^n M = 0$. So $s x^n \in \mathrm{Ann}(M) \subset \mathfrak{q}$. But $s \notin \mathfrak{q}$. So $x \in \mathfrak{q}$. Thus $\mathfrak{p} = \mathfrak{q}$. Thus (2) holds.

Assume (2). Then **(18.40)** yields both (1) and (3).

Also, assume M/Q is Noetherian. If (1) holds, then (3) holds, and so **(18.3)**(4) yields (3′). Conversely, (3′) implies (1) by **(18.3)**(5), as desired. □

Exercise (18.56) . — Let R be a ring, M a module, Σ the set of minimal primes of $\mathrm{Ann}(M)$. Assume M is finitely generated. Set $N := \bigcap_{\mathfrak{p}\in\Sigma} 0^{S_{\mathfrak{p}}}$. Show:

(1) Given $\mathfrak{p} \in \Sigma$, the saturation $0^{S_{\mathfrak{p}}}$ is the smallest old-primary submodule Q with $\mathrm{nil}(M/Q) = \mathfrak{p}$.
(2) Say $0 = \bigcap_{i=1}^r Q_i$ with the Q_i old-primary. For all j, assume $Q_j \not\supset \bigcap_{i\neq j} Q_i$. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$. Then $N = 0$ if and only if $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \Sigma$.
(3) If $M = R$, then $N \subset \mathrm{nil}(R)$.

Solution: For (1), note $\mathrm{nil}(M/0^{S_{\mathfrak{p}}}) = \mathfrak{p}$ and $0^{S_{\mathfrak{p}}}$ is old-primary by **(18.55)**. But $0^{S_{\mathfrak{p}}} \subset Q$ for any old-primary Q with $\mathrm{nil}(M/Q) = \mathfrak{p}$ by **(18.50)**. So (1) holds.

In (2), if $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \Sigma$, then $Q_i \supset 0^{S_{\mathfrak{p}_i}}$ for all i by (1), and thus $N = 0$.

Conversely, assume $\bigcap_{\mathfrak{p}\in\Sigma} 0^{S_{\mathfrak{p}}} =: N = 0$. But **(18.49)**(1) with $N = 0$ implies $\Sigma \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$; so Σ is finite. Also $0^{S_{\mathfrak{p}}}$ is old-primary for all $\mathfrak{p} \in \Sigma$ by (1).

Given $\mathfrak{p} \in \Sigma$, set $\Sigma' := \Sigma - \{\mathfrak{p}\}$. Let's show $0^{S_{\mathfrak{p}}} \not\supset \bigcap_{\mathfrak{q}\in\Sigma'} 0^{S_{\mathfrak{q}}}$. If not, then (1) and **(18.37)**(2) give

$$\mathfrak{p} = \mathrm{nil}(M/0^{S_{\mathfrak{p}}}) \supset \mathrm{nil}\big(M/\textstyle\bigcap_{\mathfrak{q}\in\Sigma'} 0^{S_{\mathfrak{q}}}\big) = \bigcap_{\mathfrak{q}\in\Sigma'} \mathfrak{q}$$

so **(2.25)**(1) yields $\mathfrak{p} \supset \mathfrak{q}$ for some $\mathfrak{q}$; but $\mathfrak{p}$ is minimal, so $\mathfrak{p} = \mathfrak{q}$, a contradiction. Thus $0^{S_{\mathfrak{p}}} \not\supset \bigcap_{\mathfrak{q}\in\Sigma'} 0^{S_{\mathfrak{q}}}$ for all $\mathfrak{p} \in \Sigma$. Hence both Σ and $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ are equal to the set $\mathcal{D}(M)$ of **(18.39)** by **(18.39)**(4), so to each other. Thus (2) holds.

For (3), given $\mathfrak{p} \in \Sigma$, note $\mathfrak{p}$ is old-primary by **(18.2)**. So $0^{S_{\mathfrak{p}}} \subset \mathfrak{p}$ by (1). Hence $N \subset \bigcap_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Thus **(3.17)** yields (3). □

Exercise (18.57) . — Let R be a ring, $N \subsetneqq M$ modules. Assume there exists a decomposition $N = \bigcap_{i=1}^n Q_i$ with the Q_i old-primary. Show that there are at most finitely many submodules of M of the form N^S where S is a multiplicative subset.

Solution: Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$. Then $N^S = \bigcap_{i\in I} Q_i$ where $I := \{i \mid S \cap \mathfrak{p}_i = \emptyset\}$ by **(18.47)**. But there are at most 2^n subsets $I \subset \{1, \ldots, n\}$. □

Exercise (18.58) . — Let R be a ring, M a module, $\mathfrak{p} \in \mathrm{Supp}(M)$. Fix $m, n \geq 1$. Set $(\mathfrak{p}M)^{(n)} := (\mathfrak{p}^n M)^{S_{\mathfrak{p}}}$ and $\mathfrak{p}^{(n)} := (\mathfrak{p})^{(n)}$. (We call $\mathfrak{p}^{(n)}$ the ***n*th symbolic power** of $\mathfrak{p}$.) Assume M is finitely generated. Set $N := \mathfrak{p}^{(m)}(\mathfrak{p}M)^{(n)}$. Show:

(1) Then $\mathfrak{p}$ is the smallest prime containing $\mathrm{Ann}(M/\mathfrak{p}^n M)$.
(2) Then $(\mathfrak{p}M)^{(n)}$ is old-primary, and $\mathrm{nil}\big(M/(\mathfrak{p}M)^{(n)}\big) = \mathfrak{p}$.
(3) Say $\mathfrak{p}^n M = \bigcap_{i=1}^r Q_i$ with Q_i old-primary. Set $\mathfrak{p}_i := \mathrm{nil}(M/Q_i)$. Assume $\mathfrak{p}_i = \mathfrak{p}$ if and only if $i \leq t$. Then $(\mathfrak{p}M)^{(n)} = \bigcap_{i=1}^t Q_i$.
(4) Then $(\mathfrak{p}M)^{(n)} = \mathfrak{p}^n M$ if and only if $\mathfrak{p}^n M$ is old-primary.
(5) Let Q be an old-primary submodule with $\mathrm{nil}(M/Q) = \mathfrak{p}$. Assume $\mathfrak{p}$ is finitely generated modulo $\mathrm{Ann}(M/Q)$. Then $Q \supset (\mathfrak{p}M)^{(n)}$ if $n \gg 0$.
(6) Then $N^{S_{\mathfrak{p}}} = (\mathfrak{p}M)^{(m+n)}$ and $\mathfrak{p}$ is the smallest prime containing $\mathrm{Ann}(M/N)$.

(7) Say $N = \bigcap_{i=1}^{r} Q_i$ with all Q_i old-primary. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$. Assume $\mathfrak{p}_i = \mathfrak{p}$ if and only if $i \le t$. Then $Q_i = (\mathfrak{p}M)^{(m+n)}$ for some i.

Solution: For (1), note $\mathbf{V}(\operatorname{Ann}(M/\mathfrak{p}^n M)) = \operatorname{Supp}(M/\mathfrak{p}^n M)$ by **(13.4)**(3) and $\operatorname{Supp}(M/\mathfrak{p}^n M) = \operatorname{Supp}(M) \cap \mathbf{V}(\mathfrak{p}^n)$ by **(13.46)**(1). By hypothesis, $\mathfrak{p} \in \operatorname{Supp}(M)$. But $\mathfrak{p} \in \mathbf{V}(\mathfrak{p}^n)$. Thus $\mathfrak{p} \supset \operatorname{Ann}(M/\mathfrak{p}^n M)$. However, any prime $\mathfrak{q}$ that contains $\operatorname{Ann}(M/\mathfrak{p}^n M)$ contains $\mathfrak{p}^n$, so contains $\mathfrak{p}$ by **(2.25)**(1). Thus (1) holds.

Note (2) follows immediately from (1) and **(18.40)**.

For (3), note $(\mathfrak{p}M)^{(n)} = \bigcap_{i=1}^{r} Q_i^{S_\mathfrak{p}}$ by **(12.12)**(6)(a). But $\mathfrak{p}$ is the smallest prime containing $\operatorname{Ann}(M/\mathfrak{p}^n M)$ by (1). And $Q_i \supset \mathfrak{p}^n M$, so $\operatorname{Ann}(M/Q_i) \supset \operatorname{Ann}(M/\mathfrak{p}^n M)$. So $\mathfrak{p}_i \supset \mathfrak{p}$. So $S_\mathfrak{p} \cap \mathfrak{p}_i \ne \emptyset$ for $i > t$. Hence $Q_i^{S_\mathfrak{p}} = M$ for $i > t$ by **(12.23)**. Also $Q_i^{S_\mathfrak{p}} = Q_i$ for all $i \le t$ by **(18.43)**. Thus (3) holds.

In (4), if $\mathfrak{p}^n M = (\mathfrak{p}M)^{(n)}$, then $\mathfrak{p}^n M$ is old-primary by (2).

Conversely, assume $\mathfrak{p}^n M$ is old-primary. Note $\operatorname{nil}(M/\mathfrak{p}^n M) = \mathfrak{p}$ owing to (1) and **(3.14)**. So $\mathfrak{p}^n M = (\mathfrak{p}M)^{(n)}$ by **(18.43)**. Thus (4) holds.

For (5), note $\mathfrak{p}^n M \subset Q$ for $n \gg 0$ owing to **(3.38)**. So $(\mathfrak{p}M)^{(n)} \subset Q^{S_\mathfrak{p}}$ for $n \gg 0$ by **(12.12)**(5)(a). But $Q^{S_\mathfrak{p}} = Q$ by **(18.43)**. Thus (5) holds.

For (6), note $N^{S_\mathfrak{p}} = (\mathfrak{p}M)^{(m+n)}$ as $\big((\mathfrak{p}^m)^{S_\mathfrak{p}}(\mathfrak{p}^n M)^{S_\mathfrak{p}}\big)^{S_\mathfrak{p}} = (\mathfrak{p}^{m+n}M)^{S_\mathfrak{p}}$ by **(12.28)**. But $N \subset N^{S_\mathfrak{p}}$. So $\operatorname{Ann}(M/N) \subset M/\operatorname{Ann}(N^{S_\mathfrak{p}})$.

Given $x \in \operatorname{Ann}(M/N)$, therefore $xM \subset N^{S_\mathfrak{p}} = (\mathfrak{p}M)^{(m+n)}$. But M is finitely generated. So there's $s \in S_\mathfrak{p}$ with $sxM \subset \mathfrak{p}^{m+n}M$; that is, $sx \in \operatorname{Ann}(M/\mathfrak{p}^{m+n}M)$. So $sx \in \mathfrak{p}$ by (1). But $s \notin \mathfrak{p}$. So $x \in \mathfrak{p}$. Thus $\mathfrak{p} \supset \operatorname{Ann}(M/N)$.

Note $N \supset \mathfrak{p}^{m+n}M$. So $\operatorname{Ann}(M/N) \supset \operatorname{Ann}(M/\mathfrak{p}^{m+n}M)$. Hence any prime $\mathfrak{q}$ containing $\operatorname{Ann}(M/N)$ contains $\mathfrak{p}^{m+n}$, so contains $\mathfrak{p}$ by **(2.25)**(1). Thus $\mathfrak{p}$ is the smallest prime containing $\operatorname{Ann}(M/N)$. Thus (6) holds.

Finally (7) follows from (6) in the same way that (3) follows from (1). □

Exercise (18.59) . — Let R be a ring, $f \in R$, and $N, Q_1, \ldots, Q_n \subsetneqq M$ modules with $N = \bigcap_{i=1}^{n} Q_i$ and the Q_i old-primary. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$ for all i. Assume $f \in \mathfrak{p}_i$ just for $i > h$. Show $\bigcap_{i=1}^{h} Q_i = N^{S_f} = (N : \langle f^n \rangle)$ for $n \gg 0$.

Solution: First, note $f \in \mathfrak{p}_i$ if and only if $S_f \cap \mathfrak{p}_i \ne \emptyset$. So $S_f \cap \mathfrak{p}_i = \emptyset$ just for $i \le h$. Thus **(18.47)**(1) yields $Q_1 \cap \cdots \cap Q_h = N^{S_f}$.

Second, note $N^{S_f} = \bigcup_{n \ge 0} (N : \langle f^n \rangle)$ and $(N : \langle f^p \rangle) \supset (N : \langle f^n \rangle)$ for $p \ge n$. For $i > h$, as $f \in \mathfrak{p}_i$, there's n_i with $f^{n_i} \in \operatorname{Ann}(M/Q_i)$. Then given $n \ge \max\{n_i\}$ and $m \in N^{S_f}$, note $f^n m \in Q_i$ for $i > h$, but $m \in N^{S_f} = \bigcap_{i=1}^{h} Q_i$. So $f^n m \in Q_i$ for all i. Hence $f^n m \in \bigcap_{i=1}^{r} Q_i = N$. So $m \in (N : \langle f^n \rangle)$. Thus $N^{S_f} \subset (N : \langle f^n \rangle)$. Thus $N^{S_f} = (N : \langle f^n \rangle)$, as desired. □

Exercise (18.60) . — Let R be a ring, $\mathfrak{p}$ a prime ideal, M a Noetherian module. Denote the intersection of all $\mathfrak{p}$-primary submodules by N. Show $N = 0^{S_\mathfrak{p}}$.

Solution: Set $\mathfrak{P} := \mathfrak{p}R_\mathfrak{p}$. By **(18.46)** and **(18.3)**(4)–(5), $K \mapsto \varphi_{S_\mathfrak{p}}^{-1} K$ is bijective from the $\mathfrak{P}$-primary submodules K of $M_\mathfrak{p}$ onto the $\mathfrak{p}$-primary submodules of M. So $N = \varphi_{S_\mathfrak{p}}^{-1}\big(\bigcap K\big)$. But $0^{S_\mathfrak{p}} = \varphi_{S_\mathfrak{p}}^{-1} 0$ by **(12.12)**(3)(a). So let's prove $\bigcap K = 0$.

For $n > 0$, set $K_n := \mathfrak{P}^n M_\mathfrak{p}$ and $\mathfrak{Q}_n := \operatorname{nil}_{R_\mathfrak{p}}(M_\mathfrak{p}/K_n)$. Then $\mathfrak{Q}_n \supset \mathfrak{P}$. But $\mathfrak{P}$ is maximal. Hence $\mathfrak{Q}_n = \mathfrak{P}$, unless $\mathfrak{Q}_n = R_\mathfrak{p}$.

Assume $\mathfrak{Q}_n = R_\mathfrak{p}$. Then $M_\mathfrak{p} = \mathfrak{P}^n M_\mathfrak{p}$. But $R_\mathfrak{p}$ is local, and $\mathfrak{P}$ is maximal. So $M_\mathfrak{p} = 0$ by Nakayama's Lemma **(10.6)**. Thus $\bigcap K = 0$, as desired.

Assume $\mathfrak{Q}_n = \mathfrak{P}$ instead. Then $\mathfrak{P}^n(M_\mathfrak{p}/K_n) = 0$. But $\mathfrak{P}$ is maximal. So K_n is

$\mathfrak{P}$-primary by **(18.8)**(2). But $\bigcap K_n \supset \bigcap K$. Moreover, by **(18.23)** there's $x \in \mathfrak{P}$ with $(1+x)(\bigcap K_n) = 0$. But $1 + x \in R_{\mathfrak{p}}^{\times}$ is a unit by **(3.2)**, so $\bigcap K_n = 0$. Thus again $\bigcap K = 0$, as desired. □

Exercise (18.61) . — Let R be a ring, M a module, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Supp}(M)$ distinct primes, none minimal in $\operatorname{Supp}(M)$. Assume M is finitely generated, and (*) below holds (it does, by **(18.60)** and **(18.3)**(4)–(5), if M is Noetherian):

(*) For every prime $\mathfrak{p}$, the saturation $0^{S_{\mathfrak{p}}}$ is equal to the intersection of all the old-primary submodules Q with $\operatorname{nil}(M/Q) = \mathfrak{p}$.

(1) For $1 \le i < n$, assume $\mathfrak{p}_i \not\supset \mathfrak{p}_n$ and let Q_i be an old-primary submodule with $\operatorname{nil}(M/Q_i) = \mathfrak{p}_i$ and $\bigcap_{j \ne i} Q_j \not\subset Q_i$. Set $P := \bigcap_{j<n} Q_j$. Show $P \not\subset 0^{S_{\mathfrak{p}_n}}$.

(2) In the setup of (1), show there is an old-primary submodule Q_n such that $\operatorname{nil}(M/Q_n) = \mathfrak{p}_n$ and $P \not\subset Q_n$. Then show $\bigcap_{j \ne i} Q_j \not\subset Q_i$ for all i.

(3) Use (2) and induction on n to find old-primary submodules $Q_1, \ldots, Q_n$ with $\operatorname{nil}(M/Q_i) = \mathfrak{p}_i$ and $\bigcap_{j \ne i} Q_j \not\subset Q_i$ for all i.

Solution: For (1), suppose rather $P \subset 0^{S_{\mathfrak{p}_n}}$. Note $\mathfrak{p}_n \in \operatorname{Supp}(M)$; so **(13.4)**(3) yields $\mathfrak{p}_n \supset \operatorname{Ann}(M)$. So by **(3.16)**, $\mathfrak{p}_n$ contains a prime $\mathfrak{p}$ minimal containing $\operatorname{Ann}(M)$. Plainly $0^{S_{\mathfrak{p}_n}} \subset 0^{S_{\mathfrak{p}}}$. So $P \subset 0^{S_{\mathfrak{p}}}$. Thus $\operatorname{nil}(M/P) \subset \operatorname{nil}(M/0^{S_{\mathfrak{p}}})$.

Note $\bigcap_{i<n} \mathfrak{p}_i = \operatorname{nil}(M/P)$ by **(18.37)**(2). As M is finitely generated, $0^{S_{\mathfrak{p}}}$ is old-primary and $\operatorname{nil}(M/0^{S_{\mathfrak{p}}}) = \mathfrak{p}$ by **(18.40)**. Hence $\bigcap_{i<n} \mathfrak{p}_i \subset \mathfrak{p}$. So $\mathfrak{p}_i \subset \mathfrak{p}$ for some i by **(2.25)**(1). But $\mathfrak{p}$ is minimal and $\mathfrak{p}_i$ is not, a contradiction, as desired.

For (2), note $0^{S_{\mathfrak{p}_n}}$ is the intersection of all the old-primary submodules Q_n with $\operatorname{nil}(M/Q_n) = \mathfrak{p}_n$ by (*). So by (1), there's Q_n with $P \not\subset Q_n$; that is, $\bigcap_{i<n} Q_i \not\subset Q_n$.

Suppose $\bigcap_{j \ne i} Q_j \subset Q_i$ for some $i < n$. Set $L := \bigcap_{j \ne i,n} Q_j$. Then $L \not\subset Q_i$ by a hypothesis in (1). So there's $l \in L - Q_i$. Given $x \in \mathfrak{p}_n$, there's p with $x^p M \subset Q_n$. Then $x^p l \in L \cap Q_n = \bigcap_{j \ne i} Q_j \subset Q_i$. But $l \notin Q_i$. So $x^p \in \mathfrak{p}_i$. So $x \in \mathfrak{p}_i$. Thus $\mathfrak{p}_n \subset \mathfrak{p}_i$, contradicting a hypothesis in (1), as desired.

For (3), if $n = 1$, take Q_1 to be any of the submodules Q whose existence is assured by (*) with $\mathfrak{p} := \mathfrak{p}_1$. Assume $n \ge 2$. Reorder the $\mathfrak{p}_i$ so that $\mathfrak{p}_n \not\subset \mathfrak{p}_i$ for $i < n$. By induction, there are old-primary submodules $Q_1, \ldots, Q_{n-1}$ with $\operatorname{nil}(M/Q_i) = \mathfrak{p}_i$ and $\bigcap_{j \ne i} Q_j \not\subset Q_i$ for all i. Finally, (2) now yields (3). □

Exercise (18.62) . — Let R be a ring, M a module, Q an old-primary submodule. Set $\mathfrak{q} := \operatorname{Ann}(M/Q)$. Show that $\mathfrak{q}$ is old-primary.

Solution: Given $x, y \in R$ with $xy \in \mathfrak{q}$ but $y \notin \mathfrak{q}$, there's $m \in M$ with $ym \notin Q$, but $xym \in Q$. But Q is old-primary. So $x \in \operatorname{nil}(M/Q)$. But $\operatorname{nil}(M/Q) := \sqrt{\mathfrak{q}}$, and $\mathfrak{q} = \operatorname{Ann}(R/\mathfrak{q})$; so $\operatorname{nil}(M/Q) = \operatorname{nil}(R/\mathfrak{q})$. Thus $\mathfrak{q}$ is old-primary. □

Exercise (18.63) . — Let $\varphi\colon R \to R'$ be a ring map, and M an R-module. Set $M' := M \otimes_R R'$ and $\alpha := 1_M \otimes \varphi$. Let $N' = \bigcap_{i=1}^{r} Q_i'$ be a decomposition in M' with each Q_i' old-primary. Set $N := \alpha^{-1} N'$ and $Q_i := \alpha^{-1} Q_i'$. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$ and $\mathfrak{p}_i' := \operatorname{nil}(M'/Q_i')$. Show:

(1) Then $N = \bigcap_{i=1}^{r} Q_i$ with Q_i old-primary, and $\mathfrak{p}_i = \varphi^{-1}\mathfrak{p}_i'$ for all i.
(2) Assume R' is flat and $N' = R'\alpha(N)$. Assume $N' \ne \bigcap_{i \ne j} Q_i'$ for all j, but $N = \bigcap_{i=1}^{t} Q_i$ with $t < r$. Fix $t < i \le r$. Then $\mathfrak{p}_i \subset \mathfrak{p}_j$ for some $j \le t$.

Solution: In (1), trivially $N = \bigcap Q_i$. Now. $R'\alpha(Q_i) \subset Q'_i \subsetneqq M'$ for all i, but $R'\alpha(M) = M'$; so $Q_i \subsetneqq M$. Thus (**18.45**) yields (1).

For (2), first assume $N' = R'\alpha(N)$. Then the inclusion $N \hookrightarrow M$ induces a map $N \otimes R' \to M'$ with image N'. Thus (**8.10**) yields $(M/N) \otimes R' = M'/N'$.

Assume R' is flat too. Then every nonzerodivisor on M/N is also a nonzerodivisor on M'/N'. But $\mathfrak{p}'_i \subset \operatorname{z.div}(M'/N')$ by (**18.37**)(6). Hence every $x \in \mathfrak{p}_i$ is a zerodivisor on M/N. Thus $\mathfrak{p}_i \subset \operatorname{z.div}(M/N)$. But $\operatorname{z.div}(M/N) \subset \bigcup_{j=1}^t \mathfrak{p}_j$ by (**18.37**)(5). Thus (**3.12**) yields the desired j. □

Exercise (18.64) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module, $0 = \bigcap Q_i$ a finite decomposition with Q_i old-primary. Set $\mathfrak{p}_i = \operatorname{nil}(M/Q_i)$. Show $\Gamma_{\mathfrak{a}}(M) = \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$. (If $\mathfrak{a} \subset \mathfrak{p}_i$ for all i, then $\bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i = M$ by convention.)

Solution: Given $m \in \Gamma_{\mathfrak{a}}(M)$, recall $\mathfrak{a} \subset \sqrt{\operatorname{Ann}(m)}$ by definition (**4.14**) of $\Gamma_{\mathfrak{a}}(M)$. Given i with $\mathfrak{a} \not\subset \mathfrak{p}_i$, take $a \in \mathfrak{a} - \mathfrak{p}_i$. Then there's $n \geq 0$ with $a^n m = 0$. So $a^n m \in Q_i$. But Q_i is old-primary. So $m \in Q_i$. Thus $m \in \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$.

Conversely, given $m \in \bigcap_{\mathfrak{a}\not\subset\mathfrak{p}_i} Q_i$, let $a \in \mathfrak{a}$. Given j with $\mathfrak{a} \subset \mathfrak{p}_j$, there's n_j with $a^{n_j} m \in Q_j$ as $\mathfrak{p}_j = \operatorname{nil}(M/Q_j)$. Set $n := \max\{n_j\}$. Then $a^n m \in Q_i$ for all i, if $\mathfrak{a} \subset \mathfrak{p}_i$ or not. So $a^n m \in \bigcap Q_i = 0$. Thus $\mathfrak{a} \subset \sqrt{\operatorname{Ann}(m)}$, or $m \in \Gamma_{\mathfrak{a}}(M)$. □

Exercise (18.65) . — Let R be a ring; N, $Q_i \subset M$ modules with Q_i old-primary.

(1) Assume $N = \bigcap_{i=1}^r Q_i$. Set $\mathfrak{p}_i = \operatorname{nil}(M/Q_i)$. Show $N = \bigcap_{i=1}^r \varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i})$.

(2) Assume M/N is Noetherian. Show $\bigcap_{\mathfrak{p}\in\operatorname{Ass}(M/N)} \varphi_{\mathfrak{p}}^{-1}(N_{\mathfrak{p}}) = N$.

Solution: For (1), note $\varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) = N^{S_{\mathfrak{p}_i}}$ by (**12.12**)(3)(a). So by (**18.47**)(1), $\varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) = \bigcap_{\mathfrak{p}_j\subset\mathfrak{p}_i} Q_j$. So $\bigcap_{i=1}^r \varphi_{\mathfrak{p}_i}^{-1}(N_{\mathfrak{p}_i}) = \bigcap_{i=1}^r \bigl(\bigcap_{\mathfrak{p}_j\subset\mathfrak{p}_i} Q_j\bigr) = \bigcap_{i=1}^r Q_i = N$.

For (2), note N has an irredundant primary decomposition $N = Q_1 \cap \cdots Q_r$ by (**18.19**). Say Q_i is $\mathfrak{p}_i$-primary. Then $\operatorname{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ by (**18.18**). So $\mathfrak{p}_i = \operatorname{nil}(M/Q_i)$ and Q_i is old-primary for all i by (**18.3**)(5). Thus (1) yields (2). □

Exercise (18.66) . — Let $\varphi\colon R \to R'$ be a ring map, M' an R'-module, $M \subset M'$ an R-submodule, and $\mathfrak{p} \in \mathcal{D}_R(M)$. Assume $0 = \bigcap_{i=1}^r Q'_i$ with the Q'_i old-primary R'-submodules. Show there's $\mathfrak{p}' \in \mathcal{D}_{R'}(M')$ with $\varphi^{-1}\mathfrak{p}' = \mathfrak{p}$.

Solution: Omit some Q'_i so r is minimal; then $\mathcal{D}_{R'}(M') = \{\mathfrak{p}'_1\}_{i=1}^r$ by (**18.39**)(4).

For all i, set $\mathfrak{p}'_i := \operatorname{nil}(M'/Q'_i)$ and $\mathfrak{p}_i := \varphi^{-1}\mathfrak{p}'_i$ and $Q_i := Q'_i \cap M$. Say $Q_i \supsetneqq M$ just for $i \leq t$. Then $0 = \bigcap_{i=1}^t Q_i$, with Q_i old-primary and $\mathfrak{p}_i = \operatorname{nil}(M/Q_i)$ by (**18.45**). So $\mathcal{D}_R(M) \subset \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$ by (**18.37**)(4). Thus $\mathfrak{p} = \mathfrak{p}_i$ for some i □

Exercise (18.67) . — Let R be a ring, M a module, $0 = \bigcap_{i=1}^n Q_i$ an old-primary decomposition in M. Set $\mathfrak{p}_i := \operatorname{nil}(M/Q_i)$. Assume $\bigcap_{j\neq i} Q_j \neq 0$ for all i, the $\mathfrak{p}_i$ are distinct, M is finitely generated, and $\mathfrak{p}_1$ is finitely generated mod $\operatorname{Ann}(M)$. Show:

(1) Suppose that $\mathfrak{p}_1$ is minimal over $\operatorname{Ann}(M)$. Then $Q_1 = (\mathfrak{p}_1 M)^{(r)}$ for $r \gg 0$.

(2) Suppose that $\mathfrak{p}_1$ is not minimal over $\operatorname{Ann}(M)$. Show that replacing Q_1 by $(\mathfrak{p}_1 M)^{(r)}$ for $r \gg 0$ gives infinitely many distinct old-primary decompositions of 0, still with $\bigcap_{j\neq i} Q_j \neq 0$ for all i and the $\mathfrak{p}_i$ distinct. (Thus, when R is Noetherian, then 0 has infinitely many irredundant primary decompositions, which differ only in the first component.)

Solution: For (1), note that $Q_1 = 0^{S_{\mathfrak{p}_1}}$ by **(18.48)** with $N := 0$ amd $t := 1$. But $0^{S_{\mathfrak{p}_1}} \supset (\mathfrak{p}_1 M)^{(r)}$ for $r \gg 0$ by **(18.58)**(5), and $(\mathfrak{p}_1 M)^{(r)}$ is old-primary for all r by **(18.58)**(2). Now, $0^{S_{\mathfrak{p}_1}}$ is the smallest old-primary submodule Q with $\mathrm{nil}(M/Q) = \mathfrak{p}_1$ by **(18.56)**(1). Thus (1) holds.

For (2), set $\mathfrak{p} := \mathfrak{p}_1$. For a moment, assume $(\mathfrak{p}M)^{(r)} = (\mathfrak{p}M)^{(r+1)}$ for some r, or what's the same, $(\mathfrak{p}^r M)^{S_{\mathfrak{p}}} = (\mathfrak{p}^{r+1} M)^{S_{\mathfrak{p}}}$. Then $\mathfrak{p}^r M_{\mathfrak{p}} = \mathfrak{p}^{r+1} M_{\mathfrak{p}}$ by **(12.12)**(3)(b). Set $A := R_{\mathfrak{p}}$. Then $\mathfrak{p}^{r+1} M_{\mathfrak{p}} = (\mathfrak{p}A)(\mathfrak{p}^r M_{\mathfrak{p}})$. But $\mathfrak{p}^r M_{\mathfrak{p}}$ is finitely generated as $\mathfrak{p}/\operatorname{Ann}(M)$ and M are. So $\mathfrak{p}^r M_{\mathfrak{p}} = 0$ by Nakayama's Lemma. So $\mathfrak{p}^r A \subset \operatorname{Ann}_A(M_{\mathfrak{p}})$. Hence $\mathfrak{p}A$ is minimal over $\operatorname{Ann}_A(M_{\mathfrak{p}})$. Hence $\mathfrak{p}$ is, by **(11.12)**(2), minimal over $\operatorname{Ann}_R(M)$, contrary to hypothesis. Thus the $(\mathfrak{p}M)^{(r)}$ are distinct.

However, $Q_1 \supset (\mathfrak{p}M)^{(r)}$ for $r \gg 0$ by **(18.58)**(5). So $0 = (\mathfrak{p}M)^{(r)} \cap Q_2 \cap \cdots \cap Q_n$. But $(\mathfrak{p}M)^{(r)}$ is old-primary by **(18.58)**(2). Thus replacing Q_1 by $(\mathfrak{p}M)^{(r)}$ for $r \gg 0$ gives infinitely many distinct old-primary decompositions of 0.

Fix r. Note $\mathrm{nil}(M/(\mathfrak{p}M)^{(r)}) = \mathfrak{p}$ by **(18.58)**(2). Thus replacing Q_1 by $(\mathfrak{p}M)^{(r)}$ leaves the $\mathfrak{p}_i$ the same, so still distinct. Moreover, after replacement, if $\bigcap_{j \neq i} Q_j = 0$ for some i, then by **(18.39)**(4), the set of $\mathfrak{p}_j$ for $j \neq i$ would be the same as the set of all $\mathfrak{p}_j$, a contradiction. Thus (2) holds. □

19. Length

Exercise (19.2) . — Let R be a ring, M a module. Prove these statements:

(1) If M is simple, then any nonzero element $m \in M$ generates M.
(2) M is simple if and only if $M \simeq R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and if so, then $\mathfrak{m} = \operatorname{Ann}(M)$.
(3) If M has finite length, then M is finitely generated.

Solution: Obviously, Rm is a nonzero submodule. So it is equal to M, because M is simple. Thus (1) holds.

Assume M is simple. Then M is cyclic by (1). So $M \simeq R/\mathfrak{m}$ for $\mathfrak{m} := \operatorname{Ann}(M)$ by **(4.7)**. Since M is simple, $\mathfrak{m}$ is maximal owing to the bijective correspondence of **(1.9)**. By the same token, if, conversely, $M \simeq R/\mathfrak{m}$ with $\mathfrak{m}$ maximal, then M is simple. Thus (2) holds.

Assume $\ell(M) < \infty$. Let $M = M_0 \supset M_1 \supset \cdots \supset M_m = 0$ be a composition series. If $m = 0$, then $M = 0$. Assume $m \geq 1$. Then M_1 has a composition series of length $m - 1$. So, by induction on m, we may assume M_1 is finitely generated. Further, M/M_1 is simple, so finitely generated by (1). Hence M is finitely generated by **(16.13)**(1). Thus (3) holds. □

Exercise (19.4) . — Let R be a ring, M a Noetherian module. Show that the following three conditions are equivalent:

(1) M has finite length;
(2) $\operatorname{Supp}(M)$ consists entirely of maximal ideals;
(3) $\operatorname{Ass}(M)$ consists entirely of maximal ideals.

Show that, if the conditions hold, then $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ are equal and finite.

Solution: Assume (1). Then **(19.3)** yields (2).

Assume (2). Then **(17.16)** and **(19.2)**(2) yield (1) and (3).

Finally, assume (3). Then **(17.13)** and **(17.14)** imply that $\operatorname{Ass}(M)$ and $\operatorname{Supp}(M)$ are equal and consist entirely of maximal ideals. In particular, (2) holds. However,

$\mathrm{Ass}(M)$ is finite by (**17.17**). Thus the last assertion holds. □

Exercise (19.16) . — Let R be a ring, M a module, Q a $\mathfrak{p}$-primary submodule, and $Q_1 \supsetneqq \cdots \supsetneqq Q_m := Q$ a chain of $\mathfrak{p}$-primary submodules. Set $M' := M/Q$. Assume that M' is Noetherian. Show that $m \le \ell(M'_\mathfrak{p}) < \infty$, and that $m = \ell(M'_\mathfrak{p})$ if and only if m is maximal.

Solution: Given a submodule P of M containing Q, set $P' := P/Q$. Note $M'/P' = M/P$. So P' is $\mathfrak{p}$-primary in M' if and only if P is $\mathfrak{p}$-primary in M. Thus $P \mapsto P'$ is a bijection from the $\mathfrak{p}$-primary submodules of M containing Q onto the $\mathfrak{p}$-primary submodules of M'.

Set $\mathfrak{m} := \mathfrak{p}R_\mathfrak{p}$. Then $P' \mapsto P'_\mathfrak{p}$ is bijective from the $\mathfrak{p}$-primary submodules of M' to the $\mathfrak{m}$-primary submodules of $M'_\mathfrak{p}$ by (**18.20**). Thus $(Q'_1)_\mathfrak{p} \supsetneqq \cdots \supsetneqq (Q'_m)_\mathfrak{p} = 0$ is a chain of $\mathfrak{m}$-primary submodules of $M'_\mathfrak{p}$.

In particular, 0 is $\mathfrak{m}$-primary in $M'_\mathfrak{p}$. So $\mathrm{Ass}_{R_\mathfrak{p}}(M'_\mathfrak{p}) = \{\mathfrak{m}\}$ by definition. But M' is Noetherian by (**16.33**). Thus $\ell(M'_\mathfrak{p}) < \infty$ by (**19.4**). and $m \le \ell(M'_\mathfrak{p})$ by (**19.3**).

Further, $\mathfrak{m}^n M'_\mathfrak{p} = 0$ for some $n \ge 1$ by (**18.5**). So any proper submodule of $M'_\mathfrak{p}$ is $\mathfrak{m}$-primary by (**18.8**)(2). But by (**19.3**), any chain of submodules of $M'_\mathfrak{p}$ can be refined to a composition series, and every composition series is of length $\ell(M'_\mathfrak{p})$. But $(Q'_1)_\mathfrak{p} \supsetneqq \cdots \supsetneqq (Q'_m)_\mathfrak{p} = 0$ is a chain. Thus that chain is a composition series if and only if m is maximal; if so, then $m = \ell(M'_\mathfrak{p})$. □

Exercise (19.17) . — Let k be a field, R an algebra-finite extension. Prove that R is Artinian if and only if R is a finite-dimensional k-vector space.

Solution: As k is Noetherian and as R/k is algebra-finite, R is Noetherian by (**16.10**). Assume R is Artinian. Then $\ell(R) < \infty$ by (**19.5**). So R has a composition series. The successive quotients are isomorphic to residue class fields by (**19.2**)(2). These fields are finitely generated k-algebras, as R is. Hence these fields are finite extension fields of k by the Zariski Nullstellensatz (**15.4**). Thus R is a finite-dimensional k-vector space. The converse holds by (**16.42**). □

Exercise (19.18) . — Given a prime $p \in \mathbb{Z}$, find all four different Artinian rings R with p^2 elements. Which R are $\mathbb{F}_p$-algebras?

Solution: By (**19.11**), $R = \prod_{\mathfrak{m} \in \mathrm{Spec}(R)} R_\mathfrak{m}$. Say $R_\mathfrak{m}$ consists of $n_\mathfrak{m}$ elements. Then $p^2 = \prod n_\mathfrak{m}$. So either there are two $\mathfrak{m}$ and $n_\mathfrak{m} = p$, or there's only one $\mathfrak{m}$. If two, then each $R_\mathfrak{m}$ is equal to its residue field, which must be $\mathbb{F}_p$; thus $R = \mathbb{F}_p \times \mathbb{F}_p$.

So assume R is local with maximal ideal $\mathfrak{m}$. If $\mathfrak{m} = 0$, then $R = \mathbb{F}_{p^2}$.

So assume $\mathfrak{m} \ne 0$. Form the map $\varphi\colon \mathbb{Z} \to R$ with $\varphi(1) = 1$. Say $\mathrm{Ker}(\varphi) = \langle k \rangle$ with $k \ge 0$. Note $0 \ne \mathbb{Z}/\langle k \rangle \hookrightarrow R$, as additive groups. Thus $k = p$ or $k = p^2$.

First, assume $k = p$. Then $\mathbb{F}_p \subset R$. Note $\mathbb{F}_p^\times \bigcap \mathfrak{m} = \emptyset$. Fix a nonzero $x \in \mathfrak{m}$, and a variable X. Form the $\mathbb{F}_p$-algebra map $\psi\colon \mathbb{F}_p[X] \to R$ with $\psi(X) = x$. Then $\mathrm{Im}(\psi)$ is an additive subgroup of R with at least $p+1$ elements. So ψ is surjective. Say $\mathrm{Ker}(\psi) = \langle X^m \rangle$. Then $\mathbb{F}_p[X]/\langle X^m \rangle \xrightarrow{\sim} R$. But R has p^2 elements. So $m = 2$. Thus $R = \mathbb{F}_p[X]/\langle X^2 \rangle$.

Instead, assume $k = p^2$. Then $\mathbb{Z}/\langle p^2 \rangle \subset R$. But both rings have p^2 elements. Thus $R = \mathbb{Z}/\langle p^2 \rangle$. In this case, and only this case, R is not an $\mathbb{F}_p$-algebra. □

Exercise (19.19) . — Let k be a field, A a local k-algebra. Assume the map from k to the residue field is bijective. Given an A-module M, prove $\ell(M) = \dim_k(M)$.

Solution: If $M = 0$, then $\ell(M) = 0$ and $\dim_k(M) = 0$. If $M \simeq k$, then $\ell(M) = 1$ and $\dim_k(M) = 1$. Assume $1 \le \ell(M) < \infty$. Then M has a submodule M' with $M/M' \simeq k$ by **(19.3)**. So Additivity of Length, **(19.7)**, yields $\ell(M') = \ell(M) - 1$ and $\dim_k(M') = \dim_k(M) - 1$. Hence $\ell(M') = \dim_k(M')$ by induction on $\ell(M)$. Thus $\ell(M) = \dim_k(M)$.

If $\ell(M) = \infty$, then for every $m \ge 1$, there exists a chain of submodules,

$$M = M_0 \supsetneqq M_1 \supsetneqq \cdots \supsetneqq M_m = 0.$$

Thus $\dim_k(M) = \infty$. □

Exercise (19.20) . — Prove these conditions on a Noetherian ring R equivalent:

(1) R is Artinian. (2) $\operatorname{Spec}(R)$ is discrete and finite. (3) $\operatorname{Spec}(R)$ is discrete.

Solution: Condition (1) holds, by **(19.8)**, if and only if $\operatorname{Spec}(R)$ consists of finitely points and each is a maximal ideal. But a prime $\mathfrak{p}$ is a maximal ideal if and only if $\{\mathfrak{p}\}$ is closed in $\operatorname{Spec}(R)$ by **(13.16)**(2). It follows that (1) and (2) are equivalent.

Trivially, (2) implies (3). Conversely, (3) implies (2), since $\operatorname{Spec}(R)$ is quasi-compact by **(13.2)**. Thus all three conditions are equivalent. □

Exercise (19.21) . — Let $\varphi\colon R \to R'$ be a map of rings. Assume R' is algebra finite over R. Given $\mathfrak{p} \in \operatorname{Spec}(R)$, set $k := \operatorname{Frac}(R/\mathfrak{p})$. Consider these statements:

(1) The fibers of $\operatorname{Spec}(\varphi)$ are finite.
(2) The fibers of $\operatorname{Spec}(\varphi)$ are discrete.
(3) All $R' \otimes_R k$ are finite-dimensional k-vector spaces.
(4) R' is module finite over R.

Show (1), (2), and (3) are equivalent and follow from (4). Show (4) holds if R' is integral over R. If R' is integral, but not algebra finite, and if (1) holds, does (4)?

Solution: The fiber over $\mathfrak{p} \in \operatorname{Spec}(R)$ is $\operatorname{Spec}(R' \otimes_R k)$ by **(13.28)**(1). But R' is algebra finite over R by hypothesis. So $R' \otimes k$ is algebra finite over k by **(10.39)**(3). So $R' \otimes k$ is Noetherian by **(16.10)**, and it is Jacobson by **(15.7)** or by **(15.37)**(2).

Suppose (1) holds. Since $R' \otimes k$ is Jacobson, each $\mathfrak{q}$ in $\operatorname{Spec}(R' \otimes_R k)$ is the intersection of all the maximal ideals $\mathfrak{m}$ containing $\mathfrak{q}$. But there are only finitely many such $\mathfrak{m}$, as (1) holds. So $\mathfrak{q} = \mathfrak{m}$ for some $\mathfrak{m}$ by **(2.25)**(2). So $\mathfrak{q}$ is closed in $\operatorname{Spec}(R' \otimes_R k)$ by **(13.16)**(2). Thus (2) holds.

Conversely, since each $R' \otimes k$ is Noetherian, (2) implies (1) by **(19.20)**. By the same token, (2) holds if and only if each $R' \otimes k$ is Artinian. But each is algebra finite over k. So each is Artinian if and only if each is a finite dimensional k-vector space by **(19.17)**. Thus (1), (2), and (3) are equivalent.

If (4) holds, then (3) follows owing to **(10.39)**(2).

Since R' is algebra finite over R, if it's integral too, then **(10.18)** yields (4).

Finally, if R' is integral over R, but not algebra finite, then (4) can fail even if (1) holds. For example, take R to be $\mathbb{Q}$ and R' to be the field of algebraic numbers. □

Exercise (19.22) . — Let A be a local ring, $\mathfrak{m}$ its maximal ideal, B a module-finite algebra, and $\{\mathfrak{n}_i\}$ its set of maximal ideals. Show the $\mathfrak{n}_i$ are precisely the primes lying over $\mathfrak{m}$, and $\mathfrak{m}B$ is a parameter ideal of B; conclude B is semilocal.

Solution: Let A' be the image of A in B. Then B is module finite over A', so integral by **(10.18)**(3)⇒(1). So by **(14.3)**(1), each $\mathfrak{n}_i$ lies over a maximal ideal of A', which must be the image $\mathfrak{m}'$ of $\mathfrak{m}$; also, every prime of B lying over $\mathfrak{m}'$ is maximal, so one of the $\mathfrak{n}_i$. Thus the $\mathfrak{n}_i$ are precisely the primes of B lying over $\mathfrak{m}$.

Hence $\mathfrak{m}B \subset \operatorname{rad}(B)$. Moreover, $B/\mathfrak{m}B$ is module finite over $A/\mathfrak{m}$, which is a field; so $B/\mathfrak{m}B$ has finite length. Thus $\mathfrak{m}B$ is a parameter ideal. So **(19.15)**(1) implies B is semilocal. □

Exercise (19.23) . — Let R be an Artinian ring. Show that $\operatorname{rad}(R)$ is nilpotent.

Solution: Set $\mathfrak{m} := \operatorname{rad}(R)$. Then $\mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots$ is a descending chain. So $\mathfrak{m}^r = \mathfrak{m}^{r+1}$ for some r. But R is Noetherian by **(19.8)**. So $\mathfrak{m}$ is finitely generated. Thus Nakayama's Lemma **(10.6)** yields $\mathfrak{m}^r = 0$.

Alternatively, R is Noetherian and $\dim R = 0$ by **(19.8)**. So $\operatorname{rad}(R)$ is finitely generated and $\operatorname{rad}(R) = \operatorname{nil}(R)$. Thus **(3.38)** implies $\mathfrak{m}^r = 0$ for some r. □

Exercise (19.24) . — Find another solution to **(18.67)**(1). Begin by setting $\mathfrak{p} := \mathfrak{p}_1$ and $A := (R/\operatorname{Ann}(M))_{\mathfrak{p}}$ and showing A is Artinian.

Solution: Set $\mathfrak{m} := \mathfrak{p}A$. Then $\mathfrak{m}$ is the only prime of A; moreover, $\mathfrak{m}$ is finitely generated. Thus A is, by **(16.8)**, Noetherian, so by **(19.20)** Artinian.

So $\mathfrak{m}^r = \langle 0\rangle$ for $r \gg 0$ by **(19.23)**. So $\mathfrak{p}^r M_{\mathfrak{p}} = 0$. Set $Q := Q_1$. Then $Q_{\mathfrak{p}} = 0$ by **(18.47)**(1) with $N := 0$ and $t := 1$. So $Q_{\mathfrak{p}} = \mathfrak{p}^r M_{\mathfrak{p}}$. So $Q^{S_{\mathfrak{p}}} = (\mathfrak{p}^r M)^{S_{\mathfrak{p}}}$ by **(12.12)**(3)(a). But $Q^{S_{\mathfrak{p}}} = Q$ by **(18.43)**, and $(\mathfrak{p}^r M)^{S_{\mathfrak{p}}} =: (\mathfrak{p}M)^{(r)}$. Thus $Q = (\mathfrak{p}M)^{(r)}$, as desired. □

Exercise (19.25) . — Let R be a ring, $\mathfrak{p}$ a prime ideal, and R' a module-finite R-algebra. Show that R' has only finitely many primes $\mathfrak{p}'$ over $\mathfrak{p}$, as follows: reduce to the case that R is a field by localizing at $\mathfrak{p}$ and passing to the residue rings.

Solution: First note that, if $\mathfrak{p}' \subset R'$ is a prime lying over $\mathfrak{p}$, then $\mathfrak{p}'R'_{\mathfrak{p}} \subset R'_{\mathfrak{p}}$ is a prime lying over the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. Hence, by **(11.12)**(2), it suffices to show that $R'_{\mathfrak{p}}$ has only finitely many such primes. Note also that $R'_{\mathfrak{p}}$ is module finite over $R_{\mathfrak{p}}$. Hence we may replace R and R' by $R_{\mathfrak{p}}$ and $R'_{\mathfrak{p}}$, and thus assume that $\mathfrak{p}$ is the unique maximal ideal of R. Similarly, we may replace R and R' by $R/\mathfrak{p}$ and $R'/\mathfrak{p}R'$, and thus assume that R is a field.

There are a couple of ways to finish. First, R' is now Artinian by **(19.10)** or by **(16.42)**; thus, R' has only finitely many primes by **(19.8)**. Alternatively, every prime is now minimal by incomparability **(14.3)**(2). Further, R' is Noetherian by **(16.10)**. Thus R' has only finitely many minimal primes by **(17.29)**. □

Exercise (19.26) . — Let R be a ring, and M a Noetherian module. Show the following four conditions are equivalent:

(1) M has finite length;
(2) M is annihilated by some finite product of maximal ideals $\prod \mathfrak{m}_i$;
(3) every prime $\mathfrak{p}$ containing $\operatorname{Ann}(M)$ is maximal;
(4) $R/\operatorname{Ann}(M)$ is Artinian.

Solution: Assume (1). Let $M = M_0 \supset \cdots \supset M_m = 0$ be a composition series; set $\mathfrak{m}_i := \operatorname{Ann}(M_{i-1}/M_i)$. Then $\mathfrak{m}_i$ is maximal by **(19.2)**(2). Also, $\mathfrak{m}_i M_{i-1} \subset M_i$. Hence $\mathfrak{m}_i \cdots \mathfrak{m}_1 M_0 \subset M_i$. Thus (2) holds.

Assume (2). Let $\mathfrak{p}$ be a prime containing $\operatorname{Ann}(M)$. Then $\mathfrak{p} \supset \prod \mathfrak{m}_i$. So $\mathfrak{p} \supset \mathfrak{m}_i$

for some i [[by (**2.25**)(1). So $\mathfrak{p} = \mathfrak{m}_i$ as $\mathfrak{m}_i$ is maximal. Thus (3) holds.

Assume (3). Then $\dim(R/\mathrm{Ann}(M)) = 0$. But as M is Noetherian, (**16.16**) implies $R/\mathrm{Ann}(M)$ is Noetherian. Thus (**19.8**) yields (4).

If (4) holds, then (**19.9**) yields (1), because M is a finitely generated module over $R/\operatorname{Ann}(M)$. □

Exercise (19.27) . — (1) Prove that a finite product rings $R := \prod_{i=1}^r R_i$ is a PIR if and only if each R_i is a PIR.

(2) Using a primary decomposition of $\langle 0\rangle$ and (**18.27**), prove that a PIR R is uniquely a finite product of PIDs and Artinian local PIRs.

Solution: For (1), note that, given ideals $\mathfrak{a}_i$ of R_i, their product $\mathfrak{a} := \prod \mathfrak{a}_i$ is an ideal of R. Conversely, every ideal $\mathfrak{a}$ of R is of that form by (**1.23**) and induction on r. Plainly, $x := (x_1, \ldots, x_n)$ generates $\mathfrak{a}$ if and only if x_i generates $\mathfrak{a}_i$ for all i. Thus R is a PIR if and only if each R_i is, as desired.

For (2), note R is Noetherian. So by (**18.19**), there's an irredundant primary decomposition $\langle 0\rangle = \bigcap_{i=1}^r \mathfrak{q}_i$, Set $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.

Suppose $\mathfrak{p}_i \subsetneqq \mathfrak{p}_j$. Then $\mathfrak{p}_i = \mathfrak{q}_i$ by (**18.27**)(2). But $\mathfrak{p}_i \subset \mathfrak{q}_j$ by (**18.27**)(1). So $\mathfrak{q}_i \subset \mathfrak{q}_j$, contradicting irredundancy. Thus $\mathfrak{p}_i \not\subset \mathfrak{p}_j$ for all $i \neq j$.

Hence the $\mathfrak{p}_i$ are pairwise comaximal by (**18.27**)(4). So for any $n_i \geq 1$, the $\mathfrak{p}_i^{n_i}$ are pairwise comaximal by (**1.21**)(3). But $\mathfrak{q}_i \supset \mathfrak{p}_i^{n_i}$ for some $n_i \geq 1$ by (**3.40**). So the $\mathfrak{q}_i$ are pairwise comaximal. So $\langle 0\rangle = \prod_{i=1}^r \mathfrak{q}_i$ by (**1.21**)(4)(b). Thus (**1.21**)(4)(c) yields $R \xrightarrow{\sim} \prod_{i=1}^r (R/\mathfrak{q}_i)$.

As R is a PIR, so is each $R/\mathfrak{q}_i$. If $\mathfrak{p}_i$ is not maximal, then $\mathfrak{p}_i = \mathfrak{q}_i$ by (**18.27**)(2), and thus $R/\mathfrak{q}_i$ is a domain. Else, $\mathfrak{p}_i/\mathfrak{q}_i$ is maximal in $R/\mathfrak{q}_i$. But $\mathfrak{q}_i \supset \mathfrak{p}_i^{n_i}$. Hence $\mathfrak{p}_i/\mathfrak{q}_i$ lies in any prime of $R/\mathfrak{q}_i$, and so is the only prime. Thus $R/\mathfrak{q}_i$ is local, and by (**19.8**), Artinian. Thus R is a finite product of PIDs and Artinian local PIRs.

As to uniqueness, suppose $R \simeq \prod_{i=i}^s R_i$ where R_i is a PID or an Artinian local PIR. Let $\pi_i\colon R \to R_i$ be the projection, and set $\mathfrak{q}_i' := \pi_i^{-1}\langle 0\rangle$. Then an adaptaion of the solution to (**18.31**) shows that $\langle 0\rangle = \bigcap_{i=1}^s \mathfrak{q}_i'$ is an irredundant primary decomposition and that $\mathfrak{q}_i'$ is $\mathfrak{p}_i'$-primary where $\mathfrak{p}_i' := \pi_i^{-1}\operatorname{nil}(R_i)$. So the $\mathfrak{p}_i'$ are minimal. So the $\mathfrak{p}_i'$ and the $\mathfrak{q}_i'$ are uniquely determined by (**18.18**) and (**18.22**). But $R/\mathfrak{q}_i' \xrightarrow{\sim} R_i$ for all i. Thus R is a finite product of PIDs and Artinian local PIRs in one and only one way. □

Exercise (19.28) . — Let A be a local Artinian ring, $\mathfrak{m}$ its maximal ideal, B an algebra, N an A-flat B-module of finite length. Show $\ell_B(N) = \ell_A(A)\cdot\ell_B(N/\mathfrak{m}N)$.

Solution: By (**19.10**) there is a composition series $A = \mathfrak{a}_0 \supset \cdots \supset \mathfrak{a}_r = 0$. It yields $N = \mathfrak{a}_0 N \supset \cdots \supset \mathfrak{a}_r N = 0$. But N is A-flat, so $\mathfrak{a}_i N = \mathfrak{a}_i \otimes N$ by (**9.15**). Hence $\mathfrak{a}_{i-1}N/\mathfrak{a}_i N = (\mathfrak{a}_{i-1}/\mathfrak{a}_i) \otimes N$ by (**8.10**). But $\mathfrak{a}_{i-1}/\mathfrak{a}_i \simeq A/\mathfrak{m}$, and $(A/\mathfrak{m}) \otimes N = N/\mathfrak{m}N$ by (**8.27**)(1). Hence $\ell_B(N) = r \cdot \ell_B(N/\mathfrak{m}N)$ by repeated use of (**19.7**). But $r = \ell_A(A)$ by (**19.3**). Thus the asserted formula holds. □

Exercise (19.29) . — Let R be a decomposable ring; say $R := \prod R_i$ with R_i local. Let $\mathfrak{q}_i$ be a parameter ideal of R_i for each i. Set $\mathfrak{q} := \prod \mathfrak{q}_i$. Show that $\mathfrak{q}$ is a parameter ideal of R. Conclude that R has a parameter ideal.

Solution: Note $R/\mathfrak{q} = \prod R_i/\mathfrak{q}_i$ by (**1.23**). So $\ell(R/\mathfrak{q}) = \sum \ell(R_i/\mathfrak{q}_i)$ by (**19.7**). But $\ell(R_i/\mathfrak{q}_i) < \infty$ for all i. Thus $\ell(R/\mathfrak{q}) < \infty$.

Let $\mathfrak{m}_i$ be the maximal ideal of R_i. Then $\mathfrak{q}_i \subset \mathfrak{m}_i$. But the $\mathfrak{m}_i \times \prod_{j\neq i} R_j$ are all the maximal ideals of R by **(2.29)**. So $\mathfrak{q} \subset \mathrm{rad}(R)$. Thus $\mathfrak{q}$ is a parameter ideal.

Plainly, $\mathfrak{m}_i$ is a parameter ideal of R_i. Thus, $\prod \mathfrak{m}_i$ is a parameter ideal of R. □

Exercise (19.30) . — Let R be a ring, $\mathfrak{a} \subset \mathrm{nil}(R)$ an ideal. Set $R' := R/\mathfrak{a}$. Use **(19.15)**(3) to reprove **(13.23)**(1) ⇔ (2): R is decomposable if and only if R' is.

Solution: If $R = \prod R_i$, then $R/\mathfrak{a} = \prod R_i/\mathfrak{a}_i$ for suitable ideals $\mathfrak{a}_i \subset R_i$ by **(1.23)**. Thus if R is decomposable, then plainly R' is too.

Conversely, assume R' decomposable. By **(19.29)**, R' has a parameter ideal, say $\mathfrak{q}'$ with preimage $\mathfrak{q} \subset R$. Then $R/\mathfrak{q} = R'/\mathfrak{q}'$. So $\ell_R(R/\mathfrak{q}) = \ell_{R'}(R'/\mathfrak{q}') < \infty$. Also $\mathfrak{q} \subset \mathrm{rad}(R)$ as $\mathfrak{q}' \subset \mathrm{rad}(R')$ and $\mathfrak{a} \subset \mathrm{nil}(R) \subset \mathrm{rad}(R)$. Thus $\mathfrak{q}$ is a parameter ideal.

By **(3.36)**, $\mathrm{Idem}(R) \to \mathrm{Idem}(R')$ is bijective. And $\mathrm{Idem}(R') \to \mathrm{Idem}(R'/\mathfrak{q}')$ is so by **(19.15)**(3). Hence $\mathrm{Idem}(R) \to \mathrm{Idem}(R/\mathfrak{q})$ is bijective. Thus **(19.15)**(3) implies R is decomposable. □

20. Hilbert Functions

Exercise (20.14) . — Let k be a field, $k[X,Y]$ the polynomial ring. Show $\langle X, Y^2\rangle$ and $\langle X^2, Y^2\rangle$ have different Hilbert Series, but the same Hilbert Polynomial.

Solution: Set $\mathfrak{m} := \langle X, Y\rangle$ and $\mathfrak{a} := \langle X, Y^2\rangle$ and $\mathfrak{b} := \langle X^2, Y^2\rangle$. They are graded by degree. So $\ell(\mathfrak{a}_1) = 1$, and $\ell(\mathfrak{a}_n) = \ell(\mathfrak{m}_n)$ for all $n \ge 2$. Further, $\ell(\mathfrak{b}_1) = 0$, $\ell(\mathfrak{b}_2) = 2$, and $\ell(\mathfrak{b}_n) = \ell(\mathfrak{m}_n)$ for $n \ge 3$. Thus the three ideals have the same Hilbert Polynomial, namely $h(n) = n+1$, but different Hilbert Series. □

Exercise (20.15) . — Let k be a field, $P := k[X,Y,Z]$ the polynomial ring in three variables, $F \in P$ a homogeneous polynomial of degree $d \ge 1$. Set $R := P/\langle F\rangle$. Find the coefficients of the Hilbert Polynomial $h(R,n)$ explicitly in terms of d.

Solution: Clearly, the following sequence is exact:

$$0 \to P(-d) \xrightarrow{\mu_F} P \to R \to 0.$$

Hence, Additivity of Length, **(19.7)**, yields $h(R,n) = h(P,n) - h(P(-d),n)$. But $P(-d)_n = P(n-d)$, so $h(P(-d),n) = h(P, n-d)$. Therefore, **(20.4)** yields

$$h(R,n) = \binom{2+n}{2} - \binom{2-d+n}{2} = dn - (d-3)d/2. \qquad \square$$

Exercise (20.16) . — Let K be a field, $X_1, \dots, X_r$ variables, $k_1, \dots, k_r$ positive integers. Set $R := K[X_1, \dots, X_r]$, and define a grading on R by $\deg(X_i) := k_i$. Set $q_r(t) := \prod_{i=1}^r (1 - t^{k_i}) \in \mathbb{Z}[t]$. Show $H(R,\, t) = 1/q_r(t)$.

Solution: Induct on r. If $r = 0$, then $q_r(t) = 1$, and $H(R,\, t) = 1$ as $R = K$.

Assume $r \ge 1$. Set $R' := K[X_1, \dots, X_{r-1}]$. Note $R' = R/\langle X_r\rangle$ by **(1.17)**(3). Furthermore, R is a domain by **(2.4)**. Hence the following sequence is exact:

$$0 \to R(-k_r) \xrightarrow{\mu_{X_r}} R \to R' \to 0$$

So $H(R,t) - H(R(-k_1), t) = H(R', t)$. By induction, $H(R',\, t) = 1/q_{r-1}(t)$. So $(1 - t^{k_r})H(R,t) = 1/q_{r-1}(t)$ by **(20.3.1)**. Thus $H(R,t) = 1/q_r(t)$. □

Exercise (20.17) . — Under the conditions of **(20.6)**, assume there is a homogeneous nonzerodivisor $f \in R$ with $M_f = 0$. Prove $\deg h(R,n) > \deg h(M,n)$; start with the case $M := R/\langle f^k\rangle$.

Solution: Suppose $M := R/\langle f^k\rangle$. Set $c := k\deg f$. Form the exact sequence $0 \to R(-c) \xrightarrow{\mu} R \to M \to 0$ where μ is multiplication by f^k. Then Additivity of Length **(19.7)** yields $h(M,n) = h(R,n) - h(R,n-c)$. But

$$h(R,n) = \tfrac{e(1)}{(d-1)!}n^{d-1} + \cdots \quad \text{and} \quad h(R,n-c) = \tfrac{e(1)}{(d-1)!}(n-c)^{d-1} + \cdots .$$

by **(20.6)**. Thus $\deg h(R,n) > \deg h(M,n)$.

In the general case, there is k with $f^kM = 0$ by **(12.17)**(2). Set $M' := R/\langle f^k\rangle$. Then generators $m_i \in M_{c_i}$ for $1 \le i \le r$ yield a surjection $\bigoplus_i M'(-c_i) \twoheadrightarrow M$. Hence $\sum_i \ell(M'_{n-c_i}) \ge \ell(M_n)$ for all n. But $\deg h(M'(-c_i),n) = \deg h(M',n)$. Hence $\deg h(M',n) \ge \deg h(M,n)$. But $\deg h(R,n) > \deg h(M',n)$ by the first case. Thus $\deg h(R,n) > \deg h(M,n)$. □

Exercise (20.18) . — Let R be a ring, $\mathfrak{q}$ an ideal, and M a Noetherian module. Assume $\ell(M/\mathfrak{q}M) < \infty$. Set $\mathfrak{m} := \sqrt{\mathfrak{q}}$. Show

$$\deg p_{\mathfrak{m}}(M,n) = \deg p_{\mathfrak{q}}(M,n).$$

Solution: Set $\mathfrak{a} := \mathrm{Ann}(M)$ and set $R' := R/\mathfrak{a}$. Set $\mathfrak{q}' := (\mathfrak{q}+\mathfrak{a})/\mathfrak{a}$ and set $\mathfrak{m}' := (\mathfrak{m}+\mathfrak{a})/\mathfrak{a}$. Then $\mathfrak{m}' = \sqrt{\mathfrak{q}'}$ by **(3.39)**(1). Moreover, M is a Noetherian R'-module and $\ell(M/\mathfrak{q}^nM) = \ell(M/\mathfrak{q}'^nM)$ for all n. So $p_{\mathfrak{q}}(M,n) = p_{\mathfrak{q}'}(M,n)$ and similarly $p_{\mathfrak{m}}(M,n) = p_{\mathfrak{m}'}(M,n)$. Thus we may replace R by R' and owing to **(16.16)** assume R is Noetherian.

There is an m such that $\mathfrak{m} \supset \mathfrak{q} \supset \mathfrak{m}^m$ by **(3.38)**. Hence

$$\mathfrak{m}^nM \supset \mathfrak{q}^nM \supset \mathfrak{m}^{mn}M$$

for all $n \ge 0$. Dividing into M and extracting lengths yields

$$\ell(M/\mathfrak{m}^nM) \le \ell(M/\mathfrak{q}^nM) \le \ell(M/\mathfrak{m}^{mn}M).$$

Therefore, for large n, we get

$$p_{\mathfrak{m}}(M,n) \le p_{\mathfrak{q}}(M,n) \le p_{\mathfrak{m}}(M,nm).$$

The two extremes are polynomials in n of the same degree, say d, (but not the same leading coefficient). Dividing by n^d and letting $n \to \infty$, we conclude that the polynomial $p_{\mathfrak{q}}(M,n)$ also has degree d, as desired.. □

Exercise (20.19) . — In the setup of **(20.10)**, prove these two formulas:

$$(1)\ \ e(\mathfrak{q},M) = \lim_{n\to\infty} d!\,\ell(M/\mathfrak{q}^nM)/n^d \quad \text{and} \quad (2)\ \ e(\mathfrak{q}^k,M) = k^d e(\mathfrak{q},M).$$

Solution: For (1), recall from Definition **(20.11)** that $e(\mathfrak{q},M)/d!$ is the leading coefficient of the polynomial $p_{\mathfrak{q}}(M,n)$ of degree d. Thus **(20.10.2)** yields (1).

Derive (2) from (1) as follows:

$$\begin{aligned} e(\mathfrak{q}^kM) &= \lim_{n\to\infty} d!\,\ell(M/\mathfrak{q}^{kn}M)/n^d \\ &= k^d \lim_{n\to\infty} d!\,\ell(M/\mathfrak{q}^{kn}M)/(kn)^d = k^d e(\mathfrak{q},M). \end{aligned}$$ □

Exercise (20.20) . — Let R be a ring, $\mathfrak{q} \subset \mathfrak{q}'$ nested ideals, and M a Noetherian module. Assume $\ell(M/\mathfrak{q}M) < \infty$. Prove these two statements:

(1) Then $e(\mathfrak{q}',M) \le e(\mathfrak{q},M)$, with equality if the $\mathfrak{q}'$-adic filtration is $\mathfrak{q}$-stable.

(2) Assume $\ell(M) < \infty$ and $\mathfrak{q} \subset \mathrm{rad}(M)$. Then $e(\mathfrak{q},M) = \ell(M)$.

Solution: For (1), consider the surjection $M/\mathfrak{q}^nM \twoheadrightarrow M/\mathfrak{q}'^nM$ for each $n \ge 0$. It yields $p_{\mathfrak{q}}(M,n) \ge p_{\mathfrak{q}'}(M,n)$ for $n \gg 0$. Thus $e(\mathfrak{q},M) \ge e(\mathfrak{q}',M)$. If the $\mathfrak{q}'$-adic filtration is $\mathfrak{q}$-stable, then $e(\mathfrak{q},M) = e(\mathfrak{q}',M)$ by **(20.11)**. Thus (1) holds

In (2), M is Artinian by **(19.5)**. So $M \supset \mathfrak{q}M \supset \mathfrak{q}^2M \supset \cdots$ stabilizes. Say $\mathfrak{q}^mM = \mathfrak{q}^{m+1}M$. But $\mathfrak{q}^mM$ is Noetherian as M is. Also, $\mathrm{Ann}(\mathfrak{q}^mM) \supset \mathrm{Ann}(M)$; so $\mathrm{rad}(\mathfrak{q}^mM) \supset \mathrm{rad}(M) \supset \mathfrak{q}$. So $\mathfrak{q}^mM = 0$ by Nakayama's Lemma **(10.6)**. So $\ell(M) = \ell(M/\mathfrak{q}^nM)$ for $n \gg 0$. So $p_{\mathfrak{q}}(M,n) = \ell(M)$. Thus (2) holds. □

Exercise (20.21) . — Let R be a ring, $\mathfrak{q}$ an ideal, and M a Noetherian module with $\ell(M/\mathfrak{q}M) < \infty$. Set $S := \mathrm{Supp}(M) \cap \mathbf{V}(\mathfrak{q})$. Set $d := \max_{\mathfrak{m}\in S} \dim(M_{\mathfrak{m}})$ and $\Lambda := \{\mathfrak{m} \in S \mid \dim(M_{\mathfrak{m}}) = d$. Show

$$e(\mathfrak{q},M) = \textstyle\sum_{\mathfrak{m}\in\Lambda} e(\mathfrak{q}R_{\mathfrak{m}}, M_{\mathfrak{m}}). \qquad \textbf{(20.21.1)}$$

Solution: Given $n \ge 0$, recall $\mathbf{V}(\mathfrak{q}) = \mathbf{V}(\mathfrak{q}^n)$ from **(13.1)**. So **(13.46)**(1) yields $S = \mathrm{Supp}(M/\mathfrak{q}^nM)$. So **(19.3.1)** yields

$$M/\mathfrak{q}^nM \xrightarrow{\sim} \textstyle\prod_{\mathfrak{m}\in S} M_{\mathfrak{m}}/\mathfrak{q}^nM_{\mathfrak{m}}.$$

Hence $\ell(M/\mathfrak{q}^nM) = \sum \ell(M_{\mathfrak{m}}/\mathfrak{q}^nM_{\mathfrak{m}})$ owing to **(19.7)**. Hence

$$p_{\mathfrak{q}}(M,n) = \textstyle\sum_{\mathfrak{m}\in S} p_{\mathfrak{q}R_{\mathfrak{m}}}(M_{\mathfrak{m}},n).$$

The terms of degree d are positive, so can't cancel. Thus **(20.21.1)** holds. □

Exercise (20.22) . — Derive the Krull Intersection Theorem, **(18.23)**, from the Artin–Rees Lemma, **(20.12)**.

Solution: In the notation of **(18.23)**, by **(10.3)** we must prove $N = \mathfrak{a}N$. So apply **(20.12)** to N and the $\mathfrak{a}$-adic filtration of M; thus we get an m such that $\mathfrak{a}(N \cap \mathfrak{a}^mM) = N \cap \mathfrak{a}^{m+1}M$. But $N \cap \mathfrak{a}^nM = N$ for all $n \ge 0$. Thus $N = \mathfrak{a}N$. □

20. Appendix: Homogeneity

Exercise (20.25) . — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, and M a graded module. Show that $\sqrt{\mathfrak{a}}$ and $\mathrm{Ann}(M)$ and $\mathrm{nil}(M)$ are homogeneous.

Solution: Take $x := \sum_{i\ge r}^{r+n} x_i \in R$ with the x_i the homogeneous components.

First, suppose $x \in \sqrt{\mathfrak{a}}$. Say $x^k \in \mathfrak{a}$. Either x_r^k vanishes or it is the initial component of x^k. But $\mathfrak{a}$ is homogeneous. So $x_r^k \in \mathfrak{a}$. So $x_r \in \sqrt{\mathfrak{a}}$. So $x - x_r \in \sqrt{\mathfrak{a}}$ by **(3.15)**. So all the x_i are in $\sqrt{\mathfrak{a}}$ by induction on n. Thus $\sqrt{\mathfrak{a}}$ is homogeneous.

Second, suppose $x \in \mathrm{Ann}(M)$. Let $m \in M$. Then $0 = xm = \sum x_im$. If m is homogeneous, then $x_im = 0$ for all i, since M is graded. But M has a set of homogeneous generators. Thus $x_i \in \mathrm{Ann}(M)$ for all i, as desired.

Finally, $\mathrm{nil}(M)$ is homogeneous, as $\mathrm{nil}(M) = \sqrt{\mathrm{Ann}(M)}$ by **(12.22)**. □

Exercise (20.26) . — Let R be a graded ring, M a graded module, and Q an old-primary submodule. Let $Q^* \subset Q$ be the submodule generated by the homogeneous elements of Q. Show that Q^* is old-primary.

Solution: Let $x \in R$ and $m \in M$ be homogeneous with $xm \in Q^*$. Assume $x \notin \mathrm{nil}(M/Q^*)$. Then, given $\ell \ge 1$, there is $m' \in M$ with $x^\ell m' \notin Q^*$. So m' has a homogeneous component m'' with $x^\ell m'' \notin Q^*$. Then $x^\ell m'' \notin Q$ by definition of Q^*. Thus $x \notin \mathrm{nil}(M/Q)$. Since Q is old-primary, $m \in Q$. Since m is homogeneous, $m \in Q^*$. Thus Q^* is old-primary by **(20.24)**. □

Exercise (20.30) (*Nakayama's Lemma for a graded module*) . — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, M a graded module. Assume $\mathfrak{a} = \sum_{i \ge i_0} \mathfrak{a}_i$ with $i_0 > 0$ and $M = \sum_{n \ge n_0} M_n$ for some n_0. Assume $\mathfrak{a}M = M$. Show $M = 0$.

Solution: Assume $M \ne 0$. Then there is a minimal n_0 with $M_{n_0} \ne 0$. But $\mathfrak{a}M \subset \sum_{n \ge i_0 + n_0} M_n$ and $i_0 > 0$. So $M_{n_0} \not\subset \mathfrak{a}M$, a contradiction. Thus $M = 0$. □

Exercise (20.31) (*Homogeneous prime avoidance*) . — Let R be a graded ring, $\mathfrak{a}$ a homogeneous ideal, $\mathfrak{a}^\flat$ its subset of homogeneous elements, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ primes. Adapt the method of (3.12) to prove the following assertions:

(1) If $\mathfrak{a}^\flat \not\subset \mathfrak{p}_j$ for all j, then there is $x \in \mathfrak{a}^\flat$ such that $x \notin \mathfrak{p}_j$ for all j.

(2) If $\mathfrak{a}^\flat \subset \bigcup_{i=1}^n \mathfrak{p}_i$, then $\mathfrak{a} \subset \mathfrak{p}_i$ for some i.

Solution: For (1), proceed by induction on n. If $n = 1$, the assertion is trivial. Assume that $n \ge 2$ and by induction that, for every i, there is an $x_i \in \mathfrak{a}^\flat$ such that $x_i \notin \mathfrak{p}_j$ for all $j \ne i$. Set $d_i := \deg(x_i)$, set $y_n := x_n^{d_1 + \cdots + d_{n-1}}$, and set $y_i := x_i^{d_n}$ for $i < n$. Then $y_i \notin \mathfrak{p}_j$ for $i \ne j$. We may assume $y_i \in \mathfrak{p}_i$ for each i else we're done. Set $x := (y_1 \cdots y_{n-1}) + y_n$. Then $x \in \mathfrak{a}$ and is homogeneous of degree $(d_1 + \cdots + d_{n-1})d_n$. So $x \in \mathfrak{a}^\flat$. But $x \notin \mathfrak{p}_j$ as, if $j = n$, then $y_n \in \mathfrak{p}_n$ and $\mathfrak{p}_n$ is prime, and if $j < n$, then $y_n \notin \mathfrak{p}_j$ and $y_j \in \mathfrak{p}_j$. Thus (1) holds.

Assertion (2) is equivalent to (1), since $\mathfrak{a}$ is homogeneous, so generated by $\mathfrak{a}^\flat$. □

Exercise (20.32) . — Let $R = \bigoplus R_n$ be a graded ring, $M = \bigoplus M_n$ a graded module, $N = \bigoplus N_n$ a homogeneous submodule. Assume M/N is Noetherian. Set

$$N' := \{\, m \in M \mid R_n m \in N \text{ for all } n \gg 0 \,\}.$$

(1) Show that N' is the largest homogeneous submodule of M containing N and having, for all $n \gg 0$, its degree-n homogeneous component N'_n equal to N_n.

(2) Let $N = \bigcap Q_i$ be a primary decomposition. Say Q_i is $\mathfrak{p}_i$-primary. Set $R_+ := \bigoplus_{n>0} R_n$. Show that $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$.

Solution: In (1), plainly N' is a submodule containing N. Given $m \in N'$, let m_i be a homogeneous component. As $R_n m \in N$ for all $n \gg 0$ and as N is homogeneous, $R_n m_i \in N$ for all $n \gg 0$. So $m_i \in N'$. Thus N' is homogeneous.

Plainly, to check the rest of (1), we may replace M by M/N. Thus we may assume M is Noetherian and $N = 0$.

As M is Noetherian, N' is finitely generated, say by $g_1, \ldots, g_r$. Replacing the g_i by all their homogeneous components, we may assume each g_i is homogeneous, say of degree d_i. Set $d := \max d_i$. Also, say $R_n g_i = 0$ for $n \ge \nu$ and for all i.

Set $k := \nu + d$. Given $m \in N'_n$ with $n \ge k$, say $m = \sum x_i g_i$ with $x_i \in R_{n-d_i}$. Then $n - d_i \ge k - d =: \nu$. So $x_i g_i = 0$. So $m = 0$. Thus $N'_n = 0$ for $n \ge k$.

Let $N'' \subset M$ be homogeneous with $N''_n = 0$ for $n \ge k'$. Given p and $m \in N''_p$, note $R_n m \in N''_{n+p}$; so $R_n m = 0$ for $n \ge k'$. Thus $N'' \subset N'$. Thus (1) holds.

For (2), note $0 = \bigcap (Q_i/N)$ in M/N. By (18.64),

$$\Gamma_{R_+}(M/N) = \bigcap_{\mathfrak{p}_i \not\supset R_+} (Q_i/N).$$

But $\Gamma_{R_+}(M/N) = N'/N$ by definition (4.14). Thus $N' = \bigcap_{\mathfrak{p}_i \not\supset R_+} Q_i$. □

Exercise (20.33) . — Under the conditions of (20.6), assume R is a domain whose integral closure $\overline{R}$ in $\operatorname{Frac}(R)$ is module finite (see (24.18)). Prove the following:

(1) There is a homogeneous $f \in R$ with $R_f = \overline{R}_f$.
(2) The Hilbert Polynomials of R and $\overline{R}$ have the same degree and same leading coefficient.

Solution: By (**20.29**), $\overline{R}$ is a graded R-algebra. But $\overline{R}$ is module finite. So there are finitely many homogeneous generators $x_1, \ldots, x_r$ of $\overline{R}$ as an R-module. Say $x_i = a_i/b_i$ with $a_i, b_i \in R$ homogeneous. Set $f := \prod b_i$. Then $fx_i \in R$ for each i. So $\overline{R}_f = R_f$. Thus (1) holds.

Consider the short exact sequence $0 \to R \to \overline{R} \to \overline{R}/R \to 0$. Then $(\overline{R}/R)_f = 0$ by (**12.13**). So $\deg h(\overline{R}/R, n) < \deg h(\overline{R}, n)$ by (**20.17**) and (1). But

$$h(\overline{R}, n) = h(R, n) + h(\overline{R}/R, n)$$

by (**19.7**) and (**20.6**). Thus (2) holds. □

Exercise (20.34) . — Let $R = \bigoplus R_n$ be a graded ring with R_0 Artinian. Assume $R = R_0[x_1, \ldots, x_r]$ with $x_i \in R_{k_i}$ and $k_i \ge 1$. Set $q(t) := \prod_{i=1}^{r}(1-t^{k_i})$. Let $\mathcal{C}$ be the subcategory of $((R\text{-mod}))$ of all finitely generated *graded* R-modules $M = \bigoplus M_n$ and all homogeneous maps of degree 0; let $\mathcal{C}_0$ be its subcategory of all M with $M_n = 0$ for all $n < 0$. Using the notation of (**17.34**), let $\lambda_0\colon K_0(R_0) \to \mathbb{Z}$ be a $\mathbb{Z}$-map. Show that assigning to each $M \in \mathcal{C}$ the series $\sum_{n\in\mathbb{Z}} \lambda_0(\gamma_0(M_n))t^n$ gives rise to $\mathbb{Z}$-maps $K(\mathcal{C}) \to (1/q(t))\mathbb{Z}[t, 1/t]$ and $K(\mathcal{C}_0) \to (1/q(t))\mathbb{Z}[t]$.

Solution: Replacing ℓ by $\lambda_0\gamma_0$ in the proof of (**20.5**) shows $\sum_{n\in\mathbb{Z}} \lambda_0(\gamma_0(M_n))t^n$ lies in $(1/q(t))\mathbb{Z}[t, 1/t]$ for each $M \in \mathcal{C}$ and lies in $(1/q(t))\mathbb{Z}[t]$ if $M_n = 0$ for all $n < 0$. Now, a sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ in $\mathcal{C}$ with $M_i = \bigoplus M_{in}$ is exact (if and) only if each sequence $0 \to M_{1n} \to M_{2n} \to M_{3n} \to 0$ is exact. Thus (**17.34**)(1) yields the assertion. □

21. Dimension

Exercise (21.10) . — (1) Let A be a Noetherian local ring with a principal prime $\mathfrak{p}$ of height at least 1. Prove A is a domain by showing any prime $\mathfrak{q} \subsetneqq \mathfrak{p}$ is $\langle 0\rangle$.

(2) Let k be a field, $P := k[[X]]$ the formal power series ring in one variable. Set $R := P \times P$. Prove that R is Noetherian and semilocal, and that R contains a principal prime $\mathfrak{p}$ of height 1, but that R is not a domain.

Solution: To prove (1), say $\mathfrak{p} = \langle x\rangle$. Take $y \in \mathfrak{q}$. Then $y = ax$ for some a. But $x \notin \mathfrak{q}$ since $\mathfrak{q} \subsetneqq \mathfrak{p}$. Hence $a \in \mathfrak{q}$. Thus $\mathfrak{q} = \mathfrak{q}x$. But x lies in the maximal ideal of the local ring A, and $\mathfrak{q}$ is finitely generated since A is Noetherian. Hence Nakayama's Lemma (**10.6**) yields $\mathfrak{q} = \langle 0\rangle$. Thus $\langle 0\rangle$ is prime, and so A is a domain.

Alternatively, as $a \in \mathfrak{q}$, also $a = a_1x$ with $a_1 \in \mathfrak{q}$. Repeating yields an ascending chain of ideals $\langle a\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \cdots$. It stabilizes as A is Noetherian: there's a k such that $a_k \in \langle a_{k-1}\rangle$. Then $a_k = ba_{k-1} = ba_kx$ for some b. So $a_k(1-bx) = 0$. But $1 - bx$ is a unit by (**3.5**) as A is local. So $a_k = 0$. Thus $y = 0$, so A is a domain.

As to (2), every nonzero ideal of P is of the form $\langle X^n\rangle$ by (**3.8**). Hence P is Noetherian. Thus R is Noetherian by (**16.14**).

The primes of R are of the form $\mathfrak{q}\times P$ or $P\times\mathfrak{q}$ where $\mathfrak{q}$ is a prime of P by (**2.29**). Further, $\mathfrak{m} := \langle X\rangle$ is the unique maximal ideal by (**3.7**). Hence R has just two maximal ideals $\mathfrak{m}\times P$ and $P\times\mathfrak{m}$. Thus R is semilocal.

Set $\mathfrak{p} := \langle (X, 1)\rangle$. Then $\mathfrak{p} = \mathfrak{m}\times P$. So $\mathfrak{p}$ is a principal prime. Further, $\mathfrak{p}$ contains just one other prime $0 \times P$. Thus $\mathrm{ht}(\mathfrak{p}) = 1$.

Finally, R is not a domain as $(1,0) \cdot (0,1) = 0$. □

Exercise (21.22) . — Let k be a field, R a finitely generated k-algebra, $\mathfrak{m}$ a maximal ideal of R, and $\overline{k}$ an algebraic closure of k. Set $A := R_{\mathfrak{m}}$, set $r := \dim(A)$, set $K := A/\mathfrak{m}A$, and set $\overline{A} := A \otimes_k \overline{k}$. Fix a maximal ideal $\mathfrak{n}$ of $\overline{A}$.

(1) Show $\overline{A}$ is semilocal, $\dim(\overline{A}_{\mathfrak{n}}) = r$, and $\overline{A}_{\mathfrak{n}}/\mathfrak{n}\overline{A}_{\mathfrak{n}} = \overline{k}$.

(2) Assume $\overline{A}_{\mathfrak{n}}$ is regular. Show A is regular.

Solution: For (1), note that $R/\mathfrak{m}$ is a finite extension field of k by **(15.4)**. But by **(12.16)**, $R/\mathfrak{m} = K$. So $K \otimes_k \overline{k}$ is a finite dimensional $\overline{k}$-vector space by **(10.39)**(2). But $K \otimes_k \overline{k} = \overline{A}/\mathfrak{m}\overline{A}$. So $\overline{A}/\mathfrak{m}\overline{A}$ is Artinian by **(19.17)**. So $\overline{A}/\mathfrak{m}\overline{A}$ has only finitely many maximal ideals by **(19.20)**. But $\overline{k}/k$ is integral; so $\overline{A}/A$ is too by **(10.39)**(1). So every maximal ideal of $\overline{A}$ contains $\mathfrak{m}$ by **(14.3)**(1). Thus $\overline{A}$ is semilocal.

Note that $\overline{k}$ is flat over k by **(9.5)**. So $\overline{A}$ is flat over A by **(9.22)**. But $\overline{A}_{\mathfrak{n}}$ is flat over $\overline{A}$ by **(12.14)**. Thus $\overline{A}_{\mathfrak{n}}$ is flat over A by **(9.23)**. But $\overline{A}/\mathfrak{m}\overline{A}$ is Artinian; so $\dim(\overline{A}_{\mathfrak{n}}/\mathfrak{m}\overline{A}_{\mathfrak{n}}) = 0$ by **(19.8)**. Thus **(21.7)** yields $\dim(\overline{A}_{\mathfrak{n}}) = r$.

Note that $(\overline{A}/\mathfrak{m}\overline{A})_{\mathfrak{n}}$ is a quotient of $\overline{A}/\mathfrak{m}\overline{A}$ by **(19.11)**. But $(\overline{A}/\mathfrak{m}\overline{A})_{\mathfrak{n}} = \overline{A}_{\mathfrak{n}}/\mathfrak{m}\overline{A}_{\mathfrak{n}}$ and $\mathfrak{n} \supset \mathfrak{m}$. So $\overline{A}_{\mathfrak{n}}/\mathfrak{n}\overline{A}_{\mathfrak{n}}$ is a finite extension field of $\overline{k}$. Thus $\overline{A}_{\mathfrak{n}}/\mathfrak{n}\overline{A}_{\mathfrak{n}} = \overline{k}$. Thus (1) holds.

□

Exercise (21.13) . — Let A be a Noetherian local ring of dimension r. Let $\mathfrak{m}$ be the maximal ideal, and $k := A/\mathfrak{m}$ the residue class field. Prove that

$$r \leq \dim_k(\mathfrak{m}/\mathfrak{m}^2),$$

with equality if and only if $\mathfrak{m}$ is generated by r elements.

Solution: By **(21.4)**, $\dim(A)$ is the smallest number of elements that generate a parameter ideal. But $\mathfrak{m}$ is a parameter ideal, and the smallest number of generators of $\mathfrak{m}$ is $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ by **(10.8)**(2). The assertion follows. □

Exercise (21.16) . — Let A be a Noetherian local ring of dimension r, and let $x_1, \ldots, x_s \in A$ with $s \leq r$. Set $\mathfrak{a} := \langle x_1, \ldots, x_s \rangle$ and $B := A/\mathfrak{a}$. Prove equivalent:

(1) A is regular, and there are $x_{s+1}, \ldots, x_r \in A$ with $x_1, \ldots, x_r$ a regular sop.

(2) B is regular of dimension $r - s$.

Solution: Assume (1). Then $x_1, \ldots, x_r$ generate the maximal ideal $\mathfrak{m}$ of A. So the residues of $x_{s+1}, \ldots, x_r$ generate that $\mathfrak{n}$ of B. Hence $\dim(B) \leq r - s$ by **(21.13)**. But $\dim(B) \geq r - s$ by **(21.5)**. So $\dim(B) = r - s$. Thus (2) holds.

Assume (2). Then $\mathfrak{n}$ is generated by $r - s$ elements, say by the residues of $x_{s+1}, \ldots, x_r \in A$. Hence $\mathfrak{m}$ is generated by $x_1, \ldots, x_r$. Thus (1) holds. □

Exercise (21.20) . — Let R be a ring, R' an algebra, and N a nonzero R'-module that's a Noetherian R-module. Prove the following statements:

(1) $\dim_R(N) = \dim_{R'}(N)$.

(2) Each prime in $\mathrm{Supp}_{R'}(N)$ contracts to a prime in $\mathrm{Supp}_R(N)$. Moreover, one is maximal if and only if the other is.

(3) Each maximal ideal in $\mathrm{Supp}_R(N)$ is the contraction of at least one and at most finitely many maximal ideals in $\mathrm{Supp}_{R'}(N)$.

(4) $\mathrm{rad}_R(N)R' \subset \mathrm{rad}_{R'}(N)$.

(5) N is semilocal over R if and only if N is semilocal over R'.

Solution: Set $R_1 := R/\operatorname{Ann}_R(N)$ and $R'_1 := R'/\operatorname{Ann}_{R'}(N)$. Then

$$\operatorname{Supp}_R(N) = \operatorname{Spec}(R_1) \quad \text{and} \quad \operatorname{Supp}_{R'}(N) = \operatorname{Spec}(R'_1)$$

by **(13.4)**(3) as N is finitely generated over R. So by definition **(21.1)**,

$$\dim_R(N) = \dim(R_1) \quad \text{and} \quad \dim_{R'}(N) = \dim(R'_1).$$

Say $n_1, \dots, n_r$ generate N. Define $\alpha\colon R' \to N^{\oplus r}$ by $\alpha(x) := (xn_1, \dots, xn_r)$. Plainly $\operatorname{Ker}(\alpha) = \operatorname{Ann}_{R'}(N)$. Hence α induces an injection $R'_1 \hookrightarrow N^{\oplus r}$. But $N^{\oplus r}$ is Noetherian over R. Thus R'_1 is module finite over R_1, so integral over R_1.

Note that $\operatorname{Ann}_{R'}(N)$ contracts to $\operatorname{Ann}_R(N)$. Thus R'_1 is an extension of R_1.

For (1), apply **(15.26)**. For (2), apply **(14.3)**(1).

For (3), fix a maximal ideal $\mathfrak{m} \in \operatorname{Supp}_R(N)$. Then $\mathfrak{m}$ is the contraction of at least one prime $\mathfrak{n}$ in $\operatorname{Supp}_{R'}(N)$ by **(14.3)**(3), and $\mathfrak{n}$ is maximal by **(14.3)**(1). There are at most finitely many such $\mathfrak{n}$ by **(19.25)**. Thus (3) holds.

For (4), note that each maximal ideal $\mathfrak{n}$ in $\operatorname{Supp}_{R'}(N)$ contracts to a maximal ideal in $\operatorname{Supp}_R(N)$ by (2). So $\operatorname{rad}_R(N)R' \subset \mathfrak{n}$. Thus (4) holds.

For (5), note that, each maximal ideal in $\operatorname{Supp}_R(N)$ is the contraction of at least one maximal ideal in $\operatorname{Supp}_{R'}(N)$ by (3). So $\operatorname{Supp}_R(N)$ contains only finitely many maximal ideals if $\operatorname{Supp}_{R'}(N)$ does. The converse holds, as each maximal ideal $\mathfrak{n}$ in $\operatorname{Supp}_{R'}(N)$ contracts to a maximal ideal $\mathfrak{m}$ in $\operatorname{Supp}_R(N)$ by (2), and as this $\mathfrak{m}$ is the contraction of at most finitely many such $\mathfrak{n}$ by (3). Thus (5) holds. □

Exercise (21.21) . — Let R be a ring, M a nonzero Noetherian semilocal module, $\mathfrak{q}$ a parameter ideal, and $0 = M_0 \subset M_1 \subset \cdots \subset M_r = M$ a chain of submodules with $M_i/M_{i-1} \simeq R/\mathfrak{p}_i$ for some $\mathfrak{p}_i \in \operatorname{Supp}(M)$. Set $d := \dim(M)$ and set

$$I := \{\, i \mid \dim(R/\mathfrak{p}_i) = d \,\} \quad \text{and} \quad \Phi := \{\, \mathfrak{p} \in \operatorname{Supp}(M) \mid \dim(R/\mathfrak{p}) = d \,\}.$$

Prove: (1) $e(\mathfrak{q}, M) = \sum_{i \in I} e(\mathfrak{q},\, R/\mathfrak{p}_i)$ and (2) $e(\mathfrak{q}, M) = \sum_{\mathfrak{p} \in \Phi} \ell_{R_\mathfrak{p}}(M_\mathfrak{p}) e(\mathfrak{q},\, R/\mathfrak{p})$.

Solution: Given any $\mathfrak{p} \in \operatorname{Supp}(M)$, recall $\mathfrak{p} \supset \operatorname{Ann}(M)$ by **(13.4)**(3). But M is semilocal. So $\operatorname{Ann}(M)$ lies in just finitely many maximal ideals; so $\mathfrak{p}$ does too. Thus $R/\mathfrak{p}$ is semilocal. In addition, as M is Noetherian, so is $R/\operatorname{Ann}(M)$ by **(16.16)**; thus, $R/\mathfrak{p}$ is Noetherian.

For (1), form the exact sequences $0 \to M_{i-1} \to M_i \to R/\mathfrak{p}_i \to 0$. By **(20.13)**(2), the polynomials $p_\mathfrak{q}(M_i,\, n)$ and $p_\mathfrak{q}(M_{i-1},\, n) + p_\mathfrak{q}(R/\mathfrak{p}_i,\, n)$ have the same degree and the same leading coefficients. Hence, so do the polynomials $p_\mathfrak{q}(M,\, n)$ and $\sum_{i \in I} p_\mathfrak{q}(R/\mathfrak{p}_i, n)$. But the degree of $p_\mathfrak{q}(R/\mathfrak{p}_i, n)$ is $\dim(R/\mathfrak{p}_i)$ by the Dimension Theorem **(21.4)**. Also $d = \max \dim(R/\mathfrak{p}_i)$ by **(21.1.1)**. Thus (1) holds.

For (2), note **(17.16)** provides a chain as in (1). Fix $\mathfrak{p} \in \Phi$. If $\mathfrak{p}_i \neq \mathfrak{p}$, then $\mathfrak{p}_i \not\subset \mathfrak{p}$ as $\mathfrak{p}$ is minimal, and so $R_\mathfrak{p}/\mathfrak{p}_i R_\mathfrak{p} = 0$ by **(11.8)**(2). On the other hand, if $\mathfrak{p} = \mathfrak{p}_i$, then $R_\mathfrak{p}/\mathfrak{p}_i R_\mathfrak{p}$ is a field. So $M_\mathfrak{p} := (M_r)_\mathfrak{p} \supset \cdots \supset (M_0)_\mathfrak{p} = 0$ becomes a composition series after eliminating duplicates; moreover, $\ell_{R_\mathfrak{p}}(M_\mathfrak{p})$ is the number of i with $\mathfrak{p}_i = \mathfrak{p}$. Thus (1) yields (2). □

Exercise (21.23) . — Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal, $\mathfrak{q}$ a parameter ideal, $P := (A/\mathfrak{q})[X_1, \dots, X_s]$ a polynomial ring for some $s \geq 0$. Show:

(1) Set $\mathfrak{M} := (\mathfrak{m}/\mathfrak{q})[X_1, \dots, X_s]$. Then $\operatorname{z.div}(P) = \mathfrak{M}$.

(2) Assume $\mathfrak{q}$ is generated by a sop $x_1, \dots, x_s$. Let $\phi_s\colon P \to G_\mathfrak{q}(A)$ be the map of **(21.11.1)**. Then $\operatorname{Ker}(\phi_s) \subset \operatorname{z.div}(P)$.

Solution: For (1), fix $F \in \mathrm{z.div}(P)$. Then **(8.32)** gives $x \in A/\mathfrak{q}$ with $xF = 0$ but $x \neq 0$. Fix a coefficient a of F. Then $xa = 0$. So $a \notin (A/\mathfrak{q})^\times$. So $a \in \mathfrak{m}/\mathfrak{q}$. Thus $\mathrm{z.div}(P) \subset \mathfrak{M}$.

Conversely, fix $F \in \mathfrak{M}$. Note $A/\mathfrak{q}$ is Artinian by **(19.12)** and **(19.10)**. So there's $r > 0$ with $(\mathfrak{m}/\mathfrak{q})^r = 0$ by **(19.23)**. So $F^r = 0$. Thus $F \in \mathrm{z.div}(P)$. Thus (1) holds.

For (2), set $\mathfrak{a} := \mathrm{Ker}(\phi_s)$. Note $\mathfrak{a}$ is homogeneous, $\mathfrak{a} = \oplus \mathfrak{a}_n$. Suppose there's $F \in \mathfrak{a}_m$, but $F \notin \mathrm{z.div}(P)$. Then for all $n \geq m$, the map $P_{n-m} \xrightarrow{\times F} \mathfrak{a}_n$ is injective; so $\ell(P_{n-m}) \leq \ell(\mathfrak{a}_n)$. But there's an exact sequence, $0 \to \mathfrak{a}_n \to P_n \to \mathfrak{q}^n/\mathfrak{q}^{n+1} \to 0$; so **(19.7)** yields $\ell(\mathfrak{q}^n/\mathfrak{q}^{n+1}) = \ell(P_n) - \ell(\mathfrak{a}_n)$. So $\ell(\mathfrak{q}^n/\mathfrak{q}^{n+1}) \leq \ell(P_n) - \ell(P_{n-m})$.

So **(20.4)** yields $\ell(\mathfrak{q}^n/\mathfrak{q}^{n+1}) \leq \ell(A/\mathfrak{q})\left(\binom{s-1+n}{s-1} - \binom{s-1+n-m}{s-1}\right)$. The latter is a polynomial in n of degree $s-2$. But **(21.4)** yields $s = \deg(p_{\mathfrak{q}}(A, n))$. So $\deg(h(G_{\mathfrak{q}}(A), n)) = s - 1$ by **(20.11)**, a contradiction. Thus $\mathfrak{a}_m \subset \mathrm{z.div}(P)$ for all m. But $\mathrm{z.div}(P)$ is closed under sum by (1), hence contains $\mathfrak{a}$. Thus (2) holds. □

Exercise (21.24) . — Let A be a Noetherian local ring, $k \subset A$ a **coefficient** field (or field of representatives) — that is, k maps isomorphically onto the residue field — $x_1, \ldots, x_s$ a sop. Using **(21.23)**, show the x_i are algebraically independent over k.

Solution: Set $\mathfrak{q} := \langle x_1, \ldots, x_s \rangle$. Let $Q := k[X_1, \ldots, X_s]$ be the polynomial ring in variables X_i. Given $F \in Q$, say $F = \sum_{i=t}^{u} F_i$ with F_i homogeneous of degree i. Note $F_i(x_1, \ldots, x_s) \in \mathfrak{q}^i$ for all i. Assume $F_t \neq 0$.

Assume $F(x_1, \ldots, x_s) = 0$. So $F_t(x_1, \ldots, x_s) \in \mathfrak{q}^{t+1}$. Set $P := (A/\mathfrak{q})[X_1, \ldots, X_s]$. Let $\phi_s \colon P \to G_{\mathfrak{q}}(A)$ be the map of **(21.11.1)**. View $Q \subset P$. Then $\phi_s(F_t) = 0$. So by **(21.23)**(1)–(2), the coefficients of F_t are in the maximal ideal of $A/\mathfrak{q}$. But they're in k too. So they're 0. Thus the x_i are algebraically independent over k. □

Exercise (21.25) . — Let k be an algebraically closed field, R an algebra-finite domain, $\mathfrak{m}$ a maximal ideal of R. Using the dimension theory in this chapter and **(15.1)**(1), but not (2), show $\dim(R) = \dim(R_{\mathfrak{m}}) = \mathrm{tr.deg}_k(\mathrm{Frac}(R))$. (Compare with **(15.10)** and **(15.12)**.)

Solution: As $\dim(R) = \sup_{\mathfrak{m}} \dim(R_{\mathfrak{m}})$, the second equality implies the first.

To prove the second equality, note that $R/\mathfrak{m}$ is a finite algebraic extension of k by **(15.4)**. So $k = R/\mathfrak{m}$, because k is algebraically closed. But $R/\mathfrak{m} = R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$ by **(12.16)**. Thus k is a coefficient field of $R_{\mathfrak{m}}/\mathfrak{m}R_{\mathfrak{m}}$.

Let $x_1, \ldots, x_d \in \mathfrak{m}R_{\mathfrak{m}}$ form a sop for $R_{\mathfrak{m}}$. The x_i are algebraically independent over k by **(21.24)**. Set $K := \mathrm{Frac}(R)$ and $n := \mathrm{tr.deg}_k(K)$. Then $n \geq d$.

By **(15.1)**(1), there are algebraically independent elements $t_1, \ldots, t_\nu \in R$ such that R is module finite over $P := k[t_1, \ldots, t_\nu]$. Then K is a finite extension field of $k(t_1, \ldots, t_\nu)$. Thus $\nu = n$.

Set $\mathfrak{n}; = \mathfrak{m} \cap P$. Then $\mathfrak{n}$ is maximal and $\dim(R_{\mathfrak{m}}) = \dim(P_{\mathfrak{n}})$ by **(15.27)**. By **(15.5)**, there are $a_1, \ldots, a_\nu \in k$ such that $\mathfrak{n} = \langle u_1, \ldots, u_\nu \rangle$ where $u_i := t_i - a_i$. Then $\langle u_1, \ldots, u_\nu \rangle \supsetneqq \cdots \supsetneqq \langle u_1 \rangle \supsetneqq \langle 0 \rangle$ is a chain of primes of length ν. Thus $\dim(P_{\mathfrak{n}}) \geq \nu$.

In sum, $\dim(R_{\mathfrak{m}}) = \dim(P_{\mathfrak{n}}) \geq \nu = n \geq d$. But $d = \dim(R_{\mathfrak{m}})$ by **(21.4)**. Thus $\dim(R_{\mathfrak{m}}) = n$, as desired. □

Exercise (21.26) . — Let R be a ring, N a Noetherian semilocal module, and $y_1, \ldots, y_r$ a sop for N. Set $N_i := N/\langle y_1, \ldots, y_i \rangle N$. Show $\dim(N_i) = r - i$.

Solution: First, $\dim(N) = r$ by **(21.4)**. But **(4.21)** with $\mathfrak{a} := \langle y_1, \ldots, y_{i-1}\rangle$ and $\mathfrak{b} := \langle y_i\rangle$ yields $N_i \xrightarrow{\sim} N_{i-1}/y_iN_{i-1}$. Hence $\dim(N_i) \ge \dim(N_{i-1}) - 1$ for all i by **(21.5)**, and $\dim(N_r) = 0$ by **(19.26)**(1) $\Rightarrow$ (3). Thus $\dim(N_i) = r - i$ for all i. $\square$

Exercise (21.27) . — Let R be a ring, $\mathfrak{p}$ a prime, M a finitely generated module. Set $R' := R/\operatorname{Ann} M$. Prove these two statements: (1) $\dim(M_\mathfrak{p}) = \dim(R'_\mathfrak{p})$.
(2) If $\operatorname{Ann}(M) = \langle 0\rangle$, then $\dim(M_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p})$.

Solution: For (1), note $\operatorname{Supp}(M_\mathfrak{p}) = \operatorname{Spec}(R_\mathfrak{p}/\operatorname{Ann} M_\mathfrak{p})$ owing to **(13.4)**(3). But $\operatorname{Ann} M_\mathfrak{p} = (\operatorname{Ann} M)_\mathfrak{p}$ by **(12.17)**(1). So $R_\mathfrak{p}/\operatorname{Ann} M_\mathfrak{p} = R'_\mathfrak{p}$ by **(12.15)**. So $\operatorname{Supp}(M_\mathfrak{p}) = \operatorname{Spec}(R'_\mathfrak{p})$. Thus the definitions **(21.1)** and **(15.9)** yield (1).
For (2), recall $\dim(R_\mathfrak{p}) = \operatorname{ht}(\mathfrak{p})$ by **(21.6.1)**. Thus (1) yields (2). $\square$

Exercise (21.28) . — Let R be a Noetherian ring, and $\mathfrak{p}$ be a prime minimal containing $x_1, \ldots, x_r$. Given r' with $1 \le r' \le r$, set $R' := R/\langle x_1, \ldots, x_{r'}\rangle$ and $\mathfrak{p}' := \mathfrak{p}/\langle x_1, \ldots, x_{r'}\rangle$. Assume $\operatorname{ht}(\mathfrak{p}) = r$. Prove $\operatorname{ht}(\mathfrak{p}') = r - r'$.

Solution: Let $x'_i \in R'$ be the residue of x_i. Then $\mathfrak{p}'$ is minimal containing $x'_{r'+1}, \ldots x'_r$. So $\operatorname{ht}(\mathfrak{p}') \le r - r'$ by **(21.8)**.
On the other hand, $R'_{\mathfrak{p}'} = R'_\mathfrak{p}$ by **(11.15.1)**, and $R'_\mathfrak{p} = R_\mathfrak{p}/\langle x_1/1, \ldots, x_{r'}/1\rangle$ by **(12.15)** Hence $\dim(R'_{\mathfrak{p}'}) \ge \dim(R_\mathfrak{p}) - r'$ by repeated application of **(21.5)** with $R_\mathfrak{p}$ for both R and M. Thus $\operatorname{ht}(\mathfrak{p}') \ge r - r'$ by **(21.6.1)**, as required. $\square$

Exercise (21.29) . — Let R be a Noetherian ring, $\mathfrak{p}$ a prime of height at least 2. Prove that $\mathfrak{p}$ is the union of height-1 primes, but not of finitely many.

Solution: If $\mathfrak{p}$ were the union of finitely many height-1 primes $\mathfrak{p}'$, then by Prime Avoidance **(3.12)**, one $\mathfrak{p}'$ would be equal to $\mathfrak{p}$, a contradiction.
To prove $\mathfrak{p}$ is the union of height-1 primes, we may replace R by $R/\mathfrak{q}$ where $\mathfrak{q} \subset \mathfrak{p}$ is a minimal prime, as preimage commutes with union. Thus we may assume R is a domain. Given a nonzero $x \in \mathfrak{p}$, let $\mathfrak{q}_x \subset \mathfrak{p}$ be a minimal prime of $\langle x\rangle$. Then $\operatorname{ht}(\mathfrak{q}_x) = 1$ by the Krull Principal Theorem **(21.9)**. Plainly $\bigcup \mathfrak{q}_x = \mathfrak{p}$. $\square$

Exercise (21.30) . — Let R be a Noetherian ring of dimension at least 1. Show that the following conditions are equivalent:

(1) R has only finitely many primes.
(2) R has only finitely many height-1 primes.
(3) R is semilocal of dimension exactly 1.

Solution: Trivially, (1) implies (2).
Assume (2). Then, by **(21.29)**, there's no prime of height at least 2. Thus $\dim(R) = 1$. But, the height-0 primes are minimal, so finite in number by **(17.29)**. Thus (1) and (3) hold.
Finally, assume (3). Since $\dim(R) = 1$, the height-1 primes are maximal. Since R is semilocal, R has only finitely many maximal ideals. Thus (2) holds. $\square$

Exercise (21.31) (*Artin–Tate* [2, Thm. 4]) . — Let R be a Noetherian domain, X a variable. Set $K := \operatorname{Frac}(R)$. Prove the following equivalent:

(1) $\langle fX - 1\rangle \subset R[X]$ is a maximal ideal for some nonzero $f \in R$.
(2) $K = R_f$ for some nonzero $f \in R$.
(3) K is algebra finite over R.
(4) Some nonzero $f \in R$ lies in every nonzero prime.

(5) R has only finitely many height-1 primes.
(6) R is semilocal of dimension 1.

Solution: First, $R_f = R[X]/\langle fX-1\rangle$ by **(11.7)**. But $R \subset R_f \subset K$, and K is the smallest field containing R; see **(11.2)** and **(2.3)**. So R_f is a field if and only if $R_f = K$. Thus (1) and (2) are equivalent, and they imply (3).

Assume (3), and say $K = R[x_1, \ldots, x_n]$. Let f be a common denominator of the x_i. Then given any $y \in K$, clearly $f^m y \in R$ for some $m \ge 1$.

Let $\mathfrak{p} \subset R$ be a nonzero prime. Take a nonzero $z \in \mathfrak{p}$. By the above, $f^m(1/z) \in R$ for some $m \ge 1$. So $f^m(1/z)z \in \mathfrak{p}$. So $f \in \mathfrak{p}$. Thus (3) implies (4).

Assume (4). Given $0 \ne y \in R$, the Scheinnullstellensatz **(3.14)** yields $f \in \sqrt{\langle y\rangle}$. So $f^n = xy$ for some $n \ge 1$ and $x \in R$. So $1/y = x/f^n$. Thus (4) implies (2).

Again assume (4). Let $\mathfrak{p}$ be a height-1 prime. Then $f \in \mathfrak{p}$. So $\mathfrak{p}$ is minimal containing $\langle f\rangle$. So $\mathfrak{p}$ is one of finitely many primes by **(17.29)**. Thus (5) holds.

Note (5) and (6) are equivalent by **(21.30)**(2) $\Rightarrow$ (3).

Finally, assume (6). Then there are only finitely many nonzero primes, each of height 1. Take a nonero element in each; let f be their product. Thus (4) holds. □

Exercise (21.32) . — Let R be a Noetherian domain, and p a prime element. Show that $\langle p\rangle$ is a height-1 prime ideal.

Solution: By **(2.5)**, the ideal $\langle p\rangle$ is prime. Thus by **(21.9)** it's height-1. □

Exercise (21.33) . — Let R be a UFD, and $\mathfrak{p}$ a height-1 prime ideal. Show that $\mathfrak{p} = \langle p\rangle$ for some prime element p.

Solution: As $\operatorname{ht}(\mathfrak{p}) = 1$, there's a nonzero $x \in \mathfrak{p}$. Factor x. One prime factor p must lie in $\mathfrak{p}$ as $\mathfrak{p}$ is prime. Then $\langle p\rangle$ is a prime ideal as p is a prime element by **(2.5)**. But $\langle 0\rangle \ne \langle p\rangle \subset \mathfrak{p}$ and $\operatorname{ht}(\mathfrak{p}) = 1$. Thus, $\langle p\rangle = \mathfrak{p}$, as desired. □

Exercise (21.34) . — Let R be a Noetherian domain such that every height-1 prime ideal $\mathfrak{p}$ is principal. Show that R is a UFD.

Solution: It suffices to show that every irreducible element p is prime; see **(2.5)**. Take a minimal prime $\mathfrak{p}$ of $\langle p\rangle$. Then $\operatorname{ht}(\mathfrak{p}) = 1$ by **(21.9)**. So by hypothesis $\mathfrak{p} = \langle x\rangle$ for some x. Then x is prime by **(2.5)**. And $p = xy$ for some y as $p \in \mathfrak{p}$. But p is irreducible. So y is a unit. Thus p is prime, as desired. □

Exercise (21.35) (*Gauss' Lemma*) . — Let R be a UFD; X a variable; $F, G \in R[X]$ nonzero. Call F **primitive** if its coefficients have no common prime divisor.

(1) Show that F is primitive if and only if $c(F)$ lies in no height-1 prime ideal.
(2) Assume that F and G are primitive. Show that FG is primitive.
(3) Let f, g, h be the gcd's of the coefficients of F, G, FG. Show $fg = h$.
(4) Assume $c(F) = \langle f\rangle$ with $f \in R$. Show f is the gcd of the coefficients of F.

Solution: For (1), note that F is not primitive if and only if $c(F) \subset \langle p\rangle$ for some prime element p. But such $\langle p\rangle$ are precisely the height-1 prime ideals by **(21.33)** and **(21.32)**. Thus (1) holds.

For (2), given a height-1 prime ideal $\mathfrak{p}$, note $c(F) \not\subset \mathfrak{p}$ and $c(G) \not\subset \mathfrak{p}$ by (1). So **(2.36)**(1) implies $c(FG) \not\subset \mathfrak{p}$. So FG is primitive by (1). Thus (2) holds.

For (3), say $F = fF'$ and $G = gG'$. Then F' and G' are primitive. So $F'G'$ is primitive by (2). But $FG = fgF'G'$. Thus (3) holds.

For (4), given $g \in R$, note that g divides all the coefficients of F if and only if

$c(F) \subset \langle g \rangle$. But $c(F) = \langle f \rangle$; also $\langle f \rangle \subset \langle g \rangle$ if and only if $g \mid f$. Hence, f divides all the coefficients of F, and if g does too, then $g \mid f$. Thus (4) holds. □

Exercise (21.36) . — Let R be a finitely generated algebra over a field. Assume R is a domain of dimension r. Let $x \in R$ be neither 0 nor a unit. Set $R' := R/\langle x \rangle$. Prove that $r - 1$ is the length of any chain of primes in R' of maximal length.

Solution: A chain of primes in R' of maximal length lifts to a chain of primes $\mathfrak{p}_i$ in R of maximal length with $\langle x \rangle \subseteq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_d$. As x is not a unit, $d \geq 1$. As $x \neq 0$, also $\mathfrak{p}_1 \neq 0$. But R is a domain. So Krull's Principal Ideal Theorem, (**21.9**), yields $\operatorname{ht} \mathfrak{p}_1 = 1$. So $0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ is of maximal length in R. But R is a finitely generated algebra over a field. Thus $d = \dim R$ by (**15.8**), as desired. □

Exercise (21.37) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, R_1 and R_2 two P-algebra-finite domains, and $\mathfrak{p}$ a minimal prime of $R_1 \otimes_P R_2$.

(1) Set $C := R_1 \otimes_k R_2$, and let $\mathfrak{q} \subset C$ denote the preimage of $\mathfrak{p}$. Use (**8.28**)(1) to prove that $\mathfrak{q}$ is a minimal prime of an ideal generated by n elements.

(2) Use (**15.12**) and (**15.29**) to prove this inequality:

$$\dim(R_1) + \dim(R_2) \leq n + \dim\big((R_1 \otimes_P R_2)/\mathfrak{p}\big). \qquad \textbf{(21.37.1)}$$

Solution: For (1), note $R_1 \otimes_P R_2 = C/\mathfrak{d}_P C$ by (**8.28**)(1). So $\mathfrak{q}$ is a minimal prime of $\mathfrak{d}_P C$. But $\mathfrak{d}_P$ is, by (**8.19**), generated by n elements, as desired.

For (2), say $\{x_i\}$ is a set of P-algebra generators of R_1. Then together with the images of the X_j in R_1, the x_i plainly form a set of k-algebra generators of R_1. Thus R_1 is algebra finite over k. Similarly, R_2 is too.

Say $\{u_i\}$ and $\{v_j\}$ are sets of k-algebra generators of R_1 and of R_2. Then, in C, the $u_i \otimes 1$ and $1 \otimes v_j$ plainly form a set of k-algebra generators. Thus C is k-algebra finite. So C is Noetherian by the Hilbert Basis Theorem (**16.10**). So owing to (1), Corollary (**21.8**) yields $\operatorname{ht}(\mathfrak{q}) \leq n$.

There is a minimal prime $\mathfrak{q}_0 \subset \mathfrak{q}$ by (**3.16**). Set $C_0 := C/\mathfrak{q}_0$. Then (**21.6.1**) yields $\dim((C_0)_{\mathfrak{q}C_0}) = \operatorname{ht}(\mathfrak{q}/\mathfrak{q}_0)$. So $\dim((C_0)_{\mathfrak{q}C_0}) \leq n$. But C_0 is a domain, and is k-algebra finite as C is. So (**15.12**) yields

$$\dim(C_0) = \dim((C_0)_{\mathfrak{q}C_0}) + \dim(C_0/\mathfrak{q}C_0).$$

But $C_0/\mathfrak{q}C_0 = C/\mathfrak{q} = (R_1 \otimes_P R_2)/\mathfrak{p}$. Moreover, $\dim(C_0) = \dim(R_1) + \dim(R_2)$ by (**15.29.1**). Thus (**21.37.1**) holds. □

Exercise (21.38) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, R' a P-algebra-finite domain. Let $\mathfrak{p}$ be a prime of P, and $\mathfrak{p}'$ a minimal prime of $\mathfrak{p}R'$. Prove this inequality: $\operatorname{ht}(\mathfrak{p}') \leq \operatorname{ht}(\mathfrak{p})$.

Solution: Set $R_1 := R'$ and $R_2 := P/\mathfrak{p}$. Then $R_1 \otimes_P R_2 = R'/\mathfrak{p}R'$ by (**8.27**)(1). Set $\mathfrak{P} := \mathfrak{p}'/\mathfrak{p}R'$. Then $\mathfrak{P}$ is minimal, and $(R_1 \otimes_P R_2)/\mathfrak{P} = R'/\mathfrak{p}'$. So by (**21.37**)

$$\dim(R') + \dim(P/\mathfrak{p}) \leq n + \dim(R'/\mathfrak{p}'). \qquad \textbf{(21.38.1)}$$

But $\dim(P/\mathfrak{p}) = n - \operatorname{ht}(\mathfrak{p})$ and $\dim(R'/\mathfrak{p}') = \dim(R') - \operatorname{ht}(\mathfrak{p}')$ by (**21.6.1**) and (**15.12**) and (**15.11**). Thus (**21.38.1**) yields $\operatorname{ht}(\mathfrak{p}') \leq \operatorname{ht}(\mathfrak{p})$, as desired. □

Exercise (21.39) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ primes of P, and $\mathfrak{p}$ a minimal prime of $\mathfrak{p}_1 + \mathfrak{p}_2$. Prove this inequality:

$$\operatorname{ht}(\mathfrak{p}) \leq \operatorname{ht}(\mathfrak{p}_1) + \operatorname{ht}(\mathfrak{p}_2). \qquad \textbf{(21.39.1)}$$

Solution: Set $R_i := P/\mathfrak{p}_i$. Then $R_1 \otimes_P R_2 = P/(\mathfrak{p}_1 + \mathfrak{p}_2)$ by (**8.27**)(2). Set $\mathfrak{P} := \mathfrak{p}/(\mathfrak{p}_1 + \mathfrak{p}_2)$. Then $\mathfrak{P}$ is minimal, and $(R_1 \otimes_P R_2)/\mathfrak{P} = P/\mathfrak{p}$. So (**21.37**) yields

$$\dim(P/\mathfrak{p}_1) + \dim(P/\mathfrak{p}_2) \le n + \dim(P/\mathfrak{p}). \tag{21.39.2}$$

But given any prime $\mathfrak{q}$ of P, note $\dim(P/\mathfrak{q}) = n - \mathrm{ht}(\mathfrak{q})$ by (**21.6.1**) and (**15.12**) and (**15.11**). Thus (**21.39.2**) yields (**21.39.1**). □

Exercise (21.40) . — Let k be a field, $k[X, Y, Z, W]$ the polynomial ring. Set

$$\mathfrak{q}_1 := \langle X, Y\rangle \quad\text{and}\quad \mathfrak{q}_2 := \langle Z, W\rangle \quad\text{and}\quad \mathfrak{q} := \langle X, Y, Z, W\rangle \quad\text{and}$$
$$R := k[X, Y, Z, W]/\langle XZ - YW\rangle \quad\text{and}\quad \mathfrak{p}_i := \mathfrak{q}_i R \quad\text{and}\quad \mathfrak{p} := \mathfrak{q}R.$$

Show that $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}$ are primes of heights $1, 1, 3$. Does (**21.39.1**) hold with $P := R$?

Solution: Note $XZ - YW$ is irreducible. So R is a domain. Also $\dim R = 3$ by (**21.36**) and (**15.11**). But $R/\mathfrak{p}_1 = k[X, Y, Z, W]/\mathfrak{q}_1 = k[Z, W]$. So $\mathfrak{p}_1$ is prime; also (**15.11**) yields $\dim(R/\mathfrak{p}_1) = 2$. Thus (**21.6.1**) and (**15.12**) yield $\mathrm{ht}(\mathfrak{p}_1) = 1$. Similarly, $\mathfrak{p}_2$ is prime of height 1, and $\mathfrak{p}$ is prime of height 3.

Lastly, no, (**21.39.1**) does not hold with R for P, as $\mathfrak{p} = \mathfrak{p}_1 + \mathfrak{p}_2$ but $3 > 1+1$. □

Exercise (21.41) . — Let R be a Noetherian ring, $X, X_1, \ldots, X_n$ variables. Show:

$$\dim(R[X]) = 1 + \dim(R) \quad\text{and}\quad \dim(R[X_1, \ldots, X_n]) = n + \dim(R).$$

Solution: The second eequation follows from the first by induction on n.

To prove the first equation, let $\mathfrak{P} \subset R[X]$ be a prime, $\mathfrak{p} \subset R$ its contraction. Note that the monomials X^i for $i \ge 0$ form a free basis of $R[X]$; so it'ss a flat R-algebra. So the local homomorphism $R_\mathfrak{p} \to R[X]_\mathfrak{P}$ is flat by (**13.60**). So (**21.7**) gives

$$\dim(R[X]_\mathfrak{P}) = \dim(R_\mathfrak{p}) + \dim\big(R[X]_\mathfrak{P}/\mathfrak{p}R[X]_\mathfrak{P}\big). \tag{21.41.1}$$

Set $k := \mathrm{Frac}(R/\mathfrak{p})$. Then $k = (R/\mathfrak{p})_\mathfrak{p}$ by (**12.16**). So $R[X]_\mathfrak{P}/\mathfrak{p}R[X]_\mathfrak{P} = k[X]_\mathfrak{P}$ by (**12.32**) with $\mathfrak{a} := \mathfrak{p}$ and $S := R - \mathfrak{p}$ and $T := R[X] - \mathfrak{P}$. But $\dim(k[X]_\mathfrak{P}) \le 1$ by (**15.11**) and (**15.12**). Plainly, $\dim(R_\mathfrak{p}) \le \dim(R)$. Thus (**21.41.1**) yields $\dim(R[X]_\mathfrak{P}) \le \dim(R) + 1$.

Plainly, $\dim(R[X]) = \sup_\mathfrak{P}\{\dim(R[X]_\mathfrak{P})\}$. Hence, $\dim(R[X]) \le \dim(R) + 1$. Finally, the opposite inequality holds by (**15.32**). □

Exercise (21.42) (*Jacobian Criterion*) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ the polynomial ring, $\mathfrak{A} \subset P$ an ideal, $\mathbf{x} := (x_1, \ldots, x_n) \in k^n$. Set $R := P/\mathfrak{A}$ and $\mathfrak{M} := \langle X_1 - x_1, \ldots, X_n - x_n\rangle$. Prove the following statements:

(1) Say $\mathfrak{A} = \langle F_1, \ldots, F_m\rangle$. Assume $F_i(\mathbf{x}) = 0$ for all i. For all i, j, define $\partial F_i/\partial X_j \in P$ formally as in (**1.18.1**), and set $a_{ij} := (\partial F_i/\partial X_j)(\mathbf{x})$. Let r be the rank of the m by n matrix (a_{ij}). Set $d := \dim R_\mathfrak{M}$. Then these conditions are equivalent: (a) $R_\mathfrak{M}$ is regular; (b) $r = n - d$; and (c) $r \ge n - d$.

(2) Assume $\mathfrak{A}$ is prime, $F \notin \mathfrak{A}$, and k is algebraically closed. Then there's a choice of $\mathbf{x}$ with $F(\mathbf{x}) \neq 0$ and $\mathfrak{A} \subset \mathfrak{M}$ and $R_\mathfrak{M}$ regular.

Start with the case $\mathfrak{A} = \langle G\rangle$. Then reduce to it by using a separating transcendence basis for $K := \mathrm{Frac}(R)$ over k and a primitive element.

Solution: In (1), plainly $X_1 - x_1, \ldots, X_n - x_n$ form a minimal generating set of $\mathfrak{M}$. But $\mathfrak{M}$ is maximal and $k = P/\mathfrak{M}$ by (**2.14**). So $X_1 - x_1, \ldots, X_n - x_n$ induce a basis of $\mathfrak{M}/\mathfrak{M}^2$ over k by (**10.8**)(2). Set $\mathfrak{m} := \mathfrak{M}P_\mathfrak{M}$. Then $\mathfrak{M}/\mathfrak{M}^2 = \mathfrak{m}/\mathfrak{m}^2$ by (**12.34**) with $M := \mathfrak{M}$ and $\mathfrak{m} := \mathfrak{M}$. Thus $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = n$.

Set $\mathfrak{a} := \mathfrak{A}P_{\mathfrak{M}}$. By (**1.18**), the residues of the m polynomials $\sum_j a_{ij}(X_j - x_j)$ span $(\mathfrak{m}^2 + \mathfrak{a})/\mathfrak{m}^2$. But (a_{ij}) has rank r. Thus $\dim_k(\mathfrak{m}^2 + \mathfrak{a})/\mathfrak{m}^2 = r$. Set $\mathfrak{n} := \mathfrak{m}/\mathfrak{a}$ and $d' := \dim_k(\mathfrak{n}/\mathfrak{n}^2)$. The exact sequence $0 \to (\mathfrak{m}^2 + \mathfrak{a})/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{n}/\mathfrak{n}^2 \to 0$ of (**21.18**) yields $n - r = d'$. But $\mathfrak{M}R_{\mathfrak{M}} = \mathfrak{n}$ and $d := \dim(R_{\mathfrak{M}})$. So $d \le d'$ by (**21.13**), and $R_{\mathfrak{M}}$ is regular if and only if $d = d'$ by (**21.14**), as $\mathfrak{M}R_{\mathfrak{M}} = \mathfrak{n}$. Thus (1) holds.

For (2), first consider the case $\mathfrak{A} = \langle G \rangle$. Then G is irreducible as $\mathfrak{A}$ is prime. Assume $\partial G/\partial X_j = 0$ for all j, and let's find a contradiction. Let p be the characteristic of k. If $p = 0$, then G is constant, a contradiction. If $p > 0$, then the only monomials $X_1^{i_1} \cdots X_n^{i_n}$ appearing in G have $p \mid i_j$ for all j. But the coefficients of G are pth powers, as k is algebraically closed. Hence $G = G_1^p$ for some $G_1 \in P$, a contradiction. Thus $\partial G/\partial X_j \neq 0$ for some j.

Then $\partial G/\partial X_j \notin \mathfrak{A} := \langle G \rangle$, as $\deg G > \deg \partial G/\partial X_j$ and G is irreducible. By hypothesis, $F \notin \mathfrak{A}$. Set $H := F \cdot \partial G/\partial X_j$. Then $H \notin \mathfrak{A}$.

By the Hilbert Nullstellensatz (**15.37**)(2), P is Jacobson, since k is Jacobson by (**15.33**). So there's a choice of maximal ideal $\mathfrak{M}$ of P such that $\mathfrak{A} \subset \mathfrak{M}$, but $H \notin \mathfrak{M}$ by (**15.33.1**) as $\mathfrak{A}$ is prime. Since k is algebraically closed, $\mathfrak{M}$ corresponds to an $\mathbf{x}$ by (**15.5**). Then $G(\mathbf{x}) = 0$, but $F(\mathbf{x}) \neq 0$ and $(\partial G/\partial X_j)(\mathbf{x}) \neq 0$. Also $\dim P = n$ by (**15.11**), so $\dim P_{\mathfrak{M}} = n$ by (**15.12**), so $\dim R_{\mathfrak{M}} = n - 1$ by (**21.5**). Thus (1) implies $R_{\mathfrak{M}}$ is regular of dimension $n-1$. Thus (2) holds when $\mathfrak{A} = \langle G \rangle$.

For $\mathfrak{A}$ arbitrary, set $d := \dim R$. As R is a domain, $d := \operatorname{tr.deg}_k K$ by (**15.10**). But k is algebraically closed. So [**14**, Prp. 4.11(c), p. 367] or [**18**, Thm. 31, p. 105] provides a transcendence basis $\xi_1, \dots, \xi_d$ of K/k such that K is separable over $L := k(\xi_1, \dots, \xi_d)$. So [**14**, Thm. 4.6, p. 243] or [**18**, Thm. 19, p. 84] provides a primitive element $\xi_{d+1} \in K$; that is, $K = L(\xi_{d+1})$.

Set $R' = k[\xi_1, \dots, \xi_{d+1}]$. Then $K = \operatorname{Frac}(R')$. So $\dim(R') = d$ by (**15.10**). Let $P' := k[X'_1, \dots, X'_{d+1}]$ be the polynomial ring. Define $P' \twoheadrightarrow R'$ by $X'_i \mapsto \xi_i$ for all i, and let $\mathfrak{A}'$ be the kernel. Then $P'/\mathfrak{A}' = R'$. But $\dim(R') = d$ and $\dim(P') = d+1$ by (**15.11**). So $\operatorname{ht}(\mathfrak{A}') = 1$ by (**15.12**) as $\operatorname{ht}(\mathfrak{A}') = \dim(P'_{\mathfrak{A}'})$. But P' is a UFD. Thus (**21.33**) provides a $G' \in P'$ such that $\mathfrak{A}' = \langle G' \rangle$.

Note $K = \operatorname{Frac}(R') = \operatorname{Frac}(R)$. Say $\xi_i = x_i/s_i$ with $x_i, s_i \in R$ and $s_i \neq 0$ for all i. Set $s := \prod s_i$. Then $\xi_i \in R_s$ for all i. Thus $R' \subset R_s$. Similarly, $R_s \subset R'_{s'}$ for some nonzero $s' \in R'$. So $R' \subset R_s \subset R'_{s'}$. So $R'_{s'} \subset (R_s)_{s'} \subset (R'_{s'})_{s'}$. But s' is a unit in $R'_{s'}$. So $(R'_{s'})_{s'} = R'_{s'}$. Thus $R'_{s'} = (R_s)_{s'}$.

Let $f \in R$ be the residue of F. Say $f = f'/s'^n$ with $f' \in R'$. Then $f' \neq 0$ as $f \neq 0$ since $F \notin \mathfrak{A}$. Say f' is the residue of $F' \in P'$. The first case yields a maximal ideal $\mathfrak{M}' \supset \mathfrak{A}'$ of P' with $F' \notin \mathfrak{M}'$ and $R'_{\mathfrak{M}'}$ regular of dimension d. Let $\mathfrak{M} \subset P$ be the preimage of $\mathfrak{M}'R'_{s'}$. Then $\mathfrak{M}(R_s)_{s'} = \mathfrak{M}'R'_{s'}$ by (**11.12**)(2). So $F \notin \mathfrak{M}$ as $F' \notin \mathfrak{M}'$. Also, $R_{\mathfrak{M}} = R'_{\mathfrak{M}'}$ by (**11.16**) as $(R_s)_{s'} = R'_{s'}$. Also $\mathfrak{A} \subset \mathfrak{M}$ as $R_{\mathfrak{M}} \neq 0$. As k is algebraically closed, $\mathfrak{M}$ corresponds to an $\mathbf{x}$ by (**15.5**). Thus (2) holds. □

22. Completion

Exercise (22.3) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Prove that

$$\operatorname{Ker}(\kappa_M) = \bigcap F^n M. \qquad (\mathbf{22.3.1})$$

where κ_M is the map of **(22.1.2)**. Conclude that these conditions are equivalent:

(1) $\kappa_M\colon M \to \widehat{M}$ is injective; (2) $\bigcap F^n M = \{0\}$; (3) M is separated.

Assume M is Noetherian and $F^\bullet M$ is the $\mathfrak{a}$-adic filtration for a proper ideal $\mathfrak{a}$ with either (a) $\mathfrak{a} \subset \operatorname{rad}(M)$ or (b) R a domain and M torsionfree. Prove $M \subset \widehat{M}$.

Solution: A constant sequence (m) has 0 as a limit if and only if $m \in F^n M$ for all n. Thus **(22.3.1)** holds. So (1) and (2) are equivalent. Moreover, (2) and (3) are equivalent, as in **(22.1)** each was proved to hold if and only $\{0\}$ is closed.

Assume M is Noetherian. First, assume (a) too. Then (2) holds by **(18.35)** with $N := 0$, and so (1) follows. Thus $M \subset \widehat{M}$.

Instead, assume (b). Set $N := \bigcap \mathfrak{a}^n M$. By **(18.23)** or **(20.22)**, there's $x \in \mathfrak{a}$ with $(1+x)N = \langle 0 \rangle$. But $1+x \neq 0$ as $\mathfrak{a}$ is proper. Also, M is torsionfree. So again (2) holds and (1) follows. Thus $M \subset \widehat{M}$. □

Exercise (22.8) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Use **(22.7)** to compute $\widehat{F^k M} \subset \widehat{M}$. Then use **(22.3)** to show $\widehat{M}$ is separated.

Solution: By **(22.7)**, we may identify $\widehat{M}$ with the set of $(q_n) \in \prod_{n\geq 0} M/F^n M$ such that q_n is the residue of q_{n+1}. Then $\widehat{F^k M}$ is the subset of (q_n) such that $q_n \in (F^k M \cap F^n M)/F^n M$. So $q_n = 0$ for $n \leq k$. So $\bigcap \widehat{F^k M} = 0$. Thus **(22.3)** implies $\widehat{M}$ is separated. □

Exercise (22.9) . — Let $Q_0 \supset Q_1 \supset Q_2 \supset \cdots$ be a descending chain of modules, $\alpha_n^{n+1}\colon Q_{n+1} \hookrightarrow Q_n$ the inclusions. Show $\bigcap Q_n = \varprojlim Q_n$.

Solution: Define $\delta\colon \bigcap Q_n \to \prod Q_n$ by $\delta(q) := (q_n)$ where $q_n := q$. Plainly δ is a canonical isomorphism from $\bigcap Q_n$ onto $\varprojlim Q_n$, viewed inside $\prod Q_n$.

Alternatively, let $\alpha_n\colon \bigcap Q_n \hookrightarrow Q_n$ be the inclusion. Plainly a family of maps $\beta_n\colon P \to Q_n$ with $\alpha_n^{n+1}\beta_{n+1} = \beta_n$ amounts to a single map $\beta\colon P \to \bigcap Q_n$ via $\alpha_n\beta = \beta_n$ for all n. Thus $\bigcap Q_n$ has the requisite UMP. □

Exercise (22.12) . — Let R be a ring, M a module, $F^\bullet M$ a filtration, and $N \subset M$ a submodule. Give N and M/N the induced filtrations: $F^n N := N \cap F^n M$ and $F^n(M/N) := F^n M/F^n N$. Show the following: (1) $\widehat{N} \subset \widehat{M}$ and $\widehat{M}/\widehat{N} = \widehat{M/N}$.

(2) If $N \supset F^k M$ for some k, then $\kappa_{M/N}$ is bijective, $\kappa_{M/N}\colon M/N \xrightarrow{\sim} \widehat{M/N}$.

Solution: Set $P := M/N$. Then $F^n P := F^n M/F^n N := F^n M/(N \cap F^n M)$.

For (1), form this commutative diagram, whose rows are exact:

$$\begin{array}{ccccccccc}
0 & \to & F^n N & \to & F^n M & \to & F^n P & \to & 0\\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & P & \longrightarrow & 0
\end{array}$$

By the nine lemma, **(5.24)**, the next commutative diagram has exact rows too:

$$\begin{array}{ccccccccc}
0 & \to & N/F^{n+1}N & \to & M/F^{n+1}M & \to & P/F^{n+1}P & \to & 0\\
 & & \downarrow{\scriptstyle \alpha_n^{n+1}} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & N/F^n N & \longrightarrow & M/F^n M & \longrightarrow & P/F^n P & \longrightarrow & 0
\end{array}$$

Furthermore, α_n^{n+1} is surjective. So **(22.10)**(1)–(2) and **(22.7)** yield the desired exact sequence $0 \to \widehat{N} \to \widehat{M} \to \widehat{P} \to 0$. Thus (1) holds.

Note (2) holds, as $F^n P = 0$ for $n \geq k$, so every Cauchy sequence stabilizes. $\square$

Exercise (22.13) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Show:

(1) The canonical map $\kappa_M \colon M \to \widehat{M}$ is surjective if and only if M is complete.

(2) Given $(m_n) \in C(M)$, its residue $m \in \widehat{M}$ is the limit of the sequence $(\kappa_M m_n)$.

Solution: For (1), first assume κ_M surjective. Given $(m_n) \in C(M)$, let $m \in \widehat{M}$ be its residue. Say $m = \kappa_M m'$. Then the constant sequence (m') has residue m too. Set $m'_n := m_n - m'$ for all n. Then $(m'_n) \in Z(M)$ as $\widehat{M} := C(M)/Z(M)$. So (m_n) converges to m'. Thus M is complete.

Conversely, assume M complete. Given $m \in \widehat{M}$, say that m is the residue of $(m_n) \in C(M)$. As M is complete, (m_n) has a limit, say $m' \in M$. Set $m'_n := m_n - m'$ for all n. Plainly the residue of (m'_n) is equal to $m - \kappa_M m'$. But (m'_n) converges to 0, so its residue is 0. So $m - \kappa_M m' = 0$. Thus κ_M is surjective. Thus (1) holds.

In (2), given n_0, we must find n_1 with $m - \kappa_M m_{n'} \in \widehat{F^{n_0} M}$ for all $n' \geq n_1$. But (m_n) is Cauchy. So $m_n - m_{n'} \in F^{n_0} M$ for all $n, n' \geq n_1$ for some n_1. Fix $n' \geq n_1$ and set $m'_n := m_n - m_{n'}$. Then $m'_n - m'_{n''} = m_n - m_{n''}$ for all n''. But (m_n) is Cauchy, so (m'_n) is too. Let $m' \in \widehat{M}$ be its residue. Plainly $m' = m - \kappa_M m_{n'}$. But $m'_n \in F^{n_0} M$ for all $n \geq n_1$. So $m' \in \widehat{F^{n_0} M}$ by **(22.1)**. Thus (2) holds. $\square$

Exercise (22.14) . — Let R be a ring, M a module, and $F^\bullet M$ a filtration. Show that the following statements are equivalent: (1) κ_M is bijective;

(2) M is separated and complete; (3) κ_M is an isomorphism of filtered modules.

Assume M is Noetherian and $F^\bullet M$ is the $\mathfrak{a}$-adic filtration for a proper ideal $\mathfrak{a}$ with either (a) $\mathfrak{a} \subset \operatorname{rad}(M)$ or (b) R a domain and M torsionfree. Prove that M is complete if and only if $M = \widehat{M}$.

Solution: Note (1) and (2) are equivalent by **(22.3)** and **(22.13)**(1). Trivially, (3) implies (1), and the converse holds, since $\kappa_M^{-1} \widehat{F^n M} = F^n M$ by **(22.1)**.

To do the second part, note M is separated by **(22.3)**, and apply (2)$\Leftrightarrow$(1). $\square$

Exercise (22.15) . — Let R be a ring, $\alpha \colon M \to N$ a map of filtered modules, $\alpha' \colon \widehat{M} \to \widehat{N}$ a continuous map such that $\alpha' \kappa_M = \kappa_N \alpha$. Show $\alpha' = \widehat{\alpha}$.

Solution: Given $m \in \widehat{M}$, say m is the residue of $(m_n) \in C(M)$. Then m is the limit of $(\kappa_M m_n)$ by **(22.13)**(2). But α' is continuous. So $\alpha' m$ is the limit of $(\alpha' \kappa_M m_n)$. But $\alpha' \kappa_M = \kappa_N \alpha$. Thus $\alpha' m$ is the limit of $(\kappa_N \alpha m_n)$.

By construction, $\widehat{\alpha} m$ is the residue of (αm_n). So $\widehat{\alpha} m$ is the limit of $(\kappa_N \alpha m_n)$ by **(22.13)**(2). But $\widehat{N}$ is separated by **(22.8)**. So the limit of $(\kappa_N \alpha m_n)$ is unique. Thus $\alpha' m = \widehat{\alpha} m$. Thus $\alpha' = \widehat{\alpha}$. $\square$

Exercise (22.16) . — Let R be a ring, M a module, $F^\bullet M$ a filtration. Show:

(1) $G(\kappa_M) \colon G(M) \to G(\widehat{M})$ is bijective. (2) $\widehat{\kappa_M} \colon \widehat{M} \to \widehat{\widehat{M}}$ is bijective.

(3) $\kappa_{\widehat{M}} = \widehat{\kappa_M}$. (4) $\widehat{M}$ is separated and complete.

Solution: In (1), the maps $G_n(\kappa_M) \colon F^n M / F^{n+1} M \to F^n \widehat{M} / F^{n+1} \widehat{M}$ are, by definition, induced by κ_M. But $F^k \widehat{M} := \widehat{F^k M}$ for all k. Also, κ_M induces a bijection $F^n M / F^{n+1} M \xrightarrow{\sim} \widehat{F^n M} / \widehat{F^{n+1} M}$ by **(22.12)**(1)–(2). Thus (1) holds.

For (2), let $\kappa_n\colon M/F^nM \to \widehat{M}/F^n\widehat{M}$ be the map induced by κ_M for $n \geq 0$. Then $\widehat{\kappa_M} = \varprojlim \kappa_n$ by **(22.7)**. But $F^n\widehat{M} := \widehat{F^nM}$. So κ_n is bijective by **(22.12)**(1)–(2). Thus (2) holds.

For (3), recall from **(22.1)** that κ_M and $\kappa_{\widehat{M}}$ are maps of filtered modules, so continuous. Apply **(22.15)** with $\alpha := \kappa_M$ and $\alpha' := \kappa_{\widehat{M}}$. Thus (3) holds.

For (4), note $\kappa_{\widehat{M}}$ is bijective by (2) and (3). Thus **(22.14)** yields (4). □

Exercise (22.28) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable. Filter $R[[X]]$ with the ideals $\mathfrak{b}_n$ consisting of the $H =: \sum h_iX^i$ with $h_i \in \mathfrak{a}^n$ for all i. Show: (1) that $\widehat{R}[[X]] = R[[X]]^{\widehat{}}$ and (2) that if R is separated and complete, then so is $R[[X]]$.

Solution: For (1), owing to **(22.7)**, it suffices to find a canonical isomorphism $\varphi\colon (\varprojlim R/\mathfrak{a}^n)[[X]] \xrightarrow{\sim} \varprojlim(R[[X]]/\mathfrak{b}_n)$. Plainly $(R/\mathfrak{a}^n)[[X]] = R[[X]]/\mathfrak{b}_n$. So given $F = \sum f_iX^i \in (\varprojlim R/\mathfrak{a}^n)[[X]]$, let $f_{i,n} \in R/\mathfrak{a}^n$ be the image of f_i for all i, n. Note that the vector $\big(\sum_i f_{i,n}X^i\big)$ lies in $\varprojlim(R[[X]]/\mathfrak{b}_n)$. Set $\varphi(F) := \big(\sum_i f_{i,n}X^i\big)$.

Suppose $\varphi(F) = 0$. Then $f_{i,n} = 0$ for all i, n. So $F = 0$. Thus φ is injective.

Finally, given $G =: (\sum_i g_{i,n}X^i) \in \varprojlim(R[[X]]/\mathfrak{b}_n)$, note $g_i := (g_{i,n}) \in \varprojlim(R/\mathfrak{a}^n)$ for all i. Note $\varphi\big(\sum g_iX^i\big) = G$. Thus φ is surjective, so an isomorphism.

For (2), note $R = \widehat{R}$ by **(22.14)**. Also, $R[[X]]^{\widehat{}}$ is separated and complete by **(22.16)**(4). Thus (1) implies (2).

Alternatively, here's a direct proof of (2). First, as R is separated, $\bigcap \mathfrak{a}^n = 0$ by **(22.3)**. So $\bigcap \mathfrak{b}_n = 0$. Thus **(22.3)** implies $R[[X]]$ is separated.

As to the completeness of $R[[X]]$, fix a Cauchy sequence (F_n). Given n_0, there's n_1 with $F_n - F_{n'} \in \mathfrak{b}_{n_0}$ for $n, n' \geq n_1$. Say $F_n =: \sum f_{n,i}X^i$. Then $f_{n,i} - f_{n',i} \in \mathfrak{a}^{n_0}$ for all i. Thus $(f_{n,i})$ is Cauchy in R. But R is separated and complete. So $(f_{n,i})$ has a unique limit g_i.

Set $G := \sum_{i\geq 0} g_iX^i$. Let's show $G = \lim F_n$. Given i, there's $n' \geq n_1$ with $f_{n',i} - g_i \in \mathfrak{a}^{n_0}$. But $f_{n,i} - g_i = f_{n,i} - f_{n',i} + f_{n',i} - g_i$. So $f_{n,i} - g_i \in \mathfrak{a}^{n_0}$ for $n \geq n_1$. So $F_n - G \in \mathfrak{b}_{n_0}$. Thus $G = \lim F_n$. Thus $R[[X]]$ is complete. □

Exercise (22.29) . — In $\widehat{\mathbb{Z}}_2$, evaluate the sum $s := 1 + 2 + 4 + 8 + \cdots$.

Solution: Set $a_n := 2^n$ and $b_n := 1 - a_{n+1}$ and $c_n := 1 + a_1 + \cdots + a_n$. Then (b_n) converges to 1. Moreover, (c_n) is Cauchy, and it represents $s \in \widehat{\mathbb{Z}}_2$. But $b_0c_n = b_n$. Hence $b_0s = 1$. Thus $s = 1/b_0 = 1/(1-2) = -1$. □

Exercise (22.30) . — Let R be a ring, $\alpha_n^{n+1}\colon Q_{n+1} \to Q_n$ linear maps for $n \geq 0$. Set $\alpha_n^m := \alpha_n^{n+1} \cdots \alpha_{m-1}^m$ for $m > n$ and $\alpha_n^n = 1$. Assume the **Mittag-Leffler Condition**: for all $n \geq 0$, there's $m \geq n$ such that

$$Q_n \supset \alpha_n^{n+1}Q_{n+1} \supset \cdots \supset \alpha_n^mQ_m = \alpha_n^{m+1}Q_{m+1} = \cdots .$$

Set $P_n := \bigcap_{m\geq n} \alpha_n^mQ_m$, and prove $\alpha_n^{n+1}P_{n+1} = P_n$. Conclude that $\varprojlim^1 Q_n = 0$.

Solution: Given n, there's $m > n+1$ with $P_n = \alpha_n^mQ_m$ and $P_{n+1} = \alpha_{n+1}^mQ_m$. But $\alpha_n^mQ_m = \alpha_n^{n+1}\alpha_{n+1}^mQ_m$. Thus $\alpha_n^{n+1}P_{n+1} = P_n$.

To conclude $\varprojlim^1 Q_n = 0$, form this commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \to & \prod P_n & \to & \prod Q_n & \to & \prod(Q_n/P_n) & \to & 0\\
 & & \big\downarrow{\scriptstyle\theta} & & \big\downarrow{\scriptstyle\theta} & & \big\downarrow{\scriptstyle\theta} & & \\
0 & \to & \prod P_n & \to & \prod Q_n & \to & \prod(Q_n/P_n) & \to & 0
\end{array}$$

where each θ is the map of (**22.5**). Apply the Snake Lemma (**5.10**). It yields the following exact sequence of cokernels:

$$\varprojlim^1 P_n \to \varprojlim^1 Q_n \to \varprojlim^1 (Q_n/P_n).$$

Since $\alpha_n^{n+1}P_{n+1} = P_n$, the restriction $\alpha_n^{n+1}\big|P_{n+1}$ is surjective. So $\varprojlim^1 P_n = 0$ by (**22.10**)(1). Thus it suffices to show $\varprojlim^1(Q_n/P_n) = 0$.

Since $\alpha_n^m Q_m = P_n$, the induced map $(Q_m/P_m) \to (Q_n/P_n)$ is 0. Thus replacing each Q_n with Q_n/P_n, we need only show $\varprojlim^1 Q_n = 0$ assuming $\alpha_n^m = 0$.

Given $(q_n) \in \prod Q_n$, set $p_n := \sum_{h=n}^{\infty} \alpha_n^h q_h$, noting $\alpha_n^h = \alpha_n^m \alpha_m^h = 0$ for all $h \ge m$. Then $\theta p_n := p_n - \alpha_n^{n+1} p_{n+1} = q_n$. So θ is surjective. Thus $\varprojlim^1 Q_n = 0$. □

Exercise (22.31) . — Let R be a ring, and $\mathfrak{a}$ an ideal. Set $S := 1 + \mathfrak{a}$ and set $T := \kappa_R^{-1}(\widehat{R}^\times)$. Given $t \in R$, let $t_n \in R/\mathfrak{a}^n$ be its residue for all n. Show:

(1) Given $t \in R$, then $t \in T$ if and only if $t_n \in (R/\mathfrak{a}^n)^\times$ for all n.
(2) Then $T = \{t \in R \mid t$ lies in no maximal ideal containing $\mathfrak{a}\}$.
(3) Then $S \subset T$, and $\widehat{R}$ is the completion of $S^{-1}R$ and of $T^{-1}R$.
(4) Assume $\kappa_R \colon R \to \widehat{R}$ is injective. Then $\kappa_{S^{-1}R}$ and $\kappa_{T^{-1}R}$ are too.
(5) Assume $\mathfrak{a}$ is a maximal ideal $\mathfrak{m}$. Then $\widehat{R} = \widehat{R_{\mathfrak{m}}}$.

Solution: For (1), by (**22.7**), regard $\widehat{R}$ as a submodule of $\prod R/\mathfrak{a}^n$. Then each t_n is equal to the projection of $\kappa_R(t)$. Thus t_n is a unit if $\kappa_R(t)$ is. Conversely, assume t_n is a unit for each n. Then there are $u_n \in R$ with $u_n t \equiv 1 \pmod{\mathfrak{a}^n}$. By the uniqueness of inverses, $u_{n+1} \equiv u_n$ in $R/\mathfrak{a}^n$ for each n. Set $u := (u_n) \in \prod R/\mathfrak{a}^n$. Then $u \in \widehat{R}$, and $u\kappa_R(t) = 1$. Thus $\kappa_R(t)$ is a unit. Thus (1) holds.

For (2), note $T = \{t \in R \mid t_n \in (R/\mathfrak{a}^n)^\times$ for all $n\}$ by (1). But $t_n \in (R/\mathfrak{a}^n)^\times$ if and only if t_n lies in no maximal ideal of $R/\mathfrak{a}^n$ by (**2.22**). Thus (**1.9**) yields (2).

For (3), note $S \subset T$ owing to (2) as no maximal ideal can contain both x and $1 + x$. Moreover, the UMP of localization (**11.3**) yields this diagram:

$$\begin{tikzcd} R \arrow[d, "\varphi_S"'] \arrow[dr, "\varphi_T"] \arrow[drr, "\kappa_R"] & & \\ S^{-1}R \arrow[r] & T^{-1}R \arrow[r] & \widehat{R} \end{tikzcd}$$

Further, S and T map into $(R/\mathfrak{a}^n)^\times$; hence, (**11.4**) and (**12.15**) yield:

$$R/\mathfrak{a}^n = S^{-1}R/\mathfrak{a}^n S^{-1}R \quad \text{and} \quad R/\mathfrak{a}^n = T^{-1}R/\mathfrak{a}^n T^{-1}R.$$

Therefore, $\widehat{R}$ is, by (**22.7**), equal to the completion of each of $S^{-1}R$ and $T^{-1}R$ in their $\mathfrak{a}$-adic topology. Thus (3) holds.

For (4), say $\kappa_{S^{-1}R}(x/s) = 0$. But $\kappa_{S^{-1}R}(x/s) = \kappa_R(x)\kappa_R(s)^{-1}$. So $\kappa_R(x) = 0$. But κ_R is injective. So $x = 0$. So $x/s = 0$ in $S^{-1}R$. Thus $\kappa_{S^{-1}R}$ is injective. Similarly, $\kappa_{T^{-1}R}$ is injective. Thus (4) holds.

For (5), note $T = R - \mathfrak{m}$ by (2). Thus (3) yields (5). □

Exercise (22.32) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a finitely generated module. Show $\widehat{R} \cdot \kappa_M(M) = \widehat{M}$.

Solution: As M is finitely generated, the canonical map $\widehat{R} \otimes M \to \widehat{M}$ is surjective by (**22.19**). But its image is $\widehat{R} \cdot \kappa_M(M)$. Thus $\widehat{R} \cdot \kappa_M(M) = \widehat{M}$. □

Exercise (22.33) . — Let R be a ring, M a module, $F^\bullet M$ a filtration, and N a submodule. Give N the induced filtration: $F^nN := N \cap F^nM$ for all n. Show:

(1) $\widehat{N}$ is the closure of $\kappa_M N$ in $\widehat{M}$. (2) $\kappa_M^{-1}\widehat{N}$ is the closure of N in M.

Solution: For (1), set $P := M/N$, and give P the induced filtration. Then the canonical sequence $0 \to \widehat{N} \to \widehat{M} \xrightarrow{\widehat{\alpha}} \widehat{P} \to 0$ is exact by **(22.12)**(1). So $\widehat{N} = \widehat{\alpha}^{-1}\{0\} \subset \widehat{M}$. But $\widehat{P}$ is separated by **(22.16)**(4); so $\{0\}$ is closed by **(22.1)**. But $\widehat{\alpha}$ is continuous by **(22.1)**. Thus $\widehat{N}$ is closed in $\widehat{M}$.

Every $m \in \widehat{N}$ is the residue of some sequence $(m_n) \in C(N)$ by **(22.1)**. Then m is the limit in $\widehat{N}$ of $(\kappa_N m_n)$ by **(22.13)**(2). But $\kappa_N = \kappa_M|N$ and the inclusion $\widehat{N} \hookrightarrow \widehat{M}$ is continuous; see **(22.1)**. So m is the limit in $\widehat{M}$ of $(\kappa_M m_n)$. Thus $\kappa_M N$ is dense in $\widehat{N}$. But $\widehat{N}$ is closed in $\widehat{M}$ by the above. Thus (1) holds.

For (2), first let's show that every open set U of M is equal to $\kappa_M^{-1}V$ for some open set V of $\widehat{M}$. Write U as the union of the sets $m + F^nM$ for suitable m and n. Let V be the corresponding union of the sets $\kappa_M m + F^n\widehat{M}$. Then V is open.

Moreover, $\kappa_M^{-1}V$ is the union of the sets $\kappa_M^{-1}(\kappa_M m + F^n\widehat{M})$. And it is easy to check that $\kappa_M^{-1}(\kappa_M m + F^n\widehat{M}) = m + \kappa_M^{-1}F^n\widehat{M}$. But $\kappa_M^{-1}F^n\widehat{M} = F^nM$ by **(22.1)**. Thus $U = \kappa_M^{-1}V$.

Finally, given a closed set X of M containing N, set $U := N - X$. By the above, $U = \kappa_M^{-1}V$ for some open set V of $\widehat{M}$. Set $Y := \widehat{M} - V$. Then $\kappa_M^{-1}Y = X$. So $Y \supset \kappa_M N$. So (1) implies $Y \supset \widehat{N}$. So $X \supset \kappa_M^{-1}\widehat{N}$. Now, $\widehat{N}$ is closed in $\widehat{M}$ by (1), and κ_M is continuous by **(22.1)**; so $\kappa_M^{-1}\widehat{N}$ is closed in M. Thus $\kappa_M^{-1}\widehat{N}$ is the smallest closed set containing N; in other words, (2) holds.

Alternatively, note that **(22.7)** yields

$$\widehat{N} = \varprojlim N/(N \cap F^nM) = \varprojlim (N + F^nM)/F^nM \subset \varprojlim M/F^nM = \widehat{M}.$$

Now, given $m \in M$, let q_n be the residue of m in M/F^nM. Then $\kappa_M(m)$ is the vector (q_n). Hence $\kappa_M(m) \in \widehat{N}$ if and only if $m \in N + F^nM$ for all n, that is, if and only if $m \in \bigcap(N + F^nM)$. Thus $\kappa_M^{-1}\widehat{N} = \bigcap(N + F^nM)$. But $\bigcap(N + F^nM)$ is equal to the closure of N in M by **(22.1)**. Thus (2) holds. □

Exercise (22.34) . — Let R be a ring, $\mathfrak{a}$ an ideal. Show that every closed maximal ideal $\mathfrak{m}$ contains $\mathfrak{a}$.

Solution: As $\mathfrak{m}$ is closed, $\mathfrak{m} = \bigcap_n(\mathfrak{m} + \mathfrak{a}^n)$. But $\mathfrak{m} \neq R$. So $\mathfrak{m} + \mathfrak{a}^n \neq R$ for some n. But $\mathfrak{m}$ is maximal. So $\mathfrak{m} = \mathfrak{m} + \mathfrak{a}^n \supset \mathfrak{a}^n$. But $\mathfrak{m}$ is prime. Thus $\mathfrak{m} \supset \mathfrak{a}$. □

Exercise (22.35) . — Let R be a ring, $\mathfrak{a}$ an ideal. Show equivalent:

(1) $\mathfrak{a} \subset \operatorname{rad}(R)$. (2) Every element of $1 + \mathfrak{a}$ is invertible.

(3) Given any finitely generated R-module M, if $M = \mathfrak{a}M$, then $M = 0$.

(4) Every maximal ideal $\mathfrak{m}$ is closed.

Show, moreover, that (1)–(4) hold if R is separated and complete.

Solution: Assume (1). Then **(3.2)** yields (2).

Assume (2). By **(10.3)**, there's $a \in \mathfrak{a}$ with $(1 + a)M = 0$. Thus (2) implies (3).

Assume (3). Consider (4). Set $M := R/\mathfrak{m}$. Then $M \neq 0$. So (3) yields $M \neq \mathfrak{a}M$. But $\mathfrak{a}M = (\mathfrak{a} + \mathfrak{m})/\mathfrak{m}$. So $\mathfrak{a} + \mathfrak{m} \neq R$. So $\mathfrak{a} \subset \mathfrak{m}$. Thus **(22.1)** yields (4).

Assume (4). Then **(22.34)** yields (1).

Moreover, assume R is complete. Form the $\mathfrak{a}$-adic completions $\widehat{R}$ and $\widehat{\mathfrak{a}}$. Then $R = \widehat{R}$, and $\mathfrak{a} = \widehat{\mathfrak{a}}$ by **(22.14)**(2)⇒(3). But $\widehat{\mathfrak{a}} \subset \mathrm{rad}(\widehat{R})$ by **(22.4)**. Thus (1) holds, and so (2)–(4) hold too □

Exercise (22.36) . — Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Show equivalent:

(1) R is a **Zariski ring**; that is, R is Noetherian, and $\mathfrak{a} \subset \mathrm{rad}(R)$.
(2) Every finitely generated module M is separated.
(3) Every submodule N of every finitely generated module M is closed.
(4) Every ideal $\mathfrak{b}$ is closed. (5) Every maximal ideal $\mathfrak{m}$ is closed.
(6) Every faithfully flat, finitely generated module M has a faithfully R-flat $\widehat{M}$.
(7) The completion $\widehat{R}$ is faithfully R-flat.

Solution: Assume (1). In (2), M is finitely generated. But R is Noetherian. So M is Noetherian. Set $N := \bigcap_{n\ge 0} \mathfrak{a}^n M$. Then there's $a \in \mathfrak{a}$ with $(1+a)N = 0$ by **(18.23)**. But $1 + a \in R^\times$ by **(22.35)**. So $N = 0$. Thus, **(22.3)** yields (2).

Assume (2). Then in (3), M/N is separated. So $\{0\}$ is closed by **(22.1)**. Also, the quotient map $M \to M/N$ is continuous by **(22.1)**. Thus (3) holds.

Trivially, (3) implies (4), and (4) implies (5). And (5) implies (1) by **(22.35)**.

Assume (1) again. To prove (6), note $\widehat{M}$ is flat over R by **(22.22)**. So by **(9.19)** (3)⇒(1), it remains to show $\widehat{M} \otimes (R/\mathfrak{m}) \neq 0$ for all maximal ideals $\mathfrak{m}$ of R.

Note $\widehat{M} \otimes (R/\mathfrak{m}) = \widehat{M}/\mathfrak{m}\widehat{M}$ by **(8.27)**(1). And $\mathfrak{m}\widehat{M} = (\mathfrak{m}M)\widehat{\ }$ by **(22.20)**. Set $N := M/\mathfrak{m}M$. Then $\widehat{M}/(\mathfrak{m}M)\widehat{\ } = \widehat{N}$ by **(22.12)**(1). Thus $\widehat{M} \otimes (R/\mathfrak{m}) = \widehat{N}$.

Note $\mathfrak{a} \subset \mathrm{rad}(R)$ by (1). So $\mathfrak{a} \subset \mathfrak{m}$. So $\mathfrak{a}^r N = 0$ for all r. So every Cauchy sequence stabilizes. Hence $N = \widehat{N}$. So $\widehat{M} \otimes (R/\mathfrak{m}) = N$. But $N = M \otimes (R/\mathfrak{m})$, and M is faithfully flat; so $N \neq 0$ by **(9.19)**(1)⇒(3). Thus (1) implies (6).

Trivially (6) implies (7).

Finally, assume (7). Given a maximal ideal $\mathfrak{m}$, set $k := R/\mathfrak{m}$. Then $\widehat{R} \otimes k \neq 0$ by **(9.19)**(1)⇒(3). But $\widehat{R} \otimes k = \widehat{k}$ by **(22.19)**. So $\varprojlim (k/\mathfrak{a}^n k) \neq 0$ by **(22.7)**. So $k/\mathfrak{a}^n k \neq 0$ for some $n \geq 1$. So $\mathfrak{a}^n k = 0$. So $\mathfrak{a}^n \subset \mathfrak{m}$. So $\mathfrak{a} \subset \mathfrak{m}$. Thus (1) holds. □

Exercise (22.37) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module. Prove:

(1) $\bigcap_{n=1}^\infty \mathfrak{a}^n M = \bigcap_{\mathfrak{m}\in\Psi} \mathrm{Ker}(M \xrightarrow{\varphi_\mathfrak{m}} M_\mathfrak{m})$ where $\Psi := \{\, \mathfrak{m} \supset \mathfrak{a} \mid \mathfrak{m} \text{ maximal} \,\}$.
(2) $\widehat{M} = 0$ if and only if $\mathrm{Supp}(M) \cap \mathbf{V}(\mathfrak{a}) = \emptyset$.

Solution: Set $N := \bigcap_n \mathfrak{a}^n M$ and $K := \bigcap_{\mathfrak{m}\in\Psi} \mathrm{Ker}(\varphi_\mathfrak{m})$.

For (1), use double inclusion. The Krull Intersection Theorem **(18.23)** yields $x \in \mathfrak{a}$ with $(1+x)N = 0$. Given $\mathfrak{m} \in \Psi$, note $(1+x)\varphi_\mathfrak{m}(N) = 0$. But $x \in \mathfrak{a} \subset \mathfrak{m}$; so $(1+x)/1 \in R_\mathfrak{m}^\times$ by **(3.2)**. So $\varphi_\mathfrak{m}(N) = 0$. So $N \subset \mathrm{Ker}(\varphi_\mathfrak{m})$. Thus $N \subset K$.

To show $N \supset K$, fix a maximal ideal $\mathfrak{m}$. By **(12.4)**(2), $(\varphi_\mathfrak{m})_\mathfrak{m} \colon M_\mathfrak{m} \xrightarrow{\sim} (M_\mathfrak{m})_\mathfrak{m}$. So $\mathrm{Ker}((\varphi_\mathfrak{m})_\mathfrak{m}) = 0$. Thus **(12.13)** and **(9.3)** yield $(\mathrm{Ker}(\varphi_\mathfrak{m}))_\mathfrak{m} = \mathrm{Ker}((\varphi_\mathfrak{m})_\mathfrak{m}) = 0$.

Suppose $\mathfrak{m} \in \Psi$. Then $K \subset \mathrm{Ker}(\varphi_\mathfrak{m})$. Hence $(\mathfrak{a}K)_\mathfrak{m} \subset K_\mathfrak{m} \subset (\mathrm{Ker}(\varphi_\mathfrak{m}))_\mathfrak{m}$ by **(12.12)**(1)(b). Thus $(\mathfrak{a}K)_\mathfrak{m} = K_\mathfrak{m} = 0$.

Suppose $\mathfrak{m} \notin \Psi$. Then $\mathfrak{a}R_\mathfrak{m}$ contains a unit. Thus $(\mathfrak{a}K)_\mathfrak{m} = K_\mathfrak{m}$.

So $(\mathfrak{a}K)_\mathfrak{m} = K_\mathfrak{m}$ in any case. So **(13.53)** yields $\mathfrak{a}K = K$. So

$$K = \mathfrak{a}K = \mathfrak{a}^2 K = \cdots = \textstyle\bigcap_{n=1}^\infty \mathfrak{a}^n K.$$

But $\mathfrak{a}^n M \supset \mathfrak{a}^n K$ for all n. Thus $N \supset K$. But $N \subset K$. So $N = K$. Thus (1) holds.

For (2), first assume $\widehat{M} = 0$. Then **(22.3.1)** gives $M = N$. But $M \supset \mathfrak{a}M \supset N$.

Thus $M = \mathfrak{a}M$. Conversely, assume $M = \mathfrak{a}M$. Then $\mathfrak{a}^n M = \mathfrak{a}^{n+1}M$ for all $n \geq 0$. So $\mathfrak{a}^n M = M$ for all n. Hence $C(M) = Z(M)$. Thus $\widehat{M} = 0$.

Thus $\widehat{M} = 0$ if and only if $M = \mathfrak{a}M$, or equivalently, $M/\mathfrak{a}M = 0$. But $M/\mathfrak{a}M = 0$ if and only if $\mathrm{Supp}(M/\mathfrak{a}M) = \emptyset$ by **(13.8)**. And $\mathrm{Supp}(M/\mathfrak{a}M) = \mathrm{Supp}(M) \cap \mathbf{V}(\mathfrak{a})$ by **(13.46)**(1) as M is finitely generated. Thus (2) holds. □

Exercise (22.38) . — Let R be a ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ maximal ideals, and M module. Set $\mathfrak{m} := \bigcap \mathfrak{m}_i$, and give M the $\mathfrak{m}$-adic topology. Show $\widehat{M} = \prod \widehat{M_{\mathfrak{m}_i}}$.

Solution: For each $n > 0$, the $\mathfrak{m}_i^n$ are pairwise comaximal by **(1.21)**(3). So $R/\mathfrak{m}^n = \prod_{i=1}^m R/\mathfrak{m}_i^m$ by **(1.21)**(4)(b)–(c). Tensor with M; then **(8.27)**(1) and **(8.10)** yield $M/\mathfrak{m}^n M = \prod_{i=1}^m M/\mathfrak{m}_i^n M$. But $M/\mathfrak{m}_i^n M = M_{\mathfrak{m}_i}/\mathfrak{m}_i^n M_{\mathfrak{m}_i}$ by **(12.34)**. So $M/\mathfrak{m}^n M = \prod_{i=1}^m (M_{\mathfrak{m}_i}/\mathfrak{m}_i^n M_{\mathfrak{m}_i})$. Taking inverse limits, we obtain the assertion by **(22.7)**, because inverse limit commutes with finite product by its construction, or by **(8.14)** as completion is a linear functor by **(22.1)**. □

Exercise (22.39) . — (1) Let R be a ring, $\mathfrak{a}$ an ideal. If $G_{\mathfrak{a}}(R)$ is a domain, show $\widehat{R}$ is an domain. If also $\bigcap_{n\geq 0} \mathfrak{a}^n = 0$, show R is a domain.

(2) Use (1) to give an alternative proof that a regular local ring A is a domain.

Solution: Consider (1). Let $x, y \in \widehat{R}$ be nonzero. Note $\widehat{R}$ is separated by **(22.16)**(4). So $\bigcap_{n\geq 0} \widehat{\mathfrak{a}}^n = 0$ by **(22.3)**. So there are $r, s \geq 0$ with $x \in \widehat{\mathfrak{a}}^{\,r} - \widehat{\mathfrak{a}}^{\,r+1}$ and $y \in \widehat{\mathfrak{a}}^{\,s} - \widehat{\mathfrak{a}}^{\,s+1}$. Let $x' \in G_r(\widehat{R})$ and $y' \in G_s(\widehat{R})$ be the residues of x and y. Then $x' \neq 0$ and $y' \neq 0$. Note $G(\widehat{R}) = G(R)$ by **(22.16)**(1).

Assume $G(R)$ is a domain. Then $x'y' \neq 0$. Hence $x'y' \in G_{r+s}(\widehat{R})$ is the residue of $xy \in \widehat{\mathfrak{a}}^{\,r+s}$. Hence $xy \neq 0$. Thus $\widehat{R}$ is a domain, as desired.

Assume $\bigcap \mathfrak{a}^n = 0$. Then $R \subset \widehat{R}$ by **(22.3)**. Thus R is a domain if $\widehat{R}$ is, as desired.

As to (2), denote the maximal ideal of A by $\mathfrak{m}$. Then $\bigcap_{n\geq 0} \mathfrak{m}^n = 0$ owing to **(18.23)** and **(3.2)**. But $G(A)$ is a polynomial ring by **(21.15)**, so a domain. Thus A is a domain by (1), as desired. □

Exercise (22.40) . — (1) Let R be a Noetherian ring, $\mathfrak{a}$ an ideal. Assume that $G_{\mathfrak{a}}(R)$ is a normal domain and that $\bigcap_{n\geq 0}(sR + \mathfrak{a}^n) = sR$ for any $s \in R$. Show using induction on n and applying **(16.40)** that R is a normal domain.

(2) Use (1) to prove a regular local ring A is normal.

Solution: In (1), $G_{\mathfrak{a}}(R)$ is a domain; so R is one too by **(22.39)**. Given any $x \in \mathrm{Frac}(R)$ that is integral over R, there is a nonzero $d \in R$ such that $dx^n \in R$ for all $n \geq 0$ by **(16.40)**. Say $x = y/s$ with $y, s \in R$. Let's show $y \in sR + \mathfrak{a}^n$ for all n by induction. Then $y \in \bigcap_{n\geq 0}(sR + \mathfrak{a}^n) = sR$. So $y/s \in R$ as desired.

For $n = 0$, trivially $y \in sR + \mathfrak{a}^n$. Given $n \geq 0$ with $y \in sR + \mathfrak{a}^n$, say $y = sz + w$ with $z \in R$ and $w \in \mathfrak{a}^n$. Given $q \geq 0$, set $w_q := d(x - z)^q$. Then $w_q = \sum_i \pm\binom{q}{i} dx^i z^{q-i}$. But $dx^i \in R$. So $w_q \in R$. But $x = z + (w/s)$. So $d(w/s)^q = w_q$ or $dw^q = w_q s^q$.

Given any nonzero $a, a' \in R$, let $v(a)$ be greatest with $a \in \mathfrak{a}^{v(a)}$; there is such a $v(a)$, as $\bigcap_{n\geq 0} \mathfrak{a}^n = 0$ by the hypothesis with $s := 0$. Denote the residue of a in $G_{v(a)}(R)$ by $G(a)$. Plainly $G(aa') = G(a)G(a')$ if and only if $G(a)G(a') \neq 0$.

But $G(R)$ is a domain. Hence $G(d)G(w)^q = G(dw^q) = G(w_q s^q) = G(w_q)G(s)^q$. So $G(d)\big(G(w)/G(s)\big)^q = G(w_q) \in G(R)$. But $G(R)$ is normal. So **(16.40)** yields $G(w)/G(s) \in G(R)$. Plainly $G(w)/G(s) \in G_v(R)$ where $v := v(w) - v(s)$. Say

$G(w)/G(s) = G(t)$ for $t \in R$. But $w \in \mathfrak{a}^n$. Hence $w \equiv st \pmod{\mathfrak{a}^{n+1}}$. Hence $y \equiv s(z+t) \pmod{\mathfrak{a}^{n+1}}$. Thus $y \in sR + \mathfrak{a}^{n+1}$ as desired.

For (2), let $\mathfrak{m}$ denote the maximal ideal. Since A is Noetherian, **(18.35)** yields $sA = \bigcap_{n\ge 0}(sA + \mathfrak{m}^n)$ for every s. Since A is regular, $G(A)$ is a polynomial ring by **(21.15)**. But a polynomial ring is a normal domain by **(10.22)**(1). Thus (2) follows from (1). □

Exercise (22.41) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module with $\ell_R(M) < \infty$.

(1) Assume M is simple. Show $\widehat{M}$ is simple if $\mathfrak{a} \subset \operatorname{Ann}(M)$, but $\widehat{M} = 0$ if not.

(2) Show $\ell_{\widehat{R}}(\widehat{M}) \le \ell_R(M)$, with equality if and only if $\mathfrak{a} \subset \operatorname{rad}(M)$.

Solution: For (1), set $\mathfrak{m} := \operatorname{Ann}(M)$. Assume $\mathfrak{a} \subset \mathfrak{m}$. Then $\mathfrak{a}^n M = 0$ for $n \ge 1$. So every Cauchy sequence stabilizes. So $M = \widehat{M}$. Thus $\widehat{M}$ is simple.

Conversely, assume $\mathfrak{a} \not\subset \mathfrak{m}$. Now, $\mathfrak{m}$ is maximal by **(19.2)**(2). So $\mathfrak{a}^n + \mathfrak{m} = R$. So $\mathfrak{a}^n M = M$. So every sequence converges to 0. Thus $\widehat{M} = 0$. Thus (1) holds.

In (2), M is Noetherian by **(19.5)**. Let $M = M_0 \supset M_1 \supset \cdots \supset M_m = 0$ be a composition series. Set $\mathfrak{m}_i := \operatorname{Ann}(M_{i-1}/M_i)$. Then $\widehat{M} \supset \widehat{M}_1 \supset \cdots \supset \widehat{M}_m = 0$ is a chain of submodules by **(22.18)**, in which $\widehat{M_{i-1}}/\widehat{M}_i$ is simple if $\mathfrak{a} \subset \mathfrak{m}_i$ and is 0 if not by (1). So by **(19.3)**, $\ell_{\widehat{R}}(\widehat{M}) \le \ell_R(M)$, with equality if and only if $\mathfrak{a} \subset \mathfrak{m}_i$ for all i. But the $\mathfrak{m}_i$ are maximal by **(19.2)**(2), and $\{\mathfrak{m}_i\} = \operatorname{Supp}(M)$ by **(19.3)** again; so $\bigcap \mathfrak{m}_i = \operatorname{rad}(M)$. Thus (2) holds. □

Exercise (22.42) . — Let R be a ring, M a module with two filtrations $F^\bullet M$ and $G^\bullet M$. For all m, give $G^m M$ the filtration induced by $F^\bullet M$, and let $(G^m M)^F$ be its completion; filter M^F by the $(G^m M)^F$, and let $(M^F)^G$ be the completion. Define $H^\bullet M$ by $H^p M := F^p M + G^p M$, and let M^H be the completion. Show:

$$(M^F)^G = \varprojlim_m \varprojlim_n M/(F^n M + G^m M) = M^H. \qquad \textbf{(22.42.1)}$$

Solution: Note $(M^F)^G = \varprojlim_m M^F/(G^m M)^F$ by **(22.7)**. Now, for all m,

$$M^F/(G^m M)^F = (M/G^m M)^F = \varprojlim_n \big((M/G^m M)/(F^n(M/G^m M)\big)$$

by **(22.12)**(1) and by **(22.7)** again. But $F^n(M/G^m M) = F^n M/(F^n M \cap G^m M)$ by definition. So $(M/G^m M)/F^n(M/G^m M) = M/(F^n M + G^m M)$ by the two Noether isomorphisms, **(4.8.2)** and **(4.8.1)**. Thus the first equality in **(22.42.1)** holds.

For the second equality in **(22.42.1)**, note that $M^H = \varprojlim_p M/H^p M$ by **(22.7)** again. Set $M_{m,n} := M/(F^n M + G^m M)$. Thus it suffices to find a canonical map $\alpha\colon \varprojlim_m \varprojlim_n M_{m,n} \to \varprojlim_p M_{p,p}$ and to show α is an isomorphism.

Let's show the projections $\pi\colon \prod_m \prod_n M_{m,n} \to \prod_p M_{p,p}$ induce the desired α.

Let $(x_{m,n}) \in \prod_m \prod_n M_{m,n}$ be in $\varprojlim_m \varprojlim_n M_{m,n}$. Then the residue $x'_{m,n}$ of $x_{m,n}$ in $M_{p,q}$ is $x_{p,q}$ for all $p \le m$ and $q \le n$ according to **(22.5)**. In particular, $x'_{p,p} = x_{q,q}$ for all $q \le p$. So $(x_{p,p}) \in \varprojlim_p M_{p,p}$. Thus π induces a map α.

Suppose $\alpha\big((x_{m,n})\big) = 0$. Then $x_{p,p} = 0$ for all p. Hence $x_{m,n} = 0$ for any m, n, as $x_{m,n} = x'_{p,p}$ if $p \ge \max\{m,n\}$. Thus α is injective.

For surjectivity, given $(x_{p,p}) \in \varprojlim M_{p,p}$, set $x_{m,n} := x'_{p,p}$ where $p \ge \max\{m,n\}$. Then $x_{m,n}$ is well defined, as $(x_{p,p}) \in \varprojlim M_{p,p}$. Plainly $(x_{m,n}) \in \varprojlim \varprojlim M_{m,n}$. Plainly $\alpha\big((x_{m,n})\big) = (x_{p,p})$. Thus α is surjective, so bijective, as desired. □

Exercise (22.43) . — Let R be a ring, $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Given any module M, let $M^{\mathfrak{a}}$ be its $\mathfrak{a}$-adic completion. Set $\mathfrak{c} := \mathfrak{a} + \mathfrak{b}$. Assume M is Noetherian. Show:

(1) Then $(M^{\mathfrak{a}})^{\mathfrak{b}} = M^{\mathfrak{c}}$. (2) Assume $\mathfrak{a} \supset \mathfrak{b}$ and $M^{\mathfrak{a}} = M$. Then $M^{\mathfrak{b}} = M$.

Solution: For (1), use (22.42). Let $F^{\bullet}M$ be the $\mathfrak{a}$-adic filtration, $G^{\bullet}M$ the $\mathfrak{b}$-adic filtration. Then $H^pM := \mathfrak{a}^pM + \mathfrak{b}^pM$. So $\mathfrak{c}^{2p-1}M \subset H^pM \subset \mathfrak{c}^pM$. Thus $M^{\mathfrak{c}} = M^H$. Now, $M^{\mathfrak{a}} = M^F$. And $(M^{\mathfrak{a}})^{\mathfrak{b}}$ is the $\mathfrak{b}$-adic completion of $M^{\mathfrak{a}}$, whereas $(M^{\mathfrak{a}})^G$ is the completion under the filtration by the $(\mathfrak{b}^mM)^{\mathfrak{a}}$. But $\mathfrak{b}^mM^{\mathfrak{a}} = (\mathfrak{b}^mM)^{\mathfrak{a}}$ by (22.20). Thus $(M^{\mathfrak{a}})^{\mathfrak{b}} = (M^F)^G$. Thus (22.42) yields (1).

For (2), note $\mathfrak{c} = \mathfrak{a}$. Thus (1) yields (2). □

Exercise (22.44) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $F_n,\, G \in R[[X]]$ for $n \ge 0$. In $R[[X]]$, set $\mathfrak{b} := \langle \mathfrak{a},\, X\rangle$. Show the following:

(1) Then $\mathfrak{b}^m$ consists of all $H =: \sum h_iX^i$ with $h_i \in \mathfrak{a}^{m-i}$ for all $i < m$.
(2) Say $F_n =: \sum f_{n,i}X^i$. Then (F_n) is Cauchy if and only if every $(f_{n,i})$ is.
(3) Say $G =: \sum g_iX^i$. Then $G = \lim F_n$ if and only if $g_i = \lim f_{n,i}$ for all i.
(4) If R is separated or complete, then so is $R[[X]]$.
(5) The $\mathfrak{b}$-adic completion of $R[X]$ is $\widehat{R}[[X]]$.

Solution: For (1), given such an H, note $h_iX^i \in \mathfrak{b}^m$ for all $i < m$. Moreover, $\sum_{i\ge m} h_iX^i = \big(\sum_{i\ge m} h_{i-m}X^{i-m}\big)X^m \in \mathfrak{b}^m$. Thus $H \in \mathfrak{b}^m$.

Conversely, given $H =: \sum h_iX^i \in \mathfrak{b}^m$, let's show $h_i \in \mathfrak{a}^{m-i}$ for all $i < m$. If $m = 1$, then $H = h_0 + \big(\sum_{i\ge 1} h_{i-1}X^{i-1}\big)X$ with $h_0 \in \mathfrak{a}$. So assume $m \ge 1$.

Note that H is a finite sum of series of the form $(a + FX)G$ with $a \in \mathfrak{a}$, with $F \in R[[X]]$, and with $G \in \mathfrak{b}^{m-1}$. Then $aG \in \mathfrak{b}^m$. But $FG \in \mathfrak{b}^{m-1}$. So by induction, $FG = \sum a_iX^i$ with $a_i \in \mathfrak{a}^{m-1-i}$ for $i < m-1$. So $FGX = \sum_{i\ge 1} a_{i-1}X^i$ with $a_{i-1} \in \mathfrak{a}^{m-i}$ for $i < m$. Thus $h_i \in \mathfrak{a}^{m-i}$ for all $i < m$. Thus (1) holds.

For (2), first assume (F_n) is Cauchy. Fix $i \ge 0$. Given n_0, there's $n_1 > i$ with $F_n - F_{n+1} \in \mathfrak{b}^{n_0+i}$ for $n \ge n_1$. So $f_{n,i} - f_{n+1,i} \in \mathfrak{a}^{n_0}$ by (1). Thus $(f_{n,i})$ is Cauchy.

Conversely, assume every $(f_{n,i})$ is Cauchy. Given n_0, there's n_1 with $f_{n,i} - f_{n+1,i}$ in $\mathfrak{a}^{n_0-i}$ for $n \ge n_1$ and $i < n_0$. So $F_n - F_{n+1} \in \mathfrak{b}^{n_0}$ for $n \ge n_1$ by (1). Thus (F_n) is Cauchy. Thus (2) holds.

For (3), the proof is similar to that of (2).

For (4), first assume R is separated. Given $H \in \bigcap_{m\ge 0}\mathfrak{b}^m$, say $H =: \sum h_iX^i$. Fix i. Then $h_i \in \bigcap_{m\ge 0}\mathfrak{a}^m$ by (1). So $h_i = 0$. So $H = 0$. Thus $R[[X]]$ is separated.

Instead, assume R is complete. Assume (F_n) is Cauchy. Say $F_n =: \sum f_{n,i}X^i$. Then every $(f_{n,i})$ is Cauchy by (2), so has a limit, g_i say. Set $G := \sum g_iX^i$. Then $G = \lim F_n$ by (3). Thus $R[[X]]$ is complete. Thus (4) holds.

For (5), set $\mathfrak{c} := \mathfrak{a}R[X]$. Then $\mathfrak{c}^n = \mathfrak{a}^nR[X]$ for all $n \ge 0$. To use (22.42), set $M = R[X]$ and let $F^{\bullet}M$ be the $\mathfrak{c}$-adic filtration and $G^{\bullet}M$ the $\langle X\rangle$-adic filtration. Then $H^pM := \mathfrak{a}^pM + \langle X\rangle^pM$. So $\langle \mathfrak{a},\, X\rangle^{2p-1} \subset H^pM \subset \langle \mathfrak{a},\, X\rangle^pM$. So M^H is the completion in question in (5). Moreover, $M_{m,n} := R[X]/(\mathfrak{c}^n + \langle X\rangle^m)$. Thus owing to (22.42), it remains to show $\varprojlim_m \varprojlim_n M_{m,n} = \widehat{R}[[X]]$.

Note that $M_{m,n} = (R[X]/\mathfrak{c}^n)\big/((\mathfrak{c}^n + \langle X\rangle^m)/\mathfrak{c}^n)$. But $R[X]/\mathfrak{c}^n = (R/\mathfrak{a}^n)[X]$ by (1.16). Thus $M_{m,n} = (R/\mathfrak{a}^n)[X]/\langle X\rangle^m = \sum_{i=0}^{m-1}(R/\mathfrak{a}^n)X^i$.

Note that $\prod_{n=0}^{\infty}\big(\prod_{i=0}^{m-1}(R/\mathfrak{a}^n)X^i\big) = \prod_{i=0}^{m-1}\big(\prod_{n=0}^{\infty} R/\mathfrak{a}^n\big)X^i$. Hence, for all m, $\varprojlim_n M_{m,n} = \big((\varprojlim_n R/\mathfrak{a}^n)[X]\big)/\langle X\rangle^m$. But $\varprojlim_n R/\mathfrak{a}^n = \widehat{R}$ by (22.7). Moreover, $\varprojlim_m \widehat{R}[X]/\langle X\rangle^m = \widehat{R}[[X]]$ by (22.6). Thus $\varprojlim_m \varprojlim_n M_{m,n} = \widehat{R}[[X]]$. □

Exercise (22.45) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module, $x \in R$. Prove: if $x \notin \mathrm{z.div}(M)$, then $x \notin \mathrm{z.div}(\widehat{M})$; and the converse holds if $\mathfrak{a} \subset \mathrm{rad}(M)$.

Solution: Assume $x \notin \mathrm{z.div}(M)$. Then μ_x is injective on M. So by Exactness of Completion (22.18), the induced map $\widehat{\mu}_x$ is injective on $\widehat{M}$. Thus $x \notin \mathrm{z.div}(\widehat{M})$.

Conversely, assume $x \notin \mathrm{z.div}(\widehat{M})$ and $\mathfrak{a} \subset \mathrm{rad}(M)$. Then $\widehat{\mu}_x$ is injective on $\widehat{M}$. So its restriction is injective on the image of $\kappa_M \colon M \to \widehat{M}$. But κ_M is injective by (22.3) as $\mathfrak{a} \subset \mathrm{rad}(M)$; further, $\widehat{\mu}_x$ induces μ_x. Thus $x \notin \mathrm{z.div}(\widehat{M})$. □

Exercise (22.46) . — Let k be a field with $\mathrm{char}(k) \neq 2$, and X, Y variables. Set $P := k[X, Y]$ and $R := P/\langle Y^2 - X^2 - X^3\rangle$. Let x, y be the residues of X, Y, and set $\mathfrak{m} := \langle x, y\rangle$. Prove R is a domain, but its completion $\widehat{R}$ with respect to $\mathfrak{m}$ isn't.

Solution: First off, R is a domain as $Y^2 - X^2 - X^3$ is irreducible in P.

Set $\mathfrak{M} := \langle X, Y\rangle$. Then (22.2) yields $\widehat{P} = k[[X, Y]]$. Moreover, (22.20) yields $\langle Y^2 - X^2 - X^3\rangle\widehat{\ } = \langle Y^2 - X^2 - X^3\rangle\widehat{P}$. But on R, the $\mathfrak{M}$-adic topology coincides with the $\mathfrak{m}$-adic. Thus (22.12)(1) yields $\widehat{R} = \widehat{P}/\langle Y^2 - X^2 - X^3\rangle$.

In $\widehat{P}$, the binomial theorem yields

$$\sqrt{1+X} = 1 + (1/2)X - (1/8)X^2 + \cdots .$$

Moreover, $Y^2 - X^2 - X^3$ is not irreducible; in fact,

$$Y^2 - X^2 - X^3 = (Y - X\sqrt{1+X})(Y + X\sqrt{1+X}).$$

Thus $\widehat{R}$ is not a domain. □

Exercise (22.47) . — Given modules $M_1, M_2, \ldots$, set $P_k := \prod_{n=1}^{k} M_n$, and let $\pi_k^{k+1} \colon P_{k+1} \to P_k$ be the projections. Show $\varprojlim_{k\geq 1} P_k = \prod_{n=1}^{\infty} M_n$.

Solution: Let $\xi_k \colon P_k \to M_k$ be the projections. It's easy to see that a family of maps $\beta_k \colon N \to P_k$ with $\beta_k = \pi_k^{k+1}\beta_{k+1}$ amounts to an arbitrary family of maps $\alpha_k \colon N \to M_k$ via $\alpha_k = \xi_k\beta_k$. Thus $\varprojlim_{k\geq 1} P_k$ and $\prod_{n=1}^{\infty} M_n$ have equivalent UMPs, which are described in (22.5) and (4.13). □

Exercise (22.48) . — Let $p \in \mathbb{Z}$ be prime. For $n > 0$, define a $\mathbb{Z}$-linear map

$$\alpha_n \colon \mathbb{Z}/\langle p\rangle \to \mathbb{Z}/\langle p^n\rangle \quad \text{by} \quad \alpha_n(1) = p^{n-1}.$$

Set $A := \bigoplus_{n\geq 1} \mathbb{Z}/\langle p\rangle$ and $B := \bigoplus_{n\geq 1} \mathbb{Z}/\langle p^n\rangle$. Set $\alpha := \bigoplus \alpha_n$; so $\alpha \colon A \to B$.

(1) Show that α is injective and that the p-adic completion $\widehat{A}$ is just A.

(2) Show that, in the topology on A induced by the p-adic topology on B, the completion $\overline{A}$ is equal to $\prod_{n=1}^{\infty} \mathbb{Z}/\langle p\rangle$.

(3) Show that the natural sequence of p-adic completions

$$\widehat{A} \xrightarrow{\widehat{\alpha}} \widehat{B} \xrightarrow{\widehat{\beta}} (B/A)\widehat{\ }$$

is not exact at $\widehat{B}$. (Thus p-adic completion is *neither* left exact *nor* right exact.)

Solution: In (1), plainly each α_n is injective; so α is too. Now, note $pA = 0$. So every Cauchy sequence stabilizes. Thus $A = \widehat{A}$, as desired.

For (2), set $A_k := \alpha^{-1}(p^k B)$. These A_k are the fundamental open neighborhoods of 0 in the topology induced from the p-adic topology of B. And

$$A_k = \alpha^{-1}\big(0 \oplus \cdots \oplus 0 \oplus \textstyle\bigoplus_{n>k} \langle p^k\rangle/\langle p^n\rangle\big) = \big(0 \oplus \cdots \oplus 0 \oplus \textstyle\bigoplus_{n>k} \mathbb{Z}/\langle p\rangle\big).$$

Hence $A/A_k = \bigoplus_{i=1}^k \mathbb{Z}/\langle p\rangle = \prod_{n=1}^k \mathbb{Z}/\langle p\rangle$. But $\overline{A} = \varprojlim_{k\ge1} A/A_k$ by **(22.7)**. Thus $\overline{A} = \varprojlim_{k\ge1} \prod_{n=1}^k \mathbb{Z}/\langle p\rangle$. Finally, take $M_n := \mathbb{Z}/\langle p\rangle$ in **(22.47)**. Thus (2) holds.

For (3), note that, by (2) and **(22.12)**(1), the following sequence is exact:

$$0 \to \overline{A} \to \widehat{B} \xrightarrow{\widehat{\beta}} (B/A)^{\widehat{\ }} \to 0.$$

But $\widehat{A} = A$ by (1). And $A \neq \overline{A}$ as A is countable yet $\overline{A}$ isn't. Thus $\mathrm{Im}(\widehat{\alpha}) \neq \mathrm{Ker}(\widehat{\beta})$, as desired. □

Exercise (22.49) . — Preserve the setup of **(22.48)**. Set $A_k := \alpha^{-1}(p^kB)$ and $P := \prod_{k=1}^{\infty} \mathbb{Z}/\langle p\rangle$. Show $\varprojlim^1_{k\ge1} A_k = P/A$, and conclude $\varprojlim$ is not right exact.

Solution: The sequences $0 \to A_k \to A \to A/A_k \to 0$ give this exact sequence:

$$0 \to \varprojlim A_k \to \varprojlim A \to \varprojlim A/A_k \to \varprojlim{}^1 A_k \to \varprojlim{}^1 A$$

by **(22.10)**(2). Now, $\varprojlim^1 A = 0$ by **(22.10)**(1). Also, $\varprojlim A = A$ by **(22.9)** with $Q_n := A$ for all n. And $\varprojlim A_k = 0$ by **(22.9)** with $Q_n := A_n$ for all n, as $\bigcap A_n = 0$.

Thus the following sequence is exact:

$$0 \ \to A \to \varprojlim A/A_k \to \varprojlim{}^1 A_k \to 0.$$

But $A/A_k = \prod_{n=1}^k \mathbb{Z}/\langle p\rangle$; see the solution to **(22.48)**(2). So $\varprojlim A/A_k = P$ by **(22.47)**. Moreover, $A := \bigoplus \mathbb{Z}/\langle p\rangle$. Thus $\varprojlim^1_{k\ge1} A_k = P/A$.

Note $P/A \neq 0$. So $A \to \varprojlim A/A_k$ isn't surjective. Thus $\varprojlim$ isn't right exact. □

Exercise (22.50) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a module. Show that $\mathrm{Ann}_R(M)\widehat{R} \subset \mathrm{Ann}_{\widehat{R}}(\widehat{M})$, with equality if R is Noetherian, M finitely generated.

Solution: Given $x \in \mathrm{Ann}_R(M)$ and (m_n) Cauchy in M, note $xm_n = 0$ for $n \ge 0$. So $x(m_n) = (0)$. So $\mathrm{Ann}_R(M) \subset \mathrm{Ann}_{\widehat{R}}(\widehat{M})$. Thus $\mathrm{Ann}_R(M)\widehat{R} \subset \mathrm{Ann}_{\widehat{R}}(\widehat{M})$.

Assume R is Noetherian and M is finitely generated. Then $\widehat{R}$ is flat by **(22.22)**. So **(9.34)** yields $\mathrm{Ann}_R(M)\widehat{R} = \mathrm{Ann}_{\widehat{R}}(M \otimes_R \widehat{R})$. But **(22.19)** yields $M \otimes_R \widehat{R} = \widehat{M}$. Thus equality holds, as desired. □

Exercise (22.51) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Assume $\mathfrak{a}M = 0$. Set $\mathfrak{b} := \mathrm{Ann}_R(M)$. Show $\widehat{\mathfrak{b}} = \mathrm{Ann}_{\widehat{R}}(\widehat{M})$.

Solution: First, note $\mathfrak{a} \subset \mathfrak{b} \subset R$. Hence $\mathfrak{a}^{n+1} \subset \mathfrak{a}^n\mathfrak{b} \subset \mathfrak{a}^n$ for any $n \ge 0$. Thus the topology on R induces that on $\mathfrak{b}$. Thus **(22.1)** yields $\widehat{\mathfrak{b}} \subset \widehat{R}$.

Given a Cauchy sequence (b_n) in $\mathfrak{b}$ and one (m_n) in M, their product (b_nm_n) is (0). But $\widehat{\mathfrak{b}} \subset \widehat{R}$. Thus $\widehat{\mathfrak{b}} \subset \mathrm{Ann}_{\widehat{R}}(\widehat{M})$. It remains to show $\mathrm{Ann}_{\widehat{R}}(\widehat{M}) \subset \widehat{\mathfrak{b}}$.

Given $x \in \mathrm{Ann}_{\widehat{R}}(\widehat{M})$, represent x by a Cauchy sequence $(x_n) \in C(R)$. Then there's n_1 with $x_n - x_{n'} \in \mathfrak{a}$ for all $n, n' \ge n_1$.

Given any $m \in M$, note $(x_n - x_{n'})m \in \mathfrak{a}M$ for all $n, n' \ge n_1$. But (x_nm) represents $x\kappa_M(m)$, which is 0; so $x_nm \in \mathfrak{a}M$ for $n \gg 0$. So $x_nm \in \mathfrak{a}M$ for $n \ge n_1$. But $\mathfrak{a}M = 0$. So $x_n \in \mathfrak{b}$ for $n \ge n_1$. So $x \in \widehat{\mathfrak{b}}$. Thus $\mathrm{Ann}_{\widehat{R}}(\widehat{M}) \subset \widehat{\mathfrak{b}}$, as desired.

(In passing, note that **(22.1)** yields $M = \widehat{M}$ as R-modules.) □

Exercise (22.52) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M, N, P modules. Assume $\mathfrak{a}M \subset P \subset N \subset M$. Prove:

(1) The ($\mathfrak{a}$-adic) topology on M induces that on N.

(2) Then $(\mathfrak{a}M)\widehat{\ } \subset \widehat{P} \subset \widehat{N} \subset \widehat{M}$, and $N/P = \widehat{N}/\widehat{P}$.

(3) The map $Q \mapsto \widehat{Q}$ is a bijection from the R-submodules Q with $P \subset Q \subset N$ to the $\widehat{R}$-submodules Q' with $\widehat{P} \subset Q' \subset \widehat{N}$. Its inverse is $Q' \mapsto \kappa_M^{-1}(Q')$.

Solution: For (1), note $\mathfrak{a}M \subset N \subset M$. Multiplying by $\mathfrak{a}^n$ for any $n \ge 0$ yields $\mathfrak{a}^{n+1}M \subset \mathfrak{a}^n N \subset \mathfrak{a}^n M$. Thus (1) holds.

For (2), note (1) implies the topology on M induces the topologies on N, P, $\mathfrak{a}M$. Hence, the topology on N induces that on P, and that on P induces that on $\mathfrak{a}M$. Thus **(22.12)**(1)–(2) yield (2).

For (3), note $Q \mapsto Q/P$ is a bijection from the R-submodules Q with $P \subset Q \subset N$ to the R-submodules of N/P, and $Q' \mapsto Q'/\widehat{P}$ is a bijection from the $\widehat{R}$-submodules Q' with $\widehat{P} \subset Q' \subset \widehat{N}$ to the $\widehat{R}$-submodules of $\widehat{N}/\widehat{P}$. But $N/P = \widehat{N}/\widehat{P}$ and $Q/P = \widehat{Q}/\widehat{P}$ by (2); also, these identifications come from κ_M. Thus (3) holds. □

Exercise (22.53) . — Let R be a ring, $\mathfrak{a} \subset \mathfrak{b}$ ideals, and M a finitely generated module. Let Φ be the set of maximal ideals $\mathfrak{m} \in \mathrm{Supp}(M)$ with $\mathfrak{m} \supset \mathfrak{a}$. Use the $\mathfrak{a}$-adic topology. Prove:

(1) Then $\widehat{M}$ is a finitely generated $\widehat{R}$-module, and $\widehat{\mathfrak{b}}\widehat{M} = \widehat{\mathfrak{b}M} \subset \widehat{M}$.

(2) The map $\mathfrak{p} \mapsto \widehat{\mathfrak{p}}$ is a bijection $\mathrm{Supp}(M/\mathfrak{b}M) \xrightarrow{\sim} \mathrm{Supp}(\widehat{M}/\widehat{\mathfrak{b}}\widehat{M})$. Its inverse is $\mathfrak{p}' \mapsto \kappa_R^{-1}\mathfrak{p}'$. It restricts to a bijection on the subsets of maximal ideals.

(3) Then $\mathrm{Supp}(\widehat{M}/\widehat{\mathfrak{a}}\widehat{M})$ and $\mathrm{Supp}(\widehat{M})$ have the same maximal ideals.

(4) Then the $\widehat{\mathfrak{m}}$ with $\mathfrak{m} \in \Phi$ are precisely the maximal ideals of $\widehat{R}$ in $\mathrm{Supp}(\widehat{M})$.

(5) Then $\kappa_R^{-1}\,\mathrm{rad}(\widehat{M}) = \bigcap_{\mathfrak{m}\in\Phi}\mathfrak{m}$ and $\mathrm{rad}(\widehat{M}) = \big(\bigcap_{\mathfrak{m}\in\Phi}\mathfrak{m}\big)\widehat{\ }$.

(6) Then Φ is finite if and only if $\widehat{M}$ is semilocal.

(7) If $M = R$, then $\Phi = \{\mathfrak{b}\}$ if and only if $\widehat{R}$ is local with maximal ideal $\widehat{\mathfrak{b}}$.

Solution: For (1), fix a surjection $R^r \twoheadrightarrow M$. It induces a map $\widehat{R^r} \to \widehat{M}$, which is surjective by **(22.12)**(1). But completion is a linear functor, so $\widehat{R^r} = \widehat{R}^r$ by **(8.14)**. So there's a surjection $\widehat{R}^r \twoheadrightarrow \widehat{M}$. Thus $\widehat{M}$ is a finitely generated $\widehat{R}$-module.

Let's use $R^r \twoheadrightarrow M$ to construct the following commutative diagram:

$$\begin{array}{ccc}
\widehat{\mathfrak{b}}\widehat{R^r} & \xrightarrow{\alpha} & \widehat{\mathfrak{b}}\widehat{M} \\
{\scriptstyle\beta}\big\downarrow & & {\scriptstyle\gamma}\big\downarrow \\
\widehat{\mathfrak{b}R^r} & \xrightarrow{\delta} & \widehat{\mathfrak{b}M}
\end{array}$$

First, $\widehat{\mathfrak{b}M} \subset \widehat{M}$ by **(22.52)**(2) with $P := \mathfrak{b}M$ and $N := M$. Next, $\widehat{\mathfrak{b}}\widehat{M} \subset \widehat{M}$ by definition; namely, the product of a Cauchy sequence in $\mathfrak{b}$ and one in M is one in M. In fact, the latter is a sequence in $\mathfrak{b}M$. So take γ to be the inclusion.

Similarly, take β to be the inclusion of submodules of $\widehat{R^r}$. Plainly, $\widehat{R^r} \to \widehat{M}$ restricts to give α and δ. Trivially, the resulting diagram is commutative.

Plainly, multiplication by $\mathfrak{b}$ preserves surjections; so $\mathfrak{b}R^r \to \mathfrak{b}M$ is surjective. But again, completion preserves surjections by **(22.12)**(1). Thus δ is surjective.

Again, completion preserves finite direct sums; so $\widehat{R^r} = \widehat{R}^r$ and $\widehat{\mathfrak{b}^{\oplus r}} = \widehat{\mathfrak{b}}^{\oplus r}$. But plainly, multiplication by an ideal preserves finite direct sums; so $\widehat{\mathfrak{b}}\widehat{R}^r = \widehat{\mathfrak{b}}^{\oplus r}$ and $\mathfrak{b}R^r = \mathfrak{b}^{\oplus r}$. Hence $\widehat{\mathfrak{b}}\widehat{R^r} = \widehat{\mathfrak{b}}^{\oplus r}$ and $\widehat{\mathfrak{b}R^r} = \widehat{\mathfrak{b}}^{\oplus r}$; correspondingly, $\beta = 1$. So $\delta\beta$ is surjective; so γ is too. Thus (1) holds.

For (2), set $\mathfrak{c} := \mathrm{Ann}_R(M/\mathfrak{b}M)$. Note $\mathfrak{a}(M/\mathfrak{b}M) = 0$. So $\widehat{\mathfrak{c}} = \mathrm{Ann}_{\widehat{R}}(\widehat{M/\mathfrak{b}M})$

by (**22.51**). As M is finitely generated, so is $M/\mathfrak{b}M$; hence, $\widehat{M/\mathfrak{b}M}$ is too by (1). Thus (**13.4**) yields $\operatorname{Supp}(M/\mathfrak{b}M) = \mathbf{V}(\mathfrak{c})$ and $\operatorname{Supp}(\widehat{M/\mathfrak{b}M}) = \mathbf{V}(\widehat{\mathfrak{c}})$.

The topology on M induces that on $\mathfrak{b}M$ by (**22.52**)(1); so $\widehat{M/\mathfrak{b}M} = \widehat{M}/\widehat{\mathfrak{b}M}$ by (**22.12**)(1). Moreover, $\widehat{\mathfrak{b}}\widehat{M} = \widehat{\mathfrak{b}M}$ by (1). Thus $\operatorname{Supp}(\widehat{M}/\widehat{\mathfrak{b}}\widehat{M}) = \mathbf{V}(\widehat{\mathfrak{c}})$.

The map $\mathfrak{p} \mapsto \mathfrak{p}/\mathfrak{c}$ is a bijection from the ideals $\mathfrak{p}$ containing $\mathfrak{c}$ to the ideals of $R/\mathfrak{c}$; also, $\mathfrak{p}$ is prime or maximal if and only if $\mathfrak{p}/\mathfrak{c}$ is. The map $\mathfrak{p}' \mapsto \mathfrak{p}'/\widehat{\mathfrak{c}}$ is similar. By (**22.52**)(1), the topology on $\mathfrak{p}$ induces that on $\mathfrak{c}$. So κ_R induces an identification $\mathfrak{p}/\mathfrak{c} = \widehat{\mathfrak{p}}/\widehat{c}$ by (**22.12**) (1)–(2). In particular, $R/\mathfrak{c} = \widehat{R}/\widehat{\mathfrak{c}}$; this identification is a ring isomorphism, so preserves prime ideals and maximal ideals. Thus (2) holds.

For (3), note $\widehat{M}$ is finitely generated by (1). So $\operatorname{Supp}(\widehat{M}/\widehat{\mathfrak{a}}\widehat{M}) = \operatorname{Supp}(\widehat{M}) \bigcap \mathbf{V}(\widehat{\mathfrak{a}})$ by (**13.46**)(1). But every maximal ideal of $\widehat{R}$ contains $\widehat{\mathfrak{a}}$ by (**22.4**). Thus (3) holds.

For (4), note $\operatorname{Supp}(M/\mathfrak{a}M) = \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{a})$ by (**13.46**)(1) as M is finitely generated. Thus (2) with $\mathfrak{b} = \mathfrak{a}$ and (3) yield (4).

For (5), note $\bigcap_{\mathfrak{m}\in\Phi} \widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{M})$ by (4). So $\kappa_R^{-1} \operatorname{rad}(\widehat{M}) = \bigcap_{\mathfrak{m}\in\Phi} \kappa_R^{-1}\widehat{\mathfrak{m}}$. But $\kappa_R^{-1}\widehat{\mathfrak{m}} = \mathfrak{m}$ by (2). So $\kappa_R^{-1} \operatorname{rad}(\widehat{M}) = \bigcap_{\mathfrak{m}\in\Phi} \mathfrak{m}$. Thus (**22.52**)(3) yields (5).

Finally, (6) and (7) both follow immediately from (4). □

Exercise (22.54) (*UMP of completion***) . —** (1) Let R be a ring, M a filtered module. Show $\kappa_M \colon M \to \widehat{M}$ is the universal example of a map of filtered modules $\alpha \colon M \to N$ with N separated and complete. (2) Let R be a filtered ring. Show κ_R is the universal filtered ring map $\varphi \colon R \to R'$ with R' separated and complete.

Solution: For (1), first note that $\widehat{M}$ is separated and complete by (**22.16**)(4), and κ_M is a map of filtered modules by (**22.1**).

Second, recall from (**22.1**) that any given α induces a map of filtered modules $\widehat{\alpha} \colon \widehat{M} \to \widehat{N}$ with $\widehat{\alpha}\kappa_M = \kappa_N\alpha$. But N is separated and complete. So κ_N is injective by (**22.3**) and surjective by (**22.13**)(1). Thus κ_N is an isomorphism of filtered modules by (**22.1**).

Set $\beta := \kappa_N^{-1}\widehat{\alpha}$. Then $\beta \colon \widehat{M} \to N$ is a map of filtered modules with $\beta\kappa_M = \alpha$. Finally, given any map of filtered modules $\beta' \colon \widehat{M} \to N$ with $\beta'\kappa_M = \alpha$, note $\kappa_N\beta'\kappa_M = \kappa_N\alpha$. So $\kappa_N\beta' = \widehat{\alpha}$ by (**22.15**). Thus $\beta' = \beta$, as desired.

For (2), revisit the proof of (1) taking $\alpha := \varphi$. It is clear from their construction in (**22.1**) that $\widehat{\alpha}$ and κ_R are maps of filtered rings; thus β is too, as desired. □

Exercise (22.55) (*UMP of formal power series***) . —** Let R be a ring, R' an algebra, $\mathfrak{b}$ an ideal of R', and $x_1, \ldots, x_n \in \mathfrak{b}$. Let $A := R[[X_1, \ldots, X_n]]$ be the formal power series ring. Assume R' is separated and complete in the $\mathfrak{b}$-adic topology. Show there's a unique map of R-algebras $\varphi \colon A \to R'$ with $\varphi(X_i) = x_i$ for all i, and φ is surjective if the induced map $R \to R'/\mathfrak{b}$ is surjective and the x_i generate $\mathfrak{b}$.

Solution: Set $P := R[X_1, \ldots, X_n]$ and $\mathfrak{a} := \langle X_1, \ldots, X_n\rangle$. Give P the $\mathfrak{a}$-adic filtration. Then $\widehat{P} = A$ by (**22.2**). Form the unique R-algebra map $\pi : P \to R'$ with $\pi(X_i) = x_i$. Notice π respects the filtrations. So by (**22.54**)(2), there's a unique map of filtered rings $\varphi \colon A \to R'$ with $\varphi\kappa_P = \pi$.

Assume $R \to R'/\mathfrak{b}$ is surjective and the x_i generate $\mathfrak{b}$. Then $P/\mathfrak{a} \to R'/\mathfrak{b}$ and $\mathfrak{a}/\mathfrak{a}^2 \to \mathfrak{b}/\mathfrak{b}^2$ are surjective. But $\mathfrak{b}/\mathfrak{b}^2$ generates $G(R')$ as an $R'/\mathfrak{b}$-algebra. So $G(\pi)$ is surjective. So $G(\varphi)$ is too, as $G(\varphi)G(\kappa_P) = G(\pi)$. Thus φ is by (**22.23**)(2). □

Exercise (22.56) . — Let R be a ring, $\mathfrak{a}$ a finitely generated ideal, and $X_1, \dots, X_n$ variables. Set $P := R[[X_1, \dots, X_n]]$. Prove $P/\mathfrak{a}P = (R/\mathfrak{a})[[X_1, \dots, X_n]]$. (But, it's not always true that $R' \otimes_R P = R'[[X_1, \dots, X_n]]$ for an R-algebra R'; see (8.18).)

Solution: Let $\kappa\colon R \to R/\mathfrak{a}$ be the quotient map. By (22.55), there is a unique ring map $\varphi\colon P \to (R/\mathfrak{a})[[X_1, \dots, X_n]]$ with $\varphi|R = \kappa$ and $\varphi(X_i) = X_i$ for all i. As κ is surjective, so is φ. But $\mathrm{Ker}(\varphi)$ consists of the power series whose coefficients map to 0 under κ, that is, lie in $\mathfrak{a}$. Hence $\mathrm{Ker}(\varphi) = \mathfrak{a}P$ by (3.19)(5) as $\mathfrak{a}$ is finitely generated. Thus φ induces an isomorphism $P/\mathfrak{a}P \xrightarrow{\sim} (R/\mathfrak{a})[[X_1, \dots, X_n]]$.

Alternatively, the two R-algebras are equal, as they have the same UMP: each is universal among complete R-algebras R' with distinguished elements x_i and with $\mathfrak{a}R' = 0$. Namely, the structure map $\varphi\colon R \to R'$ induces a unique map $\pi\colon P \to R'$ such that $\pi(X_i) = x_i$ for all i by (22.55). Then π factors through a unique map $P/\mathfrak{a}P \to R'$. Indeed π factors through the quotient $P/\mathfrak{A}$ where $\mathfrak{A}$ is the ideal of power series with coefficients in $\mathfrak{a}$ as $\mathfrak{a}R' = 0$. But $\mathfrak{A} = \mathfrak{a}P$ by (3.19)(5) as $\mathfrak{a}$ is finitely generated. So π factors through $P/\mathfrak{a}P$. On the other hand, φ factors through a unique map $\psi\colon R/\mathfrak{a} \to R'$ as $\mathfrak{a}R' = 0$; then ψ factors through a unique map $(R/\mathfrak{a})[[X_1, \dots, X_n]] \to R'$ such that $\pi(X_i) = x_i$ for all i by (22.55). □

Exercise (22.57) (*Cohen Structure Theorem I*) . — Let $A \to B$ be a local homomorphism, $\mathfrak{b} \subset B$ an ideal. Assume that $A = B/\mathfrak{b}$ and that B is separated and complete in the $\mathfrak{b}$-adic topology. Prove the following statements:

(1) The hypotheses hold if B is a complete Noetherian local ring, $\mathfrak{b}$ is its maximal ideal, and A is a coefficient field.
(2) Then $B \simeq A[[X_1, \dots, X_r]]/\mathfrak{a}$ for some r, variables X_i, and some ideal $\mathfrak{a}$.

Solution: For (1), note $A = B/\mathfrak{b}$ holds by definition of coefficient field (21.24). Moreover, as B is Noetherian, it is separated by (22.3). Thus (1) holds.

For (2), say $\mathfrak{b} = \langle x_1, \dots, x_r\rangle$, and take variables $X_1, \dots, X_r$. Form the unique surjection of A-algebras $\varphi\colon A[[X_1, \dots, X_r]] \twoheadrightarrow B$ with $\varphi(X_i) = x_i$ of (22.55), and set $\mathfrak{a} := \mathrm{Ker}(\varphi)$. Then $A[[X_1, \dots, X_r]]/\mathfrak{a} \xrightarrow{\sim} B$. Thus (2) holds. □

Exercise (22.58) (*Cohen Structure Theorem II*) . — Let $A \to B$ be a flat local homomorphism of complete Noetherian local rings, and $\mathfrak{b} \subset B$ an ideal. Denote the maximal ideal of A by $\mathfrak{m}$, and set $B' := B/\mathfrak{m}B$. Assume that $A \xrightarrow{\sim} B/\mathfrak{b}$ and that B' is regular of dimension r. Find an A-isomorphism $\psi\colon B \xrightarrow{\sim} A[[X_1, \dots, X_r]]$ for variables X_i with $\psi(\mathfrak{b}) = \langle X_1, \dots, X_r\rangle$. Moreover, if $\mathfrak{b} = \langle x_1, \dots, x_r\rangle$ for given x_i, find such a ψ with $\psi(x_i) = X_i$.

Solution: As B is complete, Noetherian, and local, $B = \widehat{B}$ by (22.14). So B is equal to its completion in the $\mathfrak{b}$-adic topology by (22.43)(2). Thus by (22.16)(4) or by (22.14) again, B is separated and complete in the $\mathfrak{b}$-adic topology.

Set $k := A/\mathfrak{m}$. Then $B' = B \otimes k$. Form the exact sequence of A-modules $0 \to \mathfrak{b} \to B \to A \to 0$. It yields $0 \to \mathfrak{b} \otimes k \to B' \to k \to 0$, which is exact by (9.8)(1). Let $\mathfrak{n}'$ be the maximal ideal of B'. Now, k is a field. Thus $\mathfrak{b} \otimes k = \mathfrak{n}'$.

As B' is regular of dimension r, there are $x_1, \dots, x_r \in \mathfrak{b}$ whose images in $\mathfrak{n}'$ form a regular sop, and so generate $\mathfrak{n}'$. But $\mathfrak{n}' = \mathfrak{b} \otimes k = \mathfrak{b}/\mathfrak{m}\mathfrak{b}$, and $\mathfrak{m}\mathfrak{b} = (\mathfrak{m}B)\mathfrak{b}$. Also, $\mathfrak{b}$ is finitely generated as B is Noetherian. Thus by (10.8)(2), the x_i generate $\mathfrak{b}$.

Fix any $x_1, \dots, x_r \in \mathfrak{b}$ that generate $\mathfrak{b}$. Then their images in $\mathfrak{n}'$ generate $\mathfrak{n}'$, and so form a regular sop as $\dim(B') = r$. Set $P := A[[X_1, \dots X_r]]$ for variables X_i. By (22.55), there's a surjection of A-algebras $\varphi\colon P \twoheadrightarrow B$ with $\varphi(X_i) = x_i$. Set

$\mathfrak{a} := \operatorname{Ker}(\varphi)$. We must show $\mathfrak{a} = 0$, for then ψ is bijective, and $\varphi := \psi^{-1}$ works.

As $A \to B$ is flat, $0 \to \mathfrak{a} \otimes k \to P \otimes k \xrightarrow{\varphi \otimes k} B \otimes k \to$ is exact by (**9.8**)(1). Now, $B \otimes k = B'$, and $G(B')$ is the polynomial ring, over $B'/\mathfrak{n}'$, in the images of $x_1, \dots, x_r$ by (**21.15**), and $B'/\mathfrak{n}' = k$ owing to the second paragraph above. Moreover, $P \otimes k = k[[X_1, \dots X_r]]$ owing to (**22.56**). But $\varphi(X_i) = x_i$. Hence $G(\varphi \otimes k) = 1$. So $\varphi \otimes k$ is bijective by (**22.23**). Hence $\mathfrak{a} \otimes k = 0$. Thus $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$.

As A is Noetherian, so is P by (**22.27**). Hence $\mathfrak{a}$ is finitely generated as a P-module. But $\mathfrak{a} = (\mathfrak{m}P)\mathfrak{a}$. Thus (**10.6**) implies $\mathfrak{a} = 0$, as desired. □

Exercise (22.59) . — Let k be a field, $A := k[[X_1, \dots, X_n]]$ the power series ring in variables X_i with $n \ge 1$, and $F \in A$ nonzero. Find an algebra automorphism φ of A such that $\varphi(F)$ contains the monomial X_n^s for some $s \ge 0$; do so as follows. First, find suitable $m_i \ge 1$ and use (**22.55**) to define φ by

$$\varphi(X_i) := X_i + X_n^{m_i} \text{ for } 1 \le i \le n-1 \text{ and } \varphi(X_n) := X_n. \qquad (\mathbf{22.59.1})$$

Second, if k is infinite, find suitable $a_i \in k^\times$ and use (**22.55**) to define φ by

$$\varphi(X_i) := X_i + a_i X_n \text{ for } 1 \le i \le n-1 \text{ and } \varphi(X_n) := X_n. \qquad (\mathbf{22.59.2})$$

Solution: First, note that (**22.55**) yields, for any m_i, a unique endomorphism φ of A defined by (**22.59.1**). Plainly, φ is an automorphism, whose inverse φ' is defined by $\varphi'(X_i) := X_i - X_n^{m_i}$ for $1 \le i \le n-1$ and $\varphi'(X_n) := X_n$.

To find suitable m_i, order the monomials of F lexicographically. Say $\prod X_i^{s_i}$ is smallest. Take $m > \max\{s_i\}$ and $m_i := m^{n-i}$. Then $\varphi\big(\prod X_i^{s_i}\big)$ contains X_n^s with $s := \sum m_i s_i$. Given any other $\prod X_i^{t_i}$ in F, say $t_i = s_i$ for $i < h$, but $t_h > s_h$. Set $t := \sum m_i t_i$. Then $t - s \ge m^{n-h} - \sum_{i>h}^n m^{n-i} s_i > 0$. Thus $\varphi(F)$ contains X_n^s.

Second, note that similarly (**22.55**) yields, for any a_i, a unique automorphism φ of A defined by (**22.59.2**). Suppose now k is infinite.

To find suitable a_i, say $F = \sum_{i \ge s} F_i$ with F_i homogeneous of degree i and $F_s \ne 0$. As k is infinite, $F_s(a_1, \dots, a_n) \ne 0$ for some $a_i \in k^\times$ by (**3.28**)(1) with $\mathcal{S} := k^\times$. As F_s is homogeneous, we may replace a_i by a_i/a_n. Set $c := F_s(a_1, \dots, a_{n-1}, 1)$. Then $\varphi(F)$ contains the term cX_n^s, as desired. □

Exercise (22.60) . — Let A be a complete Noetherian local ring, k a coefficient field, $x_1, \dots, x_s$ a sop, $X_1, \dots, X_s$ variables. Set $B := k[[X_1, \dots, X_s]]$. Find an injective map $\varphi\colon B \to A$ such that $\varphi(X_i) = x_i$ and A is B-module finite.

Solution: As A is Noetherian, A is separated by (**22.3**). Set $\mathfrak{q} := \langle x_1, \dots, x_s \rangle$. It's a parameter ideal. So A has the $\mathfrak{q}$-adic topology by (**22.1**). Thus (**22.55**) provides $\varphi\colon B \to A$ with $\varphi(X_i) = x_i$.

Set $\mathfrak{n} := \langle X_1, \dots, X_s \rangle$, and form this canonical commutative diagram:

$$\begin{tikzcd} k[X_1, \dots, X_s] \arrow[r, hook] \arrow[d, "1"'] & (A/\mathfrak{q})[X_1, \dots, X_s] \arrow[d, "\phi_s"] \\ G_{\mathfrak{n}}(B) \arrow[r, "G(\varphi)"] & G_{\mathfrak{q}}(A) \end{tikzcd}$$

where ϕ_s the surjective map of (**21.11.1**).

Given $F \in \operatorname{Ker}(G(\varphi))$, view $F \in (A/\mathfrak{q})[X_1, \dots, X_s]$. Then $\phi_s(F) = 0$. So by (**21.23**)(1)–(2), the coefficients of F are in the maximal ideal of $A/\mathfrak{q}$. But they're in k too. So they're 0. So $G(\varphi)$ is injective. Thus by (**22.23**)(1), also $\widehat{\varphi}$ is injective.

Note B is complete by (**22.2**). So $\widehat{\varphi} = \varphi$. Thus φ is injective.

As $A/\mathfrak{q}$ has finite length, it has finite k-dimension by **(19.19)**. But the $\phi_s(X_i)$ generate $\mathfrak{q}/\mathfrak{q}^2$ over $A/\mathfrak{q}$. Hence $G_{\mathfrak{q}}(A)$ is $G_{\mathfrak{n}}(B)$-module finite. But B is complete. Also A is separated. Thus by **(22.24)**, A is B-module finite. □

Exercise (22.61) . — Let R be a ring, M a nonzero Noetherian module, and $\mathfrak{q}$ a parameter ideal of M. Show: (1) $\widehat{M}$ is a nonzero Noetherian $\widehat{R}$-module, and $\widehat{\mathfrak{q}}$ is a parameter ideal of $\widehat{M}$; and (2) $e(\mathfrak{q}, M) = e(\widehat{\mathfrak{q}}, \widehat{M})$ and $\dim(M) = \dim(\widehat{M}\,)$.

Solution: First, for all $n \ge 0$, note $\widehat{M/\mathfrak{q}^n M} = \widehat{M}/\widehat{\mathfrak{q}^n M}$ by **(22.12)**(1). And $\widehat{\mathfrak{q}^n M} = \widehat{\mathfrak{q}}^n \widehat{M}$ by **(22.20)**. Also, $\ell_R(M/\mathfrak{q}^n M) < \infty$ by **(20.9)**. Thus by **(22.41)**(2)

$$\ell_R(M/\mathfrak{q}^n M) = \ell_{\widehat{R}}(\widehat{M}/\widehat{\mathfrak{q}}^n \widehat{M}). \tag{22.61.1}$$

For (1), note $\kappa_M\colon M \to \widehat{M}$ is injective by **(22.3)**. But $M \neq 0$. Thus $\widehat{M} \neq 0$. Moreover, $\widehat{M}$ is a Noetherian $\widehat{R}$-module by **(22.26)**.

Set $\mathfrak{m} := \operatorname{rad}(M)$. Then $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{M})$ owing to **(22.53)**(5). But $\mathfrak{q} \subset \mathfrak{m}$. Thus $\widehat{\mathfrak{q}} \subset \widehat{\mathfrak{m}}$ by **(22.1)**. Also, $\ell_{\widehat{R}}(\widehat{M}/\widehat{\mathfrak{q}}\widehat{M}) < \infty$ by **(22.61.1)**. Thus $\widehat{\mathfrak{q}}$ is a parameter ideal. Thus (1) holds.

For (2), note $p_{\mathfrak{q}}(M, n) = p_{\widehat{\mathfrak{q}}}(\widehat{M}, n)$ owing to **(22.61.1)** and **(20.10.2)**. Hence. $d(M) = d(\widehat{M}\,)$ by **(21.2)**; so $\dim(M) = \dim(\widehat{M}\,)$ by **(21.4)**. Thus (2) holds. □

Exercise (22.62) . — Let A be a Noetherian local ring, $\mathfrak{m}$ the maximal ideal, k the residue field. Show: (1) $\widehat{A}$ is a Noetherian local ring with $\widehat{\mathfrak{m}}$ as maximal ideal and k as residue field; and (2) A is regular of dimension r if and only if $\widehat{A}$ is so.

Solution: For (1), note $\widehat{A}$ is Noetherian by **(22.26)**, and it's local with $\widehat{\mathfrak{m}}$ as maximal ideal by **(22.53)**(7). And $\widehat{A}/\widehat{\mathfrak{m}} = k$ by **(22.12)**(1)–(2). Thus (1) holds.

For (2), note (1) holds. So $\mathfrak{m}/\mathfrak{m}^2 = \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}^2}$ by **(22.12)**(1)–(2). But $\widehat{\mathfrak{m}^2} = \widehat{\mathfrak{m}}^2$ by **(22.20)**. So $\mathfrak{m}/\mathfrak{m}^2 = \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2$. But $\dim(A) = \dim(\widehat{A}\,)$ by **(22.61)**(2). Thus the second paragraph of **(21.14)** implies (2). □

Exercise (22.63) . — Let A be a Noetherian local ring, $k \subset A$ a coefficient field. Show A is regular if and only if, given any surjective k-map of finite-dimensional local k-algebras $B \twoheadrightarrow C$, every local k-map $A \to C$ lifts to a local k-map $A \to B$.

Solution: First, assume A is regular. Given $\alpha\colon B \twoheadrightarrow C$ and $\gamma\colon A \to C$, we must lift γ to some $\beta\colon A \to B$. As B and C are finite dimensional, they're Artinian by **(16.42)**. It follows, as explained in **(22.1)**, that B and C are separated and complete. Let $\mathfrak{n}$ and $\mathfrak{p}$ be the maximal ideals of B and C.

So **(22.54)**(2) yields a map of filtered rings $\psi : \widehat{A} \to C$ with $\psi\kappa_A = \gamma$. Now, A ia regular, so $\widehat{A}$ is too by **(22.62)**(2). So $\widehat{A} = k[[X_1, \dots, X_r]]$ for variables X_i by **(22.58)**. As ψ is a map of filtered rings, $\psi(X_i) \in \mathfrak{p}$ for all i.

As $\alpha\colon B \twoheadrightarrow C$ is surjective, each $\psi(X_i)$ lifts to some $x_i \in \mathfrak{n}$. So **(22.55)** yields a k-algebra map $\varphi\colon \widehat{A} \to B$ with $\varphi(X_i) = x_i$ for all i. Then $\alpha\varphi(X_i) = \psi(X_i)$. So **(22.55)** implies $\alpha\varphi = \psi$. Set $\beta := \varphi\kappa_A$. Then $\alpha\beta = \gamma$, as desired.

Conversely, assume, given any $\alpha\colon B \twoheadrightarrow C$, every $\gamma\colon A \to C$ lifts to a $\beta\colon A \to B$. Let $\mathfrak{m}$ be the maximal ideal of A. By **(22.62)**, $\widehat{A}$ is Noetherian and local with $\widehat{\mathfrak{m}}$ as maximal ideal and k as coefficent field; also, if $\widehat{A}$ is regular, then so is A.

Say $x_1, \dots, x_r \in \widehat{\mathfrak{m}}$ generate, and r is minimal. Then $\dim_k(\widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2) = r$ by **(10.9)**. So $\dim_k(\widehat{A}/\widehat{\mathfrak{m}}^2) = r + 1$. Let $P := k[[X_1, \dots, X_r]]$ be the power series ring. By

(**22.55**), there's a surjective map of k-algebras $\varphi\colon P \twoheadrightarrow \widehat{A}$ with $\varphi(X_i) = x_i$. Set $\mathfrak{a} := \langle X_1, \dots, X_r\rangle$. Then φ induces a surjection $\varphi_2\colon P/\mathfrak{a}^2 \twoheadrightarrow \widehat{A}/\widehat{\mathfrak{m}}^2$. But plainly $\dim_k(P/\mathfrak{a}^2) = r+1$. Hence φ_2 is bijective. Precede φ_2^{-1} by the quotient map $\widehat{A} \twoheadrightarrow \widehat{A}/\widehat{\mathfrak{m}}^2$ to get $\psi_2\colon \widehat{A} \to P/\mathfrak{a}^2$. Notice $\psi_2(x_i)$ is the residue of X_i.

Recursively, let's construct a local k-map $\psi_m\colon \widehat{A} \to P/\mathfrak{a}^m$ lifting ψ_{m-1} for $m > 2$. By hypothesis, $\psi_{m-1}\kappa_A$ lifts to some local k-map $\beta\colon A \to P/\mathfrak{a}^m$. So (**22.54**)(2) yields a local k-map $\psi_m : \widehat{A} \to P/\mathfrak{a}^m$ with $\psi_m\kappa_A = \beta$. Let $\gamma\colon P/\mathfrak{a}^m \twoheadrightarrow P/\mathfrak{a}^{m-1}$ be the quotient map. Then $\gamma\psi_m\kappa_A = \psi_{m-1}\kappa_A$. Thus (**22.54**)(2) yields $\gamma\psi_m = \psi_{m-1}$.

By (**22.6**), $P = \varprojlim P_n$. So (**22.5**) yields a local k-map $\psi\colon \widehat{A} \to P$ lifting all ψ_m. So $\psi(x_i) \equiv X_i \pmod{\mathfrak{a}^2}$ for all i. But $\varphi(X_i) = x_i$. So $\psi\varphi(X_i) \equiv X_i \pmod{\mathfrak{a}^2}$. But $G(P) = k[X_1, \dots, X_r]$. So $G(\psi\varphi) = 1$. So $\psi\varphi$ is bijective by (**22.23**). Hence φ is injective. But φ is also surjective. So φ is bijective. But by (**22.27**), P is regular, so $\widehat{A}$ is regular too, as desired. □

Exercise (22.64) . — Let k be a field, $\varphi\colon B \to A$ a local homomorphism of Noetherian local k-algebras, and $\mathfrak{n}$, $\mathfrak{m}$ the maximal ideals. Assume $k = B/\mathfrak{n} = A/\mathfrak{m}$, the induced map $\varphi'\colon \mathfrak{n}/\mathfrak{n}^2 \to \mathfrak{m}/\mathfrak{m}^2$ is injective, and A is regular. Show B is regular.

Solution: Let's reduce to the case where A and B are complete. Note (**22.62**) (1)–(2) imply $\widehat{A}$ and $\widehat{B}$ are Noetherian local rings with $\widehat{\mathfrak{m}}$ and $\widehat{\mathfrak{n}}$ as maximal ideals, $\widehat{A}$ is regular, and if $\widehat{B}$ is regular, so is B. Also, (**22.12**)(1)–(2) and (**22.20**) yield

$$\widehat{B}/\widehat{\mathfrak{n}} = B/\mathfrak{n}, \quad \widehat{A}/\widehat{\mathfrak{m}} = A/\mathfrak{m}, \quad \widehat{\mathfrak{n}}/\widehat{\mathfrak{n}}^2 = \mathfrak{n}/\mathfrak{n}^2, \quad \text{and} \quad \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2 = \mathfrak{m}/\mathfrak{m}^2;$$

hence, $k = \widehat{B}/\widehat{\mathfrak{n}} = \widehat{A}/\widehat{\mathfrak{m}}$, and the induced map $\widehat{\varphi}'\colon \widehat{\mathfrak{n}}/\widehat{\mathfrak{n}}^2 \to \widehat{\mathfrak{m}}/\widehat{\mathfrak{m}}^2$ is injective. So we may replace A and B by $\widehat{A}$ and $\widehat{B}$, and thus assume A and B complete.

Take $b_1, \dots, b_n \in \mathfrak{n}$ whose residues in $\mathfrak{n}/\mathfrak{n}^2$ form a k-basis. Set $a_i := \varphi(b_i)$ for all i. As φ' is injective, the residues of $a_1, \dots, a_n$ are linearly independent in $\mathfrak{m}/\mathfrak{m}^2$. Complete $a_1, \dots, a_n$ to $a_1, \dots, a_r \in \mathfrak{m}$ whose residues form a basis of $\mathfrak{m}/\mathfrak{m}^2$. As A is regular, $r = \dim(A)$ by (**21.14**). So by (**22.58**), there's a canonical isomorphism $A = k[[X_1, \dots, X_r]]$ for some variables X_i and with a_i corresponding to X_i.

Set $A' := k[[X_1, \dots, X_n]]$. Then (**22.55**) yields k-surjections $\psi\colon A' \to B$ and $\kappa\colon A \to A'$ with $\psi(X_i) = b_i$ for all i and $\kappa(X_i) = X_i$ for $1 \le i \le n$ and $\kappa(X_i) = 0$ for $n < i \le r$. Then $\kappa\varphi\psi(X_i) = X_i$ for $1 \le i \le n$; so $\kappa\varphi\psi = 1_{A'}$ by (**22.55**). So ψ is injective too. So ψ is an isomorphism. Thus (**22.27**) implies B is regular. □

Exercise (22.65) . — Let R be a Noetherian ring, and $X_1, \dots, X_n$ variables. Show that $R[[X_1, \dots, X_n]]$ is faithfully flat.

Solution: The inclusion of R in $R[[X_1, \dots, X_n]]$ factors as follows:

$$R \to R[X_1, \dots, X_n] \to R[[X_1, \dots, X_n]].$$

The first map is flat by (**9.20**). The second map is flat by (**22.22**). Hence the composition is flat by (**9.23**). Given any ideal $\mathfrak{a}$ of R, its extension $\mathfrak{a}R[[X_1, \dots, X_n]]$ contains only power series with all coefficients in $\mathfrak{a}$; so $\mathfrak{a} = \mathfrak{a}R[[X_1, \dots, X_n]] \cap R$. Thus (**9.28**)(3)⇒(1) yields the result. □

Exercise (22.66) (*Gabber–Ramero* [**8**, Lem. 7.1.6]**) . —** Let R be a ring, $\mathfrak{a}$ an ideal, N a module. Assume N is flat. Prove the following:

(1) The functor $M \mapsto (M \otimes N)\widehat{\ }$ is exact on the Noetherian modules M.

(2) Assume R is Noetherian. Then for all finitely generated modules M, there's a canonical isomorphism $M \otimes \widehat{N} \xrightarrow{\sim} (M \otimes N)\widehat{\ }$, and $\widehat{N}$ is flat over R.

Solution: For (1), let $0 \to M' \to M \to M'' \to 0$ be an exact sequence of Noetherian modules. As N is flat, $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact too. Hence $0 \to (M' \otimes N)\widehat{\ } \to (M \otimes N)\widehat{\ } \to (M'' \otimes N)\widehat{\ } \to 0$ is exact by **(22.12)**(1), provided the ($\mathfrak{a}$-adic) topology on $M \otimes N$ induces that on $M' \otimes N$.

Set $F^n M' := M' \cap \mathfrak{a}^n M$ and $F^n(M' \otimes N) := (M' \otimes N) \cap (\mathfrak{a}^n M \otimes N)$. The $F^n M'$ form an $\mathfrak{a}$-stable filtration by the Artin–Rees Lemma **(20.12)**. But N is flat. So $(F^n M') \otimes N = F^n(M' \otimes N)$ by **(9.18)**. Hence the $F^n(M' \otimes N)$ form an $\mathfrak{a}$-stable filtration. Thus by **(22.1)**, it defines the $\mathfrak{a}$-adic topology. Thus (1) holds.

In (2), the first assertion follows from (1) and **(8.14)** (and **(16.15)**). The second assertion results from the Ideal Criterion **(9.15)**: given any ideal $\mathfrak{a}$, the inclusion $\mathfrak{a} \hookrightarrow R$ induces an injection $\mathfrak{a} \otimes \widehat{N} \hookrightarrow \widehat{N}$ owing to the first assertion and to (1). □

Exercise (22.67) . — Let P be the polynomial ring over $\mathbb{C}$ in variables $X_1, \dots, X_n$, and A its localization at $\langle X_1, \dots, X_n \rangle$. Let C be the ring of all formal power series in $X_1, \dots, X_n$, and B its subring of series converging about the origin in $\mathbb{C}^n$. Assume basic Complex Analysis (see [7, pp. 105–123]). Show B is local, and its maximal ideal is generated by $X_1, \dots, X_n$. Show $P \subset A \subset B \subset C$, and $\widehat{P} = \widehat{A} = \widehat{B} = C$. Show C is faithfully flat over both A and B, and B is faithfully flat over A.

Solution: Set $\mathfrak{m}_B := \{ F \in B \mid F(0) = 0 \}$. Plainly, $\mathfrak{m}_B$ is an ideal. But $B - \mathfrak{m}_B$ consists of units (see **(22.89)** or [7, 1., p. 108]). Thus by **(3.5)**, B is local, and $\mathfrak{m}_B$ maximal.

Trivially, $P \subset B \subset C$. Set $\mathfrak{m}_P := \{ F \in P \mid F(0) = 0 \}$. Then $\mathfrak{m}_P = \mathfrak{m}_B \cap P$. But plainly $\mathfrak{m}_P = \langle X_1, \dots, X_n \rangle$. So $\mathfrak{m}_P$ is maximal. Moreover, by **(11.3)**, the inclusion $P \hookrightarrow B$ induces an inclusion $A \hookrightarrow B$. Thus $P \subset A \subset B \subset C$.

Let $\mathfrak{m}_A$ and $\mathfrak{m}_C$ be the ideals of A and C generated by $X_1, \dots, X_n$. They are the maximal ideals of A and C by **(11.12)**(1) and **(3.7)**. Next, let $\mathfrak{b}$ be the ideal of B generated by $X_1, \dots, X_n$, and let's show $\mathfrak{b} = \mathfrak{m}_B$.

More generally, fix $r \geq 1$. Let's show $\mathfrak{b}^r = \mathfrak{m}_B^r = B \cap \mathfrak{m}_C^r$. Note $X_1, \dots, X_n \in \mathfrak{m}_B$. So $\mathfrak{b}^r \subset \mathfrak{m}_B^r$. Now, $\mathfrak{m}_B$ lies in the set of all $F \in C$ with vanishing constant term, which is plainly equal to $\mathfrak{m}_C$. So $\mathfrak{m}_B^r \subset m_C^r$. Thus it suffices to show $B \cap \mathfrak{m}_C^r \subset \mathfrak{b}^r$.

Given $F \in \mathfrak{m}_C^r$, say $F = \sum_{j=1}^m M_j G_j$ where the M_j are the monomials of degree r and $G_j \in C$. By induction on $d \geq 0$, let's define $G_{j,d}$ for all j so that (1) $G_{j,d}$ and $G_{j,d-1}$ differ only in degree d if $d \geq 1$ and (2) there's no monomial N of degree $r + d$ that appears in $M_j G_{j,d}$ for two different j and (3) $F = \sum_{j=1}^m M_j G_{j,d}$.

Set $G_{j,0} := G_j$ for all j. Then (2) and (3) hold with $d := 0$.

Assume $d \geq 1$ and the $G_{j,d-1}$ are defined. Initially set $G_{j,d} := G_{j,d-1}$ for all j. If there's a monomial N of degree $r + d$ that appears in both $M_j G_{j,d}$ and $M_i G_{i,d}$ with $1 \leq i < j \leq m$, then let a be the coefficient of N in $M_j G_{j,d}$, replace $G_{j,d}$ by $G_{j,d} - (aN/M_j)$, and replace $G_{i,d}$ by $G_{i,d} + (aN/M_i)$. Repeat until (2) holds (only finitely many triples N, j, i are involved). Then (1) and (3) hold for the $G_{j,d}$ too.

Replace G_j by $\lim_{d \to \infty} G_{j,d}$, which exists owing to (1). Note $F = \sum_{j=1}^m M_j G_j$ owing to (3). Also, all the $M_j G_j$ have different monomials owing to (2). Hence, each monomial N of each $M_j G_j$ appears in F, and N has the same coefficient in both $M_j G_j$ and F.

Suppose also $F \in B$. Then F is absolutely uniformly convergent in a neighborhood U of the origin. Hence, owing to the preceding paragraph, each $M_j G_j$ too is absolutely uniformly convergent in U by the Comparison Test. So $G_j \in B$ for all j. Thus $F \in \mathfrak{b}^r$. Thus $B \cap \mathfrak{m}_C^r \subset \mathfrak{b}^r$. Thus $\mathfrak{b}^r = \mathfrak{m}_B^r = B \cap \mathfrak{m}_C^r$.

Suppose also $F \in P$. Recall that each monomial of each M_jG_j appears in F. So $G_j \in P$ for all j. Thus $P \cap \mathfrak{m}_C^r \subset \mathfrak{m}_P^r$. But plainly $\mathfrak{m}_P^r \subset \mathfrak{m}_C^r$. Thus $\mathfrak{m}_P^r = P \cap \mathfrak{m}_C^r$.

So $\mathfrak{m}_P^r = P \cap (A \cap \mathfrak{m}_C^r)$. But $\mathfrak{m}_P^r$ is $\mathfrak{m}_P$-primary by **(18.9)**, so saturated by **(18.20)**; so $P \cap \mathfrak{m}_P^r A = \mathfrak{m}_P^r$ by **(11.12)**(1). But $\mathfrak{m}_P^r A = \mathfrak{m}_A^r$. Thus $P \cap (A \cap \mathfrak{m}_C^r) = P \cap \mathfrak{m}_A^r$. Thus, by **(11.12)**(1) again, $\mathfrak{m}_A^r = A \cap \mathfrak{m}_C^r$.

So $\mathfrak{m}_A^r = A \cap (B \cap \mathfrak{m}_C^r)$. But $\mathfrak{m}_B^r = B \cap \mathfrak{m}_C^r$. Thus $\mathfrak{m}_A^r = A \cap \mathfrak{m}_B^r$.

Hence, there are induced injections:

$$P/\mathfrak{m}_P^r \hookrightarrow A/\mathfrak{m}_A^r \hookrightarrow B/\mathfrak{m}_B^r \hookrightarrow C/\mathfrak{m}_C^r.$$

But the composition $P/\mathfrak{m}_P^r \hookrightarrow C/\mathfrak{m}_C^r$ is plainly surjective. So all the displayed maps are bijective. Thus **(22.7)** yields $\widehat{P} = \widehat{A} = \widehat{B} = \widehat{C}$. But $\widehat{P} = C$ by **(22.2)**. Thus $\widehat{P} = \widehat{A} = \widehat{B} = C$.

Recall P is Noetherian by the Hilbert Basis Theorem, **(16.10)**; so A is Noetherian by **(16.33)**. Recall B is Noetherian by **(22.89)** or [7, 3.7, p. 122]. But A and B are local. So **(22.36)**(1)⇒(7) implies $\widehat{A}$ is faithfully flat over A, and $\widehat{B}$ is faithfully flat over B. But $\widehat{A} = \widehat{B} = C$. Thus C is faithfully flat over both A and B. Finally, by **(9.25)**, B is flat over A; so by **(10.30)**, faithfully flat. □

Exercise (22.68) . — Let R be a Noetherian ring, and $\mathfrak{a}$ and $\mathfrak{b}$ ideals. Assume $\mathfrak{a} \subset \operatorname{rad}(R)$, and use the $\mathfrak{a}$-adic toplogy. Prove $\mathfrak{b}$ is principal if $\mathfrak{b}\widehat{R}$ is.

Solution: Since R is Noetherian, $\mathfrak{b}$ is finitely generated. But $\mathfrak{a} \subset \operatorname{rad}(R)$. Hence, $\mathfrak{b}$ is principal if $\mathfrak{b}/\mathfrak{ab}$ is a cyclic R-module by **(10.8)**(2). But $\mathfrak{b}/\mathfrak{ab} = \widehat{\mathfrak{b}}/(\mathfrak{ab})\widehat{}$ by **(22.12)**(1)–(2), and $\widehat{\mathfrak{b}} = \mathfrak{b}\widehat{R}$ by **(22.20)**.

Assume $\mathfrak{b}\widehat{R} = \widehat{R}b$ for some $b \in \widehat{R}$. Then $\widehat{\mathfrak{b}}/(\mathfrak{ab})\widehat{} = \widehat{R}b'$ where b' is the residue of b. Given $x \in \widehat{R}$, say x is the limit of the Cauchy sequence $(\kappa_R y_n)$ with $y_n \in R$. Then $x - \kappa_R y_n \in \widehat{\mathfrak{a}}$ for some n. So $xb' = y_n b'$ as $\widehat{\mathfrak{b}}\widehat{\mathfrak{a}} \subset (\mathfrak{ba})\widehat{}$. Thus $\mathfrak{b}/\mathfrak{ab} = Rb'$, as desired. □

Exercise (22.69) (*Nakayama's Lemma for adically complete rings*) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a module. Assume R is complete, and M separated. Show $m_1, \dots, m_n \in M$ generate assuming their images $m_1', \dots, m_n'$ in $M/\mathfrak{a}M$ generate.

Solution: Note that $m_1', \dots, m_n'$ generate $G(M)$ over $G(R)$. Thus $m_1, \dots, m_n$ generate M over R by the proof of **(22.24)**.

Alternatively, by **(22.24)**, M is finitely generated over R and complete. As M is separated, $M = \widehat{M}$ by **(22.3)** and **(22.13)**(1). So M is also an $\widehat{R}$-module. As R is complete, $\kappa_R \colon R \to \widehat{R}$ is surjective by **(22.13)**(1). But $\mathfrak{a}$ is closed by **(22.1)**; so $\mathfrak{a}$ is complete; so $\kappa_{\mathfrak{a}} \colon \mathfrak{a} \to \widehat{\mathfrak{a}}$ is surjective too. Hence $\mathfrak{a}M = \widehat{\mathfrak{a}}M$. Thus $M/\mathfrak{a}M = M/\widehat{\mathfrak{a}}M$. So the m_i generate $M/\widehat{\mathfrak{a}}M$. But $\widehat{\mathfrak{a}} \subset \operatorname{rad}(\widehat{R})$ by **(22.4)**. So by Nakayama's Lemma **(10.8)**(2), the m_i generate M over $\widehat{R}$, so also over R as κ_R is surjective. □

Exercise (22.70) . — Let $A \to B$ be a local homomorphism of Noetherian local rings, $\mathfrak{m}$ the maximal ideal of A. Assume B is **quasi-finite** over A; that is, $B/\mathfrak{m}B$ is a finite-dimensional $A/\mathfrak{m}$-vector space. Show that $\widehat{B}$ is module finite over $\widehat{A}$.

Solution: Take $y_1, \ldots, y_n \in B$ whose residues generate the vector space $B/\mathfrak{m}B$. By (**22.69**), the y_i generate $\widehat{B}$ as an $\widehat{A}$-module if their residues y_i' generate $\widehat{B}/\widehat{\mathfrak{m}}\widehat{B}$ and if $\widehat{B}$ is separated in the $\widehat{\mathfrak{m}}$-adic topology. Let's check those two conditions.

Set $\mathfrak{b} := \mathfrak{m}B$. Let $\mathfrak{n}$ be the maximal ideal of B. Given $n \geq 0$, note $(\mathfrak{b}^n)\widehat{\ } = \mathfrak{b}^n\widehat{B}$ by (**22.20**) with $R := B$ and $\mathfrak{a} := \mathfrak{n}$. But $\mathfrak{b}^n\widehat{B} = \mathfrak{m}^n\widehat{B} = (\mathfrak{m}^n\widehat{A})\widehat{B}$. Moreover, $\mathfrak{m}^n\widehat{A} = (\widehat{\mathfrak{m}})^n$ by (**22.20**) with $R := A$ and $\mathfrak{a} := \mathfrak{m}$. Thus

$$(\mathfrak{b}^n)\widehat{\ } = (\widehat{\mathfrak{m}})^n\widehat{B}. \tag{22.70.1}$$

Since $B/\mathfrak{b}$ is finite-dimensional over $A/\mathfrak{m}$, it is Artinian by (**19.10**). So $\mathfrak{n}/\mathfrak{b}$ is nilpotent by (**19.23**). Thus there is $m > 0$ with $\mathfrak{n}^m \subset \mathfrak{b} \subset \mathfrak{n}$.

Hence $B/\mathfrak{b}$ is discrete in the $\mathfrak{n}$-adic topology. So $B/\mathfrak{b} = (B/\mathfrak{b})\widehat{\ }$. However, $(B/\mathfrak{b})\widehat{\ } = \widehat{B}/\widehat{\mathfrak{b}}$ by (**22.18**) with $R := B$ and $\mathfrak{a} := \mathfrak{n}$. Also $\widehat{\mathfrak{b}} = \widehat{\mathfrak{m}}\widehat{B}$ by (**22.70.1**) with $n := 1$. Hence $B/\mathfrak{b} = \widehat{B}/\widehat{\mathfrak{m}}\widehat{B}$. Thus the y_i' generate $\widehat{B}/\widehat{\mathfrak{m}}\widehat{B}$ over A, so over $\widehat{A}$.

Again since $\mathfrak{n}^m \subset \mathfrak{b} \subset \mathfrak{n}$, the $\mathfrak{m}$-adic topology on B is the same as the $\mathfrak{n}$-adic. But $\widehat{B}$ is the separated completion of B for the $\mathfrak{n}$-adic topology. So $\widehat{B}$ has the topology defined by the filtration $F^n\widehat{B} := (\mathfrak{b}^n)\widehat{\ }$. But $(\mathfrak{b}^n)\widehat{\ } = (\widehat{\mathfrak{m}})^n\widehat{B}$ by (**22.70.1**). Thus $\widehat{B}$ has the $\widehat{\mathfrak{m}}$-adic topology, and by (**22.16**)(4), is separated in it, as desired. □

Exercise (22.71) . — Let A be the non-Noetherian local ring of (**18.24**). Using E. Borel's theorem that every formal power series in x is the Taylor expansion of some C^∞-function (see [**13**, Ex. 5, p. 244]), show $\widehat{A} = \mathbb{R}[[x]]$, and $\widehat{A}$ is Noetherian; moreover, show $\widehat{A}$ is a quotient of A (so module finite).

Solution: Consider the Taylor-series map $\tau\colon A \to \mathbb{R}[[x]]$ of (**18.24**); it's defined by $\tau(F) := \sum_{n=0}^{\infty} \frac{F^{(n)}(0)}{n!}x^n$. It's a ring map; so $\tau(x^kA) \subset x^k\mathbb{R}[[x]]$ for each k. By Borel's Theorem, τ is surjective. Thus τ induces a surjective map

$$\tau_k\colon A/x^kA \twoheadrightarrow \mathbb{R}[[x]]/x^k\mathbb{R}[[x]].$$

Suppose $\tau(F) = x^kG$ where $G \in \mathbb{R}[[x]]$. By Borel's Theorem, $G = \tau(H)$ for some $H \in A$. So $\tau(F - x^kH) = 0$. But $\mathrm{Ker}(\tau) = \bigcap_{n\geq 0} x^nA$ by (**18.24**). Hence $F - x^kH \in x^kA$. Thus τ_k is injective, so bijective. Thus $\widehat{A} = \mathbb{R}[[x]]$ by (**22.7**). Finally, $\mathbb{R}[[x]]$ is Noetherian by (**22.27**), so $\widehat{A}$ is Noetherian too.

Moreover, since τ is surjective, $\widehat{A}$ is a quotient of A. □

Exercise (22.72) . — Let R be a ring, $\mathfrak{q}$ an ideal, M a module. Prove that, if M is free, then $M/\mathfrak{q}M$ is free over $R/\mathfrak{q}$ and multiplication of $G_\mathfrak{q}(R)$ on $G_\mathfrak{q}(M)$ induces an isomorphism $\sigma_M\colon G_\mathfrak{q}(R) \otimes_{R/\mathfrak{q}} M/\mathfrak{q}M \xrightarrow{\sim} G_\mathfrak{q}(M)$. Prove the converse holds if either (a) $\mathfrak{q}$ is nilpotent, or (b) M is Noetherian, and $\mathfrak{q} \subset \mathrm{rad}(M)$.

Solution: Recall from (**20.7**) that $G_\mathfrak{q}(M)$ is a graded $G_\mathfrak{q}(R)$-module and that $G_\mathfrak{q}(R)$ is a graded $G_{\mathfrak{q},0}(R)$-algebra; also $G_0(M) = M/\mathfrak{q}M$ and $G_{\mathfrak{q},0}(R) = R/\mathfrak{q}$. Thus the multiplication pairing induces the desired map σ_M.

Note that σ_R is an isomorphism by (**8.5**)(2) applied with $R/\mathfrak{q}$ for R.

Assume M is free, say $M = R^\Lambda$ for some Λ. Let's show $\sigma_M = \sigma_R^\Lambda$. First, given ideals $\mathfrak{a}$, $\mathfrak{b}$, set $\mathfrak{c} := \mathfrak{a}/\mathfrak{b}$, and note that $\mathfrak{a}M = \mathfrak{a}^\Lambda$ by (**4.28**) and that $\mathfrak{a}^\Lambda/\mathfrak{b}^\Lambda = \mathfrak{c}^\Lambda$ by (**5.4**). Given $n \geq 0$, take $\mathfrak{a} := \mathfrak{q}^n$ and $\mathfrak{b} := \mathfrak{q}^{n+1}$. Thus $G_{\mathfrak{q},\mathfrak{n}}(M) = (G_{\mathfrak{q},n}(R))^\Lambda$.

Taking $n := 0$ yields $M/\mathfrak{q}M = (R/\mathfrak{q})^\Lambda$. Thus $M/\mathfrak{q}M$ is a free $R/\mathfrak{q}$-module, as desired. But $G_\mathfrak{q}(R) \otimes_{R/\mathfrak{q}} (R/\mathfrak{q})^\Lambda = (G_\mathfrak{q}(R) \otimes_{R/\mathfrak{q}} (R/\mathfrak{q}))^\Lambda$ by (**8.10**). Thus $\sigma_M = \sigma_R^\Lambda$. But σ_R is an isomorphism, thus σ_M is too, as desired.

Conversely, assume $M/\mathfrak{q}M$ is free over $R/\mathfrak{q}$. Say $m_\lambda \in M$ for $\lambda \in \Lambda$ yield a free basis of $M/\mathfrak{q}M$. Set $F := R^\Lambda$, and define $\alpha\colon F \to M$ by $\alpha(e_\lambda) := m_\lambda$ where the e_λ form the standard basis. Then α induces an isomorphism $\alpha'\colon F/\mathfrak{q}F \xrightarrow{\sim} M/\mathfrak{q}M$.

Assume σ_M is an isomorphism too. Consider the commutative diagram

$$\begin{array}{ccc} G_{\mathfrak{q}}(R) \otimes_{R/\mathfrak{q}} F/\mathfrak{q}F & \xrightarrow{\sigma_F} & G_{\mathfrak{q}}(F) \\ {\scriptstyle 1\otimes\alpha'}\big\downarrow & & \big\downarrow{\scriptstyle G_{\mathfrak{q}}(\alpha)} \\ G_{\mathfrak{q}}(R) \otimes_{R/\mathfrak{q}} M/\mathfrak{q}M & \xrightarrow{\sigma_M} & G_{\mathfrak{q}}(M) \end{array}$$

Its top, left, and bottom maps are isomorphisms. So its right map $G_{\mathfrak{q}}(\alpha)$ is too. So $\widehat{\alpha}\colon \widehat{F} \to \widehat{M}$ is an isomorphism by **(22.23)**. But $\mathfrak{q}^n = \langle 0 \rangle$ for some n in case (a), and $\bigcap \mathfrak{q}^n M = 0$ by **(18.35)** in case (b); so $M \hookrightarrow \widehat{M}$ by **(22.3)**. Thus α is injective.

For surjectivity of α, set $N := \mathrm{Im}(\alpha)$. Then $M = N + \mathfrak{q}M$ as α' is surjective. Hence $\mathfrak{q}(M/N) = M/N$. So $M/N = 0$, in case (a) by **(3.31)**, and in case (b) by **(10.6)**. So $M = N$. Hence α is surjective, so bijective. Thus M is free. □

22. Appendix: Hensel's Lemma

Exercise (22.76) . — Let R be a ring, $\mathfrak{a}$ an ideal, X a variable, $F \in R[X]$. Assume its residue $\overline{F} \in (R/\mathfrak{a})[X]$ has a supersimple root $\widetilde{a} \in R/\mathfrak{a}$, and R is separated and complete. Then F has a unique supersimple root $a \in R$ with residue $\widetilde{a}$.

Solution: Set $\widetilde{G} := (X - \widetilde{a})$. As $\widetilde{a}$ is a supersimple root, **(2.34)** yields a unique $\widetilde{H} \in (R/\mathfrak{a})[X]$ coprime to $\widetilde{G}$ with $\overline{F} = \widetilde{G}\widetilde{H}$. So **(22.75)** yields unique coprime $G, H \in R[X]$ with $F = GH$, with residues $\widetilde{G}, \widetilde{H}$, and with G monic. Hence $G = X - a$ with $a \in R$ with residue $\widetilde{a}$. Thus, by **(2.34)**, a is as desired. □

Exercise (22.86) . — Show that **(22.75)** is a formal consequence of **(22.85)** when R is a local ring with maximal ideal $\mathfrak{a}$ such that $k := R/\mathfrak{a}$ is algebraically closed.

Solution: Set $n := \deg(\widetilde{G})$. Induct on n. Note that the case $n = 0$ is trivial.

Assume $n \geq 1$. As k is algebraically closed, $\widetilde{G} = (X - c)^s \widetilde{G}_1$ with $c \in k$ and $s \geq 1$ and $\widetilde{G}_1(0) \neq 0$. Let φ be the R-algebra automorphism of $R[X]$ defined by $\varphi(X) := X + c$, and let $\overline{\varphi}$ be the corresponding k-algebra automorphism of $k[X]$. Replace F by $\varphi(F)$ and $\widetilde{G}$, $\widetilde{G}_1$, $\widetilde{H}$ by $\widetilde{\varphi}(\widetilde{G})$, $\widetilde{\varphi}(\widetilde{G}_1)$, $\widetilde{\varphi}(\widetilde{H})$, and thus assume $c = 0$.

Set $\widetilde{U} := \widetilde{G}_1\widetilde{H}$. Then $\overline{F} = X^s\widetilde{U}$ and $\widetilde{U}(0) \neq 0$. Say $F =: \sum f_i X^i$. Then reducing mod $\mathfrak{a}[X]$ yields $\overline{f}_s = \widetilde{U}(0)$ and $\overline{f}_i = 0$ for $i < s$. So $f_s \in R^\times$ and $f_i \in \mathfrak{a}$ for $i < s$. Thus **(22.85)** yields $U, V \in R[X]$ where $U(0) \in R^\times$ and where $V = X^s + v_{s-1}X^{s-1} + \cdots + v_0$ with all $v_i \in \mathfrak{a}$ such that $F = UV$.

Reducing mod $\mathfrak{a}[X]$ yields $\overline{F} = \overline{UV}$ and $\overline{V} = X^s$. But $k[X]$ is a UFD. So $\overline{U} = \widetilde{U}$. So $\overline{U} = \widetilde{G}_1\widetilde{H}$. But $\deg(\widetilde{G}_1) = \deg(\widetilde{G}) - s$ and $s \geq 1$. Also, $\widetilde{G}_1$ is monic as $\widetilde{G}$ is, and $\widetilde{G}_1$ and $\widetilde{H}$ are coprime as $\widetilde{G}$ and $\widetilde{H}$ are. So by induction, $U = G_1H$ where G_1 is monic and G_1 and H are coprime with residues $\widetilde{G}_1$ and $\widetilde{H}$.

Set $G := VG_1$. Then $F = UV = VG_1H = GH$ and $\overline{G} = X^s\overline{G}_1 = \widetilde{G} \bmod \mathfrak{a}[X]$. As V and G_1 are monic, so is G. By **(10.33)**(2), as $\widetilde{G}$ and $\widetilde{H}$ are coprime, so are G and H. Finally, the factorization $F = GH$ is unique by **(22.73)**. □

Exercise (22.87) . — Let k be a field, $B_n := k[[X_1, \ldots, X_n]]$ the local ring of power series in n variables X_i. Use (**22.59**) and (**22.84**) to recover, by induction, the conclusion of (**22.27**), that B_n is Noetherian.

Solution: The case $n = 0$ is trivial. So assume $n \geq 1$ and B_{n-1} Noetherian. Given a nonuzero ideal $\mathfrak{a} \subset B_n$, take a nonzero $F =: \sum f_i X_n^i \in \mathfrak{a}$. By (**22.59**), there's an algebra automorphism φ of B_n such that $\varphi(F)$ contains a term of the form cX_n^s with $c \neq 0$. Say s is smallest; then $f_j(0) = 0$ for $j < s$ and $f_s(0) \neq 0$. It suffices to show $\varphi(\mathfrak{a})$ is finitely generated; so replace $\mathfrak{a}$ by $\varphi(\mathfrak{a})$ and F by $\varphi(F)$.

For any $G \in \mathfrak{a}$, there are $Q \in B_n$ and $P \in B_{n-1}[X_n]$ with $G = QF + P$ and with $\deg(P) < s$ by (**22.84**). Set $M := \mathfrak{a} \cap \sum_{i=0}^{s-1} B_{n-1} X_n^i$. Then $P \in M$. Thus $\mathfrak{a} = \langle F \rangle + M$. But B_{n-1} is Noetherian; so M is a finitely generated B_{n-1}-submodule of $\sum_{i=0}^{s-1} B_{n-1} X_n^i$. Thus $\mathfrak{a}$ is finitely generated, as desired. □

Exercise (22.88) . — Let k be a field, $B_n := k[[X_1, \ldots, X_n]]$ the local ring of power series in n variables X_i. Use (**22.27**) and (**22.59**) and (**22.85**) to show, by induction, that B_n is a UFD.

Solution: The case $n = 0$ is trivial. So assume $n \geq 1$. Fix a nonzero nonunit $F \in B_n$. Now, B_n is Noetherian by (**22.27**). So $F = F_1, \cdots F_r$ with F_i irreducible. Suppose also $F = F'_1, \cdots F'_{r'}$ with F'_j irreducible. We must show that $r = r'$ and that after reordering, $F_i = W_i F'_i$ with W_i a unit.

By (**22.59**), there's an algebra automorphism φ of B_n with $(\varphi F)(0, \ldots, 0, X_n)$ nonzero. Plainly, we may replace F, F_i, and F'_j by φF, φF_i, and $\varphi F'_j$. Then $F(0, \ldots, 0, X_n)$ is nonzero. So the $F_i(0, \ldots, 0, X_n)$ and $F_j(0, \ldots, 0, X_n)$ are too.

By (**22.85**), $F = UV$ and $F_i = U_i V_i$ and $F'_j = U'_j V'_j$ with $U, U_i, U'_j \in B_n^\times$ and $V, V_i, V'_j \in B_{n-1}[X_n]$ monic with all nonleading coefficients in $\langle X_1, \ldots, X_{n-1} \rangle$. But F_i and F'_j are irreducible in B_n. So V_i and V'_j are irreducible in $B_{n-1}[X_n]$. Moreover, $UV = \prod U_i V_i = \prod U'_j V'_j$. So $U = \prod U_i = \prod U'_j$ and $V = \prod V_i = \prod V'_j$ owing to the uniqueness assertion in (**22.85**).

By induction, B_{n-1} is a UFD. So $B_{n-1}[X_n]$ is a UFD too. Hence $r = r'$ and $V_i = W'_i V'_i$ with $W'_i \in B_{n-1}[X_n]^\times$. Thus $F_i = W_i F'_i$ with $W_i \in B_n^\times$, as desired. □

Exercise (22.90) . — (Implicit Function Theorem) Let R be a ring, $T_1, \ldots, T_n, X$ variables. Given a polynomial $F \in R[T_1, \ldots, T_n, X]$ such that $F(0, \ldots, 0, X)$ has a supersimple root $a_0 \in R$. Show there's a unique power series $a \in R[[T_1, \ldots, T_n]]$ with $a(0, \ldots, 0) = a_0$ and $F(T_1, \ldots, T_n, a) = 0$.

Solution: Set $A := R[[T_1, \ldots, T_n]]$ and $\mathfrak{a} = \langle T_1, \ldots, T_n \rangle$. Then A is $\mathfrak{a}$-adically separated and complete by (**22.2**), and $A/\mathfrak{a} = R$ by (**3.7**).

View $F \in A[X]$. Its residue in $R[X]$ is $F(0, \ldots, 0, X)$. So (**22.76**) implies F has a unique supersimple root $a \in A$ with $a(0, \ldots, 0) = a_0$, as desired. □

Exercise (22.91) . — Let A be the filtered direct limit of Henselian local rings A_λ with local transition maps. Show A is local and Henselian.

Solution: For all λ, let $\mathfrak{m}_\lambda$ be the maximal ideal of A_λ. Set $\mathfrak{m} := \varinjlim \mathfrak{m}_\lambda$. Then A is local with maximal ideal $\mathfrak{m}$ by (**7.21**). Set $k := A/\mathfrak{m}$ and $k_\lambda := A_\lambda/\mathfrak{m}_\lambda$. Then (**7.9**) imples $k = \varinjlim k_\lambda$. Use '$\overline{}$' to indicate residues modulo $\mathfrak{m}$ and $\mathfrak{m}_\lambda$.

Let X be a variable. Given $F \in A[X]$ monic, assume $\overline{F} = \widetilde{G}\widetilde{H}$ with $\widetilde{G}, \widetilde{H} \in k[X]$ monic and coprime. By (**7.5**)(1) applied coefficientwise, there's λ_0 such that F and

$\widetilde{G}$, $\widetilde{H}$ come from $F_{\lambda_0} \in A_{\lambda_0}[X]$ and $\widetilde{G}_{\lambda_0}$, $\widetilde{H}_{\lambda_0} \in k_{\lambda_0}[X]$. Take them monic. For all $\lambda \ge \lambda_0$, let $F_\lambda \in A_\lambda[X]$ and $\widetilde{G}_\lambda$, $\widetilde{H}_\lambda \in k_\lambda[X]$ be the images of F_{λ_0} and $\widetilde{G}_{\lambda_0}$, $\widetilde{H}_{\lambda_0}$.

Note $\overline{F} - \widetilde{G}\widetilde{H} = 0$. So **(7.5)**(3) yields $\lambda_1 \ge \lambda_0$ with $\overline{F}_{\lambda_1} = \widetilde{G}_{\lambda_1}\widetilde{H}_{\lambda_1}$.

As $\widetilde{G}$, $\widetilde{H}$ are coprime, there are $\widetilde{G}'$, $\widetilde{H}' \in k[X]$ with $\widetilde{G}'\widetilde{G} + \widetilde{H}'\widetilde{H} = 1$. By **(7.5)**(1), (3), there's $\lambda_2 \ge \lambda_1$ such that $\widetilde{G}'$, $\widetilde{H}'$ come from $\widetilde{G}'_{\lambda_2}$, $\widetilde{H}'_{\lambda_2} \in k_{\lambda_2}[X]$ and $\widetilde{G}'_{\lambda_2}\widetilde{G}_{\lambda_2} + \widetilde{H}'_{\lambda_2}\widetilde{H}_{\lambda_2} = 1$. Thus $\widetilde{G}_{\lambda_2}$, $\widetilde{H}_{\lambda_2}$ are coprime.

As A_{λ_2} is Henselian, $F_{\lambda_2} = G_{\lambda_2}H_{\lambda_2}$ with monic and coprime $G_{\lambda_2}, H_{\lambda_2}$ having residues $\widetilde{G}_{\lambda_2}$, $\widetilde{H}_{\lambda_2}$. Let G, $H \in A[X]$ be the images of G_{λ_2}, H_{λ_2}. Then $F = GH$ with monic and coprime G, H having residues $\widetilde{G}$, $\widetilde{H}$. Thus A is Henselian. □

Exercise (22.92) . — Let A be a local Henselian ring, $\mathfrak{m}$ its maximal ideal, B an integral A-algebra, and $\mathfrak{n}$ a maximal ideal of B. Set $\overline{B} = B/\mathfrak{m}B$. Show:

(1) $\mathrm{Idem}(B) \to \mathrm{Idem}(\overline{B})$ is bijective. (2) $B_\mathfrak{n}$ is integral over A, and Henselian.

Solution: For (1), let $\{B_\lambda\}$ be the set of module-finite subalgebras of B. By **(10.14)**(1)⇒(2), every $x \in B$ lies in some B_λ, namely $A[x]$. By **(10.18)**(2)⇒(3), given λ, μ, there's ν with B_λ, $B_\lambda \subset B_\nu$. Thus **(7.2)** yields $B = \varinjlim B_\lambda$.

Set $\overline{B}_\lambda := B_\lambda/\mathfrak{m}B_\lambda$. Then $\overline{B} = \varinjlim \overline{B}_\lambda$ by **(7.9)**. Furthermore, **(7.5)** implies $\mathrm{Idem}(B) = \varinjlim \mathrm{Idem}(B_\lambda)$ and $\mathrm{Idem}(\overline{B}) = \varinjlim \mathrm{Idem}(\overline{B}_\lambda)$. But A is Henselian; so each B_λ is decomposable by **(22.78)**(1)⇒(3); so $\mathrm{Idem}(B_\lambda) \to \mathrm{Idem}(\overline{B}_\lambda)$ is bijective by **(19.15)**(5). Thus (1) holds.

For (2), let $\mathfrak{n}_\lambda$ be the contraction of $\mathfrak{n}$ in B_λ. Then $B_\mathfrak{n} = \varinjlim (B_\lambda)_{\mathfrak{n}_\lambda}$ by **(11.25)**. But $(B_\lambda)_{\mathfrak{n}_\lambda}$ is module-finite over A, as it is a direct summand of B_λ by **(11.18)**. So $(B_\lambda)_{\mathfrak{n}_\lambda}$ is integral over A by **(10.18)**(3)⇒(1). Thus $B_\mathfrak{n}$ is integral over A.

As each $(B_\lambda)_{\mathfrak{n}_\lambda}$ is module-finite over A, each is Henselian by **(22.79)**. So $B_\mathfrak{n}$ is Henselian by **(22.91)**. Thus (2) holds. □

Exercise (22.93) . — Let A be local ring. Show that A is Henselian if and only if, given any module-finite algebra B and any maximal ideal $\mathfrak{n}$ of B, the localization $B_\mathfrak{n}$ is integral over A.

Solution: If A is Henselian, then **(22.92)**(2) implies $B_\mathfrak{n}$ is integral over A.

Conversely, by **(22.78)**, we need only to show that B is decomposable. Now, B is semilocal by **(19.22)**. So by **(13.59)**, given maximal ideals $\mathfrak{n}_1$, $\mathfrak{n}_2 \subset B$ with $(B_{\mathfrak{n}_1})_{\mathfrak{n}_2} \ne 0$, we need only to show that $\mathfrak{n}_1 = \mathfrak{n}_2$.

Fix a prime of $(B_{\mathfrak{n}_1})_{\mathfrak{n}_2}$, and let $\mathfrak{p} \subset B$ and $\mathfrak{q} \subset A$ be its contractions. Then $\mathfrak{p}$ can contain no element outside of either $\mathfrak{n}_1$ or $\mathfrak{n}_2$; so $\mathfrak{p}$ lies in both $\mathfrak{n}_1$ and $\mathfrak{n}_2$.

Plainly $B/\mathfrak{p}$ is an integral extension of $A/\mathfrak{q}$. And both $\mathfrak{n}_i/\mathfrak{p}$ lie over the unique maximal ideal of $A/\mathfrak{q}$ by **(14.3)**(1). Also, $B/\mathfrak{p}$ is a domain. But both $B_{\mathfrak{n}_i}$ are integral over A, and $B_{\mathfrak{n}_i}/\mathfrak{p}B_{\mathfrak{n}_i} = (B/\mathfrak{p})_{\mathfrak{n}_i}$ by **(12.15)**; hence, both $(B/\mathfrak{p})_{\mathfrak{n}_i}$ are integral over $A/\mathfrak{q}$. So $\mathfrak{n}_1/\mathfrak{p} = \mathfrak{n}_2/\mathfrak{p}$ by **(14.16)**. Thus $\mathfrak{n}_1 = \mathfrak{n}_2$, as desired. □

Exercise (22.94) . — Let A be a local ring, and $\mathfrak{a}$ an ideal. Assume $\mathfrak{a} \subset \mathrm{nil}(A)$. Set $A' := A/\mathfrak{a}$. Show that A is Henselian if and only if A' is so.

Solution: If A is Henselian, then A' is Henselian owing to **(22.73)**.

Conversely, assume A' is Henselian. Let B be a module-finite A-algebra. Set $B' := B/\mathfrak{a}B$. Then B' is a module-finite A'-algebra. So B' is decomposable by **(22.78)**(1)⇒(3). But $\mathfrak{a}B \subset \mathrm{nil}(B)$. So B is decomposable by **(13.23)**(2)⇒(1) or by **(19.30)**. Thus A is Henselian by **(22.78)**(3)⇒(1). □

Exercise (22.95) . — Let A be a local ring. Assume A is separated and complete. Use **(22.78)**(4)⇒(1) to give a second proof (compare **(22.75)**) that A is Henselian.

Solution: Let $\mathfrak{m}$ be the maximal ideal of A, and B a module-finite A-algebra with an isomorphism $\alpha\colon B \xrightarrow{\sim} A^r$. Give B the $\mathfrak{m}$-adic topology. Then $\widehat{\alpha}\kappa_B = \kappa_{A^r}\alpha$ by **(22.54)**(1). Plainly $\kappa_{A^r} = \kappa_A^r$. But κ_A is an isomorphism by **(22.14)**(2)⇒(3). Thus κ_B is an isomorphism; put otherwise, $B = \widehat{B}$.

Moreover, **(19.15)**(1) implies B has finitely many maximal ideals $\mathfrak{n}_i$ and they're precisely the primes lying over $\mathfrak{m}$.

For $n \ge 1$, let $\kappa_n\colon B/\mathfrak{m}^nB \to B/\mathfrak{m}B$ be the quotient map. Then $\mathrm{Idem}(\kappa_n)$ is bijective by **(3.36)**, as $\mathfrak{m}B/\mathfrak{m}^nB \subset \mathrm{nil}(B/\mathfrak{m}^nB)$. So $B/\mathfrak{m}^nB$ is decomposable by **(19.15)**(3). Hence $B/\mathfrak{m}^nB = \prod(B/\mathfrak{m}^nB)_{\mathfrak{n}_i}$ by **(11.18)**. Thus **(12.15)** yields $B/\mathfrak{m}^nB = \prod B_{\mathfrak{n}_i}/\mathfrak{m}^nB_{\mathfrak{n}_i}$.

Set $B_i := \varprojlim B_{\mathfrak{n}_i}/\mathfrak{m}^nB_{\mathfrak{n}_i}$. Then B_i is the $\mathfrak{m}$-adic completion of $B_{\mathfrak{n}_i}$ by **(22.7)**. Also $\varprojlim B/\mathfrak{m}^nB = \widehat{B}$, but $B = \widehat{B}$ by the above. Thus $B = \prod B_i$. But B_i is local by**(22.53)**(7). So B is decomposable. Thus A is Henselian by **(22.78)**(4)⇒(1). □

Exercise (22.96) . — Let R be a ring, $\mathfrak{a}$ an ideal, $u \in R^\times$, and $n \ge 2$. Assume R is separated and complete, and $u \equiv 1 \pmod{n^2\mathfrak{a}}$. Find an nth root of u.

Solution: Set $F(X) := X^n - u$. Then $F(1) = 1 - u \equiv 1 \pmod{n^2\mathfrak{a}}$, and $(\partial F/\partial X)(1) = n$. Hence **(22.82)** yields a root $a \in R$ of F. Thus $a^n = u$. □

Exercise (22.97) . — Let p, $a_1, \ldots, a_s$, k be integers, and $X_1, \ldots, X_s$ variables. Set $F := a_1X_1^k + \cdots + a_sX_s^k$. Assume p prime, each a_i and k prime to p, and $s > k > 0$. Using **(2.46)**, show F has a nontrivial zero in $\widehat{\mathbb{Z}}_p^s$.

Solution: Note $F(0, \ldots, 0) = 0$. So **(2.46)** yields $b_i \in \mathbb{Z}$ with $F(b_1, \ldots, b_s) \equiv 0 \pmod{p}$, but $b_j \not\equiv 0 \pmod{p}$ for some j. Set $G(X) := F(b_1, \ldots, X, \ldots, b_s)$ with X in the jth position. Then $G(b_j) \equiv 0 \pmod{p}$ and $(\partial G/\partial X_j)(G(b_j) = kb_j^{k-1} \not\equiv 0 \pmod{p}$. So G has a root in $\widehat{\mathbb{Z}}_p$ by **(22.76)**. Thus F has a nontrivial zero in $\widehat{\mathbb{Z}}_p^s$. □

Exercise (22.98) . — Find a cube root of 2 in $\widehat{\mathbb{Z}}_5$.

Solution: Set $F := X^3 - 2 \in \mathbb{Z}[X]$ and $F' := \partial F/\partial X$. Then $F(3) = 25 \equiv 0 \pmod{5}$ and $F'(3) = 27 \equiv 2 \pmod{5}$. So **(22.76)** yields a root in $\widehat{\mathbb{Z}}_{\langle 5\rangle}$. □

Exercise (22.99) . — Find a cube root of 10 in $\widehat{\mathbb{Z}}_3$.

Solution: Set $F := X^3 - 10 \in \mathbb{Z}[X]$ and $F' := \partial F/\partial X$. Then $F(1) = -9$ and $F'(1) = 3$. So $F(1) \equiv 0 \pmod{3}$. But $F'(1) \equiv 0 \pmod{3}$ and $F(1) \notin 9\langle 3\rangle$; so both **(22.76)** and **(22.82)** appear to fail to provide a root. However, $F(4) = 54 \equiv 0 \pmod{3}$. Moreover, $F'(4) = 48$; so $F(4) \in (F'(4))^2\langle 3\rangle$. Thus after all, **(22.82)** does yield a root of F, so a cube root of 10. □

Exercise (22.100) . — In the setup of **(22.84)**, if $n \ge 1$, find an alternative proof for the existence of Q and P as follows: take a variable Y; view $R[[X]]$ as an $R[[Y]]$-algebra via the map φ with $\varphi(Y) := F$: and show $1, X, \ldots, X^{n-1}$ generate $R[[X]]$ as a module by using Nakayama's Lemma for adically complete rings **(22.69)**.

Solution: Give $R[[X]]$ the $\langle\mathfrak{a},\, X\rangle$-adic topology. Then $R[[X]]$ is separated and complete by **(22.44)**(4). But $F \in \langle\mathfrak{a},\, X\rangle$. So **(22.55)** yields an R-algebra map $\varphi\colon R[[Y]] \to R[[X]]$ with $\varphi(Y) = F$. Via φ, view $R[[X]]$ as an $R[[Y]]$-algebra.

Give $R[[Y]]$ the $\langle\mathfrak{a},\, Y\rangle$-adic topology. Then $R[[Y]]$ is complete by **(22.44)**(4). As $\varphi(Y) = F$, the topology induced on $R[[X]]$ is the $\langle\mathfrak{a},\, F\rangle$-adic. But $\langle\mathfrak{a},\, F\rangle \subset \langle\mathfrak{a},\, X\rangle$. Since the $\langle\mathfrak{a},\, X\rangle$-adic topology is separated, so is the $\langle\mathfrak{a},\, F\rangle$-adic.

Note $R[[X]]/\mathfrak{a}R[[X]] = (R/\mathfrak{a})[[X]]$ by **(22.56)**. Denote the residue of F by $\overline{F}$. Then $\overline{F} = X^n U$ with U a unit in $(R/\mathfrak{a})[[X]]$ by **(3.7)**. Hence

$$R[[X]]/\langle\mathfrak{a},\, F\rangle = (R/\mathfrak{a})[[X]]/\langle\overline{F}\rangle = (R/\mathfrak{a})[[X]]/\langle X^n\rangle.$$

Thus $1, X, \ldots, X^{n-1}$ generate $R[[X]]/\langle\mathfrak{a},\, F\rangle$ over $R[[Y]]$.

So $1, X, \ldots, X^{n-1}$ generate $R[[X]]$ over $R[[Y]]$ owing to **(22.69)**. So there are $G_i \in R[[Y]]$ such that $G = \sum_{i=0}^{n-1} \varphi(G_i)X^i$. Say $G_i = g_i + H_i(Y)Y$ with $g_i \in R$ and $H_i \in R[[Y]]$. Set $P := \sum g_i X^i$ and $Q := \sum \varphi(H_i)X^i$. Thus $G = QF + P$. □

23. Discrete Valuation Rings

Exercise (23.7) . — Let R be a normal Noetherian domain, $x \in R$ a nonzero nonunit, $\mathfrak{a}$ an ideal. Show that every $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ has height 1. Conversely, if R is a UFD and if every $\mathfrak{p} \in \operatorname{Ass}(R/\mathfrak{a})$ has height 1, show $\mathfrak{a}$ is principal.

Solution: Given $\mathfrak{p} \in \operatorname{Ass}(R/xR)$, note $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}(R_{\mathfrak{p}}/xR_{\mathfrak{p}})$ by **(17.8)**. Hence $\operatorname{depth}(R_{\mathfrak{p}}) = 1$ by **(23.5)**(2). But $R_{\mathfrak{p}}$ is normal by **(11.32)**. Hence $\dim(R_{\mathfrak{p}}) = 1$ by **(23.6)**(3)⇒(4). Thus **(21.6.1)** yields $\operatorname{ht}(\mathfrak{p}) = 1$, as desired.

Conversely, assume that R is a UFD and that all the primes $\mathfrak{p}_i$ of $\mathfrak{a}$ have height 1. Then $\mathfrak{p}_i = \langle p_i\rangle$ for some prime element $p_i \in R$ by **(21.33)** as R is a UFD. The corresponding primary ideal of $\mathfrak{a}$ is $\mathfrak{p}_i^{n_i}$ for some n_i by **(18.7)**. Thus $\mathfrak{a} = \bigcap\langle p_i^{n_i}\rangle$.

Finally, set $y := \prod p_i^{n_i}$. Then $\langle y\rangle \subset \bigcap\langle p_i^{n_i}\rangle$. Conversely, if all $p_i^{n_i}$ divide some z, then y divides z too, as the p_i are distinct prime elements in R, a UFD. Hence the opposite inclusion holds. Thus $\langle y\rangle = \bigcap\langle p_i^{n_i}\rangle = \mathfrak{a}$, as desired. □

Exercise (23.9) . — Let A be a DVR with fraction field K, and $f \in A$ a nonzero nonunit. Prove A is a maximal proper subring of K. Prove $\dim(A) \neq \dim(A_f)$.

Solution: Let R be a ring, $A \subsetneqq R \subset K$. Then there's an $x \in R - A$. Say $x = ut^n$ where $u \in A^{\times}$ and t is a uniformizing parameter. Then $n < 0$. Set $y := u^{-1}t^{-n-1}$. Then $y \in A$. So $t^{-1} = xy \in R$. Hence $wt^m \in R$ for any $w \in A^{\times}$ and $m \in \mathbb{Z}$. Thus $R = K$, as desired.

Since f is a nonzero nonunit, $A \subsetneqq A_f \subset K$. Hence $A_f = K$ by the above. Thus $\dim(A_f) = 0$. But $\dim(A) = 1$ by **(23.6)**, as desired. □

Exercise (23.11) . — Let R be a domain, M a Noetherian module. Show that M is torsionfree if and only if it satisfies (S_1).

Solution: Assume M satisfies (S_1). By **(23.10)**, the only prime in $\operatorname{Ass}(M)$ is $\langle 0\rangle$. Hence $\operatorname{z.div}(M) = \{0\}$ by **(17.12)**. Thus M is torsionfree.

Conversely, assume M is torsionfree. Suppose $\mathfrak{p} \in \operatorname{Ass}(M)$. Then $\mathfrak{p} = \operatorname{Ann}(m)$ for some $m \in M$. But $\operatorname{Ann}(m) = \langle 0\rangle$ for all $m \in M$. So $\mathfrak{p} = \langle 0\rangle$ is the only associated prime. Thus M satisfies (S_1) by **(23.10)**. □

Exercise (23.12) . — Let R be a Noetherian ring. Show that R is reduced if and only if (R_0) and (S_1) hold.

Solution: Assume (R_0) and (S_1) hold. Consider any irredundant primary decomposition $\langle 0\rangle = \bigcap \mathfrak{q}_i$. Set $\mathfrak{p}_i := \sqrt{\mathfrak{q}_i}$. Then $\mathfrak{p}_i \in \operatorname{Ass}(R)$ by **(18.3)**(5) and **(18.18)**. So $\mathfrak{p}_i$ is minimal by (S_1). Hence the localization $R_{\mathfrak{p}_i}$ is a field by (R_0). So $\mathfrak{p}_i R_{\mathfrak{p}_i} = 0$. But $\mathfrak{p}_i R_{\mathfrak{p}_i} \supset \mathfrak{q}_i R_{\mathfrak{p}_i}$. Hence $\mathfrak{p}_i R_{\mathfrak{p}_i} = \mathfrak{q}_i R_{\mathfrak{p}_i}$. Therefore, $\mathfrak{p}_i = \mathfrak{q}_i$ by **(18.20)**. So $\langle 0\rangle = \bigcap \mathfrak{p}_i = \sqrt{\langle 0\rangle}$. Thus R is reduced.

Conversely, assume R is reduced. Then $R_{\mathfrak{p}}$ is reduced for any prime $\mathfrak{p}$ by **(13.57)**. So if $\mathfrak{p}$ is minimal, then $R_{\mathfrak{p}}$ is a field. Thus (R_0) holds. But $\langle 0\rangle = \bigcap_{\mathfrak{p}\ \text{minimal}} \mathfrak{p}$. So $\mathfrak{p}$ is minimal whenever $\mathfrak{p} \in \operatorname{Ass}(R)$ by **(18.18)**. Thus R satisfies (S_1). □

Exercise (23.16) . — Show an equicharacteristic regular local ring A is a UFD.

Solution: First, $\widehat{A}$ too is a regular local ring by **(22.62)**. And $\widehat{A}$ is faithfully flat by **(22.36)**(1)⇒(7). Thus by **(23.8)**, it suffices to show $\widehat{A}$ is a UFD.

By **(22.16)**(4), $\widehat{A}$ is separated and complete. But $\widehat{A}$ is equicharacteristic. Hence, $\widehat{A}$ contains a coefficient field, say k, by **(22.81)**. So $\widehat{A} \cong k[[X_1, \dots, X_r]]$ where $r := \dim(\widehat{A})$ by **(22.58)**. Thus $\widehat{A}$ is a UFD by **(22.88)**, as desired. □

Exercise (23.17) . — Let R be a ring, $0 \to N \to M \to L \to 0$ a short exact sequence, and $x_1, \dots, x_n \in R$. Set $\mathfrak{a}_i : \langle x_1, \dots, x_i\rangle$ for $0 \le i \le n$. Prove:

(1) Assume $x_1, \dots, x_n$ is L-regular. Then $\mathfrak{a}_i M \cap N = \mathfrak{a}_i N$ for $0 \le i \le n$.

(2) Then $x_1, \dots, x_n$ is both N-regular and L-regular if and only if $x_1, \dots, x_n$ is M-regular, $\mathfrak{a}_i M \cap N = \mathfrak{a}_i N$ for $0 \le i \le n$, and $N/\mathfrak{a}_n N \ne 0$ and $L/\mathfrak{a}_n L \ne 0$.

Solution: First, for all i, set $N_i := N/\mathfrak{a}_i N$ and $M_i := M/\mathfrak{a}_i M$ and $L_i := L/\mathfrak{a}_i L$. Then there's a canonical sequence $N_i \xrightarrow{\alpha_i} M_i \xrightarrow{\beta_i} L_i \to 0$. It's exact, because plainly, β_i is surjective, and $\operatorname{Ker}\beta_i = (N + \mathfrak{a}_i M)/\mathfrak{a}_i M = \operatorname{Im}\alpha_i$. Plainly, α_i is injective if and only if $\mathfrak{a}_i M \cap N = \mathfrak{a}_i N$.

If α_i is injective, then for $0 \le i < n$ this commutative diagram has exact rows:

$$\begin{array}{ccccccccc} 0 & \to & N_i & \xrightarrow{\alpha_i} & M_i & \to & L_i & \to & 0 \\ & & {\scriptstyle \mu_{x_{i+1}}}\downarrow & & {\scriptstyle \mu_{x_{i+1}}}\downarrow & & {\scriptstyle \mu_{x_{i+1}}}\downarrow & & \\ 0 & \to & N_i & \xrightarrow{\alpha_i} & M_i & \to & L_i & \to & 0 \end{array}$$

The three vertical cokernels are N_{i+1}, M_{i+1}, L_{i+1} by **(23.4.1)**. Denote the three kernels by A_i, B_i, C_i. If α_i is injective, then **(5.10)** yields this exact sequence:

$$0 \to A_i \to B_i \to C_i \to N_{i+1} \xrightarrow{\alpha_{i+1}} M_{i+1} \to L_{i+1} \to 0 \qquad \textbf{(23.17.1)}$$

For (1), induct on i. If $i = 0$, then (1) is trivial, since $\mathfrak{a}_0 = \langle 0\rangle$. Given i with $0 \le i < n$, assume $\mathfrak{a}_i M \cap N = \mathfrak{a}_i N$. Then **(23.17.1)** is exact. But $x_1, \dots, x_n$ is L-regular. So $C_i = 0$. So α_{i+1} is injective. Thus $\mathfrak{a}_{i+1} M \cap N = \mathfrak{a}_{i+1} N$, as desired.

For (2), first assume $x_1, \dots, x_n$ is L-regular. Then $C_i = 0$ for $0 \le i < n$. Further, (1) yields $\mathfrak{a}_i M \cap N = \mathfrak{a}_i N$ for $0 \le i \le n$. Hence **(23.17.1)** is exact for $0 \le i < n$. Assume $x_1, \dots, x_n$ is N-regular too. Then $A_i = 0$ for $0 \le i < n$. Hence $B_i = 0$ for $0 \le i < n$. Further, $N_n \ne 0$ and $L_n \ne 0$ as $x_1, \dots, x_n$ is both N-regular and L-regular. So $M_n \ne 0$. Thus $x_1, \dots, x_n$ is M-regular.

Conversely, assume $\mathfrak{a}_i M \cap N = \mathfrak{a}_i N$ for $0 \le i \le n$. Then α_i is injective for $0 \le i \le n$. So **(23.17.1)** is exact for $0 \le i < n$. Assume $x_1, \dots, x_n$ is M-regular too. Then $B_i = 0$ for $0 \le i < n$. Hence A_i and $C_i = 0$ for $0 \le i \le n$. Assume $N/\mathfrak{a}_n N \ne 0$ and $L/\mathfrak{a}_n L \ne 0$ too. Then $x_1, \ldots, x_n$ is both N-regular and L-regular. Thus (2) holds. □

Exercise (23.18) . — Let R be a ring, M a module, $F\colon ((R\text{-mod})) \to ((R\text{-mod}))$ a left-exact functor. Assume $F(M)$ is nonzero and finitely generated. Show that, for $d = 1, 2$, if M has depth at least d, then so does $F(M)$.

Solution: As F is linear, $\operatorname{Ann}(M) \subset \operatorname{Ann}(F(M))$. Thus $\operatorname{rad}(M) \subset \operatorname{rad}(F(M))$.

Assume $\operatorname{depth}(M) \ge 1$. Then there's $x \in \operatorname{rad}(M)$ with $M \xrightarrow{\mu_x} M$ injective. So $x \in \operatorname{rad}(F(M))$. Also, as F is left exact, $F(M) \xrightarrow{\mu_x} F(M)$ is injective too. Thus $\operatorname{depth}(F(M)) \ge 1$.

Assume $\operatorname{depth}(M) \ge 2$. So there's an M-sequence $x, y \in \operatorname{rad}(M) \subset \operatorname{rad}(F(M))$. Notice x, y yield the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \to & M & \xrightarrow{\mu_x} & M & \to & M/xM \\ & & \Big\downarrow{\scriptstyle\mu_y} & & \Big\downarrow{\scriptstyle\mu_y} & & \Big\downarrow{\scriptstyle\mu_y} \\ 0 & \to & M & \xrightarrow{\mu_x} & M & \to & M/xM \end{array}$$

Applying the left-exact functor F yields this commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \to & F(M) & \xrightarrow{\mu_x} & F(M) & \to & F(M/xM) \\ & & \Big\downarrow{\scriptstyle\mu_y} & & \Big\downarrow{\scriptstyle\mu_y} & & \Big\downarrow{\scriptstyle\mu_y} \\ 0 & \to & F(M) & \xrightarrow{\mu_x} & F(M) & \to & F(M/xM) \end{array}$$

Thus again x is a nonzerodivisor on $F(M)$. Further $F(M)/xF(M) \hookrightarrow F(M/xM)$.

As $M/xM \xrightarrow{\mu_y} M/xM$ is injective and F is left exact, the right-hand vertical map μ_y is injective. So its restriction

$$F(M)/xF(M) \xrightarrow{\mu_y} F(M)/xF(M)$$

is also injective. Thus x, y is an $F(M)$-sequence. Thus $\operatorname{depth}(F(M)) \ge 2$. □

Exercise (23.19) . — Let k be a field, A a ring intermediate between the polynomial ring and the formal power series ring in one variable: $k[X] \subset A \subset k[[X]]$. Suppose that A is local with maximal ideal $\langle X \rangle$. Prove that A is a DVR. (Such local rings arise as rings of power series with curious convergence conditions.)

Solution: Let's show that the ideal $\mathfrak{a} := \bigcap_{n \ge 0} \langle X^n \rangle$ of A is zero. Clearly, $\mathfrak{a}$ is a subset of the corresponding ideal $\bigcap_{n \ge 0} \langle X^n \rangle$ of $k[[X]]$, and the latter ideal is clearly zero. Hence (23.3) implies A is a DVR. □

Exercise (23.20) . — Let L/K be an algebraic extension of fields; $X_1, \ldots, X_n$ variables; P and Q the polynomial rings over K and L in $X_1, \ldots, X_n$. Prove this:

(1) Let $\mathfrak{q}$ be a prime of Q, and $\mathfrak{p}$ its contraction in P. Then $\operatorname{ht}(\mathfrak{p}) = \operatorname{ht}(\mathfrak{q})$.
(2) Let $F, G \in P$ be two polynomials with no common prime factor in P. Then F and G have no common prime factor $H \in Q$.

Solution: In (1), $Q = L \otimes_K P$ by (8.18). But L/K is algebraic. So Q/P is integral by (10.39)(1). Further, P is normal by (10.22)(1), and Q is a domain.

Hence we may apply the Going-down Theorem (14.6): given any chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r = \mathfrak{p}$, proceed by descending induction on i for $0 \le i \le r$, and thus construct a chain of primes $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r = \mathfrak{q}$ with $\mathfrak{q}_i \cap P = \mathfrak{p}_i$. Thus $\operatorname{ht}\mathfrak{p} \le \operatorname{ht}\mathfrak{q}$.

Conversely, any chain of primes $\mathfrak{q}_0 \subsetneqq \cdots \subsetneqq \mathfrak{q}_r = \mathfrak{q}$ contracts to a chain of primes $\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_r = \mathfrak{p}$, and $\mathfrak{p}_i \ne \mathfrak{p}_{i+1}$ by Incomparability, **(14.3)**(2); so $\operatorname{ht}\mathfrak{p} \ge \operatorname{ht}\mathfrak{q}$. Hence $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{q}$. Thus (1) holds.

Alternatively, by **(15.12)**, $\operatorname{ht}(\mathfrak{p}) + \dim(P/\mathfrak{p}) = n$ and $\operatorname{ht}(\mathfrak{q}) + \dim(Q/\mathfrak{q}) = n$ as both P and Q are polynomial rings in n variables over a field. But, by **(15.10)**, $\dim P/\mathfrak{p} = \operatorname{tr.deg}_K \operatorname{Frac}(P/\mathfrak{p})$ and $\dim Q/\mathfrak{q} = \operatorname{tr.deg}_L \operatorname{Frac}(Q/\mathfrak{q})$, and these two transcendence degrees are equal as Q/P is integral. Thus again, (1) holds.

For (2), assume F, G have a common prime factor $H \in Q$. Set $\mathfrak{q} := QH$. Then $\mathfrak{q}Q_{\mathfrak{q}}$ is principal and nonzero. Hence $Q_{\mathfrak{q}}$ is a DVR by **(23.6)**. Thus $\operatorname{ht}(\mathfrak{q}) = 1$.

Set $\mathfrak{p} := \mathfrak{q} \cap P$. Then $\mathfrak{p}$ contains F; whence, $\mathfrak{p}$ contains some prime factor H' of F. Then $\mathfrak{p} \supseteq PH'$, and PH' is a nonzero prime. Hence $\mathfrak{p} = PH'$ since $\operatorname{ht}\mathfrak{p} = 1$ by (1). However, $\mathfrak{p}$ contains G too. Therefore, $H' \mid G$, contrary to the hypothesis. Thus (2) holds. (Caution: if $F := X_1$ and $G := X_2$, then F and G have no common factor, yet there are no φ and ψ such that $\varphi F + \psi G = 1$.) □

Exercise (23.21) . — Prove that a Noetherian domain R is normal if and only if, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_{\mathfrak{p}}$ is principal.

Solution: Assume R normal. Say $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$. Then $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}((R/\langle x\rangle)_{\mathfrak{p}})$ by **(17.8)**. But $R/\langle x\rangle)_{\mathfrak{p}} = R_{\mathfrak{p}}/\langle x/1\rangle)$ by **(12.15)**. So $\operatorname{depth}(R_{\mathfrak{p}}) = 1$ by **(23.5)**(2). But $R_{\mathfrak{p}}$ is normal by **(11.32)**. Hence $\mathfrak{p}R_{\mathfrak{p}}$ is principal by **(23.6)**.

Conversely, assume that, given any prime $\mathfrak{p}$ associated to a principal ideal, $\mathfrak{p}R_{\mathfrak{p}}$ is principal. Given any prime $\mathfrak{p}$ of height 1, take a nonzero $x \in \mathfrak{p}$. Then $\mathfrak{p}$ is minimal containing $\langle x\rangle$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ by **(17.14)**. So, by hypothesis, $\mathfrak{p}R_{\mathfrak{p}}$ is principal. So $R_{\mathfrak{p}}$ is a DVR by **(23.6)**. Thus R satisfies (R_1).

Given any prime $\mathfrak{p}$ with $\operatorname{depth}(R_{\mathfrak{p}}) = 1$, say $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}(R_{\mathfrak{p}}/\langle x/s\rangle)$ with $x \ne 0$ by **(23.5)**(2). Then $\langle x/s\rangle = \langle x/1\rangle \subset R_{\mathfrak{p}}$. So $\mathfrak{p} \in \operatorname{Ass}(R/\langle x\rangle)$ by **(17.8)** and **(12.15)**. So, by hypothesis, $\mathfrak{p}R_{\mathfrak{p}}$ is principal. So $\dim(R_{\mathfrak{p}}) = 1$ by **(23.6)**. Thus R also satisfies (S_2). So R is normal by Serre's Criterion, **(23.15)**. □

Exercise (23.22) . — Let R be a ring, M a nonzero Noetherian module. Set

$$\Phi := \{\,\mathfrak{p} \text{ prime} \mid \dim(M_{\mathfrak{p}}) = 1\,\} \quad\text{and}\quad \Sigma := \{\,\mathfrak{p} \text{ prime} \mid \operatorname{depth}(M_{\mathfrak{p}}) = 1\,\}.$$

Assume M satisfies (S_1). Show $\Phi \subset \Sigma$, with equality if and only if M satisfies (S_2).

Set $S := R - \operatorname{z.div}(M)$. Without assuming (S_1), show this sequence is exact:

$$M \to S^{-1}M \to \textstyle\prod_{\mathfrak{p}\in\Sigma} S^{-1}M_{\mathfrak{p}}/M_{\mathfrak{p}}. \tag{23.22.1}$$

Solution: Assume (S_1). Then, given $\mathfrak{p} \in \Phi$, note $\mathfrak{p} \notin \operatorname{Ass}(M)$ by **(23.10)**. So **(17.12)** yields a nonzerodivisor $x \in \mathfrak{p}$. Plainly, $\mathfrak{p}$ is minimal containing $\langle x\rangle$. So $\mathfrak{p}$ is minimal in $\operatorname{Supp}(M/xM)$ by **(13.46)**(2). So $\mathfrak{p} \in \operatorname{Ass}(M/xM)$ by **(17.14)**. So $\mathfrak{p}R_{\mathfrak{p}} \in \operatorname{Ass}((M/xM)_{\mathfrak{p}})$ by **(17.8)**. But $(M/xM)_{\mathfrak{p}} = M_{\mathfrak{p}}/xM_{\mathfrak{p}}$ by **(12.15)**. Hence $\operatorname{depth}(M_{\mathfrak{p}}) = 1$ by **(23.5)**(2). Thus $\Phi \subset \Sigma$.

However, as (S_1) holds, (S_2) holds if and only if $\Phi \supset \Sigma$. Thus $\Phi = \Sigma$ if and only if M satisfies (S_2).

Finally without assuming (S_1), consider**(23.22.1)**. Trivially the composition is equal to 0. Conversely, given $m \in S^{-1}M$ vanishing in $\prod S^{-1}M_{\mathfrak{p}}/M_{\mathfrak{p}}$, say $m = n/s$ with $n \in M$ and $s \in S$. Then $n/1 \in sM_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Sigma$. But $s/1 \in R_{\mathfrak{p}}$ is, plainly, a nonzerodivisor on $M_{\mathfrak{p}}$ for every prime $\mathfrak{p}$; so if $\mathfrak{p} \in \operatorname{Ass}(M_{\mathfrak{p}}/sM_{\mathfrak{p}})$, then $\mathfrak{p} \in \Sigma$ by **(23.5)**(2). Hence $n \in sM$ by **(18.65)**)2). So $m \in M$. Thus **(23.22.1)** is exact. □

Exercise (23.23) (*Serre's Criterion*) . — Let R be a Noetherian ring, and K its total quotient ring. Set $\Phi := \{\, \mathfrak{p} \text{ prime} \mid \mathrm{ht}(\mathfrak{p}) = 1 \,\}$. Prove equivalent:

(1) R is normal.
(2) (R_1) and (S_2) hold.
(3) (R_1) and (S_1) hold, and $R \to K \to \prod_{\mathfrak{p}\in\Phi} K_{\mathfrak{p}}/R_{\mathfrak{p}}$ is exact.

Solution: Assume (1). Then R is reduced by **(14.25)**. So **(23.12)** yields (R_0) and (S_1). But $R_{\mathfrak{p}}$ is normal for any prime $\mathfrak{p}$ by **(14.9)**. Thus (2) holds by **(23.6)**.

Assume (2). Then (R_1) and (S_1) hold trivially. Thus **(23.22)** yields (3).

Assume (3). Let $x \in K$ be integral over R. Then $x/1 \in K$ is integral over $R_{\mathfrak{p}}$ for any prime $\mathfrak{p}$. Now, $R_{\mathfrak{p}}$ is a DVR for all $\mathfrak{p}$ of height 1 as R satisfies (R_1). Hence, $x/1 \in R_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Phi$. So $x \in R$ by the exactness of the sequence in (3). But R is reduced by **(23.12)**. Thus **(14.25)** yields (1). □

23. Appendix: M-sequences

Exercise (23.24) . — Let R be a ring, M a module, and x, y an M-sequence.

(1) Given $m, n \in M$ with $xm = yn$, find $p \in M$ with $m = yp$ and $n = xp$.
(2) Assume $y \notin \mathrm{z.div}(M)$. Show y, x is an M-sequence too.

Solution: For (1), let n_1 be the residue of n in $M_1 := M/xM$. Then $yn_1 = 0$, but $y \notin \mathrm{z.div}(M_1)$. Hence $n_1 = 0$. So there's $p \in M$ with $n = xp$. So $x(m - yp) = 0$. But $x \notin \mathrm{z.div}(M)$. Thus $m = yp$.

For (2), note $M/\langle y, x\rangle M \neq 0$ as x, y is an M-sequence. Set $M_1 := M/yM$. Given $m_1 \in M_1$ with $xm_1 = 0$, lift m_1 to $m \in M$. Then $xm = yn$ for some $n \in M$. By (1), there's $p \in M$ with $m = yp$. Thus $m_1 = 0$. Thus $x \notin \mathrm{z.div}(M_1)$. □

Exercise (23.26) . — Let R be a ring, $\mathfrak{a} \subset R$ an ideal, M a module, $x_1, \ldots, x_r$ an M-sequence in $\mathfrak{a}$, and R' an algebra. Set $M' := M \otimes_R R'$. Assume R' flat and $M'/\mathfrak{a}M' \neq 0$. Prove $x_1, \ldots, x_r$ is an M'-sequence in $\mathfrak{a}R'$.

Solution: For all i, set $M_i := M/\langle x_1, \ldots, x_i\rangle M$ and $M'_i := M'/\langle x_1, \ldots, x_i\rangle M'$. Then $M'_i = M_i \otimes_R R'$ by right exactness of tensor product **(8.10)**. Moreover, by hypothesis, x_{i+1} is a nonzerodivisor on M_i. Thus the multiplication map $\mu_{x_{i+1}} \colon M_i \to M_i$ is injective. Hence $\mu_{x_{i+1}} \colon M'_i \to M'_i$ is injective by flatness. Finally $\langle x_1, \ldots, x_r\rangle \subset \mathfrak{a}$, so $M'_r \neq 0$. Thus the assertion holds. □

Exercise (23.27) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module with $M/\mathfrak{a}M \neq 0$. Let $x_1, \ldots, x_r$ be an M-sequence in $\mathfrak{a}$, and $\mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)$. Prove: (1) $x_1/1, \ldots, x_r/1$ is an $M_{\mathfrak{p}}$-sequence in $\mathfrak{a}_{\mathfrak{p}}$, and (2) $\mathrm{depth}(\mathfrak{a}, M) \le \mathrm{depth}(\mathfrak{a}_{\mathfrak{p}}, M_{\mathfrak{p}})$.

Solution: First, $(M/\mathfrak{a}M)_{\mathfrak{p}} \neq 0$ as $\mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)$. Thus **(12.15)** yields $M_{\mathfrak{p}}/\mathfrak{a}M_{\mathfrak{p}} \neq 0$. Second, $R_{\mathfrak{p}}$ is R-flat by **(12.14)**. Thus **(23.26)** yields (1). Thus the definition of depth in **(23.4)** first yields $r \le \mathrm{depth}(\mathfrak{a}_{\mathfrak{p}}, M_{\mathfrak{p}})$, and then yields (2). □

Exercise (23.31) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a Noetherian module with $M/\mathfrak{a}M \neq 0$, and $x \in \mathfrak{a} - \mathrm{z.div}(M)$. Show $\mathrm{depth}(\mathfrak{a}, M/xM) = \mathrm{depth}(\mathfrak{a}, M) - 1$.

Solution: Set $r := \mathrm{depth}(\mathfrak{a}, M/xM)$. Then there's a maximal M/xM-sequence $x_2, \ldots, x_r$ in $\mathfrak{a}$ by **(23.29)**. Plainly $x, x_2, \ldots, x_r$ is a maximal M-sequence in $\mathfrak{a}$. Thus $\mathrm{depth}(\mathfrak{a}, M) = r + 1$. □

Exercise (23.32) . — Let R be a ring, M a nonzero Noetherian semilocal module, and $x \in \mathrm{rad}(M) - \mathrm{z.div}(M)$. Show that $\mathrm{depth}(M) = \dim(M)$ if and only if $\mathrm{depth}(M/xM) = \dim(M/xM)$.

Solution: Note $\mathrm{rad}(M/xM) = \mathrm{rad}(M)$ by **(23.4.2)**. So M/xM is semilocal. Also **(23.31)** yields $\mathrm{depth}(M/xM) = \mathrm{depth}(M) - 1$. Moreover, **(21.5)** yields $\dim(M/xM) = \dim(M) - 1$. Thus the assertion holds. □

Exercise (23.33) . — Let R be a ring, R' an algebra, and N a nonzero R'-module that's a Noetherian R-module. Assume N is semilocal over R (or equivalently by **(21.20)**(5), semilocal over R'). Show $\mathrm{depth}_R(N) = \mathrm{depth}_{R'}(N)$.

Solution: Set $r := \mathrm{depth}_R(N)$. By **(23.29)**, there is a maximal N-sequence $x_1, \dots, x_r$ in $\mathrm{rad}_R(N)$. Its image in R' lies in $\mathrm{rad}_{R'}(N)$ by **(21.20)**(4), and is plainly N-regular. Set $N_r := N/\langle x_1, \dots, x_r\rangle N$. Then $\mathrm{depth}_{R'}(N_r) = \mathrm{depth}_{R'}(N) - r$ and $\mathrm{depth}_R(N_r) = 0$ by **(23.31)**. Thus we have to prove $\mathrm{depth}_{R'}(N_r) = 0$.

By **(23.5)**(1), there's a maximal ideal $\mathfrak{m} \in \mathrm{Ass}_R(N_r)$. Say $\mathfrak{m} = \mathrm{Ann}_R(n)$ where $n \in N_r$. Set $R'_1 := R'/\mathrm{Ann}_{R'}(N_r)$. Then R'_1 is Noetherian by **(16.16)**. Let $\mathcal{S}$ be the set of annihilators in R'_1 of nonzero elements of N_r. Let $\mathcal{T}$ be the subset of annihilators that contain $\mathrm{Ann}_{R'_1}(n)$. Then $\mathcal{T}$ has a maximal element, $\mathfrak{M}_1$ say. Then $\mathfrak{M}_1 \in \mathrm{Ass}_{R'_1}(N_r)$ by **(17.9)**. Let $\mathfrak{n}$ be the preimage in R' of $\mathfrak{M}_1$.

Then $\mathfrak{n} \in \mathrm{Ass}_{R'}(N_r)$ by **(17.4)**. Let $\mathfrak{m}'$ be the contraction of $\mathfrak{n}$ in R. Then $\mathfrak{m}' \supset \mathfrak{m}$. But $\mathfrak{m}$ is maximal. So $\mathfrak{m}' = \mathfrak{m}$. So $\mathfrak{n}$ is maximal by **(17.13)** and **(21.20)**(2). Thus **(23.5)**(1) implies $\mathrm{depth}_{R'}(N_r) = 0$, as desired. □

Exercise (23.40) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a Noetherian module with $M/\mathfrak{a}M \neq 0$. Find a maximal ideal $\mathfrak{m} \in \mathrm{Supp}(M/\mathfrak{a}M)$ with

$$\mathrm{depth}(\mathfrak{a}, M) = \mathrm{depth}(\mathfrak{a}_\mathfrak{m}, M_\mathfrak{m}). \qquad \textbf{(23.40.1)}$$

Solution: There is a maximal M-sequence $x_1, \dots, x_r$ in $\mathfrak{a}$ by **(23.29)**. Given any $\mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)$, note $x_1/1, \dots, x_r/1$ is an $M_\mathfrak{p}$-sequence by **(23.27)**(1).

Set $M_r := M/\langle x_1, \dots, x_r\rangle M$. Then $\mathfrak{a} \subset \mathrm{z.div}(M_r)$ by maximality. So $\mathfrak{a} \subset \mathfrak{p}$ for some $\mathfrak{p} \in \mathrm{Ass}(M_r)$ by **(17.20)**. Fix any maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$.

Then $\mathfrak{m} \in \mathrm{Supp}(M_r)$ by **(17.13)**. But M_r is a quotient of M. So $\mathfrak{m} \in \mathrm{Supp}(M)$. But $\mathfrak{a} \subset \mathfrak{m}$; so $\mathfrak{m} \in \mathbf{V}(\mathfrak{a})$. Thus **(13.46)**(1) yields $\mathfrak{m} \in \mathrm{Supp}(M/\mathfrak{a}M)$.

Further, **(17.8)** yields $\mathfrak{p}R_\mathfrak{m} \in \mathrm{Ass}((M_r)_\mathfrak{m})$. So $\mathfrak{p}R_\mathfrak{m} = \mathrm{Ann}(m)$ for some nonzero $m \in (M_r)_\mathfrak{m}$. So $\mathfrak{a}R_\mathfrak{m} \subset \mathfrak{p}R_\mathfrak{m} \subset \mathrm{z.div}(M_r)_\mathfrak{m}$. But $(M_r)_\mathfrak{m} = M_\mathfrak{m}/\langle x_1, \dots, x_r\rangle M_\mathfrak{m}$ by **(12.15)**. So $x_1/1, \dots, x_r/1$ is maximal in $\mathfrak{a}R_\mathfrak{m}$. Thus **(23.29)** yields **(23.40.1)**. □

Exercise (23.42) . — Let R be a ring, and M a nonzero Noetherian semilocal module. Set $d := \dim(M)$. Show $\mathrm{depth}(M) = d$ if and only if M is Cohen–Macaulay and $\dim(M_\mathfrak{m}) = d$ for all maximal $\mathfrak{m} \in \mathrm{Supp}(M)$.

Solution: Assume $\mathrm{depth}(M) = d$. Then $\mathrm{depth}(M_\mathfrak{p}) = \dim(M_\mathfrak{p})$ for all $\mathfrak{p}$ in $\mathrm{Supp}(M)$ by **(23.39)**. Thus M is Cohen–Macaulay. Moreover, all maximal chains of primes in $\mathrm{Supp}(M)$ are of length d by **(23.37)**. Thus $\dim(M_\mathfrak{m}) = d$ for all maximal $\mathfrak{m} \in \mathrm{Supp}(M)$.

Conversely, assume that M is Cohen–Macaulay and that $\dim(M_\mathfrak{m}) = d$ for all maximal $\mathfrak{m} \in \mathrm{Supp}(M)$. Now, by **(23.40)**, there's some maximal $\mathfrak{m} \in \mathrm{Supp}(M)$ with $\mathrm{depth}(M) = \mathrm{depth}(M_\mathfrak{m})$. But $\mathrm{depth}(M_\mathfrak{m}) = \dim(M_\mathfrak{m})$ as M is Cohen–Macaulay. Moreover, $\dim(M_\mathfrak{m}) = d$ as $\mathfrak{m}$ is maximal. Thus $\mathrm{depth}(M) = d$. □

Exercise (23.51) . — Let R be a ring, M a module, and $x_1, \ldots, x_n \in R$. Set $\mathfrak{a} := \langle x_1, \ldots, x_n\rangle$ and assume $M/\mathfrak{a}M \neq 0$. For all $\mathfrak{p} \in \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{a})$, assume $x_1/1, \ldots, x_n/1$ is $M_{\mathfrak{p}}$-regular. Prove $x_1, \ldots, x_n$ is M-regular.

Solution: Induct on n. If $n = 0$, then the assertion is trivial.

Assume $n \geq 1$ and $x_1, \ldots, x_{n-1}$ is M-regular. Set $M_i := M/\langle x_1, \ldots, x_i\rangle M$. We have to prove $\mu_{x_n}\colon M_{n-1} \to M_{n-1}$ is injective. By **(13.9)**, it suffices to prove $\mu_{x_n/1}\colon (M_{n-1})_{\mathfrak{p}} \to (M_{n-1})_{\mathfrak{p}}$ is injective for every prime $\mathfrak{p}$.

Assume $\mathfrak{p} \notin \operatorname{Supp}(M)$. Then $M_{\mathfrak{p}} = 0$. In any event, **(12.15)** yields

$$(M_{n-1})_{\mathfrak{p}} = M_{\mathfrak{p}}/\langle x_1/1, \ldots, x_{n-1}/1\rangle M_{\mathfrak{p}}. \qquad \mathbf{(23.51.1)}$$

So $(M_{n-1})_{\mathfrak{p}} = 0$. Thus, in this case, $\mu_{x_n/1}$ is injective.

Assume $\mathfrak{a} \not\subset \mathfrak{p}$. Then $x_j \notin \mathfrak{p}$ for some j. So $x_j/1 \in R_{\mathfrak{p}}^{\times}$. If $j \leq n-1$, then $(M_{n-1})_{\mathfrak{p}} = 0$ owing to **(23.51.1)**. If $j = n$, then $\mu_{x_n/1}$ is invertible. Thus, in both these cases, $\mu_{x_n/1}$ is injective.

So assume $\mathfrak{p} \in \operatorname{Supp}(M) \bigcap \mathbf{V}(\mathfrak{a})$. Then $x_1/1, \ldots, x_n/1$ is $M_{\mathfrak{p}}$-regular. Thus $\mu_{x_n/1}$ is, by **(23.51.1)**, injective, as desired. □

Exercise (23.52) . — Let R be a ring, M a Noetherian module, $x_1, \ldots, x_n$ an M-sequence in $\operatorname{rad}(M)$, and σ a permutation of $1, \ldots, n$. Prove that $x_{\sigma 1}, \ldots, x_{\sigma n}$ is an M-sequence too; first, say σ just transposes i and $i+1$.

Solution: Say σ transposes i and $i+1$. Set $M_j := M/\langle x_1, \ldots, x_j\rangle M$. Then $M_{j+1} \xrightarrow{\sim} M_j/x_{j+1}M_j$ by **(23.4.1)**, and $\operatorname{rad}(M_j) = \operatorname{rad}(M)$ by **(23.4.2)**. Hence x_i, x_{i+1} is an M_{i-1}-sequence. Hence x_{i+1}, x_i is an M_{i-1}-sequence too owing to **(23.24)**(1) and to **(23.25)**. So $x_1, \ldots, x_{i-1}, x_{i+1}, x_i$ is an M-sequence. But $M/\langle x_1, \ldots, x_{i-1}, x_{i+1}, x_i\rangle M = M_{i+1}$. Thus $x_{\sigma 1}, \ldots, x_{\sigma n}$ is an M-sequence.

In general, σ is a composition of transpositions of successive integers. Thus the general assertion follows.

Alternatively, note $x_1, \ldots, x_n$ is M-quasi-regular by **(23.48)**. So $x_{\sigma 1}, \ldots, x_{\sigma n}$ is, plainly, M-quasi-regular for any σ. Arguing as in the proof of **(23.50)**(2)⇒(3), we conclude that $x_{\sigma 1}, \ldots, x_{\sigma n}$ is an M-sequence. □

Exercise (23.53) . — Let R be a ring, $\mathfrak{a}$ an ideal, and M a Noetherian module. Let $x_1, \ldots, x_r$ be an M-sequence, and $n_1, \ldots, n_r \geq 1$. Prove these two assertions:

(1) $x_1^{n_1}, \ldots, x_r^{n_r}$ is an M-sequence. (2) $\operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(\sqrt{\mathfrak{a}}, M)$.

Solution: For (1), induct on r. If $r = 0$, then assertion is trivial.

Assume $r > 0$. Set $M_i := M/\langle x_1, \ldots, x_i\rangle M$ and $M_i' := M/\langle x_1^{n_1}, \ldots, x_r^{n_r}\rangle M$ for all i. Then M_r is nonzero and a quotient of M_r'. Thus $M_r' \neq 0$.

Given $\mathfrak{p} \in \operatorname{Supp}(M) \bigcap \mathbf{V}(\langle x_1, \ldots, x_r\rangle)$, note $\mathfrak{p} \in \operatorname{Supp}(M_r)$ by **(13.46)**(1) as M is Noetherian. So $x_1/1, \ldots, x_r/1$ is $M_{\mathfrak{p}}$-regular by **(23.27)**(1). But $\mathbf{V}(\langle x_1, \ldots, x_r\rangle)$ is equal to $\mathbf{V}(\langle x_1^{n_1}, \ldots, x_r^{n_r}\rangle)$. So by **(23.51)**, it suffices to prove $x_1^{n_1}/1, \ldots, x_r^{n_r}/1$ is $M_{\mathfrak{p}}$-regular. So replacing R, M, x_i by $R_{\mathfrak{p}}$, $M_{\mathfrak{p}}$, $x_i/1$, we may assume R is local.

Since $x_1, \ldots, x_r$ is M-regular, $x_r \notin \operatorname{z.div}(M_{r-1})$. So $x_r^{n_r} \notin \operatorname{z.div}(M_{r-1})$. Hence $x_1, \ldots, x_{r-1}, x_r^{n_r}$ is M-regular. But R is local; so $x_1, \ldots, x_{r-1}, x_r^{n_r} \in \operatorname{rad}(M)$. Thus **(23.52)** yields that $x_r^{n_r}, x_1, \ldots, x_{r-1}$ is M-regular.

Set $N := M/\langle x_r^{n_r}\rangle$. Then therefore $x_1, \ldots, x_{r-1}$ is N-regular. So $x_1^{n_1}, \ldots, x_{r-1}^{n_{r-1}}$ is N-regular by induction. Hence $x_r^{n_r}, x_1^{n_1}, \ldots, x_{r-1}^{n_{r-1}}$ is M-regular. But R is local. Thus **(23.52)** yields that $x_1^{n_1}, \ldots, x_r^{n_r}$ is M-regular, as desired.

For (2), note $\operatorname{depth}(\mathfrak{a}, M) \leq \operatorname{depth}(\sqrt{\mathfrak{a}}, M)$ as $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$. Furthermore, the opposite inequality holds since, given any M-sequence $x_1, \dots, x_r$ in $\sqrt{\mathfrak{a}}$, there are $n_i \ge 1$ with $x_i^{n_i} \in \mathfrak{a}$, and since $x_1^{n_1}, \dots, x_r^{n_r}$ is M-regular by (1). Thus (2) holds. □

Exercise (23.54) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a nonzero Noetherian module, $x \in R$. Assume $\mathfrak{a} \subset \mathrm{z.div}(M)$ and $\mathfrak{a} + \langle x\rangle \subset \mathrm{rad}(M)$. Show $\mathrm{depth}(\mathfrak{a} + \langle x\rangle, M) \le 1$.

Solution: Set $\mathfrak{b} := \mathfrak{a} + \langle x\rangle$. Assume $\mathrm{depth}(\mathfrak{b}, M) \ge 1$. Then there's $b \in \mathfrak{b}$ with $b \notin \mathrm{z.div}(M)$. Say $b = a + xy$ with $a \in \mathfrak{a}$ and $y \in R$. Then **(17.33)** yields $r \ge 1$ with $b_r := a^r + x \notin \mathrm{z.div}(M)$.

Given any $b' \in \mathfrak{b}$, say $b' = a' + xy'$ with $a' \in \mathfrak{a}$ and $y' \in R$. Set $a'' := a' - a^r y'$. Then $a'' \in \mathfrak{a}$. So $a'' \in \mathrm{z.div}(M)$. So a'', b_r is not M-regular. But a'', $b_r \in \mathrm{rad}(M)$. So b_r, a'' too isn't M-regular by **(23.52)**. So $a'' \in \mathrm{z.div}(N)$ where $N := M/b_rM$. Say $a''n = 0$ with $n \in N$ nonzero.

Note $y'b_rn = 0$. So $(a'' + y'b_r)n = 0$. But $a'' + y'b_r = b'$. So $b'n = 0$. Thus $\mathfrak{b} \subset \mathrm{z.div}(N)$. So the M-sequence b_r is maximal in $\mathfrak{b}$. Thus **(23.29)** yields $\mathrm{depth}(\mathfrak{b}, M) = 1$. □

Exercise (23.55) . — Let R be a ring, $\mathfrak{a}$ an ideal, M a nonzero Noetherian module, $x \in R$. Set $\mathfrak{b} := \mathfrak{a}+\langle x\rangle$. Assume $\mathfrak{b} \subset \mathrm{rad}(M)$. Show $\mathrm{depth}(\mathfrak{b}, M) \le \mathrm{depth}(\mathfrak{a}, M)+1$.

Solution: Set $r := \mathrm{depth}(\mathfrak{a}, M)$. By **(23.29)**, there's a maximal M-sequence $x_1, \dots, x_r$ in $\mathfrak{a}$. Set $M_r := M/\langle x_1, \dots, x_r\rangle M$. Then $\mathfrak{a} \subset \mathrm{z.div}(M_r)$; moreover, $\mathrm{rad}(M) \subset \mathrm{rad}(M_r)$. So $\mathrm{depth}(\mathfrak{b}, M_r) \le 1$ by **(23.54)**. Thus by induction on r, **(23.31)** yields $\mathrm{depth}(\mathfrak{b}, M) \le r + 1$, as desired. □

Exercise (23.56) . — Let R be a ring, M a nonzero Noetherian module. Given any proper ideal $\mathfrak{a}$, set $c(\mathfrak{a}, M) := \min\{\dim M_\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)\}$. Prove M is Cohen–Macaulay if and only if $\mathrm{depth}(\mathfrak{a}, M) = c(\mathfrak{a}, M)$ for all proper ideals $\mathfrak{a}$.

Solution: Given any maximal ideal $\mathfrak{m} \in \mathrm{Supp}(M)$, note $\mathrm{Supp}(M/\mathfrak{m}M) = \{\mathfrak{m}\}$ by **(13.46)**(1). So $c(\mathfrak{m}, M) = \dim(M_\mathfrak{m})$. But $\mathrm{depth}(\mathfrak{m}, M) \le \mathrm{depth}(M_\mathfrak{m}) \le \dim(M_\mathfrak{m})$ by **(23.27)**(2) and **(23.5)**(3). Thus, for all such $\mathfrak{m}$, if $\mathrm{depth}(\mathfrak{m}, M) = c(\mathfrak{m}, M)$, then $\mathrm{depth}(M_\mathfrak{m}) = \dim(M_\mathfrak{m})$; that is, M is Cohen–Macaulay.

Conversely, assume M is Cohen–Macaulay, and fix a proper ideal $\mathfrak{a}$. Recall $\mathrm{Supp}(M/\mathfrak{a}M) = \mathrm{Supp}(M) \cap \mathbf{V}(\mathfrak{a})$ by **(13.46)**(1), and $\mathrm{Supp}(M) = \mathbf{V}(\mathrm{Ann}(M))$ by **(13.4)**(3). Set $R' := R/\mathrm{Ann}(M)$. Then M is a Noetherian R'-module. Given any ideal $\mathfrak{b}$ of R, set $\mathfrak{b}' := \mathfrak{b}R'$. Then $\mathfrak{a}M = \mathfrak{a}'M$.

Moreover, **(1.9)** and **(2.7)** imply the map $\mathfrak{p} \mapsto \mathfrak{p}'$ is a bijection from the primes of R containing $\mathrm{Ann}(M)$ to the primes of R'. Note $M_\mathfrak{p} = M_{\mathfrak{p}'}$ by **(12.26)**(2). So $\mathfrak{p} \in \mathrm{Supp}_R(M)$ if and only if $\mathfrak{p}' \in \mathrm{Supp}_{R'}(M)$. Also $\mathfrak{p} \supset \mathfrak{a}$ if and only if $\mathfrak{p}' \supset \mathfrak{a}'$. Thus $\mathfrak{p} \mapsto \mathfrak{p}'$ restricts to a bijection from $\mathrm{Supp}_R(M/\mathfrak{a}M)$ to $\mathrm{Supp}_{R'}(M/\mathfrak{a}'M)$. Moreover $\dim_{R_\mathfrak{p}}(M_\mathfrak{p}) = \dim_{R'_{\mathfrak{p}'}}(M_{R_{\mathfrak{p}'}})$ by **(21.20)**(1). Thus $c(\mathfrak{a}, M) = c(\mathfrak{a}', M)$.

Further $\mathrm{depth}(\mathfrak{a}, M) = \mathrm{depth}(\mathfrak{a}', M)$, as plainly a sequence in $\mathfrak{a}$ is an M-sequence if and only if its image in $\mathfrak{a}'$ is an M-sequence. Thus replacing R by R' and $\mathfrak{a}$ by $\mathfrak{a}'$, we may assume $\mathrm{Ann}(M) = 0$, and, by **(16.16)**, that R is Noetherian.

Note $\mathrm{Supp}(M) = \mathrm{Spec}(R)$ by **(13.4)**(3). So $\dim(M_\mathfrak{p}) = \mathrm{ht}(\mathfrak{p})$ for $\mathfrak{p} \in \mathrm{Supp}(M)$.

For any $\mathfrak{p} \in \mathrm{Supp}(M/\mathfrak{a}M)$, note $\mathrm{depth}(\mathfrak{a}, M) \le \mathrm{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p})$ by **(23.27)**(2). But, plainly, $\mathrm{depth}(\mathfrak{a}_\mathfrak{p}, M_\mathfrak{p}) \le \mathrm{depth}(M_\mathfrak{p})$. Finally, $\mathrm{depth}(M_\mathfrak{p}) \le \dim(M_\mathfrak{p})$ by **(23.5)**(3). Thus $\mathrm{depth}(\mathfrak{a}, M) \le c(\mathfrak{a}, M)$. It remains to show the opposite inequality.

There's a maximal ideal $\mathfrak{m} \in \mathrm{Supp}(M/\mathfrak{a}M)$ with $\mathrm{depth}(\mathfrak{a}, M) = \mathrm{depth}(\mathfrak{a}_\mathfrak{m}, M_\mathfrak{m})$ by **(23.40)**. So it suffices to prove $\mathrm{depth}(\mathfrak{a}_\mathfrak{m}, M_\mathfrak{m}) \ge c(\mathfrak{a}_\mathfrak{m}, M_\mathfrak{m})$ because, plainly,

$c(\mathfrak{a}_\mathfrak{m}, M_\mathfrak{m}) \ge c(\mathfrak{a}, M)$. Thus replacing R by $R_\mathfrak{m}$, we may assume R is local.

Suppose $\mathfrak{a}$ is $\mathfrak{m}$-primary. Then $\operatorname{depth}(\mathfrak{a}, M) = \operatorname{depth}(M)$ by **(23.53)**(2). Also $c(\mathfrak{a}, M) = \dim(M)$. But M is Cohen–Macaulay, so $\operatorname{depth}(M) = \dim(M)$. Thus $\operatorname{depth}(\mathfrak{a}, M) = c(\mathfrak{a}, M)$, as desired.

Suppose $\mathfrak{a}$ is not $\mathfrak{m}$-primary, and belongs to the set $\mathcal{S}$ of all ideals $\mathfrak{a}'$ such that $\operatorname{depth}(\mathfrak{a}', M) \ne c(\mathfrak{a}', M)$. As R is Noetherian, $\mathcal{S}$ has maximal elements. We may suppose $\mathfrak{a}$ is maximal.

Let Φ be the set of minimal primes $\mathfrak{p}$ of $\mathfrak{a}$. Note $c(\mathfrak{a}, M) = \min_{\mathfrak{p}\in\Phi} \operatorname{ht}(\mathfrak{p})$. As R is Noetherian, Φ is finite by **(17.29)**. As $\mathfrak{a}$ is not $\mathfrak{m}$-primary, $\mathfrak{m} \notin \Phi$. Hence by **(3.12)**, there's $x \in \mathfrak{m} - \bigcup_{\mathfrak{p}\in\Phi} \mathfrak{p}$. Set $\mathfrak{b} := \mathfrak{a} + \langle x\rangle$. Then $c(\mathfrak{b}, M) > c(\mathfrak{a}, M)$.

Say $\mathfrak{a}$ can be generated by r elements, but not fewer. Then $c(\mathfrak{a}, M) = r$ by **(21.8)**. But $\mathfrak{b}$ can be generated by $r + 1$ elements. So $c(\mathfrak{b}, M) \le r + 1$ by **(21.8)** again. So $c(\mathfrak{a}, M) + 1 \ge c(\mathfrak{b}, M) > c(\mathfrak{a}, M)$. Thus $c(\mathfrak{a}, M) + 1 = c(\mathfrak{b}, M)$.

But $\mathfrak{a}$ is maximal in $\mathcal{S}$; so $\mathfrak{b} \notin \mathcal{S}$. So $\operatorname{depth}(\mathfrak{b}, M) = c(\mathfrak{b}, M)$. But **(23.55)** yields $\operatorname{depth}(\mathfrak{b}, M) \le \operatorname{depth}(\mathfrak{a}, M) + 1$. Thus $c(\mathfrak{a}, M) \le \operatorname{depth}(\mathfrak{a}, M)$, as desired. □

Exercise (23.57) . — Prove that a Noetherian local ring A of dimension $r \ge 1$ is regular if and only if its maximal ideal $\mathfrak{m}$ is generated by an A-sequence. Prove that, if A is regular, then A is Cohen–Macaulay and universally catenary.

Solution: Assume A is regular. Given a regular sop $x_1, \ldots, x_r$, let's show it's an A-sequence. Set $A_1 := A/\langle x_1\rangle$. Then A_1 is regular of dimension $r - 1$ by **(21.16)**. So $x_1 \ne 0$. But A is a domain by **(21.17)**. So $x_1 \notin \operatorname{z.div}(A)$. Further, if $r \ge 2$, then the residues of $x_2, \ldots, x_r$ form a regular sop of A_1; so we may assume they form an A_1-sequence by induction on r. Thus $x_1, \ldots, x_r$ is an A-sequence.

Conversely, if $\mathfrak{m}$ is generated by an A-sequence $x_1, \ldots, x_n$, then $n \le \operatorname{depth}(A) \le r$ by **(23.4)** and **(23.5)**(3), and $n \ge r$ by **(21.13)**. Thus then $n = \operatorname{depth}(A) = r$, and so A is regular and Cohen–Macaulay, so universally catenary by **(23.45)**. □

Exercise (23.58) . — Let R be a ring, and M a nonzero Noetherian semilocal module. Set $\mathfrak{m} := \operatorname{rad}(M)$. Prove: (1) $\widehat{M}$ is a nonzero Noetherian semilocal $\widehat{R}$-module, and $\widehat{\mathfrak{m}} = \operatorname{rad}(\widehat{M})$; and (2) $\operatorname{depth}_R(M) = \operatorname{depth}_R(\widehat{M}) = \operatorname{depth}_{\widehat{R}}(\widehat{M})$.

Solution: For (1), note $\mathfrak{m}$ is a parameter ideal for M by **(19.14)**. So $\widehat{M}$ is a nonzero Noetherian $\widehat{R}$-module by **(22.61)**(1). Now, in **(22.53)**, set $\mathfrak{a} := \mathfrak{m}$; then Φ is the set of maximal ideals in $\operatorname{Supp}(M)$. So $\widehat{M}$ is semilocal by **(22.53)**(6). And $\operatorname{rad}(\widehat{M}) = \big(\bigcap_{\mathfrak{p}\in\Phi} \mathfrak{p}\big)\widehat{\ } = \widehat{\mathfrak{m}}$ by **(22.53)**(5) and **(13.4)**(4). Thus (1) holds.

For (2), given an M-sequence $x_1, \ldots, x_r$ in $\mathfrak{m}$, set $M_i := M/\langle x_1, \ldots, x_i\rangle M$. Then

$$\widehat{M_i} = \widehat{M}/(\langle x_1, \ldots, x_i\rangle M)\widehat{\ } = \widehat{M}/\langle x_1, \ldots, x_i\rangle \widehat{M}$$

by **(22.18)** and **(22.20)**(b). But $x_{i+1} \notin \operatorname{z.div}(M_i)$; so $x_{i+1} \notin \operatorname{z.div}(\widehat{M_i})$ by **(22.18)**. Also $\widehat{M_r} \ne 0$ as $x_1, \ldots, x_r \in \operatorname{rad}(\widehat{M})$ by (1). Thus $\operatorname{depth}_R(M) \le \operatorname{depth}_R(\widehat{M})$.

Given any $x \in R$, note $xy = \kappa_R(x)y$ for all $y \in \widehat{M}$. Hence, given any $\widehat{M}$-sequence $x_1, \ldots, x_r$ in $\mathfrak{m}$, the $\kappa_R(x_i)$ form an $\widehat{M}$-sequence in $\widehat{\mathfrak{m}}$, that is in $\operatorname{rad}(\widehat{M})$ by (1). Thus $\operatorname{depth}_R(\widehat{M}) \le \operatorname{depth}_{\widehat{R}}(\widehat{M})$.

By **(23.29)**, there's an M-sequence $x_1, \ldots, x_r$ in $\mathfrak{m}$ with $\mathfrak{m} \subset \operatorname{z.div}(M_r)$ and $r = \operatorname{depth}_R(M)$. Then **(17.20)** yields a nonzero R-map $\alpha\colon R/\mathfrak{m} \to M_r$. Its completion is an $\widehat{R}$-map $\widehat{\alpha}\colon \widehat{R}/\widehat{\mathfrak{m}} \to \widehat{M_r}$, as $\widehat{R}/\widehat{\mathfrak{m}} = \widehat{R/\mathfrak{m}}$ by **(22.18)**.

Plainly, $\widehat{\alpha}(1) = \kappa_{M_r}\alpha(1)$. But $\alpha(1) \ne 0$ as $\alpha \ne 0$. And $\kappa_{M_r}\colon M_r \to \widehat{M_r}$ is injective by (**22.3**). So $\widehat{\alpha}(1) \neq 0$. So $\widehat{\alpha} \neq 0$. So $\widehat{\mathfrak{m}} \subset \mathrm{z.div}(\widehat{M_r})$ as $\widehat{\mathfrak{m}}\widehat{\alpha}(1) = 0$. So $r = \mathrm{depth}_{\widehat{R}}(\widehat{M})$ by (**23.29**). But $r = \mathrm{depth}_R(M) \leq \mathrm{depth}_R(\widehat{M}\,) \leq \mathrm{depth}_{\widehat{R}}(\widehat{M})$. Thus (2) holds. □

Exercise (23.59) . — Let A be a DVR, t a uniformizing parameter, X a variable. Set $P := A[X]$. Set $\mathfrak{m}_1 := \langle 1 - tX\rangle$ and $\mathfrak{m}_2 := \langle t, X\rangle$. Prove P is Cohen–Macaulay, and each $\mathfrak{m}_i$ is maximal with $\mathrm{ht}(\mathfrak{m}_i) = i$.

Set $S_i := P - \mathfrak{m}_i$ and $S := S_1 \cap S_2$. Set $B := S^{-1}P$ and $\mathfrak{n}_i := \mathfrak{m}_i B$. Prove B is semilocal and Cohen–Macaulay, $\mathfrak{n}_i$ is maximal, and $\dim(B_{\mathfrak{n}_i}) = i$.

Solution: Set $K := \mathrm{Frac}(A)$. Let $\varphi\colon P \to K$ be the ring map with $\varphi(X) = t^{-1}$ and $\varphi|A$ the inclusion $A \hookrightarrow K$. Set $\mathfrak{n} := \mathrm{Ker}(\varphi)$. Plainly φ is surjective, so $\mathfrak{n}$ is maximal. So by (**2.20**)(2), either $\mathfrak{n} = \langle F\rangle$ with F irreducible, or $\mathfrak{n} = \langle t, G\rangle$ with $G \in P$. But $t \notin \mathfrak{n}$ as $\varphi|A$ is the inclusion. Thus $\mathfrak{n} = \langle F\rangle$.

However, $1 - tX \in \mathfrak{n}$. So $1 - tX = FH$. But $1 - tX$ is irreducible. So H is a unit. So $\mathfrak{m}_1 = \mathfrak{n}$. Thus $\mathfrak{m}_1$ is maximal. Further, (**21.8**) yields $\mathrm{ht}(\mathfrak{m}_1) = 1$.

However, $P/\langle X\rangle = A$, and $A/\langle t\rangle$ is a field. Thus $\mathfrak{m}_2$ is maximal too. Further, $\mathfrak{m}_2$ isn't principal, as no nonunit divides both t and X. Thus (**21.8**) yields $\mathrm{ht}(\mathfrak{m}_2) = 2$.

Let $\mathfrak{m}$ be any maximal ideal of P other than $\mathfrak{m}_1$ or $\mathfrak{m}_2$. By (**3.12**), there's $x \in \mathfrak{m} - \mathfrak{m}_1 \cup \mathfrak{m}_2$. So $x \in \mathfrak{m} \cap S$. But $\mathfrak{m}_1 \cap S = \emptyset$ and $\mathfrak{m}_2 \cap S = \emptyset$. Hence (**11.12**)(2) implies $\mathfrak{n}_1$ and $\mathfrak{n}_2$ are the only maximal ideals of B. Thus B is semilocal. But A is Cohen–Macaulay. So P is Cohen–Macaulay by (**23.43**). But $P_{\mathfrak{m}_i} = B_{\mathfrak{n}_i}$ by (**12.25**)(2) as $\mathfrak{m}_i \cap S = \emptyset$. Thus B is Cohen–Macaulay by (**23.41**). Lastly, $\dim(B_{\mathfrak{n}_i}) = i$ as $\mathrm{ht}(\mathfrak{m}_i) = i$. □

Exercise (23.60) . — Let R be a ring, M a nonzero Noetherian semilocal module, and $x_1, \ldots, x_m \in \mathrm{rad}(M)$. For all i, set $M_i := M/\langle x_1, \ldots, x_i\rangle M$. Assume that $\mathrm{depth}(M) = \dim(M)$ and $\dim(M_m) = \dim(M) - m$. For all i, show $x_1, \ldots, x_i$ is an M-sequence, and $\mathrm{depth}(M_i) = \dim(M_i) = \dim(M) - i$.

Solution: Note that $\mathrm{rad}(M) = \mathrm{rad}(M_i)$ for all i by (**23.4.2**). Hence (**21.5**) gives $\dim(M_i/x_{i+1}M_i) \geq \dim(M_i) - 1$ for all i. But $M_i/x_{i+1}M_i = M_{i+1}$ by (**23.4.1**). And $\dim(M_m) = \dim(M) - m$. Thus $\dim(M_i) = \dim(M) - i$ for all i.

Proceed by induction on i. The case $i = 0$ is trivial. So fix $i < m$, and assume the assertions hold as stated.

Note $\dim(M_i/x_{i+1}M_i) = \dim(M_i) - 1$. So $x_{i+1} \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Supp}(M_i)$ with $\dim(R/\mathfrak{p}) = \dim(M_i)$ by (**21.5**). But $\mathrm{depth}(M_i) = \dim(M_i)$. So $x_{i+1} \notin \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}(M_i)$ by (**23.37**). So $x_{i+1} \notin \mathrm{z.div}(M_i)$ by (**17.12**). But $x_1, \ldots, x_i$ form an M-sequence. Thus $x_1, \ldots, x_i, x_{i+1}$ do too.

Finally, note $\mathrm{depth}(M_i) = \dim(M_i)$ and $x_{i+1} \in \mathrm{rad}(M) - \mathrm{z.div}(M_i)$. But $\mathrm{rad}(M) = \mathrm{rad}(M_i)$. Thus (**23.32**) gives $\mathrm{depth}(M_{i+1}) = \dim(M_{i+1})$. □

Exercise (23.61) . — Let k be a field, $P := k[X_1, \ldots, X_n]$ a polynomial ring, and $F_1, \ldots, F_m \in P$. Set $\mathfrak{A} := \langle F_1, \ldots, F_m\rangle$. For all i, j, define $\partial F_i/\partial X_j \in P$ formally as in (**1.18.1**). Let $\mathfrak{A}'$ be the ideal generated by $\mathfrak{A}$ and all the maximal minors of the m by n Jacobian matrix $(\partial F_i/\partial X_j)$. Set $R := P/\mathfrak{A}$ and $R' := P/\mathfrak{A}'$. Assume $\dim R = n - m$. Show that R is Cohen–Macaulay, and that, when k is algebraically closed, R is normal if and only if either $R' = 0$ or $\dim R' \leq n - m - 2$.

Solution: Given a maximal ideal $\mathfrak{M} \supset \mathfrak{A}$ of P, note $P_{\mathfrak{M}}$ is regular of dimension n by (**21.14**), so Cohen–Macaulay by (**23.57**). But repeated use of (**21.5**) gives

$\dim R_{\mathfrak{M}} \ge n-m$, and $\dim R_{\mathfrak{M}} \le n-m$ as $\dim R = n-m$; so $\dim R_{\mathfrak{M}} = n-m$. So **(23.60)** implies $R_{\mathfrak{M}}$ is Cohen–Macaulay. Thus R is Cohen–Macaulay.

So **(23.39)** implies (S_q) holds for all q. In particular (S_2) holds for R. Thus Serre's Criterion **(23.23)** yields R is normal if and only if (R_1) holds. From now on, assume k is algebraically closed.

First, suppose $n-m=0$. Then $\dim R_{\mathfrak{M}} = 0$ for every $\mathfrak{M}$. So (R_1) holds if and only if every $R_{\mathfrak{M}}$ is regular. As k is algebraically closed, $\mathfrak{M} = \langle X_1 - x_1, \ldots, X_n - x_n\rangle$ for some $\mathbf{x} := (x_1, \ldots, x_n) \in k^n$ by **(15.5)**. So $R_{\mathfrak{M}}$ is regular if and only if the Jacobian matrix $(\partial F_i/\partial X_j)$ has rank n at $\mathbf{x}$ by **(21.42)**(1), so if and only if its determinant D is nonzero at $\mathbf{x}$, that is, $D \notin \mathfrak{M}$. But $\mathfrak{A}' = \langle \mathfrak{A}, D\rangle$, so $D \notin \mathfrak{M}$ if and only if $\mathfrak{A}' P_{\mathfrak{M}} = P_{\mathfrak{M}}$. Hence $R_{\mathfrak{M}}$ is regular if and only if $R'_{\mathfrak{M}} = 0$. Thus (R_1) holds if and only if $R'_{\mathfrak{M}} = 0$ for all $\mathfrak{M}$, or equivalently by **(13.8)**, $R' = 0$, as desired.

So from now on, suppose $n-m \ge 1$. Then no minimal prime $\mathfrak{q}$ of R is maximal, as $\dim R_{\mathfrak{M}} = n-m$ for every $\mathfrak{M}$. So every minimal $\mathfrak{q}$ lies in some height-1 prime $\mathfrak{p}$. Then **(12.25)**(3) implies $R_{\mathfrak{q}}$ is the localization of $R_{\mathfrak{p}}$ at $\mathfrak{q}R_{\mathfrak{p}}$, which is a minimal prime. Hence, if $R_{\mathfrak{p}}$ is a domain, then $R_{\mathfrak{q}}$ is its fraction field.

So (R_0) holds if $R_{\mathfrak{p}}$ is a domain for every height-1 prime $\mathfrak{p}$ of R. So by **(23.10)**, (R_1) holds if and only if $R_{\mathfrak{p}}$ is a DVR for every such $\mathfrak{p}$. Thus we must show that $R_{\mathfrak{p}}$ is a DVR for every height-1 prime $\mathfrak{p}$ if and only if either $R' = 0$ or $\dim R' \le n-m-2$.

Note that, $\dim R' > n-m-2$ means there exists a maximal chain of primes $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ in R with $\mathfrak{A}'/\mathfrak{A} \subset \mathfrak{p}_0$ and $r > n-m-2$. In such a chain, $\mathfrak{p}_r$ is maximal. So $\dim R_{\mathfrak{p}_r} = n-m$. So $n-m \ge r$. So either $r = n-m$ or $r = n-m-1$. If $r = n-m$, then $\mathfrak{p}_1$ has height 1. If $r = n-m-1$, then $\mathfrak{p}_0$ can't be minimal by **(23.37)**, as $R_{\mathfrak{p}_r}$ is Cohen–Macaulay of dimension $n-m$. Thus $\mathfrak{p}_0$ has height 1.

Conversely, given a height-1 prime $\mathfrak{p}$ of R with $\mathfrak{A}'/\mathfrak{A} \subset \mathfrak{p}$, let $\mathfrak{m}$ be any maximal ideal containing $\mathfrak{p}$. Then $R_{\mathfrak{m}}$ is Cohen–Macaulay of dimension $n-m$. So by **(23.37)**, in any maximal chain of primes $\mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ with $\mathfrak{p}_1 = \mathfrak{p}$ and $\mathfrak{p}_r = \mathfrak{m}$, necessarily $r = n-m-1$. Thus $\dim R' > n-m-2$.

Hence $\dim R' \le n-m-2$ if and only if every height-1 prime $\mathfrak{p}$ of R satisfies $\mathfrak{p} \not\supset \mathfrak{A}'/\mathfrak{A}$. Thus it now suffices to prove this: fix any height-1 prime $\mathfrak{p}$ of R; then $R_{\mathfrak{p}}$ is a DVR if and only if $\mathfrak{p} \not\supset \mathfrak{A}'/\mathfrak{A}$.

Given a maximal ideal $\mathfrak{m} \supset \mathfrak{p}$, note $(R_{\mathfrak{m}})_{\mathfrak{p}} = R_{\mathfrak{p}}$ by **(12.25)**(3). But $R_{\mathfrak{m}}$ is Cohen–Macaulay. Thus **(23.37)** yields $\dim R_{\mathfrak{m}} = 1 + \dim(R_{\mathfrak{m}}/\mathfrak{p}R_{\mathfrak{m}})$.

First, suppose $R_{\mathfrak{p}}$ is a DVR. Say $\mathfrak{p}R_{\mathfrak{p}} = \langle t/s\rangle$ with $t \in R$ and $s \in R - \mathfrak{p}$. Say $\mathfrak{p} = \langle g_1, \ldots, g_a\rangle$ with $g_i \in R$. Then $g_i/1 = tt_i/ss_i$ for some $t_i \in R$ and $s_i \in R - \mathfrak{p}$. Set $f := ss_1 \cdots s_a$. Then $\mathfrak{p}R_f = tR_f$. Since $\mathfrak{p}$ is prime, its contraction in P is also prime. So **(21.42)**(2) yields a maximal ideal with $\mathfrak{m} \supset \mathfrak{p}$ but $f \notin \mathfrak{m}$ such that $(R/\mathfrak{p})_{\mathfrak{m}}$ is regular. So **(12.25)**(2) and **(12.15)** yield

$$(R/\mathfrak{p})_{\mathfrak{m}} = ((R/\mathfrak{p})_f)_{\mathfrak{m}} = (R_f/\mathfrak{p}R_f)_{\mathfrak{m}} = R_{\mathfrak{m}}/tR_{\mathfrak{m}}.$$

So $R_{\mathfrak{m}}$ is regular by **(21.16)** with $\mathfrak{a} := \langle t\rangle$ as $\dim R_{\mathfrak{m}}/tR_{\mathfrak{m}} = \dim(R_{\mathfrak{m}}) - 1$. So $\mathfrak{m} \not\supset \mathfrak{A}'/\mathfrak{A}$ by **(21.42)**(1). Thus $\mathfrak{p} \not\supset \mathfrak{A}'/\mathfrak{A}$.

Conversely, suppose $\mathfrak{p} \not\supset \mathfrak{A}'/\mathfrak{A}$. Say $f \in \mathfrak{A}'/\mathfrak{A}$, but $f \notin \mathfrak{p}$. Then **(21.42)**(2) yields a maximal ideal $\mathfrak{m} \supset \mathfrak{p}$ with $f \notin \mathfrak{m}$ and $(R/\mathfrak{p})_{\mathfrak{m}}$ regular. So $\mathfrak{m} \not\supset \mathfrak{A}'/\mathfrak{A}$. So $R_{\mathfrak{m}}$ is regular by **(21.42)**(1). So $R_{\mathfrak{m}}$ is normal by **(22.40)**(2). So $(R_{\mathfrak{m}})_{\mathfrak{p}}$ is normal by **(11.32)**. But $R_{\mathfrak{p}} = (R_{\mathfrak{m}})_{\mathfrak{p}}$. Thus, by **(23.6)**(2)⇒(1), $R_{\mathfrak{p}}$ is a DVR, as desired. □

24. Dedekind Domains

Exercise (24.4) . — Let R be a domain, S a multiplicative subset.

(1) Assume $\dim(R) = 1$. Then $\dim(S^{-1}R) = 1$ if and only if there is a nonzero prime $\mathfrak{p}$ of R with $\mathfrak{p} \cap S = \emptyset$.

(2) Assume $\dim(R) \geq 1$. Then $\dim(R) = 1$ if and only if $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero prime $\mathfrak{p}$ of R.

Solution: Consider (1). Suppose $\dim(S^{-1}R) = 1$. Then there's a chain of primes $0 \subsetneqq \mathfrak{p}'$ in $S^{-1}R$. Set $\mathfrak{p} := \mathfrak{p}' \cap R$. Then $\mathfrak{p}$ is as desired by **(11.12)**(2).

Conversely, suppose there's a nonzero $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $0 \subsetneqq \mathfrak{p}S^{-1}R$ is a chain of primes in $S^{-1}R$ by **(11.12)**(2); so $\dim(S^{-1}R) \geq 1$. Now, given a chain of primes $0 = \mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ in $S^{-1}R$, set $\mathfrak{p}_i := \mathfrak{p}'_i \cap R$. Then $0 = \mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ is a chain of primes in R by **(11.12)**(2). So $r \leq 1$ as $\dim(R) = 1$. Thus $\dim(S^{-1}R) = 1$.

Consider (2). If $\dim(R) = 1$, then (1) yields $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero $\mathfrak{p}$.

Conversely, let $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_r$ be a chain of primes in R. Set $\mathfrak{p}'_i := \mathfrak{p}_i R_{\mathfrak{p}_r}$. Then $\mathfrak{p}'_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}'_r$ is a chain of primes in $R_{\mathfrak{p}_r}$ by **(11.12)**(2). So if $\dim(R_{\mathfrak{p}_r}) = 1$, then $r \leq 1$. Thus if $\dim(R_{\mathfrak{p}}) = 1$ for every nonzero $\mathfrak{p}$, then $\dim(R) \leq 1$, as required. □

Exercise (24.5) . — Let R be a Dedekind domain, and S a multiplicative subset. Assume $0 \notin S$. Show that $S^{-1}R$ is Dedekind if there's a nonzero prime $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$, and that $S^{-1}R = \mathrm{Frac}(R)$ if not.

Solution: Note $S^{-1}R$ is a domain by **(11.2)** as $0 \notin S$.

Assume there's a nonzero $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $\dim(S^{-1}R) = 1$ by **(24.4)**(1). Moreover, $S^{-1}R$ is Noetherian by **(16.7)**. And $S^{-1}R$ is normal by **(11.32)**. Thus $S^{-1}R$ is Dedekind.

Assume there's no nonzero $\mathfrak{p}$ with $\mathfrak{p} \cap S = \emptyset$. Then $\langle 0 \rangle$ is maximal by **(11.12)**(2). So $S^{-1}R$ is a field by **(2.12)**. Thus **(2.3)** gives $S^{-1}R = \mathrm{Frac}(R)$. □

Exercise (24.19) . — Let R be a Dedekind domain, and $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ ideals. By first reducing to the case that R is local, prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}),$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

Solution: By **(13.53)**, it suffices to establish the two equations after localizing at each maximal ideal $\mathfrak{p}$. But localization commutes with intersection and sum by **(12.12)**(6)(b), (7)(b). So the new equations look like the original ones, but with $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ replaced by $\mathfrak{a}_{\mathfrak{p}}$, $\mathfrak{b}_{\mathfrak{p}}$, $\mathfrak{c}_{\mathfrak{p}}$. And $R_{\mathfrak{p}}$ is a DVR by **(24.6)**. So replace R by $R_{\mathfrak{p}}$.

Take a uniformizing parameter t. Then **(23.1.3)** yields i, j, k with $\mathfrak{a} = \langle t^i \rangle$ and $\mathfrak{b} = \langle t^j \rangle$ and $\mathfrak{c} = \langle t^k \rangle$. So the two asserted equations are equivalent to these two:

$$\max\{i, \min\{j, k\}\} = \min\{\max\{i, j\}, \max\{i, k\}\},$$
$$\min\{i, \max\{j, k\}\} = \max\{\min\{i, j\}, \min\{i, k\}\}.$$

However, these two equations are easy to check for any integers i, j, k. □

Exercise (24.20) . — Let R be a Dedekind domain; $x_1, \ldots, x_n \in R$; and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals. Prove that the system of congruences $x \equiv x_i \bmod \mathfrak{a}_i$ for all i has a solution $x \in R$ if and only if $x_i \equiv x_j \bmod (\mathfrak{a}_i + \mathfrak{a}_j)$ for $i \neq j$. In other words, prove the exactness (in the middle) of the sequence of R-modules

$$R \xrightarrow{\varphi} \bigoplus_{i=1}^{n} R/\mathfrak{a}_i \xrightarrow{\psi} \bigoplus_{i<j} R/(\mathfrak{a}_i + \mathfrak{a}_j)$$

where $\varphi(y)$ is the vector of residues of y in the $R/\mathfrak{a}_i$ and where $\psi(y_1, \dots, y_n)$ is the vector of residues of the $y_i - y_j$ in $R/(\mathfrak{a}_i + \mathfrak{a}_j)$.

Solution: Plainly $\mathrm{Ker}(\psi) \supset \mathrm{Im}(\varphi)$. To prove $\mathrm{Ker}(\psi) \subset \mathrm{Im}(\varphi)$, it suffices, by **(13.9)**, to do so after localizing at any maximal ideal. So assume R is local. Then **(24.6)** implies R is a DVR.

Each $\mathfrak{a}_i$ is now a power of the maximal ideal by **(23.1.3)**. Reorder the $\mathfrak{a}_i$ so that $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_n$. Then $\mathfrak{a}_1 + \mathfrak{a}_j = \mathfrak{a}_j$ for all j. Given $z \in \mathrm{Ker}(\psi)$, represent z by $(z_1, \dots, z_n)$ with $z_i \in R$. Then $z_1 - z_j \in \mathfrak{a}_j$ for all j. So $(z_1, \dots, z_1)$ represents z too. So $\mathrm{Im}(z_1) = z$. Thus $\mathrm{Ker}(\psi) \subset \mathrm{Im}(\varphi)$, as desired. □

Exercise (24.21) . — Prove that a semilocal Dedekind domain A is a PID. Begin by proving that each maximal ideal is principal.

Solution: Let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the maximal ideals of A. Let's prove they are principal, starting with $\mathfrak{p}_1$. By Nakayama's lemma **(10.6)**, $\mathfrak{p}_1 A_{\mathfrak{p}_1} \neq \mathfrak{p}_1^2 A_{\mathfrak{p}_1}$; so $\mathfrak{p}_1 \neq \mathfrak{p}_1^2$. Take $y \in \mathfrak{p}_1 - \mathfrak{p}_1^2$. The ideals $\mathfrak{p}_1^2,\ \mathfrak{p}_2,\ \dots,\ \mathfrak{p}_r$ are pairwise comaximal because no two of them lie in the same maximal ideal. Hence, by the Chinese Remainder Theorem, **(1.21)**(4)(c), there's an $x \in A$ with $x \equiv y \bmod \mathfrak{p}_1^2$ and $x \equiv 1 \bmod \mathfrak{p}_i$ for $i \geq 2$.

The Main Theorem of Classical Ideal Theory **(24.8)** gives $\langle x \rangle = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2} \cdots \mathfrak{p}_r^{n_r}$ with $n_i \geq 0$. But $x \notin \mathfrak{p}_i$ for $i \geq 2$; so $n_i = 0$ for $i \geq 2$. Further, $x \in \mathfrak{p}_1 - \mathfrak{p}_1^2$; so $n_1 = 1$. Thus $\mathfrak{p}_1 = \langle x \rangle$. Similarly, all the other $\mathfrak{p}_i$ are principal.

Finally, let $\mathfrak{a}$ be any nonzero ideal. Then the Main Theorem, **(24.8)**, yields $\mathfrak{a} = \prod \mathfrak{p}_i^{m_i}$ for some m_i. Say $\mathfrak{p}_i = \langle x_i \rangle$. Then $\mathfrak{a} = \langle \prod x_i^{m_i} \rangle$, as desired. □

Exercise (24.22) . — Let R be a Dedekind domain, and $\mathfrak{a}$ a nonzero ideal. Prove (1) $R/\mathfrak{a}$ is a PIR, and (2) $\mathfrak{a}$ is generated by two elements.

Solution: To prove (1), let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the associated primes of $\mathfrak{a}$, and set $S := \bigcap_i S_{\mathfrak{p}_i}$. Then S is multiplicative. Set $R' := S^{-1}R$. Then R' is Dedekind by **(24.5)**. Let's prove R' is semilocal.

Let $\mathfrak{q}$ be a maximal ideal of R'. Set $\mathfrak{p} := \mathfrak{q} \cap R$. Then $\mathfrak{q} = \mathfrak{p}R'$ by **(11.12)**(2). So $\mathfrak{p}$ is nonzero, whence maximal since R has dimension 1. Suppose $\mathfrak{p}$ is distinct from all the $\mathfrak{p}_i$. Then $\mathfrak{p}$ and the $\mathfrak{p}_i$ are pairwise comaximal. So, by the Chinese Remainder Theorem, **(1.21)**(4)(c), there's a $u \in R$ that is congruent to 0 modulo $\mathfrak{p}$ and to 1 modulo each $\mathfrak{p}_i$. But $S_{\mathfrak{p}_i} := R - \mathfrak{p}_i$. Hence, $u \in \mathfrak{p} \cap S$, but $\mathfrak{q} = \mathfrak{p}R'$, a contradiction. Thus $\mathfrak{p}_1 R', \dots, \mathfrak{p}_r R'$ are all the maximal ideals of R'.

So R' is a PID by **(24.21)**; so every ideal in $R'/\mathfrak{a}R'$ is principal. But by **(12.15)**, $R'/\mathfrak{a}R' = S^{-1}(R/\mathfrak{a})$. Finally, note that each $u \in S$ maps to a unit in $R/\mathfrak{a}$, as its image lies in no maximal ideal of $R/\mathfrak{a}$. So $S^{-1}(R/\mathfrak{a}) = R/\mathfrak{a}$ by **(11.15.1)** and **(11.4)**. Thus (1) holds.

Alternatively, we can prove (1) without using **(24.21)**, as follows. The Main Theorem of Classical Ideal Theory, **(24.8)**, yields $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$ for distinct maximal ideals $\mathfrak{p}_i$. The $\mathfrak{p}_i^{n_i}$ are pairwise comaximal. So, by the Chinese Remainder Theorem, **(1.21)**(4)(c), there's a canonical isomorphism:

$$R/\mathfrak{a} \xrightarrow{\sim} R/\mathfrak{p}_1^{n_1} \times \cdots \times R/\mathfrak{p}_k^{n_k}.$$

Next, we prove each $R/\mathfrak{p}_i^{n_i}$ is a PIR. Thus **(19.27)**(1) yields (1).

To prove $R/\mathfrak{p}_i^{n_i}$ is a PIR, note $\mathfrak{p}_i/\mathfrak{p}_i^{n_i}$ is the only prime in $R/\mathfrak{p}_i^{n_i}$, so each $u \in S_{\mathfrak{p}_i}$ maps to a unit in $R/\mathfrak{p}_i^{n_i}$. So $R/\mathfrak{p}_i^{n_i} = S_{\mathfrak{p}_i}^{-1}(R/\mathfrak{p}_i^{n_i})$ by **(11.15.1)** and **(11.4)**. But $S_{\mathfrak{p}_i}^{-1}(R/\mathfrak{p}_i^{n_i}) = R_{\mathfrak{p}_i}/\mathfrak{p}_i^{n_i}R_{\mathfrak{p}_i}$ by **(12.15)**. Further, $R_{\mathfrak{p}_i}$ is a DVR by **(24.6)**, so a PIR by **(23.1.3)**. Thus $R/\mathfrak{p}_i^{n_i}$ is a PIR. Thus again (1) holds.

Consider (2). Let $x \in \mathfrak{a}$ be nonzero. By (1), there is a $y \in \mathfrak{a}$ whose residue generates $\mathfrak{a}/\langle x\rangle$. Then $\mathfrak{a} = \langle x, y\rangle$. □

Exercise (24.23) . — Let R be a Dedekind domain, and M a finitely generated module. Assume M is **torsion**; that is, $T(M) = M$. Show $M \simeq \bigoplus_{i,j} R/\mathfrak{p}_i^{n_{ij}}$ for unique nonzero primes $\mathfrak{p}_i$ and unique $n_{ij} > 0$.

Solution: Say $m_1, \ldots, m_n$ generate M. Since M is torsion, for each j there's a nonzero $x_j \in R$ with $x_j m_j = 0$. As R is a domain, $x_1 \cdots x_n$ is nonzero, and it is in $\operatorname{Ann}(M)$. Thus $\operatorname{Ann}(M) \neq 0$.

Using **(24.8)**, write $\operatorname{Ann}(M) = \prod_{i=1}^n \mathfrak{p}_i^{v_i}$. Then $\mathbf{V}(\operatorname{Ann}(M)) = \bigcup_{i=1}^n \mathbf{V}(\mathfrak{p}_i)$ by **(13.1)**. But $\mathbf{V}(\operatorname{Ann}(M)) = \operatorname{Supp}(M)$ by **(13.4)**(3). Also, as each $\mathfrak{p}_i$ is maximal, $\mathbf{V}(\mathfrak{p}_i) = \{\mathfrak{p}_i\}$ by **(13.16)**(1), (2). Thus $\operatorname{Supp}(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Hence M has finite length by **(19.26)**. Thus **(19.3)** yields $M = \prod_{i=1}^n M_{\mathfrak{p}_i}$.

By **(24.6)**, each $R_{\mathfrak{p}_i}$ is a DVR; so each is a local PID by **(23.1)**. Therefore, $M_{\mathfrak{p}_i} = \bigoplus R_{\mathfrak{p}_i}/\mathfrak{p}_i^{n_{ij}}R_{\mathfrak{p}_i}$ with unique $n_{ij} > 0$ by **(5.41)**(3). But $\mathfrak{p}_i$ is maximal. So $R_{\mathfrak{p}_i}/\mathfrak{p}_i^{n_{ij}}R_{\mathfrak{p}_i} = R/\mathfrak{p}_i^{n_{ij}}$ by **(12.34)**. Thus $M \simeq \bigoplus_{i,j} R/\mathfrak{p}_i^{n_{ij}}$. □

Exercise (24.24) . — Let R be a Dedekind domain; X a variable; $F, G \in R[X]$. Show $c(FG) = c(F)c(G)$.

Solution: By **(13.56)**, it suffices to show $c(FG)R_{\mathfrak{p}} = c(F)c(G)R_{\mathfrak{p}}$ for any given nonzero prime $\mathfrak{p}$. But $R_{\mathfrak{p}}$ is a DVR by **(24.6)**, so a UFD by **(23.1)**. So **(21.35)**(4) implies that $c(F)R_{\mathfrak{p}} = \langle f\rangle$ and $c(G)R_{\mathfrak{p}} = \langle g\rangle$ and $c(FG)R_{\mathfrak{p}} = \langle h\rangle$ where f, g, h are the gcd's of the coefficients of F, G, FG viewed in $R_{\mathfrak{p}}[X]$. But $fg = h$ by **(21.35)**(3). Thus $c(FG) = c(F)c(G)$, as desired. □

Exercise (24.25) . — Let k be an algebraically closed field, $P := k[X_1, \ldots, X_n]$ a polynomial ring, and $F_1, \ldots, F_m \in P$. Set $\mathfrak{P} := \langle F_1, \ldots, F_m\rangle$. For all i, j, define $\partial F_i/\partial X_j \in P$ formally as in **(1.18.1)**. Let $\mathfrak{A}$ be the ideal generated by $\mathfrak{P}$ and all the $n-1$ by $n-1$ minors M of the m by n matrix $(\partial F_i/\partial X_j)$. Set $R := P/\mathfrak{P}$. Assume R is a domain of dimension 1. Show R is Dedekind if and only if $1 \in \mathfrak{A}$.

Solution: Let $\mathfrak{M} \supset \mathfrak{P}$ be a maximal ideal of P. Since k is algebraically closed, $\mathfrak{M} = \langle X_1 - x_1, \ldots, X_n - x_n\rangle$ for some $\mathbf{x} := (x_1, \ldots, x_n) \in k^n$ by **(15.5)**.

Assume $1 \in \mathfrak{A}$. Then there's a minor $M \notin \mathfrak{M}$. So $M(\mathbf{x}) \neq 0$. So $((\partial F_i/\partial X_j)(\mathbf{x}))$ has rank at least $n-1$. But $\dim R_{\mathfrak{M}} = 1$ by **(15.12)**. Hence $R_{\mathfrak{M}}$ is regular by **(21.42)**1)(c)⇒(a), so a DVR by **(23.6)**. Thus **(24.6)** implies R is Dedekind.

Assume $1 \notin \mathfrak{A}$. Then there's an $\mathfrak{M} \supset \mathfrak{A}$. So $M(\mathbf{x}) = 0$ for every minor M. So $((\partial F_i/\partial X_j)(\mathbf{x}))$ has rank less than $n-1$. So $R_{\mathfrak{m}}$ is not regular by **(21.42)**(1). Thus **(24.6)** implies R is not Dedekind. □

25. Fractional Ideals

Exercise (25.2) . — Let R be a domain, M and N nonzero fractional ideals. Prove that M is principal if and only if there exists some isomorphism $M \simeq R$. Construct the following canonical surjection and canonical isomorphism:

$$\pi\colon M \otimes N \twoheadrightarrow MN \quad \text{and} \quad \alpha\colon (M : N) \xrightarrow{\sim} \operatorname{Hom}(N, M).$$

Solution: If $M \simeq R$, let x correspond to 1; then $M = Rx$. Conversely, assume $M = Rx$. Then $x \neq 0$ as $M \neq 0$. Form the map $R \to M$ with $a \mapsto ax$. It's surjective as $M = Rx$. It's injective as $x \neq 0$ and $M \subset \operatorname{Frac}(R)$.

Form the canonical map $M \times N \to MN$ with $(x, y) \mapsto xy$. It's bilinear. So it induces a map $\pi\colon M \otimes N \to MN$, and plainly π is surjective.

Define α as follows: given $z \in (M : N)$, define $\alpha(z)\colon N \to M$ by $\alpha(z)(y) := yz$. Clearly, α is R-linear. Say $y \neq 0$. Then $yz = 0$ implies $z = 0$; thus, α is injective.

Finally, given $\theta\colon N \to M$, fix a nonzero $n \in N$, and set $z := \theta(n)/n$. Given $y \in N$, say $y = a/b$ and $n = c/d$ with $a, b, c, d \in R$. Then $bcy = adn$. So $bc\theta(y) = ad\theta(n)$. Hence $\theta(y) = yz$. Therefore, $z \in (M : N)$ as $y \in N$ is arbitrary and $\theta(y) \in M$; further, $\theta = \alpha(z)$. Thus, α is surjective, as desired. □

Exercise (25.6) . — Let R be a domain, M and N fractional ideals. Prove that the map $\pi\colon M \otimes N \to MN$ of (**25.2**) is an isomorphism if M is locally principal.

Solution: By (**13.9**), it suffices to prove that, for each maximal ideal $\mathfrak{m}$, the localization $\pi_\mathfrak{m}\colon (M \otimes N)_\mathfrak{m} \to (MN)_\mathfrak{m}$ is bijective. But $(M \otimes N)_\mathfrak{m} = M_\mathfrak{m} \otimes N_\mathfrak{m}$ by (**12.30**), and $(MN)_\mathfrak{m} = M_\mathfrak{m} N_\mathfrak{m}$ by (**25.4**). By hypothesis, $M_\mathfrak{m} = R_\mathfrak{m} x$ for some x. Clearly $R_\mathfrak{m} x \simeq R_\mathfrak{m}$. And $R_\mathfrak{m} \otimes N_\mathfrak{m} = N_\mathfrak{m}$ by (**8.5**)(2). Thus $\pi_\mathfrak{m} \simeq 1_{N_\mathfrak{m}}$. □

Exercise (25.9) . — Let R be a domain, M and N fractional ideals. Prove this:

(1) Assume N is invertible. Then $(M : N) = M \cdot N^{-1}$.

(2) Both M and N are invertible if and only if their product MN is. If so, then $(MN)^{-1} = N^{-1}M^{-1}$.

Solution: For (1), note that $N^{-1} = (R : N)$ by (**25.8**). So $M(R : N)N = M$. Thus $M(R : N) \subset (M : N)$. Conversely, note that $(M : N)N \subset M$. Hence $(M : N) = (M : N)N(R : N) \subset M(R : N)$. Thus (1) holds.

In (2), if M and N are invertible, then $(MN)N^{-1}M^{-1} = MM^{-1} = R$; thus MN is invertible, and $N^{-1}M^{-1}$ is its inverse. Conversely, if MN is invertible, then $R = (MN)(MN)^{-1} = M(N(MN)^{-1})$; thus, M is invertible. Similarly, N is invertible. Thus (2) holds. □

Exercise (25.12) . — Let R be a UFD. Show that a fractional ideal M is invertible if and only if M is principal and nonzero.

Solution: By (**25.7**), a nonzero principal ideal is always invertible.

Conversely, assume M is invertible. Then trivially $M \neq 0$. Say $1 = \sum_{i=1}^r m_i n_i$ with $m_i \in M$ and $n_i \in M^{-1}$. Fix a nonzero $m \in M$.

Then $m = \sum_{i=1}^r m_i n_i m$. But $n_i m \in R$ as $m \in M$ and $n_i \in M^{-1}$. Set

$$d := \gcd\{n_i m\}_{i=1}^r \in R \quad \text{and} \quad x := \textstyle\sum_{i=1}^r (n_i m/d) m_i \in M.$$

Then $m = dx$.

Given $m' \in M$, write $m'/m = a/b$ where $a, b \in R$ are relatively prime. Then

$$d' := \gcd\{n_i m'\}_{i=1}^r = \gcd\{n_i m a/b\}_{i=1}^r = a \gcd\{n_i m\}_{i=1}^r / b = ad/b.$$

So $m' = (a/b)m = (ad/b)x = d'x$. But $d' \in R$. Thus $M = Rx$. □

Exercise (25.15) . — Show that it is equivalent for a ring R to be either a PID, a 1-dimensional UFD, or a Dedekind UFD.

Solution: If R is a PID, then R is a 1-dimensional UFD by **(2.17)**.

Assume R is a 1-dimensional UFD. Then every nonzero prime is of height 1, so principal by **(21.33)**. So R is Noetherian by **(16.8)**. Also R is normal by **(10.21)**. Thus R is Dedekind.

Finally, assume R is a Dedekind UFD. Then every nonzero ordinary ideal is invertible by **(25.14)**, so is principal by **(25.12)**. Thus R is a PID.

Alternatively and more directly, every nonzero prime is of height 1 as $\dim R = 1$, so is principal by **(21.33)**. But, by **(24.8)**, every nonzero ideal is a product of nonzero prime ideals. Thus again, R is a PID. □

Exercise (25.17) . — Let R be a ring, M an invertible module. Prove that M is finitely generated, and that, if R is local, then M is free of rank 1.

Solution: Say $\alpha\colon M \otimes N \xrightarrow{\sim} R$ and $1 = \alpha(\sum m_i \otimes n_i)$ with $m_i \in M$ and $n_i \in N$. Given $m \in M$, set $a_i := \alpha(m \otimes n_i)$. Form this composition:

$$\beta\colon M = M \otimes R \xrightarrow{\sim} M \otimes M \otimes N = M \otimes N \otimes M \xrightarrow{\sim} R \otimes M = M.$$

Then $\beta(m) = \sum a_i m_i$. So the m_i generate $\beta(M)$. But β is an isomorphism. Thus the m_i generate M.

Suppose R is local. Then $R - R^\times$ is an ideal. So $u := \alpha(m_i \otimes n_i) \in R^\times$ for some i. Set $m' := u^{-1} m_i$ and $n' := n_i$. Then $\alpha(m' \otimes n') = 1$. Thus $\beta(m) = \alpha(m \otimes n')m'$.

Define $\nu\colon M \to R$ by $\nu(m) := \alpha(m \otimes n')$. Then $\nu(m') = 1$; so ν is surjective. Define $\mu\colon R \to M$ by $\mu(x) := xm'$. Then $\mu\nu(m) = \nu(m)m' = \beta(m)$, or $\mu\nu = \beta$. But β is an isomorphism. So ν is injective. Thus ν is an isomorphism, as desired. □

Exercise (25.18) . — Show these conditions on an R-module M are equivalent:

(1) M is invertible.
(2) M is finitely generated, and $M_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ at each maximal ideal $\mathfrak{m}$.
(3) M is locally free of rank 1.

Assuming the conditions, show M is finitely presented and $M \otimes \operatorname{Hom}(M, R) = R$.

Solution: Assume (1). Then M is finitely generated by **(25.17)**. Further, say $M \otimes N \simeq R$. Let $\mathfrak{m}$ be a maximal ideal. Then $M_{\mathfrak{m}} \otimes N_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$. Hence $M_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ again by **(25.17)**. Thus (2) holds.

Conditions (2) and (3) are equivalent by **(13.62)**.

Assume (3). Then (2) holds; so $M_{\mathfrak{m}} \simeq R_{\mathfrak{m}}$ at any maximal ideal $\mathfrak{m}$. Also, M is finitely presented by **(13.15)**; so $\operatorname{Hom}_R(M, R)_{\mathfrak{m}} = \operatorname{Hom}_{R_{\mathfrak{m}}}(M_{\mathfrak{m}}, R_{\mathfrak{m}})$ by **(12.19)**.

Consider the evaluation map

$$\operatorname{ev}(M, R)\colon M \otimes \operatorname{Hom}(M, R) \to R \quad \text{defined by} \quad \operatorname{ev}(M, R)(m, \alpha) := \alpha(m).$$

Plainly, $\operatorname{ev}(M, R)_{\mathfrak{m}} = \operatorname{ev}(M_{\mathfrak{m}}, R_{\mathfrak{m}})$. Plainly, $\operatorname{ev}(R_{\mathfrak{m}}, R_{\mathfrak{m}})$ is bijective. So $\operatorname{ev}(M, R)$ is bijective by **(13.9)**. Thus the last assertions hold; in particular, (1) holds. □

Exercise (25.23) . — Let R be a Dedekind domain, S a multiplicative subset. Prove $M \mapsto S^{-1}M$ induces a surjective group map $\pi\colon \operatorname{Pic}(R) \to \operatorname{Pic}(S^{-1}R)$.

Solution: First, assume $S^{-1}R = \mathrm{Frac}(R)$. Since $\mathrm{Frac}(R)$ is a field, plainly $\mathrm{Pic}(S^{-1}R) = 0$. Thus, trivially, π is a surjective group map.

So assume $S^{-1}R \neq \mathrm{Frac}(R)$. By **(24.5)**, then $S^{-1}R$ is Dedekind.

Given fractional ideals M and N of R, note $(S^{-1}M)(S^{-1}N) = S^{-1}(MN)$ by **(25.4)**. So if $MN = R$, then $(S^{-1}M)(S^{-1}N) = S^{-1}R$; in other words, if M is invertible, so is $S^{-1}M$. Thus $M \mapsto S^{-1}M$ defines a map $\mathcal{F}(R) \to \mathcal{F}(S^{-1}R)$, and as noted, this map preserves multiplication; in other words, it's a group map.

Suppose $M = xR$ for some nonzero $x \in K$. Then $S^{-1}M = xS^{-1}R$. Thus $M \mapsto S^{-1}M$ carries $\mathcal{P}(R)$ into $\mathcal{P}(S^{-1}R)$, so induces a group map on the quotients, namely, $\pi\colon \mathrm{Pic}(R) \to \mathrm{Pic}(S^{-1}R)$.

Finally, given $P \in \mathcal{F}(S^{-1}R)$, note P is finitely generated over $S^{-1}R$ by **(25.10)**. So there's a nonzero $y \in S^{-1}R$ with $yP \subset S^{-1}R$ by **(25.3)**. Hence there's a nonzero ordinary ideal $\mathfrak{a}$ of R with $S^{-1}\mathfrak{a} = yP$ by **(11.12)**(1). Since R is Dedekind, $\mathfrak{a}$ is invertible by **(25.20)**. Thus $\mathcal{F}(R) \to \mathcal{F}(S^{-1}R)$ is surjective, so π is too. □

26. Arbitrary Valuation Rings

Exercise (26.3) . — Prove that a valuation ring V is normal.

Solution: Set $K := \mathrm{Frac}(V)$, and let $\mathfrak{m}$ be the maximal ideal. Take $x \in K$ integral over V, say $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with $a_i \in V$. Then

$$1 + a_1x^{-1} + \cdots + a_nx^{-n} = 0. \qquad \mathbf{(26.3.1)}$$

If $x \notin V$, then $x^{-1} \in \mathfrak{m}$ by **(26.2)**. So **(26.3.1)** yields $1 \in \mathfrak{m}$, a contradiction. Hence $x \in V$. Thus V is normal. □

Exercise (26.11) . — Let V be a valuation ring. Prove these statements:

(1) Every finitely generated ideal $\mathfrak{a}$ is principal.

(2) V is Noetherian if and only if V is a DVR.

Solution: To prove (1), say $\mathfrak{a} = \langle x_1, \ldots, x_n\rangle$ with $x_i \neq 0$ for all i. Let v be the valuation. Suppose $v(x_1) \le v(x_i)$ for all i. Then $x_i/x_1 \in V$ for all i. So $x_i \in \langle x_1\rangle$. Hence $\mathfrak{a} = \langle x_1\rangle$. Thus (1) holds.

To prove (2), first assume V is Noetherian. Then V is local by **(26.2)**, and by (1) its maximal ideal $\mathfrak{m}$ is principal. Hence V is a DVR by **(23.6)**. Conversely, assume V is a DVR. Then V is a PID by **(23.1)**, so Noetherian. Thus (2) holds. □

Exercise (26.16) . — Let V be a domain. Show that V is a valuation ring if and only if, given any two ideals $\mathfrak{a}$ and $\mathfrak{b}$, either $\mathfrak{a}$ lies in $\mathfrak{b}$ or $\mathfrak{b}$ lies in $\mathfrak{a}$.

Solution: First, suppose V is a valuation ring. Suppose also $\mathfrak{a} \not\subset \mathfrak{b}$; say $x \in \mathfrak{a}$, but $x \notin \mathfrak{b}$. Take $y \in \mathfrak{b}$. Then $x/y \notin V$; else $x = (x/y)y \in \mathfrak{b}$. So $y/x \in V$. Hence $y = (y/x)x \in \mathfrak{a}$. Thus $\mathfrak{b} \subset \mathfrak{a}$.

Conversely, let $x, y \in V - \{0\}$, and suppose $x/y \notin V$. Then $\langle x\rangle \not\subset \langle y\rangle$; else, $x = wy$ with $w \in V$. Hence $\langle y\rangle \subset \langle x\rangle$ by hypothesis. So $y = zx$ for some $z \in V$; in other words, $y/x \in V$. Thus V is a valuation ring. □

Exercise (26.17) . — Let V be a valuation ring of K, and $V \subset W \subset K$ a subring. Prove that W is also a valuation ring of K, that its maximal ideal $\mathfrak{p}$ lies in V, that $V/\mathfrak{p}$ is a valuation ring of the field $W/\mathfrak{p}$, and that $W = V_{\mathfrak{p}}$.

Solution: First, let $x \in K - W \subset K - V$. Then $1/x \in V \subset W$. Thus W is a valuation ring of K.

Second, let $y \in \mathfrak{p}$. Then **(26.2)** implies $1/y \in K - W \subset K - V$. So $y \in V$.

Third, $x \in W - V$ implies $1/x \in V$; whence, $V/\mathfrak{p}$ is a valuation ring of $W/\mathfrak{p}$.

Fourth, $V_\mathfrak{p} \subset W_\mathfrak{p} = W$. Conversely, let $x \in W - V$. Then $1/x \in V$. But $1/x \notin \mathfrak{p}$ as $\mathfrak{p}$ is the maximal ideal of W. So $x \in V_\mathfrak{p}$. Thus $W = V_\mathfrak{p}$. □

Exercise (26.18) . — Let K be a field, $\mathcal{S}$ the set of local subrings ordered by domination. Show that the valuation rings of K are the maximal elements of $\mathcal{S}$.

Solution: Given a valuation ring V of K, note $V \in \mathcal{S}$ by **(26.2)**. Given $W \in \mathcal{S}$ dominating V, let $\mathfrak{m}$ and $\mathfrak{n}$ be the maximal ideals of V and W.

Given any nonzero $x \in W$, note $1/x \notin \mathfrak{n}$ as $x(1/x) = 1 \notin \mathfrak{n}$. So also $1/x \notin \mathfrak{m}$. So $x \in V$ by **(26.2)**. Hence, $W = V$. Thus V is maximal.

Alternatively, $\mathfrak{n} \subset V$ and $W = V_\mathfrak{n}$ by **(26.17)**. But $\mathfrak{n} \supset \mathfrak{m}$ as W dominates V. So $\mathfrak{n} = \mathfrak{m}$. Hence, $W = V$. Thus V again is maximal.

Conversely, let $V \in \mathcal{S}$ be maximal. By **(26.6)**, V is dominated by a valuation ring W of K. By maximality, $V = W$. □

Exercise (26.19) . — Let V be a valuation ring of a field K. Let $\varphi\colon V \to R$ and $\psi\colon R \to K$ be ring maps. Assume $\operatorname{Spec}(\varphi)$ is closed and $\psi\varphi\colon V \to K$ is the inclusion. Set $W := \psi(R)$. Show $W = V$.

Solution: Since $\psi\varphi\colon V \to K$ is the inclusion, $V \subset W \subset K$. So W is also a valuation ring, its maximal ideal $\mathfrak{p}$ lies in V, and $W = V_\mathfrak{p}$ by **(26.17)**.

Set $\mathfrak{m} := \psi^{-1}\mathfrak{p}$. Then $\mathfrak{m}$ is a maximal ideal of R, as $W := \psi(R)$. So $\{\mathfrak{m}\}$ is a closed subset of $\operatorname{Spec}(R)$ by **(13.16)**(2). But $\operatorname{Spec}(\varphi)$ is closed. So $\{\varphi^{-1}\mathfrak{m}\}$ is a closed subset of $\operatorname{Spec}(V)$. So $\varphi^{-1}\mathfrak{m}$ is the maximal ideal of V by **(13.16)**(2). But $\varphi^{-1}\mathfrak{m} = \varphi^{-1}\psi^{-1}\mathfrak{p} = \mathfrak{p} \cap V = \mathfrak{p}$. So $V_\mathfrak{p} = V$. Thus $W = V$. □

Exercise (26.20) . — Let $\varphi\colon R \to R'$ be a map of rings. Prove that, if R' is integral over R, then for any R-algebra C, the map $\operatorname{Spec}(\varphi \otimes_R C)$ is closed; further, the converse holds if also R' has only finitely many minimal primes. To prove the converse, start with the case where R' is a domain, take C to be an arbitrary valuation ring of $\operatorname{Frac}(R')$ containing $\varphi(R)$, and apply **(26.19)**.

Solution: First, assume R' is integral over R. Then $R' \otimes_R C$ is integral over C by **(10.39)**(1). Thus **(14.11)** implies that $\operatorname{Spec}(\varphi \otimes_R C)$ is closed.

For the converse, replacing R by $\varphi(R)$, we may assume $\varphi\colon R \hookrightarrow R'$ is an inclusion.

First, assume R' is a domain. Set $K := \operatorname{Frac}(R')$. By **(26.7)**, the integral closure of R in K is the intersection of all valuation rings V of K containing R. So given a V, it suffices to show $R' \subset V$. By hypothesis, $\operatorname{Spec}(\varphi \otimes_R V)$ is closed. Define $\psi\colon R' \otimes_R V \to K$ by $\psi(x \otimes y) = xy$. Then $\psi \circ (\varphi \otimes_R V)\colon V \to K$ is the inclusion. So **(26.19)** yields $\psi(R' \otimes_R V) = V$. Thus $R' \subset V$, as desired.

To derive the general case, let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the minimal primes of R', and $\kappa_i\colon R' \to R'/\mathfrak{p}_i$ the quotient map. Given any R-algebra C, note that $\kappa_i \otimes_R C$ is surjective. So $\operatorname{Spec}(\kappa_i \otimes_R C)$ is closed by **(13.1.7)**. But a composition of closed maps is closed. So by the first case, each $R'/\mathfrak{p}_i$ is integral over R. Thus **(10.42)**(1) implies that $\prod_{i=1}^r R'/\mathfrak{p}_i$ is integral over R.

Set $\mathfrak{N} := \bigcap_{i=1}^r \mathfrak{p}_i$. Then the canonical map $R'/\mathfrak{N} \to \prod_{i=1}^r R'/\mathfrak{p}_i$ is injective. So $R'/\mathfrak{N}$ is integral over R. So given any $x \in R'$, there are $a_i \in R$ and $n \geq 1$ with

$y := x^n + a_1x^{n-1} + \cdots + a_n \in \mathfrak{N}$. But $\mathfrak{N}$ is the nilradical of R' by **(3.17)**. So $y^m = 0$ for some $m \geq 1$. Thus x is integral over R, as desired. □

Exercise (26.21) . — Let V be a valuation ring with valuation $v\colon K^\times \to \Gamma$, and $\mathfrak{p}$ a prime of V. Set $\Delta := v(V_\mathfrak{p}^\times)$. Prove the following statements:

(1) Δ and Γ/Δ are the value groups of the valuation rings $V/\mathfrak{p}$ and $V_\mathfrak{p}$.
(2) $v(V - \mathfrak{p})$ is the set of nonegative elements $\Delta_{\geq 0}$ of Δ, and $\mathfrak{p} = V - v^{-1}\Delta_{\geq 0}$.
(3) Δ is **isolated** in Γ; that is, given $\alpha \in \Delta$ and $0 \leq \beta \leq \alpha$, also $\beta \in \Delta$.

Solution: For (1), set $L := V_\mathfrak{p}/\mathfrak{p}V_\mathfrak{p}$. Note that $\mathfrak{p} = \mathfrak{p}V_\mathfrak{p}$ and that $V/\mathfrak{p}$ and $V_\mathfrak{p}$ are valuation rings of L and K by **(26.17)** with $W := V_\mathfrak{p}$.

By definition, the value group of $V/\mathfrak{p}$ is $L^\times/(V/\mathfrak{p})^\times$. Let's see that the latter is equal to Δ. Form the quotient map $\kappa\colon V_\mathfrak{p} \to L$. Note $V_\mathfrak{p} - \mathfrak{p} = \kappa^{-1}(L - 0)$. But $V_\mathfrak{p} - \mathfrak{p} = V_\mathfrak{p}^\times$ and $L - 0 = L^\times$. So κ induces a surjection $\sigma\colon V_\mathfrak{p}^\times \twoheadrightarrow L^\times$. Moreover, as κ is a ring map, σ is a homorphism of multiplicative groups.

Let $\mathfrak{m}$ be the maximal ideal of V. Then $V - \mathfrak{m} = \kappa^{-1}((V/\mathfrak{p}) - (\mathfrak{m}/\mathfrak{p}))$. But $V - \mathfrak{m} = V^\times$ and $(V/\mathfrak{p}) - (\mathfrak{m}/\mathfrak{p}) = (V/\mathfrak{p})^\times$. So $V^\times = \sigma^{-1}(V/\mathfrak{p})^\times$. So σ induces an isomorphism $V_\mathfrak{p}^\times/V^\times \xrightarrow{\sim} L^\times/(V/\mathfrak{p})^\times$. Thus the value group of $V/\mathfrak{p}$ is equal to $V_\mathfrak{p}^\times/V^\times$, which is just Δ.

The value group of $V_\mathfrak{p}$ is $K^\times/V_\mathfrak{p}^\times$. Form the canonical map $K^\times/V^\times \to K^\times/V_\mathfrak{p}^\times$. It is surjective, its source is Γ, and its kernel is $V_\mathfrak{p}^\times/V^\times$, or Δ. Thus (1) holds.

For (2), recall $\Gamma_{\geq 0} := v(V - 0)$. But $\Delta_{\geq 0} := v(V_\mathfrak{p}^\times) \cap \Gamma_{\geq 0}$. Thus $\Delta_{\geq 0} \supset v(V - \mathfrak{p})$.

Conversely, given $\alpha \in \Delta_{\geq 0}$, say $\alpha = v(x)$ with $x \in V_\mathfrak{p}^\times$ and $\alpha = v(y)$ with $y \in V - 0$. Then $v(x) = v(y)$. So $x = yu$ with $u \in V^\times$. So $x \in V$. But x isn't in the maximal ideal of $V_\mathfrak{p}$, which is $\mathfrak{p}$ by **(26.17)**. Thus $x \in V - \mathfrak{p}$. Thus $\Delta_{\geq 0} = v(V - \mathfrak{p})$.

So $V - \mathfrak{p} \subset v^{-1}\Delta_{\geq 0}$. Conversely, given $x \in K^\times$ with $v(x) \in \Delta_{\geq 0}$, say $v(x) = v(y)$ with $y \in V - \mathfrak{p}$. Then $x = yu$ with $u \in V^\times$. So $x \in V - \mathfrak{p}$. Thus $V - \mathfrak{p} = v^{-1}\Delta_{\geq 0}$. Thus (2) holds.

For (3), given $\alpha \in \Delta$ and $0 \leq \beta \leq \alpha$, say $\alpha = v(x)$ with $x \in V - \mathfrak{p}$ owing to (2) and say $\beta = v(y)$ with $y \in V - 0$. But $\alpha - \beta \geq 0$. So $v(x/y) \geq 0$. So $x/y \in V$, or $x \in yV$. But $x \notin \mathfrak{p}$. So $y \notin \mathfrak{p}$. So $y \in V_\mathfrak{p}^\times$. Thus $\beta \in \Delta$. Thus (3) holds. □

Exercise (26.22) . — Let V be a valuation ring with valuation $v\colon K^\times \to \Gamma$. Prove that $\mathfrak{p} \mapsto v(V_\mathfrak{p}^\times)$ is a bijection γ from the primes $\mathfrak{p}$ of V onto the isolated subgroups Δ of Γ and that its inverse is $\Delta \mapsto V - v^{-1}\Delta_{\geq 0}$.

Solution: The $v(V_\mathfrak{p}^\times)$ are isolated by **(26.21)**(3). So γ is well defined. It is injective owing to **(26.21)**(2). Let's prove it is surjective and find its inverse.

Given an isolated subgroup Δ, set $\mathfrak{p} := V - v^{-1}\Delta_{\geq 0}$. Let's check that $\mathfrak{p}$ is an ideal. Given nonzero $x, y \in \mathfrak{p}$ and $z \in V$, note $v(x), v(y), v(z) \geq 0$. Suppose $x + yz \neq 0$. Then **(26.8.2)** and **(26.8.1)** yield

$$v(x + yz) \geq \min\{v(x), v(yz)\} = \min\{v(x), v(y) + v(z)\} \geq \min\{v(x), v(y)\} \geq 0.$$

But $x, y \in \mathfrak{p}$, so $v(x), v(y) \notin \Delta$. But Δ is isolated. So $v(x+yz) \notin \Delta$. So $x+yz \in \mathfrak{p}$. Thus $\mathfrak{p}$ is an ideal.

Let's check $\mathfrak{p}$ is prime. Given $x, y \in V - \mathfrak{p}$, note $v(x), v(y) \in \Delta_{\geq 0}$. But $\Delta_{\geq 0}$ is a semigroup. So $v(xy) = v(x) + v(y) \in \Delta_{\geq 0}$. Thus $xy \in V - \mathfrak{p}$. Thus $\mathfrak{p}$ is prime.

Finally, **(26.21)**(2) now implies that $v(V - \mathfrak{p}) = v(V_\mathfrak{p}^\times)_{\geq 0}$. But $v(V - \mathfrak{p}) = \Delta_{\geq 0}$ by definition of $\mathfrak{p}$. Thus $v(V_\mathfrak{p}^\times) = \Delta$, as desired. □

Exercise (26.23) . — Let V be a valuation ring, such as a DVR, whose value group Γ is **Archimedean**; that is, given any nonzero $\alpha, \beta \in \Gamma$, there's $n \in \mathbb{Z}$ such that $n\alpha > \beta$. Show that V is a maximal proper subring of its fraction field K.

Solution: Let R be a subring of K strictly containing V, and fix $a \in R - V$. Given $b \in K$, let α and β be the values of a and b. Then $\alpha < 0$. So, as Γ is Archimedean, there's $n > 0$ such that $-n\alpha > -\beta$. Then $v(b/a^n) > 0$. So $b/a^n \in V$. So $b = (b/a^n)a^n \in R$. Thus $R = K$. □

Exercise (26.24) . — Let R be a Noetherian domain, $K := \operatorname{Frac}(R)$, and L a finite extension field (possibly $L = K$). Prove the integral closure $\overline{R}$ of R in L is the intersection of all DVRs V of L containing R by modifying the proof of **(26.7)**: show y is contained in a height-1 prime $\mathfrak{p}$ of $R[y]$ and apply **(26.14)** to $R[y]_{\mathfrak{p}}$.

Solution: Every DVR V is normal by **(23.6)**. So if V is a DVR of L and $V \supset R$, then $V \supset \overline{R}$. Thus $\bigcap_{V \supset R} V \supset \overline{R}$.

To prove the opposite inclusion, take any $x \in K - \overline{R}$. To find a DVR V of L with $V \supset R$ and $x \notin V$, set $y := 1/x$. If $1/y \in R[y]$, then for some n,

$$1/y = a_0 y^n + a_1 y^{n-1} + \cdots + a_n \quad \text{with} \quad a_\lambda \in R.$$

Multiplying by x^n yields $x^{n+1} - a_n x^n - \cdots - a_0 = 0$. So $x \in \overline{R}$, a contradiction.

Thus y is a nonzero nonunit of $R[y]$. Also, $R[y]$ is Noetherian by the Hilbert Basis Theorem **(16.10)**. So y lies in a height-1 prime $\mathfrak{p}$ of $R[y]$ by the Krull Principal Ideal Theorem **(21.9)**. Then $R[y]_{\mathfrak{p}}$ is Noetherian of dimension 1.

However, L/K is a finite field extension; so $L/\operatorname{Frac}(R[y])$ is one too. Hence the integral closure R' of $R[y]_{\mathfrak{p}}$ in L is a Dedekind domain by **(26.14)**. So by the Going-up Theorem **(14.3)**(3), there's a prime $\mathfrak{q}$ of R' lying over $\mathfrak{p}R[y]_{\mathfrak{p}}$. Then as R' is Dedekind, $R'_{\mathfrak{q}}$ is a DVR of L by **(24.6)**. Further, $y \in \mathfrak{q}R'_{\mathfrak{q}}$. Thus $x \notin R'_{\mathfrak{q}}$, as desired. □

References

[1] Alon, N., *Combinatorial Nullstellensatz,* Combin. Probab. Comput., **8.1–2** (1999), 7–29.

[2] Artin, E., and Tate, J. T., *A note on finite ring extensions,* J. Math. Soc. Japan, **3.1** (1951), 74–77.

[3] Artin, M., "Algebra," Prentice-Hall, 1991.

[4] Atiyah, M., and Macdonald, I., "Introduction to Commutative Algebra," Addison-Wesley, 1969.

[5] Cox, D., Little, J., and O'Shea, D., "Ideals, Varieties, and Algorithms," Second edition. Springer-Verlag, 1997

[6] Eisenbud, D., "Commutative Algebra with a View Toward Algebraic Geometry," Springer-Verlag, 1999.

[7] Fritzsche, K.; Grauert, H., "From holomorphic functions to complex manifolds." Graduate Texts in Mathematics, **213**. Springer-Verlag, 2002.

[8] Gabber, O.; Romero, L., "Almost Ring Theory," Lect. Notes Math. **1800**, Springer-Verlag, 2003.

[9] Grothendieck, A., and Dieudonné, J., "Eléments de Géométrie Algébrique I," Grundlehren **166**, Springer-Verlag, 1971.

[10] Hartshorne, R., "Algebraic Geometry" Graduate Texts in Mathematics **52**, Springer-Verlag, 1977.

[11] Judson, T., "Abstract algebra: theory and applications," Open source, Electronic Book, http://abstract.ups.edu, 2011/11/08.

[12] Lang, S., "Complex analysis," Third edition. Graduate Texts in Mathematics, 103. Springer-Verlag, New York, 1993.

[13] Lang, S., 'Undergraduate analysis," Second edition. Undergraduate Texts in Mathematics. Springer-Verlag, 1997.

[14] Lang, S., "Algebra" Graduate Texts in Mathematics **211**, Springer-Verlag, 2002.

[15] Munkres, J., "Topology: a first course," Prentice-Hall, 1975,

[16] Reid, M., "Undergraduate Commutative Algebra," Cambridge University Press, 1995.

[17] Stark H., "An Introduction to Number Theory," MIT Press, 1978.

[18] Zariski, O., and Samuel, P., "Commutative Algebra," Vol. I, D. Van Nostrand Co., 1958.

Disposition of the Exercises in [4]

Chapter 1, text

1.12, p. 8,— Essentially (**4.16**)
1.13, p. 9,— Essentially (**3.13**) and (**3.32**)
1.18, p. 10,— Essentially (**1.13**) and (**3.39**)

Chapter 1, pp. 10–16

1.— Essentially (**3.2**), owing to (**3.13.1**).
2.— Essentially (**3.42**) and (**4.20**) and (**2.36**)(2)
3.— Essentially (**3.43**) and (**8.32**) and (**2.36**)(2)
4.— Contained in (**3.44**)(2)
5.— Contained in (**3.7**), (**3.19**), and (**3.20**)
6.— Essentially (**3.33**)(1)
7.— Essentially (**2.38**)
8.— Contained in (**3.16**)
9.— Essentially (**3.14**)
10.— Essentially (**3.37**)
11.— Contained in (**1.2**), (**2.37**), and (**1.24**)(5)
12.— Essentially (**3.22**)
13.— Essentially (**14.13**)
14.— Essentially (**2.26**)
15.— Contained in (**13.1**)
16.— Essentially (**13.17**) and (**16.68**)
17.— Contained in (**13.1**), (**13.2**), (**13.39**), and (**13.41**)
18.— Essentially (**13.16**)
19.— Essentially (**16.49**)
20.— Contained in (**16.50**), (**16.69**), and (**16.51**)(3)
21.— Contained in (**13.1**), (**13.1.6**), and (**13.36**), and (**13.35**)
22.— Essentially contained in (**13.18**), (**1.12**), and (**13.1**)
23.— Essentially (**13.43**), and (**1.24**)(5)
24.— Essentially (**1.25**), (**1.26**), (**1.27**), and (**1.28**)
25.— Essentially (**13.44**)
26.— Essentially (**14.26**)
27.— Contained in (**1.29**)(1), (**1.17**)(2),(3), (**2.13**), and (**15.5**)
28.— Contained in (**1.29**)

Chapter 2, text

2.2, p. 20,— Contained in (**4.17**)
2.15, p. 27— Contained in (**8.8**)
2.20, p. 29— Contained in (**9.22**)

Chapter 2, pp. 31–35

1.— Essentially (**8.29**)
2.— Essentially (**8.27**)(1)
3.— Essentially (**10.10**)(2)
4.— Contained in (**9.5**)
5.— Contained in (**9.20**)
6.— Essentially (**8.31**)
7.— Contained in (**2.32**)
8.— i) Contained in (**9.21**)
ii) Contained in (**9.23**)
9.— Essentially (**5.5**)
10.— Essentially (**10.27**)
11.— Contained in (**10.5**)(2), (**8.25**), and (**5.32**)
12.— Immediate from (**5.15**), (**5.16**), and (**5.7**)
13.— Contained in (**8.21**)
14.— Contained in (**7.4**)
15.— Contained in (**7.5**)
16.— Essentially (**6.4**)
17.— Essentially (**7.2**), and (**7.11**)
18.— Essentially (**6.4**)
19.— Essentially (**7.9**)
20.— Essentially (**8.10**)
21.— Contained in (**7.4**) and (**7.16**)(1)
22.— Essentially (**7.20**), and (**7.16**)(2)
23.— Essentially (**8.33**)
24.— Essentially (**9.15**)
25.— Essentially (**9.8**)(2)
26.— Essentially (**9.15**)
27.— Contained in (**10.25**)
28.— Essentially (**10.26**), and (**2.38**) and (**13.22**)

Chapter 3, text

3.0, p. 37,— Essentially (**11.1**)

Chapter 3, pp. 43–49

1.— Essentially (**12.17**)(2)
2.— Essentially (**12.27**)
3.— Contained in (**12.26**)(2) and (3)
4.— Essentially (**11.15.1**)
5.— Essentially (**13.57**)
6.— Essentially (**3.26**)
7.— Contained in (**3.24**) and (**3.25**)
8.— Essentially (**11.23**) and (**3.25**)
9.— Essentially (**2.26**), (**14.7**), and (**11.26**)
10.— Essentially (**13.21**)
11.— Essentially (**13.22**) and (**13.2**)
12.— Contained in (**12.38**)
13.— Contained in (**12.38**) and (**13.52**)
14.— Essentially (**13.54**)
15.— Essentially (**10.5**) or (**5.32**)(2)
16.— Essentially (**9.28**) and (**13.47**)
17.— Essentially (**9.25**)
18.— Essentially (**13.48**)

19.— i) essentially (**13.8**) and (**13.1**);
iii), iv), v) contained in (**13.4**);
vi) essentially (**13.7**);
ii), vii) essentially (**13.46**);
viii) essentially (**13.49**)
20.— Essentially (**13.24**),
21.— i) essentially (**13.25**);
ii) (**13.26**);
iii) (**13.27**);
iv) (**13.28**)
22.— Essentially (**13.29**)
23.— Essentially (**13.39**) and (**13.40**)
24.— Essentially (**13.42**)(2)
25.— Essentially (**13.30**)
26.— Essentially (**13.31**)
27.— Essentially (**13.32**)
28.— Contained in (**13.33**)
29.— Essentially (**13.34**)
30.— Essentially (**13.33**)(4)

Chapter 4, pp. 55–58

1.— Essentially (**18.49**)(2)
2.— Contained in (**18.32**)(1)
3.— Essentially (**18.51**)
4.— Essentially (**18.28**)
5.— Essentially (**18.29**)
6.— Essentially (**18.52**)
7.— Essentially (**1.15**)(1), (**2.32**)(1), and (**18.53**)
8.— Essentially (**18.54**)
9.— Contained in (**18.39**)
10.— Contained in (**18.50**), (**18.55**), (**12.12**)(8), and (**18.39**)(2)
11.— Essentially (**18.56**)
12.— Contained in (**12.12**)(6a),(4a), (**12.41**), and (**18.57**)
13.— Contained in (**18.58**)
14.— Essentially (**17.9**)
15.— Essentially (**18.59**)
16.— Contained in (**18.47**)
17.— Essentially (**18.41**)(2)
18.— Contained in (**18.44**)
19.— Essentially (**18.50**) and (**18.61**)
20.— Essentially (**4.17**)(2) and (**12.22**) and (**12.42**) and (**18.58**)(2)
21.— Essentially (**18.62**) and (**18.3**)(2) and (**18.12**)(1) and (**4.17**)(4) and (**18.38**)
22.— Essentially (**18.39**)(4)
23.— Contained in (**18.49**)(1) and (**18.37**)(6) and (**12.23**) and (**18.43**) and (**18.46**) and (**18.47**) and (**18.48**)

Chapter 5, pp. 67–73

1.— Essentially (**14.11**)
2.— Essentially (**14.12**)
3.— Contained in (**10.39**)
4.— Essentially (**14.17**)
5.— Essentially (**14.10**)
6.— Essentially (**10.41**)
7.— Essentially (**10.38**)
8.— Essentially (**14.4**)
9.— Essentially (**15.17**)
10.— Essentially (**13.37**) and (**13.38**)
11.— Essentially (**14.8**)
12.— Essentially (**10.35**) and (**11.22**)
13.— Essentially (**14.18**)
14.— Essentially (**10.36**) and (**10.37**)
15.— Essentially (**14.19**)
16.— Contained in (**15.1**) and (**15.2**)
17.— Contained in (**15.5**)
18.— Essentially (**15.4**)
19.— Contained in (**15.5**)
20.— Essentially (**15.3**)
21.— Essentially (**15.19**)
22.— Contained in (**15.20**)
23.— Contained in (**15.33**) and (**15.44**)
24.— Essentially (**15.37**)(2), and (**15.46**)
25.— Essentially (**15.43**)
26.— Essentially (**15.39**), and (**15.40**)
27.— Essentially (**26.18**)
28.— Essentially (**26.16**), and part of (**26.17**)
29.— Contained in (**26.17**)
30.— Contained in (**26.8**)
31.— Contained in (**26.8**)
32.— Essentially (**26.21**), and (**26.22**)
33.— Essentially (**26.9**)
34.— Essentially (**26.19**)
35.— Essentially (**26.20**)

Chapter 6, pp. 78–79

1.— Essentially (**10.4**), and (**16.46**)
2.— Contained in (**16.11**)
3.— Essentially (**16.47**)
4.— Contained in (**16.16**) and (**16.44**)
5.— Essentially (**16.53**)
6.— Essentially (**16.70**)
7.— Essentially (**16.54**) and (**16.55**)
8.— Essentially (**16.56**) and (**16.58**)
9.— Contained in (**16.51**)(3) and (**16.55**)
10.— Essentially (**16.72**)
11.— Essentially (**16.59**)
12.— Essentially (**16.56**)(2) and (**16.57**)

Chapter 7, pp. 84–88

1.— Essentially (**16.8**)
2.— Essentially (**16.25**)
3.— Contained in (**18.34**)
4.— Essentially (**16.31**)
5.— Essentially (**16.18**)
6.— Essentially (**15.41**)
7.— Follows easily from (**16.10**)
8.— Essentially (**16.26**)
9.— Essentially (**16.29**)
10.— Essentially (**16.32**)
11.— Essentially (**16.67**)

12.— Essentially (**16.28**)
13.— Essentially (**16.71**)
14.— Essentially (**15.21**)
15.— Essentially (**10.12**), and (**9.15**)
16.— Contained in (**13.15**)
17.— Contained in (**18.33**)
18.— Contained in (**18.18**), (**17.3**), and (**17.16**)
19.— Contained in (**18.18**) and (**18.34**)
20.— Essentially (**16.63**) and (**16.64**)
21.— Essentially (**16.65**)
22.— Essentially (**16.73**)
23.— Essentially (**16.66**)
24.— Essentially (**16.74**)
25.— Contained in (**16.75**)
26.— Contained in (**17.34**)
27.— Essentially (**17.35**)

Chapter 8, pp. 91–92

1.— Essentially (**18.58**)(5), and (**18.67**)
2.— Essentially (**19.20**)
3.— Essentially (**19.17**)
4.— Essentially (**19.21**)
5.— Essentially (**19.25**)
6.— Essentially (**19.16**)

Chapter 9, p. 99

1.— Essentially (**24.5**) and (**25.23**)
2.— Essentially (**24.24**)
3.— Essentially (**26.11**)(2)
4.— Essentially (**23.3**)
5.— Contained in (**25.21**)
6.— Essentially (**24.23**)
7.— Essentially (**24.22**)
8.— Essentially (**24.19**)
9.— Essentially (**24.20**)

Chapter 10, pp. 113–115

1.— Contained in (**22.48**)
2.— Essentially (**22.49**)
3.— Essentially (**22.37**)
4.— Contained in (**22.45**) and (**22.46**)
5.— Essentially (**22.43**)(1)
6.— Contained in (**22.35**)
7.— Contained in (**22.36**)
8.— Essentially (**22.67**)
9.— Essentially (**22.75**)
10.— Contained in (**22.76**) and (**22.83**) and (**22.90**)
11.— Essentially (**22.71**)
12.— Essentially (**22.65**)

Chapter 11, pp. 125–126

1.— Contained in (**21.42**)
2.— Essentially (**22.60**)
3.— Essentially (**15.10**) with (**15.12**)
4.— Essentially (**16.30**)
5.— Essentially (**20.34**)
6.— Essentially (**15.32**)
7.— Essentially (**21.41**)

Use of the Exercises in this Book

List of Abbreviations

Cor.= Corollary	Ex.= Exercise	Prp.= Proposition	Sbs.= Subsection
Eg.= Example	Lem.= Lemma	Rmk.= Remark	Thm.= Theorem

"Ap" in front of any of the above indicates the subsection is in an appendix.

NOTE: an exercise is indexed only if it's used later.

Ex. (3.24) is used in Ex. (2.26), Ex. (3.25), Ex. (3.26), and Ex. (13.40).
Ex. (3.25) is used in Ex. (3.26), Ex. (11.23), Ex. (11.24), Ex. (13.39), and Ex. (13.40).
Ex. (3.27) is used in Ex. (16.30).
Ex. (3.28) is used in Rmk. (15.2) and Ex. (22.59).
Ex. (3.31) is used in Eg. (10.7) and Ex. (22.72).
Ex. (3.32) is used in Ex. (18.7) and ApPrp. (18.37)
Ex. (3.33) is used in Ex. (13.44).
Ex. (3.34) is used in Ex. (10.23) and Ex. (13.44).
Ex. (3.35) is used in Ex. (3.36) and ApEx. (13.18).
Ex. (3.36) is used in Ex. (19.30) and ApEx. (22.95).
Ex. (3.37) is used in Prp. (18.8).
Ex. (3.38) is used in Ex. (3.39), Ex. (3.40), Ex. (4.14), Ex. (16.25), Lem. (18.4), Thm. (18.23), ApEx. (18.58), Thm. (19.8), Lem. (19.13), Ex. (19.23), Ex. (20.18). and Prp. (24.7).
Ex. (3.39) is used in Ex. (13.36) and Ex. (20.18).
Ex. (3.40) is used in Ex. (18.26) and Ex. (19.27).
Ex. (3.41) is used in Ex. (13.58).
Ex. (3.42) is used in Ex. (3.43) and Ex. (3.44).
Ex. (3.44) is used in Ex. (18.53).

Chapter 4

Ex. (4.3) is used in Sbs. (4.13), Ex. (5.28), Ex. (6.20), Sbs. (7.10), Cor. (8.9), Thm. (8.13), Ex. (9.33), and Ex. (16.37).
Ex. (4.14) is used in Ex. (7.15), Ex. (9.17), Ex. (18.64), and ApEx. (20.32).
Ex. (4.15) is used in Lem. (10.6), Ex. (17.33), and Ex. (18.35).
Ex. (4.16) is used in Ex. (4.17) and ApLem. (18.38).
Ex. (4.17) is used in ApPrp. (18.37).
Ex. (4.18) is used in Ex. (6.17), Ex. (12.31), ApEx. (18.53), and ApPrp. (23.43).
Ex. (4.19) is used in ApEx. (18.53).
Ex. (4.20) is used in Ex. (8.32).
Ex. (4.21) is used in Ex. (8.27), Cor. (21.7), Ex. (21.26), Sbs. (23.4), ApPrp. (23.49).
Ex. (4.24) is used in Ex. (10.41).
Ex. (4.25) is used in ApThm. (5.38) and Ex. (13.18).
Ex. (4.26) is used in Prp. (5.8) and Ex. (8.14).
Ex. (4.28) is used in Ex. (22.72).
Ex. (4.29) is used in ApEx. (5.41).

Chapter 5

Ex. (5.5) is used in Prp. (5.19), Prp. (5.20), and Prp. (16.13).
Ex. (5.15) is used in Prp. (5.20), Ex. (5.28), Prp. (10.12), Thm. (13.15), and Ex. (17.35).
Ex. (5.18) is used in Prp. (5.19), Prp. (5.20), Ex. (5.29), Ex. (5.30), Sbs. (7.8), Prp. (10.12), Prp. (12.18), and Prp. (13.14).
Ex. (5.21) is used in ApEx. (5.41).
Ex. (5.22) is used in ApEx. (5.42).
Ex. (5.24) is used in Prp. (20.13) and Ex. (22.12).
Ex. (5.27) is used in Ex. (9.33).
ApEx. (5.36) is used in ApEx. (5.37).
ApEx. (5.37) is used in ApThm. (5.38).
ApEx. (5.41) is used in ApEx. (5.42), Ex. (8.26), and Ex. (24.23).

Chapter 6

Ex. (6.15) is used in Ex. (6.20), Thm. (8.13), Lem. (9.5). and Ex. (9.33),
Ex. (6.17) is used in Ex. (8.31).
Ex. (6.19) is used in Prp. (7.7) and Ex. (7.23).

Chapter 7

Ex. (7.2) is used in Eg. (7.3), Prp. (7.7), Ex. (7.11), Ex. (7.12), Ex. (7.13), Ex. (7.14), Ex. (7.15), Ex. (7.23), and ApEx. (22.92).
Ex. (7.14) is used in Ex. (7.16).
Ex. (7.15) is used in Ex. (13.20).
Ex. (7.16) is used in Ex. (7.18), Ex. (13.31), Ex. (13.32), and Ex. (14.13).
Ex. (7.17) is used in Ex. (7.21).
Ex. (7.19) is used in Ex. (7.20) and Ex. (7.21).
Ex. (7.21) is used in ApEx. (22.91).
Ex. (7.22) is used in Ex. (7.23).

Chapter 8

Ex. (8.7) is used in Thm. (8.8), Sbs. (8.19), Ex. (8.28), Ex. (10.10), and Ex. (12.30).
Ex. (8.14) is used in Sbs. (8.15), Ex. (9.33), Ex. (17.35), Cor. (22.19), Ex. (22.38), Ex. (22.53), and Ex. (22.66).
Ex. (8.22) is used in Eg. (9.16).
Ex. (8.24) is used in Ex. (10.10), Ex. (13.30), and Ex. (13.49).
Ex. (8.27) is used in Ex. (8.28), Ex. (8.29), Ex. (8.30), Ex. (8.34), Ex. (9.27), Ex. (9.28), Ex. (10.10), Ex. (10.25), Ex. (10.30), Ex. (13.28), Ex. (13.46), Ex. (13.47), Ex. (13.49), Thm. (14.8), Prp. (17.20), Ex. (19.28), Ex. (21.38),

Ex. (21.39), Ex. (22.36), Ex. (22.38), ApPrp. (23.43), and ApPrp. (23.47).
Ex. (8.28) is used in Ex. (21.37).
Ex. (8.30) is used in Ex. (12.35).
Ex. (8.31) is used in Ex. (8.32), and ApPrp. (23.43)
Ex. (8.32) is used in Ex. (21.23).
Ex. (8.33) is used in Ex. (13.32).

Chapter 9

Ex. (9.14) is used in Lem. (9.15), and Ex. (9.35).
Ex. (9.18) is used in Ex. (22.66).
Ex. (9.19) is used in Ex. (9.25), Ex. (9.26), Ex. (9.28), Ex. (10.30), Ex. (13.47), Ex. (16.28), and Ex. (22.36).
Ex. (9.20) is used in Ex. (22.65).
Ex. (9.22) is used in Prp. (13.12), Ex. (13.21), Ex. (13.47), Ex. (13.48), Thm. (14.8), Ex. (17.35), and Cor. (22.22).
Ex. (9.23) is used in Ex. (13.60), Ex. (14.20), Ex, (21.22), and Ex. (22.65).
Ex. (9.24) is used in Ex. (14.20), and Ex. (17.35).
Ex. (9.25) is used in Ex. (22.67).
Ex. (9.26) is used in Ex. (13.48).
Ex. (9.27) is used in Ex. (10.24).
Ex. (9.28) is used in Ex. (9.29), Ex. (9.31), Ex. (10.31), Ex. (22.65), and Thm. (23.8).
Ex. (9.30) is used in Ex. (9.31).
Ex. (9.33) is used in Prp. (12.19).
Ex. (9.34) is used in Ex. (12.17) and Ex. (22.50).
Ex. (9.35) is used in ApPrp. (23.47) and Thm. (25.21).

Chapter 10

Ex. (10.9) is used in Prp. (10.12), Ex. (14.23), Sbs. (21.14), Ex. (21.42), and Ex. (22.63).
Ex. (10.10) is used in Prp. (10.12) and Prp. (13.7).
Ex. (10.23) is used in Ex. (10.24).
Ex. (10.24) is used in Ex. (10.25).
Ex. (10.25) is used in Ex. (10.26), Ex. (13.21), and Ex. (13.22).
Ex. (10.26) is used in Ex. (13.21), Ex. (13.61), and ApEg. (16.57).
Ex. (10.29) is used in Prp. (13.11).
Ex. (10.30) is used in Ex. (10.31), Ex. (13.48), Ex. (13.60), and Ex. (22.67).
Ex. (10.32) is used in ApThm. (22.78).
Ex. (10.33) is used in Ex. (10.34), ApSbs. (22.73), ApThm. (22.75), ApThm. (22.78), and ApEx. (22.86).
Ex. (10.34) is used in ApThm. (22.75).
Ex. (10.35) is used in Ex. (14.18) and Thm. (16.18).
Ex. (10.36) is used in Ex (10.37).
Ex. (10.37) is used in Ex (14.19).
Ex. (10.39) is used in Ex. (15.17), ApEx. (16.71), Ex. (19.21), Ex. (21.22), Ex. (23.20), and Ex. (26.20).
Ex. (10.41) is used in Ex. (14.25).
Ex. (10.42) is used in Ex. (14.25) and Ex. (26.20).

Chapter 11

Ex. (11.5) is used in Prp. (11.18), Ex. (11.21), and Ex. (13.58).
Ex. (11.19) is used in Thm. (15.7).
Ex. (11.23) is used in Ex. (11.24), Ex. (13.39), and Ex. (13.40).
Ex. (11.24) is used in Ex. (13.39).
Ex. (11.25) is used in Ex. (13.40) and ApEx. (22.92).
Ex. (11.28) is used in Ex. (13.22) and Ex. (13.57).
Ex. (11.29) is used in Ex. (11.32), Thm. (14.3), Ex. (14.12), Ex. (14.15), and Ex. (14.25).
Ex. (11.30) is used in Ex. (11.31) and Thm. (24.13).
Ex. (11.31) is used in Thm. (15.4).
Ex. (11.32) is used in Sbs. (14.9), Ex. (14.25), Ex. (23.7), Thm. (23.8), Thm. (23.14), Thm. (23.15), Ex. (23.21), ApEx. (23.61). and Ex. (24.5).
Ex. (11.34) is used in Ex. (11.35), Ex. (12.31), Ex. (15.32), and Ex. (16.30).

Chapter 12

Ex. (12.4) is used in Prp. (12.3), Ex. (12.5), Prp. (12.12), Ex. (12.24), Ex. (12.25), Ex. (12.33), Ex. (12.34), Ex. (13.21), Ex. (13.28), Ex. (13.51), Ex. (13.59), Thm. (19.3), and Ex. (22.37).
Ex. (12.5) is used in Prp. (12.18), Ex. (12.24), Ex. (12.25), Prp. (13.14), and Thm. (13.15),
Ex. (12.6) is used in Thm. (12.13), Cor. (12.14), Ex. (13.38), and ApEx. (15.47).
Ex. (12.17) is used in Prp. (12.18), Ex. (12.27), Prp. (13.4), ApThm. (18.39), ApLem. (18.40), Ex. (20.17), Ex. (21.27), and ApThm. (23.45),
Ex. (12.24) is used in Ex. (12.25) and Ex. (12.32).
Ex. (12.25) is used in Ex. (13.48), Ex. (13.50), Ex. (13.60), Ex. (13.62), ApEx. (15.48), Ex. (16.30), ApDfn. (23.41), ApPrp. (23.43), ApEx. (23.59), and ApEx. (23.61).
Ex. (12.26) is used in Ex. (12.33),

Ex. (14.25), ApPrp. (23.43), and ApEx. (23.56).
Ex. (12.28) is used in ApEx. (18.58).
Ex. (12.30) is used in Ex. (12.33), Prp. (13.7), Prp. (13.12), Ex. (13.28), ApEx. (23.47), and Ex. (25.6).
Ex. (12.31) is used in Ex. (12.32) and ApPrp. (23.43).
Ex. (12.32) is used in Ex. (21.41).
Ex. (12.33) is used in Ex. (12.35).
Ex. (12.34) is used in Ex. (21.42), Ex. (22.38), and Ex. (24.23).
Ex. (12.36) is used in Ex. (13.64).
Ex. (12.37) is used in Ex. (12.38).
Ex. (12.38) is used in Ex. (13.52).
Ex. (12.40) is used in ApPrp. (18.43).
Ex. (12.41) is used in ApPrp. (18.44).
Ex. (12.42) is used in Lem. (18.12).

Chapter 13

Ex. (13.10) is used in Prp. (13.14) and Ex. (16.29).
Ex. (13.16) is used in Ex. (13.22), Ex. (13.23), ApEx. (15.40), ApEx. (16.74), Ex. (19.20), Ex. (19.21), Ex. (24.23), and Ex. (26.19).
Ex. (13.18) is used in Ex. (13.22) and Ex. (13.23).
Ex. (13.19) is used in Ex. (13.20).
Ex. (13.21) is used in Ex. (13.22) and Ex. (13.61).
Ex. (13.22) is used in Ex. (13.33) and Ex. (13.61).
Ex. (13.23) is used in ApEx. (19.30) and ApEx. (22.94).
Ex. (13.24) is used in Ex. (14.11).
Ex. (13.25) is used in Ex. (13.26), Ex. (13.29), Ex. (13.38), and Thm. (14.8).
Ex. (13.26) is used in Ex. (13.28).
Ex. (13.27) is used in Ex. (13.28).
Ex. (13.28) is used in Ex. (13.30), Ex. (13.31), ApEx. (16.71), and Ex. (19.21).
Ex. (13.29) is used in Ex. (13.38).
Ex. (13.30) is used in Ex. (13.32).
Ex. (13.31) is used in Ex. (13.32), Ex. (13.33), and Ex. (13.38).
Ex. (13.32) is used in Ex. (13.33).
Ex. (13.33) is used in Ex. (13.34).
Ex. (13.36) is used in Ex. (13.37) and ApThm. (16.66).
Ex. (13.37) is used in ApPrp. (16.59).
Ex. (13.38) is used in ApEx. (16.74).
Ex. (13.39) is used in Ex. (13.40) and ApPrp. (16.49).
Ex. (13.41) is used in Ex. (13.43).
Ex. (13.43) is used in Ex. (13.44) and Ex. (13.45).
Ex. (13.44) is used in Ex. (13.45).
Ex. (13.46) is used in Ex. (13.47), ApEx. (18.58), Lem. (19.13), Lem. (20.9), Prp. (20.13), Ex. (20.21), Sbs. (21.2), Lem. (21.3), Thm. (21.4), Cor. (21.5), Ex. (22.37), Ex. (22.53), Sbs. (23.4), Ex. (23.22), ApEx. (23.40), ApEx. (23.53), and ApEx. (23.56).
Ex. (13.47) is used in Ex. (13.48).
Ex. (13.48) is used in Thm. (14.8).
Ex. (13.49) is used in Thm. (14.8), Prp. (17.20), ApPrp. (23.43), and ApEx. (23.53).
Ex. (13.53) is used in Ex. (13.54), Ex. (13.55), Ex. (13.64), Ex. (22.37), Ex. (24.19), and Prp. (25.13).
Ex. (13.55) is used in Ex. (13.56) and Ex. (14.25).
Ex. (13.56) is used in Ex. (24.24).
Ex.,(13.57) is used in Ex. (13.58), Ex. (13.61), Ex. (14.21), Ex. (14.25), ApEx. (15.48), and Ex. (23.12).
Ex. (13.58) is used in Ex. (14.22), and Ex. (14.25).
Ex. (13.59) is used in Thm. (19.3) and ApEx. (22.93).
Ex. (13.60) is used in Ex. (21.41).
Ex. (13.61) is used in ApEg. (16.57), ApEx. (16.67), and ApEx. (18.51).
Ex. (13.62) is used in Ex. (13.63), Ex. (13.64), ApEx. (15.48), and Ex. (25.18).
Ex. (13.63) is used in Ex. (14.24).

Chapter 14

Ex. (14.11) is used in Ex. (26.20).
Ex. (14.12) is used in Ex. (14.13), Ex. (15.19), Ex. (15.23), and Prp. (26.6).
Ex. (14.13) is used in Ex. (15.20) and Prp. (26.6).
Ex. (14.15) is used in Ex. (14.17).
Ex. (14.16) is used in Ex. (14.17) and ApEx. (22.93).
Ex. (14.18) is used in Ex. (14.19).
Ex. (14.20) is used in Ex. (15.29).
Ex. (14.21) is used in Ex. (14.22), Ex. (14.23), and ApEx. (15.48).
Ex. (14.22) is used in Ex. (14.23) and Ex. (14.25).
Ex. (14.23) is used in Ex. (14.24), ApEx. (15.48), and ApPrp. (23.47).
Ex. (14.25) is used in Ex. (23.23).
Ex. (14.26) is used in ApEx. (18.52).

Chapter 15

Ex. (15.18) is used in ApThm. (16.66).
Ex. (15.19) is used in Ex. (15.20).
Ex. (15.24) is used in Cor. (21.7).

Ex. (**15.25**) is used in Prp. (**21.19**).
Ex. (**15.26**) is used in Ex. (**15.29**), Ex. (**21.20**), Eg. (**24.3**), Cor. (**24.14**), and Eg. (**24.16**).
Ex. (**15.27**) is used in Ex. (**21.25**).
Ex. (**15.29**) is used in Ex. (**21.37**).
Ex. (**15.32**) is used in Ex. (**21.41**).
ApEx. (**15.39**) is used in ApEx. (**15.40**).

Chapter 16

Ex. (**16.2**) is used in Lem. (**16.9**), Ex. (**16.24**), Ex. (**16.27**), Ex. (**16.28**), and Ex. (**16.32**).
Ex. (**16.29**) is used in Ex. (**16.30**).
Ex. (**16.33**) is used in Ex. (**19.16**) and Ex. (**22.67**).
Ex. (**16.37**) is used in Ex. (**16.38**) and ApLem. (**23.35**).
Ex. (**16.40**) is used Ex. (**22.40**).
Ex. (**16.41**) is used in Ex. (**16.42**).
Ex. (**16.42**) is used in Ex. (**16.43**), Ex. (**19.17**), Ex. (**19.25**), and Ex. (**22.63**).
Ex. (**16.43**) is used in Thm. (**19.8**).
Ex. (**16.44**) is used in Eg. (**19.6**).
ApEx. (**16.51**) is used in ApEx. (**16.56**), ApPrp. (**16.59**), ApThm. (**16.66**), ApEx. (**16.68**), ApEx. (**16.74**), Ex. (**17.30**), and ApPrp. (**18.49**).
ApEx. (**16.56**) is used in ApEg. (**16.57**), ApEg. (**16.58**), ApThm. (**16.66**), ApEx. (**16.68**), ApEx. (**16.71**), ApEx. (**16.72**), and ApEx. (**16.74**).
ApEx. (**16.61**) is used in ApLem. (**16.62**), ApPrp. (**16.63**), ApLem. (**16.65**), and ApThm. (**16.66**).
ApEx. (**16.73**) is used in ApEx. (**16.74**).
ApEx. (**16.74**) is used in ApEx. (**16.75**).

Chapter 17

Ex. (**17.4**) is used in Prp. (**17.10**), Prp. (**17.12**), Thm. (**17.14**), Prp. (**17.18**), Prp. (**17.19**), Prp. (**17.20**), Ex. (**18.6**), and ApEx. (**23.33**).
Ex. (**17.21**) is used in Ex. (**17.23**), Ex. (**17.24**), Lem. (**18.12**), Lem. (**18.17**), Ex. (**18.25**), and Ex. (**18.32**).
Ex. (**17.22**) is used in Ex. (**18.25**).
Ex. (**17.28**) is used in Ex. (**17.29**).
Ex. (**17.29**) is used in Ex. (**17.30**), Ex. (**18.32**), Ex. (**19.25**), Ex. (**21.30**), Ex. (**21.31**), and ApEx. (**23.56**).
Ex. (**17.31**) is used in Sbs. (**19.1**).
Ex. (**17.32**) is used in Sbs. (**19.1**).
Ex. (**17.33**) is used in ApEx. (**23.54**).
Ex. (**17.34**) is used in Ex. (**17.35**) and ApEx. (**20.34**).

Chapter 18

Ex. (**18.6**) is used in Eg. (**18.16**) and Ex. (**18.30**).
Ex. (**18.7**) is used in Eg. (**18.16**), Ex. (**18.25**), Ex. (**18.30**), and Ex. (**23.7**).
Ex. (**18.27**) is used in Ex. (**19.27**).
Ex. (**18.31**) is used in Ex. (**19.27**).
Ex. (**18.35**) is used in Ex. (**22.3**), Ex. (**22.40**), Ex. (**22.72**), and ApPrp. (**23.50**).
ApEx. (**18.45**) is used in ApPrp. (**18.46**), ApPrp. (**18.47**), ApEx. (**18.63**), and ApEx. (**18.66**).
ApEx. (**18.50**) is used in ApEx. (**18.56**).
ApEx. (**18.53**) is used in ApEx. (**18.54**).
ApEx. (**18.55**) is used in ApEx. (**18.56**).
ApEx. (**18.56**) is used in ApEx. (**18.67**).
ApEx. (**18.58**) is used in ApEx. (**18.67**).
ApEx. (**18.60**) is used in ApEx. (**18.61**).
ApEx. (**18.63**) is used in Thm. (**23.8**).
ApEx. (**18.64**) is used in ApEx. (**20.32**).
ApEx. (**18.65**) is used in Lem. (**23.13**) and Ex. (**23.22**).
ApEx. (**18.67**) is used in Ex. (**19.24**).

Chapter 19

Ex. (**19.2**) is used in Thm. (**19.3**), Ex. (**19.4**), Eg. (**19.6**), Ex. (**19.17**), Ex. (**19.26**), Ex. (**22.41**), and Thm. (**26.13**).
Ex. (**19.4**) is used in Thm. (**19.8**), Cor. (**19.9**), Lem. (**19.13**), Ex. (**19.16**).Lem. (**20.9**), Prp. (**20.13**), Thm. (**21.4**), Lem. (**26.12**), and Thm. (**26.13**).
Ex. (**19.17**) is used in Ex. (**19.21**) and Ex. (**21.22**).
Ex. (**19.19**) is used in Ex. (**22.60**).
Ex. (**19.20**) is used in Ex. (**19.21**) and Ex. (**19.24**) and Ex. (**21.22**).
Ex. (**19.22**) is used in ApEx. (**22.93**).
Ex. (**19.23**) is used in Ex. (**19.24**), Ex. (**21.23**), Sbs. (**22.1**), and Ex. (**22.70**).
Ex. (**19.25**) is used in Ex. (**21.20**).
Ex. (**19.26**) is used in Ex. (**21.26**) and Ex. (**24.23**).
Ex. (**19.27**) is used in Ex. (**24.22**).
Ex. (**19.30**) is used in ApEx. (**22.94**).

Chapter 20

Ex. (**20.17**) is used in ApEx. (**20.33**).
Ex. (**20.18**) is used in Sbs. (**21.2**).
Ex. (**20.22**) is used in Ex. (**22.3**).
ApEx. (**20.25**) is used in ApThm. (**20.27**).
ApEx. (**20.26**) is used in ApThm. (**20.27**).

Chapter 21

Ex. (**21.10**) is used in Thm. (**21.17**) and Thm. (**23.6**).
Ex. (**21.13**) is used in Sbs. (**21.14**), Ex. (**21.16**), Ex. (**21.42**), Eg. (**22.27**), and ApEx. (**23.57**).

Ex. (21.16) is used in Thm. (21.17), Prp. (21.19), ApPrp. (23.47), ApEx. (23.57), and ApEx. (23.61).
Ex. (21.20) is used in ApEx. (23.33), ApPrp. (23.43), and ApEx. (23.56).
Ex. (21.23) is used in Ex. (21.24) and Ex. (22.60).
Ex. (21.24) is used in Ex. (21.25) and Ex. (22.57).
Ex. (21.26) is used in ApPrp. (23.38).
Ex. (21.29) is used in Ex. (21.30).
Ex. (21.30) is used in Ex. (21.31).
Ex. (21.32) is used in Ex. (21.35).
Ex. (21.33) is used in Ex. (21.35), Ex. (21.42), Ex. (23.7), Ex. (25.15), and Sbs. (25.22) .
Ex. (21.34) is used in Thm. (23.8) and Sbs. (25.22).
Ex. (21.35) is used in Ex. (24.24).
Ex. (21.36) is used in Ex. (21.40).
Ex. (21.37) is used in Ex. (21.38) and Ex. (21.39).
Ex. (21.39) is used in Ex. (21.40).
Ex. (21.42) is used in ApEx. (23.61) and Ex. (24.25).

Chapter 22

Ex. (22.3) is used in Ex. (22.8), Ex. (22.14), Lem. (22.24), Ex. (22.28), Ex. (22.36), Ex. (22.37), Ex. (22.39), Ex. (22.45), Ex. (22.54), Ex. (22.57), Ex. (22.60), Ex. (22.61), Ex. (22.69), Ex. (22.72), Eg. (23.2), and ApEx. (23.58).
Ex. (22.8) is used in Ex. (22.15).
Ex. (22.9) is used in Eg. (22.11) and Ex. (22.49).
Ex. (22.12) is used in Ex. (22.16), Thm. (22.18), Cor. (22.19), Cor. (22.20), Thm. (22.26), Ex. (22.33), Ex. (22.36), Ex. (22.42), Ex. (22.46), Ex. (22.48), Ex. (22.52), Ex. (22.53), Ex. (22.61), Ex. (22.62), Ex. (22.64), Ex. (22.66), Ex. (22.68), and Eg. (23.2).
Ex. (22.13) is used in Sbs. (22.1), Ex. (22.14), Ex. (22.15), Lem. (22.24), Ex. (22.33), Ex. (22.54), and Ex. (22.69).
Ex. (22.14) is used in Ex. (22.16), Ex. (22.28), Ex. (22.35), Ex. (22.58), ApThm. (22.81), and ApEx. (22.95).
Ex. (22.15) is used in Ex. (22.16) and Ex. (22.54).
Ex. (22.16) is used in Sbs. (22.1), Thm. (22.26), Ex. (22.28), Ex. (22.33), Ex. (22.39), Ex. (22.54), Ex. (22.58), Ex. (22.70), and Ex. (23.16).
Ex. (22.28) is used in ApThm. (22.84).
Ex. (22.34) is used in Ex. (22.35).
Ex. (22.35) is used in Ex. (22.36), ApThm. (22.75), and ApCor. (22.85).
Ex. (22.36) is used in Ex. (22.67) and Ex. (23.16).
Ex. (22.39) is used in Ex. (22.40).
Ex. (22.40) is used ion Ex. (23.61).
Ex. (22.41) is used in Ex. (22.61).
Ex. (22.42) is used in Ex. (22.43) and Ex. (22.44).
Ex. (22.43) is used in Ex. (22.58).
Ex. (22.44) is used in ApEx. (22.100).
Ex. (22.47) is used in Ex. (22.48) and Ex. (22.49).
Ex. (22.48) is used in Ex. (22.49).
Ex. (22.51) is used in Ex. (22.53).
Ex. (22.52) is used in Ex. (22.53).
Ex. (22.53) is used in Ex. (22.61), Ex. (22.62), ApEx. (22.95), and ApEx. (23.58).
Ex. (22.54) is used in Sbs. (22.1), Ex. (22.55), Ex. (22.63), and ApEx. (22.95).
Ex. (22.55) is used in Ex. (22.56), Ex. (22.57), Ex. (22.58), Ex. (22.59), Ex. (22.60), Ex. (22.63), Ex. (22.64), ApThm. (22.82), and ApEx. (22.100).
Ex. (22.56) is used in Ex. (22.58), ApEx. (22.100), and ApEg. (23.30).
Ex. (22.58) is used inEx. (22.63), Ex. (22.64), Eg. (23.2), and Ex. (23.16).
Ex. (22.59) is used in ApEx. (22.87), ApEx. (22.88), and ApSbs. (22.89).
Ex. (22.61) is used in Ex. (22.62) and ApEx. (23.58).
Ex. (22.62) is used in Ex. (22.63), Ex. (22.64), ApSbs. (22.89), and Ex. (23.16).
Ex. (22.67) is used in ApSbs. (22.89).
Ex. (22.69) is used in Ex. (22.70) and ApEx. (22.100).
ApEx. (22.76) is used in ApThm. (22.81), ApEg. (22.83), ApEx. (22.90), ApEx. (22.97), ApEx. (22.98), and ApEx. (22.99).
ApEx. (22.86) is used in ApSbs. (22.89).
ApEx. (22.87) is used in ApSbs. (22.89).
ApEx. (22.88) is used in ApSbs. (22.89) and Ex. (23.16).
ApEx. (22.91) is used in ApEx. (22.92).
ApEx. (22.92) is used in ApEx. (22.93).

Chapter 23

Ex. (23.7) is used in Thm. (23.8).
Ex. (23.11) is used in Lem. (23.13) and ApPrp. (23.47).
Ex. (23.12) is used in Thm. (23.15) and Ex. (23.23).
Ex. (23.17) is used in ApThm. (23.48).
Ex. (23.22) is used in Ex. (23.23).

Ex. (**23.23**) is used in ApEx. (**23.61**).
ApEx. (**23.24**) is used in ApThm. (**23.29**) and ApEx. (**23.52**).
ApEx. (**23.26**) is used in ApEx. (**23.27**) and ApPrp. (**23.34**).
ApEx. (**23.27**) is used in ApThm. (**23.29**), ApLem. (**23.36**), ApPrp. (**23.39**), ApEx. (**23.40**), ApEx. (**23.53**), and ApEx. (**23.56**).
ApEx. (**23.31**) is used in ApEx. (**23.32**), ApEx. (**23.33**), ApPrp. (**23.39**), and ApEx. (**23.55**).
ApEx. (**23.32**) is used in ApPrp. (**23.38**), ApPrp. (**23.39**), ApPrp. (**23.43**), ApPrp. (**23.47**), and ApEx. (**23.60**).
ApEx. (**23.33**) is used in ApPrp. (**23.43**).
ApEx. (**23.40**) is used in ApDfn (**23.41**), ApEx. (**23.42**), and ApEx. (**23.56**).
ApEx. (**23.42**) is used in ApPrp. (**23.43**).
ApEx. (**23.51**) is used in ApEx. (**23.53**).
ApEx. (**23.52**) is used in ApEx. (**23.53**) and ApEx. (**23.54**).
ApEx. (**23.53**) is used in ApEx. (**23.56**).
ApEx. (**23.54**) is used in ApEx. (**23.55**).
ApEx. (**23.55**) is used in ApEx. (**23.56**).
ApEx. (**23.57**) is used in ApEx. (**23.61**).
ApEx. (**23.60**) is used in ApEx. (**23.61**).

Chapter 24

Ex. (**24.4**) is used in Ex. (**24.5**), Prp. (**24.6**), and Cor. (**24.9**).
Ex. (**24.5**) is used in Prp. (**24.6**), Ex. (**24.22**), and Ex. (**25.23**).
Ex. (**24.21**) is used in Ex. (**24.22**).

Chapter 25

Ex. (**25.2**) is used in Ex. (**25.6**) and Sbs. (**25.22**).
Ex. (**25.6**) is used in Prp. (**25.19**) and Sbs. (**25.22**).
Ex. (**25.9**) is used in Thm. (**25.14**).
Ex. (**25.12**) is used in Ex. (**25.15**).
Ex. (**25.15**) is used in Sbs. (**25.22**).
Ex. (**25.17**) is used in Ex. (**25.18**) and Sbs. (**25.22**).
Ex. (**25.18**) is used in Prp. (**25.19**) and Sbs. (**25.22**).

Chapter 26

Ex. (**26.3**) is used in Thm. (**26.7**).
Ex. (**26.11**) is used in Cor. (**26.15**).
Ex. (**26.17**) is used in Ex. (**26.18**), Ex. (**26.19**), and Ex. (**26.21**).
Ex. (**26.19**) is used in Ex. (**26.20**).
Ex. (**26.21**) is used in Ex. (**26.22**).

Notation

Notation

Index

Index

A Term of Commutative Algebra

Worldwide Center of Mathematics, LLC
www.centerofmath.org