A Survey of Primary Decomposition using Gröbner Bases

by

Michelle Wilson

B.S., Mathematics

Howard University, 1992

Submitted to the Department of
Mathematics in Partial Fulfillment of
the Requirement for the
Degree of

MASTER OF SCIENCE
in Mathematics
at the

Massachusetts Institute of Technology

June 1995

Signature of Author ....
Michelle Wilson

Certified by ....
Steven Kleiman
Professor of Pure Mathematics
Thesis Advisor

Accepted by ....
David Vogan, Jr.
Chairman, Graduate Mathematics Committee

Abstract

A Survey of Primary Decomposition using Gröbner Bases

MICHELLE WILSON

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of
Master of Science

We present a survey of primary decomposition of ideals in a noetherian commutative polynomial ring $\mathrm{R}[\mathbf{x}] = \mathrm{R}[x_1, \ldots, x_n]$. With the use of ideal operations introduced and the lexicographical Gröbner bases of ideals in $\mathrm{R}[\mathbf{x}]$, we show that it is possible to compute a primary decomposition of these ideals. Our method involves the reduction of the general primary decomposition problem to the case of zero-dimensional ideals. Furthermore, we solve the general primary decomposition problem when the coefficient ring is a principal ideal domain.

For the zero-dimensional ideals in $\mathrm{R}[\mathbf{x}]$, we compute inductively their irredundant primary decomposition. In addition, we show that we can compute primary decomposition of zero-dimensional ideals over a field of characteristic zero. We do this by considering ideals in "general position".

Finally, we present algorithms to perform the computation of primary decomposition in the cases discussed.

Thesis Advisor: *Dr. Steven Kleiman*
Title: *Professor of Pure Mathematics*

Contents

Chapter 1

Introduction

1.1 Introduction

In a polynomial ring over a field, it is known that every ideal can be decomposed into finitely many primary components (see [A-M], Chapter 4). This fact was discovered by E. Lasker [L] and F. Macaulay [M]. By 1921, the special case of primary decomposition of zero-dimensional ideals was introduced by E. Noether [N]. In 1926, G. Hermann made an attempt to describe a constructive way to find the primary decomposition of a given polynomial ideal over a field which allows constructive factorization. Unfortunately, Hermann's attempts were based on the erroneous assumption that polynomials can be factored constructively over all ground fields.

Early constructive approaches were based on methods of solving linear equations in a module over the polynomial ring. However, by 1965, we were equipped with the powerful method of Gröbner bases. Gröbner bases were introduced by B. Buchberger [B]. More importantly, Buchberger developed an algorithm for computing Gröbner bases. This algorithm constructs a Gröbner basis for an ideal I when a set of generators for I are given (see [C-L-O], Chapter 2.7).

This paper surveys the study of primary decomposition using the methods introduced by P. Gianni, B. Trager and G. Zacharias [G-T-Z]. Their method uses ideals in "general position" and factorization. In addition, we present a set of algorithms for computing primary decomposition. In Chapter 1, we lay the foundation for the discussion of primary decomposition of ideals in a polynomial ring $R[\mathbf{x}] = R[x_1, \ldots, x_n]$ with coefficients in a noetherian commutative ring R. The main result in Section 1.2 is a reduction algorithm for a polynomial f in $R[\mathbf{x}]$. In Section 1.3, we discuss various ideal operations, such as the construction of saturations in R and the construction of the ring of fractions using Gröbner bases. The final section of Chapter 1 deals with the development of a test to verify the primality of a ideal in $R[\mathbf{x}]$.

Chapter 2, begins with the examination of properties of zero-dimensional ideals using integral extensions and the Gröbner bases of these zero-dimensional ideals. In addition, we investigate the structure of zero-dimensional primary ideals. This is done by looking at verifiable conditions on the lexicographical Gröbner bases of zero-dimensional primary ideals. In Section 2.3, there is a two-fold aim. The first is the computation of the irredundant primary decomposition of zero-dimensional ideals in $R[\mathbf{x}]$. Secondly, we compute primary decomposition of zero-dimensional ideals over a field of characteristic zero. Section 2.4 deals with the reduction of the general primary decomposition problem to the zero-dimensional case. In this section, the coefficient ring is a principal ideal domain.

Chapter 3 presents algorithms to perform some of the computational results introduced in the first two chapters. We present an algorithm which verifies the primality of ideals which was discussed in Section 1.4. We also present algorithms which compute primary decomposition for the cases discussed in Sections 2.3 and 2.4.

1.2 Preliminaries

Throughout this paper, R denotes a commutative noetherian ring and $\mathrm{R}[\mathbf{x}] = \mathrm{R}[x_1, \ldots, x_n]$, the polynomial ring in n variables over R. For basic facts of commutative algebra, the reader may consult Atiyah-Macdonald [A-M]. In this section, we present some of the elementary facts about Gröbner bases (see [C-L-O]).

Definition 1.1 We say that linear equations are *solvable* in R if

(i) (ideal membership) given $f, f_1, \ldots, f_n \in \mathrm{R}$, it is possible to determine whether f is in the ideal $(f_1, \ldots, f_n)\mathrm{R}$, and if so, find $g_1, \ldots, g_n$ such that $f = \sum g_i f_i$,

(ii) (syzygies) given $f_1, \ldots, f_n \in \mathrm{R}$, it is possible to find a finite set of generators for the R -module $\{(g_1, \ldots, g_n) \in \mathrm{R}^n | \sum g_i f_i = 0\}$.

The first condition in Definition 1.1 is necessary in order to make the reduction process we will discuss in Proposition 1.8 computable.

In Gröbner bases computations, the notion of an order is very important. We now define an arbitrary order on a set.

Definition 1.2 Any relation $\succ$ on $\mathbf{N^n}$ is called an *order* if

(i) $\succ$ is a total ordering on $\mathbf{N^n}$;

(ii) if $\alpha \succ \beta$ and γ arbitrary, then $\alpha + \gamma \succ \beta + \gamma$;

(iii) $\succ$ is a well-ordering on $\mathbf{N^n}$.

The lexicographic order is an order which is commonly used. We will now define the lexicographic order.

Definition 1.3 Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n)$. We define the *lexicographic order* on $\mathbf{N^n}$ by $\mathbf{x}^\alpha \succ \mathbf{x}^\beta$ if $\alpha_i \succ \beta_i$ for the first index i with $\alpha_i \neq \beta_i$. We denote this order by $\succ_{lex}$.

When comparing polynomials in R[x], it is sometimes convenient to compare the leading term, the leading coefficient, or the degree. Here we define these useful notations.

Definition 1.4 Let f be a non-zero polynomial in R[x] = R$[x_1, \ldots, x_n]$ such that

$$f = cx^\alpha + f'$$

with $c \in$ R, and $c \neq 0$, and $\alpha \succ \alpha'$ for every nonzero term $c'\alpha'$ of f'. Then

(i) $lt(f) = cx^\alpha$ is the *leading term* of f;

(ii) $lc(f) = c$ is the *leading coefficient* of f;

(iii) $deg(f) = \alpha$ is the *degree* of f.

Definition 1.5 For a subset G of R[x], define the *leading-term ideal* of G, denoted by $LT(G)$, as the ideal generated by $\{lt(g) | g \in G\}$.

With the above notation, it is now possible to define the important notions of a Gröbner basis and a minimal Gröbner basis. These definitions will be used throughout the paper.

Definition 1.6 A finite subset G = $\{g_1, \ldots, g_s\}$ of an ideal I in R[x] is a *Gröbner basis* for I if $LT(G) = LT(\mathrm{I})$.

A *minimal Gröbner basis* for I is a Gröbner basis G for I such that

(i) $lc(g) = 1$ for all $g \in G$, and

(ii) $lt(g) \notin LT(G - \{g\})$, for all $g \in G$.

The following lemma shows that any given Gröbner basis can be made minimal by removing any g with $lt(g) \in LT(G - \{g\})$ from G.

Lemma 1.7 *Let G be a Gröbner basis for an ideal* I *in* R[x]. *Let $g \in G$ be such that $lt(g) \in LT(G - \{g\})$. Then $G-$ $\{g\}$ is a Gröbner basis for* I.

Proof. If $lt(g) \in LT(G- \{g\})$, then $LT(G- \{g\}) = LT(G)$. Since $LT(G) = LT(\mathrm{I})$, it follows, $G-$ $\{g\}$ is a Gröbner basis of I. ■

The following proposition is called the Reduction Algorithm because it gives a reduction of any given f in R[x]. Of course, the proposition is not given in the usually step-by-step fashion of algorithms, but it constructs a "reduction" of f in a style similar to that done in algorithms.

Proposition 1.8 (Reduction Algorithm) *Given f and $G = \{g_1, \ldots, g_s\}$ in* R[x], *we can construct f' such that $f = f' mod(g_1, \ldots, g_s)$*R[x] *and $lt(f') \notin LT(G)$.*

Proof. The ideal membership condition on R insures that we can determine whether $lt(f) \in LT(G)$, and if so, find terms t_i such that $lt(f) = \sum t_i lt(g_i)$. If not, it suffices to let $f' = f$. Otherwise, let $f_1 = f- \sum t_i lt(g_i)$. Then the leading term of $\sum t_i lt(g_i)$ cancels the leading term of f. Hence, $deg(f_1) < deg(f)$. So, by induction on the well-ordering $<$, we can find f' such that $lt(f') \notin LT(G)$ with $f' \equiv f_1 \operatorname{mod}(g_1, \ldots, g_s)$. But $f \equiv f_1$, so $f \equiv f'$ as required. ■

Definition 1.9 Let f and $G = \{g_1, \ldots, g_s\}$ be in R[x]. If $lt(f) \notin LT(G)$, then f is called *reduced modulo G*. Otherwise, f is called *reducible modulo G*.

Corollary 1.10 *For any f and G, there exists a reduced f' with $f = f'$ modulo the ideal generated by G.*

Using the reduction algorithm, we can now prove one of the fundamental properties of Gröbner bases.

Proposition 1.11 *Let G be a Gröbner basis for an ideal* I *in* R[**x**]. *Then $f \in$ I if and only if application of the reduction algorithm to f returns* 0.

Proof. Let f be a non-zero element of R[**x**], and let f' be as in Proposition 1.8. Since $G \subset$ I, we have $f \equiv f'$ mod I. Thus, if $f' = 0$, then $f \in$ I. Conversely, if $f \in$ I, then $f' \in$ I and $lt(f') \in LT(\mathrm{I}) = LT(G)$. But by assumption, f' is reduced modulo G, so we have $f' = 0$. ■

Corollary 1.12 *It is possible to determine ideal membership in* I *given a Gröbner basis G for* I.

Proof. The statement follows directly from Proposition 1.11. ■

The following proposition reveals one of the special properties of Gröbner bases. This property is a consequence of the Hilbert Basis Theorem (see [C-L-O], Chapter 2.5, Theorem 4).

Proposition 1.13 *Every non-zero ideal* I *of* R[**x**] *has a Gröbner basis.*

Proof. Since R is noetherian, the Hilbert Basis Theorem implies that the polynomial ring R[**x**] is also noetherian. So the leading-term ideal $LT(\mathrm{I})$ has a finite generating set which can be assumed to be of the form $\{lt(g_1), \ldots, lt(g_n)\}$ with $g_1, \ldots, g_n \in$ I. If we set G $= \{g_1, \ldots, g_n\}$, then we have $LT(G) = LT(I)$. Hence, G is a Gröbner basis for I. ■

Corollary 1.14 *If* G *is a Gröbner basis for* I, *then* G *generates* I.

Proof. If G $= \{g_1, \ldots, g_n\}$ is a Gröbner basis for I, then $LT(I)$ is the ideal generated by the elements $lt(g_1), \ldots, lt(g_n)$. Clearly, the ideal generated by the elements $g_1, \ldots, g_n$ is contained in I, since each $g_i \in$ I. Conversely, let $f \in$ I be any polynomial. Using the division algorithm (see [A-D], Algorithm 4.1.1), we can divide f by $g_1, \ldots, g_n$. Then we get a remainder, r, which is reduced modulo G. That is, r is divisible by none of $lt(g_1), \ldots, lt(g_n)$. We claim that $r = 0$. Indeed, if $r \neq 0$, then $lt(r) \in LT(I)$, and hence $lt(r)$ must be divisible by some $lt(g_i)$. This contradicts the fact that r is reduced modulo G, and, consequently, r must be zero. Thus, f is an element of the ideal generated by $g_1, \ldots, g_n$, which shows the reverse inclusion. This completes the proof. ∎

Corollary 1.15 *If* J $\subset$ I *are ideals in* R[x] *and* $LT(I) = LT(J)$, *then* I = J.

Proof. The ideal J forms a non-finite Gröbner basis for I, so by Corollary 1.10, we may conclude that J generates I. But since J is an ideal, it only generates itself, so J = I. ∎

1.3 Ideal Operations

We now discuss the use of Gröbner bases to perform basic ideal operations in R[x]. We show we can construct saturations and the ring of fractions using Gröbner bases without much difficulty.

Proposition 1.16 *Let* I *be an ideal in* R[**y**, **x**] $=$ R$[y_1, \ldots, y_n, x_1, \ldots, x_m]$. *Given any two orders* $\succ_1$ *and* $\succ_2$ *on monomials in* **x** *and* **y** *respectively, define an order* $\succ$ *by*

$x^\alpha y^\beta \succ x^{\alpha'} y^{\beta'}$ if $x^\alpha \succ_1 x^{\alpha'}$, or if $x^\alpha = x^{\alpha'}$ and $y^\beta \succ_2 y^{\beta'}$. If $G \subset \mathrm{R}[\mathbf{y}, \mathbf{x}]$ is a Gröbner basis for I *with respect to $\succ$ then*

(i) G is a Gröbner basis for I *with respect to the order $\succ_1$ on* $(\mathrm{R}[\mathbf{y}])[\mathbf{x}]$, *the polynomial ring in $x_1, \ldots, x_m$ with coefficients in* $\mathrm{R}[\mathbf{y}]$.

(ii) $G \cap \mathrm{R}[\mathbf{y}]$ is a Gröbner basis for $\mathrm{I} \cap \mathrm{R}[\mathbf{y}]$ *with respect to the order $\succ_2$.*

Proof. (i) For any $f \in \mathrm{R}[\mathbf{y}, \mathbf{x}]$, we have $lt_\succ(lt_{\succ_1}(f)) = lt_\succ(f)$ by the definition of $\succ$. So

$$LT_\succ(LT_{\succ_1}(G)) = LT_\succ(G) = LT_\succ(\mathrm{I}) = LT_\succ(LT_{\succ_1}(\mathrm{I})).$$

Thus, since $G \subset \mathrm{I}$ and G is a Gröbner basis for I, we have $LT_{\succ_1}(G) = LT_{\succ_1}(\mathrm{I})$.

(ii) Since, no term involving any x_i can be $\succ$-larger than a term involving only y_i. Hence, $lt_\succ(g) \in \mathrm{R}[\mathbf{y}]$ if and only if $g \in \mathrm{R}[\mathbf{y}]$. Thus,

$$LT_\succ(G \cap \mathrm{R}[\mathbf{y}]) = LT_\succ(G) \cap \mathrm{R}[\mathbf{y}] = LT_\succ(\mathrm{I}) \cap \mathrm{R}[\mathbf{y}] = LT_\succ(\mathrm{I} \cap \mathrm{R}[\mathbf{y}]).$$

Therefore, $G \cap \mathrm{R}[\mathbf{y}]$ is a Gröbner basis for $\mathrm{I} \cap \mathrm{R}[\mathbf{y}]$ with respect to $\succ$. But $\succ$ coincides with $\succ_2$ on $\mathrm{R}[\mathbf{y}]$. ■

The preceding proposition has significant practical importance for Gröbner basis computations. Part (i) shows that we can combine the coefficient variable **y** and the ground ring variables **x**, using an appropriate order, and compute Gröbner bases over R. This allows for the simplification of our computations when the ground ring R is a field or a principal ideal domain (PID).

As a consequence of this proposition, in the remainder of this paper, we will perform our computations using the simpler field or PID variant of the Gröbner basis algorithm (see [A-D]) whenever we require calculation of Gröbner bases with coefficients in a polynomial ring constructed from a ground ring. This is, of course, provided the ground ring is a field or a PID.

Part (ii) of the proposition shows that we can compute the contraction of an ideal to a coordinate subring. To do so, we simply compute the Gröbner basis for the ideal with respect to an order $\succ$ based on whatever order $\succ_2$ we want for the contraction. Futhermore, the Gröbner basis involving only the subring variables is a Gröbner basis for the contraction.

The following proposition fully characterizes these facts.

Proposition 1.17 *Fix an order* $\succ$ *on the leading term of elements in* $\mathrm{R}[\mathbf{x}]$. *Let* I *in* $\mathrm{R}[\mathbf{x}]$ *be an ideal and let* $\pi : \mathrm{R}[\mathbf{x}] \longrightarrow (\mathrm{R}/\mathrm{I} \cap \mathrm{R})[\mathbf{x}]$ *be the quotient map. Then for* $G \subset \mathrm{I}$ *we have*

(i) If G *is a Gröbner basis for* I *then* $G \cap \mathrm{R}$ *generates* $\mathrm{I} \cap \mathrm{R}$ *and* $\pi(G)$ *is a Gröbner basis for* $\pi(\mathrm{I})$.

(ii) G *is a minimal Gröbner basis for* I *if and only if* $G \cap \mathrm{R}$ *is a minimal basis for* $\mathrm{I} \cap \mathrm{R}$, *the image* $\pi(G- \ G \cap \mathrm{R})$ *is a minimal Gröbner basis for* $\pi(\mathrm{I})$, *and* $\pi(lt(g)) \neq 0$ *for all* $g \in (G- \ G \cap \mathrm{R})$.

Proof. For any $f \in \mathrm{I}$, the image $\pi(lt(f))$ is either 0 or $lt(\pi(f))$, so we have $\pi(LT(\mathrm{I})) \subset LT(\pi(\mathrm{I}))$. Conversely, given $f \in \mathrm{I}$, we can write $f = f_0 + f_1$ where $\pi(f_0) = 0$ and $\pi(lc(f_1)) \neq 0$. Furthermore, $f_0 \in \mathrm{I}$ and so $f_1 \in \mathrm{I}$ and

$$lt(\pi(f)) = lt(\pi(f_1)) = \pi(lt(f_1)) \in \pi(LT(\mathrm{I})).$$

Hence, we have $\pi(LT(\mathrm{I})) = LT(\pi(\mathrm{I}))$. The result follows from the definitions and Proposition 1.16(ii). ∎

Finally, we observe that Gröbner bases are well behaved under the formation of the ring of fractions of R[x] and we will examine the importance of the construction of the saturation $S^{-1}\mathrm{I} \cap \mathrm{R[x]}$ where S is a multiplicatively closed subset of R.

Proposition 1.18 *Fix an order $\succ$ on the leading term of the elements in* R[x]. *Let S be a multiplicatively closed subset of* R. *If G is a Gröbner basis for an ideal* I *in* R[x], *then it is a Gröbner basis for $S^{-1}\mathrm{I} \subset (S^{-1}\mathrm{R})[\mathrm{x}]$.*

Proof. We observe that

$$LT(S^{-1}\mathrm{I}) = S^{-1}LT(\mathrm{I}) = S^{-1}LT(G).$$

That is, the leading terms of the elements of G generate $LT(S^{-1}\mathrm{I})$ in $S^{-1}\mathrm{R[x]}$. ■

The construction of the saturation $S^{-1}\mathrm{I} \cap \mathrm{R[x]}$ can be determined from the behavior of the leading-term ideal. This is explored in the following lemma.

Lemma 1.19 *Let $T \subset S$ be multiplicatively closed subsets of* R, *and let* I *be an ideal in* R[x]. *If*

$$S^{-1}LT(\mathrm{I}) \cap \mathrm{R[x]} = T^{-1}LT(\mathrm{I}) \cap \mathrm{R[x]}$$

then

$$S^{-1}\mathrm{I} \cap \mathrm{R[x]} = T^{-1}\mathrm{I} \cap \mathrm{R[x]}.$$

Proof. We have

$$\begin{aligned} LT(S^{-1}\mathrm{I} \cap T^{-1}\mathrm{R[x]}). &\subseteq LT(S^{-1}\mathrm{I}) \cap T^{-1}\mathrm{R[x]} \\ &= S^{-1}LT(\mathrm{I}) \cap T^{-1}\mathrm{R[x]} \\ &= T^{-1}(S^{-1}LT(\mathrm{I}) \cap \mathrm{R[x]}) \text{ since } \mathrm{T} \subset \mathrm{S} \end{aligned}$$

$$
\begin{aligned}
&= T^{-1}(T^{-1}LT(\mathrm{I}) \cap \mathrm{R}[\mathbf{x}]) \text{ by assumption} \\
&= T^{-1}LT(\mathrm{I}) \\
&= LT(T^{-1}\mathrm{I}).
\end{aligned}
$$

Since $T^{-1}\mathrm{I} \subset S^{-1}\mathrm{I} \cap T^{-1}\mathrm{R}[\mathbf{x}]$, we have $LT(S^{-1}\mathrm{I} \cap T^{-1}\mathrm{R}[\mathbf{x}]) = LT(T^{-1}\mathrm{I})$. Thus, by Corollary 1.15, $S^{-1}\mathrm{I} \cap T^{-1}\mathrm{R}[\mathbf{x}] = T^{-1}\mathrm{I}$. Now taking intersections with R[x] gives $S^{-1}\mathrm{I} \cap \mathrm{R}[\mathbf{x}] = T^{-1}\mathrm{I} \cap \mathrm{R}[\mathbf{x}]$ as required. ■

Remark 1.20 Taking $T = \{1\}$ shows I is saturated with respect to S if $LT(\mathrm{I})$ is saturated with respect to S.

We now make a further reduction of the problem of computing the saturation $S^{-1}\mathrm{I}$ $\cap$ R[x] of an arbitrary ideal I in R[x] to an analogous problem for ideals generated by terms.

Proposition 1.21 *Let S be a multiplicatively closed subset of* R*, and* I *an ideal in* R[x] *. If for some $s \in S$,*

$$S^{-1}LT(\mathrm{I}) \cap \mathrm{R}[\mathbf{x}] = (LT(\mathrm{I})\mathrm{R}_s[\mathbf{x}]) \cap \mathrm{R}[\mathbf{x}]$$

then

$$S^{-1}\mathrm{I} \cap \mathrm{R}[\mathbf{x}] = \mathrm{I}\mathrm{R}_s[\mathbf{x}] \cap \mathrm{R}[\mathbf{x}]$$

.

Proof. Apply the lemma with $T = \{s^n\}$. ■

In the case where $S =$ R$-$ P, for a prime ideal P in R, the localization R_{P} is of particular interest. There are no general algorithms for computing saturations of an ideal of R with respect to arbitrary prime ideals P; however, the problem can be solved in the case where P is a principal ideal. We now present a proposition, which will be central to a dimension reduction process, which will be developed later.

Proposition 1.22 *Let* R *be an integral domain, and* (p) *a principal prime ideal in* R. *For any given ideal* $\mathrm{I} \subset \mathrm{R}[\mathrm{x}]$, *it is possible to find* $s \in \mathrm{R}- (p)$ *such that*

$$\mathrm{IR}_{(p)}[\mathrm{x}] \cap \mathrm{R}[\mathrm{x}] \quad = \quad \mathrm{IR}_s[\mathrm{x}] \cap \mathrm{R}[\mathrm{x}].$$

In particular, the generators of $\mathrm{IR}_{(p)}[\mathrm{x}] \cap \mathrm{R}[\mathrm{x}]$ *can be computed.*

Proof. Since R is a domain, we have $\cap(p^k) = 0$. Thus, for any non-zero element r of R, there exists a k such that $r \in (p^k)$, and $r \notin (p^{k+1})$. Hence $r = sp^k$ for some $s \notin (p)$. Applying the ideal membership algorithm (See [A-D]) , we can compute k and s. Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis for I. Write $lt(g_i) = s_i p^{k_i} x^{\alpha_i}$, where $s \notin (p)$. Then $LT(\mathrm{I}) = (s_i p^{k_i} x^{\alpha_i})$ and $LT(\mathrm{I})\mathrm{R}_{(p)}[\mathrm{x}] \cap \mathrm{R}[\mathrm{x}] = (p^{k_i} x^{\alpha_i})$. Thus in order to apply Proposition 1.21, we need to find an s such that every s_i is invertible in $\mathrm{R}_s[\mathrm{x}]$. The choice $s = \Pi s_i$ satisfies this condition. ∎

Corollary 1.23 *Let* R *be an integral domain,* K *the quotient field of* R. *Then for any given ideal* I *in* R[x] *it is possible to compute* $\mathrm{IK}[\mathrm{x}] \cap \mathrm{R}[\mathrm{x}]$.

Proof. Apply the proposition with $p = 0$. ∎

1.4 Primality Test

In this section we will develop a test to verify whether an ideal I is prime. We first recall some basic facts about prime ideals.

Lemma 1.24 *An ideal* I *in* R[x] *is prime if and only if* I ∩ R *is prime and the image of* I *in* (R/I ∩ R)[x] *is prime.*

Proof. See Zariski and Samuel [Z-S], Chapter III, Theorem 11. ∎

Lemma 1.25 *Let* R *be an integral domain,* K *the quotient field of* R. *If* I *is an ideal of* R[x] *such that* I ∩ R = (0) *then* I *is prime if and only if* IK[x] *is prime and* I = IK[x] ∩ R[x].

Proof. See Zariski and Samuel [Z-S], Chapter IV, Theorem 16. ∎

Assuming we have a primality test for ideals in R and we can test the irreducibility of univariate polynomials over quotient fields of residue rings of R[x], then we obtain the following proposition.

Proposition 1.26 *It is possible to decide the primality of ideals in* R[x].

Proof. Proceeding by induction on the number of variables we may assume that we have an ideal I in R[x_1]. By Proposition 1.16(ii), we can compute I^c = I ∩ R. If I^c is not prime then neither is I. Otherwise by Lemma 1.24, we need only test the primality of the image of I in R/I^c[x_1]. Replacing R by R/I^c, we may assume R is an integral domain and I ∩ R = (0). Let K be the quotient field of R. Then IK[x_1] is a principal ideal. Thus, we can test its primality by checking the irreducibility of its generator. By Corollary 1.23, we can compute IK[x_1] ∩ R[x_1]. Hence, we can test the primality of I by Lemma 1.25. ∎

Chapter 2

Main Results

2.1 Introduction

In this chapter we examine the structure of zero-dimensional ideals using the properties of Gröbner bases. First, we show that it is possible to determine whether an ideal is zero-dimensional by inspection of its Gröbner basis. We then give a complete characterization of zero-dimensional primary ideals in terms of verifiable conditions on their lexicographical Gröbner bases. Secondly, we compute the irredundant primary decomposition of zero-dimensional ideals in R[**x**]. Finally, we show how to reduce the general primary decomposition problem to the zero-dimensional case when the coefficient ring is a principal ideal domain.

So to reiterate the set-up, we assume we are given a noetherian commutative ring R and let R[**x**] = R$[x_1, \ldots, x_n]$. We then have from the Hilbert Basis Theorem, that R[**x**] is also a noetherian ring. We assume that we have an order on the leading terms of the elements of R[**x**].

2.2 Zero-dimensional Ideals

In this section we examine properties of zero-dimensional ideals using integral extensions and Gröbner bases of zero-dimensional ideals. In doing so, we will completely characterize zero-dimensional primary ideals using their lexicographical Gröbner bases.

Lemma 2.1 *Let* I *in* $\mathrm{R}[\mathbf{x}]$ *be an ideal such that* $\mathrm{I} \cap \mathrm{R}$ *is zero-dimensional. Then* I *is zero-dimensional if and only if* $\mathrm{R}[\mathbf{x}]/\mathrm{I}$ *is integral over* R.

Proof. Suppose $\mathrm{R}[\mathbf{x}]/\mathrm{I}$ is integral over R. Then it is also integral over the subring $\mathrm{R}/(\mathrm{I} \cap \mathrm{R})$ of $\mathrm{R}[\mathbf{x}]/\mathrm{I}$. Thus, $\mathrm{R}/(\mathrm{I} \cap \mathrm{R})$ and $\mathrm{R}[\mathbf{x}]/\mathrm{I}$ have the same dimension.

Conversely, suppose I is zero-dimensional. Let $\mathrm{I} = \bigcap Q_k$ be a primary decomposition of I, and let $\mathrm{M}_k := \sqrt{Q_k}$. By assumption, M_k is maximal. Since $\mathrm{M}_k \cap \mathrm{R}$ contains I $\cap$ R, it is zero-dimensional and hence maximal. Therefore, by the Nullstellensatz, the field $\mathrm{R}[\mathbf{x}]/\mathrm{M}_k$ is a finite algebraic extension of the subfield $\mathrm{R}/(\mathrm{M}_k \cap \mathrm{R})$. In particular, M_k contains a monic polynomial $f_{i,k}(x_i)$, for each i. Then $(f_{i,k}(x_i))^n \in \mathrm{Q}_k$ for some n, and so $\Pi_k(f_{i,k}(x_i))^n \in \mathrm{I}$ establishes integral dependence for x_i mod I. ■

Remark 2.2 The requirement that $\mathrm{I} \cap \mathrm{R}$ be zero-dimensional in Lemma 2.1 is necessary. For instance, consider $\mathrm{R} = \mathbf{Z}_{(2)}$, the localization of $\mathbf{Z}$ at the prime ideal generated by 2. Then the ideal $\mathrm{I} = (2x - 1)\mathrm{R}$ in $\mathrm{R}[\mathbf{x}]$ is maximal but contains no monic polynomials. Hence, x mod I is not integral over R, and indeed, $\mathrm{I} \cap \mathrm{R} = (0)$ is not zero-dimensional. The condition $\mathrm{I} \cap \mathrm{R}$ zero-dimensional for every zero-dimensional ideal I of $\mathrm{R}[\mathbf{x}]$ is satisfied for polynomial rings with coefficients in a field. Futhermore, it follows from the lemma that, if I and $\mathrm{I} \cap \mathrm{R}$ are zero-dimensional, then so is $\mathrm{I} \cap \mathrm{R}[x_i, \ldots, x_n]$ for any i.

We now give an effective criterion for detecting integral extensions.

Proposition 2.3 *The ring* R[x]/I *is integral over* R *if and only if* $(x_1, \ldots, x_n) \subset \sqrt{LT(\mathrm{I})}$.

Proof. Let

$$\pi : \mathrm{R}[\mathbf{x}] \longrightarrow \mathrm{R}[\mathbf{x}]/\mathrm{I}$$

be the natural surjection. Suppose $\pi(x_i) \in \mathrm{R}[\mathbf{x}]/\mathrm{I}$ is integral over R. Then I contains a monic polynomial $f(x_i) \in \mathrm{R}[x_i]$,for each i. So $lt(f(x_i)) \in LT(\mathrm{I})$, but on the other hand, the leading term of $f(x_i)$ is a power of x_i. Hence, $(x_1, \ldots, x_n) \subset \sqrt{LT(\mathrm{I})}$.

We are now going to show that R[x]/I is finitely generated as an R-module, and thus it is integral over R. Suppose $x_i^{m_i} \in LT(\mathrm{I})$, and consider the finitely generated R-module

$$\mathrm{K} := \sum_{a_i < m_i} \mathrm{R} x_1^{a_1} \ldots x_n^{a_n}.$$

We claim that the residue-class map

$$\pi : \mathrm{K} \longrightarrow \mathrm{R}[\mathbf{x}]/\mathrm{I},$$

is surjective. Indeed, take $f \in \mathrm{R}[\mathbf{x}]$ and consider $\pi(f) \in \mathrm{R}[\mathbf{x}]/\mathrm{I}$. We may assume $f \notin$ I, since 0 is in the image of K. Now, by Corollary 1.10, there exists an f' such that $f' \equiv f \mod \mathrm{I}$ and $lt(f') \notin LT(\mathrm{I})$. In particular, $lt(f') \notin (x_1^{m_1}, \ldots, x_n^{m_n})$, so $lt(f') \in \mathrm{K}$. Furthermore, since $f - f' \in \mathrm{I}$ and $lt(f') \notin LT(\mathrm{I})$, we have $lt(f - f') \neq lt(f')$. It follows that $deg(f') \leq deg(f)$ and so $deg(f' - lt(f')) < deg(f)$. By induction on the degree of f, we may assume that $(f' - lt(f'))$ is in the image of K. Say $\pi(f' - lt(f')) = h$ for some $h \in \mathrm{K}$. Then

$$\pi(lt(f') + h) = \pi(lt(f')) + \pi(h) = \pi(lt(f')) + \pi(f' - lt(f')) = \pi(f') = \pi(f).$$

Thus $\pi(f)$ is in the image of K. The proof is now complete. ■

If G is a Gröbner basis for I, let

$$G_i := \{\, g \in G \,|\, lt(g) = cx_i^m \text{ for some c} \in \mathrm{R}, \text{and m} \geq 0\}.$$

Let $\mathrm{L}_i \subset \mathrm{R}$ be the ideal generated by the leading coefficients of elements of G_i. Clearly, $LT(\mathrm{G}_i) = LT(G) \cap \mathrm{R}[x_i]$, so $x_i \in \sqrt{LT(\mathrm{I})} = \sqrt{LT(G)}$ if and only if $x_i \in \sqrt{LT(G_i)}$. The latter happens if and only if $\mathrm{L}_i = (1)$. Furthermore, it follows from the first part of the proof that if $x_i \notin \sqrt{LT(I)}$, then $\pi(x_i)$ cannot be integral over R. Hence, we have the following Corollary.

Corollary 2.4 *It is possible to determine whether* R[x]/I *is integral over* R, *and if not, to find i such that the residue class of x_i is integral over* R.

Application of Lemma 2.1, we get the following Corollary.

Corollary 2.5 *If* $\mathrm{I} \cap \mathrm{R}$ *is zero-dimensional. then it is possible to determine whether* I *is zero-dimensional, and if not, to find an i such that* $\mathrm{I} \cap \mathrm{R}[x_i]$ *is not zero-dimensional.*

We can simplify the criterion above when $\mathrm{I} \cap \mathrm{R}$ is primary. The following proposition addresses this fact.

Proposition 2.6 *Let* I *in* R[x] *be an ideal such that* $\mathrm{I} \cap \mathrm{R}$ *is zero-dimensional primary. Let* G *be a Gröbner basis for* I. *Then* I *is zero-dimensional if and only if for each i there exists* $g_i \in \mathrm{G}$ *such that* $lt(g_i) = c_i x_i^{m_i}$ *where* $c_i \in \mathrm{R}$ *is a unit modulo* $\mathrm{I} \cap \mathrm{R}$.

Proof. Let G_i and L_i be as described in Proposition 2.3. Note, G_i contains $\mathrm{G} \cap \mathrm{R}$, and so L_i contains $\mathrm{I} \cap \mathrm{R}$. Now, since $\sqrt{\mathrm{I} \cap \mathrm{R}}$ is maximal, $\mathrm{L}_i = (1)$ if and only if $\mathrm{L}_i \not\subset \sqrt{\mathrm{I} \cap \mathrm{R}}$. The latter occurs if and only if there is some $g_i \in \mathrm{G}_i$ such that $lc(g_i) \notin \sqrt{\mathrm{I} \cap \mathrm{R}}$. But this is equivalent to the requirement that $(lc(g_i), \mathrm{I} \cap \mathrm{R}) = (1)$. ■

Remark 2.7 If G is a minimal Gröbner basis, then all the elements of G_i other than g_i have degree in x_i strictly smaller than m_i. Hence, to decide whether I is zero-dimensional using a minimal Gröbner basis, we need only check that G_i contains exactly one element of maximal degree, and that the leading coefficient of this element together with G ∩ R generate the unit ideal. It is not necessary to check the leading coefficients of any other elements of G_i. Conversely, if I is known to be zero-dimensional, then g_i can be uniquely identified as the highest degree element of G_i.

We next investigate the structure of zero-dimensional primary ideals. We say a polynomial has some property modulo an ideal J in R if its image as a polynomial in R/J has that property. However, before preceding, we will give a few univariate results. These results are key part of the argument used in the characterization of zero-dimensional primary ideals.

Lemma 2.8 *Let* I *in* $R[x_1]$ *be an ideal such that* I ∩ R *is zero-dimensional. Suppose* $x_1^m \in LT(I)$ *and* $x_1^{m-1} \notin LT(I)$. *Then every* $f \in I$ *with* $deg(f) < m$ *is a zero-divisor modulo* I ∩ R.

Proof. Let L in R be the ideal generated by the leading coefficients of the elements of I of degree less than m. Let $LR[x_1]$ be the extension of L in $R[x_1]$. We claim that, if $f \in I$ has degree less than m, then $f \equiv 0 \mod LR[x_1]$. Indeed, let $f = c_1x_1^{m-1} + \ldots + c_m$. Then either c_1 is 0 or it is the leading coefficient of f, so $c_1 \in L$. By hypothesis, there exists $g \in I$ with $lt(g) = x_1^m$. Let $f' = x_1 f - c_1 g$. Then $f' \in I$ and $f' = c_1'x_1^{m-1} + \ldots + c_m'$ with $c_i' = c_{i+1} \mod L$. It follows by induction that $c_i \in L$ for all i, proving the claim. Now, if L = (1), then I contains a monic polynomial of degree less than m. This is contrary to the assumption. Thus, L is a proper ideal. Since $\mathrm{I} \cap \mathrm{R} \subset \mathrm{L}$ and $\mathrm{I} \cap \mathrm{R}$ is zero-dimensional, L is contained in some associated prime of $\mathrm{I} \cap \mathrm{R}$. Hence, there exists $a \notin \mathrm{I} \cap \mathrm{R}$ such that $a\mathrm{L} \subseteq \mathrm{I} \cap \mathrm{R}$. Then $af \equiv 0 \bmod \mathrm{I} \cap \mathrm{R}$ whenever $deg(f) < m$. ∎

Lemma 2.9 *Let* I *in* $\mathrm{R}[x_1]$ *be a zero-dimensional ideal such that* $\mathrm{I} \cap \mathrm{R}$ *is zero-dimensional primary. Let* G *be a minimal Gröbner basis for* I, *and let* $g_1 \in \mathrm{G}$ *be as in Proposition 2.6. Then*

$$\sqrt{\mathrm{I}} = \sqrt{(g_1, \mathrm{I} \cap \mathrm{R})}.$$

Proof. Let $lt(g_1) = c_1 x_1^{m_1}$. By assumption, c_1 is a unit modulo $\mathrm{I} \cap \mathrm{R}$, so $x_1^{m_1} \in LT(g_1, \mathrm{I} \cap \mathrm{R})$ which is contained in $LT(\mathrm{I})$. Now, $LT(\mathrm{I})$ cannot contain any smaller powers of x_1. Otherwise, g_1 would be reducible modulo G, and this contradicts the minimality of G. Let $f \in \mathrm{I}$ of degree less than m_1. Then by Lemma 2.8, every such f is a zero-divisor modulo $\mathrm{I} \cap \mathrm{R}$. But since $\mathrm{I} \cap \mathrm{R}$ is primary, the set of zero-divisors modulo $\mathrm{I} \cap \mathrm{R}$ is exactly $\sqrt{\mathrm{I} \cap \mathrm{R}}$. Thus, if $f \in \mathrm{I}$, and $deg(f) < m_1$, then $f \equiv 0 \bmod \sqrt{\mathrm{I} \cap \mathrm{R}}$. Now, by Proposition 1.8, there exists $f' \equiv f \bmod (g_1, \mathrm{I} \cap \mathrm{R})$ such that f' is reduced modulo $(g_1, \mathrm{I} \cap \mathrm{R})$. Since $x_1^{m_1} \in LT(g_1, \mathrm{I} \cap \mathrm{R})$, we know f' has degree less than m_1, so $f' \equiv 0 \bmod \sqrt{\mathrm{I} \cap \mathrm{R}}$. Thus,

$$f \in (g_1, \mathrm{I} \cap \mathrm{R}) + (\sqrt{\mathrm{I} \cap \mathrm{R}})\mathrm{R}[x_1] = (g_1, \sqrt{\mathrm{I} \cap \mathrm{R}}).$$

In other words, we have

$$\mathrm{I} \subset (g_1, \sqrt{\mathrm{I} \cap \mathrm{R}}) \subset \sqrt{\mathrm{I}}.$$

Taking radicals proves the lemma. ∎

With these univariate results, we now can completely characterize zero-dimensional primary ideals in terms of verifiable conditions on their lexicographical Gröbner bases.

Proposition 2.10 *Let* I *in* R[x] *be a zero-dimensional ideal such that* $\mathrm{I} \cap \mathrm{R}$ *is zero-dimensional primary. Let* G *be a minimal Gröbner basis for* I *with respect to the lexicographical order, and let* $g_1, \ldots, g_n \in \mathrm{G}$ *be as in Proposition 2.6. Then* I *is primary if and only if* g_i *is a power of an irreducible polynomial modulo* $\sqrt{\mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]}$, *for all* i. *If the latter is the case, then for every* $h \in \mathrm{G} \cap \mathrm{R}[x_i, \ldots, x_n] - \{g_i\}$, *we have* $h \equiv 0$ *mod* $\sqrt{\mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]}$.

Proof. Let $\mathrm{R}' := \mathrm{R}[x_2, \ldots, x_n]$, and $\mathrm{I}' := \mathrm{I} \cap \mathrm{R}'$. In view of Proposition 1.16, we may proceed by induction to conclude that the proposition holds for I'. and $g_2, \ldots, g_n \in \mathrm{G} \cap \mathrm{R}'$. Thus, we need only show I is primary if and only if both I' is primary and g_1 is a power of an irreducible polynomial modulo $\sqrt{\mathrm{I}'}$. In this case, $h \equiv 0 \bmod \sqrt{\mathrm{I}'}$ for $h \in \mathrm{G} - \{g_1\}$.

Clearly, we may conclude that I' is primary since I is primary. Let $lt(g_1) = c_1 x_1^{m_1}$. If h is an element of G other than g_1, then it must have degree less than m_1 in x_1. Otherwise, h would be (g_1, I)-reducible. Thus by Lemma 2.8 and the assumption that I' is primary, we have $h \equiv 0 \bmod \sqrt{\mathrm{I}'}$, proving the second part of the proposition. Since I is zero-dimensional, it is primary if and only if its radical is prime. By Lemma 2.9,

$$\sqrt{\mathrm{I}} = \sqrt{(g_1, \mathrm{I}')} = \sqrt{(g_1, \sqrt{\mathrm{I}'})}.$$

Thus, I is primary if and only if $(g_1, \sqrt{\mathrm{I}'})$ is primary, or equivalently, if and only if the ideal generated by g_1 in $(\mathrm{R}'/\sqrt{\mathrm{I}'})[x_1]$ is primary. ∎

Proposition 2.11 *Let* I *in* R[x] *be a zero-dimensional ideal such that* $\mathrm{I} \cap \mathrm{R}$ *is zero-dimensional prime. Let* G *be a minimal Gröbner basis for* I *with respect to the lexicographical order, and let* $g_1, \ldots, g_n \in \mathrm{G}$ *as in Proposition 2.6. Then* I *is prime if and only if* g_i *is irreducible modulo* $\mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$*, for all* i*. If this is the case, then* $\mathrm{G} = \{g_1, \ldots, g_n\} \cup (\mathrm{G} \cap \mathrm{R})$.

Proof. Suppose I is prime. By Proposition 2.10, we have $g_i \equiv h_i^{k_i}$ for some h_i irreducible modulo $\mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$. Since I is prime, we must have $h_i \in \mathrm{I}$. If $k_i > 1$, then g_i would be reducible by h_i, an element of smaller degree, contradicting the minimality of G. Thus, $k_i = 1$, and so g_i is irreducible mod $\mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$.

Conversely, suppose $\mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$ is prime and g_i is irreducible modulo $\mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$. Then $(g_i\,, \mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]) \subset \mathrm{R}[x_i, \ldots, x_n]$ is prime. Furthermore, if h is an element of $\mathrm{G} \cap \mathrm{R}[x_i, \ldots, x_n]$ other than g_i, then by the previous proposition, $h \equiv 0 \bmod \mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$. In particular, h is reducible modulo $\mathrm{G} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$, so from minimality of G, it follows that $h \in \mathrm{G} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]$. Thus,

$$\mathrm{G} \cap \mathrm{R}[x_i, \ldots, x_n] = \{g_i\} \cup (\mathrm{G} \cap \mathrm{R}[x_{i+1}, \ldots, x_n]),$$

and consequently,

$$\mathrm{I} \cap \mathrm{R}[x_i, \ldots, x_n] = (g_i\,, \mathrm{I} \cap \mathrm{R}[x_{i+1}, \ldots, x_n])$$

is prime. The proposition now follows by induction. ∎

2.3 Zero-dimensional Primary Decomposition

With the theory we have developed, we are now in the position to compute primary decomposition of zero-dimensional ideals. The aim of this section is two-fold. First, we will compute irredundant primary decomposition of zero-dimensional ideals in R[**x**]. Then we will compute primary decomposition of zero-dimensional ideals over a field of characteristic zero. In order to do the latter, we will introduce the notion of an ideal in "general position". Throughout this section, we will assume that for any given maximal ideal M in R, it is possible to factor univariate polynomials over finitely generated extensions of R/M.

Our first main result of this section is the computation of irredundant primary decomposition of zero-dimensional ideals in R[**x**]. In summary, we will compute the primary decomposition of $I \cap R[x_n]$. We will then extend this decomposition to a, not necessarily primary, decomposition of all of I, and then proceeding by induction, we will construct a complete primary decomposition of each component. The following proposition describes the induction step.

Proposition 2.12 *Let* I *in* R[**x**] *be a zero-dimensional ideal such that* $I \cap R$ *is* M-*primary, where* M *is a maximal ideal in* R. *Then it is possible to construct zero-dimensional ideals* $I_1, \dots, I_m$ *in* R[**x**] *and distinct maximal ideals* $M_1, \dots, M_m$ *in* $R[x_n]$ *such that* $I = \bigcap_i I_i$ *and such that* $I_i \cap R[x_n]$ *is* M_i*-primary.*

Proof. Let $I^c := I \cap R[x_n]$. By Lemma 2.9, we can find $g \in I^c$ such that $\sqrt{I^c} = \sqrt{(g\,,\, M)}$. Let $g(x_n) \equiv \Pi p_i(x_n)^{s_i}$ mod M be a complete factorization of g modulo M. That is, the images of $p_i(x_n)$ in $(R/M)[x_n]$ are pairwise comaximal irreducible non-units. Since $\Pi p_i{}^{s_i} \in (g\,,\, M) \subset \sqrt{I^c}$, we have $(\Pi p_i{}^{s_i})^s \in I^c$ for some s. Now, since p_i and p_j are comaximal modulo M, and I contains a power of M, then p_i and p_j are comaximal modulo I. Thus,

$$\bigcap_i (p_i^{s_i s}\,,\, I) = (\Pi p_i{}^{s_i s}\,,\, I) = I.$$

Let $\mathrm{I}_i := (p_i^{s_i s}, \mathrm{I})$, and $\mathrm{M}_i := (p_i, \mathrm{M})\mathrm{R}[x_n]$. Then M_i is clearly maximal, and since $\mathrm{I}_i \cap \mathrm{R}[x_n]$ contains a power of M_i, it is either M_i-primary or the unit ideal. We have $\Pi_{i \neq j} p_j{}^{s_j s} \mathrm{I}_i$ in I, so if $\mathrm{I}_i = (1)$, then

$$\Pi_{i \neq j} p_j \in \sqrt{\mathrm{I}^c} = \sqrt{(g\, ,\, \mathrm{M})}.$$

This contradicts the assumption that p_i is not a unit modulo M. Thus, I_i is M_i-primary. ■

By recursively applying the proposition to M_i and $\mathrm{I}_i \cap \mathrm{R}[x_1]$ over the ground ring $\mathrm{R}[x_n]$, we can compute the complete primary decomposition of I along with the associated primes.

We now proceed with the second part of the two-fold aim of this section. Here, we assume that K is a field of characteristic zero, and that all the Gröbner bases G are normalized so that $lc(g) = 1$ for all $g \in \mathrm{G}$.

If I is an ideal in $\mathrm{K}[\mathbf{x}] = \mathrm{K}[x_1, \ldots, x_n]$, set $\mathrm{I}_i := \mathrm{I} \cap \mathrm{K}[x_i, \ldots, x_n]$. If I is a zero-dimensional prime ideal, then by Proposition 2.11, every minimal Gröbner basis for I has the form $\{g_1(x_1, \ldots, x_n), g_2(x_2, \ldots, x_n), \ldots, g_n(x_n)\}$, with g_i a monic polynomial in x_i and irreducible modulo I_{i+1}. We can in fact obtain the following stronger result.

Proposition 2.13 *Let* I *be a zero-dimensional prime ideal in* $\mathrm{K}[\mathbf{x}]$, *and* $\mathrm{G} = \{g_1(x_1, \ldots x_n), \ldots, g_n(x_n)\}$, *a minimal Gröbner basis for* I *with respect to the lexicographical order. Then "almost all" linear transformations of coordinates,* $g_i = x_i - p_i(x_{i+1}, \ldots, x_n)$ *for* $i < n$.

Proof. By the proof of the primitive element theorem (Zariski and Samuel [Z-S]

Chapter 2.9), for almost all $a_1, \ldots, a_n \in \mathrm{K}$,

$$\mathrm{K}[\mathbf{x}]/\mathrm{I} \simeq \mathrm{K}(\sum a_i x_i).$$

If we choose new coordinates $z_1, \ldots, z_n$ such that $z_n = \sum a_i x_i$, then

$$\mathrm{K}[z_1, \ldots, z_n]/\mathrm{I} \simeq \mathrm{K}(z_n).$$

Now, since $z_i \in \mathrm{K}(z_n)$ for every i, we have that $z_i = f_i(z_n)$ holds in $\mathrm{K}[z_1, \ldots, x_n]/\mathrm{I}$, and hence, I contains polynomials of the form $z_i - f_i(z_n)$, for all $i < n$. If G is a Gröbner basis relative to the coordinates $z_1, \ldots, z_n$, then $z_i - f_i(z_n)$ is reducible modulo G. Now, since the only element of G which could reduce z_i is g_i, we have $lt(g_i) = z_i$ as required. ■

We now introduce the notion of an ideal in general position.

Definition 2.14 If I is a zero-dimensional prime ideal in $\mathrm{K}[\mathbf{x}]$ such that its lexicographical minimal Gröbner basis satisfies Proposition 2.13, we say that I is in *general position.* Furthermore, if I is an arbitrary zero-dimensional ideal, we say I is in general position if all of its associated primes are in general position and their contractions to $\mathrm{K}[x_n]$ are pairwise comaximal.

Corollary 2.15 *If* I *is a zero-dimensional primary ideal in general position, then the* g_i *in Proposition 2.10 are powers of linear equations modulo* $\sqrt{\mathrm{I}_{i+1}}$, *for* $i < n$.

As an example, consider the ideal

$$\mathrm{I} = (x_1^2 + 1\,,\, x_2) \subset \mathbf{Q}[x_1\,,\, x_2].$$

Now, x_2 is irreducible over $\mathbf{Q}$ and $x_1^2 + 1$ is irreducible over $\mathbf{Q}[x_2]/(x_2)$; so by Proposition 2.11, we have that I is a zero-dimensional prime ideal. It is not in general position because $x_1^2 + 1$ is not linear in x_1. If we make the substitution $x_2 = ax_1 + x_2$, and consider the ideal $I_a = (x_1^2 + 1\,,\, ax_1 + x_2)$, we find that $G_a = \{(ax_1 + x_2\,,\, x_2^2 + a^2)\}$ is a Gröbner basis for I_a whenever $a \neq 0$. In that case, G_a is as required in Definition 2.14. So we see that any nonzero value of a is sufficient to bring I into general position.

Remark 2.16 From the proof of Proposition 2.13, it follows that in order to put a zero-dimensional prime ideal into general position, it is sufficient to replace x_n by $x_n + \sum c_i x_i$ for random $c_i \in K$. Furthermore, it is always possible to put any zero-dimensional ideal in general position. The intent is to separate all the zeros in the algebraic closure by the last coordinate. To do so, we simply choose c_i such that all values $x_n + \sum c_i x_i$ are distinct as $(x_1, \ldots, x_n)$ ranges over the set of zeros of the ideal in the algebraic closure of K. The set of bad choices form a proper algebraic subset of K^{n-1}, and almost all choices of c_i are good.

Proposition 2.17 *Let* I *in* K[**x**] *be a zero-dimensional ideal in general position,* G *a lexicographical Gröbner basis for* I, *and let* $g_1, \ldots, g_n \in G$ *be as in Proposition 2.6. If* $g_n = \Pi p_i^{s_i}$ *is the irreducible decomposition of* g_n, *then* $I = \bigcap_i (p_i^{s_i}\,,\, I)$ *is the primary decomposition of* I.

Proof. $(p_i^{s_i}\,,\, I)$ is a zero-dimensional ideal. By definition of general position, $(p_i^{s_i}\,,\, I)$ is contained in exactly one prime ideal. Hence, it must be a primary ideal. ∎

If we are given a zero-dimensional ideal I, not necessarily in general position, then the above construction will yield a decomposition that is, not necessarily into primary components. If the minimal Gröbner basis for $(p_i^{s_i}\,,\, I)$ is not in the form predicted in

Corollary 2.4, then I is not in general position. We can then proceed by choosing a different set of coordinates. We remark, however, that a random substitution almost always works.

2.4 Primary Decomposition in Principal Ideal Domains

In this section we show how to reduce the general primary decomposition problem to the zero-dimensional case when the coefficient ring is a PID.

Lemma 2.18 *Let* S *be a multiplicatively closed subset of* R, *and* $s \in$ S. *If* $S^{-1}\mathrm{I} \cap \mathrm{R} \subset (\mathrm{I} : s)$, *then*

$$\mathrm{I} = (\mathrm{I} : s) \cap (\mathrm{I}, s).$$

Proof. The forward inclusion is clear. To prove the reverse inclusion, suppose $f \in (\mathrm{I} : s) \cap (\mathrm{I}, s)$, so that $f = i + as$, with $i \in \mathrm{I}$. Then $i + as \in (\mathrm{I} : s)$ implies $is + as^2 \in \mathrm{I}$. Thus, $a \in S^{-1}\mathrm{I} \cap \mathrm{R}$, and so $a \in (\mathrm{I} : s)$. This implies $as \in \mathrm{I}$, so we have $f \in \mathrm{I}$ as required. ∎

Combining the lemma with the construction of Proposition 1.22, we obtain the following fundamental decomposition mechanism.

Proposition 2.19 *Let* R *be an integral domain, and* (p) *a principal prime ideal in* R. *For any given ideal* I *of* R[x], *it is possible to find* $r \in \mathrm{R} - (p)$ *such that*

$$\mathrm{I} = (\mathrm{I}, r) \cap \mathrm{I}^{cc},$$

where $\mathrm{I}^{cc} = \mathrm{IR}_{(p)}[\mathrm{x}] \cap \mathrm{R}[\mathrm{x}]$.

Proof. By Proposition 1.22, we can find $s \in \mathrm{R} - (p)$ such that $\mathrm{I}^{cc} = \mathrm{IR}_s[\mathbf{x}] \cap \mathrm{R}[\mathbf{x}]$. Thus, we can compute I^{cc}. Since R is noetherian, there exists an m such that $s^m \mathrm{I}^{cc} \subset \mathrm{I}$. Given a Gröbner basis G for I^{cc} we can compute m by testing whether $s^m \mathrm{G} \subset \mathrm{I}$ for successive values of m. By the lemma, $r = s^m$ is as required. ∎

Remark 2.20 The preceding lemma and proposition are used to reduce the dimension of I. We choose s so that the dimension of (I, s) is strictly less than the dimension of I, and $(\mathrm{I} : s) = \mathrm{I}^{cc}$ is the contraction of the extension of I to the polynomial ring of lower dimension.

The following proposition gives a primary decomposition of an ideal I if $\mathrm{I} \cap \mathrm{R}$ is primary.

Proposition 2.21 *Let* R *be a PID,* I *an ideal in* $\mathrm{R}[\mathbf{x}]$, *and* (p) *a maximal ideal in* R. *If* $\mathrm{I} \cap \mathrm{R}$ *is* (p)*-primary, then it is possible to compute a primary decomposition for* I.

Proof. If I is zero-dimensional, then we can compute its decomposition using the propositions in Section 2.3. Otherwise, by Proposition 2.6, we can find an i such that $\mathrm{I} \cap \mathrm{R}[x_i]$ is not zero-dimensional. Let $\mathrm{R}' := \mathrm{R}[x_i]$ and $x' := x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, so that $\mathrm{R}'[\mathbf{x}'] := \mathrm{R}[\mathbf{x}]$, and $\mathrm{I} \cap \mathrm{R}'$ is not zero-dimensional. Applying Proposition 2.19, we can find $r' \in \mathrm{R}' - (p)\mathrm{R}'$ such that

$$\mathrm{I} = (\mathrm{I}, r') \cap \mathrm{I}^{cc} = \mathrm{IR}'_{(p)}[\mathbf{x}'] \cap \mathrm{R}'[\mathbf{x}'].$$

Thus, to decompose I it is sufficient to separately decompose (I, r') and I^{cc}.

Since $(\mathrm{I}, r') \cap \mathrm{R}'$ contains both the (p)-primary ideal $\mathrm{I} \cap \mathrm{R}$ and the element $r \notin (p)\mathrm{R}'$, either $(\mathrm{I}, r') \cap \mathrm{R}'$ is zero-dimensional or it is the unit ideal. In the former case, we can compute the primary decomposition of (I, r') by induction on the number of x_k such that the contraction of the ideal to $R[x_k]$ is not zero-dimensional. In the latter case, $I = I^{cc}$, and so we only need to compute the decomposition of I^{cc}.

In order to decompose I^{cc}, we only need to decompose $I^c = IR'_{(p)}[x']$, and then contract the decomposition back to $R'[x']$ using Proposition 1.22. Note, that $R'_{(p)}$ is again a PID, and $(p)R'_{(p)}$ is a maximal ideal. We claim that $I^c \cap R'_{(p)}$ is $(p)R'_{(p)}$-primary. Indeed, since $I \cap R$ is (p)-primary, then I, and hence $IR'_{(p)}$, contain a power of p. This is sufficient to show that $IR'[x'] \cap R' \subset (p)R'$. Let P be a nonzero-dimensional associated prime of $I \cap R'$. Then $(p)R' \subset P$. But $(p)R'$ is one dimensional, so $P = (p)R'$, which proves the claim. Thus. $I^c \subset R'_{(p)}[x']$ satisfies the hypothesis of the proposition, and so we may decompose it by induction on the number of variables. ∎

Corollary 2.22 *If* K *is a field, then it is possible to compute the primary decomposition of any ideal in* $K[x]$.

Proof. Take $p = 0$ in the proposition.

Here is the central result which computes primary decomposition of any given ideal in the case where the coefficient ring is a PID.

Proposition 2.23 *Let* R *be a PID, and* I *an ideal in* $R[x]$. *Then it is possible to compute a primary decomposition for* I.

Proof. If $I \cap R$ is not zero-dimensional, that is, $I \cap R = 0$ and R is not a field, then apply Proposition 2.19 to $(0) \subset R$ to find $r \neq 0$ such that

$$I = (I, r) \cap (IR_{(0)}[x] \cap R[x]).$$

Since $R_{(0)}$ is a field, $IR_{(0)}[x]$ can be decomposed using Corollary 2.5, and the results contracted to $R[x]$ using Proposition 2.19. We are then left with $(I : r)$, which contracts to a zero-dimensional ideal in R.

Thus, we may assume I $\cap$ R is zero-dimensional, say I $\cap$ R $= (\Pi p_i^{m_i})$, where (p_i)R is maximal. Then $(p_i^{m_i}$, I) $\cap$ R is (p_i)-primary. Hence, $(p_i^{m_i}$, I) can be decomposed using Proposition 2.21. Since I $= \bigcap_i (p_i^{m_i}$, I), we get a decomposition for I. ■

Remark 2.24 The decomposition obtained above is not irredundant.

Chapter 3

Algorithms

In this chapter we present algorithms for computing various aspects of primary decomposition of polynomial ideals. In each case we outline the basic steps, and we disregard questions of efficiency.

Algorithm PT : Primality Test.

Input: A ring R, variables $x = x_1, \ldots, x_n$, and an ideal $\mathrm{I} \subset \mathrm{R}[\mathbf{x}]$.

Assumptions: None.

Output: If I is prime, return TRUE. Otherwise, return FALSE.

1. If $n = 0$, and if $\mathrm{I} \subset \mathrm{R}$ is prime, then return TRUE. Otherwise, return FALSE.

2. Compute $\mathrm{J} := \mathrm{I} \cap \mathrm{R}[x_2, \ldots, x_n]$.

3. If $PT(\mathrm{R}; x_2, \ldots, x_n; \mathrm{J}) =$ FALSE, then return FALSE.

4. Let $\mathrm{R}' := \mathrm{R}[x_2, \ldots, x_n]/\mathrm{J}$, $\mathrm{I}' := \mathrm{IR}'[x_1]$, and K' the quotient field of R'.

5. Compute $\mathrm{I}'\mathrm{K}'[x_1] = (f)$.

6. If f is not irreducible over K', then return FALSE.

7. Compute $\mathrm{I}^{cc} = \mathrm{I}'\mathrm{K}'[x_1] \cap \mathrm{R}'[x_1]$.

8. If $\mathrm{I}^{cc} \subset \mathrm{I}'$, then return TRUE. Otherwise, return FALSE.

Algorithm ZPD : Zero-dimensional Primary Decomposition.

Input: A ring R, variables $x = x_1, \ldots, x_n$, an ideal $\mathrm{I} \subset \mathrm{R}$, and an ideal $\mathrm{M} \subset \mathrm{R}$.

Assumptions: M is maximal, I is zero-dimensional, and $\mathrm{I} \cap \mathrm{R}$ is M-primary.

Output: $\{(Q_1, M_1), \ldots, (Q_m, M_m)\}$, where Q_i and M_i are ideals in $\mathrm{R}[\mathbf{x}]$ such that M_i is maximal, and for $M_i \neq M_j$, we have Q_i is M_i-primary. Then $\mathrm{I} = \bigcap_i Q_i$.

1. If $n = 0$, then return $\{(\mathrm{I}, \mathrm{M})\}$.

2. Compute a minimal Grobner basis G for $\mathrm{I} \cap \mathrm{R}[x_n]$.

3. Select the $g \in \mathrm{G}$ of largest degree.

4. Compute the factorization of g modulo M,

$$g = \Pi p_i^{s_i} \text{ in } \mathrm{R}/\mathrm{M}[x_n], \text{ where } p_i \in \mathrm{R}[x_n].$$

5. Find s such that $(\Pi p_i^{s_i})^s \in \mathrm{I} \cap \mathrm{R}[x_n]$.

6. Let $\mathrm{I}_i := (p_i^{s_i s}, \mathrm{I})$, and $\mathrm{M}_i := (p_i, \mathrm{M})\mathrm{R}[x_n]$.

7. Return $\bigcup_i ZPD(\mathrm{R}[x_n]; x_1, \ldots, x_{n-1}; \mathrm{I}_i; \mathrm{M}_i)$.

Comments. The primary decomposition resulting after Step 7 is irredundant. This algorithm can also compute the associated primes.

Algorithm ZPDF : Zero-dimensional Primary Decomposition over a Field.

Input: A field K, variables $x = x_1, \ldots, x_n$, and an ideal $\mathrm{I} \subset \mathrm{K}[\mathbf{x}]$.

Assumptions: K is a field of characteristic zero, and I is zero-dimensional.

Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset$ K[x] is a primary ideal, I $= \bigcap_i Q_i$, and $\sqrt{Q_i} \neq \sqrt{Q_j}$.

1. Select at random $c_1, \ldots, c_{n-1} \in$ K and replace x_n by $x_n + \sum c_i x_i$.
2. Compute I $\cap$ K[x_n] $= (g)$.
3. Compute the complete factorization of g, so that $g = \Pi p_i^{s_i}$.
4. If ($p_i^{s_i}$, I) is not a primary ideal in general position, then go to Step 1.
5. Replace x_n by $x_n - \sum c_i x_i$.
6. Return $\{(p_i^{s_i}$, I$)\}$.

Comments. The computation in Step 2 follows from the results in Proposition 1.16. In Step 4, it would be sufficient to test ($p_i^{s_i}$, I) for being primary using Proposition 2.10, but the simpler test of Corollary 2.4 will be satisfied in almost all cases.

Algoirithm PPD-0 : Primary Decomposition over a PID, Primary Contraction Case.

Input: A ring R, variables $x = x_1, \ldots, x_n$, an ideal I $\subset$ R[x], and $p \in$ R.

Assumptions: R is a PID.

Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset$ R[x] is primary, and I $= \bigcap_i Q_i$.

1. If I is zero-dimensional, then return its decomposition using Alogorithm ZPD or Algorithm ZPDF.
2. Find i such that I $\cap$ R[x_i] is not zero-dimensional.

```
3. Let $\mathrm{R}' := \mathrm{R}[x_i]$, $x' := x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$, and $\mathrm{I}^c = \mathrm{I}\mathrm{R}'_{(p)}[\mathbf{x}']$.
4. Find $r' \in \mathrm{R} - (p)\mathrm{R}'$ such that
       $\mathrm{I} = (\mathrm{I}, r') \cap (\mathrm{I}^c \cap \mathrm{R}'[\mathbf{x}])$.
5. Let $\{Q_1, \ldots, Q_m\} := PPD - 0(\mathrm{R}'_{(p)}; \mathbf{x}'; \mathrm{I}^c; p)$.
6. Let $Q_i^c := Q_i \cap \mathrm{R}'[\mathbf{x}']$.
7. If $(\mathrm{I}, r') = (1)$, then return $\{Q_1^c, \ldots, Q_m^c\}$.
8. Let $\{Q_1', \ldots, Q_k'\} := PPD - 0(\mathrm{R}; \mathbf{x}; (\mathrm{I}, r'); p)$.
9. Return $\{Q_1^c, \ldots, Q_m^c, Q_1', \ldots, Q_k'\}$.
```

Comments. At the point where Algorithm PPD-0 is ready to call Alogorithm ZPD or Algorithm ZPDF, we have reduced the problem to a zero-dimensional ideal whose contraction to R, the underlying PID, is (p)-primary.

Algorthm PPD: Primary Decomposition over a PID.

Input: A ring R, variables $x = x_1, \ldots, x_n$, and an ideal $\mathrm{I} \subset \mathrm{R}[\mathbf{x}]$.

Assumptions: R is a PID.

Output: $\{Q_1, \ldots, Q_m\}$ such that $Q_i \subset \mathrm{R}[\mathbf{x}]$ is primary, and $\mathrm{I} = \bigcap_i Q_i$.

```
1. Find $r \neq 0$ such that
       $\mathrm{I} = (\mathrm{I}, r) \cap (\mathrm{I}\mathrm{R}_{(0)}[\mathbf{x}] \cap \mathrm{R}[\mathbf{x}])$.
2. Let $\{Q_1, \ldots Q_k\} := PPD - 0(\mathrm{R}_{(0)}; \mathbf{x}; \mathrm{I}\mathrm{R}_{(0)}[\mathbf{x}]; 0)$.
3. Let $Q_i^c := Q_i \cap \mathrm{R}[\mathbf{x}]$.
```

4. Compute $(\mathrm{I}\,, r) \cap \mathrm{R} \;=\; (r')$.

5. If r' is a unit, then return $\{Q_1^c, \ldots, Q_m^c\}$.

6. Factor $r' \;=\; \Pi p_i^{m_i}$, with p_i irreducible.

7. For each i, let $\{Q_1^i, \ldots, Q_{k_i}^i\} \;:=\; PPD - 0(\mathrm{R};\, \mathrm{x};\, (\mathrm{I}\,,\, p_i^{m_i});\, p_i)$.

8. Return $\{Q_1^c, \ldots, Q_k^c\} \bigcap_i \{Q_1^i, \ldots, Q_{k_i}^i\}$.

Comments. The correctness of Step 1 follows from Proposition 2.19.

Bibliography

[A-D] Adams, W., and Loustaunau, P., *An Introduction to Gröbner Bases* (Graduate Studies in Mathematics, Volume 3, American Mathematical Society, New York, 1994).

[A-M] Atiyah, M., and Macdonald, I., *Introduction to Commutative Algebra* (Addison-Wesley, Massachusetts, 1969).

[B] Buchberger, B., *Ein algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal* (Ph.D Thesis, Universitat Innsbruck, 1965).

[C-L-O] Cox, D., Little, J., O'Shea, D., *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra* (Springer-Verlag, New York, 1992).

[G-T-Z] Gianni, P., Trager, B., Zacharias, G., *Gröbner Bases and Priimary Decomposition of Polynomial Ideals* (Journal of Symbolic Computation **6**(1988), p. 149-167).

[L] Lasker, E., *Zur Theorie der Modulin und Ideale* (Math. Ann. Bd. **60**(1905), p. 20-116).

[M] Macaulay, F., *Algebraic Theory of Modular Systems* (Cambridge Tracts in Mathematics, Volume 19, Cambridge, 1916).

[N] Noether, E., *Ideal Theorie in Ringbereichen* (Math. Ann. Bd. **83**(1921), p. 24-66).

[Z-S] Zariski, O., Samuel, P., *Commutative Algebra, Volume 1* (Graduate Text in Mathematics, Volume 28, Springer-Verlag, Neildeberg, 1975).