Applications of Algebraic Geometry to Coding & Cryptography

by

William Erik Anderson

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Master of Science in Electrical Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2001

Author ....
Department of Electrical Engineering and Computer ~~Science~~
May 25, 2001

Certified by ....
Vahid Tarokh
Associate Professor
Thesis Supervisor

Accepted by ....
Arthur C. Smith
Chairman, Department Committee on Graduate Students

Applications of Algebraic Geometry to Coding & Cryptography

by

William Erik Anderson

Submitted to the Department of Electrical Engineering and Computer Science
on May 25, 2001, in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering

Abstract

In this thesis, we develop a geometric foundation for classical coding over fields and commutative rings using modern algebraic geometry and the language of schemes. Using this framework we construct an equivalence between the category of geometric linear codes over $\operatorname{Spec} k$ and linear codes over k. We also study the minimum distance properties of codes under base changes and localizations. Finally, we give an introduction to elliptic curve cryptography.

Thesis Supervisor: Vahid Tarokh
Title: Associate Professor

Acknowledgments

I would like to thank all the people who supported and encouraged me throughout my academics here at MIT. I would especially like to thank my mother and sister. Your love and support, were invaluable, and I love you dearly.

I would also like to thank my friends back in California for all the wonderful memories. It seems like only yesterday we were having lunch and discusing the philosophy of mathematics and engineering.

I would like to pay special thanks to the faculty and students in the Laboratory for Information and Decision Systems (LIDS) and MIT Mathcmatics Department for the wonderful and stimulating environment.

Many thanks, to James Kang, Alan Radnitz, and Weiqing Xie. You were a wonderful source of inspiration. Thank you for encouraging me to pursue my dreams and aspirations.

Finally, I would like to thank my advisor Vahid Tarokh, for his encouragement and understanding. You are one of those few great engineers who has a flare for learning and brilliant capacity to pursue new ideas.

Lastly, I would like to thank the National Science Foundation for their sponsorship and financial support of this project.

Contents

Chapter 1

Introduction

Since the beginning of the era of communications, researchers have tried to find new ways of improving the quality and secrecy of communications. A major breakthrough was due to Shannon who showed that both reliable and private communication is achievable as long as the transmission is less than a fundamental quantity, namely the capacity. Unfortunately, Shannon's construction were worse case designs in the sense that his channel codes lacked any structure and were random. Also, his ciphers were not the best constructive ciphers, since they had the structure of random noise. Following the invention of random coding and cryptography by Shannon, many researchers tried to improve upon his methods. For codes to be useful in communications they need to have structure and simple encoding and decoding techniques. For cryptographic systems, they need to be computationally feasible and secure even if partial information about the cipher is known.

1.1 Structure of Linear Codes

In 1960 Slepian [14] introduced the first structure theory for binary linear codes. He proved that every linear code is the sum of *indecomposable codes* and that the best codes for a given block length and dimension are indecomposable. (An indecomposable code is any code that is not the direct sum of two other codes). His goal was to derive a canonical form for the generator matrix of an equivalence class of codes, so that he could read off the properties from the generator matrix. Although we now know this is impossible, he raised the question on whether a suitable representation theory existed for linear codes.

Following Slepian a somewhat more abstract approach was taken by E.F. Assmus, H.F. Mattson [3] and Ross [12]. Recently the topic has been revisited by E.F. Assmus [2]. Assmus defined what he calls *critical indecomposable codes* which is an indecomposable code such that the removal of any column of the generator matrix results in a decomposable code. He shows that every indecomposable code can be obtained from a critical indecomposable code by appending columns to the generator matrix. In this light, this improves upon Slepians method and moves one step closer to a representation theory.

In this thesis, we develop a general theoretical framework for geometric systems having error structures. Our main motivation will be to use this framework to study classical codes over commutative rings and fields. To this end, we will use the basic language of category theory to lay out the foundation. To integrate error structure into our geometries, we introduce the notion of a diagram of group schemes over a directed graph. This allows us to define classical coding errors and more general geometric error structures. Our codes will be taken as the R-valued points of a subscheme of $\mathbb{A}^n_R$ over a commutative ring R. In the case $R = k$ is a field, the points correspond to the k-rational points. Our definition of a code is motivated by the fact that every non-singular algebraic variety X over the complex numbers $\mathbb{C}$ has a natural structure as a complex manifold over it's $\mathbb{C}$-rational points $X(\mathbb{C})$. Therefore every non-singular code X can be looked at as a submanifold $X(\mathbb{C}) \hookrightarrow \mathbb{C}^n$.

The above definition of a code allows for a much broader analysis of coding and error structures. Although we will not explicitly review quantum coding in this thesis, the above complex analytic interpretation can easily fit to model quantum structures.

Finally, we give a brief introduction to elliptic curve cryptography. Using the Riemann-Roch Theorem and divisors we construct an abelian group over the rational points of an elliptic curve. For a more complete account of cryptography we refer the reader to the main reference, [8].

1.2 Thesis Outline

The outline of this thesis is as follows. In Chapter 2, we introduce classical algebraic coding over an algebraically closed field. The ideas in Chapter 2 are intended to help motivate Chapter 3, where we generalize our geometry to the more modern language of schemes. We will place special emphasis on the functorial point of view, since applications arise naturally in this setting. In Chapter 3, we review sheaves, schemes, sheaves of modules, functor of points, groups schemes, and G-spaces. These topics are needed for the next chapter where we discuss coding. In Chapter 4, we give a general framework for geometric systems with error structures. Using this framework we construct an equivalence between the category of geometric linear codes over $\operatorname{Spec} k$ and linear codes over k. We also study the minimum distance properties of codes under base changes and localisations. In Chapter 5, we give an introduction to elliptic curve cryptography.

Included at the end, is an appendix on Category Theory. The first four chapters assume Category Theory as a prerequisite. To fully obtain a complete coherence of the material it is recommended that the reader have a background in commutative algebra and algebraic geometry. One can find a more self contained treatment in any of the main references- [4], [7], [10], or [11].

Chapter 2

Classical Algebraic Geometry

As a preparation for scheme theory, we will first review the classical treatment of algebraic geometry over an algebraically closed field. For a more complete account of the material, we refer the reader to, [7], [11]. In the following section we will give a brief introduction to sheaf theory and schemes. We will focus most of our attention on the functorial point of view, since applications arise naturally in this setting.

2.1 Algebraic Sets

In the most naive sense, algebraic geometry may be described as the study of all solutions to a system of equations

$$f_i(x_1, \dots , x_n) = 0, \qquad i = 1, \dots , l$$

with coefficients in a field k. This is a rather vague statement, since simultaneous solutions may not exist. For example in the case of the polynomial $x^2+y^2+1 = 0$ over the field of real numbers, there are no solutions. If the field is enlarged to include the complex numbers then there are many solutions. This fact has a natural geometric interpretation given by the Hilbert Nullstellensatz, which we will describe shortly.

Definition 2.1.1. Let k be an algebraically closed field. The set of n-tuples $(a_1, \dots, a_n)$ of elements k in k^n, is called the *affine n-space* over k.

We will denote the set of all solutions to a system of equations as the set

$$V(f_1, \dots, f_l) := \{ (a_1, \dots, a_n) \in \mathbb{A}^n \mid f_i(a_1, \dots, a_n) = 0 \text{ for each } i = 1, \dots, l \}$$

Observe that if we take the ideal $(f_1, \dots, f_l) \subseteq k[x_1, \dots, x_n]$ generated by the polynomials f_i, then any element $g \in (f_1, \dots, f_l)$ is necessarily zero over $V(f_1, \dots, f_l)$. Therefore we will view the set $V(f_1, \dots, f_l)$ as the set of solutions of the ideal generated by the polynomials f_i, $i = 1, \dots, l$.

Theorem 2.1.1 (Weak Nullstellensatz). *Let k be any field. If $\mathfrak{m}$ is a maximal ideal of a polynomial ring $k[x_1, \dots, x_n]$, then the residue field*

$$k[x_1, \dots, x_n]/\mathfrak{m} = k(\mathfrak{m})$$

is a finite dimensional vector space over k.

In the case our field is algebraically closed we have the following corollary.

Corollary 2.1.2. *A maximal ideal of the polynomial ring $k[x_1, \dots, x_n]$ over an algebraically closed field k has the following form,*

$$(x_1 - a_1, \dots, x_n - a_n), \qquad a_i \in k$$

Proof. Let $\mathfrak{m} \subset k[x_1, \dots, x_n]$ be a maximal ideal and consider the k-algebra homomorphism,

$$k \to k[x_1, \dots, x_n]/\mathfrak{m} = k(\mathfrak{m})$$

By theorem 2.1.1, $k(\mathfrak{m})$ is a finite dimensional vector space over k. Since k is algebraically closed the above map must be an isomorphism, since every finite extension of an algebraically closed field is the original field. Taking the value $x_i = a_i$, $a_i \in k$, for each i, we have $(x_1 - a_1, \dots, x_n - a_n) \subseteq \mathfrak{m}$. □

Therefore,

Corollary 2.1.3. *If an ideal I in the polynomial ring $k[x_1, \dots, x_n]$ over an algebraically closed field does not contain the identity, then $V(I) \neq \emptyset$.*

From the above corollary, we can conclude every system of polynomials f_i, $i = 1, \dots, l$, that does not generate the unit element has a solution.

The sets $\{\, \mathbb{A}^n \setminus V(I) \mid I \subset k[x_1, \dots, x_n] \,\}$ form a topology on $\mathbb{A}^n$, since $V(I) \cup V(J) = V(I \cdot J)$ and $\cap V(I_\alpha) = V(\Sigma I_\alpha)$. We will refer to this as the *Zariski Topology* on $\mathbb{A}^n$. The Zariski topology is almost never Hausdorff, since open sets are very large. For instance, every closed set in $\mathbb{A}^1$ has a finite number of points and therefore every open set has an infinite number of points. We will call the closed sets of the Zariski topology *algebraic sets.* When a closed set is topologically irreducible we will call it an *irreducible algebraic set.*

Ultimately, we would like to assign some algebra to our geometry. To do this we define the ideal $I(V)$ over an algebraic set V as,

$$I(V) = \{\, f \in k[x_1, \dots, x_n] \mid f(a_1, \dots, a_n) = 0 \text{ for all } (a_1, \dots, a_n) \in V \,\}$$

and the corresponding *coordinate ring* of V as,

$$k[V] := k[x_1, \dots, x_n]/I(V)$$

The ideal $I(V)$ is necessarily a radical ideal since, f^n vanishes on V implies f also vanishes. A radical ideal is any ideal such that $f^n \in I$ implies $f \in I$. We usually write a radical ideal as $\sqrt{I}$. If A is any algebra with the property $a^n = 0$ implies $a = 0$, then we call it a nilpotent free algebra. Therefore, the coordinate ring $k[V]$ is a finitely generated nilpotent free k-algebra.

Definition 2.1.4. A pair $(V, k[V])$ consisting of an algebraic set V and it's coordinate ring $k[V]$ is said to be an *affine algebraic variety* or more simply *affine variety.*

Proposition 2.1.5. *For an algebraic set V, there exists a one-to-one correspondence between the points on V and the maximal ideals in $k[V]$.*

Proof. Observe, by corollary 2.1.2 every maximal ideal of the coordinate ring,

$$k[V] = k[x_1, \ldots, x_n]/I(V)$$

has the form $(x_1 - a_1, \ldots, x_n - a_n)$, $a_i \in k$. But, this implies $(a_1, \ldots, a_n) \in V$. Similarly give any point in V we can construct a maximal ideal containing $I(V)$. □

A morphism between two affine varieties $(V, k[V])$ and $(W, k[W])$ is a pair $(\phi, \phi^{\#})$, with a continuous map $\phi : V \to W$, and k-homomorphism $\phi^{\#} : k[W] \to k[V]$ satisfying $\phi^{\#-1}(\mathfrak{m}_a) = \mathfrak{m}_b$ for every maximal ideal $\mathfrak{m}_a$ and $\mathfrak{m}_b$, whenever $\phi(a) = b$. Note that for any k-homomorphism $\psi : S \to R$ between k-algebras, the inverse image of a maximal ideal of R is a maximal ideal of S. This is clear, since for any maximal $\mathfrak{m} \subset R$, the image $S/\psi^{-1}(\mathfrak{m}) \to R/\mathfrak{m} = k$ is surjective.

We write a morphism as,

$$(\phi, \phi^{\#}) : (V, k[V]) \to (W, k[W])$$

If ϕ is homeomorphic and $\phi^{\#}$ a k-isomorphism, then the morphism $(\phi, \phi^{\#})$ is said to be an isomorphism.

Example 2.1.6. Consider the curve $C = V(y^2 - x^3) \subseteq \mathbb{A}^2$ and the affine line $\mathbb{A}^1$. We define a morphism $\phi : \mathbb{A}^1 \to C$, by the map $a \mapsto (a^2, a^3)$ and k-algebra homomorphism,

$$\begin{aligned} \phi^{\#} : k[x,y]/(y^2 - x^3) &\to k[t] \\ f(x,y) &\mapsto f(t^2, t^3) \end{aligned}$$

Checking one discovers that ϕ is a homeomorphism, but $\phi^{\#}$ is not an isomorphism. Therefore two affine varieties that are topologically equivalent does not imply their coordinate rings are. The above example fails since the curve $y^2 - x^3$ has a singularity at the point $(0, 0)$.

We finish our discussion on classical algebraic geometry, by stating a classical result that is at the very essence of Algebraic Geometry, since it constructs a bridge between geometric objects and algebra. First, we need a lemma that shows that every finitely generated nilpotent free k-algebra comes from an affine variety.

Lemma 2.1.7. *For any finitely generated nilpotent free k-algebra A, there exists an affine variety $(V, k[V])$ such that $k[V] = A$.*

Proof. Since A is a finitely generated k-algebra there exists a surjective map,

$$k[x_1, \ldots, x_n] \twoheadrightarrow A$$

for some n. Taking the radical ideal $J \subset k[x_1, \ldots, x_n]$ such that $k[x_1, \ldots, x_n]/J \cong A$, we claim that $(V(J), k[V(J)])$ is the desired affine variety. Indeed, it is enough to check $I(V(J)) = J$. Let $f \in I(V(J))$, then $f(x) = 0$ for every $x \in V(J)$. By corollary 2.1.2, $f \in \bigcap_{\mathfrak{m} \supseteq J} \mathfrak{m}$; but $\bigcap_{\mathfrak{m} \supseteq J} \mathfrak{m} = \sqrt{J} = J$. □

Proposition 2.1.8. *Let $(V, k[V])$ be an affine variety. Then the contravariant functor*

$$(V, k[V]) \mapsto k[V]$$

taking an affine variety to it's coordinate ring induces an arrow reversing equivalence between the category of affine varieties over an algebraically closed field k and the category of finitely generated nilpotent free k-algebras.

For proof see §I.3.8 of [7].

Chapter 3

Modern Algebraic Geometry

In the previous section we showed there is a one-to-one correspondence between affine varieties and finitely generated nilpotent free k-algebras over an algebraically closed field k. More generally we are interested in extending the above case by replacing k-algebras with commutative rings. Naturally, this raises the question, of what type of geometry is needed? The answer turns out to be a *scheme.*

The construction of schemes parallels the definition of a differentiable manifold. Instead of taking a topological space $\mathcal{M}$ that is locally homeomorphic to an open subset of $\mathbb{R}^n$ and a sheaf of differentiable functions $C^\infty(\mathcal{M})$, a scheme is a topological space glued together by affine schemes with a corresponding sheaf of regular functions.

We begin by defining the spectrum of a ring, sheaf, and the associated structure sheaf of a ring. This will eventually lead us to the definition of an affine scheme, and more generally schemes.

Definition 3.0.9. Let A be a commutative ring with unit. We define Spec$A$ called the *spectrum* of A, to be the set of all prime ideals contained in A.

Each prime ideal $\mathfrak{p}$ can be viewed as a point in the set Spec A. The spectrum of a ring has a natural topological structure called the *Zariski* topology. A closed subset with respect to an ideal $I \subset A$, is defined as the set of elements

$$V(I) = \{\, \mathfrak{p} \in \mathrm{Spec}A \mid f(\mathfrak{p}) = 0 \text{ for all } f \in I\}$$

The evaluation of f at a point $\mathfrak{p}$ is the image of f in the residue field $k(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ induced by the canonical map $A \to A_\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. We use the notation $A_\mathfrak{p}$ to denote the local ring at a prime ideal $\mathfrak{p}$. The local ring $A_\mathfrak{p}$ is defined as the ring of elements r/s, such that $r, s \in A$ and $s \in A \setminus \mathfrak{p}$, with equivalence relation $r/s = r'/s'$ whenever there exists $t \in A \setminus \mathfrak{p}$ satisfying $t(rs' - r's) = 0$.

To show Spec$A$ is a topological space it is enough to check that both the intersection of an arbitrary collection of closed sets and the finite union of closed sets, is closed. This follows immediately since for any two ideals $I, J \subset A$, $V(I) \cup V(J) = V(I \cdot J)$ and for any arbitrary collection of ideals $\{I_\alpha\}$ in A, $\cap V(I_\alpha) = V(\Sigma I_\alpha)$.

Example 3.0.10. Consider the affine line $\mathbb{A}^1_k = \mathrm{Spec}\, k[t]$ over a finite field k. The points in $\mathbb{A}^1_k$ correspond to the (0) ideal and the irreducible polynomials contained in $k[t]$. A point x is closed if and only if the residue field $k(x)$ is a finite field extension of k.

Definition 3.0.11. An important type of open set are the distinguished open sets. A *distinguished* open set associated to an element $f \in A$, is defined as $D(f) := \mathrm{Spec}A \setminus V(f) \cong \mathrm{Spec}A_f$.

This corresponds to all the points in Spec$A$ where $f(\mathfrak{p}) \neq 0$. The distinguished open sets naturally forms a basis for the Zariski topology, since every open set has the form $U = \mathrm{Spec}A \setminus V(I) = \cup_{f \notin I} D(f)$.

We remark that the spectrum of a ring is a basic generalization of the points on an affine variety given by Definition 2.1.4. In fact, for any affine variety Y over an algebraically closed field, the maximal ideals m-Spec $k[Y]$ of the affine coordinate ring $k[Y]$ is naturally homeomorphic to Y, given the induced topology. So in general, the spectrum of a ring adds more points, increasing the geometric information. This is perhaps most clearly reflected in Example 3.0.10, if we take the field k to be algebraically closed. In classical algebraic geometry the points on the affine variety correspond to the maximal ideals $\{(t-a)\}_{a\in k}$. However, we have added one more point in $\operatorname{Spec} k[t]$, namely the (0) ideal whose closure is all of $\mathbb{A}^1_k$.

3.1 Sheaves

An important concept in modern geometry is the notion of a sheaf. Sheaves are classical structures, originating out of set theory and can be conveniently described as a family of sets with certain relations. The main motivation for using sheaves in algebraic geometry is to add local structure to our geometries. We begin by first describing presheaves, a precursor to sheaves.

Definition 3.1.1. Let X be a topological space. A *presheaf* $\mathcal{F}$ of sets on X consists of the following:

1. for each open set $U \subseteq X$, assign a set $\mathcal{F}(U)$

2. for every nested pair of open sets $V \subset U \subseteq X$ a restriction map $\rho_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$

satisfying

3. $\rho_{U,U}$ is the identity map

4. $\rho_{U,V} \circ \rho_{V,W} = \rho_{U,W}$ for all $W \subset V \subset U \subseteq X$.

Equivalently, we can define a presheaf to be a contravariant functor $\mathcal{F} : \mathbf{Top}(X) \to$ **Sets** taking open sets in X, to sets. A presheaf of abelian groups, rings, or algebras are defined in a similar way by changing the category of **Sets** to the categories **Ab**, **Rngs**, or **Alg**.

Example 3.1.2. Consider $\operatorname{Spec}\mathbb{Z}_6 = \{(2),(3)\}$ consisting of two closed points. Define $\mathcal{F}(\operatorname{Spec}\mathbb{Z}_6) = \mathbb{Z}_6$, $\mathcal{F}((2)) = \mathbb{Z}_3$, $\mathcal{F}((3)) = \mathbb{Z}_3$, and $\mathcal{F}(\emptyset) = 0$ with canonical map $\mathbb{Z}_6 \to \mathbb{Z}_3$. Then $\mathcal{F}$ defines a presheaf on $\operatorname{Spec}\mathbb{Z}_6$.

The elements of $\mathcal{F}(U)$ are called the *sections* of $\mathcal{F}$ over U and *global sections* if $U = X$.

Definition 3.1.3. A presheaf $\mathcal{F}$ on a topological space X is called a *sheaf*, if it satisfies the following axiom. Namely for every open set V and open covering $\{U_\alpha\}$ of V with elements $f_\alpha \in \mathcal{F}(U_\alpha)$ satisfying $\rho_{U_\alpha,U_\alpha\cap U_\beta}(f_\alpha) = \rho_{U_\beta,U_\alpha\cap U_\beta}(f_\beta)$, there exists a unique $f \in \mathcal{F}(V)$ such that $\rho_{V,U_\alpha}(f) := f|_{U_\alpha} = f_\alpha$ for every α.

Example 3.1.4. The above example does not form a sheaf since we can take $2 \in \mathcal{F}((2)) \cap \mathcal{F}((3))$ which satisfies the criterion $2|_{(2)\cap(3)} = 0$, however there does not exist a unique element $f \in \mathcal{F}(\operatorname{Spec}\mathbb{Z}_6)$ whose restriction over the points $\{(2)\}$ and $\{(3)\}$ give 2, since both $2, 5 \in \mathcal{F}(\operatorname{Spec}\mathbb{Z}_6)$ both map $2|_{(2)} = 5|_{(2)} = 2$ and $2|_{(3)} = 5|_{(3)} = 2$. If we instead replace $\mathcal{F}((2))$ with $\mathbb{Z}_2$, then we have a sheaf.

Definition 3.1.5. The *stalk* of a presheaf at a point $x \in X$ contains important information about the presheaf. We define the stalk $\mathcal{F}_x$ at x to be the direct limit

$$\mathcal{F}_x := \varinjlim_{x\in U} \mathcal{F}(U)$$

Equivalently, the stalk is the initial object in the category of $\mathbf{CoCones}(\Sigma, \mathrm{Top}(X))$ over the filtered diagram of open sets containing the point x. Since the open sets containing x are filtered under inclusion, it follows by corollary A.2.6, that $\mathcal{F}_x$ has a natural abelian group, ring, or module structure whenever the collection $\{\mathcal{F}(U)\}$ are respectively abelian groups, rings, or modules. Moreover, the stalk can be looked at as the collection of objects $(V,t) \in \cup_{x\in U, s\in\mathcal{F}(U)}(U,s)/\sim$, under the equivalence relation $(U,s) \sim (V,t)$ whenever there exists $W \subseteq U \cap V$ with $\rho_{U,W}(s) = \rho_{V,W}(t)$.

A morphism $\phi : \mathcal{F} \to \mathcal{G}$ between two presheaves on a topological space X is defined as the collection of maps $\phi_U : \mathcal{F}(U) \to \mathcal{G}(U)$ satisfying the commutative diagram

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\phi_U"] \arrow[d, "\rho_{U,V}"'] & \mathcal{G}(U) \arrow[d, "\rho'_{U,V}"] \\
\mathcal{F}(V) \arrow[r, "\phi_V"] & \mathcal{G}(V)
\end{tikzcd}$$

for every inclusion $U \subset V$. Equivalently, we can say a morphism between two presheaves is a natural transformation between the functors $\mathcal{F}, \mathcal{G} : \mathbf{Top}(X) \to \mathbf{Sets}$. Observe from the definition we have an induced map on the stalks $\phi_x : \mathcal{F}_x \to \mathcal{G}_x$ for each $x \in X$. The following proposition illustrates how stalks preserve information about the sheaves.

Proposition 3.1.6. *Let $\phi : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves on a topological space X. Then ϕ is a monomorphism(respectively epimorphism) if and only if the induced map on the stalk $\phi_x : \mathcal{F}_x \to \mathcal{G}_x$ is a monomorphism(respectively epimorphism).*

See §II.1.1 [7] for proof.

There is a natural sheaf structure associated to the spectrum of a ring. Conceptually, we would like to make each element $f \in A$ behave as much like a continuous function as possible. The only difficulty is that f takes values in different residue fields for each point $\mathfrak{p} \in \operatorname{Spec} A$. Let $A_{\mathfrak{p}}$ denote the local ring at $\mathfrak{p}$. For each open set $U \subseteq X = \operatorname{Spec} A$, we define $\mathcal{O}_X(U)$ which we will sometimes write as $\Gamma(U, \mathcal{O}_X)$ to be the set of all functions $s : U \to \coprod_{\mathfrak{p} \in U} A_{\mathfrak{p}}$, with $s(\mathfrak{p}) \in A_{\mathfrak{p}}$ for each $\mathfrak{p} \in \operatorname{Spec} A$, such that s is locally the quotient of elements in A. That is, for each $\mathfrak{p} \in U$ there exists an open set W and elements $r, t \in A$ such that $s = r/t$ for each $q \in W$. Notice this means that $t \notin q$ for each $q \in W$. From the definition it is clear this forms a sheaf on $\operatorname{Spec} A$, with restriction maps $\rho_{U,V} : \mathcal{O}_X(U) \to \mathcal{O}_X(V)$ taking a section $s \in \mathcal{O}_X(U)$ and restricting it to the open set V. The above sheaf $\mathcal{O}_X$ is called the *structure sheaf* of $\operatorname{Spec} A$.

Proposition 3.1.7. *Let A be a ring.*

1. *For any $\mathfrak{p} \in \operatorname{Spec} A$, the stalk $\mathcal{O}_{\operatorname{Spec} A_{\mathfrak{p}}}$ of the sheaf $\mathcal{O}_{\operatorname{Spec} A}$ is isomorphic to the local ring $A_{\mathfrak{p}}$.*

2. *For any element $f \in A$, the ring $\Gamma(D(f), \mathcal{O}_{\operatorname{Spec} A}) \cong A_f$, in particular, $\Gamma(\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A}) \cong A$.*

See §II.2.2 [7] for proof.

Definition 3.1.8. The pair $(\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$ consisting of the spectrum of a ring and it's structure sheaf will be called an *affine scheme.*

Notice the similarities between this definition and that of an affine variety. Instead of a finitely generated nilpotent free k-algebra we replaced it with the structure sheaf $\mathcal{O}_{\operatorname{Spec} A}$ which can be viewed as a $\mathbb{Z}$-algebra over it's global sections.

In the following section we generalize the notion of an affine scheme/affine variety by looking at more general geometric structures glued together by a bunch of affine schemes. This is analogous to the case when we construct manifolds by gluing together open subsets of $\mathbb{R}^n$.

3.2 Schemes

A *scheme* X is a topological space together with a sheaf of rings $\mathcal{O}_X$, that locally looks like an affine scheme. In particular, for each point $x \in X$ there exists an open set U containing x, such that the sheaf restricted to $U \cong \operatorname{Spec} A$ for some commutative ring A. A morphism between two schemes X and Y is a continuous map $f : X \to Y$ and a map of sheaves $f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X$, defined by

$$f^{\#}_U : \mathcal{O}_Y(U) \to f_*\mathcal{O}_X(U) := \mathcal{O}_X(f^{-1}(U)) \quad \text{for each open } U \subseteq Y$$

such that the induced map $f_x^\# : \mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ of stalks is a local homomorphism of local rings for each point $x \in X$. That is, $f_x^\#$ takes the maximal ideal $\mathfrak{m}_x$ in $\mathcal{O}_{X,x}$ to the maximal ideal $\mathfrak{m}_{f(x)}$ in $\mathcal{O}_{Y,f(x)}$. The local criterion ensures that a section s of the structure sheaf $\mathcal{O}_Y$ vanishes at a point $f(\mathfrak{p})$ in the residue field $k(f(\mathfrak{p}))$ if and only if the section $f^\#(s)$ also vanishes at $\mathfrak{p}$.

Example 3.2.1. Consider the affine line $\mathbb{A}_k^1 = \operatorname{Spec} k[t]$ and the parabola $\operatorname{Spec} k[x,y]/(y-x^2)$. We define a morphism $\psi : \operatorname{Spec} k[t] \to \operatorname{Spec} k[x,y]/(y-x^2)$ by the ring homomorphism $\alpha : k[x,y]/(y-x^2) \to k[t]$, taking $x \mapsto t$, $y \mapsto t^2$. The induced map on their topologies is given by $\psi(\mathfrak{p}) := \alpha^{-1}(\mathfrak{p})$. It is not difficult to see that this induces a local homomorphism on each of it's stalks. In fact, any ring homomorphism $\phi : R \to S$ induces a local homomorphism, since the map $\phi_\mathfrak{p} : R_{\phi^{-1}(\mathfrak{p})} \to S_\mathfrak{p}$ of local rings is naturally a local homomorphism. Therefore we have morphisms of schemes. In fact you can check this is actually an isomorphism.

Let U be an open subset of X. Then the sheaf restricted to U is also a scheme on U, since for each point $x \in U$, we can find a distinguished open set $D(f)$ containing x in U with $D(f) \cong \operatorname{Spec} A_f$ for some ring A and $f \in A$.

We would like to have the notion of open and closed subschemes of a scheme. Analogous to the case of manifolds, we have the following definitions.

Definition 3.2.2. An open subset U of X is called an *open subscheme* of X, with the induced structure.

Definition 3.2.3. A *closed immersion* is a morphism $f : Y \to X$ of schemes such that f induces a homeomorphism of Y with some closed subset of X and the induced map of sheaves $f^\# : \mathcal{O}_Y \to f_*\mathcal{O}_X$ is surjective. A *closed subscheme* of a scheme X is then defined as the equivalence class of closed immersions, where $f : Y \to X$ and $g : Y' \to X$ are equivalent provided there is an isomorphism $h : Y \to Y'$ with $f = g \circ h$.

If $X = \operatorname{Spec} A$ is an affine scheme, then each ideal $I \subset A$ represents a closed subscheme of X, since the map $\operatorname{Spec} A/I \hookrightarrow \operatorname{Spec} A$ induced by the ring homomorphism $A \to A/I$ is a surjection on the stalks. Note there may be many closed subschemes assigned to a closed subset in X. For instance $V(I)$ and $V(\sqrt{I})$ are both equivalent as topological spaces but they differ on their structure sheaf whenever $I \neq \sqrt{I}$.

Example 3.2.4. If $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$ are a collection of polynomials then the set $V(f_1, \ldots, f_m)$ is a closed subscheme of the affine n-space $\mathbb{A}_k^n$. The structure sheaf is given by the ring $k[t_1, \ldots, t_n]/(f_1, \cdots, f_m)$.

Definition 3.2.5. For each closed subscheme Y of X, there exists a closed subscheme smaller than any other with the same underlying topological space as Y. We call this closed subscheme $\alpha : Y_{red} \hookrightarrow X$ the *reduced induced* subscheme of Y.

It has the universal property that for any closed subscheme $\beta : Y' \hookrightarrow X$ with the same underlying topological space Y, Y_{red} factors through Y'. That is, there exists a morphism $\pi : Y_{red} \to Y'$ with $\beta \circ \pi = \alpha$.

Example 3.2.6. For affine schemes $\operatorname{Spec} A$ the reduced induced subscheme associated to the closed subscheme $V(I)$, is the closed subscheme induced by the radical ideal $V(\sqrt{I})$.

3.3 Connection Between Affine Schemes and Rings

Eventually, we would like to prove a more general statement of proposition 2.1.8 by replacing affine varieties with affine schemes and finitely generated nilpotent free k-algebras with rings. First we need the following proposition.

Proposition 3.3.1. *For any scheme X and any ring A, the morphisms*

$$\phi : X \to \operatorname{Spec} A$$

is in one to one correspondence with the homomorphism of rings

$$\phi^{\#} : A \to \mathcal{O}_X(X)$$

Proof. It is enough to show that for any two scheme morphisms $\phi, \psi : X \to \operatorname{Spec} A$ that induce the same ring homomorphism of global sections are necessarily equal. Let $x \in X$. Taking the canonical map

$$A \xrightarrow{\phi^{\#}} \mathcal{O}_X(X) \xrightarrow{\pi} \mathcal{O}_{X,x}$$

we define $\psi : X \to \operatorname{Spec} A$, as $\psi(x) := (\pi\phi^{\#})^{-1}(\mathfrak{m}_x)$. The map ψ is continuous, since the inverse image of any distinguished open $D(f)$, with $f \in \Gamma(X, \mathcal{O}_X)$ is equal to

$$\psi^{-1}(D(f)) = D(\phi^{\#}(f))$$

We can define a morphism $\psi^{\#}$ of sheaves over the distinguished open of $\operatorname{Spec} A$ by,

$$\begin{array}{rcl} A_f & \to & (\phi_*\mathcal{O}_X)(D(f)) = \Gamma(D(\phi^{\#}(f)), \mathcal{O}_X) \\ \dfrac{a}{f^k} & \mapsto & \dfrac{\phi^{\#}(a)}{\phi^{\#}(f)^k} \end{array}$$

This is enough to give a unique morphism of sheaves $\mathcal{O}_{\operatorname{Spec} A} \to \phi_*\mathcal{O}_X$. Taking limits, we have the induced map $\psi^{\#}_x : A_{\psi(x)} \to \mathcal{O}_{X,x}$, which is a local morphism, since

$$\psi^{\#\,-1}_x(\mathfrak{m}_x) = (\pi\phi^{\#})^{-1}(\mathfrak{m}_x) \cdot A_{\psi(x)} = \psi(x) \cdot A_{\psi(x)}$$

Hence, the pair $(\psi, \psi^{\#})$ is a morphism of schemes and clearly $\phi = \psi$. □

Corollary 3.3.2. *The category of affine schemes is equivalent to the opposite category of commutative rings with identity, with arrows reversed.*

The above corollary shows that every affine scheme has a dual interpretation as a commutative ring and vice versa. As a result of proposition 3.3.1 the affine scheme $\operatorname{Spec}\mathbb{Z}$ is the terminal object in the category of schemes since every morphism $\psi : X \to \operatorname{Spec}\mathbb{Z}$ is the necessarily unique morphism induced by the ring map $\psi^{\#} : \mathbb{Z} \to \mathcal{O}_X(X)$. Generally, when speaking about the categories of schemes we will usually mean the category of schemes with terminal object $\operatorname{Spec}\mathbb{Z}$. If we replace $\operatorname{Spec}\mathbb{Z}$ with another object S and assign a unique morphism $X \to S$ for each scheme X, then we have what we call S-schemes or schemes over S. In this category, S is the terminal object. We can view a base change as replacing the $\mathbb{Z}$-algebra structure of a structure sheaf to an S-algebra whenever our base S is affine. Restricting ourselves to schemes over a different base is useful since it may introduce a more natural interpretation of the geometry. For instance, if we consider the point "0" corresponding to the maximal ideal (t) on the affine line $\operatorname{Spec}\mathbb{C}[t]$, we would expect that the automorphism group of the point is trivial. In fact this is the case, when we consider it as a scheme over $\operatorname{Spec}\mathbb{C}$. However, the automorphism group of the point over $\operatorname{Spec}\mathbb{Z}$ is the Galois group $\operatorname{Gal}(\mathbb{C}/\mathbb{Q})$, which is very large.

A morphism of two S-schemes X and Y is a morphism $X \to Y$ making the diagram commute,

$$\begin{tikzcd}
X \arrow[rr] \arrow[dr] & & Y \arrow[dl] \\
& \mathrm{S} &
\end{tikzcd}$$

We write the set of morphisms between two S-schemes X and Y as $\operatorname{Mor}_S(X,Y)$.

The fibered product of two S-schemes X and Y is defined as the pullback $X \times_S Y$ of the diagram

$$\begin{tikzcd}
X \times_S Y \arrow[r] \arrow[d] & X \arrow[d] \\
Y \arrow[r] & S
\end{tikzcd}$$

If $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, and $S = \operatorname{Spec} R$ are affine schemes then the fibered product is the scheme $\operatorname{Spec}(A \otimes_R B)$. This follows since the functor $F : \textbf{R-Alg} \to \textbf{R-Sch}^{\circ}$ given by,

$$A \mapsto (\operatorname{Spec} A, \mathcal{O}_{\operatorname{Spec} A})$$

induces an equivalence of categories with the functor taking global sections. By proposition A.3.2, F must preserve colimits, and hence

$$\operatorname{Spec} A \times_{\operatorname{Spec} R} \operatorname{Spec} B = \operatorname{Spec}(A \otimes_R B)$$

More generally, the fibered product of arbitrary schemes exists and requires the gluing of affine schemes over suitable open sets. For a more detailed account we refer the reader to §II.3 [7].

Example 3.3.3. The fibered product of two schemes does not necessarily preserve the fibered product of it's underlying set of points. The points in $\operatorname{Spec} \mathbb{C}[x]$ correspond to the maximal ideals $\{(x-a)\}_{a \in \mathbb{C}}$ and the zero ideal (0). However, $\operatorname{Spec} \mathbb{C}[x] \times_{\mathbb{C}} \operatorname{Spec} \mathbb{C}[y] = \operatorname{Spec} \mathbb{C}[x, y]$ contains irreducible polynomials that are not in the fibered product of it's underlying sets.

An important application of fibered products is base extensions of schemes. Given a morphism $S' \to S$ we can take the fibered product of an S-scheme $X \to S$ to get an S'-scheme. Taking base changes is functorial since any S-morphism $f : X \to Y$ induces a unique morphism $f' : X \times_S S' \to Y \times_S S'$. This is useful for studying schemes over different field extensions. Another important use is in studying morphisms under base extensions.

Proposition 3.3.4. *Open and closed immersions are stable under base extensions.*

Therefore every open and closed subscheme, stays open and closed under base change.

3.4 Sheaves of Modules

Up until now we have only considered the structure sheaf associated to a scheme. More generally, we are interested in constructing sheaves of modules over a given scheme. Let $(X, \mathcal{O}_X)$ be an affine scheme. A *sheaf of $\mathcal{O}_X$-modules* is a sheaf $\mathcal{F}$ on X, such for each open set $U \subseteq X$, $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module, and for each inclusion of open sets $V \subseteq U$, the restriction homomorphism $\mathcal{F}(U) \to \mathcal{F}(V)$ is compatible with the module structure. A morphism $\mathcal{F} \to \mathcal{G}$ of sheaves of $\mathcal{O}_X$-modules is a morphism of sheaves, such that for each open set $U \subseteq X$, the map $\mathcal{F}(U) \to \mathcal{G}(U)$ is a homomorphism of $\mathcal{O}_X(U)$-modules.

Definition 3.4.1. An $\mathcal{O}_X$-module M is said to be *quasi-coherent* if it is locally presented. In other words there exists an open cover $\{U_\alpha\}$ such that for every α, $M|_{U_\alpha}$ is presented

$$\bigoplus_{i \in I_1} \mathcal{O}_X|_{U_\alpha} \to \bigoplus_{i \in I_0} \mathcal{O}_X|_{U_\alpha} \to M|_{U_\alpha} \to 0$$

If we can choose I_0, I_1 finite, then M is called *coherent.*

Given an affine scheme $(X, \mathcal{O}_X) = (\operatorname{Spec} R, \mathcal{O}_{\operatorname{Spec} R})$ and an R-module M, we define the sheaf $\widetilde{M}$ associated to M to be the sheaf, such that $\widetilde{M}(D(f)) = M_f$ over every distinguished open set $D(f)$.

Proposition 3.4.2. *Let R be a ring, and M an R-module, with associated structure sheaf $\widetilde{M}$ on* $\operatorname{Spec} R$*. Then,*

1. *$\widetilde{M}$ is an $\mathcal{O}_X$-module*
2. *for each $\mathfrak{p} \in \operatorname{Spec} R$, the stalk $(\widetilde{M})_\mathfrak{p}$ is isomorphic to the localized module $M_\mathfrak{p}$.*
3. *for any $f \in R$, the A_f-module $\widetilde{M}(D(f))$ is isomorphic to the localized module M_f*

4. $\Gamma(\operatorname{Spec} R, \widetilde{M}) = M$

See §II.5.1 [7] for proof.

Proposition 3.4.3. *If N is a sheaf of $\mathcal{O}_X$-modules on $X = \operatorname{Spec} R$, and M is any R-module, then the functor $\widetilde{(-)}$ taking M to it's associated sheaf of modules is adjoint to the functor $\Gamma(X, -)$ taking global sections. ie*

$$\operatorname{Hom}_{\mathcal{O}_X}(\widetilde{M}, N) \cong \operatorname{Hom}_R(M, \Gamma(X, N))$$

Proof. It is clear that the above is a natural transformation. The only non-trivial part is showing that every homomorphism $M \to \Gamma(X, N)$ of R-modules induces a morphism of $\mathcal{O}_X$-modules. Let $\phi : M \to \Gamma(X, N)$ be a map of R-modules and $D(f) \subseteq \operatorname{Spec} R$, $f \in R$ a distinguished open set. Then there exists a unique map,

$$\begin{tikzcd}
M \arrow[r, "\phi"] \arrow[d] & \Gamma(X, N) \arrow[d] \\
M_f \arrow[r, dashed, "\exists!"] & \Gamma(D(f), N)
\end{tikzcd}$$

extending ϕ. This is enough to induce a unique morphism of $\mathcal{O}_X$-modules and hence the desired result follows. □

In particular we can say that the functor $\widetilde{(-)}$ gives an equivalence between the category of R-modules and the category of quasi-coherent $\mathcal{O}_X$-modules.

In the next section we introduce the functor of points of a scheme. The functor of points will play an important role in laying a foundation for applying algebraic geometry to coding.

3.5 The Functor of Points

For clarity, we introduce the functor of points in a more general categorical setting. In many categories, objects can usually be viewed as sets with some additional structure.

The underlying set of an object $|X|$ may be described as the set of morphisms from a universal object to X. For instance,

- In the category of differentiable manifolds, the underlying set of any manifold X may be described as the set of morphisms $\mathrm{Mor}(Z, X)$, where Z is the trivial manifold consisting of one point.
- In the category of groups, a group G underlying set may be described as $\mathrm{Mor}(\mathbb{Z}, G)$.
- In the category of rings with unit, a ring R underlying set $|R| = \mathrm{Mor}(\mathbb{Z}[t], R)$.

The above suggests, it may be possible to conceive an objects underlying set as the functor $X \mapsto \mathrm{Mor}(Z, X)$ for some object Z. We remark though, that this makes sense only if the functor is faithful. In other words, if two morphisms $f, g : X \to Y$ produces the same map $f', g' : \mathrm{Mor}(Z, X) \to \mathrm{Mor}(Z, Y)$, then $f = g$.

Example 3.5.1. In the category of schemes, the most intuitive object to choose would be the terminal object $\operatorname{Spec}\mathbb{Z}$. However, $\mathrm{Mor}(\operatorname{Spec}\mathbb{Z}, X)$ turns out to be very small, and is not a faithful functor. Indeed no scheme is sufficient to give a complete description

The above suggests, there might be no hope in finding a remedy to this situation. Grothendieck, suggested instead of looking at individual sets $\mathrm{Mor}(Z, X)$, why don't we consider all the sets $\cup_{Z \in \mathbf{Sch}} \mathrm{Mor}(Z, X)$? In this way, we naturally obtain a faithful functor from any category $\mathcal{C}$ to **Sets**, by associating an object X to the sets of the form $\mathrm{Mor}(Z, X)$ together with, for each morphism $f : Z \to Z'$, the mapping from $\mathrm{Mor}(Z', X)$ obtained by composing with f.

Definition 3.5.2. The *functor of points* of a scheme X is defined as the representable functor

$$\begin{aligned} h : \mathbf{Sch} &\to \mathrm{Fun}(\mathbf{Sch}^{\circ}, \mathbf{Sets}) \\ X &\mapsto h_X \end{aligned}$$

More generally, we will consider the case when we have an arbitrary base S and representable functor $h' : \textbf{S-Sch} \to \mathrm{Fun}(\textbf{S-Sch}^{\circ}, \textbf{Sets})$. The set $h_{X/S}(Y) = \mathrm{Mor}_S(Y, X)$ is called the set of Y-valued points. We will usually denote this as $X_S(Y)$. The above idea is motivated by the k-rational points of a scheme X over a field k. The k-rational points of a scheme X are defined as the points $\mathfrak{p}$ whose residue field $k(\mathfrak{p})$ is k. In this case, the k-rational points are in one-to-one correspondence with k-valued points. Indeed, any map $\mathrm{Spec}\, k$ to X is a map $\mathrm{Spec}\, k$ into some affine open subscheme $\mathrm{Spec}\, A$ of X, which is in turn determined by a k-algebra map $A \to k$. This results in a maximal ideal in A whose residue field is k and hence a rational point. Similarly, it is easy to see any k-rational point gives rise to a morphism $\mathrm{Spec}\, k \to X$ of k-schemes.

The concept of an R-valued point generalizes the notion of a set of Diophantine equations in a ring S. If we let $S := \mathbb{Z}[t_1, \dots, t_n]/(f_1, \dots, f_m)$ and $X = \mathrm{Spec}\, S$, then a morphism $\mathrm{Spec}\, R \to \mathrm{Spec}\, S$, is the same as a ring homomorphism $S \to R$. This morphism is determined by the images of t_i in R. Therefore, this results in a morphism if and only if the images a_i of t_i form a solution to the equations

$$f_1(a_1, \dots, a_n) = \cdots = f_m(a_1, \dots, a_n) = 0$$

It is important to draw a distinction between the dual use of the word "points". In a arbitrary affine scheme $X = \mathrm{Spec}\, A$, the points correspond to prime ideals in A, which are not the same as the set of R-valued points, associated to X. Also, while the set of points of $|X|$ are absolute, the set of R-valued points are relative to the base scheme we are working over. The following proposition shows, that it is enough to look at the functor of points of affine schemes whenever the base scheme is affine.

Proposition 3.5.3. *If R is a commutative ring, a scheme over R is determined by the restriction of it's functor of points to affine schemes; in fact*

$$h : \textbf{R-Sch} \to \mathrm{Fun}(\textbf{R-Alg}, \textbf{Sets})$$

is an equivalence of the category of R-schemes with a full subcategory of the category of functors.

Proof. It is enough to show every natural transformation $h_X \to h'_X$ comes from a unique morphism $f : X \to X'$. Let $\{U_i\}$ be an open cover of X. Then each inclusion $U_i \hookrightarrow X$ corresponds to a morphism $f_i : U_i \to X'$. Checking compatibility over the intersections $U_i \cap U_j$, we see that the f_i glue together to form a morphism $f : X \to X'$. Now we want to show for any affine R-scheme T, and morphism $g : T \to X$ the natural transformation takes g to $f \circ g$. Indeed, choose any affine open cover $\{V_{i,j}\}$ with $V_{i,j} \subseteq f^{-1}(U_i)$. Then the induced map $g|_{V_{i,j}} : V_{i,j} \to X$, corresponds to a morphism $g'|_{V_{i,j}} : V_{i,j} \to X'$. Checking $g'|_{V_{i,j}} = (fg)|_{V_{i,j}}$, we have the desired result. □

3.6 Characterization of Schemes among Functors

In this section we want to consider the question of when a functor F : **Rngs** $\to$ **Sets** is necessarily representable by a scheme. Since schemes are made up of open affine subschemes it seems logical that a functor should be glued together by smaller representable functors corresponding to an open affine cover. We will show under certain circumstances they are. First we define the fibered product of functors.

Definition 3.6.1. If $\mathcal{F}$, $\mathcal{G}$, and $\mathcal{H}$ are functors from a category $\mathcal{C} \to$ **Sets** and if $a : \mathcal{F} \to \mathcal{H}$ and $b : \mathcal{G} \to \mathcal{H}$ are natural transformations, the *fibered product* $\mathcal{F} \times_{\mathcal{H}} \mathcal{G}$ is the functor from $\mathcal{C} \to$ **Sets** defined by setting for each object X of $\mathcal{C}$, the set

$$(\mathcal{F} \times_{\mathcal{H}} \mathcal{G})(X) = \{\, (x, y) \in \mathcal{F}(X) \times \mathcal{G}(X) \mid a(x) = b(y) \text{ in } \mathcal{H}(X) \,\}$$

We say a functor $\mathcal{G}$ is a *subfunctor* of $\mathcal{F}$ provided there is a natural transformation $\alpha : \mathcal{G} \to \mathcal{F}$ such that for every object X the induced map of sets $\mathcal{G}(X) \to \mathcal{F}(X)$ is injective. A subfunctor $\mathcal{G}$: **Rngs** $\to$ **Sets** of a functor $\mathcal{F}$ is said to be an *open* *subfunctor* provided for each map $\psi : h_{\text{Spec}\, R} \to \mathcal{F}$ from the representable functor $h_{\text{Spec}\, R}$, the fibred product

$$\begin{tikzcd}
\mathcal{G}_\psi \arrow[r] \arrow[d] & h_{\text{Spec}\, R} \arrow[d] \\
\mathcal{G} \arrow[r] & \mathcal{F}
\end{tikzcd}$$

of functors yields a functor $\mathcal{G}_\psi \to h_{\text{Spec}\, R}$, that is naturally isomorphic to a representable functor h_U for some open $U \subseteq \text{Spec}\, R$. If X is a scheme then the open subfunctors of h_X are precisely those given by open subschemes of X.

Definition 3.6.2. An *open covering* of a functor is a collection of open subfunctors $\{G_i \to F\}$, such that for each scheme X the open subsets representing the pullback h_{U_i}, of h_X is an open cover of X.

For instance, if X is a scheme and $\{U_i\}$ an open cover of X, then the collection of open subfunctors $\{h_{U_i} \to h_X\}$ is an open covering, since the fibered product of functors $h_{U_i} \times_{h_X} h_{\text{Spec}\, R}$ for any affine scheme Spec R is necessarily the representable functor $h_{U_i \times_X \text{Spec}\, R}$ given by the fibered product of the morphism in $h_X(\text{Spec}\, R)$ and $h_X(U_i)$ corresponding to the natural transformations in proposition A.0.11.

Lemma 3.6.3. *Let $\{G_i \to F\}$ be a collection of open subfunctors of a functor F :* **Sch** $\to$ **Sets***. Then $\{G_i \to F\}$ is an open covering if and only if $F(\text{Spec}\, k) = \cup G_i(\text{Spec}\, k)$ for every field k.*

Proposition 3.6.4. *A functor F :* **Rngs** $\to$ **Sets** *is of the form h_X for some scheme X if and only if*

1. *F is a sheaf in the Zariski topology, and*
2. *there exists rings R_i corresponding to open subfunctors $h_{R_i} \to F$ such that, for any fields k, $F(\text{Spec}\, k) = \cup h_{R_i}(\text{Spec}\, k)$.*

3.7 Group Schemes

We have already seen that the product of two schemes does not necessarily preserve the product of it's underlying set of points. This prevents us from making the points of an arbitrary scheme into an abstract group. However, since the R-valued points of a product of schemes, is the set product of it's R-valued points, it makes sense to define a group structure here.

Definition 3.7.1. Let G be a scheme over a base S. G is said to be a group scheme provided there exists a morphism $\mu : G \times_S G \to G$ (group operation), $\tau : G \to G$ (inversion), and $\varepsilon : S \to G$ (identity) making the following diagrams commute,

$$\begin{tikzcd}
G \times_S G \times_S G \arrow[r, "\mathrm{id}_G \times \mu"] \arrow[d, "\mu \times \mathrm{id}_G"'] & G \times_S G \arrow[d, "\mu"] \\
G \times_S G \arrow[r, "\mu"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "\mathrm{id}_G \times \varepsilon"] \arrow[d, "\varepsilon \times \mathrm{id}_G"'] \arrow[dr, "\mathrm{id}_G"] & G \times_S G \arrow[d, "\mu"] \\
G \times_S G \arrow[r, "\mu"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
& G \times_S G \arrow[r, "\mathrm{id}_G \times \tau"] & G \times_S G \arrow[dr, "\mu"] & \\
G \arrow[ur, "\Delta_G"] \arrow[rrr, "\varepsilon\pi_G"] \arrow[dr, "\Delta_G"'] & & & G \\
& G \times_S G \arrow[r, "\tau \times \mathrm{id}_G"] & G \times_S G \arrow[ur, "\mu"'] &
\end{tikzcd}$$

In particular, if our schemes are affine, then the dual of the diagrams defines a (commutative) Hopf-Algebra, see [1].

Example 3.7.2. The polynomial ring $k[t]$ can be given the structure of a group as a k-scheme, by defining the group operation $\mu : k[t] \to k[t] \otimes_k k[t]$ as $t \mapsto t \otimes 1 + 1 \otimes t$, $\tau : t \mapsto -t$, and $\varepsilon : k[t] \to k$ as $t \mapsto 0$. The corresponding group is denoted $\mathbf{G}_a$ with k-valued points isomorphic to the underlying additive group k. Similarly, $k[t, t^{-1}]$ is a group scheme over k by taking $\mu : t \mapsto t \otimes t$, $\tau : t \mapsto t^{-1}$, and $\varepsilon : t \mapsto 1$. In this case, the affine algebraic group is denoted $\mathbf{G}_m$ and corresponds to the multiplicative group $k^{\times}$.

Proposition 3.7.3. *Let G be a scheme over S. Then G is a group scheme if and only if for every S-scheme X, $Mor_S(X, G)$ is a group under the operation $f \cdot g = \mu(f \times g)\Delta_X$, satisfying the condition; if Y is an S-scheme and $\lambda \in Mor_S(Y, X)$, then the mapping $\lambda^* : G_S(X) \to G_S(Y)$ given by $f \mapsto f\lambda$ is a group homomorphism.*

Example 3.7.4. We can define GL_n as the integral group scheme of $n \times n$ matrices,

$$\operatorname{Spec} \mathbb{Z}[x_{i,j}][\det(x_{i,j})^{-1}]$$

by associating to every ring T the group $GL_n(T)$.

Definition 3.7.5. A closed subscheme H of a group scheme G, will said to be a *group subscheme* of G provided for each scheme Y, $h_H(Y)$ is a subgroup of $h_G(Y)$.

Example 3.7.6. Suppose G is a group scheme over some affine base $\operatorname{Spec} R$. Then $\operatorname{Spec} R$ inherits a natural group subscheme structure of G by associating the trivial group to $\operatorname{Spec} R$ and identifying it with the identity element of G.

3.8 Groups Acting on Schemes

An important concept, which we will later use to construct geometric error spaces, is that of a group scheme acting on a scheme X.

Definition 3.8.1. A *G-space* is a scheme X equipped with a left G-action that is also a morphism $\alpha : G \times_S X \to X$, satisfying,

1. $\alpha(\mu \times 1_G) = \alpha(1_G \times \alpha) : G \times_S G \times_S G \times_S X \to X$.

2. $\alpha(\varepsilon \times 1_X) = p : S \times_S X \to X$, where p is the projection map.

Example 3.8.2. Let $\mathbf{G}_a = \operatorname{Spec} k[t]$ be the affine line with additive group structure. Define the morphism $\alpha : \mathbf{G}_a \times_k \mathbf{G}_a \to \mathbf{G}_a$ by the ring homomorphism $k[t] \to k[x] \otimes_k k[y]$ taking $t \mapsto x \otimes 1 + 1 \otimes y$. It is easy to check $\mathbf{G}_a$ defines a group action on itself. Indeed, on the k-rational level it is the action $(k, k') \mapsto k + k'$.

For more information on G-spaces and group varieties in general, see [15].

Chapter 4

Codes

Thus far, we have reviewed the fundamentals of modern algebraic geometry. In this section, we develop a general theoretical framework for geometric systems having error structures.

We proceed first, by defining a diagram of groups schemes over a directed graph. This will provide the necessary structure in which we can integrate errors into our geometries. Throughout this section, we will assume all of our schemes are over an arbitrary base S. When a distinction is relevant we will note otherwise.

4.1 Diagram of Group Schemes

Definition 4.1.1. Let I be a directed graph. A *diagram of group schemes* Σ_G over I is a family of group schemes $\{G_i\}_{i \in I}$,that assigns each arrow $i \to j$ a corresponding group scheme morphism $g_{i,j} \in \mathrm{Mor}(G_i, G_j)$.

A morphism between two diagram of group schemes Σ_G and Σ_H, is a morphism of the underlying graphs $\alpha : I_G \to I_H$,

1. taking each $G_i \in \Sigma_G$ to a group scheme $H_{\alpha(i)} \in \Sigma_H$, by way of a group scheme morphism $\lambda_i : G_i \to H_{\alpha(i)}$

2. and for each arrow $g_{i,j} : G_i \to G_j$ an associated arrow $h_{\alpha(i),\alpha(j)} : H_{\alpha(i)} \to H_{\alpha(j)}$, satisfying $\lambda_j \circ g_{i,j} = h_{\alpha(i),\alpha(j)} \circ \lambda_i$ for every $G_i, G_j \in \Sigma_G$.

Definition 4.1.2. A Σ_G*-space* over a diagram of group schemes Σ_G is defined as a pair (X, Σ_G) consisting of the following data:

1. for every $G_i \in \Sigma_G$, there is a G-space action $\sigma_i : G_i \times_S X \to X$,
2. for every arrow of group scheme morphisms $g_{i,j} : G_i \to G_j$, $\sigma_j \circ (g_{i,j} \times \mathrm{id}_X) = \sigma_i$.

Example 4.1.3. Consider the diagram of group k-schemes,

$$\operatorname{Spec} k \xrightarrow{g} \operatorname{Spec} k[x_{11}, x_{12}, x_{21}, x_{22}][\det(x_{ij})^{-1}]$$

with arrow map $g^{\#}$ taking $x_{11} \mapsto 1$, $x_{12} \mapsto 0$, $x_{21} \mapsto 0$, $x_{22} \mapsto 1$. The object $\operatorname{Spec} k[x_{11}, x_{12}, x_{21}, x_{22}][\det(x_{ij})^{-1}]$ is the group scheme of invertible 2×2 matrices GL_2 and $\operatorname{Spec} k$ the trivial group mapping to the identity matrix in GL_2. We view $\operatorname{Spec} k$ as having a null-error structure and GL_2 as a single error structure. The direction of the arrow map determines this. Taking the affine plane $\mathbb{A}^2_k = \operatorname{Spec} k[x, y]$, we can construct the Σ_G-space $(\mathbb{A}^2_k, \Sigma_{\mathrm{GL}_2})$ by the k-valued action

$$(k, k') \mapsto (k, k') \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad ad - bc \neq 0$$

At the k-valued level we have the two-dimensional vector space k^2 with single error actions determined by invertible transformations and null-error action given by the identity.

Example 4.1.4. Consider the additive group scheme $\mathbf{G}^n_a$ corresponding to the polynomial ring $k[x_1, \ldots, x_n]$ over a field k. Let

$$G_i := \operatorname{Spec} k[x_1, \ldots, x_n]/\Sigma_{j \neq i}(x_j)$$

be the induced additive group subscheme of $\mathbf{G}_a^n$. The k-rational points of G_i have the form $\{\,(a_1,\ldots,a_n) \in k^n \mid a_j = 0 \text{ for } j \neq i\}$. Consider the diagram scheme,

$$\begin{tikzcd}
G_1 & \cdots & G_i & \cdots & G_n \\
 & & \operatorname{Spec} k \arrow[ull] \arrow[u] \arrow[urr] & &
\end{tikzcd}$$

Taking the affine scheme $\mathbb{A}_k^n$ we define the Σ_G-space as the pair $(\mathbb{A}_k^n, \Sigma_G)$ with G_i acting on $\mathbb{A}_k^n$ by addition. For each i, the map $G_i \times_k \mathbb{A}_k^n \to \mathbb{A}_k^n$ is determined by the ring homomorphism

$$\begin{array}{rcl}
k[x_1,\ldots,x_n] & \to & k[x_1,\ldots,x_n]/\Sigma_{j\neq i}(x_j) \otimes_k k[x_1,\ldots,x_n] \\
x_l & \mapsto & x_l \otimes 1 + 1 \otimes x_l
\end{array}$$

We can view this on the k-rational level as the system of errors on k^n taking an element

$$(a_1,\ldots,a_n) \mapsto (a_1,\ldots,a_n) + (0,\ldots,k_i,\ldots,0)$$

with the restriction that errors cannot occur at more than one position.

Definition 4.1.5. A morphism of Σ_G-spaces (X, Σ_G) and (Y, Σ_H) is a pair of morphisms (f, α), $f : X \to Y$ and $\alpha : \Sigma_G \to \Sigma_H$ such that for every map $\lambda_i : G_i \to H_{\alpha(i)}$ the following diagram commutes

$$\begin{tikzcd}
G_i \times_S X \arrow[r, "\sigma_i"] \arrow[d, "\lambda_i \times f"'] & X \arrow[d, "f"] \\
H_{\alpha(i)} \times_S Y \arrow[r, "\sigma'_{\alpha(i)}"'] & Y
\end{tikzcd}$$

We will refer to the class of objects consisting of Σ_G-spaces and morphisms, as the category of Σ_G-spaces.

If we are working over a base scheme S, the sets of the form $\mathrm{Mor}_S(X, S)$ contain only one point. From this observation, it is clear the pair of objects (S, S) forms a canonical Σ_G-space. In fact, every Σ_G-space (X, Σ_G) has a unique morphism to (S, S). Therefore (S, S) is the terminal object in the category of Σ_G-spaces over S.

Proposition 4.1.6. *Let (X, Σ_G) and (Y, Σ_H) be Σ_G-spaces over a base scheme S, then the fibered product over the terminal object (S, S) exists and has the form $(X \times_S Y, \Sigma_{G\times H})$, where $\Sigma_{G\times H}$ is the product of the diagram schemes Σ_G and Σ_H.*

Note, the fibered product in general does not exist if we replace the object (S, S) by another Σ_G-space.

Example 4.1.7. Let $G \neq H$ and (X, G), (X, H) two distinct Σ_G-spaces over the trivial graph containing one point. Take the object $(X, \{G, H\})$ where G and H lie over the discrete graph consisting of only two points. Then we have canonical maps from (X, G) and (X, H) to $(X, \{G, H\})$. However, a pullback does not exist.

Example 4.1.8. Consider the Σ_G-space $(\mathbb{A}^1_k, \Sigma_k)$, where Σ_k is defined as the diagram of group schemes $g : \mathrm{Spec}\, k \to \mathbf{G}_a$ with $g^\# : k[t] \to k$, taking $t \mapsto 0$. The group scheme $\mathbf{G}_a$ acts on $\mathbb{A}^1_k$ by addition. The product of $(\mathbb{A}^1_k, \Sigma_k)$ with itself over $(\mathrm{Spec}\, k, \mathrm{Spec}\, k)$ is the Σ_G-space corresponding to the diagram of group schemes,

$$\begin{tikzcd}
\mathbf{G}_a \arrow[r, "g \times \varepsilon"] & \mathbf{G}_a \times_k \mathbf{G}_a \\
\mathrm{Spec}\, k \arrow[u, "g"] \arrow[r, "g"'] & \mathbf{G}_a \arrow[u, "\varepsilon \times g"']
\end{tikzcd}$$

acting on $\mathbb{A}^2_k$. The above can be viewed as the product of two classical single error coding spaces.

4.2 Geometric Codes

Definition 4.2.1. Let (X, Σ_G) be an Σ_G-space, and C a subscheme of X. A *code* C over the Σ_G-space (X, Σ_G) is defined as the triple (C, X, Σ_G).

In a similar way to the definition of an open and closed subscheme, we define a code to be open or closed, provided it is an open or closed subscheme of X. By Yoneda's Lemma A.0.11, each code has a dual interpretation as a representable functor over it's Y-valued points. For application purposes we will restrict ourselves to a particular layer of Y-valued points. Namely, given our base scheme is S, we will only consider the S-valued points. Recall the S-valued points are the morphisms $\rho : S \to C$, satisfying $\pi_C \circ \rho = \mathrm{id}_S$.

The definition of a code is motivated by the fact that every non-singular algebraic variety X over the complex numbers $\mathbb{C}$ has a natural structure as a complex manifold over it's $\mathbb{C}$-rational points $X(\mathbb{C})$. Therefore every non-singular code $X \subseteq \mathbb{A}^n_{\mathbb{C}}$ can be viewed as a submanifold $X(\mathbb{C}) \hookrightarrow \mathbb{C}^n$. The S-valued points is a generalization of this idea.

Definition 4.2.2. A morphism between two codes (C, X, Σ_G) and (D, Y, Σ_H) is a triple (g, f, α), with $g : C \to D$, $f : X \to Y$, and $\alpha : \Sigma_G \to \Sigma_H$ satisfying the condition that the pair (f, α) is a morphism of Σ_G-spaces, and such that $f \circ \mathrm{i}_C = \mathrm{i}_D \circ g$.

If we take both Σ_G and Σ_H to have the null error diagram consisting of only the trivial group scheme $\operatorname{Spec} R$, then the above definition is based on the category of pairs of topological spaces $\mathbf{Top}^2$. Here the objects are all ordered pairs (C, X), with X a topological space and C a subspace of X. A morphism $f : (C, X) \to (D, Y)$ is an ordered pair (f, g), whenever $f : X \to Y$ is continuous and $f \circ \mathrm{i}_C = \mathrm{i}_D \circ g$.

Observe, following the same reason the pair (S, S) was a terminal object in the category of Σ_G-spaces, the triple (S, S, S) is a terminal object for every geometric code.

Proposition 4.2.3. *Let (C, X, Σ_G) and (D, Y, Σ_H) be two geometric codes, then the fibered product over the terminal object exists and has the form $(C \times_S D, X \times_S Y, \Sigma_{G\times H})$.*

At the end of section 3.2, we discussed base extensions of schemes. Using the same reasoning, we would also like to apply this same idea to codes by replacing the terminal object (S, S, S) by the object (S', S', S'), such that S' also has a trivial group structure. Given a morphism $S' \to S$, we define

$$(C \times_S S', X \times_S S', \Sigma_{G\times_S S'})$$

to be the code obtained by taking the fibered product of C, X, and Σ_G. The new object is again a geometric code since the schemes $G_\alpha \times_S S'$, $G_\alpha \in \Sigma_G$ have a natural group scheme structure over S' and the maps $G_\alpha \times_S S' \to G_\beta \times_S S'$ are again groups scheme morphisms. Therefore $\Sigma_{G\times_S S'}$ is a diagram of group schemes. Similarly, since taking base changes over schemes is functorial, it follows that taking base changes with respect to codes is also a functor, since code morphisms are a family of scheme morphisms. In fact, any closed or open code stays closed or open, by proposition 3.3.4.

Example 4.2.4. Following Example 4.1.8, let $k = \mathbb{R}$ be the field of real numbers. The Σ_G-space $(\mathbb{A}^2_{\mathbb{R}}, \Sigma_{\mathbb{R}})$ defines a classical error space structure over the two-dimensional vector space $\mathbb{R}^2$. Let

$$C = \operatorname{Spec} \mathbb{R}[x, y]/(x^2 + y^2)$$

then the triple $(C, A_{\mathbb{R}^2}, \Sigma_{\mathbb{R}})$ is a geometric code. The $\mathbb{R}$-rational points of the code is the single point $(0, 0) \in \mathbb{R}^2$. Let $\mathbb{C}$ be the complex numbers and $\mathbb{R} \hookrightarrow \mathbb{C}$ the natural embedding. Taking the base change $\operatorname{Spec} \mathbb{C} \to \operatorname{Spec} \mathbb{R}$ we have the new code

$$\big(C \times_{\mathbb{R}} \operatorname{Spec} \mathbb{C}, \mathbb{A}^2_{\mathbb{R}} \times \operatorname{Spec} \mathbb{C}, \Sigma_{\mathbb{R}} \times \operatorname{Spec} \mathbb{C}\big)$$

Since C is an affine scheme

$$\begin{aligned} C \times_{\mathbb{R}} \operatorname{Spec} \mathbb{C} &= \operatorname{Spec}(\mathbb{R}[x,y]/(x^2+y^2) \otimes_{\mathbb{R}} \mathbb{C}) \\ &= \operatorname{Spec}\big(\mathbb{C}[x,y]/(x^2+y^2)\big) \end{aligned}$$

Similarly we have $\mathbb{A}^2_{\mathbb{R}} \times \operatorname{Spec} \mathbb{C} = \mathbb{A}^2_{\mathbb{C}}$ and $\Sigma_{\mathbb{R}} \times \operatorname{Spec} \mathbb{C} = \Sigma_{\mathbb{C}}$. The new code $(C \times_{\mathbb{R}} \operatorname{Spec} \mathbb{C}, \mathbb{A}^2_{\mathbb{C}}, \Sigma_{\mathbb{C}})$ has classical error structure over the two-dimensional vector space $\mathbb{C}^2$ and rational points $\{\, (a, ai), (a, -ai) \mid a \in \mathbb{C} \,\}$.

4.3 Classical Algebraic Coding

Our approach up until now has been deliberately general for the following reasons:

- The ability to model other geometric error structures.
- Scheme theoretic approach has made the definitions and arguments much more refined.
- Has allowed for a convenient way to study the geometry of codes over commutative rings and fields.
- The powerful tools of algebraic geometry and number theory can easily be used within this framework.

In this section we begin first by defining the error diagram of classical codes. This will allow us to precisely define what we mean by single, double, and n-errors. The diagram structure will also play an important role in determining the distance between code words.

Consider the additive group scheme $\mathbf{G}_a^n$ corresponding to the polynomial ring $R[x_1, \dots, x_n]$ over some commutative ring R. Define

$$G_{(i_1,\dots,i_k)} := \operatorname{Spec} R[x_1, \dots, x_n]/\Sigma_{j \neq i_1,\dots,i_k}(x_j)$$

as the induced additive group subscheme of $\mathbf{G}_a^n$ over all tuples $(i_1, \dots, i_k)$. In this way, we obtain a natural diagram structure, consisting of vertices $G_{(i_1,\dots,i_k)}$ and arrow maps $G_{(i_1,\dots,i_l)} \to G_{(i_1,\dots,i_k)}$, whenever $\{i_1, \dots, i_l\} \subseteq \{i_1, \dots, i_k\}$. If $n = 3$, the above suggests that we have a commutative diagram of the form

$$\begin{tikzcd}
& G_{(1,2,3)} & \\
G_{(1,2)} \arrow[ur] & G_{(1,3)} \arrow[u] & G_{(2,3)} \arrow[ul] \\
G_{(1)} \arrow[u] \arrow[ur] & G_{(2)} \arrow[ul] \arrow[ur] & G_{(3)} \arrow[u] \arrow[ul] \\
& \mathrm{Spec} R \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

The above diagram structure of group schemes can be viewed as a generalization of the G-space $\mathbf{G}_a^3$ acting on itself by addition. The added structure allows one to define single, double, and triple errors. At the R-valued level the above diagram translates to,

$$\begin{tikzcd}
& R \times R \times R & \\
R \times R \times 0 \arrow[ur] & R \times 0 \times R \arrow[u] & 0 \times R \times R \arrow[ul] \\
R \times 0 \times 0 \arrow[u] \arrow[ur] & 0 \times R \times 0 \arrow[ul] \arrow[ur] & 0 \times 0 \times R \arrow[u] \arrow[ul] \\
& 0 \times 0 \times 0 \arrow[ul] \arrow[u] \arrow[ur] &
\end{tikzcd}$$

We will denote the above diagram scheme as Σ_R^n. The pair $(\mathbb{A}_R^n, \Sigma_R^n)$, then becomes an Σ_G-space with group schemes $G_{(i_1,\ldots,i_k)}$ acting on $\mathbb{A}_R^n$ by addition. A code in $(\mathbb{A}_R^n, \Sigma_R^n)$ is by definition a subscheme of $\mathbb{A}_R^n$. If C is a closed code, then $C = \operatorname{Spec}(R[x_1, \ldots, x_n]/I)$ for some ideal $I \subseteq R[x_1, \ldots, x_n]$. The R-valued points of $\mathbb{A}_R^n$ correspond to ring homomorphisms $R[x_1, \ldots, x_n] \to R$. Since each ring homomorphism is uniquely determined by the values $x_i \mapsto r_i$, there is a one-to-one correspondence between the R-valued points of $\mathbb{A}_R^n$ and points in R^n. In a similar way, the R-valued points of a code, can be viewed as the set of points $(a_1, \ldots, a_n) \in R^n$ such that $f(a_1, \ldots, a_n) = 0$, for every $f \in I$.

Definition 4.3.1. A *linear geometric code* is a closed subscheme corresponding to an ideal generated by degree one linear forms.

Example 4.3.2. Let $I = (x_1 + x_2 + x_6 + x_7, x_1 + x_2 + x_3 + x_5, x_1 + x_3 + x_4 + x_7) \subseteq \mathbb{F}_2[x_1, \ldots, x_7]$. Then the $\mathbb{F}_2$-rational points of the scheme $C = \operatorname{Spec}(\mathbb{F}_2[x_1, \ldots, x_7]/I)$ corresponds to the $[7, 4]$ binary Hamming code.

A special property that all linear codes share, is stated in the following proposition.

Proposition 4.3.3. *Suppose R is a Noetherian ring and C a closed subscheme of $\mathbb{A}_R^n$ given by an ideal generated by degree one linear forms. Then for every R-scheme X, the representable functor $C_R(-)$ is a sheaf of $\mathcal{O}_X$-modules. In the special case that $X = \operatorname{Spec} S$ is an affine scheme, $C_R(-)$ is the associated sheaf $\widetilde{C_R(-)}$ induced as an S-module.*

Proof. Let X be a scheme and $C = \operatorname{Spec}(R[x_1, \ldots, x_n]/I)$ a closed subscheme of $\mathbb{A}_R^n$ with ideal I generated by degree one linear forms. By Proposition 3.3.1 each morphism $X \to C$ is uniquely determined by the ring homomorphism of it's global sections

$$R[x_1, \ldots, x_n]/I \to \Gamma(X, \mathcal{O}_X)$$

Since the above ring homomorphism is uniquely determined by it's values $x_i \mapsto a_i \in \Gamma(X, \mathcal{O}_X)$, it follows that each $f \in C_R(X)$ has a natural representation as an n-tuple $(a_1, \ldots, a_n) \in \Gamma(X, \mathcal{O}_X)^n$. We define the addition of two morphism $f, g \in C_R(X)$ in the obvious way by taking

$$f + g := (a_1, \ldots, a_n) + (b_1, \ldots, b_n)$$

This is well defined since the ideal I is generated by degree one linear forms. It is also clear $\alpha f \in C_R(X)$, for every $\alpha \in \mathcal{O}_X(X)$. Therefore $C_R(X)$ is an $\mathcal{O}_X(X)$-module. If $U \subseteq X$ is open, then in the same way we obtain $C_R(U)$ is an $\mathcal{O}_X(U)$-module. Checking compatibility with the structure sheaf $\mathcal{O}_X$, we conclude using Proposition 3.6.4 that $C_R(-)$ is a sheaf of $\mathcal{O}_X$-modules.

Let $X = \operatorname{Spec} S$ be an affine scheme. To show $C_R(-)$ is the associated sheaf $\widetilde{C_R(X)}$ as an S-module, it is enough to check $C_R(X)_f \cong C_R(D(f))$ over each distinguished open $D(f)$, with $f \in S$. We define a map

$$\begin{array}{rcl} C_R(X)_f & \to & C_R(D(f)) \\ \frac{1}{f^k}(a_1, \ldots, a_n) & \mapsto & (\frac{a_1}{f^k}, \ldots, \frac{a_n}{f^k}) \end{array}$$

The only non-trivial part is showing this map is surjective. Let $(\frac{b_1}{f^k}, \ldots, \frac{b_n}{f^k}) \in C_R(D(f))$. Since R is a noetherian ring the ideal $I = (g_1, \ldots, g_k)$ is finitely generated. For each $j = 1, \ldots, k$ there exists f^{l_j}, $l_j \geq 0$ such that

$$f^{l_j}\, g_j(\frac{b_1}{f^k}, \ldots, \frac{b_n}{f^k}) = 0$$

Let $l := k + l_1 + \cdots + l_k$. Then the tuple $(a_1 f^l, \ldots, a_n f^l) \in C_R(X)$. Taking $\frac{1}{f^{l+k}}(a_1 f^l, \ldots, a_n f^l) \in C_R(X)_f$, we have the desired result. □

A morphism between two linear codes $(C, \mathbb{A}_R^n, \Sigma_R^n)$ and $(D, \mathbb{A}_R^m, \Sigma_R^m)$ is a morphism of codes (f, g, α) such that the maps $g^* : C_R(X) \to D_R(X)$ and $f^* : \mathbb{A}_R^n(X) \to \mathbb{A}_R^m(X)$

induces a morphism of $\mathcal{O}_X$-modules for every scheme X. We can form the subcategory of geometric linear codes with classical error structure by restricting ourselves to the objects corresponding to linear codes and linear morphisms. In this way, the above structure becomes much closer to the standard definition of a linear code. In fact we will show over an arbitrary field the two categories are equivalent. First we need to define the category of linear codes.

In a similar fashion, we define the category of linear codes as the objects (C, k^n, Σ_k^n) consisting of a linear subspace $C \subseteq k^n$ and diagram Σ_k^n of vector spaces. The diagram of vector spaces is equivalent to it's geometric counterpart, if we replace the group schemes $G_{(i_1,\dots,i_m)}$ with m-dimensional vector spaces and group scheme morphisms with k-linear maps. The actions of the vector spaces in the diagram Σ_k^n do not act linearly on k^n. We will sometimes view k^n as a set rather than a vector space with Σ_k^n acting on k^n as a set. The diagram Σ_k^n can also be interpreted as a quiver representation over a directed graph or in a dual sense as a kQ-module, where kQ is the non-commutative k-algebra generated by the paths. This insight will play an important role in code representations, but we leave this for another time. The definition of a morphism between linear codes is clear.

Proposition 4.3.4. *Let k be a field. Then the category of linear geometric codes over Spec k and the category of linear codes over k are equivalent.*

Proof. To show the equivalence of the two categories we will first construct a functor S from the category of linear geometric codes to the category of linear codes. Let k be a field and S denote the map taking a linear geometric code

$$(C, \mathbb{A}_k^n, \Sigma_G^n) \mapsto (C(k), k^n, \Sigma_k^n)$$

to it's k-rational points and a morphism

$$(g, f, \alpha) : (C, \mathbb{A}_k^n, \Sigma_G^n) \to (D, \mathbb{A}_k^n, \Sigma_G^n)$$

to $S(f, g, \alpha) = (f_k, g_k, \alpha_k)$, where $g_k : C(k) \to D(k)$, $f_k : k^n \to k^m$, and $\alpha_k : \Sigma_k^n \to \Sigma_k^m$ are the induced maps over the k-rational points. Observe that both f_k and g_k are linear maps by definition. The morphism, α_k also induces a family of k-linear maps. It is easy to check S preserves morphism composition and maps the identity map to the identity map. Therefore S is a functor.

To construct the inverse, consider the map

$$(C, k^n, \Sigma_k^n) \mapsto (\operatorname{Spec}(k[x_1, \dots, x_n]/I_C), \mathbb{A}_k^n, \Sigma_G^n)$$

where I_C is the ideal generated by all degree one linear forms $f \in k[x_1, \dots, x_n]$ such that $f(c_1, \dots, c_n) = 0$ for every $(c_1, \dots, c_n) \in C$. In order for us to construct an inverse functor T, we need to show every morphims of linear codes over k

$$(f_k, g_k, \alpha_k) : (C, k^n, \Sigma_k^n) \to (D, k^m, \Sigma_k^m)$$

extends to a morphism of geometric linear codes

$$(f, g, \alpha) : (\operatorname{Spec}(k[x_1, \dots, x_n]/I_C), \mathbb{A}_k^n, \Sigma_G^n) \to (\operatorname{Spec}(k[x_1, \dots, x_m]/I_D), \mathbb{A}_k^m, \Sigma_G^m)$$

It is enough to construct a commutative diagram of ring homomorphisms

$$\begin{tikzcd}
k[x_1, \dots, x_m] \arrow[r, "f^{\#}"] \arrow[d] & k[x_1, \dots, x_n] \arrow[d] \\
k[x_1, \dots, x_m]/I_D \arrow[r, "g^{\#}"] & k[x_1, \dots, x_n]/I_C
\end{tikzcd}$$

using the diagram of k-linear maps

$$\begin{tikzcd}
k^n \arrow[r, "f_k"] & k^m \\
C \arrow[u] \arrow[r, "g_k"] & D \arrow[u]
\end{tikzcd}$$

For each canonical basis element $e_i \in k^n$, $i = 1, \dots, n$, compute $f_k(e_i) = \sum_{k=1}^{m} a_{ik} e_k$. We define $f^{\#}(x_i) := \sum_{k=1}^{n} a_{ki} x_k$ and $g^{\#}(\overline{x_i}) := \sum_{k=1}^{n} a_{ki} \overline{x_k}$, for each $i = 1, \dots, n$. To show $g^{\#}$ is well defined, it is enough to show every linear form $l \in I_D$ maps to a linear form $f^{\#}(l) \in I_C$. Let $l = b_1 x_1 + \cdots b_m x_m$ and $(c_1, \dots, c_n) \in C$. Then

$$\begin{aligned}
(f^{\#}(l))(c_1, \dots, c_n) &= \sum_{i=1}^{m} b_i \Big(\sum_{k=1}^{n} a_{ki} c_k \Big) \\
&= \sum_{i=1}^{m} b_i f_k(c_1, \dots, c_n) \\
&= l(f_k(c_1, \dots, c_n)) \\
&= 0
\end{aligned}$$

Since this holds for any $(c_1, \dots, c_n) \in C$, $f^{\#}(l)$ is zero on all of C. If $f^{\#}(l) \notin I_C$, then $f^{\#}(l)$ is linear independent from the linear forms generating I_C and so the ideal $(I_C, f^{\#}(l))$ induces a vector space of k-rational points with dimension equal to $\dim C - 1$. This contradicts the fact that every element $(c_1, \dots, c_n) \in C$ vanishes over the ideal $(I_C, f^{\#}(l))$. Hence $f^{\#}(l) \in I_C$ and $g^{\#}$ is well defined. We can construct a diagram morphism $\alpha : \Sigma_G^n \to \Sigma_G^m$ by iterating the above process. Therefore we finish the construction of T be defining $T(f_k, g_k, \alpha_k) = (f, g, \alpha)$. It is clear, T preserves both morphism composition and the identity map. Hence T is a functor.

To complete the proof, all we have left to show is that $ST = I$ and $TS = I$, but this is clear from the constructions of S and T. □

The above proposition is analogous to Corollary 3.3.2 in which we showed the category of affine schemes is equivalent to the category of commutative rings with arrows reversed. In this particular case, we showed all the geometric information for linear codes lies in it's k-rational points. So using either the geometric or vector space view point is equivalent since we can exchange information freely between the two systems. The above proposition will not generalize to non-linear codes over an arbitrary field since taking k-rational points does not induce a faithful functor.

Therefore for the non-linear case we must use the geometric interpretation.

4.4 Error Correcting

Definition 4.4.1. A code can *correct* an error in $G_{(i_1,\dots,i_k)}$ provided the composition

$$G_{(i_1,\dots,i_k)} \times_{\operatorname{Spec} R} C \to G_{(i_1,\dots,i_k)} \times_{\operatorname{Spec} R} \mathbb{A}^n_R \to \mathbb{A}^n_R$$

is monomorphic.

From the definition it easily follows that whenever C can correct an error in $G_{(i_1,\dots,i_k)}$, then it can also correct all other errors corresponding to vertices $G_{(i_1,\dots,i_l)}$, with $\{i_1,\dots,i_l\} \subseteq \{i_1,\dots,i_k\}$.

Definition 4.4.2. The *height* $h(G_{(i_1,\dots,i_k)})$ of a vertice in Σ_G is defined as the size of the longest chain from $\operatorname{Spec} R$ to $G_{(i_1,\dots,i_k)}$. The *minimum distance* of a code C is defined as

$$d_C := \min_{G \in I} h(G)$$

over the set $I := \{G \in \Sigma_G | \, C \times G \not\hookrightarrow \mathbb{A}^n_R\}$.

Proposition 4.4.3. *Let $(C, \mathbb{A}^n_R, \Sigma^n_R)$ be a closed code over a affine Noetherian scheme* $\operatorname{Spec} R$. *Then*

$$\min_{\mathfrak{p} \in \operatorname{Spec} R} d_{C(R_\mathfrak{p})} \leq d_{C(R)}$$

In particular, if the code is linear then we have equality.

Proof. Let $\mathfrak{p} \in \operatorname{Spec} R$ and C a closed subscheme of $\mathbb{A}^n_R$. By Proposition 3.6.4, the representable functor $\operatorname{Mor}_R(-, C)$ is a sheaf on the Zariski topology in $\operatorname{Spec} R$. If we can show

$$\text{(1)} \qquad \operatorname{colim}_{\mathfrak{p}\in U} \operatorname{Mor}_R(U,C) \cong \operatorname{Mor}_R(\operatorname{Spec} R_\mathfrak{p}, C) = C(R_\mathfrak{p})$$

then the inequality will follow by Proposition 3.4.2. To show (1) we will prove the set $\operatorname{Mor}_R(\operatorname{Spec} R_\mathfrak{p}, C)$ is the initial object in that category of CoCones over the diagram of open sets containing the point $\mathfrak{p}$. It is enough to look at only the distinguished open sets containing $\mathfrak{p}$, since they form a basis on $\operatorname{Spec} R$. Let X be a CoCone over the diagram of open sets containing $\mathfrak{p}$. Then we have the commutative diagram,

$$\begin{tikzcd}
C(R_\mathfrak{p}) \arrow[rr, dashed, "\exists!\, h"] & & X \\
& C(R_f) \arrow[ul, "\alpha_f"'] \arrow[ur, "\beta_f"] \arrow[d] & \\
& C(R_{fg}) \arrow[uul, "\alpha_g"] \arrow[uur, "\beta_g"'] &
\end{tikzcd}$$

with $f, g \in R \setminus \mathfrak{p}$. To show $C(R_\mathfrak{p})$ is the initial object we must show there exists a unique map h making the diagram commute. We will construct h by showing each $\lambda \in C(R_\mathfrak{p})$ extends to a morphism over a distinguished open set $D(f)$ for some $f \notin \mathfrak{p}$. Let $\lambda \in C(R_\mathfrak{p})$. Then the ring homomorphism $\lambda^\# : R[x_1, \ldots, x_n]/I \to R_\mathfrak{p}$ is determined by it's values $x_i \mapsto a_i/f_i$. Taking $f := f_1 \cdots f_n$, we can replace each f_i with a common denominator f so that for each i, $x_i \mapsto a_i'/f$. Since R is assumed to be Noetherian, the ideal $I = (g_1, \ldots, g_k)$ is finitely generated. So for each $j = 1, \ldots, k$ there exists $l_j \in R \setminus \mathfrak{p}$ such that

$$l_j\, g_j(\frac{a_1'}{f}, \ldots, \frac{a_n'}{f}) = 0$$

Let $l := l_1 \cdots l_k$ and $f' := l\, f$. Then

$$f'\, g_j(\frac{a_1' l}{f'}, \ldots, \frac{a_n' l}{f'}) = 0 \quad \text{for each } j = 1, \ldots, k$$

Therefore there exists an extension $\lambda_{f'}$ over the distinguished open set $D(f')$ making the diagram commute

$$\begin{tikzcd}
\operatorname{Spec} R_{\mathfrak{p}} \arrow[r, "\lambda"] \arrow[d] & C \\
\operatorname{Spec} R_f \arrow[ur, "\lambda_{f'}"'] &
\end{tikzcd}$$

Define $h(\lambda) := \beta_{f'}(\lambda_{f'})$. This is well defined since any other representation $\lambda_{f''}$ must be equal to $\lambda_{f'}$ over the open set $D(f') \cap D(f'')$. Therefore

$$\begin{aligned}
\beta_{f'}(\lambda_{f'}) &= \beta_{f'f''}(\lambda_{f'}|_{D(f'f'')}) \\
&= \beta_{f''}(\lambda_{f'})
\end{aligned}$$

Moreover the uniqueness of h, follows since every map h' satisfying $h'\alpha_f = \beta_f$ for every $f \notin R \setminus \mathfrak{p}$, must be equal to h, since every $\lambda \in C(R_{\mathfrak{p}})$ can be represented by some λ_f with $\lambda = \alpha_f(\lambda_f)$. Hence by the universality of colimits (1) holds.

Since each $\operatorname{Spec} R \neq G \in V(\Sigma_G)$ is isomorphic to $\mathbb{A}_R^k$ for some $k > 0$, the product $G \times_R C$ is a closed subscheme of $\mathbb{A}_R^{n+k}$. Therefore we can use the above argument for evaluating stalks. By proposition 3.1.6 the morphism of sheaves

$$(G \times_R C)(-) \to \mathbb{A}_R^n(-) \tag{2}$$

is monomorphic if and only if it is monomorphic at the stalks. Hence

$$\min_{\mathfrak{p} \in \operatorname{Spec} R} d_{C(R_{\mathfrak{p}})} \leq d_{C(R)}$$

Next, suppose C is a linear geometric code. Then the product $G \times_R C$ is a closed subscheme of $\mathbb{A}_R^{n+k}$, corresponding to an ideal generated by degree one linear forms. By Proposition 4.3.3 the sheaf $(G \times_R C)(-)$ is a sheaf of modules over $\operatorname{Spec} R$. Since $\operatorname{Spec} R$ is an affine scheme, we know further that it's sheaf structure is the associated sheaf $(G \times_R C)\widetilde{(-)}$ induced as an R-module. Similarly it follows that the sheaf $\mathbb{A}_R^n(-)$ also has the associated sheaf structure $\mathbb{A}_R^n\widetilde{(-)}$. Since the action of G on C is addition, it follows that the morphism in (2) is actually a morphism of $\mathcal{O}_{\operatorname{Spec} R}$-modules. By Proposition 3.4.2 and the argument above, we have

$$(G \times_R C)\widetilde{(-)}_{\mathfrak{p}} \cong (G \times C)(R)_{\mathfrak{p}} \cong (G \times C)(R_{\mathfrak{p}})$$

Therefore

$$0 \to (G \times_R C)(R) \to \mathbb{A}^n_R(R)$$

is injective as R-modules if and only if

$$0 \to (G \times C)(R) \otimes R_{\mathfrak{p}} \to \mathbb{A}^n_R(R) \otimes R_{\mathfrak{p}}$$

is injective for every $\mathfrak{p} \in \operatorname{Spec} R$. Hence, equality holds. □

The above proposition does not hold in general if the code is non-linear.

Example 4.4.4. Let $R = \mathbb{Z}$ be the ring of integers and consider the code $C = \operatorname{Spec}(\mathbb{Z}[x,y]/(x, y(2y-1)) \subset \mathbb{A}^2_{\mathbb{Z}}$. Then the $\mathbb{Z}$-valued point is $C(\mathbb{Z}) = \{(0,0)\}$ which by definition has minimum distance $d_{C(\mathbb{Z})} = 2$. Taking the local ring $\mathbb{Z}_{(0)} = \mathbb{Q}$, it follows that $C(\mathbb{Q}) = \{(0,0), (0,1/2)\}$. This has minimum distance 1 and therefore equality does not hold in general.

Proposition 4.4.5. *Let $(C, \mathbb{A}^n_R, \Sigma^n_R)$ be a code over Spec R with minimum distance d_C, and $R \to S$ a ring homomorphism. Then the code*

$$(C \times_{\operatorname{Spec} R} \operatorname{Spec} S, \mathbb{A}^n_S, \Sigma^n_S)$$

under base change has minimum distance $d_C \leq d_{C \times \operatorname{Spec} S}$.

Proof. If $G \times_R C \to \mathbb{A}^n_R$ is monomorphic, then $(G \times_R C) \times_R \operatorname{Spec} S \to \mathbb{A}^n_R \times_R \operatorname{Spec} S$ is also monomorphic, since base changes preserve monomorphisms. Hence
$d_C \leq d_{C \times \operatorname{Spec} S}$ □

Chapter 5

Elliptic Curve Cryptography

Continuing with the theme of the previous sections, we introduce applications of algebraic geometry to cryptographic systems. We begin by discussing public key cryptography and the Diffie-Hellman problem. We outline the key problems and discuss how elliptic curves are used. Finally we will show how one can naturally construct an abelian group over the rational points of an elliptic curve using divisors and the Riemann-Roch theorem.

5.1 Public Key Cryptography

Increasing demand in secure communications over large networks, has made *public key* cryptography a viable way of exchanging information secretly. The ideas behind public key cryptography is conceptually simple and based on the following scenario. Suppose two users X and Y are interested in sending each other information. We suppose there is an eavesdropper who has access to the information user X and Y send each other. User X picks at random a function f, which converts plaintext messages to an encrypted one. User X publicly announces their choice of f. User Y, then takes a message m and computes $f(m)$, and sends it back to user X. The system is insecure if it is "easy" to invert $f(m)$ without knowing any extra information. We use the word easy to mean that in some realitivistic sense it is computationally feasible to find the inverse. The function f is called, a *public key encryption function.* The advantage of this system is that any two users can send information between one another without any prior contact.

An example of how the above scenario is implemented in practice is based on the Diffie-Hellman key exchange. Suppose both users X and Y agree publicly on an element g in the multiplicative group $\mathbb{F}_p^\times$ of some finite field. User X, secretly chooses at random an integer k_x, computes g^{k_x}, and sends this to user Y. In the same way, user Y sends X the value g^{k_y} for some randomly chosen integer k_y. The agreed upon key will be the value $g^{k_x k_y}$, which both user X and Y can compute. The problem of the eavesdropper is to find $g^{k_x k_y}$, given only g, g^{k_x}, and g^{k_y}. The problem can be solved provided they know how to compute discrete logarithms. That is they can find for any two pair of values $g, y \in \mathbb{F}_p^\times$, an integer k if it exists, such that $y = g^k$. For practical purposes the Diffie-Hellman key exchange is said to be secure provided that finding the discrete logarithm is not computationally feasible.

The problem with the above scheme is that it rests upon computing elements in the group $\mathbb{F}_p^\times$. Recent progress in computing finite field discrete logarithms have made key sizes grow substantially. An alternative solution proposed by Victor Miller and Neal Koblitz in 1985, is based on the abelian group of rational points of an elliptic curve. The advantage of using these groups, is that there are a large diversity of groups to choose from, and there are no current known sub-exponential time algorithms for finding discrete logarithms on supersingular curves. Before we introduce elliptic curves, we will briefly discuss projective schemes.

5.2 Projective Schemes

Let $S = R[x_0, \ldots, x_n]$ be a polynomial ring in $n+1$-variables over a commutative ring R. S has a natural grading as a ring given by,

$$S = \bigoplus_{d \geq 0} S_d$$

satisfying

$$S_d \cdot S_e \subset S_{d+e}$$

The elements of S_d are all the homogeneous polynomials of degree d. An ideal $I \subset S$ is said to be a *homogeneous ideal* provided every element can be written as the sum of homogeneous components. A homogeneous ideal is said to be prime provided it is prime in the ring S. We define,

$$\mathbb{P}^n_R = \{ \mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec} S \text{ is a homogeneous prime ideal of } S, \mathfrak{p} \not\supseteq S_+ \}$$

where

$$S_+ := \bigoplus_{d \geq 1} S_d$$

In the same way, we defined closed sets over an affine scheme we put,

$$V(I) = \{ \mathfrak{p} \in \mathbb{P}^n_R \mid \mathfrak{p} \supseteq I \}$$

to be a closed set for any homogeneous ideal $I \subset S$. Checking one can show this forms a topology on $\mathbb{P}^n_R$. The structure sheaf $\mathcal{O}_{\mathbb{P}^n_R}$ is the sheaf induced by the sheafication of the presheaf defined by,

$$\Gamma(D_+(f), \mathcal{O}) = \{\, g/f^m \mid f \in S_d, g \in S_{md}, m \geq 0 \,\} = S_f^{(0)}$$

where $S_f^{(0)}$ is the degree zero elements in the local ring S_f. From the definition it follows that the restriction $(D_+(f), \mathcal{O}_{\mathbb{P}^n_R}|_{D_+(f)})$ of $\mathbb{P}^n_R$ over the open set $D_+(f)$ is isomorphic to the affine scheme $(\operatorname{Spec}(S_f^{(0)}), \mathcal{O}_{\operatorname{Spec} S_f^{(0)}})$. Therefore $\mathbb{P}^n_R$ is a scheme, since it is locally affine. Taking the open sets $D_+(x_i)$ for each i, one can show

$$(D_+(x_i), \mathcal{O}_{\mathbb{P}^n_R}|_{D_+(x_i)}) \cong \operatorname{Spec} R[\frac{x_1}{x_i}, \ldots, \frac{x_n}{x_i}] \cong \mathbb{A}^n_R$$

So we can view projective space as the gluing of affine n-space's over suitable open sets.

If we let $R = k$ for some field, then the k-rational points,

$$\mathbb{P}^n_k(k) = \{\, (a_0, \ldots, a_n) \in k^n \backslash \{0\} \mid (a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \text{ provided there exists } k \neq 0 \text{ such that } a_i = kb_i \text{ for every } i \,\}$$

We write the points in $\mathbb{P}^n_k(k)$ as $(a_0 : \ldots : a_n)$. This confirms the classical definition of projective space, where points correspond to one-dimensional subspaces of k^{n+1}.

A *Weierstrass equation* over the projective scheme $\mathbb{P}^2_k$ is defined as the homogeneous equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_i \in k$. The curve f is said to be *non-singular* or *smooth* if the rank of the Jacobian

$$\operatorname{rk}(\partial f/\partial x_i) = 1$$

That is, for each point on the curve there exists a tangent space at that point. An *elliptic curve* is defined as a non-singular Weierstrass equation over projective space $\mathbb{P}^2_k$. There is a natural abelian group structure on the rational points of a elliptic curve, which we describe next.

5.3 Group Law of Elliptic Curves

Suppose f is an elliptic curve over an algebraically closed field and $E \subset \mathbb{P}^2_k$ is the closed subscheme corresponding to f. A *prime divisor* over E is a closed integral subscheme P of codimension one. Since f is a non-singular curve, the prime divisors correspond to the closed points in E and hence the k-rational points. A *Weil divisor* is an element of the free abelian group $\mathrm{Div}(E)$ generated by the prime divisors. A divisor over E is written as a finite sum $D = \sum n_i \cdot P_i$, where n_i are integers, and P_i are rational points. If P is a prime divisor, and $x \in P$ it's generic point, then the local ring $\mathcal{O}_{x,P}$ is a discrete evaluation ring with quotient field $k(E)$, equal to the function field of E. Let $f \in k(E)^\times$ be a non-zero meromorphic function on E. Then $v_P(f)$ is an integer. If it is positive, f is said to have a zero at P, and negative if f has a pole.

Proposition 5.3.1. *Let $f \in k(E)^\times$ be a non-zero function on E, then $v_P(f) = 0$ for all except finitely many prime divisors P.*

The *divisor* associated to f, is defined as ,

$$\mathrm{div}(f) := \sum v_P(f) \cdot P$$

where the sum is taken over all primes divisors over E. Any divisor which is equal to the divisor of a function is said to be a *principal divisor.* Two divisors D and D' are *linearly equivalent,* if $D - D'$ is a principal divisor. The group of divisors, $\mathrm{Div}(E)$ factored over the equivalence relation $D \sim D'$, whenever $D - D'$ is a principal divisor, is again a group and is called the *divisor class group*, $\mathrm{Cl}(E)$. We define a partial ordering on $\mathrm{Div}(E)$ by,

$$\sum n_p \cdot P \geq \sum m_P \cdot P \quad \text{if and only if} \quad n_P \geq m_p \quad \text{for all } P$$

In particular if, $\sum n_P \cdot P \geq 0$, then the divisor is called *effective.*

Given a divisor D, we define

$$L(D) = \{\, f \in k(E)^\times \mid \mathrm{div}(f) + D \geq 0 \,\} \cup \{0\}$$

For example, if $D = P + 2Q$, then $L(D)$ consists of the meromorphic functions having no poles outside $\{P, Q\}$ and having at most a single pole at P and a double pole at Q. Each, $L(D)$ is a finite dimensional vector space over k. We denote it's dimension by $l(D)$.

Proposition 5.3.2 (Riemann-Roch). *There exists an integer g, such that for all divisors D,*

$$l(D) \geq \deg D + 1 - g$$

with equality if $\deg D > 2g - 2$.

The integer g in the above theorem is the genus of E. Since elliptic curves are non-singular projective curves of degree 3, they will have genus 1. Accordingly, the Riemann-Roch theorem states,

$$l(D) = \deg(D) \quad \text{if} \quad \deg D \geq 1$$

Proposition 5.3.3. *Let E be a elliptic curve and $O \in E(k)$ the point at infinity.*

The map

$$\begin{aligned} E(k) &\rightarrow \mathrm{Cl}^{\mathrm{o}}(E) \\ P &\mapsto P - O \end{aligned}$$

is bijective.

Proof. We define an inverse. Let D be a divisor of degree 0. Then $D + O$ has degree one, and so there exists a meromorphic function f, unique up to multiplication be a nonzero constant, such that $\mathrm{div}(f) + D + O \geq 0$. The only divisors ≥ 0 of degree one are of the form P. Hence there is a well-defined point P such that $D + O \sim P$. □

Following the above proposition, the rational points $E(k)$ inherit a natural abelian group structure. The above group can also be determined geometrically, using the following argument.

Proposition 5.3.4 (Bezout). *, Let C and D be projective curves of degrees m and n respectively over an algebraically closed field, and assume they have no irreducible component in common. Then they intersect in exactly mn points.*

Let P and Q be two points on an elliptic curve E and L_1 the line passing through both P and Q. If $P = Q$ take the tangent line at P. By proposition 5.3.4 the line L_1 and E intersect in exactly 3 points counting multiplicity. Let R be the third point and define L_2 to be the line passing through R and the point at infinity O. Call the third point of intersection S, and define $P + Q := S$. Regarding the lines L_1 and L_2 as linear forms in X, Y, Z, let $f = L_1/L_2$. Then f has zero at P, Q, R and poles at O, S, R and so

$$\mathrm{div}(f) = P + Q + R - O - S - R = P + Q - S - O$$

Hence $P + Q \sim S + O$ which implies $P + Q = S$ according to the group structure defined by the bijection.

Appendix A

Category Theory

In this section we give a brief introduction to Category Theory, placing special emphasis on the theoretical concepts used throughout the paper. The material presented here is self-contained and only requires a minimal background in set theory and algebra. For a more complete account of Category Theory, we recommend the reader to the following reference [9].

Category Theory is the study of mathematical systems, their structures, and their relations to other systems. Its origins are based on the idea that many mathematical systems or at least the ones we are interested in studying, have a basic underlying foundation, consisting of objects and relations. The information gained from the machinery of Category Theory, is macroscopic in nature, and is essential in gaining a perspective of mathematics on a much grander scale. This is perhaps most clearly reflected in the trend of modern geometry in the past century. Up until the early half of the twentieth century, geometry was based largely on deductive reasoning and human intuition. It wasn't until a connection was drawn between geometry and algebra, that the field began to make very exciting progress. Today modern algebraic geometry is one of the fastest growing and exciting mathematical fields.

There are many natural mathematical systems, that are categories. One familiar example would be of sets. Individual sets can be viewed as objects in a system with relations corresponding to set maps. The relations between objects often play as important role as the objects themselves, since they carry information. For instance, any set can be realized by just knowing the maps between it and any other set. This is most clearly reflected, by considering the one point set. For instance, the one point set has the unique property that there exists a unique map to it from every non-empty set. Any other set with this property, is necessarily a one point set.

A more interesting example with slightly more structure are graphs. A *directed graph* G consists of a set of vertices V, arrows A, and a pair of functions

$$\begin{tikzcd} A \arrow[r, shift left, "\mathrm{dom}"] \arrow[r, shift right, "\mathrm{cod}"'] & V \end{tikzcd}$$

Each arrow f has two vertices consisting of it's domain and codomain.

Two directed graphs G and G' are related if we can construct a graph morphism between them. By a graph morphism, we mean a pair of maps $\sigma_A : A \to A'$ and $\sigma_V : V \to V'$ satisfying the relation,

$$\sigma_V \,\mathrm{cod}(f) = \mathrm{cod}\, \sigma_A(f) \quad \text{and} \quad \sigma_V \,\mathrm{dom}(f) = \mathrm{dom}\, \sigma_A(f)$$

for any arrow $f \in A$.

Notice the above two examples have the property that any two relations between objects $A \to B$ and $B \to C$ compose to give a relation from $A \to C$. Further it is easy to check these compositions are associative and every object has an identity relation. The above properties can be stated as a collection of axioms.

Definition A.0.5. Let $\mathcal{C}$ be a class of objects $\mathrm{Ob}\,\mathcal{C}$, such that

1. for each pair of objects (A, B), there is a set $\mathrm{Mor}_{\mathcal{C}}(A, B)$ whose elements are called *morphisms*, with the property $\mathrm{Mor}_{\mathcal{C}}(A, B) = \mathrm{Mor}_{\mathcal{C}}(C, D)$ if and only if $A = C$ and $B = D$.

2. there is a *composition* operation

$$\mathrm{Mor}_{\mathcal{C}}(A,B) \times \mathrm{Mor}_{\mathcal{C}}(B,C) \to \mathrm{Mor}_{\mathcal{C}}(A,C)$$

   that takes the pair $(f,g) \to fg$.

$\mathcal{C}$ is called a category if it satisfies the following axioms:

3. Associativity: For all objects $A, B, C, D \in \mathrm{Ob}\,\mathcal{C}$ and all morphisms $f \in \mathrm{Mor}_{\mathcal{C}}(A,B)$, $g \in \mathrm{Mor}_{\mathcal{C}}(B,C)$, and $h \in \mathrm{Mor}_{\mathcal{C}}(C,D)$ we have

$$h(gf) = (hg)f$$

4. Identity: For each object A, there is an identity morphism $1_A \in \mathrm{Mor}_{\mathcal{C}}(A,A)$ for which,

$$1_A f = f, \quad g 1_A = g$$

From the definition, one can deduce that both sets and directed graphs form categories. Other familiar categories are:

Grps The category of groups; objects are groups and morphisms are group homomorphisms.

Top The category of topological spaces; objects are topological spaces, and morphisms are continuous maps.

R-mod The category of R-modules; objects are R-modules and morphisms are R-linear maps.

C^∞**-Man** The category of C^∞ manifolds; objects are differentiable manifolds, and morphisms are diffeomorphisms.

We also have the notion of a subcategory. A category $\mathcal{D}$ is called a *subcategory* of $\mathcal{C}$ if,

$$\mathrm{Ob}\,\mathcal{D} \subseteq \mathrm{Ob}\,\mathcal{C} \quad \text{and} \quad \mathrm{Mor}_{\mathcal{D}}(A,B) \subseteq \mathrm{Mor}_{\mathcal{C}}(A,B)$$

for all $A, B \in \mathrm{Ob}\,\mathcal{D}$, such that the composition morphisms in $\mathcal{D}$ coincide with those in $\mathcal{C}$, and the identity morphism of each object in $\mathcal{D}$ is also the identity object viewed in $\mathcal{C}$. We say a subcategory $\mathcal{D}$ is a *full subcategory* of $\mathcal{C}$ if for any objects A and B in $\mathcal{D}$, all of $\mathrm{Mor}_{\mathcal{C}}(A,B)$ is also in $\mathrm{Mor}_{\mathcal{D}}(A,B)$. An example of a full subcategory, are a collection of objects satisfying an additional property. For example in the category of groups, the abelian groups form a full subcategory.

The ability to compare categories is a very important concept in Category Theory. It allows us to build a bridge between different mathematical systems. For instance, Algebraic Geometry depends on the mutual exchange of information between geometry and algebra. This natural translation allows us to relate certain geometric idea's in a purely algebraic setting. We can also use this natural exchange of information to translate a difficult problem in one mathematical system, to another problem that may be more tractable. In Algebraic Topology, the Brouwer Fixed Point Theorem, states for every continuous function from the disk $f : D^1 \to D^1$, there exists a fixed point x, with $f(x) = x$. The proof of this is based on a simple connectedness argument. A problem occurs, however when trying to generalize this proof to the case of continuous functions $f : D^n \to D^n$ on n-dimensional disks. In algebraic topology, we can assign each topological space X to an abelian group $H_n(X)$ called its homology group and each continuous function $f : X \to Y$ to a homomorphism of groups $H_n(f) : H_n(X) \to H_n(Y)$. The proof then becomes easier, and depends on showing that for $n \geq 0$, the n-dimensional sphere S^n is not a retract of D^{n+1}, using the fact that $H_n(D^{n+1}) = 0$ for every $n \geq 1$ and $H_n(S^n) \neq 0$ for every $n \geq 1$. The above concepts are based on the following definition.

Definition A.0.6. A *functor* $T : \mathcal{C} \to \mathcal{D}$ between two categories $\mathcal{C}$ and $\mathcal{D}$ consists of a map

1. $\mathrm{Ob}\,\mathcal{C} \ni A \mapsto T(A) \in \mathrm{Ob}\,\mathcal{D}$

2. If $f : A \to B$ in $\mathcal{C}$, then $T(f) : T(A) \to T(B)$ in $\mathcal{D}$
   such that,

3. For any morphism f, g in $\mathcal{C}$, for which gf is defined, then

$$T(gf) = T(g)T(f)$$

4. $T(1_A) = 1_{T(A)}$ for every object $A \in \mathrm{Ob}\,\mathcal{C}$.

Functors that satisfy (a) through (d) are often referred to as *covariant* functors. A functor is said to be *contravariant* if in part (c) we instead say $T(gf) = T(f)T(g)$ for all $f \in \mathrm{Mor}_{\mathcal{C}}(B, C)$, $g \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ and for all $A, B, C \in \mathrm{Ob}\,\mathcal{C}$

Example A.0.7. Consider the category of all finite dimensional vector spaces over some fixed field k. We define a functor $T : \mathbf{Vct} \to \mathbf{Vct}$ by taking a vector space $V \mapsto V^* := \mathrm{Hom}(V, k)$ to its dual space of all linear functions from V to k. T is contravariant since every morphism $f : V \to V'$, corresponds to a natural homomorphism $\mathrm{Hom}(V', k) \xrightarrow{f^*} \mathrm{Hom}(V, k)$ taking $\pi \in \mathrm{Hom}(V', k) \mapsto \pi f \in \mathrm{Hom}(V, k)$.

Naturally we can place a category on the set of functors, by introducing the notion of a Natural Transformation. A *natural transformation* between two functors $S, T : \mathcal{C} \to \mathcal{D}$ is a function which assigns to each object $A \in \mathcal{C}$, a morphism τ_A :

$S(A) \to T(A)$ in such a way that the diagram commutes

$$\begin{tikzcd}
S(A) \arrow[r, "S(f)"] \arrow[d, "\tau_A"'] & S(B) \arrow[d, "\tau_B"'] \\
T(A) \arrow[r, "T(f)"] & T(B)
\end{tikzcd}$$

Example A.0.8. Taking a vector space $V \mapsto (V^*)^*$ to it's double dual is a natural transformation.

In the category of functors, objects are functors and morphisms are natural transformations. Two functor's $S, T : \mathcal{C} \to \mathcal{D}$ are said to be naturally isomorphic if there are natural transformations ψ and ϕ satisfying, $\psi\phi = \text{id}_S$ and $\phi\psi = \text{id}_T$.

Definition A.0.9. A functor $T : \mathcal{C} \to$ **Sets** is called *representable* if for some object $A \in \mathcal{C}$, T is isomorphic to the covariant functor $h_A(-) := \text{Mor}_{\mathcal{C}}(A, -)$.

Example A.0.10. Let T : **Grps** $\to$ **Sets** be the forgetful functor that strips away the group structure. We claim that T is representable by the covariant functor $h_{\mathbb{Z}}$, where $\mathbb{Z}$ is the integers under addition. This is clear since any element $g \in T(G)$ can be mapped to $\pi_g \in \text{Mor}(\mathbb{Z}, G)$ with $\pi_g(1) := g$. Similarly any morphism $\lambda \in \text{Mor}(\mathbb{Z}, G)$ can be represented by some $\pi_g, g \in G$. Checking the conditions, we see that they are naturally isomorphic.

Proposition A.0.11 (Yoneda's Lemma). *Let $\mathcal{C}$ be a category and let A, B be objects of $\mathcal{C}$.*

1. *If T is any contravariant functor from $\mathcal{C}$ to the category of sets, the natural transformations from $Mor_{\mathcal{C}}(-, A)$ to T are in one to one correspondence with elements of $T(A)$.*

2. *If the functors $Mor_{\mathcal{C}}(-, A)$ and $Mor_{\mathcal{C}}(-, B)$ from $\mathcal{C}$ to the category of sets are isomorphic, then $A \cong B$*

Proof. (1) Let $\tau : \mathrm{Mor}_{\mathcal{C}}(-, A) \to T(-)$ be a natural transformation. We define a map

$$\begin{aligned} \mathrm{Nat}(\mathrm{Mor}_{\mathcal{C}}(-, A), T(-)) &\to T(A) \\ \tau &\mapsto \tau(1_A) \end{aligned}$$

In the opposite direction, given an element $p \in T(A)$ we can form a natural transformation by taking $f \in \mathrm{Mor}_{\mathcal{C}}(X, A)$ to $T(f)(p) \in T(X)$. Checking, one can see the above two maps are inverses of each other.

(2) If we let $T = \mathrm{Mor}_{\mathcal{C}}(-, B)$, then in part 1 we showed every natural transformation $\tau : \mathrm{Mor}_{\mathcal{C}}(-, A) \to \mathrm{Mor}_{\mathcal{C}}(-, B)$ corresponds to an element $p \in \mathrm{Mor}_{\mathcal{C}}(A, B)$ such that for any $h : X \to A$, $\tau(h) = p \circ h$. If

$$\begin{tikzcd} \mathrm{Mor}_{\mathcal{C}}(-, A) \arrow[r, shift left, "\tau"] & \mathrm{Mor}_{\mathcal{C}}(-, B) \arrow[l, shift left, "\tau^{-1}"] \end{tikzcd}$$

are isomorphic as functors, define $f := \tau(1_A)$ and $g := \tau^{-1}(1_B)$. Then it follows $f \circ g = \tau\tau^{-1}(1_B)$ and $g \circ f = \tau^{-1}\tau(1_A) = 1_A$. □

A.1 Objects and Morphisms

In this section we introduce a special class of objects and morphisms, that are universally defined in every category. Important general properties concerning all categories, can be proven as a result of these definitions.

A morphism f in a category $\mathcal{C}$ is called a *monomorphism* if for all pairs (g, h) of $\mathcal{C}$,

$$fg = fh \quad \text{if and only if} \quad g = h$$

A morphism f' in a category $\mathcal{C}$ is called an *epimorphism* if for all pairs (g, h) of $\mathcal{C}$,

$$gf' = hf' \quad \text{if and only if} \quad g = h$$

Example A.1.1. In the category of sets f is an epimorphism if and only if it is surjective as a map. In the category of commutative rings, f epimorphic, does not necessarily imply it's underlying set map is surjective. For instance, if we consider the canonical map $f' : \mathbb{Z} \to \mathbb{Q}$. Then clearly for any pair of ring homomorphisms $g, h : R \to \mathbb{Z}$, $f'g = f'h$ implies $g = h$, but the homomorphism from $\mathbb{Z}$ to $\mathbb{Q}$ is not surjective.

A morphism $f \in \operatorname{Mor}_{\mathcal{C}}(A, B)$ is called an *isomorphism* if there exists a morphism $g \in \operatorname{Mor}_{\mathcal{C}}(B, A)$ such that $fg = 1_B$ and $gf = 1_A$. Two objects, A and B are said to be isomorphic if $\operatorname{Mor}_{\mathcal{C}}(A, B)$ contains an isomorphism. If f is an isomorphism, then f is both a monomorphism and epimorphism. The converse is not true in general.

An object X in a category $\mathcal{C}$ is called *terminal*, if for every object $Y \in \operatorname{Ob}\mathcal{C}$, there is exactly one morphism $Y \to X$. Terminal objects do not necessarily exist in every category. When they do exist however, any two terminal objects are necessarily isomorphic with one isomorphism between them. Dually, we can define an *initial* object by switching the arrows in the opposite direction.

Example A.1.2. In the category of commutative rings, $\mathbb{Z}$ is an initial object, since for any commutative ring R there exists a unique morphism $\mathbb{Z} \to R$.

Let $\{X_i\}_{i \in I}$ be a family of objects in $\mathcal{C}$. A *product* of this family is an object X with morphisms $p_i : X \to A_i$ such that for any family $f_i : Y \to A_i$, $i \in I$, there is exactly one morphism $f : X \to Y$ with $p_i f = f_i$ for every $i \in I$. We denote X by, $\prod_{i \in I} X_i$.

The *coproduct* of a family of objects $\{X_i\}$ is naturally defined to be the dual of the product, by reversing the arrows. We denote the coproduct by $\coprod_{i \in I} X_i$.

Example A.1.3. The product of two directed graphs G and G' is the set product of the vertices $V \times V'$ and arrows $A \times A'$ such that $\mathrm{dom}(i \times i' \to j \times j') = \mathrm{dom}(i) \times \mathrm{dom}(i') \in V \times V'$ and $\mathrm{cod}(i \times i' \to j \times j') = \mathrm{cod}(j) \times \mathrm{cod}(j') \in V \times V'$.

A category is said to have *equalizers* if every pair of morphisms $f, g : X \to Y$, there exists an object Z and morphism $h : Z \to X$, such that $fh = gh$, and for every morphism $v : Y' \to X$ with $fv = gv$, there is exactly one morphism $w : Y' \to Z$ such that $v = hw$. Equivalently, we say Z is the universal object in the commutative diagram

$$\begin{tikzcd}
Y' \arrow[d, dashed, "\exists!\, w"'] \arrow[dr, "v"] & & \\
Z \arrow[r, "h"'] & X \arrow[r, shift left, "{f,g}"] \arrow[r, shift right] & Y
\end{tikzcd}$$

More generally we define the *fibre product* of two morphisms f and g with the same codomain to be the pullback P of the commutative diagram

$$\begin{tikzcd}
P \arrow[r, "s"] \arrow[d, "r"'] & X \arrow[d, "f"'] \\
Y \arrow[r, "g"] & Z
\end{tikzcd}$$

such that for any object D with morphisms $u : D \to X$ and $v : D \to Y$ satisfying $fu = gv$, there is exactly one morphism $w : D \to P$ with $sw = u$ and $rw = v$.

We can define coequalizers and pushouts by reversing the arrows of equalizers and fibre products

A.2 Limits

A *diagram* Σ over a directed graph I is a collection of objects $\{X_i\}_{i \in I}$ in a category $\mathcal{C}$, such that for each arrow $i \to j$ there is a corresponding morphism $f_{i,j} \in \mathrm{Mor}_{\mathcal{C}}(X_i, X_j)$. An I-diagram Σ in $\mathcal{C}$ is behaves very much like a subcategory of $\mathcal{C}$, with the exception that identities need not exist and compositions are not necessarily closed.

Definition A.2.1. Let $\mathcal{C}$ be a category and Σ an I-diagram with objects $X_i \in \mathcal{C}$, $i \in I$. A *cone* to the diagram Σ is an object $X \in \mathcal{C}$ and a family of morphisms $g_i : X \to X_i$, such that for each arrow $f_{i,j} : X_i \to X_j$, $f_{i,j} \circ g_i = g_j$ for every $i, j \in I$.

The cones over a diagram Σ form a category $\mathbf{Cones}(\Sigma, \mathcal{C})$. A morphism between two cones X and Y over a diagram Σ is a morphism $\pi : X \to Y$, such that the families of morphisms $g_i : X \to X_i$ and $h_i : Y \to X_i$ factor through π.

The *limit* of an I-diagram Σ is said to exist, if there exists a terminal object in $\mathbf{Cones}(\Sigma, \mathcal{C})$. Equivalently we say X is a limit in $\mathbf{Cones}(\Sigma, \mathcal{C})$ if for any cone Y there exists a unique morphism h making the diagram commute,

$$\begin{tikzcd}
X \arrow[rd, "g_i"] \arrow[rdd, "g_j"'] & & Y \arrow[ll, dashed, "\exists!\,\beta"'] \arrow[ld, "h_i"'] \arrow[ldd, "h_j"] \\
& X_i \arrow[d] & \\
& X_j &
\end{tikzcd}$$

Colimits are defined naturally to be the dual of the limit. Instead of taking the terminal object in the category $\mathbf{Cones}(\Sigma, \mathcal{C})$, we take the initial object in $\mathbf{CoCones}(\Sigma, \mathcal{C})$.

For our purposes, we will be interested in a particular type of limit that is more well behaved.

Definition A.2.2. A directed graph I containing identities and closed under composition, is said to be *filtered* if:

1. for every vertice i, j in I, there exists a vertice k with arrows $i \to k$ and $j \to k$.

2. for every pair of arrows $u, v : i \to j$, there exist an arrow $j \xrightarrow{w} k$, such that the arrow $wu = wv$.

Example A.2.3. The set of open sets $\mathbf{Top}(X)$ of a topological space X are filtered under inclusion.

Proposition A.2.4. *Let C be the category of* Sets *and Σ a filtered I-diagram. Then* $\mathrm{colim}_I X_i = (\coprod_{i \in I} X_i)/\sim$*, under the equivalence relation $x_i \in X_i \sim x_j \in X_j'$; if there exists k, with $i \to k$, $j \to k$, taking $x_i \mapsto x_k$ and $x_j \mapsto x_k$.*

The limit of a filtered I-diagram of sets is the equalizer

$$\lim_{i \in I} X_i \to \prod_{i \in I} X_i \rightrightarrows \prod_{i \to i'} X_{i'}$$

If I is finite we can construct $\lim X_i$ by iterated fibre products.

Proposition A.2.5. *If I is filtered, J finite, and if $X_{i,j}$ is an $I \times J$-diagram then we have an isomorphism*

$$\mathrm{colim}_I \lim_J X_{i,j} \xrightarrow{\sim} \lim_J \mathrm{colim}_I X_{i,j}$$

ie Filtered colimits and finite limits of sets commute.

Corollary A.2.6. *The underlying set of a filtered colimit of rings (resp. modules) is the colimit of the underlying set.*

The above is not true for general I-diagrams. For instance, if we choose I with $(1, \circlearrowleft)$ and $(2, \circlearrowleft)$, then

Sets: $\mathrm{colim}_I R_i = R_1 \coprod R_2$

Commutative Rings: $\mathrm{colim}_I R_i = R_1 \otimes_{\mathbb{Z}} R_2$

Abelian Groups: $\mathrm{colim}_I R_i = R_1 \oplus R_2$

A.3 Adjoints

If $F : \mathcal{C} \to \mathcal{D}$ and $G : \mathcal{D} \to \mathcal{C}$ are functors, then we say that F is a *left adjoint* for G (equivalently: G is right adjoint for F) if there is natural isomorphism $\mathrm{Mor}_{\mathcal{C}}(-, G(-)) \cong \mathrm{Mor}_{\mathcal{D}}(F(-), -)$ of the bifunctors from $\mathcal{C}^o \times \mathcal{D}$ into **Sets**. This means that for every pair of objects A of $\mathcal{C}$ and B of $\mathcal{D}$ there is an isomorphism $\pi_{A,B} : \mathrm{Mor}_{\mathcal{C}}(A, G(B)) \cong \mathrm{Mor}_{\mathcal{D}}(F(A), B)$ such that for every morphism of objects $f : A \to A'$ in $\mathcal{C}$ and $g : B \to B'$ in $\mathcal{D}$, the diagram,

$$\begin{tikzcd}
\mathrm{Mor}_{\mathcal{C}}(A', G(B)) \arrow[r, "(f_*, G(g)^*)"] \arrow[d, shift right, "\pi_{A',B}"'] & \mathrm{Mor}_{\mathcal{C}}(A, G(B')) \arrow[d, shift right, "\pi_{A,B'}"'] \\
\mathrm{Mor}_{\mathcal{D}}(F(A'), B) \arrow[r, "(F(f)_*, g^*)"] \arrow[u, shift right] & \mathrm{Mor}_{\mathcal{D}}(F(A), B') \arrow[u, shift right]
\end{tikzcd}$$

commutes. We say that (F, G) is an *adjoint pair* of functors. Pairs of adjoint functors occur very frequently in mathematics.

Example A.3.1. (a) Let R be a ring and M any R-module. The functor $N \mapsto M \otimes_R N$ from the category of **R-mod** to itself is the left adjoint to the functor $N \mapsto \mathrm{Hom}_R(M, N)$.

(b) Let R be a commutative ring, and **R-Alg** be the category of commutative R-algebras. Let F : **R-Alg** → **Sets** be the forgetful functor that associates to each R-algebra its underlying set. Then the functor G : **Sets** → **R-Alg** that takes a set X to the polynomial ring $R[X]$ whose indeterminates are elements of X is a left adjoint of F.

(c) Let F : **Cat** → **Grph** be the forgetful functor from categories to directed graphs. Then the functor H : **Grph** → **Cat** which assigns each graph G, it's free category is a left adjoint of F.

Proposition A.3.2. *Suppose (F, G) is an adjoint pair. Then F preserves colimits and G preserves limits.*

Bibliography

[1] E. Abe. *Hopf Algebras.* Cambridge University Press, 1980.

[2] E.F. Assmus. The category of linear codes. *IEEE Trans. on Information Theory,* vol. 44,(2):pp. 612–629, March 1998.

[3] E.F. Assmus and H.F. Mattson. Error-correcting codes: An axiomatic approach. *Inform. Contr.*, vol. 6:pp. 315–330, 1963.

[4] M.F. Atiyah and I.G. Mac Donald. *Introduction to Commutative Algebra.* Perseus Books, 1969.

[5] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Springer-Verlag, 1995.

[6] David Eisenbud and Joe Harris. *The Geometry of Schemes.* Springer-Verlag, 2000.

[7] Robin Hartshorne. *Algebraic Geometry.* Springer-Verlag, 1997.

[8] Neal Kobltiz. *Algebraic Aspects of Cryptography.* Springer-Verlag, 1998.

[9] Saunders Mac Lane. *Categories for the Working Mathematician.* Springer-Verlag, 1998.

[10] Hideyuki Matsumura. *Commutative Ring Theory.* Cambridge University Press, 1997.

[11] David Mumford. *The Red Book of Varieties and Schemes.* Springer-Verlag, 1999.

[12] J.E. Roos. An algebraic study of group and nongroup error-correcting codes. *Inform. Contr.*, vol. 8:pp. 195–214, 1965.

[13] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[14] D. Slepian. Some further theory of group codes. *Bell Syst. Tech. J.*, vol. 39:pp. 1219–1252, 1960.

[15] T.A. Springer. *Linear Algebraic Groups.* Birkhauser, 1998.