ABSTRACT

A PRIMER FOR THE FOUNDATIONS OF ALGEBRAIC GEOMETRY

by

Earl F Hampton III

April, 2010

Chair: Dr. M.S. Ravi

Major Department: Mathematics

The purpose of this thesis is to define the basic objects of study in algebraic geometry, namely, schemes and quasicoherent sheaves over schemes. We start by discussing algebraic sets as common zeros of polynomials and prove Hilbert's Nullstellensatz to establish a correspondence between algebraic sets and ideals in a polynomial ring. We then discuss just enough category theory to define a sheaf as a contravariant functor and then introduce ringed spaces, the spectrum of a ring, and the definition of affine schemes. We then discuss sheaves of modules over schemes. We then define projective varieties as ringed spaces. We end by proving Hilbert's syzygy theorem that can be used to study the equations defining projective varieties.

A PRIMER FOR THE FOUNDATIONS OF ALGEBRAIC GEOMETRY

A Thesis

Presented to

The Faculty of the Department of Mathematics

East Carolina University

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts in Mathematics

by

Earl F Hampton III

April, 2010

A PRIMER FOR THE FOUNDATIONS OF ALGEBRAIC GEOMETRY

by

Earl F Hampton III

APPROVED BY:

DIRECTOR OF THESIS: ______________________
Dr. M.S. Ravi

COMMITTEE MEMBER: ______________________
Dr. Chal Benson

COMMITTEE MEMBER: ______________________
Dr. Salman Abdulali

COMMITTEE MEMBER: ______________________
Dr. Richard Ericson

CHAIR OF THE DEPARTMENT OF MATHEMATICS: ______________________
Dr. Tom McConnell

DEAN OF THE GRADUATE SCHOOL: ______________________
Dr. Paul Gemperline

ACKNOWLEDGEMENTS

First, thank you to my wife, Tracie, whose support encompasses far more than this thesis. I would also thank Dr M.S. Ravi for the many hours spent proof reading and explaining crucial ideas, often many more times than expected. Thanks to Doctors Benson, Ratcliff, and Spurr for putting up with the questions. You have each had an immeasurable impact on my education.

TABLE OF CONTENTS

CHAPTER 1: Introduction

In the fall of 2008, Dr Sastry and others began a series of seminars devoted to algebraic geometry, most of which revolved around the existence of Picard schemes. One of the first lectures was a long diagram chase of tensor products, the end result being that all the faces of a cube of morphisms were in fact Cartesian. I understood absolutely nothing about the objects being manipulated, but the tools used in the manipulation seemed almost intuitive. It is the quest to understand these objects that this thesis essentially documents, hopefully, modulo the blind alleys.

Though the objects from the seminars are beyond the scope of what is covered here, a major objective is to place the definition of schemes and quasicoherent sheaves over schemes on a firm foundation.

We start by defining algebraic sets as common solutions to polynomial equations in several variables. We prove Hilbert's Nullstellensatz and use it to establish a correspondence between ideals in polynomial rings and algebraic sets. Since several ideals can define the same algebraic set, we proceed to define affine schemes to keep track of the specific ideal that is used to define the algebraic set. We make this precise by defining sheaves on topological spaces and thinking of schemes as ringed spaces.

We also define projective varieties and prove the Hilbert syzygy theorem which can be used to study the ideals defining projective varieties.

CHAPTER 2: Affine Space

In this chapter most of the machinery used throughout the rest of the thesis will be introduced in an ambient space which is easy to visualize. The development of the correspondence between closed sets in a topology with prime ideals of a ring will lead quite naturally to the definitions of ringed spaces, sheaves, varieties and, in later chapters, schemes.

For most of us, the words affine space immediately bring to mind $\mathbb{R}^n$. However, for the topics at hand, $\mathbb{C}^n$ is a better space to imagine. The main reason being that $\mathbb{C}$ is algebraically closed and throughout this thesis unless otherwise stated all fields considered will be algebraically closed, and typically denoted as k. The polynomial ring of n variables over k will be denoted as $k[X_1, \ldots, X_n]$. Similarly k^n will be the vector space of dimension n over the field k. Furthermore, all rings will be assumed to be commutative with an identity element.

2.1 Affine Algebraic Sets

Let $f \in k[X_1, \ldots, X_n]$. Then the set $V(f) = \{x \in k^n : f(x) = 0\} \subset k^n$, is called the **zero locus** of f. Now if $g \in k[X_1, \ldots, X_n]$ then $fg \in k[X_1, \ldots, X_n]$ and $V(f) \subseteq V(fg)$, because fg has "more" zeroes. If $f(x) = 0$ then $(fg)(x) = 0$. Thus, if $\langle f \rangle$ is the ideal generated by f, we have $V(f) \subseteq V(\langle f \rangle)$. So it is quite natural to associate an ideal with a zero locus. However this correspondence is not well defined because $V(f) = V(f^2) = V(f^3) = \ldots$. If we consider the other direction, that is, pick an ideal, $I \subset k[X_1, \ldots, X_n]$ then what is $V(I)$? There are many polynomials in I and thus many choices. One might immediately jump to using the intersection of zero loci for all $f \in I$, but then the question arises, is this a finite intersection? What if it is empty? It is these questions that this section focuses on.

Definition 2.1. Let $S \subset k[X_1, \ldots, X_n]$ be a set of polynomials. An **affine algebraic set** is

$$V(S) = \{c \in k^n : \forall f \in S,\ f(c) = 0\}. \tag{2.1}$$

Note

$$S \subset S' \Longrightarrow V(S') \subseteq V(S),$$

so adding polynomials to the set may decrease the size of V. If S is a finite set and $f_1, \ldots, f_n$ are the polynomials in S then $\bigcap_i^n V(f_i) = V(S)$.

Proposition 2.2. *If an ideal $\mathfrak{s} \subset k[X_1, \ldots, X_n]$ is generated by S, then $V(S) = V(\mathfrak{s})$.*

Proof. $V(\mathfrak{s}) \subseteq V(S)$ follows from the observation above. Conversely by definition, the ideal

$$\mathfrak{s} = \left\{ \sum_{i \in I} f_i g_i :\ f_i \in S,\ g_i \in k[X_1, \ldots, X_n],\ I \text{ finite} \right\}.$$

As each f_i is 0 for all $x \in V(S)$, $V(S) \subseteq V(\mathfrak{s})$. □

Next we show that any ideal in the polynomial ring has a finite number of generators.

Proposition 2.3. *[6] The following conditions on a ring R are equivalent:*

1. *Every ideal $\mathfrak{a} \subset R$ is finitely generated.*
2. *Every ascending chain of ideals*

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$$

   terminates. That is for some n, $\mathfrak{a}_n = \mathfrak{a}_m$ for all $m \geq n$.

3. *Every nonempty set of ideals of R has a maximal element.*

Proof. (1) $\Rightarrow$ (2) We are given a sequence of ideals $\mathfrak{a}_1 \subset \cdots \subset \mathfrak{a}_m \subset \cdots$, and we assume that every ideal is finitely generated.

Let $I = \cup_i \mathfrak{a}_i$. We claim that I is an ideal. If $f, g \in I$, then there exists an i such that $f, g \in \mathfrak{a}_i$. Thus $f + g \in \mathfrak{a}_i \subset I$ since $\mathfrak{a}_i$ is an ideal . Also, if $f \in I$, then there is an i such that $f \in \mathfrak{a}_i$, so if $g \in R$, then $gf \in \mathfrak{a}_i \subset I$ since $\mathfrak{a}_i$ is an ideal of R. Now since we are assuming that every ideal in R is finitely generated, $I =< f_1, \ldots, f_l >$ and we can choose n such that $f_j \in \mathfrak{a}_n$ for $j = 1, \ldots, l$. Now for $m \geq n$, $\mathfrak{a}_m = \mathfrak{a}_n$.

(2) $\Rightarrow$ (3) Let $\{\mathfrak{a}_i \,|\, i \in I\}$ be a collection of ideals with no maximal element. Choose an ideal $\mathfrak{a}_1$ in this collection. As there is no maximal element in the collection, there exists an $\mathfrak{a}_2$ such that $\mathfrak{a}_1 \subset \mathfrak{a}_2$ and $\mathfrak{a}_1 \neq \mathfrak{a}_2$. We can repeat this process infinitely since the collection does not have a maximal element. Now the sequence $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots$ never terminates.

(3) $\Rightarrow$ (1) Let $\mathfrak{b}$ be an ideal and let $H = \{\mathfrak{a} \subset \mathfrak{b} : \mathfrak{a} \text{ is finitely generated}\}$. Now H has a maximal ideal by assumption, call it $\mathfrak{c}$. Now $\mathfrak{c}$ is finitely generated because it is in H.

Claim: $\mathfrak{c} = \mathfrak{b}$. Clearly $\mathfrak{c} \subset \mathfrak{b}$ and $\langle c_1, \ldots c_n\rangle = \mathfrak{c}$ because $\mathfrak{c}$ is finitely generated. Let $b \in \mathfrak{b} \setminus \mathfrak{c}$. But then $\langle c_1, \ldots, c_n, b\rangle \subset \mathfrak{b}$, moreover it is finitely generated, hence in H. But this contradicts the assumption that $\mathfrak{c}$ was maximal. □

Definition 2.4. A ring, R, is **noetherian** if one of the conditions of Proposition 2.3 holds.

The following is an example of a ring that is not noetherian.

Example 2.5. [9] Consider $k[x^r] = \{\sum ax^r : a \in k,\ r \in \mathbb{R},\ r > 0\}$. Multiplication and addition are defined as usual; thus $\langle x^b\rangle$ is an ideal for any fixed $b \in \mathbb{R}$. Now note

$$\langle x^b\rangle \subset \langle x^{b/2}\rangle \subset \langle x^{b/4}\rangle \subset \cdots \subset \langle x^{b/2^n}\rangle \subset \ldots$$

and so the chain never terminates.

So if a ring is noetherian then all its ideals are finitely generated. Now, if k is a field, then it only has two ideals, $\{0\} =< 0 >$ and $k =< 1 >$. So clearly any field, thought of as a ring, is noetherian. We now show that $k[X_1, \ldots, X_n]$ is noetherian.

Theorem 2.6 (Hilbert Basis Theorem)**.** *If R is a noetherian ring, then $R[x]$, the ring of polynomials with coefficients in R, is a noetherian ring.*

Proof. A polynomial, $f \in R[x]$, can be written as $\sum_{i=0}^{n} a_i x^i$ where $\deg(f) = n$, and f is said to have leading coefficient a_n. Let $\mathfrak{a} \subset R[x]$ be an ideal. We need to show that $\mathfrak{a}$ is finitely generated. To do so, inductively construct two related sequences of ideals, $\mathfrak{b}_i \subset R$ and $\mathfrak{b}_i^* \subset R[x]$. Choose f_0 to be a polynomial of least degree in $\mathfrak{a}$, and denote its leading coefficient by a_0. Define $\mathfrak{b}_0^* = \langle f_0 \rangle$ and $\mathfrak{b}_0 = \langle a_0 \rangle$. Inductively choose an $f_i \in \mathfrak{a} \setminus \mathfrak{b}_{i-1}$ of least degree, and let a_i be the leading coefficient of f_i. Define

$$\mathfrak{b}_i^* = \langle f_0, \cdots, f_i \rangle$$

and

$$\mathfrak{b}_i = \langle a_0, \cdots, a_i \rangle.$$

By construction, $\mathfrak{b}_i \subset \mathfrak{b}_{i+1}$ and $\mathfrak{b}_i^* \subset \mathfrak{b}_{i+1}^*$. Moreover each $\mathfrak{b}_i$ is an ideal in R, which by assumption is noetherian. Hence the chain of ideals $\mathfrak{b}_i$ is of finite length. So $\mathfrak{b}_i = \mathfrak{b}_n$ for $i \geq n$. Since $a_{n+1} \in \mathfrak{b}_n$ there are elements $b_i \in R$ such that $a_{n+1} = \sum_0^n a_i b_i$.

Let $g = \sum_0^n b_i f_i x^{d_i}$ where $d_i = \deg(f_{n+1}) - \deg(f_i)$ ensuring $g = a_{n+1} x^{\deg(g)}$ + lower order terms. Thus $\deg(g) = \deg(f_{n+1})$ and both g and f_{n+1} have the same leading coefficient. By construction $g \in \mathfrak{b}_n^*$ and $f_{n+1} \in \mathfrak{a} \setminus \mathfrak{b}_n^*$, so $f_{n+1} - g \in \mathfrak{a} \setminus \mathfrak{b}_n^*$. However $\deg(f_{n+1}) > \deg(f_{n+1} - g)$ contradicting our assumption that f_{n+1} was a polynomial in $\mathfrak{a} \setminus \mathfrak{b}_n^*$ of least degree. Hence $\mathfrak{a} \setminus \mathfrak{b}_n^* = \emptyset$ and $\mathfrak{a} = \langle f_0, \ldots, f_n \rangle$ is finitely generated. $\square$

Noting $k[X_1, \ldots, X_n] \cong k[X_1, \ldots, X_{n-1}][X_n]$, induction shows that $k[X_1, \ldots, X_n]$ is noetherian. We need to say one more thing about the noetherian conditions even though we will not use it now.

Proposition 2.7. *If R is a noetherian ring and $\mathfrak{a} \subset R$ is an ideal then $R/\mathfrak{a}$ is also noetherian.*

Proof. If $\overline{\mathfrak{b}} \subset R/\mathfrak{a}$ is an ideal, then by the correspondence theorem for ideals there is an ideal $\mathfrak{b} \subset R$ such that under the map $\phi : R \to R/\mathfrak{a}$, $\phi(\mathfrak{b}) = \overline{\mathfrak{b}}$. But then any ascending chain in $R/\mathfrak{a}$ pulls back to an ascending chain in R which terminates. □

Back in terms of establishing a correspondence between ideals and algebraic sets, if $V(S) = V(\mathfrak{s})$ and $\mathfrak{s} \subset k[X_1, \ldots, X_n]$, then $\mathfrak{s}$ has a finite number of generators; therefore, only a finite set S need be considered. At last, the work toward a well defined correspondence between irreducible algebraic sets and prime ideals can begin to be analyzed.

Theorem 2.8 (Hilbert's Weak Nullstellensatz)**.** *Let k be an algebraically closed field. Let $S = \{f_1, \ldots f_m\} \subset k[X_1, \ldots, X_n]$ be a set of polynomials in the ring of n indeterminates over k. Then either there exists a $c \in k^n$ such that $f_1(c) = \cdots = f_m(c) = 0$, or there exist polynomials $q_1, \cdots, q_m \in k[X_1, \ldots, X_n]$ such that $\sum_{i=1}^m f_i q_i = 1$.*

If there exists polynomials $q_1, \cdots, q_m \in k[X_1, \ldots, X_n]$ such that $\sum_{i=1}^m f_i q_i = 1$, then setting $\mathfrak{s} = \langle S \rangle$ gives $1 \in \mathfrak{s}$, therefore:

Corollary 2.9. *Let k be an algebraically closed field and $\mathfrak{a} \subset k[X_1, \cdots, X_n]$ an ideal such that $V(\mathfrak{a}) = \emptyset$. Then $\mathfrak{a} = k[X_1, \cdots, X_n]$.*

Proof. $V(\mathfrak{a}) = \emptyset \iff 1 \in \mathfrak{a} \iff \langle 1 \rangle = k[X_1, \ldots, X_n] = \mathfrak{a}$. □

The next lemma will be used to restrict to maximal ideals in the proof of the Nullstellensatz.

Lemma 2.10. *For a ring, R, every proper ideal, $\mathfrak{a}$, is contained in a maximal ideal, $\mathfrak{m}$.*

Proof. Let $\mathfrak{a} \subset R$ be a proper ideal. Then the set

$$S = \{\mathfrak{b} : \mathfrak{b} \text{ is a proper ideal in } R \text{ and } \mathfrak{a} \subset \mathfrak{b}\}$$

is partially ordered by inclusion. Also, if $\{\mathfrak{b}_i\}$ is an increasing chain of ideals in S then it has a maximal element in S, namely the ideal $\mathfrak{b} = \cup_i \mathfrak{b}_i$. The fact that $\mathfrak{b}$ is an ideal follows from the arguments used in the proof of Proposition 2.3. Hence by Zorn's lemma, the set $\mathfrak{m}$ has a maximal element. Now $\mathfrak{a} \subset \mathfrak{m}$ and it is easy to see that $\mathfrak{m}$ is a maximal ideal in R. □

Proposition 2.11. *Let L be a field and k an algebraically closed subfield of L. Then if $\alpha \in L$ is algebraic over k then $\alpha \in k$.*

Proof. The proof is really just a restatement of the definitions. As α is algebraic over k by assumption, there is an $f \in k[x]$ such that $f(\alpha) = 0$. Thus α is in the algebraic closure of k, but this is k. □

The next proposition is a fact needed while proving the lemma that follows.

Proposition 2.12. *If k is algebraically closed then k is infinite.*

Proof. Using the contrapositive, if k is finite then the polynomial $(\prod_{a \in k}(X-a))-1 \in k[X]$ has no roots in k, which shows that k is not algebraically closed. □

The following lemma is the key point in the proof.

Lemma 2.13. *Let k be an algebraically closed field and let $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$. Let L be a finitely generated field extension of k, and suppose that we have $\eta_1, \ldots, \eta_n \in$*

L such that $f_i(\eta_1, \ldots, \eta_n) = 0$ for $i = 1, \ldots, m$. Then there exist $c_j \in k$ for $j = 1, \ldots, n$, such that $f_i(c_1, \ldots, c_n) = 0$ for $i = 1, \ldots, m$.

Proof. [9]Let $(\alpha_1, \ldots, \alpha_r) = \alpha$ be those elements of L that are algebraically independent over k. We will use $k[X] = k[X_1, \ldots, X_n]$ with $k(X)$ to mean its fraction field. We use $k[\alpha]$ to mean the subset of L which is the image of the natural map from $k[X]$ to L that evaluates a polynomial at $\alpha_1, \ldots, \alpha_n$. Let $k(\alpha)$ be the fraction field of $k[\alpha]$ in L. Now L is algebraic over $k(\alpha)$. We can think of $k(\alpha)$ as a subfield of L and $k(\alpha)[Y] \subset L[Y]$. Hence if $\theta \in L$, there is an irreducible polynomial in $k(\alpha)[Y]$, which can be written as

$$P(\alpha, Y) = p_0(\alpha)Y^d + \cdots + p_d(\alpha) \in k(\alpha)[Y]$$

such that θ is a zero of P.

So assume $(\eta_1, \ldots, \eta_n) = \eta \in L^n$ is the solution to $f_i(\eta) = 0$ in the statement of our lemma for all i. We can replace L by $k(\alpha)(\eta_1, \ldots, \eta_n)$ and assume that L is a finite extension of $k(\alpha)$. Hence by the primitive element theorem, we can assume that $L = k(\alpha)[\theta]$ where θ is a primitive element in L. So $\eta_j = C_j(\alpha, \theta) \in k(\alpha)[\theta]$ for all j giving

$$0 = f_i(\eta) = f_i(C_1(\alpha, \theta), \ldots, C_r(\alpha, \theta)) = \hat{f}_i(\alpha, \theta)$$

and $P(\alpha, \theta) = 0$. Now $P(\alpha, \theta) = \hat{f}_i(\alpha, \theta) = 0$ for all i, so P and $\hat{f}_i$ share the root θ, as polynomials in $k(\alpha)[Y]$. But, $P(\alpha, Y)$ is irreducible, so $P(\alpha, Y)$ divides $f_i(\eta, Y)$. Thus for some Q_i,

$$f_i(C_1(\alpha, Y), \ldots, C_n(\alpha, Y)) = P(\alpha, Y)Q_i(\alpha, Y) \in k(\alpha)[Y].$$

Since k is an infinite field by Proposition 2.12, we can choose $\beta_j \in k$ and substitute

β_j for α_j such that for all i the polynomials $P, Q_i, C_i \in k(\alpha)[Y]$ has no denominator which is 0 and $p_0 \neq 0$. Thus each polynomial has been turned into a polynomial in $k[Y]$ which now has only a finite number of roots. Denote the new polynomials as $\hat{\hat{P}} = P(\beta, Y),\ \hat{\hat{Q}}_i = Q_i(\beta, Y),\ \hat{\hat{C}}_i = C_i(\beta, Y)$.

Effectively $\hat{\hat{P}}, \hat{\hat{Q}}_i, \hat{\hat{C}}_i$ are polynomials in $k[U]$. Finally, since k is algebraically closed we can choose $\tau \in k$ such that $\hat{\hat{P}}(\tau) = 0$. Let $\hat{\hat{C}}_j(\beta, \tau) = c_j \in k$. Hence

$$f_i(c_1, \ldots, c_n) = \hat{\hat{P}}(\tau)\hat{\hat{Q}}_i(\tau) = 0.$$

Thus the elements $c_j \in k$ are the elements that we were seeking in the statement of the lemma. □

Proof: Weak Nullstellensatz. Restating Theorem 2.8: Let k be an algebraically closed field. Let $S = \{f_1, \ldots f_m\} \subset k[X_1, \ldots, X_n]$. Then either there exists a $c \in k^n$ such that $f_1(c) = \cdots = f_m(c) = 0$, or there exist polynomials $q_1 \cdots q_m \in k[X_1, \ldots, X_n]$ such that $\sum_{i=1}^{m} f_i q_i = 1$.

If $\langle S \rangle = \mathfrak{s}$ is a proper ideal, then by Lemma 2.10 there exists a maximal ideal $\mathfrak{m} \supset \mathfrak{s}$, giving $V(\mathfrak{m}) \subset V(\mathfrak{s})$, and reducing the problem to one about the maximal ideal $\mathfrak{m}$.

Therefore, set $L = k[X_1, \ldots, X_n]/\mathfrak{m}$. L is a field since $\mathfrak{m}$ is a maximal ideal. Moreover, k can viewed as a subfield of L.

Claim: Each f_i has a solution in L^n.

Consider the projection $\phi : k[X_1, \ldots, X_n] \twoheadrightarrow L$ which takes $x_i \mapsto \alpha_i = x_i + \mathfrak{m}$. Then

$$\begin{aligned} f_j(\alpha_1, \ldots, \alpha_n) &= f_j(\phi(X_1), \ldots, \phi(X_n)) \\ &= \phi(f_j(X_1, \ldots, X_n)) \qquad \text{since } \phi \text{ is a homomorphism of rings,} \end{aligned}$$

$$= 0 \qquad \text{since } f_j \in \mathfrak{m}.$$

Thus there is a solution for all f_j in L^n.

Now by Lemma 2.13 we can find a common solution in k^n.

□

A more succinct way of stating the weak Nullstellensatz is the following:

Theorem 2.14. *Let k be an algebraically closed field. Then every maximal ideal in the polynomial ring $k[X_1, \cdots, X_n]$ has the form $\langle X_1 - c_1, \cdots, X_n - c_n \rangle$ for some $c_1, \cdots, c_n \in k$. Consequently a family of polynomials on k^n with no common zeros generates the unit ideal.*

Proof. Everything has been shown except the form of the polynomials that generate the ideal. If $\mathfrak{m}$ is a maximal ideal then since $V(\mathfrak{m}) \neq \emptyset$, there is a point $c = (c_1, \ldots c_n) \in V(\mathfrak{m})$.

As $\{c\} = V(\langle X_1 - c_1, \ldots, X_n - c_n \rangle)$, it follows that $\mathfrak{m} \subseteq \langle X_1 - c_1, \ldots, X_n - c_n \rangle$ and as $\mathfrak{m}$ is a maximal ideal, equality holds. □

So summing up what has already been shown:

1. $S \subset S' \Longrightarrow V(S') \subset V(S)$
2. $V(S) = V(\langle S \rangle)$
3. If $S \subset k[X_1, \ldots, X_n]$ then $\langle S \rangle$ is finitely generated.
4. If $c = (c_1, \ldots, c_n) \in k^n$ is a point then there is a maximal ideal generated by $S = \{X_1 - c_1, \ldots, X_n - c_n\}$. Moreover every maximal ideal is of this form.

2.1.1 Zariski Topology

Next up, we define a topology which gives a correspondence between ideals and closed sets. Along the way, some properties of this topology will be explored.

Definition 2.15. The **Zariski topology** is defined on k^n by taking the affine algebraic sets given in Definition 2.1, to be all the closed subsets.

Let $\mathfrak{T}$ be the set of all affine algebraic subsets of k^n. We need to show that $\mathfrak{T}$ satisfies the axioms for the closed sets in a topology.

1. $V(k[X_1, \ldots, X_n]) = \emptyset \in \mathfrak{T}$ and $V(\langle 0 \rangle) = k^n \in \mathfrak{T}$.

2. Let $V(\mathfrak{a})$ and $V(\mathfrak{b})$ be closed sets both in $\mathfrak{T}$. Then both the ideals are finitely generated, so let $\langle a_1, \ldots, a_n \rangle = \mathfrak{a}$ and $\langle b_1, \ldots, b_m \rangle = \mathfrak{b}$. We define IJ to be the ideal generated by $a_i b_j$ for $i = 1 \ldots, , n$ and $j = 1, \ldots, m$. Then

   $$V(IJ) = V(\mathfrak{a}) \cup V(\mathfrak{b}).$$

   Thus the union of two closed sets is also a closed set.

3. Lastly $\cap V(\mathfrak{a}_i) = V(\sum \mathfrak{a}_i)$, where $\sum \mathfrak{a}_i$ is the smallest ideal that contains all the ideals $\mathfrak{a}_i$. Hence the intersection of an arbitrary collection of closed sets is also a closed set.

So $\mathfrak{T}$ is a topology of closed subsets.

While talking about the topology, open sets should not be left out. Each open set is the complement of an algebraic set. That is an open set is of the form $U = k^n - V(I)$ where I is an ideal.

On the other hand when dealing with an affine algebraic set we consider the topology induced on this set. Let X be an affine algebraic set. Just as for k^n, the affine algebraic sets which are contained in X are the closed sets of X. Again the open sets in X are defined to be the complement of the closed sets.

Definition 2.16. Let X be an affine algebraic set. If $f \in k[X_1, \ldots, X_n]$, then $X_f = X - V(\langle f \rangle)$ is an open set in X and is said to be a **distinguished open set**.

Example 2.17. Let $f, g, h \in k[X_1, \ldots, X_n]$ and $f = gh$. Then $X = V(f) = V(gh) = V(g) \cup V(h) \subset k^n$ is an affine algebraic set and $X_g = X - V(g) = V(h)$. So X_g is a proper subset that is both open and closed in X.

Example 2.18. Let $f \in k[X_1, \ldots, X_n]$ and let $X = V(f) \subset k^n$. Now consider the open sets $X_{X_1}, \ldots, X_{X_n}$. Then $\bigcup_{i=1}^{n} X_{X_i} = X \setminus \{0\}$. These distinguished open sets of an algebraic set X will be used often in later sections.

This topology is not like $\mathbb{R}^n$ or $\mathbb{C}^n$ with the usual topology, since the Zariski topology does not have enough open sets.

Proposition 2.19. *The Zariski topology is* T_1.

Proof. Recall a space is T_1 if for any two points there is an open set that contains one of the points but not the other. Assume $a, b \in X \subset k^n$ are points with $a \neq b$. If $b = (b_1, \ldots, b_n)$ then we have already observed that $\{b\} = V(\langle X_1 - b_1, \ldots, X_n - b_n \rangle)$ is a closed set. Hence $U = X \setminus \{b\}$ is an open subset of X that contains a but not b. So the Zariski topology is T_1. $\square$

Recall a space is Hausdorff if about any two points there are open sets which are disjoint from each other. It is easy to see that the Zariski topology on k^n is not Hausdorff. The open sets here are too large.

2.1.2 Ideals of an Affine Algebraic Set

Definition 2.20. Let X be a subset of k^n. Then the ideal, $I(X)$, associated to X is

$$I(X) = \{f \in k[X_1, \ldots, X_n] : \forall x \in X,\ f(x) = 0\}.$$

It's easy to see this is an ideal since if $g \in k[X_1, \ldots, X_n]$ and $f \in I(X)$ then $(fg)(x) = 0$ for all $x \in X$, so $fg \in I(X)$. Similarly, if $f, g \in I(X)$ then for all $x \in X$, $(f+g)(x) = f(x) + g(x) = 0$. So $f + g \in I(X)$.

Theorem 2.21. *Let k be an algebraically closed field. If $g, f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ and*

$$g \in I(V(f_1 \ldots, f_m))$$

then there exists an $r \geq 1$ such that $g^r \in \langle f_1, \cdots, f_m \rangle$.

Proof. Using Rabinowitsch's trick, consider the ideal $\langle f_1, \ldots, f_m, 1-gt \rangle \subset k[X_1, \ldots, X_n, t]$.

Claim: $k[X_1, \ldots, X_n, t] = \langle f_1, \ldots, f_m, 1-gt \rangle$. If $c = (c_1, \ldots, c_n) \in k^n$ is a common zero of $f_1, \ldots, f_m$, then $g(c_1, \ldots, c_n) = 0$. Hence $(1-gt)(c_1, \ldots, c_n, x) = 1$ for any value of $x \in k$. Hence

$$V(\langle f_1, \ldots, f_m, 1-gt \rangle) = \emptyset. \tag{2.2}$$

Therefore, from Theorem 2.8, the weak Nullstellensatz, $1 \in \langle f_1, \ldots, f_m, 1-gt \rangle$ and so

$$1 = q(1-tg) + \sum_{i=1}^{m} p_i f_i \tag{2.3}$$

for some $p_i, q \in k[X_1, \ldots, X_n, t]$. Now set $t = 1/g$ giving

$$1 = q(1 - \frac{1}{g}g) + \sum_{i=1}^{m} p_i(x_1, \ldots, x_n, \frac{1}{g}) f_i. \tag{2.4}$$

Clearing denominators by multiplying by g^r for a sufficiently large value of r shows that $g^r \in \langle f_1, \ldots, f_m \rangle$.

□

The proof justifies the following definition.

Definition 2.22. Let $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ be an ideal. Then $\sqrt{\mathfrak{a}}$, the **radical ideal** of $\mathfrak{a}$ is defined as

$$\sqrt{\mathfrak{a}} = \{f \in k[X_1, \ldots, X_n] : f^r \in \mathfrak{a},\ r \in \mathbb{N}\}.$$

Proposition 2.23. *The radical of* $\mathfrak{a}$ *is an ideal.*

Proof. Let $a \in \sqrt{\mathfrak{a}}$. Then clearly for any $f \in k[X_1, \ldots, X_n]$, $af \in \sqrt{\mathfrak{a}}$. So let $a, b \in \sqrt{\mathfrak{a}}$. Then $a^r \in \mathfrak{a}$ and $b^s \in \mathfrak{a}$. Then each term in the binomial expansion $(a+b)^{r+s}$ has a factor of a^r or b^s, and so $(a+b)^{r+s} \in \mathfrak{a}$ and $a + b \in \sqrt{\mathfrak{a}}$. □

Armed with this new definition, Theorem 2.21 can be restated.

Theorem 2.24 (Nullstellensatz)**.** *[3] For any ideal* $\mathfrak{a} \subset k[X_1, \cdots, X_n]$*, the ideal of functions vanishing on the common zero locus of* $\mathfrak{a}$ *is the radical of* $\mathfrak{a}$*, denoted as* $\sqrt{\mathfrak{a}}$*. In symbols*

$$I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}. \tag{2.5}$$

Proposition 2.25. $\sqrt{\mathfrak{a}} = \sqrt{\sqrt{\mathfrak{a}}}$

Proof. [7] If $a \in \sqrt{\sqrt{\mathfrak{a}}}$ then $a^r \in \sqrt{\mathfrak{a}} \Rightarrow a^{rs} = (a^r)^s \in \mathfrak{a}$, for some s. Hence $a \in \sqrt{\mathfrak{a}}$. □

In view of this, we say that an ideal $\mathfrak{a}$ is a radical ideal, if $\sqrt{\mathfrak{a}} = \mathfrak{a}$.

Proposition 2.26. *If an ideal* $\mathfrak{p}$ *is prime then* $\mathfrak{p} = \sqrt{\mathfrak{p}}$*. In other words, every prime ideal is radical.*

Proof. Assume $\mathfrak{p}$ is prime. Since $\mathfrak{p}$ is prime, if $fg \in \mathfrak{p}$ then $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$. Suppose n is the smallest power such that $f^n \in \mathfrak{p}$, and $n > 1$. Then $f \in \mathfrak{p}$ or $f^{n-1} \in \mathfrak{p}$. So $f \in \mathfrak{p}$ and $\mathfrak{p} = \sqrt{\mathfrak{p}}$. □

Corollary 2.27. *Maximal ideals are radical ideals.*

Proof. Maximal ideals are prime and prime ideals are radical. □

Proposition 2.28. *If $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are ideals then $\sqrt{\mathfrak{a}_1} \cap \sqrt{\mathfrak{a}_2}$ is radical.*

Proof. If $f^r \in \sqrt{\mathfrak{a}_1} \cap \sqrt{\mathfrak{a}_2}$, then $f^r \in \sqrt{\mathfrak{a}_\mathfrak{i}}$.

So $f \in \sqrt{\mathfrak{a}_i}$ and $f \in \sqrt{\mathfrak{a}_1} \cap \sqrt{\mathfrak{a}_2}$. □

Proposition 2.29. *The radical of an ideal in $k[X_1, \ldots, X_n]$ is equal to the intersection of the prime ideals containing it.*

The proof will be given after localization has been introduced in Claim 2.72.

Proposition 2.30. *[7] If $W \subset k^n$, then $V(I(W))$ is the smallest algebraic subset of k^n containing W. In particular, if W is an affine algebraic set, then $V(I(W)) = W$.*

Proof. Let $W \subset V$ where V is an algebraic subset of k^n. So $V = V(\mathfrak{a})$ for some ideal $\mathfrak{a}$, moreover $\mathfrak{a} \subset I(W)$, so $V(I(W)) \subset V(\mathfrak{a})$. □

To summarize, let $S = \{f_i\} \subset k[X_1, \ldots, X_n]$. Then the ideal generated by the elements of S, $\mathfrak{s} = \langle S \rangle = \langle f_1, \ldots, f_n \rangle$, is finitely generated and the following conditions hold:

1. $V(S) = V(\mathfrak{s}) = V(f_1, \ldots, f_n)$;

2. $\mathfrak{s} \subseteq I(V(S)) = \sqrt{\mathfrak{s}}$;

3. $I(\emptyset) = k[X_1, \ldots, X_n]$;

4. $I(k^n) = 0$, the zero ideal;

5. $\mathfrak{a} \subset \mathfrak{b} \Rightarrow V(\mathfrak{b}) \subset V(\mathfrak{a}) \Rightarrow I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{b}} = I(V(\mathfrak{b}))$;

6. $I(\cup V_i) = \cap I(V_i)$.

Using the new information about ideals associated to sets, we will prove a few properties of the Zariski topology.

Proposition 2.31. *[4] Let U be any subset of an affine algebraic set X. Then*

$$V(I(U)) = \overline{U},$$

where $\overline{U}$ is the closure of U in X.

Proof. By the definition of closure $U \subset \overline{U}$, and clearly $U \subset V(I(U))$. As $V(I(U))$ is a closed set, this yields $\overline{U} \subset V(I(U))$.

Now to show $V(I(U)) \subset \overline{U}$ it suffices to check that $V(I(U)) \subset C$ for all closed sets $C \subset k^n$. Since C is an affine algebraic set it can be written as $V(S)$ for some collection of polynomials $S \subset k[X_1, \ldots, X_n]$. Moreover, $S \subset I(U)$ because for any $f \in S$ we have $f|_C = 0 \Rightarrow f|_U = 0$ giving $f \in I(U)$. Then from the summary 5 above, $V(I(U)) \subset V(S) = C$ as desired.

$\square$

Proposition 2.32. *If X is an affine algebraic set then the distinguished open sets, X_f, from Definition 2.16 are a basis for the Zariski topology on X.*

Proof. So we need to show three things:

1. The distinguished open sets cover X which follows from Example 2.18.

2. The distinguished open sets are dense in X which follows from the closure Proposition 2.31.

3. That for any distinguished open sets V_f, V_g and for any $x \in V_f \cap V_g$ there exists an open V_h such that $x \in V_h \subset V_f \cap V_g$. But just set $h = fg$. Thus the sets are a basis for the Zariski topology.

Lastly to see that the topology created is the Zariski topology note that $\overline{V_f} = V$. □

So we have shown that the distinguished open sets form a basis for the Zariski topology.

Proposition 2.33. *Every open covering of X, an algebraic subset of k^n, has a finite sub-cover.*

In some of the literature this condition is called quasi-compact rather than compact because the space is not Hausdorff.

Proof. Now if for any open cover of k^n we can find a finite subcover of k^n, then a finite subcover can be found for any algebraic subset of k^n. So let $\{A_i\}$ be an open cover of k^n, and consider the collection of closed subsets $V_i = k^n \setminus A_i$. As V_i is a closed set, associate the ideal $I(V_i) \subset k[X_1, \ldots, X_n]$ to V_i.

Choose the first $I(V_i)$ arbitrarily and check if $I(V_1) = k[X_1, \ldots, X_n]$. If not choose another such that $I(V_2)$ that is not contained in $I(V_1)$. Then

$$I(V_1) \subset \sum_{i=1}^{2} I(V_i) \text{ and } I(V_1) \neq \sum_{i=1}^{2} I(V_i).$$

After selecting n such ideals we have

$$I(V_1) \subset \sum_{i=1}^{2} I(V_i) \subset \cdots \subset \sum_{i=1}^{n} I(V_i)$$

but the ring is noetherian so from Proposition 2.3 this chain of ideals terminates. If it terminates at n, then $\sum_1^n I(V_i) = k[X_1, \dots, X_n]$ and

$$V(\sum_{i=1}^{n} I(V_i)) = \bigcap_{i=1}^{n} V(I(V_i)) = \emptyset,$$

from the proof of Definition 2.15. Therefore, $\bigcup_{i=1}^{n} A_i = k^n$. □

If a topology is Hausdorff then for two distinct points there exist open neighborhoods of the two points which do not intersect. In the Zariski topology if W, Z are open sets of an algebraic set V, and $W \cap Z = \emptyset$ then $W^c \cup Z^c = V$ like Example 2.17. So it is only in very special circumstances that points can be found which have open sets which are disjoint. Again, the Zariski topology is not Hausdorff.

Definition 2.34. A ring R is **reduced** if the only nilpotent element is zero, that is $r^n = 0 \in R$ implies that $r = 0$.

Proposition 2.35. *An ideal $\mathfrak{a} \subset R$ is radical if and only if the quotient ring $R/\mathfrak{a}$ is reduced.*

Proof. Let $\phi : R \to R/\mathfrak{a}$ be the quotient map. First assume $\mathfrak{a} = \sqrt{\mathfrak{a}}$ and $\overline{f} \in R/\mathfrak{a}$. Then $\phi^{-1}(\overline{f}) = f + \mathfrak{a} \in R$. If $\overline{f}$ is nilpotent, then $f^n \in \mathfrak{a}$ and since $\mathfrak{a}$ is a radical ideal, $f \in \mathfrak{a}$, and $\overline{f} = 0 \in R/\mathfrak{a}$. So $R/\mathfrak{a}$ is reduced.

Now assume $\mathfrak{a}$ is not radical then there is an $f^n \in \mathfrak{a}$ with $f \notin \mathfrak{a}$. So $\overline{f}^n = 0 \in R/\mathfrak{a}$ but $\overline{f} \neq 0 \in R/\mathfrak{a}$. Thus $R/\mathfrak{a}$ is not a reduced ring.

□

At last the correspondence between algebraic sets and radical ideals can be formalized.

Proposition 2.36. *The map* $\mathfrak{a} \mapsto V(\mathfrak{a})$ *defines a one-to-one correspondence between the set of radical ideals in* $k[X_1, \ldots, X_n]$ *and the set of algebraic subsets of* k^n *and its inverse is* I.

Proof. $I(V(\sqrt{\mathfrak{a}})) = \sqrt{\mathfrak{a}}$ follows from Proposition 2.25 and $V(I(W)) = W$ follows from Proposition 2.30. □

So the bijection gives a correspondence between algebraic sets and radical ideals and between maximal ideals and points. In the next section a correspondence between prime ideal and irreducible algebraic sets will be shown.

2.1.3 Irreducible Sets

Definition 2.37. Let X be a non-empty topological space. We say X is **irreducible** if any of the following equivalent conditions hold:

1. X cannot be written in the form $X = F \cup G$ where F and G are closed and $X \neq F, G$.

2. If U, V are two open sets of X and $U \cap V = \emptyset$, then $U = \emptyset$ or $V = \emptyset$.

3. Any non-empty open set of X is dense in X.

Now the first two conditions are just set theoretic negations of each other, but the last should be examined more closely. So, let $A \subset X$ be open. If A is dense in X, then for every open neighborhood, $B(x)$, of a point x, $A \cap B(x) \neq \emptyset$. So assume A is not dense in X. Then there exists an $x \in X$ with an open neighborhood $B(x)$ such that $A \cap B(x) = \emptyset$. A is non-empty by assumption and $x \in B(x) \neq \emptyset$ so (2) is false. Conversely if (2) is true then for any B(x) which is non-empty $A \cap B(x) \neq \emptyset$.

Theorem 2.38. *[8] If W is an affine algebraic set equipped with the Zariski topology, then*

$$W \text{ irreducible} \iff I(W) \text{ prime} \iff k[X_1, \ldots, X_n]/I(W) \text{ is an integral domain.} \tag{2.6}$$

Proof. The last equivalence follows from the isomorphism theorems.

Assume W is reducible. Then there is an $F \cup G = W$ where F and G are closed sets with $F, G \neq W$. Now $F \subset W$ so $I(W) \subset I(F)$, and the same for $I(W) \subset I(G)$. Since $F, G \neq W$, we know that $I(F), I(G) \neq I(W)$. So we can choose $f \in I(F)$ and a $g \in I(G)$ such that $f, g \notin I(W)$. Now $F \subset V(f)$ and $G \subset V(g)$. If $x \in F \cup G$ then either $f(x) = 0$, or $g(x) = 0$. In either case $(fg)(x) = 0$. Thus $fg \in I(F \cup G) = I(W)$. So $f, g \notin I(W)$ but $fg \in I(W)$. Hence $I(W)$ is not a prime ideal.

Conversely assume $I(W)$ is not prime. Then there are $fg \in I(W)$ with $f, g \notin I(W)$. Moreover, $V(f) \neq W$ and $V(g) \neq W$. Therefore, $W \subseteq V(f) \cup V(g)$, but we need equality. So set $F = V(f) \cap W$ and $G = V(g) \cap W$ then $F \cup G = W$.

□

Proposition 2.39. *Let X be a non-empty affine algebraic set. Then $X = \bigcup_{i=1}^{r} V_i$, where each V_i is irreducible, and this decomposition is unique up to permutation.*

Proof of Existence: Assume X is non-empty algebraic set. If X is irreducible then the decomposition is complete, so assume X is reducible. Thus $X = V_1 \cup V_2$ and $V_1, V_2 \subsetneq X$, and so $V_i \nsubseteq V_j$. Similarly if V_1 is reducible, then $V_1 = V_{11} \cup V_{12}$ with the same properties as before. After some finite number of steps a tree is produced like figure 2.1 with all the leaf elements irreducible. We know this is finite because every branch must be of finite length as the ideal, $I(V)$ is noetherian. In the picture for

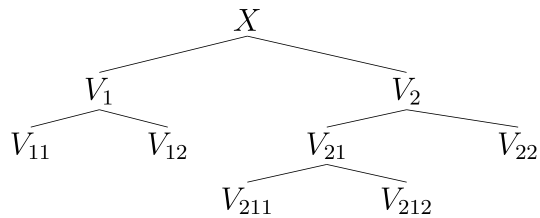


Figure 2.1: Example decomposition of an algebraic set

example

$$V_{212} \subset V_{21} \subset V_2 \subset V \Longleftrightarrow I(V) \subset I(V_2) \subset I(V_{21}) \subset I(V_{212}),$$

which is an ascending chain and so must terminate. Now it may be that some of the leaves are the same but there are only finitely many so we can compare them. Then the union of the distinct leaves is a union of irreducible subsets.

Uniqueness: Assume $X = \cup_i^n V_i = \cup_j^m W_j$ are two decompositions. Therefore $V_i = \bigcup_j (V_i \cap W_j)$, but as V_i is irreducible $V_i = V_i \cap W_j$ for a particular j. After doing the same for each V_i, we see that $m = n$ and V_i is a reordering of W_j. □

In summary, the following correspondences have been shown.

$$\text{radical ideals} \longleftrightarrow \text{Aalgebraic sets} \tag{2.7}$$

$$\text{prime ideals} \longleftrightarrow \text{irreducible closed sets} \tag{2.8}$$

$$\text{maximal ideals} \longleftrightarrow \text{single point sets} \tag{2.9}$$

The following definition will allow the correspondences to be taken even further.

Definition 2.40. Let X be an algebraic set in k^n and let $I = I(X)$. We define the coordinate ring of X in k^n to be the ring $k[X_1, \ldots, X_n]/I$.

Now the correspondence is extended:

$$\text{radical ideals} \longleftrightarrow \text{Algebraic sets} \longleftrightarrow \text{reduced rings} \tag{2.10}$$

$$\text{prime ideals} \longleftrightarrow \text{irreducible closed sets} \longleftrightarrow \text{integral domains} \tag{2.11}$$

$$\text{maximal ideals} \longleftrightarrow \text{single point sets} \longleftrightarrow \text{fields.} \tag{2.12}$$

2.1.4 Affine Dimension

From linear algebra k^n has dimension n as a vector space. But long before that we each began to develop an intuitive definition of dimension. As far back as elementary school geometric concepts of the point, line, plane, and solid were coupled to measures: counting, foot, acre, gallon. In algebraic geometry a different definition of dimension will be used. For the most part it will match the intuition developed in linear algebra and before.

Let X be an irreducible affine algebraic set. Then $I(X)$ is a prime ideal and

$$R[X] = \frac{k[X_1, \ldots, X_n]}{I(X)}$$

is an integral domain. Hence we can consider the fraction field of $R[X]$, denoted by $R(X)$, which consists of equivalence classes of fractions with the equivalence relation $\frac{s'}{t'} = \frac{s}{t} \in R(X) \Leftrightarrow s't = st' \in R[X]$.

Definition 2.41. The dimension of an irreducible affine algebraic set X, is defined as the transcendence degree of $R(X)$, over the field k, and will be denoted as $\operatorname{tr.dim}_k R(X)$.

So let us check our intuition on a few examples.

Example 2.42. Let $X = k^n$ then $R(X) \cong k(X_1, \ldots, X_n)$ giving $\operatorname{tr.dim}_R(X) = n$.

We now consider the other extreme.

Example 2.43. Let $X = p$ be a point in k^n. Then $I(X)$ is a maximal ideal and from Theorem 2.14 has the form $\langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Therefore $R[X] \cong k \cong R(X)$ and the transcendence degree of k over itself is zero.

Definition 2.44. The dimension of an affine algebraic set X, is the largest dimension of an irreducible subset, $W \subset X$.

Definition 2.45. The zero locus of a single non-constant polynomial in $k[X_1, \ldots, X_n]$ is a **hypersurface** in k^n.

Example 2.46. Let $f(X_1, \ldots, X_n) = X_n - a$ where $a \in k$. Then

$$k[X_1, \ldots, X_n]/\langle X_n - a \rangle \cong k[X_1, \ldots, X_{n-1}].$$

So $X_1, \ldots, X_{n-1}$ are algebraically independent over k giving $\operatorname{tr.dim}_k R(V(f)) = n-1$. Now note that $V(f) = \{(a_1, \ldots, a_{n-1}, a) \in k^n : a_1, \ldots, a_{n-1} \in k\} \cong k^{n-1}$.

Proposition 2.47. *A hypersurface of k^n, is of dimension $n-1$.*

Proof. We will prove the assertion assuming that f is an irreducible polynomial, since this will imply that all the irreducible components of the hypersurface have dimension $n-1$. Since f is a non-constant polynomial it must have terms of degree greater than zero. We can assume without loss of generality that the degree of f in X_n is at least one. Let $R[X] = k[X_1, \ldots, X_n]/\langle f \rangle$, and $\phi : k[X_1, \ldots, X_n] \to R[X]$ be the projection which maps $X_i \to \overline{X}_i$ for each i. Now we may write $f = \sum_{i=0}^{d} a_i X_n^i$ where $a_i \in k[X_1, \ldots, X_{n-1}]$. Then $\phi(f) = \sum_{i=0}^{d} a_i(\overline{X}_1, \ldots, \overline{X}_{n-1})\overline{X}_n^{\,i} = 0 \in R(X)$, showing $\overline{X}_n$ is algebraic over $k(\overline{X}_1, \ldots, \overline{X}_{n-1}) \in R(X)$. Thus $\operatorname{tr.dim}_k(R(X)) \leq n-1$.

Now we need to show that $\overline{X}_1, \ldots, \overline{X}_{n-1}$ are not algebraic over $R(X)$. Suppose there exists a $g \in k[X_1, \ldots, X_{n-1}]$ such that $g(\overline{X}_1, \ldots, \overline{X}_{n-1}) = 0 \in R(X)$. Then

$g \in \langle f \rangle \subset I(V(f))$. So $g = fh$ where $h \in k[X_1, \ldots, X_n]$. Now the degree of X_n in f is greater than 0. But the degree in X_n of g is 0. This contradicts the asumption that $f = hg$. Therefore such a polynomial g does not exist and $\operatorname{tr.dim}_k(R(X)) = n-1$. $\square$

Example 2.48. Let $a = (a_1, \ldots, a_n) \in k^n$ then the $I(\{a\}) = \langle X_1 - a_1, \ldots, X_n - a_n \rangle = \mathfrak{m}_a$, and

$$k[X_1, \ldots, X_n]/\mathfrak{m}_a = k \Rightarrow \operatorname{tr.dim}_k(k) = 0.$$

Moreover,

$$k[X_1, \ldots, X_n]/\langle X_i - a_i \rangle \cong k[X_1, \ldots, X_{n-1}]$$

for each i and $\operatorname{tr.dim}_k(R(V(X_i - a_i))) = n - 1$. So we have

$$a = V(\mathfrak{m}_a) = \bigcap_i V(X_i - a_i),$$

the intersection of n hypersurfaces all of dimension $n - 1$.

Once again our old linear algebra expectations are met. So the correspondence from affine algebraic sets and ideals of polynomial rings is more than just a curiosity. It carries with it the data related to dimension. Clearly the transcendence degree of a ring is an algebraic construct and dimension is a geometric one. Our correspondence links them together allowing problems to be solved in either setting.

2.2 Sheaves

In the previous section the correspondence between ideals and algebraic sets was established. Now we will generalize the correspondence and while doing so discover other data embedded in the structure.

We start by giving some basic definitions from category theory with several examples.

2.2.1 Categories

Definition 2.49. A **category**, $\mathscr{C}$, consists of the following entities:

1. A class of elements called objects, denoted $\text{obj}(\mathscr{C})$.

2. A class $\text{hom}(\mathscr{C})$ whose elements are morphisms (arrows). Each morphism has a unique source and target. If $A, B \in \text{obj}(\mathscr{C})$ then $\text{hom}(A, B)$ is the collection of all arrows with A as the source and B as the target.

3. Morphisms satisfy the following conditions:

   (a) If $A, B, C, D \in \text{obj}(\mathscr{C})$ and $f \in \text{hom}(A, B)$, $g \in \text{hom}(B, C)$, $h \in \text{hom}(C, D)$, then $f \circ g \in \text{hom}(A, C)$, $g \circ h \in \text{hom}(B, D)$, and $(f \circ g) \circ h = f \circ (g \circ h) \in \text{hom}(A, D)$.

   (b) Identity: For every object, $A \in \text{obj}(\mathscr{C})$, there exists a morphism

   $$1_A : A \to A$$

   so that for every morphism $f : A \to B$

   $$1_B \circ f = f = f \circ 1_A.$$

Examples 2.50. 1. Set is a category with objects as sets and functions as the morphisms.

2. Top is a category with topological spaces as objects and morphisms are continuous functions.

3. Grp is a category with groups as objects and morphisms are homomorphisms of groups.

4. Ring is a category with objects of rings where morphisms are homomorphisms of rings.

5. For a ring R, R-modules is a category with objects of R-modules where morphisms are R-linear functions.

6. Given a partially ordered set X, we can form the category $Poset\, X$ as follows: Each element of X is an object of $Poset\, X$, and there is exactly one arrow from x to y, if and only if $x \leq y$. The transitivity of the relation ensures that composition of morphisms is defined, and the reflexivity of the relation implies that every object has an identity morphism. So $Poset\, X$ is a category.

Taking a moment to review the definition from a slightly different perspective. A category consists of two collections, objects and morphisms (arrows). Each morphism is assigned a pair of objects: source (domain), target (codomain). For any two morphisms $f : A \to B,\ g : B \to C$ there exists a morphism $g \circ f : A \to C$. For every object there exists a morphism with both source and target the same and called the identity morphism. Then for the axioms:

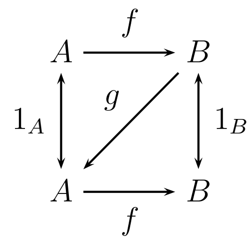
1. for $f : A \to B \Rightarrow f \circ 1_A = 1_B \circ f = f$;

2. for $f : A \to B,\ g : B \to C,\ h : C \to D$
   $\Rightarrow h \circ (g \circ f) = (h \circ g) \circ f$.

The key is that the morphisms preserve the structure of the objects. By speaking of the category the perspective has shifted. No longer is the concern tied to the properties of the objects, instead the view is of how the objects react to morphisms. The next definition is an example of the change in perspective.

Definition 2.51. An arrow $f : A \to B$ in a category is an isomorphism if it has an inverse, an arrow $g : B \to A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$.

The same concept is expressed by saying the following diagram commutes:



(2.13)

Next there are some other arrows (morphisms) that need to be defined. Most would have been seen before but the definitions are now in terms of other morphisms.

Definition 2.52. Let $\mathscr{C}$ be a category with objects A, B, C and arrows f, g, h.

1. Monomorphism: f is a monomorphism if $f : A \to B$ and for any pair $g, h : C \to A$, for any object C, then

$$f \circ g = f \circ h \Rightarrow g = h.$$

2. Epimorphism: f is an epimorphism if $f : A \to B$ and for any pair $g, h : B \to C$, for any object C, then

$$g \circ f = h \circ f \Rightarrow g = h.$$

3. An endomorphism is a morphism with both source and target the same object.

4. An automorphism is an endomorphism that is also an isomorphism.

A **subcategory** is a category that has objects and morphisms which are subcollections of another category's morphisms and objects. The next few examples are subcategories.

Examples 2.53. 1. *ABGrp* is a category with abelian groups as objects and morphisms are group homomorphisms. *ABGrp* is a subcategory of *Grp*.

2. Another subcategory of Grp is free groups, $FGrp$. Much like $ABGrp$ the objects are the free groups in Grp and morphisms from Grp which were between free groups are in $FGrps$.

3. Define $TopC$ as a sub category of Top by only allowing objects which are connected and morphisms the morphisms from Top with domain and codomain connected.

4. Similarly commutative rings, Cring, is a subcategory of ring.

5. As a variation on Top, fix a topological space X. Define the category $OpTop_X$ by letting the objects be the collection of open subsets of X. Let the morphisms be continuous functions. $OpTop_X$ is a subcategory of Top because for any $U \subset X$, U is a topological space and so $U \in \text{obj}(OpTop_X)$.

Example 2.54. Let X be a topological space. Define $ITop_X$ as a subcategory of $OpTop_X$ by setting $\text{obj}(OpTop_X) = \text{obj}(ITop_X)$. For morphisms, $f \in \text{hom}(ITop_X)$ if and only if $f \in \text{hom}(OpTop_X)$ and f is an inclusion map. The identity map is an inclusion so $1 \in \text{hom}(ITop_X)$. Therefore, $ITop_X$ is a category. It has all open sets of X as objects and all arrows are inclusions.

Example 2.55.

We say for a category, $\mathscr{C}$ the **opposite category**, $\mathscr{C}^{op}$, has the same objects but all arrows are reversed. For monomorphism and epimorphism this gives exactly what is expected. That is for $f : A \to B$ a monomorphism in $\mathscr{C}$, then $f : B \to A$ is an epimorphism in $\mathscr{C}^{op}$. Thus the statement, epimorphism is **dual** to monomorphism.

Before moving on, here is an example, that gives a bit of a flavor of category theoretic arguments and shows how passing to the opposite category may or may not be helpful.

Example 2.56. Claim: If $g \circ f$ is a monomorphism then f is monomorphism.

Proof. As $g \circ f$ is a monomorphism in $\mathscr{C}$, then $f \circ g$ is an epimorphism in $\mathscr{C}^{op}$. Therefore, for any h, k with domain=codomain(f), it needs to be shown that if

$$h \circ f = k \circ f \to h = k.$$

So assume h, k have domains=codomain(f). Then

$$\begin{aligned}
&h \circ f = k \circ f \\
&\quad \Rightarrow (h \circ f) \circ g = (k \circ f) \circ g \\
&\quad \Rightarrow h \circ (f \circ g) = k \circ (f \circ g) && \text{associative} \\
&\quad \Rightarrow h = k && f \circ g \text{ is epimorphism in } \mathscr{C}^{op} \\
&\quad \Rightarrow f \text{ epimorphism in } \mathscr{C}^{op} \\
&\quad \Rightarrow f \text{monomorphism in } \mathscr{C}.
\end{aligned}$$

□

Proof. Now without passing to $\mathscr{C}^{op}$. So assume h, k have codomains=domain(f). Then

$$\begin{aligned}
&f \circ h = f \circ k \\
&\quad \Rightarrow g \circ (f \circ h) = g \circ (f \circ k) \\
&\quad \Rightarrow (g \circ f) \circ h = (g \circ f) \circ k && \text{associative} \\
&\quad \Rightarrow h = k && g \circ f \text{ monomorphism in } \mathscr{C} \\
&\quad \Rightarrow f \text{ is a monomorphism.}
\end{aligned}$$

□

Next there is another type of map that needs some discussion. It is between categories.

Definition 2.57. Let $\mathscr{A}, \mathscr{B}$ be categories. A **Covariant functor**, F from $\mathscr{A}$ to $\mathscr{B}$ is a mapping which

1. associates to each object $X \in \mathscr{A}$ an object $F(X) \in \mathscr{B}$,
2. associates to each morphism $f : X \to Y \in \mathscr{A}$ a morphism $F(f) : F(X) \to F(Y) \in \mathscr{B}$.
3. $F(id_X) = id_{F(X)}, \forall X \in \mathscr{A}$,
4. $F(g \circ f) = F(g) \circ F(f)$ for all morphisms $f : X \to Y$ and $g : Y \to Z$.

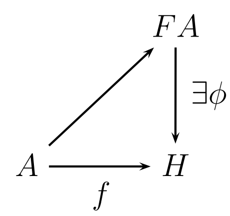
A functor can be thought of as a homomorphism of categories. In particular commutative diagrams are preserved and hence isomorphisms. For every category, $\mathscr{C}$, there is an identity functor, $1 : \mathscr{C} \to \mathscr{C}$, and there is composition of functors. That is if $F : \mathscr{A} \to \mathscr{B}$ and $G : \mathscr{B} \to \mathscr{C}$, then $(G \circ F)(X) = G(F(X))$ and $(G \circ F)(f) = G(F(f))$.

Example 2.58. Define a category, Cat, where objects are all small categories, and arrows are the functors between small categories. Composition is defined for functors so it is defined for hom(Cat). There exists an identity functor for any category so there are identity morphisms for each object in Cat. Thus a new category has been defined.

Now for a few examples of functors.

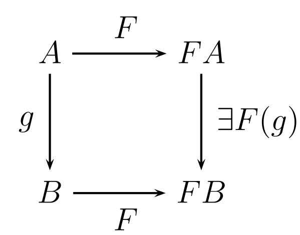
Examples 2.59.

1. For any set A, let FA denote the free group generated by A. Now from the definition of free groups given a function from a set A, $f : A \to H$, to a group H



(2.14)

there exists $\phi : F(A) \to H$. So let $B \in \text{obj}\, set$ and $g \in \hom(A, B)$ then $FA, FB \in \text{obj}\, FGrp$.



(2.15)

So F is a covariant functor from Set to Free Group.

2. Let X be a topological space. Let $\mathfrak{T}$ be the set of all open subsets of X. We can define a partial order on $\mathfrak{T}$, by $U_1 \leq U_2$, if and only if, $U_1 \subset U_2$. Then the map $r : Poset\, \mathfrak{T} \to ITop_X$ defined by $r(U) = U \in ITop_X$ is a functor between these two categories.

3. Given two categories $\mathscr{C}, \mathscr{D}$ define the product category $\mathscr{C} \times \mathscr{D}$ with objects of type $(C_0, D_0) \in \mathscr{C} \times \mathscr{D}$, and arrows $(f, g) : (C, D) \to (C', D')$ such that $f : C \to C' \in \mathscr{C}$ and $g : D \to D' \in \mathscr{D}$. Then $\pi_0 : \mathscr{C} \times \mathscr{D} \to \mathscr{C}$ and $\pi_1 : \mathscr{C} \times \mathscr{D} \to \mathscr{D}$ are functors.

4. Consider the categories Grp and AbGrp (abelian group). Let $G, K \in \text{obj}(Grp)$ and $f : G \to K \in \hom(G, K)$. Define $F(G) = G/[G, G]$ and $F(K) = K/[K, K]$,

then the following diagram commutes.

$$
\begin{array}{ccc}
G & \xrightarrow{F} & F(G) \\
{\scriptstyle f}\downarrow & \searrow^{F \circ f} & \downarrow{\scriptstyle \exists F(f)} \\
K & \xrightarrow[F]{} & F(K)
\end{array}
\tag{2.16}
$$

The bottom is obvious by definition and for the top $\ker(f) \cap [K, K] \cong [G, G] \cap \ker(Ff)$. So F is a covariant functor from Grp to AbGrp.

5. Another nice example is the fundamental group from algebraic topology. Let $TopP$ be the category whose objects are pointed topological spaces of the form (X, x_0) where X is a topological space and x_0 is a fixed point in X. The morphisms in this category are base point preserving continuous functions. So $f \in \hom((X, x_0), (Y, y_0))$ if $f : X \to Y$ is a continuous function and $f(x_0) = y_0$. In algebraic topology one associates the fundamental group to every object (X, x_0) in $TopP$ denoted by $\pi_1(X, x_0)$. Given a morphism $f \in \hom((X, x_0), (Y, y_0))$ we also get a group homomorphism $\pi_1(f) : \pi_1(X, x_0) \to \pi_1(Y, y_0)$. It can be shown that π_1 is a functor between the category $TopP$ and the category of groups.

There is a whole class of functors called forgetful functors because they forget some of the structure.

Examples 2.60. 1. $U : Group \to Set$, where U "forgets" about the group structure.

2. $F : Ring \to Group$, where F "forgets" the multiplication operation in the ring.

3. $H : Top \to Set$, where H "forgets" the topological structure.

4. $1 : \mathscr{C} \to 1$ is the functor which takes all objects to one object and all morphisms

to the identity morphism on that object. The category 1 has a single object and the identity morphism.

Another method of creating new categories from old is known as a slice.

Definition 2.61. Let $\mathscr{C}$ be a category with an object C. The slice category, $\mathscr{C}_C$ set $\text{obj}(\mathscr{C}_C) = \text{hom}(X, C)$ for all $X \in \text{obj}(\mathscr{C})$. So the objects are all the morphisms in $\mathscr{C}$ which map to C. Now assume $f_1 : X_1 \to C$ and $f_2 : X_2 \to C$ where $f_1, f_2 \in \text{hom}(\mathscr{C})$ and so $f_1, f_2 \in \text{obj}(\mathscr{C}_C)$. Then there is a $g \in \text{hom}(\mathscr{C}_C)$ if and only if $\exists h \in \text{hom}(\mathscr{C})$ such that $h : X_2 \to X_1$ with $f_2 = f_1 \circ h$. That is $g : f_1 \to f_2$ is defined as $g(f_1) = f_1 \circ h = f_2$.

Finally a definition that will be used repeatedly for the rest of the thesis.

Definition 2.62. Let $\mathscr{A}, \mathscr{B}$ be categories. A **Contravariant functor**, F from $\mathscr{A}$ to $\mathscr{B}$ is a mapping which

1. associates to each object $A \in \text{obj}(\mathscr{A})$ an object $F(A) \in \text{obj}(\mathscr{B})$,
2. associates to each morphism $f : A \to B \in \mathscr{A}$ a morphism $F(f) : F(B) \to F(A) \in \mathscr{B}$.
3. $F(id_A) = id_{F(A)}, \forall A \in \text{obj}(\mathscr{A})$,
4. $F(g \circ f) = F(f) \circ F(g)$ for all morphisms $f : A \to B$ and $g : B \to C$.

changing the order of composition.

Another way of formulating the definition would be to let $F : \mathscr{C}^{op} \to \mathscr{D}$ be a covariant functor. Then $F : \mathscr{C} \to \mathscr{D}$ is contravariant.

Examples 2.63. 1. Let $X \subset \mathbb{C}^n$ be a topological space. Recall $ITop_X$ from Example 2.54 is the category defined on X with inclusions as morphisms and $\text{obj}(ITop_X)$ are all the open subsets of X. Consider the functor $\Gamma : ITop_X \to$

$CRing$ defined as follows: $\Gamma(U)$ is the ring of complex-valued continuous functions on U, and if $U \subset V$ then there is a natural restriction map from $\Gamma(U)$ to $\Gamma(V)$. Then Γ is a contravariant functor.

2. Let $\mathbb{C}^n$ be given the usual Euclidean topology. Then we can define $\Gamma_h : ITop_{\mathbb{C}^n} \to CRings$ by associating to each open set $U \in ITop_{\mathbb{C}^n}$ the ring $\Gamma_h(U)$ of holomorphic functions on U. This is also a contravariant functor.

Finally with enough tools dropped in the box, let's define a sheaf.

Definition 2.64. Let $\mathscr{C}$ be a category and let X be a topological space. We say that the pair $(X, \mathcal{F})$, is a $\mathscr{C}$**-presheaf** on X if the following holds:

1. for every open set $U \subset X$, there exists a $\mathcal{F}(U) \in \text{obj}(\mathscr{C})$.

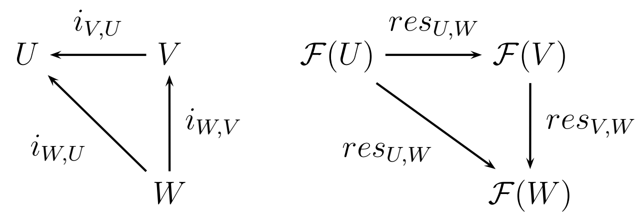
2. for every inclusion of open sets $V \subset U$, there exists a morphism $res_{U,V} : \mathcal{F}(U) \to \mathcal{F}(V)$ with $res_{U,V} \in \text{hom}(\mathscr{C})$. The morphism is called the restriction morphism and must satisfy the following two properties.

   - For every open set U in X, $res_{U,U} = 1_{\mathcal{F}(U)}$.
   - Given three open sets $W \subset V \subset U$, then $res_{V,W} \circ res_{U,V} = res_{U,W}$.

Proposition 2.65. *Let X be a topological space and let $ITop_X$ be the category defined in Example 2.54. A $\mathscr{C}$-presheaf on X is a contravariant functor from $ITop_X$ to $\mathscr{C}$.*

Proof. If $\mathcal{F}$ is a presheaf on X then we claim that the map that associates to each open set of U of X the object $\mathcal{F}(U)$ in $\mathscr{C}$ is a functor $F : \text{obj}(ITop_X)$ to $\mathscr{C}$. The conditions for F to be a functor are implied by the pre-sheaf axioms above. It is a contravariant functor because the arrows are reversed. □

Driving the contravariant point home, the following diagrams must commute.



(2.17)

The diagram on the left is the inclusion maps which are monomorphisms by definition. The diagram on the right are restriction maps in the category $\mathscr{C}$.

At last the definition of a sheaf can be formalized.

Definition 2.66. A pre-sheaf $(X, \mathcal{F})$ is a sheaf if the following holds:

Given any open cover $\{U_\alpha\}$ of an open set $U \subset X$ and elements $f_\alpha \in \mathcal{F}(U_\alpha)$ such that if $U_\alpha \cap U_\beta \neq \emptyset$ then $res_{U_\alpha, U_\alpha \cap U_\beta}(f_\alpha) = res_{U_\beta, U_\beta \cap U_\alpha}(f_\beta)$, then there exists an element $f \in \mathcal{F}(U)$ such that $res_{U,U_\alpha}(f) = f_\alpha$.

Elements f in the object $\mathcal{F}(U_i) \in \text{obj}(\mathscr{C})$ are called **sections** over U_i. Therefore, our definition requires in particular, that two sections that agree on the overlap of two open sets must extend to the union of these sets. So the condition requires that sections can be glued together and that the gluing is compatible with restrictions. For this reason a sheaf is sometimes called a pre-sheaf with the gluing property.

Similarly for a point p the directed limit using restriction maps of all open sets $\mathcal{F}(U_i)$ of U_i which contain p is called the **stalk** at p. In symbols, a stalk at p,

$$\mathcal{F}_p = \varinjlim_{U_i \ni p} \mathcal{F}(U_i). \tag{2.18}$$

So an element of a stalk is a pair (U, g), where U is an open neighborhood of p and g is an element in $\mathcal{F}(U)$. Because of the definition of direct limits, two elements (U, g) and (V, f) define the same element in $\mathcal{F}_p$, if and only if there is an open neighborhood

W of p, with $W \subset U \cap V$ such that $res_{U,W}(g) = res_{V,W}(f)$. Elements of a stalk are called **germs**.

There is actually much more that can be shown about sheaves at this point but it would require spending even more pages on category theory. Instead, additional category theory will be developed as topics are covered, In the mean time let us head back to the main topic, with the new machinery.

2.2.2 Ringed Space

One of the most commonly used sheaves will be a sheaf of rings. It will show up later in defining schemes. Before ringed space and hence sheaves of rings can be defined we must identify the rings which will be associated to open sets. This leads us to examine the algebraic concept of localization of rings.

Definition 2.67. Let A be a ring and let $S \subset A$ be a multiplicatively closed subset that does not contain 0. So $f, g \in S \Rightarrow fg \in S$. Define the localization of A with respect to S as

$$S^{-1}A = A_S = \{\frac{h}{f} : \ h \in A, \ f \in S \text{ where } \frac{h}{f} = \frac{h'}{f'} \Leftrightarrow s(hf' - h'f) = 0, \text{ for some } s \in S\}. \quad (2.19)$$

Note that A_S is a ring as elements can be added by getting common denominators just like fractions. There is a natural ring homomorphism from A to A_S obtained by sending the element $a \in A$ to $\frac{as}{s}$ for any element $s \in S$.

Examples 2.68. Let $X = V(\mathfrak{a}) \subset k^n$ be an irreducible affine algebraic set. Let $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ be the coordinate ring of X.

1. Let $f \in A$ be an element that is not nilpotent. Then $S = \{1, f, f^2, f^3, \dots\}$ is a multiplicatively closed set which does not contain zero. In this setting we denote the localized ring $S^{-1}A$ by A_f. Elements of A_f are of the form $\frac{g}{f^n}$ where $g \in A$.

2. Let $\mathfrak{p}$ be a prime ideal of A and let $S = A \setminus \mathfrak{p}$. Then S is multiplicatively closed and $0 \notin S$. Here we denote the localized ring $S^{-1}A$ by $A_{\mathfrak{p}}$.

Proposition 2.69. *Assume A is a ring with a multiplicatively closed set S which does not contain zero. Assume B is a ring and $f : A \to B$ is a homomorphism such that for every $s \in S$ there is an $f(s)^{-1} \in B$. Then $g : S^{-1}A \to B$ can be defined as $g(r/s) = f(r)f(s)^{-1}$. In other words, f factors through the localization $S^{-1}A$.*

Proof. Assume $(r, s) \sim (r', s')$ then there exists $s_1 \in S$ such that

$$s_1(s'r - sr') = 0 \Rightarrow f(s_1)(f(s')f(r) - f(s)f(r')) = 0 \Rightarrow f(r)f(s)^{-1} = f(r')f(s')^{-1}$$

by multiplying both sides by $f(s_1)^{-1}f(s')^{-1}f(s)^{-1}$. Therefore, $g(r/s) = f(r)f(s)^{-1}$. □

Corollary 2.70. *If R is an integral domain and if we define $S = R \setminus 0$, then $f : R \to S^{-1}R$ defined by $r_1 \mapsto \frac{r_1}{1}$ is injective.*

Proof. $\frac{r_1}{1} = \frac{r_2}{1} \Leftrightarrow r_3(r_1 - r_2) = 0$ for some $r_3 \in S$. But R is an integral domain and $r_3 \neq 0$ so $r_1 = r_2$. □

Next take a look at what localization does to ideals.

Proposition 2.71. *There is a one-to-one correspondence between proper ideals of $S^{-1}A$ and ideals of A that do not intersect S. Furthermore this correspondence preserves intersections and inclusions.*

Proof. Define $\phi_S(\mathfrak{a}) = S^{-1}\mathfrak{a}$ that is $\phi_s(\mathfrak{a})$ is all fractions $a/s \in S^{-1}A$ with $a \in \mathfrak{a}$ and $s \in S$. Now let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in A.

1. Let $x \in \mathfrak{a} + \mathfrak{b}$, so $x/s \in S^{-1}(\mathfrak{a} + \mathfrak{b})$. But $x = a + b$ for some $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ so $x/s = (a + b)/s = a/s + b/s$ with $a/s \in S^{-1}\mathfrak{a}$ and $b/s \in S^{-1}\mathfrak{b}$. Conversely, if $a/s_1 + a/s_2 \in S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b}$ then $as_2 + bs_1/s_1s_2 \in S^{-1}(\mathfrak{a} + \mathfrak{b})$. Therefore,

$$S^{-1}(\mathfrak{a} + \mathfrak{b}) = S^{-1}\mathfrak{a} + S^{-1}\mathfrak{b} \tag{2.20}$$

2. Next consider $x = ab \in \mathfrak{ab}$ giving $x/s = ab/s \in S^{-1}\mathfrak{ab}$. But then $(a/1) \in S^{-1}\mathfrak{a}$ and $b/s \in S^{-1}\mathfrak{b}$. The converse is just as obvious. Thus

$$S^{-1}(\mathfrak{ab}) = S^{-1}\mathfrak{a}S^{-1}\mathfrak{b} \tag{2.21}$$

3. Let $x \in \mathfrak{a} \cap \mathfrak{b}$ then $x/s \in S^{-1}(\mathfrak{a} \cap \mathfrak{b})$. Thus $x \in \mathfrak{a}$ and $\mathfrak{b}$. Hence $x/s \in S^{-1}\mathfrak{a}$ and $x/s \in S^{-1}\mathfrak{b}$. Conversely assume $a/s = b/s'$ then there is an $s_1 \in S$ such that $s_1as' = s_1bs$ but this gives $a/s = s_1bs'/s_1s's \in S^{-1}(\mathfrak{a} \cap \mathfrak{b})$. [6] Therefore,

$$S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b} \tag{2.22}$$

□

Before moving on, we provide the proof of Proposition 2.29, which we restate as a claim for convenience.

Claim 2.72. *The radical of an ideal in $k[X_1, \ldots, X_n]$ is equal to the intersection of the prime ideals containing it.*

Proof. Let $R = k[X_1, \ldots, X_n]$ and $\mathfrak{a} \subset R$ be an ideal. Let $\{\mathfrak{p}_j\} = \{\mathfrak{p} \subset R :$ $\mathfrak{p}$ is prime and $\mathfrak{a} \subseteq \mathfrak{p}\}$. Every prime ideal is radical from Proposition 2.26, and every $\mathfrak{p}_j$ contains $\mathfrak{a}$; therefore $\sqrt{\mathfrak{a}} \subseteq \mathfrak{p}_j$ for all j. Thus

$$\sqrt{\mathfrak{a}} \subseteq \bigcap_{j \in J} \mathfrak{p}_j.$$

Now assume $f^n \notin \mathfrak{a}$ for all n. Then $f \notin \sqrt{\mathfrak{a}}$. Let $S = \{f^n : n \in \mathbb{N} \cup \{0\}\}$. S is multiplicative and $0 \notin S$; therefore $S^{-1}R$ is defined. Consider $\phi : S^{-1}R \to S^{-1}R/S^{-1}\mathfrak{a}$.

Choose a maximal ideal in the image of ϕ; call it $\mathfrak{m}$. Composing with the natural map from A to $S^{-1}A$ we get a map: $\psi : R \to S^{-1}R/S^{-1}\mathfrak{a}$. Then $(\psi)^{-1}(\mathfrak{a}) \subset (\psi)^{-1}(\mathfrak{m})$ and $f \notin (\psi)^{-1}(\mathfrak{m})$. Moreover, $\mathfrak{m}$ was maximal so $(\psi)^{-1}(\mathfrak{m})$ is prime giving a prime ideal which contains $\mathfrak{a}$ but not f. The contrapositive of which, is

$$\bigcap_{j \in J} \mathfrak{p}_j \subseteq \mathfrak{a}.$$

□

To say $\mathcal{F}$ is a sheaf of rings is to say $\mathcal{F}(U)$ is a commutative ring for every U with ring homomorphisms for restriction. In most cases we will further restrict the rings $\mathcal{F}(U)$ to be finitely generated k-algebras, that is quotients of polynomial rings $k[X_1, \ldots, X_n]$. But this restriction is not necessary for the definition of ringed spaces.

Definition 2.73. A **ringed space** is a topological space X, equipped with a sheaf of rings, denoted as $\mathcal{O}_X$.

Definition 2.74. [8]Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be two ringed spaces. A morphism between them is given by $\phi : X \to Y$, with a morphism of sheaves $\phi^* : \Gamma(U, \mathcal{O}_Y) \to$

$\Gamma(\phi^{-1}U, \mathcal{O}_X)$ that is compatible with the restriction maps for the structure sheaves on X and Y.

In most cases of interest the ring $\Gamma(U, \mathcal{O}_Y)$ will be functions that are defined on the open set U and the map ϕ^* corresponds to composing a function defined on U with the function ϕ to get a function defined on $\phi^{-1}(U)$.

Definition 2.75. Let $\mathfrak{a}$ be an ideal, $\mathfrak{a} \subset k[X_1, \ldots, X_n]$. Set $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ then define

$$\operatorname{spec}(A) = \{\mathfrak{p} : \mathfrak{p} \text{ is a prime ideal in } A\}.$$

The closed sets in $\operatorname{spec} A$ are of the form $V(\mathfrak{b}) = \{\mathfrak{p} \in \operatorname{spec}(A) \mid \mathfrak{b} \subset \mathfrak{p}\}$ for an ideal $\mathfrak{b}$ in A. It is easy to see that these sets form a topology, just as we showed in the discussion following Definition 2.15 for affine algebraic sets.

For the remainder of this section we fix a ring A as above and let $X = \operatorname{spec}(A)$.

Examples 2.76.

1. Let $X = \operatorname{spec}(k)$. Then there is exactly one ideal which is not proper and so X is a single point.

2. Let I be a radical ideal of $k[X_1, \ldots, X_n]$. So $\sqrt{I} = I$ and $I(V(I)) = I$. Now $A = k[X_1, \ldots, X_n]/I$ is reduced. If k is algebraically closed, we have seen in Nullstellensatz, Theorem 2.24, that every maximal ideal in A corresponds to a point $(a_1, \ldots, a_n) \in V(I)$. We also remark that the subset $\{\mathfrak{p}\}$ of $\operatorname{spec}(A)$ is a closed point, if and only if, $\mathfrak{p}$ is a maximal ideal. Hence, if k is algebraically closed then the closed points of $\operatorname{spec}(A)$ correspond to "honest" points in $V(I)$ as defined in the previous section. However $\operatorname{spec}(A)$ also has additional points corresponding to every prime ideal in A.

3. Let $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ where $\mathfrak{a}$ is not reduced. Then if we only look at the points then $\operatorname{spec}(A)$ and $\operatorname{spec}(A/\sqrt{\mathfrak{a}})$ have the same points. This is easy to see because the points are the prime ideals and both A and $A/\sqrt{\mathfrak{a}}$ have the same prime ideals.

4. Consider $\operatorname{spec}(\mathbb{Z})$. The ring is $\mathbb{Z}$ which is a principal ideal domain with prime ideals of $\langle 0 \rangle$ and $\mathfrak{p} = \langle p \rangle$ where p is a prime number.

5. In $\operatorname{spec}(\mathbb{C}[X])$ the maximal ideals are of the form $< X - c >$ where $c \in \mathbb{C}$, which gives us one point for each complex number. But $\langle 0 \rangle$ is also prime and so there is another point. But $< 0 >$ is not a closed point since the closure of this point is all of $\operatorname{spec}(\mathbb{C}[X])$. Hence this point is called the generic point of this space.

6. Consider $\operatorname{spec}(\mathbb{R}[X])$. Here the prime ideals are $< 0 >$, $< X - a >$ and $< X^2 + aX + b >$ where $X^2 + aX + b$ is an irreducible quadratic. The maximal ideals $< X - a >$ correspond to the points $a \in \mathbb{R}$. The maximal ideal $< X^2 + aX + b >$ corresponds to the conjugate pairs of roots of the quadratic polynomial.

We remark that the proof in Proposition 2.33 goes through verbatim to show that every open cover of $X = \operatorname{spec}(A)$ has a finite subcover. For any element $f \in A$, we can define the open set $X_f = X - V(< f >)$ that consists of all prime ideals $\mathfrak{p}$ such that $f \notin \mathfrak{p}$. These sets X_f are said to be *the distinguished open sets* of X. It is easy to see that $X_f \cap X_g = X_{fg}$ and that the distinguished open sets form a basis for the Zariski topology on X.

We now proceed to define the structure of a ringed space on $\operatorname{spec} A$.

We recall from Example 2.68.(1) the local ring $A_{\mathfrak{p}}$ that is obtained by localizing the ring A at the set $S = A \setminus \mathfrak{p}$. We use these rings to associate a ring to each open set U in $\operatorname{spec}(A)$ as follows:

Definition 2.77. [4] Let $X = \text{spec}(A)$ be the spectrum of a finitely generated $k-$algebra. Thus $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ where the ideal $\mathfrak{a}$ is finitely generated. Define the structure sheaf on X to be the the sheaf $\mathcal{O}_X$ with sections, $\mathcal{O}_X(U)$, on an open set $U \subset X$ defined as follows:

$$s : U \to \coprod_{\mathfrak{p} \in U} A_{\mathfrak{p}}$$

and satisfy the following conditions:

- for all $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in A_{\mathfrak{p}}$; and
- for all $\mathfrak{p} \in U$, there exists an open neighborhood $\mathfrak{p} \in V \subset U$ and elements $g, f \in A$ such that for all $\mathfrak{q} \in V$, one has $f \notin \mathfrak{q}$ and $s(\mathfrak{q}) = g/f \in A_{\mathfrak{q}}$.

$\mathcal{O}_X(U)$ has a ring structure obtained by adding and multiplying two sections $s, t \in \mathcal{O}_X(U)$ by performing the corresponding operation on $s(\mathfrak{p})$ and $t(\mathfrak{p})$ in $A_{\mathfrak{p}}$ for every prime ideal $\mathfrak{p}$ in U. If $V \subset U$ are open sets then the map from $\mathcal{O}_X(U)$ to $\mathcal{O}_X(V)$ is just obtained by restricting the value of a section on U to V. Because of the local nature of the definition of the sections, they have the gluing property required of a sheaf, Definition 2.66, and hence $\mathcal{O}_X$ defines a sheaf of rings on X. It is also true that for this sheaf of rings the stalk at a point $\mathfrak{p}$ in X will be the local ring $A_{\mathfrak{p}}$ and it is shown in Corollary 2.80.

We now identify the ring of sections on distinguished open sets in the following proposition.

Proposition 2.78. *Let* $X = \text{spec}(A)$ *with structure sheaf* $\mathcal{O}_X$ *and let* $f \in A$. *Then* $\mathcal{O}_X(X_f) \cong A_f$.

Proof. We will define a map $\phi : A_f \to \mathcal{O}_X(X_f)$. Any element of A_f can be represented as g/f^N where $g \in A,\ N \geq 0$ and for any $\mathfrak{q} \in X_f$ then $f^N \notin \mathfrak{q}$. So $g/f^N \in A_{\mathfrak{q}}$. Thus define $\phi(g/f^N)$ to be the function $s : U \to \coprod_{\mathfrak{p} \in U} A_{\mathfrak{p}}$ given by $s(\mathfrak{q}) = g/f^N \in A_{\mathfrak{q}}$.

Let $s = g/f^N \in A_f$ and $\phi(s) = 0$. Then for every prime ideal $\mathfrak{q} \in X_f$, g/f^n is represented by $0 \in A_\mathfrak{q}$. So for each $A_\mathfrak{q}$ there is an $h_\mathfrak{q} \in A_\mathfrak{q}$ such that $h_\mathfrak{q} g = 0$. Now X_f can be covered by the open sets of the form $X_{h_\mathfrak{q}}$. By quasi-compactness, Proposition 2.33, we only need a finite number. Thus $X_f = \cup X_{h_\mathfrak{q}}$, but then $V(f) = \cap V(h_\mathfrak{q}) = V(\sum \mathfrak{q})$ giving $f^n = \sum e_\mathfrak{q} h_\mathfrak{q}$. Then multiplying by g gives $f^n g = \sum e_\mathfrak{q} h_\mathfrak{q} g = 0$. But this shows that $f^n g = f^n 0 = 0 \in A_f$. So we can deduce that $\ker(\phi) = \{0\}$.

Next we need to show that ϕ is surjective. Choose a section $s \in \mathcal{O}_X(X_f)$. Now for each prime ideal, $\mathfrak{p} \in X_f$ there is an open neighborhood of $\mathfrak{p}$, U_i, where s is represented as $s = g_i/f_i$ with $f_i \notin \mathfrak{p}$, but $g_i, f_i \in A$. Now $X_f \subset \cup U_i$ and from Proposition 2.32 the distinguished open sets are a basis for X_f; moreover, by Proposition 2.33 only finitely many need be considered. So we have a finite number of U_i which cover X_f, on each of which $s = \frac{g_i}{f_i^{n_i}}$. Furthermore since s was a section $\frac{g_i}{f_i^{n_i}} = \frac{g_j}{f_j^{n_j}}$ on $U_i \cap U_j. = X_{f_i f_j}$ So we can simplify further by noting for $V(f) = V(f^n)$ so $X_f = X_{f^n}$. We can rewrite $s = \frac{g_i}{f_i}$ for all i.

On $X_{f_i f_j}$ the restriction of $\frac{g_i}{f_i}$ and $\frac{g_j}{f_j}$ are equal. Since the map ψ from $A_{f_i f_j}$ to $\mathcal{O}_X(X_{f_1 f_j})$ is injective this implies that $\frac{g_i}{f_i} - \frac{g_{ij}}{f_j}$ equals zero in $A_{f_i f_j}$. So $(f_i f_j)^{n_{ij}}(f_j g_i - g_j f_i) = 0$ for some positive integer n_{ij}. By finiteness of the number of open sets in the cover, we can find a single integer N that works for all indices i and j. So

$$[(f_i f_j)^N]\left([g_i f_j] - [g_j f_i]\right) = [g_i f_i^N][f_j^{N+1}] - [g_j f_j^N][f_i^{N+1}] = 0 \in A$$

for all i, j between 1 and m. We can replace g_i by $g_i f_i^N$ and f_i by f_i^{N+1} for all i between 1 and m. Now $f_i g_j = f_j g_i$.

Since $X_f \subseteq \cup X_{f_i}$, is a finite cover, we have that $f \in I(V(\sum f_i))$ giving $f^n \in \langle f_1, \ldots, f_m \rangle$. So there exists $e_i \in A$ such that $f^n = \sum e_i f_i$.

Let

$$g = \sum e_i g_i.$$

Then after multiplying by f_j we have

$$gf_j = \sum e_i g_i f_j = \sum e_i f_i g_j = f^n g_j$$

for all j. Hence $\frac{g}{f^n} = \frac{g_j}{f_j} \in A_{f_j}$ for all j which shows that

$$\phi\left(\frac{g}{f^N}\right) = \phi\left(\frac{g_j}{f_j}\right) = s \text{ for all } j.$$

Hence the map $\phi : A_f \to \mathcal{O}_X(X_f)$ is an isomorphism. □

Before talking about the importance of the last proposition and a few corollaries we need some more notation.

Definition 2.79. Let $X = \text{spec}(A)$ and $(X, \mathcal{O}_X)$ the structure sheaf of X. For each open $U \subset X$ define $\Gamma(U, \mathcal{O}_X) = \mathcal{O}_X(U)$, the ring associated to U.

Corollary 2.80. *Let $X = \text{spec}(A)$ and let $\mathcal{O}_X$ be its structure sheaf. Then the following statements are true.*

1. $\Gamma(X_f, \mathcal{O}_X) = A_f$

2. $\Gamma(X, \mathcal{O}_X) = A$

3. *Let $p \in X$ then p corresponds to the prime ideal $\mathfrak{p} \subset A$ and the stalk $\mathcal{O}_{X,\mathfrak{p}} = A_{\mathfrak{p}}$.*

Proof. 1. This is just a restatement of Proposition 2.78.

2. Note $X_1 = X - V(1) = X - \emptyset = X$.

3. We have shown that the distinguished open sets form a basis for the topology in Proposition 2.32. Thus the direct limit can be computed by looking at sections of $\mathcal{O}_X$ on distinguished open sets for which $\mathfrak{p} \in X_f$. Then $\mathfrak{p} \in X_f$ if and only if $f \notin \mathfrak{p}$. Moreover the stalk is defined in equation (2.18) as

$$\mathcal{F}_p = \varinjlim_{U_i \ni p} \mathcal{F}(U_i).$$

Hence as $\mathcal{O}(X_f) = A_f$ the elements inverted are all those in $A \setminus \mathfrak{p}$.

□

Proposition 2.81. *Let $X = \text{spec}(A)$ for A a finitely generated $k-$algebra. The pair $(X, \mathcal{O}_X)$ defined by Definition 2.77 is a ringed space.*

Proof. The proposition is really a summary of what has been shown above. □

Definition 2.82. The **affine scheme** associated to A, a $k-$algebra of finite type, is the ringed space $(X, \mathcal{O}_X)$, where $X = \text{spec}(A)$.

Definition 2.83. An **affine variety** is an affine scheme associated to a finitely generated $k-$algebra A , where A is an integral domain. Hence $\text{spec}(A)$ is an irreducible space and A is a reduced ring.

Example 2.84. Let $f = y+2$ and $g = x^3 - x^2 - 2 - y$. Then the corresponding affine algebraic set is given by $V(\langle f, g\rangle) = \{(0, -2), (1, -2)\}$.

Let $A = k[x, y]/\langle f, g\rangle \cong k[x]/\langle x^2(x - 1)\rangle$ and let $X = \text{spec}(A)$. Then X has two points because there are only two prime ideals in A. We can see this because $\langle x\rangle$ and $\langle x - 1\rangle$ are the only ideals in $k[x]$ which contain $\langle x^2(x - 1)\rangle$.

Now we ask about the stalks at 1 and 0. Any $h \in \Gamma(X, \mathcal{O})$ can be written as $ax^2 + bx + c$, where $a, b, c \in k$. For each stalk we have the ring A_1 and A_0. Consider

A_0 first. No homogeneous element can be in the denominator. Thus only the non-homogeneous elements have inverses. Therefore, $A_0 \cong k[x]/\langle x^2 \rangle$. For A_1 every element except those with a root at 1 have inverses. So $A_1 \cong k[x]/\langle x-1 \rangle \cong k$.

So the scheme encodes information about how the hypersurfaces intersect. In terms of roots of polynomials the scheme keeps track of the multiplicity.

Lemma 2.85. *If there is a ring homomorphism $\phi : A \to B$ then each prime ideal $\mathfrak{p} \in B$ has a preimage that is prime in A.*

Proof. Assume $\mathfrak{p} \subset B$ is prime and $\phi^{-1}(\mathfrak{p}) \subset A$ is not prime. Then $fg \in \phi^{-1}(\mathfrak{p})$, but $f \notin \phi^{-1}\mathfrak{p}$ and $g \notin \phi^{-1}\mathfrak{p}$. Now $\phi(fg) \in \mathfrak{p}$ but $\phi(f)\phi(g) \notin \mathfrak{p}$ a contradiction to $\mathfrak{p}$ being prime. □

Note the converse is not true. In general, $\mathfrak{p}$ is prime does not imply that $\phi(\mathfrak{p})$ is prime. For example if ϕ is the inclusion, $\phi : \mathbb{Q}[X] \to \mathbb{R}[X]$ and $\mathfrak{p} = \langle X^2 - 2 \rangle$, then $\mathfrak{p} \subset \mathbb{Q}[X]$ is prime, but $\phi(\mathfrak{p})$ is not prime in $\mathbb{R}[X]$.

Proposition 2.86. *If $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ are affine schemes then there is a correspondence between morphisms of ringed spaces $\phi : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ and ring homomorphisms $\phi_* : \Gamma(Y, \mathcal{O}_Y) \to \Gamma(X, \mathcal{O}_X)$.*

Proof. By definition ϕ induces ϕ_* because a map of schemes is a map of ringed spaces and hence gives a map of rings as required. So we need to show that a map of rings induces a map of affine schemes.

Let $\Gamma(X, \mathcal{O}_X) = B$ and $\Gamma(Y, \mathcal{O}_Y) = A$ and let $\psi : A \to B$ be a ring homomorphism. So we will construct $f : (X = \text{spec}(B)) \to (Y = \text{spec}(A))$. So define $f(\mathfrak{b}) = \psi^{-1}(\mathfrak{b})$, where $\mathfrak{b} \subset B$ is prime. So by Lemma 2.86 each $\psi^{-1}(\mathfrak{b})$ is prime in A. It is clear that $f^{-1}(V(b)) = V(\psi(b))$ for every element $b \in B$, so f is a continuous map. The map ψ induces a map $\psi_b : B_b \to A_{\psi(b)}$ which gives the morphism between the schemes. □

So morphisms of affine schemes are in one to one correspondence with homomorphisms of rings. Let ASCH be the category with objects affine schemes and arrows the morphisms of affine schemes. Then spec is a contravariant functor from the category of commutative rings to ASCH. In fact, it is a bijection and so in the language of categories it is **fully faithful**.

2.2.3 Sheaves of Modules

In the last section we developed a sheaf of rings which can be associated with a topological space. Now we will show that we can associate sheaves of modules to affine schemes. Before discussing sheaves we recall a few facts about modules.

Definition 2.87. Let R be a ring, an R-module is an abelian group M (written additively) on which R acts linearly. That is to say there is a pair (M, μ) where M is an abelian group and $\mu : R \times M \to M$ such that, for $a \in R$ and $x \in M$ $\mu(a, x) \mapsto ax \in M$ linearly: So for $x, y \in M$ and $a, b \in R$

$$a(x + y) = ax + ay$$

$$(a + b)x = ax + bx$$

$$(ab)x = a(bx)$$

$$1x = x$$

If $\mathfrak{a}$ is an ideal of a ring R, then $\mathfrak{a}$ is an R-module.

Definition 2.88. Let M, N be R-modules then $f : M \to N$ is an R-module homomorphism, R-**linear**, if

$$f(x+y) = f(x) + f(y)$$
$$f(ax) = af(x)$$

for all $a \in R$ and $x, y \in M$.

Example 2.89. Consider the set of all R-module homomorphisms from M to N as an R-module by defining $(f+g)(x) = f(x)+g(x)$ and $(af)(x) = af(x)$. This module will be denoted as $\hom_R(M, N)$.

Proposition 2.90. *A homomorphism $\mu : M \to M'$ induces a homomorphism*

$$\overline{\mu} : Hom(M', N) \to Hom(M, N)$$

defined as

$$\overline{\mu}(f) = f \circ \mu,$$

$\forall f \in \hom(M', N)$.

The proof is just composition of homomorphisms and should be recognized in relation to contravariant functors. For the sheaf definition we will need objects for the restriction maps.

Definition 2.91. A submodule N of an R-module, M, is a non-empty subset of M which is closed under addition and scalar multiplication.

Proposition 2.92. *The submodules of R considered as an R-module are the ideals of R.*

Proof. By definition an ideal is closed under addition and multiplication by elements of R. $\square$

Definition 2.93. The quotient module, M/N of two R-modules, M, N where $N \subset M$, is defined as the additive group of cosets. That is to say a coset is of the form $\overline{m} = m + N$, and is made into an R-module by $a\overline{m} = \overline{am}$.

Proposition 2.94. *If $N \subset M \subset L$ are R-modules, then*

$$(L/N)/(M/N) \cong L/M.$$

Proof. [1] Define $\phi : L/N \rightarrow L/M$ by $\phi(x + N) = x + M$. So ϕ is a well defined R-module homomorphism that is onto L/M with a kernel of M/N. $\square$

Proposition 2.95. *[2] If*

$$0 \rightarrow M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \rightarrow 0 \tag{2.23}$$

is a short exact sequence of R modules, then the following are equivalent:

1. *There exists an $\alpha : M \rightarrow M_1$ such that $\alpha \circ f = 1_{M_1}$.*

2. *There exists a $\beta : M_2 \rightarrow M$ such that $g \circ \beta = 1_{M_2}$.*

When (1) and (2) hold we say that the sequence is ***split*** *exact and one has:*

$$\begin{aligned} M &\cong \mathit{image}(f) \oplus \ker(\alpha) \\ &\cong \ker(g) \oplus \mathit{image}(\beta) \\ &\cong M_1 \oplus M_2 \end{aligned}$$

Proof. 1. Suppose (1) is true and let $x \in M$. Then

$$\alpha(x - f(\alpha(x))) = \alpha(x) - (\alpha \circ f)(\alpha(x)) = 0$$

since $\alpha \circ f = 1_{M_1}$. Thus $x - f(\alpha(x)) \in \ker(\alpha)$ giving

$$M = \ker(\alpha) + \text{image}(f).$$

Suppose $f(y) = x \in \ker(\alpha) \cap \text{image}(f)$ then $0 = \alpha(x) = \alpha(f(y)) = y$; therefore,

$$M \cong \text{image}(f) \oplus \ker \alpha.$$

Assume $g(v) = u$ then define $\beta(u) = v - f(\alpha(v))$. As g is surjective we know such an element $\exists v \in M$, but it needs to be shown that the map β is well defined. Suppose $g(v) = u = g(v')$. Then $v - v' \in \ker(g) = \text{image}(f)$; therefore

$$\begin{aligned}\beta(v) - \beta(v') &= (v - f(\alpha(v))) - (v' - f(\alpha(v'))) \\ &= (v - v') + (f(\alpha(v') - f(\alpha(v))) \\ &\in \text{image}(f) \cap \ker \alpha \\ &= \{0\}.\end{aligned}$$

Thus β is well defined and from the construction $g \circ \beta = 1_{M_2}$.

2. [5]Assume (2) holds. From the right and left hand 0, g is surjective and f is injective. From exactness, $\ker(g) = \text{image}(f)$, and $\text{dom}(\beta) = \text{image}(g) = M_2$.

Consider $1 - \beta \circ g : M \to M$. Letting $m \in M$,

$$(g \circ (1 - \beta \circ g))(m) = (g - g \circ \beta \circ g)(m) = (g - 1 \circ g)(m) = 0(m) = 0 \in M_2.$$

So $\text{image}(1 - \beta \circ g) \subset \ker(g) = \text{image}(f)$. As f is injective there is a well-defined map $\alpha : M \to M_1$ for which $m - (\beta \circ g)(m) = f(\alpha(m))$ for all $m \in M$. One shows that α is a homomorphism with $\alpha \circ f = 1_M$. So (1) holds.

□

Proposition 2.96. *Let R, B be rings with $f : R \to B$ a homomorphism of rings. Let M be a B-module. Then M is an R-module via f.*

Proof. Let $r \in R$ then $f(r) \in B$ for all r. So for $m, n \in M$ and $a, b \in R$ define $am = f(a)m$ thus $(a + b)(m + n) = f(a + b)(m + n) = (f(a) + f(b))(m + n) = f(a)m + f(a)n + f(b)n + f(b)m = am + an + bn + bm$. □

Example 2.97. Let R be a ring and M an R-module. Let $\mathfrak{a}$ be an ideal of R and $A = R/\mathfrak{a}$ be the quotient ring with $\phi : R \to A$, the canonical homomorphism. Let $\mathfrak{a}M = \{m \mid m = am' \text{ where } a \in \mathfrak{a}, m' \in M\}$. Then $\mathfrak{a}M$ is an R-submodule of M. Now $\hat{\phi} : M \to M/\mathfrak{a}M$ is R-linear; moreover, $M/\mathfrak{a}M$ is also an A-module.

Definition 2.98. Let $(X, \mathcal{O}_X)$ be a ringed space. An $\mathcal{O}_X$-module is a sheaf $\mathcal{F}$ such that for any open set $U \subset X$, $\mathcal{F}(U)$ is a $\mathcal{O}_X(U)$-module and restriction maps are $\mathcal{O}_X$-linear where $\mathcal{O}_X(U) = \Gamma(U, \mathcal{O}_X)$ as described in the last section.

We know from the last section that an affine scheme is a ringed space. Furthermore, the structure sheaf of rings was denoted as $\mathcal{O}_X$.

Next, we will develop a notation which expresses localization more clearly while at the same time showing that restrictions are $\mathcal{O}_X$-linear.

Corollary 2.99. *The R-modules* $S^{-1}(M/N) \cong S^{-1}M/S^{-1}N$.

Proof. The corollary follows from parts 1 and 2 of the proof of Proposition 2.71.That is to say localization commutes with sums therefore thinking of cosets in each gives $S^{-1}(m+N) = S^{-1}m + S^{-1}N$. □

Proposition 2.100. *If there is an exact sequence of R-modules*

$$M' \xrightarrow{f} M \xrightarrow{g} M''.$$

Then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''.$$

is also exact.

Proof. [1] So $g \circ f = 0$ giving $S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0$. Thus image$(S^{-1}f) \subset \ker(S^{-1}g)$. To show the other inclusion, let $m/s \in \ker(S^{-1}g)$. Then $g(m)/s = 0 \in S^{-1}M''$, so there exists $t \in S$ such that $tg(m) = 0 \in M''$. However, $tg(m) = g(tm)$ so $tm \in \ker(g) =$image(f) implying that $tm = f(m')$ for some $m' \in M'$. Therefore $m/s = f(m')/st = (S^{-1}f)(m'/st) \in$ image$(S^{-1}f)$. □

We are now ready to define a sheaf of modules associated to a module.

Definition 2.101. Let $X = \text{spec}(A)$ where $A = k[X_1, \ldots, X_n]/\mathfrak{a}$ for some ideal $\mathfrak{a}$. Let M be a finitely generated A-module. Define a sheaf $\widetilde{M}$ with sections, $s \in \widetilde{M}(U)$, on an open set $U \subset X$ as follows:

$$s : U \to \coprod_{\mathfrak{p} \in U} M_{\mathfrak{p}}$$

and satisfy the following conditions:

- for all $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in M_p$; and
- for all $\mathfrak{p} \in U$, there exists an open neighborhood $\mathfrak{p} \in V \subset U$ and elements $m \in M$ and $f \in A$ such that for all $\mathfrak{q} \in V$, one has $f \notin \mathfrak{q}$ and $s(\mathfrak{q}) = m/f \in A_{\mathfrak{q}}$.

It is clear from the definition and the definition of the structure sheaf $\mathcal{O}_X$ on spec A that $\widetilde{M}(U)$ is a module over $\mathcal{O}_X(U)$ and hence $\widetilde{M}$ is a sheaf of $\mathcal{O}_X$ modules over X.

The proof for Proposition 2.78 goes through verbatim to show that if $f \in A$, then $\widetilde{M}(X_f) = M_f$.

Proposition 2.102. *[1] Let M, N be R-modules. There exists a pair (T, g) where T is an R-module and g a R-bilinear map $g : M \times N \to T$ with the following property:*

Given any R-module P and any $R-$bilinear mapping $f : M \times N \to P$, there exists a unique R-linear map $f' : T \to P$ such that $f = f' \circ g$.

Proof.

1. Uniqueness. Assume (T, g) and (T', g') are two pairs with the property. Then replace (T', g') with (P, f) in the proposition. Then a unique $j : T \to T'$ such that $g' = j \circ g$. Now reverse roles of T and T' to get $j' : T' \to T$ where $g = j' \circ g'$. But then $g = j' \circ g' = j' \circ j \circ g$ and $j \circ j' \circ g' = j \circ g = g'$ showing $j' \circ j = 1 = j \circ j'$.

2. Existence. Let C be a free R-module, with elements of the form $\sum_{i=1}^{n} r_i(m_i, n_i)$ where $r_i \in R$, $m_i \in M$ and $n_i \in N$. That is to say all the R-linear combinations of $M \times N$. Let D be a submodule of C generated by all elements of C of the following form:

$$\begin{aligned}
(m_i + m_j, n_k) - (m_i, n_k) - (m_j, n_k) \\
(m_i, n_j + n_k) - (m_i, n_j) - (m_j, n_k) \\
(rm, n) - r(m, n) \\
(m, rn) - r(m, n).
\end{aligned}$$

Now set $T = C/D$. Let $x \otimes y$ denote the image of generators in T giving generators of T. Now recalling the relations in D results in

$$(x + x') \otimes y = x \otimes y + x' \otimes y,$$
$$x \otimes (y + y') = x \otimes y + x \otimes y',$$
$$(rx) \otimes y = x \otimes (ry) = r(x \otimes y).$$

That is the mapping $M \times N \to T$ is $R-$bilinear.

Checking properties, let $f : M \times N \to P$ with P an R-module and f $R-$bilinear. Then f extends by linearity to $\overline{f} : C \to P$ an R-module homomorphism. Now as f was $R-$bilinear, f vanishes on all of D. Thus a well defined homomorphism is induced $f' : T \cong C/D \to P$ with $f'(x \otimes y) = f(x, y)$, satisfying the conditions of the proposition.

$\square$

Recall a few properties of the tensor product. Let M, N, P be R-modules. Then

1. $M \otimes_R N \cong N \otimes_R M$, by the map $x \otimes y \mapsto y \otimes x$,.

2. $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P) \cong M \otimes_R N \otimes_R P$.

3. $R \otimes M \cong M$ by the map $r \otimes x \mapsto rx$.

Let $f_i : M_i \to N_i$ be a set of linear maps, $i = 1, \ldots, n$. Then

$$f_i \otimes \cdots \otimes f_n \otimes_{i=1}^{n} : M_i \to \otimes_{i=1}^{n} N_i$$

is the induced linear map. Hence we get a map of R-modules:

$$\prod_{i=1}^{n} \hom_R(M_i, N_i) \to \hom_R(\otimes_{i=1}^{n} M_i, \otimes_{i=1}^{n} N_i).$$

Set $n = 2$, to simplify the notation,

$$(f, g) \to f \otimes g \qquad \text{gives}$$

$$f \otimes (g + g') = f \otimes g + f \otimes g' \qquad \text{and}$$

$$f \otimes ag = a(f \otimes g) = af \otimes g.$$

Thus fix a module M and consider the functor on the category of R-modules, defined by $\tau = \tau_M$, where $\tau_M(N) = M \otimes N$. Then

$$\tau : \hom(N', N) \to \hom(M \otimes N', M \otimes N)$$

is defined as:

$$\tau(f) = 1_M \otimes f.$$

Tensor products have many functorial properties.

Proposition 2.103. $(M \oplus N) \otimes_R P \cong (M \otimes_R P) \oplus (N \otimes_R P)$. *More generally if* $N = \oplus_{i=1}^{n} N_i$ *then*

$$M \otimes N \to \oplus_{i=1}^{n}(M \otimes N_i)$$

is an isomorphism.

Proof. Fix M and use τ_M above. So $\tau_M(N_i) = M \otimes N_i$ and letting $\pi_i : N \to N_i \subset N$.

Thus regarding N_i, N_j as submodules of N, $\pi_i \circ \pi_i = \pi_i$ and $\pi_i \circ \pi_j = 0$ giving

$$\sum_{i=1}^{n} \pi_i = 1_N.$$

Lastly $\tau_M(\pi_i) = 1 \otimes \pi_i$. □

Next we need to veer from the topic momentarily and consider free modules.

Definition 2.104. Let R be a ring and M be an R-module. A subset $S \subseteq M$ is $R-$**linearly dependent** if there exists $s_1, \ldots s_n \in S$ and $r_1, \ldots, r_n \in R$ not all zero such that

$$\sum_{i=1}^{n} r_i s_i = 0.$$

A set which is not R-linearly dependent is said to be R-**linearly independent**.

The definition should be recognized from vector spaces where R would have been a field and each s_i a vector.

Definition 2.105. Let M be an R-module. A subset S of M is a **basis** of M if S generates M and S is R-linearly independent.

If S is a basis for $M \neq 0$, an R-module, then

1. every $m \in M$ can be written as

$$m = \sum_{i=1}^{n} r_i s_i$$

   where $s_i \in S$ and $r_i \in R$;

2. if there is an equation

$$\sum_{i=1}^{n} r_i s_i = 0$$

   where the s_i are distinct, then $r_1 = \cdots = r_n = 0$.

Definition 2.106. An R-module M is a **free R-module** if it has a basis.

If M is a free R-module then M is the direct sum of copies of R, in symbols

$$M = \oplus_{i \in I} R.$$

Proposition 2.107. *Let M be a free R-module with basis S, let N be any $R-$ module with a function $h : S \to N$. Then there is a unique $f \in Hom_R(M, N)$ such that $f|_S = h$.*

Proof. So $S = \{s_j\}_{j \in J}$. Define f as

$$f(m) = \sum_{i \in J} r_i h(s_i).$$

where $m = \sum_{i \in J} r_i s_i$. Then

$$f|_S = f(s_j) = \sum_{i \in J} \delta_{ij} h(s_i) = h(s_j),$$

satisfying the proposition. □

Recall from vector spaces the dimension was the cardinality of the basis set.

Proposition 2.108. *[6] If M is a free module with finite basis $m_1, \ldots, m_n$ then every element of $M \otimes N$ has a unique expression of the form*

$$\sum_{i=1}^{n} m_i \otimes n_i, \qquad n_i \in N$$

Proof. The proof follow from the direct sum commuting with the tensor product from Proposition 2.103 □

Proposition 2.109. *Let F be a free module with a basis of n elements and E another free module with a basis consisting of m elements. Then F and E are isomorphic, if and only if, $m = n$.*

Proof. It is easy to see that if $m = n$ we can define an isomorphism by mapping a basis of F to a basis of E and extending the map linearly as in Proposition 2.107. Now suppose that $\phi : F \to E$ is an isomorphism. Let $\mathfrak{m}$ be a maximal ideal of R. Then we get an isomorphism $1 \otimes \phi : A/\mathfrak{m} \otimes F \to A/\mathfrak{m} \otimes E$. Since $\mathfrak{m}$ is a maximal ideal, $A/\mathfrak{m} \cong k$ is a field and $A/\mathfrak{m} \otimes F \cong k^n$ and $A/\mathfrak{m} \otimes E \cong k^m$ as vector spaces. Therefore $m = n$.

□

Definition 2.110. The rank of a free module is the cardinality of any basis.

Corollary 2.111. *If M and N are both free modules of finite rank, then*

$$\text{rank}(M \otimes N) = \text{rank}(M)\,\text{rank}(N)$$

Proof. As M and N are free they have bases $m_1, \ldots m_r$ and $n_1, \ldots n_k$ thus a basis for $M \otimes N$ is $m_1 \otimes n_1, \ldots, m_r \otimes n_1, m_1 \otimes n_2, \ldots, m_r \otimes n_k$ giving $rk = \text{rank}(M \otimes N)$. □

Proposition 2.112. *If F is a free module then every exact sequence*

$$0 \to M \xrightarrow{g} N \xrightarrow{f} F \to 0$$

is split exact.

Proof. Recall that a sequence is split exact if $N = \ker(f) \oplus \text{image}(g)$. Let $\{x_i\}$ be a basis for F. As f is surjective there is an $n_i \in M$ such that $f(n_i) = x_i$. So define

$h : \{x_j\} \to n_j$ as $h(x_i) = n_i$ and so h induces a unique $\phi \in Hom(F, N)$ and $f \circ \phi = 1_F$. The rest follows from Proposition 2.95 □

Now we put this additional machinery to work.

Example 2.113. Let $(X, \mathcal{O}_X)$ be an affine scheme. Let M be an A-module where $X = \operatorname{spec} A$. Let $f \in A$. Then $\widetilde{M}(X_f) = M \otimes_A A_f$.

In particular $\widetilde{M}(X) = \Gamma(X, \widetilde{M}) = M \otimes_A A = M$, and by repeating the proof of Proposition 2.78, for modules, we get that $\Gamma(X_f, \widetilde{M}) = M \otimes_A A_f$.

Proposition 2.114. *[8] The correspondence $M \mapsto \widetilde{M}$ is functorial, exact, and commutes with direct sums and tensor products.*

Proof.

1. Functorial: Assume $\phi : M \to N$ is A-linear then define $\phi_f : M_f \to N_f$ by $\phi(M \otimes_A A_f) = N \otimes_A A_f$. That is to say $\phi_f = \phi \otimes_A 1$.

2. Exact: From Proposition 2.100 localization preserves exact sequences.

3. To show that it commutes with direct sums it is enough to show that for any $f \in A$, $\widetilde{M \oplus M'}(X_f) = \widetilde{M}(X_f) \oplus \widetilde{M'}(X_f)$. But $\widetilde{M \oplus M'}(X_f) = (M \oplus M')_f = (M \oplus M') \otimes_A A_f = M \otimes_A A_f \oplus M' \otimes_A A_f = M_f \oplus M'_f = (\widetilde{M} \oplus \widetilde{M'})(X_f)$. Similarly for tensor products:

$$\begin{aligned}
\widetilde{M \otimes_A M'}(X_f) &= (M \otimes_A M')_f \\
&= (M \otimes_A M') \otimes_A A_f \\
&= (M \otimes_A M') \otimes_A A_f \otimes_A A_f && \text{from } A_f = A_f \otimes_A A_f \\
&= (M \otimes_A A_f) \otimes_A (M' \otimes_A A_f) && \text{commutative.}
\end{aligned}$$

Noting $(m \otimes 1/f^s) \otimes (m' \otimes 1/f^t) = (m \otimes 1/f^t) \otimes (m' \otimes 1/f^s)$,

$$\begin{aligned}(M \otimes_A M') \otimes_A A_f \otimes_A A_f &= (M \otimes_A A_f) \otimes_{A_f} (M' \otimes_A A_f) \\ &= M_f \otimes_{A_f} M'_f \\ &= \widetilde{M} \otimes_{A_f} \widetilde{M'}.\end{aligned}$$

□

Definition 2.115. An $\mathcal{O}_V$-module $\mathcal{F}$ isomorphic to a $\mathcal{O}_V$-module of type $\widetilde{M}$ is called quasi-coherent. If M is finitely generated over A, then $\mathcal{F}$ is said to be a coherent sheaf.

CHAPTER 3: Projective Space

Let k be a field and form the vector space k^{n+1} over k.

Definition 3.1. Projective space, $\mathbb{P}^n \simeq (k^{n+1} - \{0\})/R$, where R is the equivalence relation defined by $p \sim p' \Leftrightarrow p = \lambda p'$, for some $\lambda \in k$.

We will now give several other constructions to help in visualizing projective space. Some of these constructions only work over the field of real numbers as specified below. The following constructions are equivalent where they are defined:

1. $\mathbb{P}^n$ as described in Definition (3.1).
2. The set of lines in k^{n+1} passing through the origin. The point p in $\mathbb{P}^n$ which corresponds to the span of $(x_0, x_1, \ldots, x_n)$ in k^{n+1} is denoted by $p = [x_0 : x_1 : \cdots : x_n]$ where at least one of these coordinates is nonzero.
3. The unit sphere in $\mathbb{R}^{n+1}$ with the antipodal points identified as the same.

$1 \Leftrightarrow 2$) Let $p \in k^{n+1}$. Then the line through 0 and p can be written as λp and so for any p' on the line $p' = \lambda p$. Conversely assume p' is not on the line, then thought of as vectors p and p' are linearly independent and so $p' \neq \lambda p$.

$2 \Leftrightarrow 3$) Clearly any line passing through 0 passes through the unit sphere in $\mathbb{R}^{n+1}$ in two places which by definition are antipodal points. Conversely between any two antipodal points we can draw a line which intersects 0.

Example 3.2. The points on the Riemann sphere $\mathbb{CP}^1$ can be thought of as points of the form $[x_0 : x_1]$, where at least one of the coordinates is nonzero. So $\mathbb{CP}^1$ can be covered by two open sets: U_0 which correspond to points of the form $[1 : s]$ and the set U_1 which consists of points of the form $[t : 1]$. For the points p that lie in the intersection of U_0 and U_1 we have $p = [1 : s] = [t : 1]$, that is $t = 1/s$. An alternate way of constructing $\mathbb{CP}^1$ is to glue two copies of affine space $\mathbb{C}^1$, with coordinates s and t respectively, where for $s \neq 0$, we identify the point s on one copy of $\mathbb{C}$ with the point $1/t$ on the other copy of $\mathbb{C}$. A function, F, defined on all of $\mathbb{CP}^1$ would need $F(s) = F(1/s)$ for all s and so is a constant.

3.1 Projective Algebraic sets

If V is a linear vector space over a field k, then we denote $\mathbb{P}(V) \cong V/\sim$, where $\sim$ is the relation defined for projective space. Thus choosing a basis for V let a point $p \in V$ be written as $p = (x_0, \ldots, x_n)$. The relation $\sim$ is defined by $p \sim v \Leftrightarrow p = \lambda v$ from Definition 3.1. Just as we did in $\mathbb{P}^1$ we denote the point p in $\mathbb{P}^n$ that represents the one dimensional subspace of V that is generated by the vector $p = (x_0, \ldots, x_n)$ in terms of these coordinates in V as $p = [x_0 : \cdots : x_n]$. Since at least one of the coordinates x_i is not zero, we can cover $\mathbb{P}^n$ by open sets $U_i = \{p = [x_0 : x_1 : \cdots : x_n] \,|\, x_i \neq 0\}$. Further we can identify the points $p \in U_i$ with affine space k^n by identifying the point $[x_0 : x_1 : \cdots : x_n]$ with the point $(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots \frac{x_n}{x_i})$ in k^n.

Let $F(x_0, \cdots, x_n)$ be a homogeneous polynomial of degree d in $k[X_0, \ldots, X_n]$. Since $F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \cdots, x_n)$ we cannot consider the polynomial F as a function on projective space $\mathbb{P}^n$. However the zeros of a homogeneous polynomial are well defined in $\mathbb{P}^n$.

Definition 3.3. Let $S \subset k[X_0, \ldots, X_n]$ where each $f \in S$ is a homogeneous polynomial. Then

$$V(S) = \{x \in \mathbb{P}^n : F(x) = 0, \ \forall F \in S\},$$

is a **projective algebraic set**.

Definition 3.4. Let X be an irreducible projective algebraic set, f a homogeneous polynomial. Then

$$D_f = \{x \in X : f(x) \neq 0\}.$$

The above could also be written as $X - V(f) = D_f$. This matches the distinguished open sets from Definition 2.16. However, note that every open set is not necessarily affine. We have already remarked that the sets $\{D_{X_i}\}$ give an open cover of $\mathbb{P}^n$.

Example 3.5. Let $f = xy - t^2 \in k[x, y, t]$. Let $[x : y : t]$ be the homogeneous coordinates in $\mathbb{CP}^2$. In the open set D_t with points of the form $[x : y : 1]$ the points satisfy the equation $xy = 1$ which is a hyperbola. The curve $V(f)$ consists of the hyperbola along with the "two points at infinity", namely $[0 : 1 : 0]$ and $[1 : 0 : 0]$.

Similarly in the open set D_x with points of the form $[1 : y : t]$ the points of $V(f)$ satisfy the equation $y = t^2$ which is a parabola. So the curve $V(f)$ can also be viewed as this parabola with one point at infinity, namely the point $[0 : 1 : 0]$.

Example 3.6. If $p = [a_0 : \cdots : a_n]$ is a point in $\mathbb{P}^n$ then for some i, $a_i \neq 0$, Assume that $a_0 \neq 0$. Let $a = (1, a_1/a_0, \ldots, a_n/a_0) = (1, z_1, \ldots, z_n)$. Thus construct $S = \{X_1 - z_1 X_0, \cdots, X_n - z_n X_0\}$ which gives n homogeneous polynomials with $V(S) = \{p\}$, because if $X_0 = 0 \Rightarrow X_i = 0$ for all i and all polynomials in S are zero only when all the ratios of coordinates are the same as the ratios of the coordinates of p.

3.1.1 Homogeneous Polynomials

Let $R = k[X_0, \cdots, X_n]$ be the ring of polynomials. R has several subgroups which will be important below.

1. $\{F \in k[X_0, \cdots, X_n] : deg(F) \leq d\}$ under addition.

2. $R_d = \{F \in k[X_0, \cdots, X_n] : F \text{ is homogeneous }, deg(F) = d\} \cup \{0\}$ under addition.

Now

$$R = \bigoplus_{d=0}^{\infty} R_d$$

R is a **graded ring** in the following sense:

Definition 3.7. Let R be a ring. R is a **graded ring** if there exist additive groups G_i such that

$$R = G_1 \oplus G_2 \oplus \dots$$

and for $g \in G_s$ and $h \in G_t$, $gh \in G_{s+t}$.

Definition 3.8. A homogeneous ideal of R is an ideal that is generated by homogeneous polynomials.

If I is an homogeneous ideal each element may not be homogeneous. Consider $\langle x^2, y\rangle$, both are homogeneous but $x^2 + y$ is not homogeneous. If f is any polynomial in R then we have $f = f_0 + f_1 + \cdots + f_d$ where each f_i is homogenous of degree i. If f belongs to a homogeneous ideal I, then each $f_i \in I$ for all i. So if I is a homogeneous ideal, then

$$I = \bigoplus_{d \geq 0} I \cap R_d,$$

where each R_d has $\binom{n+d}{d}$ generators and can be thought of as a k-module. Thus any polynomial $f \in I$ can be written as $f = \sum f_d$ with each $f_d \in I \cap R_d$ for some d. In a similar vein, if I is a homogeneous ideal then R/I is a graded ring,

Example 3.9. Consider $R = k[X_0, X_1, X_2]$ then R_2 is a vector space with basis $\{X_0^2, X_0X_1, X_1^2, X_1X_2, X_2^2, X_2X_0\}$ which has cardinality $\binom{4}{2} = \frac{4!}{2!(4-2)!} = 6$.

The **homogenization** of a polynomial $f \in k[X_1, \dots, X_n]$ is defined to be a polynomial $f_h \in k[X_0, \dots, X_n]$ where $f_h = X_0^d f(X_1/X_0, \cdots, X_n/X_0)$ where d is the total degree of the polynomial f. Similarly we can define the homogenization I_h of an ideal $I \subset k[X_1, \ldots, X_n]$ by taking the homogenization of every polynomial $f \in I$.

Example 3.10. Let $f(x, y) = 3x^2y^3 + xy^2 + 6$ then

$$f_h = z^5 f(x/z, y/z)) = 3x^2y^3 + xy^2z^2 + 6z^5$$

which is homogeneous of degree 5.

3.1.2 Ringed Space

Clearly the set of homogeneous ideals is a subset of the set of ideals defined on $k[X_0, \ldots, X_n]$. Thus everything proved for affine ringed spaces, affine modules, and affine sheafs follows for projective ones. Thus what follows only mentions those areas where there are differences or places where confusion can arise.

Definition 3.11. Let X be a subset of $\mathbb{P}^n$. The ideal of X,

$$I(X) = \{F \in k[X_0, \cdots, X_n] : F \text{ is homogeneous and } \forall x \in X, F(x) = 0\}$$

1. $I(X)$ is a homogeneous radical ideal.
2. $X = V(I(X))$.
3. $I \subset I(V(I))$.
4. $I(\mathbb{P}^n) = (0)$.
5. $I(\emptyset) = k[X_0, \cdots, X_n]$.

Theorem 3.12 (Projective Nullstellensatz)**.** *[8] Assume k is algebraically closed. Let I be a homogeneous ideal of $k[X_0, \cdots, X_n]$ and $X = V(I)$.*

$$V(I) = \emptyset \Leftrightarrow \exists N \textit{ such that } \langle X_0, \cdots, X_n\rangle^N \subset I \qquad (3.1)$$
$$\Leftrightarrow \langle X_0 \cdots, X_n\rangle = \sqrt{I}$$

$$\textit{If } V(I) \neq \emptyset \textit{ then } I(V(I)) = \sqrt{I}. \qquad (3.2)$$

Proof. Consider the cone $C(V)$ as the inverse image of of the map $\pi : k^{n+1}\backslash\{0\} \to \mathbb{P}^n$. Now we can use the affine Nullstellensatz. So to say $V(I) = \emptyset$ is to say $C(V) = (0, \ldots, 0)$ the origin. Thus $\sqrt{I} = \langle X_0, \ldots, X_n\rangle$. For the second part if $V(I) \neq \emptyset$, then $I(V(I)) = I(C(V)) = \sqrt{I}$ by the affine Nullstellensatz. □

Definition 3.13. Let $R = k[X_0, \ldots, X_n]/\mathfrak{a}$ where $\mathfrak{a}$ is finitely generated homogeneous ideal. Then R is a graded module and $R = \oplus_{d>0} R_d$. The maximal ideal $\mathfrak{m} = \langle X_0, \ldots, X_n\rangle$ is said to the irrelevant ideal of R. Define

$$\mathrm{Proj}(R) = \{\mathfrak{p} \subset R : \mathfrak{p} \text{ is a homogeneous prime ideal which does not equal } \mathfrak{m}\}.$$

For every homogeneous ideal $\mathfrak{b}$ in $k[X_0, \ldots, X_n]$ we can define $V(\mathfrak{b}) = \{\mathfrak{p} \in \mathrm{Proj}(R) : \mathfrak{b} \subseteq \mathfrak{p}\}$ on Proj. As in section 2.1.1, for any ideals, $\mathfrak{b}, \mathfrak{c}$, we have $V(\mathfrak{b}\mathfrak{c}) = V(\mathfrak{b}) \cup V(\mathfrak{c})$ and if $\{\mathfrak{a}_i\}$ is a family of ideals of R, then $V(\sum \mathfrak{a}_i) = \cap V(\mathfrak{a}_i)$. Thus we can equip $\mathrm{Proj}(R)$ with the Zariski topology where we take $V(\mathfrak{b})$ as the closed sets.

Now for each $\mathfrak{p} \in \mathrm{Proj}(R)$, if S is the set of homogeneous elements in $R \setminus \mathfrak{p}$, then we denote $S^{-1}R$ by $R_{\mathfrak{p}}$ and we denote by $R_{(\mathfrak{p})}$ the elements in the localized ring of degree zero. Hence elements in $R_{(\mathfrak{p})}$ are of the form $\frac{f}{g}$ where f and g are homogeneous elements of the same degree, and $g \notin \mathfrak{p}$.

Now much like the affine case, define for each open $U \subset \operatorname{Proj}(R)$ the elements of $\mathcal{O}(U)$ by

$$s : U \to \coprod_{\mathfrak{p} \in U} R_{(\mathfrak{p})}$$

with the following conditions:

- for all $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in R_{(\mathfrak{p})}$; and
- for all $\mathfrak{p} \in U$, there exists an open neighborhood $\mathfrak{p} \in V \subset U$ and homogeneous elements $g, f \in R$ of the same degree such that for all $\mathfrak{q} \in V$, one has $f \notin \mathfrak{q}$ and $s(\mathfrak{q}) = g/f \in R_{(\mathfrak{q})}$.

Definition 3.14. [4] If R is a graded ring and $X = \operatorname{Proj}(R)$ then $(X, \mathcal{O}_X)$ is a topological space together with the sheaf of rings just constructed.

That the definition gives a sheaf is seen in the same way as we did for affine schemes, except only the degree zero elements are considered. But the degree zero elements form a subring hence the arguments are the same.

We proceed to show $\operatorname{Proj}(R)$ is a ringed space.

Proposition 3.15. *[4] For any $\mathfrak{p} \in \operatorname{Proj}(R)$ the stalk $\mathcal{O}_{X,\mathfrak{p}}$ is isomorphic to $R_{(\mathfrak{p})}$*

Proof. The proof is the same as Proposition 2.80.(1). □

Proposition 3.16. *[4] For any distinguished open set of $X = \operatorname{Proj}(R)$ there is an isomorphism of locally ringed spaces.*

$$(X_f, \mathcal{O}_{X,(f)}) \cong \operatorname{spec}(R_{(f)}).$$

Proof. The points in X_f are homogeneous prime ideals of R that do not intersect $\{f^n \mid n \geq 1\}$. These are in one-to-one correspondence with prime ideals in $R_{(f)}$. Since the definition of the sheaf $\mathcal{O}_X$ on $\operatorname{Proj} R$ is local the claim in the proposition follows. □

Definition 3.17. A **scheme** is a ringed space $(X, \mathcal{O}_X)$ that is locally isomorphic to an affine scheme.

Example 3.18. If $\mathfrak{a}$ is a homogeneous ideal of $k[X_0, \ldots, X_n]$ let $R = k[X_0, \ldots, X_n]/\mathfrak{a}$ then $X = \operatorname{Proj} R$ is a scheme. It is easy to see by the previous proposition that X_{X_i} gives an affine cover of X.

Definition 3.19. A **projective variety** is an irreducible algebraic set in $\mathbb{P}^n$.

CHAPTER 4: Hilbert's Syzygy Theorem

Let $R = k[x_1, \ldots, x_n]$ be the graded polynomial ring. The main objects of study in this chapter are graded modules over R defined as follows:

Definition 4.1. A module M over the graded ring R is said to be a **graded module**, if there is a direct sum decomposition $M = \bigoplus_{d=d_0}^{\infty} M_d$ for some $d_0 \in \mathbb{Z}$, where M_d is an additive subgroup of M, and if $f \in R$ is homogeneous of degree m, then $f \cdot M_d \subset M_{m+d}$. If $m \in M_d$ then m is said to be a homogenous element of degree d. Any element $m \in M$ can be written uniquely as $m = \sum_d m_d$ where each m_d is homogeneous of degree d and all but finitely many of the elements m_d are zero. A submodule $N \subset M$ is said to be a **graded submodule**, if $N = \bigoplus_{d=d_0}^{\infty}(M_d \cap N)$ is a graded module. Equivalently, N is a graded submodule of M if whenever $n \in N$ and $n = \sum_d n_d$ is the unique decomposition of n as a sum of homogeneous elements, then $n_d \in N$ for all d.

A specific instance of a graded R-module would be a homogeneous ideal I. Also, if N is a graded submodule of a graded module M, then there is a natural structure on M/N as a graded module. In this chapter we develop a homological method that is used to study algebraic properties of such modules by writing such modules as images of maps between free modules.

Let M be a finitely generated, graded R-module. Since M is a finitely generated R-module, it has a finite set of homogeneous generators $\{e_j\}$, for $j = 1, \ldots, r$. Let F_0 be a free R-module with the same number of generators $\{f_j\}$. Then there exists a unique surjective homomorphism

$$F_0 \to M \to 0$$

which sends $f_j \mapsto e_j$. Let E_0 be the kernel of this map. Thus $F_0/E_0 \cong M$. Since F_0 is finitely generated, and E_0 is a graded submodule of F_0, the module E_0 is also finitely generated. We can choose a finite set of homogeneous generators for E_0 and repeat the process to get a surjection from another free module F_1 to M_1. So we get the following exact sequence:

$$F_1 \stackrel{\phi_1}{\to} F_0 \stackrel{\phi_0}{\to} M \to 0 \tag{4.1}$$

Now we can find a finite set of homogeneous generators for the kernel of ϕ_1 and continue this process. The object of this chapter is to show that this chain of maps can be extended to give a "free resolution" of M which ends, after a finite number of steps, with a kernel that is itself a free module.

Definition 4.2. A **free resolution** of an $R-$module, M,

$$\to F_i \to F_{i-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

is an exact complex where each F_i is a **free** module for all $i \geq 0$. The **length** of this resolution is said to be n, if $F_n \neq 0$ and $F_i = 0$ for $i \geq n$.

Definition 4.3. Given a graded R-module M and an integer d we define the shifted module as $M(d) = \oplus_i M_i$ where $[M(d)]_i = [M]_{i+d}$.

We remark that as R-modules M and $M(d)$ are isomorphic and the difference is only in their gradings.

Lemma 4.4. *Let $R = k[X_1, \ldots, X_n]$ and let M be a graded R-module with a graded submodule N and let $f \in R$ be homogeneous of degree $d > 0$. If $M = N + fM$, then $M = N$.*

Proof. Suppose that $M \neq N$. Since N is a graded submodule of M, $N = \bigoplus_{d=d_0}^{\infty}(M_d \cap N)$. Let e be the smallest integer such that $M_e \cap N \neq M_e$ and let

$x \in M_e \setminus N$. By our assumption, $x = n_e + fm_{e-d}$ for some homogeneous elements $n_e \in N$, and $m_{e-d} \in M$. Now since $e - d < e$, by our choice of the element x, $m_{e-d} \in N \cap M_{e-d}$. But then $fm \in N$ and $x \in N$ which contradicts our choice of x. Hence $M = N$. □

Lemma 4.5. *If F is a finitely generated free R-module and I is an ideal of R, then F/IF is free over R/I.*

Proof. First recall from our notation with tensor products $F \cong R \otimes_R F$. Thus $F/IF \cong (R/I) \otimes_R F \cong (R/I) \otimes_{R/I} F$. □

We will also need the following lemma in the proof of the syzygy theorem.

Lemma 4.6. *Let N be a graded submodule of a finitely generated, graded, free module M over $R = k[X_1, \ldots, X_n]$, such that $\overline{N} = \frac{N}{\langle fN \rangle}$ is a free module over $R/\langle f \rangle$, for a homogeneous element $f \in R$ of positive degree. Then N is a free module.*

Proof. Let $\overline{e}_1, \ldots, \overline{e}_s$ be a homogeneous basis for $\overline{N}$. Then we can find homogeneous elements $e_1, \ldots, e_s \in M$, such that $\overline{e}_i = e_i + \langle fN \rangle \in \overline{N}$. We claim that the e_i form a basis for N as a free module. Suppose that e_i do not form a basis for N. Then there are relations among them of the form, $\sum g_i e_i = 0 \in N$ where the g_i are homogeneous polynomials. Choose a relation $\sum g_i e_i = 0$ where the degree of $\{g_i e_i \,|i = 1, \ldots r\}$ is the lowest possible. Since $\sum_i g_i \overline{e}_i = 0 \in \overline{N}$ and the $\overline{e}_i$ form a basis for $\overline{N}$ we have that for each i, $g_i = 0 \in R/\langle f \rangle$. Thus $g_i = fg_i'$ for some elements $g_i' \in R$. Now $\sum g_i e_i = f(\sum_i g_i' e_i) = 0 \in M$. Since M is a free module this implies that $\sum g_i' e_i = 0 \in M$. But the degree of the relation $\sum_i g_i' e_i = 0$ is lower than the degree of the relation $\sum_i g_i e_i = 0$ which contradicts the choice of this relation. Hence there is no such relation among the e_i, and the e_i form a basis for N. □

We are now ready to prove the main theorem of this chapter.

Theorem 4.7 (Hilbert's Syzygy)**.** *Let $R = k[X_1, \ldots, X_n]$ and let M be a finitely generated graded R-module. Then there exists a finite free resolution of M of length at most n.*

Proof. The proof is by induction on the number of variables n. In order for this to work we have to strengthen the conclusion of the statement of the theorem to assert that *any* free resolution of the module M has length at most n. More precisely, if we are given any exact complex of modules over R of the form:

$$0 \to E_n \to F_{n-1} \xrightarrow{\phi_{n-1}} F_{n-2} \cdots \to F_0 \xrightarrow{\phi_0} M \to 0 \tag{4.2}$$

where the F_i are free modules over R, a ring with n variables, and E_n is the kernel of ϕ_{n-1}, then E_n is a free module.

If $n = 0$ then $R = k$ and M is a vector space, which is a free module, so the inductive hypothesis holds. We now assume that the strengthened hypothesis is true for any module N over $k[X_1, \ldots, X_{n-1}]$. Now let $R = k[X_1, \ldots, X_n]$ and let M be a finitely generated R module. As remarked in the beginning of this section we can construct an exact complex of the form in equation (4.2). We need to show that E_n is a free module.

For each free module F_i we have an exact sequence

$$0 \to F_i(-1) \xrightarrow{\mu_i} F_i \xrightarrow{\pi_i} \overline{F}_i \to 0.$$

Here $F_i(-1)$ is the shifted module defined in 4.3, μ_i is the map corresponding to multiplication by X_n, and π_i is the canonical projection map. By Lemma 4.5, $\overline{F}_i$ is a free module over $\overline{R} = R/\langle X_n \rangle \cong k[X_1, \ldots X_{n-1}]$. To make the notation less cumbersome in the sequel, we define G_i to be $F_i(-1)$ for $i = 1, \ldots, n-1$, and

$G_n = E_n(-1)$. We also denote the maps $\phi_i(-1)$ by σ_i . Finally we let E_0 be the kernel of ϕ_0 and set $E_0(-1)$ to be G_0.

Thus we have the following diagram.

$$
\begin{array}{ccccccccccccc}
 & & 0 & & 0 & & 0 & & & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & G_n & \xrightarrow{\sigma_n} & G_{n-1} & \xrightarrow{\sigma_{n-1}} & G_{n-2} & \longrightarrow & \dots & \longrightarrow & G_1 & \xrightarrow{\sigma_1} & G_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mu_n} & & \downarrow{\scriptstyle \mu_{n-1}} & & \downarrow{\scriptstyle \mu_{n-2}} & & & & \downarrow{\scriptstyle \mu_1} & & \downarrow{\scriptstyle \mu_0} & & \\
0 & \longrightarrow & E_n & \xrightarrow{\phi_n} & F_{n-1} & \xrightarrow{\phi_{n-1}} & F_{n-2} & \longrightarrow & \dots & \longrightarrow & F_1 & \xrightarrow{\phi_1} & E_0 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_n} & & \downarrow{\scriptstyle \pi_{n-1}} & & \downarrow{\scriptstyle \pi_{n-2}} & & & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_0} & & \\
0 & \dashrightarrow & \overline{E}_n & \underset{\tau_n}{\dashrightarrow} & \overline{F}_{n-1} & \underset{\tau_{n-1}}{\dashrightarrow} & \overline{F}_{n-2} & \dashrightarrow & \dots & \dashrightarrow & \overline{F}_1 & \underset{\tau_1}{\dashrightarrow} & \overline{E}_0 & \dashrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & & & & 0 & & 0 & &
\end{array}
\tag{4.3}
$$

We first have to define the maps $\tau_i : \overline{F}_i \to \overline{F}_{i-1}$. If $\overline{x} \in \overline{F}_i$ then there exists an element $x \in F_i$ such that $\overline{x} = x + \text{image}(\mu_i)$. Then we define $\tau_i(\overline{x}) = \phi_i(x) + \text{image}(\mu_{i-1}) \in \overline{F}_{i-1}$. If $x + \text{image}(\mu_i) = y + \text{image}(\mu_i)$ for two elements $x, y \in F_i$, then $(x - y) \in \text{image}(\mu_i)$. So $(x - y) = \mu_i(g)$ for some element $g \in G_i$. So $\phi_i(x - y) = \phi_i(\mu_i(g)) = \mu_{i-1}(\sigma_i(g))$. So $\phi_i(x) + \text{image}(\mu_{i-1}) = \phi_i(y) + \text{image}(\mu_{i-1})$. Hence the maps τ_i are well defined.

Claim 4.8. *The bottom row in the above diagram is an exact sequence.*

1. Let $\overline{e}_0 \in \overline{E}_0$. So $\overline{e}_0 = e_0 + \text{image}(\mu_0)$ for some $e_0 \in E_0$. Since ϕ_1 is onto, there exists an element $f_1 \in F_1$ such that $\phi_1(f_1) = e_0$. Hence $\tau_1(f_1 + \text{image}(\mu_1)) = \overline{e}_0$ and τ_1 is onto.

2. Suppose $2 \leq i \leq n-1$. We will show that $\tau_i(\overline{F}_i)$ equals the kernel of τ_{i-1}. Since

$$\tau_{i-1}(\tau_i(x + \text{image}(\mu_i)) = \phi_{i-1}(\phi_i(x)) + \text{image}(\mu_{i-2})$$

and $\phi_{i-1} \circ \phi_i = 0$, the image of τ_i is contained in the kernel of τ_{i-1}. Suppose $\overline{f}_{i-1} \in \ker(\tau_{i-1})$. Let $\overline{f}_{i-1} = f_{i-1} + \text{image}(\mu_{i-1})$ for some element $f_{i-1} \in F_{i-1}$. So $\phi_{i-1}(f_{i-1}) \in \text{image}(\mu_{i-2})$. Hence there exists an element $g_{i-2} \in G_{i-2}$ such that $\phi_{i-1}(f_{i-1}) = \mu_{i-2}(g_{i-2})$. As we saw in the argument to show that τ_i is well defined, we observe that $\phi_{i-2}(\mu_{i-2}(g_{i-2})) = 0$. Hence $\mu_{i-3}(\sigma_{i-2}(g_{i-2})) = 0$ and since μ_{i-3} is injective, $\sigma_{i-2}(g_{i-2}) = 0$. Therefore there exists an element $g_{i-1} \in G_{i-1}$ such that $\sigma_{i-1}(g_{i-1}) = g_{i-2}$. So $\phi_{i-1}(\mu_{i-1}(g_{i-1})) = \phi_{i-1}(f_{i-1})$. Hence $\phi_{i-1}(f_{i-1} - \mu_{i-1}(g_{i-1})) = 0$ and since the second row of the diagram 4.3 is exact, we can find an element $f_i \in F_i$ such that $\phi_i(f_i) = f_{i-1} - \mu_{i-1}(g_{i-1})$. Now $\tau_i(f_i + \text{image}(\mu_i)) = \phi_i(f_i) + \text{image}(\mu_{i-1}) = \overline{f}_{i-1}$. Thus $\text{image}(\tau_i) = \ker(\tau_{i-1})$.

3. Finally we need to show that the map τ_n is injective. Suppose $\tau_n(\overline{e}_n) = 0 \in \overline{F}_{n-1}$. Then there exists an element $g_{n-1} \in G_{n-1}$ and an element $e_n \in E_n$ such that $\overline{e}_n = e_n + \text{image}(\mu_n)$ and $\phi_n(e_n) = \mu_{n-1}(g_{n-1})$. As we have seen before $\phi_{n-1}(\mu_{n-1}(g_{n-1})) = 0 = \mu_{n-2}(\sigma_{n-1}(g_{n-1}))$. Since μ_{n-2} is injective, $\sigma_{n-1}(g_{n-1}) = 0$. Therefore $g_{n-1} = \sigma_n(g_n)$ for some element $g_n \in G_n$. Since $\phi_n \circ \mu_n = \sigma_n \circ \mu_{n-1}$, $\phi_n(\mu_n(g_n)) = \phi_n(e_n)$. But ϕ_n is injective, so $e_n = \mu_n(g_n)$ and $\overline{e}_n = 0$. Hence τ_n is injective.

So the bottom row of diagram (4.3) is an exact sequence of $\overline{R}$-modules where $\overline{F}_i$ is free for $i = 1, \ldots, n-1$. Now using the inductive hypothesis $\overline{E}_n$ is free. We need to show that E_n is free. As $\overline{E}_n$ is free there is a finite basis, $\{\overline{e}_i\}_{i=1}^{r}$. Since π_n is surjective we can find $e_i \in E_n$ such that $\pi_n(e_i) = \overline{e}_i$ for each $i = 1, \ldots, r$. Let N be the submodule of E_n generated by $\{e_i\}_{i=1}^r$. Noting that $\overline{E}_n = \text{coker}(\mu_n)$ we can write $E_n = N + \mu(E_n) = N + X_n E_n$. By Lemma 4.4, $E_n = N$. Since $\overline{E}_n$ is free, Lemma 4.6 implies that E_n is free. □

This theorem is a powerful computational tool to study projective algebraic varieties because a lot of the geometric information about a projective variety is encoded in the free resolution of its homogeneous ideal. There are many computer algebra systems that can compute the free resolution of a module, usually homogeneous ideals, that are specified by giving its generators. We hope to study this in greater detail at a later stage.

REFERENCES

[1] Atiyah, M. and Macdonald, I. (1969). *Introduction to commutative algebra*. Addison Wesley Publishing Company.

[2] Benson, F. C. (2008). Split short exact sequences. Hand written notes given in answer to questions about exact sequences.

[3] Harris, J. (1995). *Algebraic geometry: a first course*. Graduate texts in mathematics ; 133. Springer, New York, corr. 3rd print. edition. Includes bibliographical references p. 314-315 and index.

[4] Hartshorne, R. (2000). *Algebraic geometry*. Graduate texts in mathematics: 52. Springer. xvi, 496 p. : ill. ; 25 cm. Includes index. Bibliography: p. 459-469.

[5] Hilton, P. and Wu, Y. (1989). *A Course in Modern Algebra*. Wiley-Interscience.

[6] Lang, S. (c2002). *Algebra*. Graduate texts in mathematics ; 211. Springer, New York, rev. 3rd ed. edition. Includes bibliographical references and index.

[7] Milne, J. S. (2008). Algebraic geometry (v5.10). Available at www.jmilne.org/math/.

[8] Perrin, D. (c2008). *Algebraic geometry: an introduction*. Universitext. SpringerEDP sciences, London. Includes bibliographical references and index.

[9] Vakil, R. (1999). Introduction to algebraic geometry, class 2. Lecture notes for course 725 at Massachusetts Institute of Technology fall 1999.