2003

Ideals, varieties, and Groebner bases

Joyce Christine Ahlgren

Follow this and additional works at: https://scholarworks.lib.csusb.edu/etd-project

Part of the Algebraic Geometry Commons

Recommended Citation

This Thesis is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.
IDEALS, VARIETIES, AND GROEBNER BASES

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

in

Mathematics

by

Joyce Christine Ahlgren

December 2003
ABSTRACT

Algebraic Geometry is the study of systems of polynomial equations in one or more variables. The solutions of a system of polynomial equations form a geometric object called an affine variety; the corresponding algebraic object is an ideal. There is a close connection between these objects, so a variety can be studied by studying the ideal of all polynomials that vanish on the variety.

We study one variable and multi-variable polynomials and some of the differences between them, specifically the ordering of polynomials and non-uniqueness of remainders in the division algorithm.

Given a specific system of polynomial equations we show how to construct a Groebner basis using Buchberger's Algorithm. Groebner bases have very nice properties, e.g. they do give a unique remainder in the division algorithm. We use these bases to solve systems of polynomial equations in several variables and to determine whether a function lies in the ideal.

We study Hilbert's Nullstellensatz Theorems to explore relationships between ideals and varieties over algebraically closed fields. We see that different ideals can generate the same variety and can even correspond to the empty variety. Hilbert's Nullstellensatz Theorem shows that if a polynomial vanishes at all points of some variety of an ideal then some power of the polynomial lies in the ideal. The Strong Nullstellensatz Theorem gives us a precise description of the ideal of a variety of an ideal: it is the "radical" of the ideal.
ACKNOWLEDGMENTS

My thanks to Dr. Davida Fischman without whose patience and understanding this project would never had been completed.

My thanks to my parents, Edward and Dorothy Ahlgren, without whose love and support my Master’s Degree would never had been completed.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>iii</td>
</tr>
<tr>
<td>ACKNOWLEDGMENTS</td>
<td>iv</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>vi</td>
</tr>
<tr>
<td>CHAPTER ONE: INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>CHAPTER TWO: VARIETIES</td>
<td>3</td>
</tr>
<tr>
<td>CHAPTER THREE: IDEALS IN $k[x_1, \ldots, x_n]$</td>
<td>8</td>
</tr>
<tr>
<td>CHAPTER FOUR: VARIETIES AND IDEALS</td>
<td>14</td>
</tr>
<tr>
<td>CHAPTER FIVE: POLYNOMIALS OF ONE VARIABLE</td>
<td>19</td>
</tr>
<tr>
<td>CHAPTER SIX: MULTI-VARIABLE POLYNOMIALS</td>
<td>27</td>
</tr>
<tr>
<td>CHAPTER SEVEN: GROEBNER BASES</td>
<td>35</td>
</tr>
<tr>
<td>CHAPTER 8: HILBERT'S NULLSTELLENSATZ THEOREMS</td>
<td>46</td>
</tr>
<tr>
<td>CHAPTER 9: SUMMARY</td>
<td>51</td>
</tr>
<tr>
<td>REFERENCES</td>
<td>52</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

Figure 1. Paraboloid of Revolution .................................................. 4
Figure 2. A Cone $\sqrt{z^2 - x^2 - y^2}$ for $z > 0$ ........................................... 6
Figure 3. The variety determined by $x^2 - y^2z^2 + z^3$ ......................... 6
Figure 4. The twisted cubic $V(y - x^2, z - x^3)$ ........................................ 7
Figure 5. Algebra and Geometry Analogues ........................................... 17
1 INTRODUCTION

Algebraic geometry is the study of solutions of systems of polynomial equations in one or more variables. In order to determine where polynomials vanish we will study a geometric object called an affine variety (Chapter Two), an algebraic object called an ideal (Chapter Three), and the relationship between them (Chapter Four). Varieties are curves and surfaces and higher dimensional objects defined by systems of polynomial equations. A variety can be studied by studying the ideal of all polynomials vanishing on the variety. These ideals are in the polynomial ring $k[x_1, \ldots, x_n]$. In order to link algebra and geometry, we will study polynomials over a field.

Throughout this paper, $k$ will denote a field. Examples of fields are the set of rational numbers, the set of real numbers and the set of complex numbers.

The polynomials we will consider are those in $n$ variables $x_1, \ldots, x_n$ with coefficients in an arbitrary field $k$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in $k$ is denoted by $k[x_1, \ldots, x_n]$. The set of all such polynomials is in fact not a field, although it satisfies all the field axioms except for the existence of multiplicative inverses; it is called a commutative ring. Prior to defining a polynomial, we need to define a monomial.

**Definition 1.1** A **monomial** in $x_1, \ldots, x_n$ is a product of the form $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. The **total degree** of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$. We denote $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. 

Definition 1.2 A polynomial \( f \) in variables \( x_1, \ldots, x_n \) with coefficients in a field \( k \) is a finite linear combination of monomials in \( x_1, \ldots, x_n \) with coefficients in \( k \).

A polynomial \( f \) will be written in the form \( f = \sum_{\alpha} a_{\alpha} x^\alpha \), where the sum is over a finite number of \( n \)-tuples \( \alpha = (\alpha_1, \ldots, \alpha_n) \).

There is a close relationship between ideals and the varieties they define. This relationship is one of the questions that will be investigated in this paper.

The following are the questions that will be investigated:

1. **Ideal Description Problem** Can a basis (a finite generating set) be found for every ideal in \( k[x_1, \ldots, x_n] \)?

2. **Ideal Membership Problem** Given an ideal in \( k[x_1, \ldots, x_n] \) and a polynomial \( f \), how can it be determined whether the polynomial \( f \) is an element of the ideal?

3. **Solve Systems of Polynomial Equations** Given a system of polynomial equations in several variables, how can the set of solutions of the system be determined?

4. **Variety and Ideal Relationship** What is the relationship between an ideal and its corresponding variety?

The major tool that will be used to answer these questions is a Groebner basis (Chapter Seven) and the results are described in several theorems, culminating in Hilbert’s Nullstellensatz Theorems (Chapter Eight).
2 VARIETIES

We begin by describing our basic geometric object of study, an affine variety. The variety of a set of polynomials in $n$ variables is the set of points in $n$-space that cause the polynomials to vanish. We will need to define a field prior to defining an affine variety.

**Definition 2.1** A field consists of a set $k$ and two binary operations "•" and "+" defined on $k$ for which the following conditions are satisfied:

(i) $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in k$ (the associative property).

(ii) $a + b = b + a$ and $a \cdot b = b \cdot a$ for all $a, b \in k$ (the commutative property).

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in k$ (the distributive property).

(iv) There are elements $0, 1 \in k$ such that $a + 0 = a \cdot 1 = a$ for all $a \in k$ (the additive and multiplicative identities).

(v) Given $a \in k$, there is an element $b \in k$ such that $a + b = 0$ (the additive inverse).

(vi) Given $a \in k, a \neq 0$, there exists an element $c \in k$ such that $a \cdot c = c \cdot a = 1$ (the multiplicative inverse).

Now we will define an affine variety.
Definition 2.2 Let \( k \) be a field, and let \( f_1, \ldots, f_s \) be polynomials in \( k[x_1, \ldots, x_n] \). Then we define

\[
V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n | f_i(a_1, \ldots, a_n) = 0 \ \forall \ 1 \leq i \leq s\}.
\]

We call \( V(f_1, \ldots, f_s) \) the **affine variety** defined by \( f_1, \ldots, f_s \).

Thus, an affine variety \( V(f_1, \ldots, f_s) \subset k^n \) is the set of all solutions of the system of equations \( f_1(a_1, \ldots, a_n) = \cdots = f_s(a_1, \ldots, a_n) = 0 \). A simple example is the variety \( V(x^2 + y^2 - 1) \), i.e. all the points satisfying \( x^2 + y^2 = 1 \). This variety is the set of points that yield the circle of radius 1 centered at the origin. A paraboloid of revolution \( V(z - x^2 - y^2) \), which is obtained by rotating the parabola \( z = x^2 \) about the \( z \)-axis is another example of an affine variety in three-dimensional space.

![Paraboloid of Revolution](image)

Figure 1. Paraboloid of Revolution

Some of the basic properties of affine varieties are that finite intersections and unions of affine varieties are again affine varieties. This can be seen by the following lemma.
Lemma 2.3 If $V, W \subset k^n$ are affine varieties, then so are $V \cap W$ and $V \cup W$.

Proof Suppose $V = V(f_1, \ldots, f_s)$ and $W = V(g_1, \ldots, g_t)$. We claim that $V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_t)$. To show this, let $V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \ \forall \ 1 \leq i \leq s\}$ and $V(g_1, \ldots, g_t) = \{(b_1, \ldots, b_n) \in k^n \mid g_j(b_1, \ldots, b_n) = 0 \ \forall \ 1 \leq j \leq t\}$. Then $V \cap W$ is a set of points, those that are both in $V$ and $W$, and so are the zeroes of $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$. Thus $V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_t)$, which implies that $V \cap W$ is an affine variety.

To show that $V \cup W$ is an affine variety, we show that $V \cup W = V(f_i g_j \mid 1 \leq i \leq s, \ 1 \leq j \leq t)$. Now if $(a_1, \ldots, a_n) \in V$, then $f_i(a_1, \ldots, a_n) = 0$ for all $i = 1, \ldots, s$. Since $k[x_1, \ldots, x_n]$ is commutative we have $f_i g_j(a_1, \ldots, a_n) = g_j f_i(a_1, \ldots, a_n)$. So $g_j f_i(a_1, \ldots, a_n) = g_j \cdot 0 = 0$ since $(a_1, \ldots, a_n) \in V$. Thus $V \subset V(f_i g_j)$. Similarly if $(b_1, \ldots, b_n) \in W$ then $g_j(b_1, \ldots, b_n) = 0$ for all $j = 1, \ldots, t$. Since $(b_1, \ldots, b_n) \in W$ we get $f_i g_j(b_1, \ldots, b_n) = f_i \cdot 0 = 0$. Thus $W \subset V(f_i g_j)$. Since $V \subset V(f_i g_j)$ and $W \subset V(f_i g_j)$ then $V \cup W \subset V(f_i g_j)$.

For the reverse inclusion, suppose $(a_1, \ldots, a_n) \in V(f_i g_j)$. If $(a_1, \ldots, a_n) \in V$ then we are done. Suppose $(a_1, \ldots, a_n) \notin V$, i.e. $f_{i_0}(a_1, \ldots, a_n) \neq 0$ for some $i_0 \in \{1, \ldots, s\}$. But for all $j$, $0 = f_{i_0} g_j(a_1, \ldots, a_n)$ since $(a_1, \ldots, a_n) \in V(f_i g_j)$. By the definition of multiplication in $k[x_1, \ldots, x_n]$, $0 = f_{i_0}(a_1, \ldots, a_n) g_j(a_1, \ldots, a_n)$. Since $f_{i_0}(a_1, \ldots, a_n) \neq 0$, then $0 = g_j(a_1, \ldots, a_n)$ for all $j = 1, \ldots, t$. Thus $(a_1, \ldots, a_n) \in W$ and so $V(f_i g_j) \subset V \cup W$. Hence $V \cup W$ is a variety. \qed
In a similar fashion it is proved that any finite union or intersection of affine varieties are again affine varieties. For example, consider \( V, W, X \subset k^n \); we know that \( V \cup W \) is a variety, by Lemma 2.3. If we let \( Z = V \cup W \) then \( Z \) is a variety. Then we can show that \( Z \cup X \) is a variety, by above. Thus \( V \cup W \cup X \) is a variety. Similarly it follows from Lemma 2.3 and induction that any finite union or intersection of affine varieties is again an affine variety.

Here are some more examples of affine varieties:

![Figure 2. A Cone \( \sqrt{z^2 - x^2 - y^2} \) for \( z > 0 \)](image)

![Figure 3. The variety determined by \( x^2 - y^2z^2 + z^3 \)](image)
Figure 4. The twisted cubic $V(y - x^2, z - x^3)$
3 IDEALS IN $k[x_1, \ldots, x_n]$

We now turn to our other main object of study, ideals in $k[x_1, \ldots, x_n]$. We will see ways in which ideals relate to affine varieties in Chapter Four.

Definition 3.1 A subset $I \subset k[x_1, \ldots, x_n]$ is an ideal if it satisfies:

(i) $0 \in I$;

(ii) If $f, g \in I$, then $f + g \in I$;

(iii) If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$.

The definition of an ideal reminds us of a subspace in linear algebra. Both are closed under addition. Both are closed under multiplication, with the difference that scalars are used as coefficients for multiplication in a subspace whereas in an ideal polynomials are used as coefficients for multiplication. We will see that the ideal generated by a set of polynomials is similar to the span of the vectors in a subspace since they are both generated by linear combinations - on one hand of polynomials, and on the other of vectors.

Definition 3.2 Let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then we define

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}.$$ 

$I = \langle f_1, \ldots, f_s \rangle$ is called the ideal generated by $f_1, \ldots, f_s$, and $\{f_1, \ldots, f_s\}$ is called a basis of the ideal.

We will justify this definition by showing that $I = \langle f_1, \ldots, f_s \rangle$ is an ideal.
Lemma 3.3 If \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \), then \( I = \langle f_1, \ldots, f_s \rangle \) is an ideal of \( k[x_1, \ldots, x_n] \).

Proof First \( 0 \in I = \langle f_1, \ldots, f_s \rangle \) because \( 0 = \sum_{i=1}^{s} 0 \cdot f_i \). Next suppose that \( f, g \in I \) and \( p_1, \ldots, p_s, q_1, \ldots, q_s \in k[x_1, \ldots, x_n] \) such that \( f = \sum_{i=1}^{s} p_i f_i \) and \( g = \sum_{i=1}^{s} q_i f_i \). Then \( f + g = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i = \sum_{i=1}^{s} (p_i + q_i) f_i \in I \). Next, let \( h \in k[x_1, \ldots, x_n] \), then \( h f = h \sum_{i=1}^{s} p_i f_i = \sum_{i=1}^{s} (h p_i) f_i \in I \). Thus \( I = \langle f_1, \ldots, f_s \rangle \) is an ideal. \( \square \)

If \( I \) is an ideal such that \( I \subset k[x_1, \ldots, x_n] \) and if \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \), then the following statements are equivalent.

(i) \( f_1, \ldots, f_s \in I \)

(ii) \( \langle f_1, \ldots, f_s \rangle \subset I \).

This fact is useful if we want to show one ideal is contained in another. For example, if we want to show \( \langle x + y, x - y \rangle = \langle x, y \rangle \). We know that \( x + y = 1 \cdot x + 1 \cdot y \in \langle x, y \rangle \) and \( x - y = 1 \cdot x + (-1) \cdot y \in \langle x, y \rangle \). Thus \( \langle x + y, x - y \rangle \subset \langle x, y \rangle \). Similarly \( x = \frac{1}{2} (x + y) + \frac{1}{2} (x - y) \in \langle x + y, x - y \rangle \) and \( y = \frac{1}{2} (x + y) + \frac{-1}{2} (x - y) \in \langle x + y, x - y \rangle \). Thus \( \langle x, y \rangle \subset \langle x + y, x - y \rangle \). So \( \langle x + y, x - y \rangle = \langle x, y \rangle \).

We are particularly interested in situations in which the ideal is generated by a finite set of polynomials.

Definition 3.4 An ideal \( I \subset k[x_1, \ldots, x_n] \) is finitely generated if there exist polynomials \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \) such that \( I = \langle f_1, \ldots, f_s \rangle \) and so \( \{ f_1, \ldots, f_s \} \) is a basis of \( I \).
In general, ideals in (commutative or non-commutative) rings do not have finite bases. However, we will see in Chapter Six that, similar to the one-variable case, every ideal of \( k[x_1, \ldots, x_n] \) is finitely generated. Although a given ideal may have many different bases, we will study an especially useful one, called a Groebner basis.

Now we will study ideals.

**Definition 3.5** An ideal \( I \subset k[x_1, \ldots, x_n] \) is a **monomial ideal** if there is a subset \( A \subset \mathbb{Z}^n \) (possibly infinite) such that \( I \) consists of all polynomials which are finite sums of the form \( \sum_{\alpha \in A} h_\alpha x^\alpha \), where \( h_\alpha \in k[x_1, \ldots, x_n] \). In this case, we write \( I = \langle x^\alpha : \alpha \in A \rangle \).

An example of a monomial ideal is \( I = \langle x^4 y^2, x^3 y^4, x^2 y^5 \rangle \subset k[x, y] \).

How can we characterize all the monomials that are elements of a given monomial ideal?

**Lemma 3.6** Let \( I = \langle x^\alpha : \alpha \in A \rangle \) be a monomial ideal. Then a monomial \( x^\beta \) lies in \( I \) if and only if \( x^\beta \) is divisible by \( x^\alpha \) for some \( \alpha \in A \).

**Proof** If \( x^\beta \) is a multiple of \( x^\alpha \) for some \( \alpha \in A \), then \( x^\beta \in I \) by the definition of ideal. Conversely, if \( x^\beta \in I \), then \( x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)} \), where \( h_i \in k[x_1, \ldots, x_n] \) and \( \alpha(i) \in A \). If we expand each \( h_i \) as a linear combination of monomials, we see that every term on the right side of the equation is divisible by some \( x^{\alpha(i)} \). Hence, the left side \( x^\beta \) must have the same property. \( \square \)

To see if a given polynomial \( f \) lies in a monomial ideal, we need to look at the monomials of \( f \).
Lemma 3.7 Let $I$ be a monomial ideal, and let $f \in k[x_1, \ldots, x_n]$. Then the following are equivalent:

(i) $f \in I$.

(ii) Every term of $f$ lies in $I$.

(iii) $f$ is a $k$-linear combination of the monomials in $I$.

Proof If $f$ is a $k$-linear combination of the monomials in $I$, then every term of $f$ lies in $I$ and $f \in I$. So now consider $f \in I$ where $I$ is a monomial ideal. Since $I$ is a monomial ideal, then $I$ consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$ for some $h_\alpha \in k[x_1, \ldots, x_n]$. Thus $f$ is a $k$-linear combination of monomials in $I$. □

An immediate consequence of part (iii) of the Lemma is that a monomial ideal is uniquely determined by its monomials.

Corollary 3.8 Two monomials ideal are the same if and only if they contain the same monomials.

We can now prove all monomial ideals of $k[x_1, \ldots, x_n]$ are finitely generated.

Theorem 3.9 (Dickson's Lemma) A monomial ideal $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \ldots, x_n]$ can be written down in the form $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, where $\alpha(1), \ldots, \alpha(s) \in A$. In particular, $I$ has a finite basis.
Proof  Proof by induction on $n$, the number of variables.

If $n = 1$, then $I$ is generated by the monomials $x^\alpha$, where $\alpha \in A \subset \mathbb{Z}^n$. Let $B$ be the smallest element of $A$. There is a smallest element due to the well-ordering of integers. Then $B \leq \alpha$ for all $\alpha \in A$, so that $x_1^B$ divides all other generators $x_1^\alpha$. Thus $I = \langle x_1^B \rangle$.

Suppose $n > 1$ and the hypothesis holds for $n - 1$. So we will write variables as $x_1, \ldots, x_n, y$. So the monomials in $k[x_1, \ldots, x_{n-1}, y]$ can be written as $x^\alpha y^m$, where $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{Z}^{n-1}$ and $m \in \mathbb{Z}$. Suppose that $I \subset k[x_1, \ldots, x_{n-1}, y]$ is a monomial ideal. To find finite generators of $I$, let $J$ be the ideal in $k[x_1, \ldots, x_{n-1}]$ such that $J = \{ x^\alpha \mid \exists m \mid x^\alpha y^m \in I \}$. Since $J$ is a monomial ideal in $k[x_1, \ldots, x_{n-1}]$, then by the induction hypothesis, $J$ has a finite basis say $x^\alpha(1), \ldots, x^\alpha(s)$. So for each $i = 1, \ldots, s$ there exists some $m_i$ such that $x^\alpha(i)y^{m_i} \in I$. Let $m = \max\{m_1, \ldots, m_s\}$. For $k = 0, 1, \ldots, m - 1$ set $J_k = \langle x^\beta \mid x^\beta y^k \in I \rangle \subset k[x_1, \ldots, x_{n-1}]$. Again using the induction hypothesis, each $J_k$ has a finite generating set of monomials, say $J_k = \langle x^\alpha(1), \ldots, x^\alpha(S_k) \rangle$.

Claim: $I$ is generated by the union of all the following monomials:

$$G = \{ x^\alpha(1)y^m, \ldots, x^\alpha(S)y^m, x^\alpha(1)y^0, \ldots, x^\alpha(S_0)y^0, \}
\quad x^{\alpha_1(1)}y^1, \ldots, x^{\alpha_1(S_1)}y^1, \ldots, x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(S_{m-1})}y^{m-1} \}$$

The monomials of $I$ are in $\langle G \rangle$, i.e. every monomial in $I$ is a multiple of one of the monomials in $G$. This is because if $x^\beta y^p \in I$ then $x^\beta \in J$, by the definition of $J$. If $p \leq m - 1$, then $x^\beta y^p \in J_p$ and so $x^\beta y^p \in \langle G \rangle$. If $p \geq m$, then $x^\beta y^p = (x^\beta y^m)y^{p-m}$ and since $x^\beta y^m \in J$, then $(x^\beta y^m)y^{p-m} \in J$ and $x^\beta y^p \in J$. 

12
Thus $x^\beta y^p \in \langle G \rangle$. Clearly every monomial in $\langle G \rangle$ is in $I$ by the choice of $G$, so $I$ and $\langle G \rangle$ contain the same monomials. So by Corollary 3.8, $I = \langle G \rangle$ and thus $I$ has a finite set of generators that are monomials. Now we need to show that the finite basis of $I$ is a subset of the original generating set. We know that there is a finite set of monomial generators, say $x^{\beta(1)}, \ldots, x^{\beta(t)}$ for $I$. But then

$\forall i = 1, \ldots, t$, there exists an $x^{\beta(i)} \in I = \langle x^\alpha \mid \alpha \in A \rangle$, and by Lemma 3.6 this forces each $x^{\beta(i)}$ to be divisible by an $x^{\alpha(i)}$. We now claim that

$I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)} \rangle$. First $\langle x^{\alpha(1)}, \ldots, x^{\alpha(t)} \rangle \subset \langle x^\alpha \mid \alpha \in A \rangle = I$. For the other direction, let $x^\gamma$ be a monomial in $I$. Then $x^\gamma$ is divisible by an $x^{\beta(i)}$, which in turn is divisible by $x^{\alpha(i)}$. So $x^\gamma$ is divisible by $x^{\alpha(i)}$. Then $x^\gamma \in \langle x^{\alpha(1)}, \ldots, x^{\alpha(t)} \rangle$ and so $I \subset \langle x^{\alpha(i)}, \ldots, x^{\alpha(t)} \rangle$ and so we are done. □
4 VARIETIES AND IDEALS

The relationship between varieties and ideals is very useful, as ideals can be used to compute affine varieties. We now show that a variety depends only on the ideal generated by its defining equations, not on any specific basis of the ideal.

Proposition 4.1 If \( f_1, \ldots, f_s \) and \( g_1, \ldots, g_t \) are bases of the same ideal in \( k[x_1, \ldots, x_n] \) (so that \( \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle \)), then
\[
V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t).
\]

Proof We wish to show that \( V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t) \), where
\[
V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \mid f_i(a_1, \ldots, a_n) = 0 \ \forall \ 1 \leq i \leq s \}\text{ and }
V(g_1, \ldots, g_t) = \{(b_1, \ldots, b_n) \in k^n \mid g_i(b_1, \ldots, b_n) = 0 \ \forall \ 1 \leq j \leq t \}.
\]

Consider \( (h_1 f_1 + \cdots + h_s f_s)(a_1, \ldots, a_n) \) for some \( h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \). Since \( a_1, \ldots, a_n \) is a point where \( f_i \) vanishes, \( (h_1 f_1 + \cdots + h_s f_s)(a_1, \ldots, a_n) = 0. \) But since \( \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle \), then there exist \( j_1, \ldots, j_t \) such that
\[
h_1 f_1 + \cdots + h_s f_s = j_1 g_1 + \cdots + j_t g_t\text{ so } (j_1 g_1 + \cdots + j_t g_t)(a_1, \ldots, a_n) = 0. \]
Thus \( V(g_1, \ldots, g_t) \subseteq V(f_1, \ldots, f_s) \). Similarly consider \( (j_1 g_1 + \cdots + j_t g_t)(b_1, \ldots, b_n) \) for some \( j_1, \ldots, j_s \in k[x_1, \ldots, x_n] \). Since \( b_1, \ldots, b_n \) is a point where \( g_i \) vanishes,
\[
(j_1 g_1 + \cdots + j_t g_t)(b_1, \ldots, b_n) = 0. \text{ But } h_1 f_1 + \cdots + h_s f_s = j_1 g_1 + \cdots + j_t g_t \text{ so }
(h_1 f_1 + \cdots + h_s f_s)(b_1, \ldots, b_n) = 0. \text{ Thus } V(f_1, \ldots, f_s) \subseteq V(g_1, \ldots, g_t). \text{ So }
V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t). \]

Thus the basis of an ideal can change without affecting the variety of the ideal. By choosing a particular kind of basis, a Groebner basis, determining the
variety can be made easier. This we see in Chapter Seven, when we study this basis.

Suppose \( V = V(f_1, \ldots, f_s) \subseteq k^n \) where \( f_1, \ldots, f_s \in k[x_1, \ldots, x_n] \). We know that \( f_1, \ldots, f_n \) vanish on \( V \). Are there other polynomials that also vanish on \( V \)? If so, how do we find them? We will now investigate the set of all polynomials that vanish on a given variety.

**Definition 4.2** Let \( V \subseteq k^n \) be an affine variety. Then we set

\[
I(V) = \{ f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \ \forall \ (a_1, \ldots, a_n) \in V \}
\]

We first verify that \( I(V) \) is an ideal.

**Lemma 4.3** If \( V \subseteq k^n \) is an affine variety, then \( I(V) \subseteq k[x_1, \ldots, x_n] \) is an ideal. \( I(V) \) is called the **ideal of** \( V \).

**Proof** \( 0 \in I(V) \) since the zero polynomial vanishes on all of \( k^n \), so in particular it vanishes on \( V \). To verify closure under addition, suppose \( f, g \in I(V) \) and \( (a_1, \ldots, a_n) \in V \). Then

\[
(f + g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0
\]

so \( f + g \in I(V) \). For closure under multiplication, suppose \( f \in I(V) \) and \( h \in k[x_1, \ldots, x_n] \), then

\[
(hf)(a_1, \ldots, a_n) = h(a_1, \ldots, a_n)f(a_1, \ldots, a_n) = [h(a_1, \ldots, a_n)](0) = 0
\]

so \( hf \in I(V) \). Thus \( I(V) \) is an ideal. \( \square \)

We have seen two ways in which ideals can be constructed in \( k[x_1, \ldots, x_n] \). They can be constructed by considering the set of linear
combinations of the polynomials \( f_1, \ldots, f_s \) with coefficients, which are polynomials, in the polynomial ring. They can also be constructed by starting with an affine variety, and then constructing \( I(V) \) which is the set of polynomials that vanish on all points of \( V \). We have just shown that \( I(V) \) is an ideal.

The chart on the next page illustrates some of the relationships between varieties and their ideals. We see that starting with a set of polynomials we can generate an ideal directly from them or we can consider the set of points that cause each of the polynomials to vanish. We then construct the variety that arises from the intersection of the curves/surfaces created by the points. From there we construct the ideal of the variety which is the set of polynomials whose zeroes are the variety. The question as to what the relationship is between the ideal constructed directly from the polynomials, and that constructed via their variety, is the focus of the Nullstellensatz Theorems.
Algebra

Polynomials
\{f_1, \ldots, f_s\}

\rightarrow

Ideal: set of polynomials generated by \{f_1, \ldots, f_s\}:
\[ J = \langle f_1, \ldots, f \rangle \]

\Updownarrow

Relationship?

Ideal of the variety: set of polynomials whose zeros are precisely \(V\):
\[ I(V(f_1, \ldots, f)) \]

Geometry

Zeros: points \((a_1, \ldots, a_n)\) such that
\[ f_i(a_1, \ldots, a_n) = 0 \]

\rightarrow

Variety: Intersection of curves/surfaces created by these points.
\[ V = V(f_1, \ldots, f_s) = V(J) \]

Figure 5. Algebra and Geometry Analogues
We now can show that although $I(V(f_1, \ldots, f_s))$ may not equal $(f_1, \ldots, f_s)$ the ideal of a variety always determines the variety uniquely.

**Proposition 4.4** Let $V$ and $W$ be affine varieties in $k^n$. Then:

1. (i) $V \subseteq W$ if and only if $I(W) \subseteq I(V)$.

2. (ii) $V = W$ if and only if $I(V) = I(W)$.

**Proof**

1. (i) Suppose $V \subseteq W$ and let $f \in I(W)$. Since $W$ is an affine variety, then $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in W$. Since $V \subseteq W$, any polynomial vanishing on $W$ must vanish on $V$. So $f \in I(V)$. Thus $I(W) \subseteq I(V)$. For the converse, suppose $I(W) \subseteq I(V)$, i.e. if $f \in I(W)$ then $f \in I(V)$. Let $v \in V$, then for every $f \in I(V)$, $f(v) = 0$. Thus $f \in I(W)$. Since $I(W) \subseteq I(V)$ then $f \in I(V)$. Thus $f(v) = 0$. Since this is true, we have shown that for every $f \in I(W)$, $v \in W$. Thus $V \subseteq W$.

2. (ii) $V = W$ implies $V \subseteq W$ and $W \subseteq V$. By part (i), $I(W) \subseteq I(V)$ and $I(V) \subseteq I(W)$ which implies $I(V) = I(W)$. Similarly, $I(V) = I(W)$ implies $I(V) \subseteq I(W)$ and $I(W) \subseteq I(V)$ which implies $W \subseteq V$ and $V \subseteq W$. Thus $V = W$.

□
5 POLYNOMIALS OF ONE VARIABLE

Prior to studying multi-variable polynomials, we will study the case of one variable polynomials. When dealing with a polynomial in one variable, the familiar division algorithm and concept of greatest common divisor are used to determine the structure of ideals of $k[x]$.

In order to discuss the division algorithm for polynomials in $k[x]$, we must understand the concept of the leading term of a polynomial in one variable.

**Definition 5.1** Given a nonzero polynomial $f \in k[x]$, let

$$f = a_0x^m + a_1x^{m-1} + \cdots + a_m,$$

where $a_i \in k$ and $a_0 \neq 0$ (thus $m = \deg(f)$). Then we say that $a_0x^m$ is the **leading term** of $f$, written $\text{LT}(f) = a_0x^m$.

Now we can state the division algorithm.

**Proposition 5.2 (The Division Algorithm)** Let $k$ be a field and let $g$ be a nonzero polynomial in $k[x]$. Then every $f \in k[x]$ can be written as $f = qg + r$ where $q, r \in k[x]$, and either $r = 0$ or $\deg(r) < \deg(g)$. Furthermore, $q$ and $r$ are unique, and there is an algorithm for finding $q$ and $r$.

**Proof** First we show existence of $q$ and $r$. If $f = 0$, then $q = 0$ and $r = 0$. If $\deg(f) < \deg(g)$, then choose $q = 0$ and $r = f$. Now if $n = \deg(f) \geq \deg(g) = m$, then denote $f = a_nx^n + \cdots + a_0$ and $g = b_mx^m + \cdots + b_0$ and use long division and induction on $\deg(f)$ to prove the proposition. Note that $b_m \neq 0$, and let $f_1 = f - a_n(b_m)^{-1}x^{n-m}g$. Then
$f_1(x) = 0$ or $\deg(f_1) < \deg(f)$. So by the induction hypothesis, there exists $q_1$ and $r_1$ in $k$ such that $f_1 = gq_1 + r_1$ where $r_1 = 0$ or $\deg(r_1) < \deg(g)$. Thus

\[
f = a_n(b_m)^{-1}x^{n-m}g + f_1
\]

\[
f = a_n(b_m)^{-1}x^{n-m}g + q_1g + r_1
\]

\[
f = [a_n(b_m)^{-1}x^{n-m} + q_1]g + r_1
\]

So $q = a_n(b_m)^{-1}x^{n-m} + q_1$ and $r = r_1$ have the desired properties.

To prove uniqueness, suppose $f = qg + r$ and $f = q'g + r'$ where $r = 0$ or $\deg(r) < \deg(g)$ and $r' = 0$ or $\deg(r') < \deg(g)$. Subtracting the two equations, we obtain

\[
0 = qg + r - q'g - r'
\]

\[
0 = g(q - q') + (r - r')
\]

\[
r - r' = g(q' - q)
\]

If $r \neq r'$, then $\deg(r - r') < \deg(g)$ since $\deg(r) < \deg(g)$ and $\deg(r') < \deg(g)$. But by above,

\[
\deg(r - r') = \deg(g(q' - q))
\]

\[
\deg(r - r') = \deg(g) + \deg(q' - q)
\]

\[
\deg(r - r') \geq \deg(g)
\]

But this is a contradiction because $\deg(r - r')$ cannot be less than and greater than or equal to $\deg(g)$. So $r = r'$. If $r = r'$, then $r - r' = 0$. And from this it follows that $q = q'$.
We will use this division algorithm to determine the structure of all ideals in \( k[x] \).

**Corollary 5.3** If \( k \) is a field, then every ideal of \( k[x] \) can be written in the form \( \langle f \rangle \) for some \( f \in k[x] \). Furthermore, \( f \) is unique up to multiplication by a nonzero constant in \( k \).

**Proof** To prove existence, let \( I \subset k[x] \) be an ideal. If \( I = \{0\} \), then \( I = \langle 0 \rangle \) and we are done. If \( I \neq \{0\} \), then \( I \) contains an element of minimal degree since otherwise for any nonzero polynomial in \( I \), we can choose one of smaller degree, thus creating an infinite sequence of polynomials of decreasing degrees. This is impossible since \( k[x] \) has only elements of non-negative degree. So let \( f \in I \) such that \( f \) is a nonzero polynomial of minimal degree. Claim \( \langle f \rangle = I \). Now, \( f \in I \) implies \( \langle f \rangle \subset I \) because \( I \) is an ideal. For the reverse inclusion, let \( g \in I \), then by the division algorithm, \( g = qf + r \) for some \( q, r \in k[x] \) where \( r = 0 \) or \( \deg(r) < \deg(f) \). Since \( I \) is an ideal and \( f \in I \), then \( qf \in I \). Since \( r = g - qf \) and \( gf \in I \) and \( g \in I \), then \( g - qf \in I \) which implies \( r \in I \). If \( r \neq 0 \), then \( \deg(r) < \deg(f) \) but \( f \) was chosen to be of minimal degree. So this is a contradiction. Thus \( r = 0 \), so \( g = qf \) which implies \( g = qf \in \langle f \rangle \) and thus \( g \in \langle f \rangle \). Thus \( I \subset \langle f \rangle \). So \( \langle f \rangle = I \).

To prove uniqueness, suppose \( \langle f \rangle = \langle g \rangle \). Then \( f \in \langle g \rangle \) which implies there exists \( h \), a polynomial, such that \( f = hg \). Thus \( \deg(f) = \deg(h) + \deg(g) \). So \( \deg(f) \geq \deg(g) \). Similarly, if \( \langle f \rangle = \langle g \rangle \), then \( g \in \langle f \rangle \) which implies there exists \( j \), a polynomial, such that \( g = jf \). Thus \( \deg(g) = \deg(j) + \deg(f) \). So \( \deg(g) \geq \deg(f) \). Thus \( \deg(f) \geq \deg(g) \) and \( \deg(g) \geq \deg(f) \) implies
deg(f) = deg(g). So deg(h) = 0 and deg(j) = 0 which implies h and j are nonzero constants.

Thus f is unique up to multiplication by a nonzero constant, and so a generator of an ideal in \( k[x] \) is the nonzero polynomial of minimal degree contained in the ideal. An ideal generated by one element is called a **principal ideal**. Thus we can say, due to Corollary 5.3, \( k[x] \) is a **principal ideal domain**. At this point it is not yet practical to find a generator of a given ideal, because it would require checking the degrees of all the polynomials in the ideal to determine the minimal degree polynomial and there are infinitely many polynomials in an ideal. But to find the generator of an ideal in \( k[x] \), all we need to do is to find the greatest common divisor.

**Definition 5.4** A **greatest common divisor** of polynomials \( f, g \in k[x] \) is a polynomial \( h \) such that:

(i) \( h \) divides \( f \) and \( g \).

(ii) If \( p \) is another polynomial which divides \( f \) and \( g \), then \( p \) divides \( h \).

When \( h \) has these properties, we write \( h = \gcd(f, g) \).

**Proposition 5.5** Let \( f_1, \ldots, f_s \in k[x] \), where \( s \geq 2 \). Then:

(i) \( \gcd(f_1, \ldots, f_s) \) exists and is unique up to multiplication by a nonzero constant in \( k \).

(ii) \( \gcd(f_1, \ldots, f_s) \) is a generator of the ideal \( \langle f_1, \ldots, f_s \rangle \).
(iii) If \( s \geq 3 \), then \( \gcd(f_1, \ldots, f_s) = \gcd(f_1, \gcd(f_2, \ldots, f_s)) \).

(iv) There is an algorithm for finding \( \gcd(f_1, \ldots, f_s) \).

Proof

(i) Consider the ideal \( \langle f_1, \ldots, f_s \rangle \). Since every ideal of \( k[x] \) is principal, there exists an \( f \) such that \( \langle f \rangle = \langle f_1, \ldots, f_s \rangle \). Claim: \( f \) is a gcd of \( \{f_1, \ldots, f_s\} \).

First note that \( f \) divides each \( f_i \) for all \( 1 \leq i \leq s \) because \( f_i \in \langle f \rangle \). Thus the first part of Definition 5.4 is satisfied. Now suppose \( g \in k[x] \) divides each \( f_i \) for all \( 1 \leq i \leq s \). Thus \( f_i = h_i g \) for some \( h_i \in k[x] \) for all \( 1 \leq i \leq s \). Since \( f \in \langle f_1, \ldots, f_s \rangle \), there exist some \( j_i \) such that \( f = \sum_{i=1}^{s} j_i f_i \). Thus \( f = \sum j_i f_i = \sum j_i (h_i g) = (\sum j_i h_i) g \) which shows that \( g \) divides \( f \). The second part of Definition 5.4 is satisfied. Thus \( f = \gcd(f_1, \ldots, f_s) \). To prove uniqueness, suppose \( f' \) is another gcd of \( \{f_1, \ldots, f_s\} \). Then by the second part of Definition 5.4, \( f \) and \( f' \) would divide each other. Thus \( f \) is a nonzero constant multiple of \( f' \) since they divide each other.

(ii) By the way we defined \( f \) as \( f = \gcd(f_1, \ldots, f_s) \), \( f \) is a generator of the ideal \( \langle f_1, \ldots, f_s \rangle \).

(iii) Let \( h = \gcd(f_2, \ldots, f_s) \). By part (ii), this implies \( \langle h \rangle = \langle f_2, \ldots, f_s \rangle \) since a generator \( h \) is the gcd of \( f_2, \ldots, f_s \) for \( \langle f_2, \ldots, f_s \rangle \) is the gcd of \( f_2, \ldots, f_s \). So now we wish to show \( \langle f_1, h \rangle = \langle f_1, f_2, \ldots, f_s \rangle \). Consider \( \langle f_1, \ldots, f_s \rangle \). By
Since \( h \) is \( \gcd(f_2, \ldots, f_s) \) then \( h \neq 0 \) and it divides \( f_2, \ldots, f_s \). Thus
\[
\langle f_1, f_2, \ldots, f_s \rangle \subset \langle f_1, h \rangle.
\]
Now consider
\[
\langle f_1, h \rangle = \{ \sum_{i=1}^{s} j_i f_i + lh \mid j, l \in k[x] \}.
\]
We know \( \langle h \rangle = \langle f_2, \ldots, f_s \rangle \). The gcd can be written as a linear combination of \( f_2, \ldots, f_s \). This is because \( h \in \langle h \rangle \). This implies \( h \in \langle f_2, \ldots, f_s \rangle \) since \( \langle h \rangle = \langle f_2, \ldots, f_s \rangle \). Therefore \( h \in \langle f_2, \ldots, f_s \rangle \) implies \( h = j_2 f_2 + \cdots + j_s f_s \) where \( j_2, \ldots, j_s \in k[x] \). So
\[
\langle f, h \rangle = \{ j_1 f_1 + lh \mid l \in k[x] \}
\]
\[
\langle f, h \rangle = \{ j_1 f_1 + j_2 f_2 + \cdots + j_s f_s \mid j_k \in k[x] \}
\]
Therefore, \( \langle f, h \rangle \subset \langle f_2, \ldots, f_s \rangle \). Thus \( \langle f, h \rangle = \langle f_2, \ldots, f_s \rangle \).

(iv) To prove the algorithm for finding \( \gcd(f_1, \ldots, f_s) \) combine part (iii) with the Euclidean Algorithm. (we will not prove this here).

Rather than prove the algorithm we will do an example showing how the algorithm works.
Example 5.6 Here we determine the greatest common divisor for the ideal 
\( \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle \subset k[x] \). First determine \( \gcd(x^4 - 1, x^6 - 1) \). By the division algorithm, 
\( x^4 - 1 = 0(x^6 - 1) + 1(x^4 - 1) \) and \( x^6 - 1 = x^2(x^4 - 1) + x^2 - 1 \). But
\[
\begin{align*}
x^4 - 1 &= (x^2 + 1)(x^2 - 1) \\
x^4 - 1 &= (x^2 + 1)(x - 1)(x + 1)
\end{align*}
\]
and
\[
\begin{align*}
x^6 - 1 &= x^2(x^4 - 1) + x^2 - 1 \\
x^6 - 1 &= x^2(x^2 + 1)(x^2 - 1) \\
x^6 - 1 &= (x^2 - 1)[x^2(x^2 + 1) + 1] \\
x^6 - 1 &= (x + 1)(x - 1)[x^2(x^2 + 1) + 1]
\end{align*}
\]
Thus \( \gcd(x^4 - 1, x^6 - 1) = (x^2 - 1) = (x + 1)(x - 1) \). Now consider
\( \gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) \). By part (iii),
\[
\begin{align*}
\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \gcd(x^3 - 3x + 2, \gcd(x^4 - 1, x^6 - 1)) \\
\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \gcd(x^3 - 3x + 2, x^2 - 1) \\
\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= \gcd((x - 1)(x - 1)(x + 2), (x - 1)(x + 1)) \\
\gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) &= x - 1
\end{align*}
\]
By Proposition 5.5 (ii), the \( \gcd(x^3 - 3x + 2, x^4 - 1, x^6 - 1) \) is a generator of the ideal \( \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle \). Thus \( \langle x^3 - 3x + 2, x^4 - 1, x^6 - 1 \rangle = (x - 1) \).
In order to determine whether a polynomial lies in an ideal, we first need to determine a generator. Then we can use the generalized division algorithm to see if a polynomial is in the ideal generated by the gcd.

**Example 5.7** Is \( x^3 + 4x^2 + 3x - 7 \) an element of \( (x^3 - 3x + 2, x^4 - 1, x^6 - 1) \)?

Since \( x - 1 \) is a generator of this ideal, we can now ask if \( x^3 + 4x^2 + 3x - 7 \) is an element of \( (x - 1) \)? Using the division algorithm, we find

\[
x^3 + 4x^2 + 3x - 1 = (x^2 + 5x + 8)(x - 1) + 1.
\]

So \( x^3 + 4x^2 + 3x - 7 \) is not an element of \( (x - 1) \) and thus \( x^3 + 4x^2 + 3x - 7 \) is not an element of \( (x^3 - 3x + 2, x^4 - 1, x^6 - 1) \).
MULTI-VARIABLE POLYNOMIALS

One way to describe an ideal is to determine a basis for the ideal. In the one-variable case it is easily shown that such a basis exists and in fact we find one explicitly as follows: The division algorithm and the Euclidean algorithm are used to find a greatest common divisor of the polynomials of the ideal (gcd). This gcd is a basis of one element and will generate the ideal. Once this gcd is determined, it is easy to determine whether a polynomial is an element of the ideal. It will be an element of the ideal if and only if division of the polynomial by this gcd renders a remainder of 0.

This method will not apply "as is" to the multi-variable case. It is necessary to generalize this method in order to use it for ideals in $k[x_1, \ldots, x_n]$. When using the division algorithm in a single variable, the polynomial is ordered by using the highest power of the variable and then writing the other powers of the variable in descending order. How then are multi-variable polynomials ordered?

For example, which of the following orderings is correct? Is there more than one valid ordering?

\[ x^2y^2 + xy^4 \quad \text{or} \quad xy^4 + x^2y^2 \]

In fact, both are "correct", as this is an example of two types of valid orderings. However, one is better than the other for our purposes.
Another issue in the single variable vs. multi-variable saga is the remainder in division. In the one-variable division algorithm, the remainder is unique. But this is not so for the multi-variable case.

Example 6.1 Consider

\[ f = x^2y + xy^2 + y^2 \]

Dividing by \( f_1 = xy - 1 \) and then by \( f_2 = y^2 - 1 \), we obtain

\[ f = x^2y + xy^2 + y^2 = (x + y)(xy - 1) + 1(y^2 - 1) + x + y + 1 \]

But dividing by \( f_2 + y^2 - 1 \) and then by \( f_1 = xy - 1 \), we obtain

\[ f = x^2y + xy^2 + y^2 = (x + 1)(y^2 - 1) + x(xy - 1) + 2x + 1 \]

Thus we see that the order in which we choose variables to divide is important in determining the result.

It is necessary to arrange the terms of a polynomial in a "descending" order so that the ordering will be consistent. In other words, it will be needed to be able to compare every pair of monomials to establish their proper relative position. This will require a linear ordering on monomials. This means that for every pair of monomials \( x^\alpha \) and \( x^\beta \) exactly one of the following must hold

\[ x^\alpha < x^\beta, \quad x^\alpha > x^\beta \quad \text{or} \quad x^\alpha = x^\beta. \]

For addition another property must be added. If \( \alpha > \beta \), then \( \alpha + \gamma > \beta + \gamma \) for all \( \gamma \in \mathbb{Z}^n \). Linear ordering is vital in showing the termination of certain algorithms.
Definition 6.2 A monomial ordering on \( k[x_1, \ldots, x_n] \) is any relation \( > \) on \( \mathbb{Z}^n \), or equivalently, any relation on the set of monomials \( x^\alpha, \alpha \in \mathbb{Z}^n \) satisfying:

(i) \( > \) is a total (or linear) ordering on \( \mathbb{Z}^n \).

(ii) If \( \alpha > \beta \) and \( \gamma \in \mathbb{Z}^n \), then \( \alpha + \gamma > \beta + \gamma \).

(iii) \( > \) is a well-ordering on \( \mathbb{Z}^n \). This means that every nonempty subset of \( \mathbb{Z}^n \) has a smallest element under \( > \).

The following Lemma will help explain the "well-ordering condition" of part (iii).

Lemma 6.3 An order relation \( > \) on \( \mathbb{Z}^n \) is a well-ordering if and only if every strictly decreasing sequence in \( \mathbb{Z}^n \), \( \alpha(1) > \alpha(2) > \alpha(3) > \cdots \) eventually terminates.

Proof Prove the contrapositive: \( > \) is not a well-ordering if and only if there is an infinite strictly decreasing sequence in \( \mathbb{Z}^n \). If \( > \) is not a well-ordering, then there is some nonempty subset \( S \subset \mathbb{Z}^n \) that has no least element. If \( \alpha(1) \in S \), then \( \alpha(1) \) is not a least element. So there is an \( \alpha(2) \in S \) such that \( \alpha(1) > \alpha(2) \). But \( \alpha(2) \) is also not a least element, so there is an \( \alpha(3) \in S \) such that \( \alpha(2) > \alpha(3) \). Continuing in this way, we get an infinite strictly decreasing sequence \( \alpha(1) > \alpha(2) > \alpha(3) \cdots \). Conversely, given an infinite strictly decreasing sequence \( \alpha(1) > \alpha(2) > \alpha(3) \cdots \). Then \( \{\alpha(1), \alpha(2), \alpha(3), \ldots \} \) is a nonempty subset of \( \mathbb{Z}^n \) with no least element. By Definition 6.1, since \( \{\alpha(1), \alpha(2), \alpha(3), \ldots \} \) has no least element, \( > \) is not a well-ordering. \( \square \)
Three of the possible types of orderings are lexicographic order (lex), graded lex order (grlex), and graded reverse lex order (grevlex). The first type, lexicographic order, feels most natural and is very useful as it gives a Groebner basis that nicely eliminates variables in order to solve a system of polynomial equations. This is the one we will consider here. It is like that of a dictionary for words of a fixed length. For example bases < basis since bas is the same in both, but e < i. We say that $x^\alpha >_{\text{lex}} x^\beta$ and $\alpha >_{\text{lex}} \beta$ if and only if $\alpha - \beta >_{\text{lex}} 0$ in some sense, as defined below:

**Definition 6.4** Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}$. We say $\alpha >_{\text{lex}} \beta$ in lexicographic order, if, in the vector difference $\alpha - \beta \in \mathbb{Z}$, the left-most nonzero entry is positive. We will say $x^\alpha >_{\text{lex}} x^\beta$ if $\alpha >_{\text{lex}} \beta$.

For example, consider the polynomial $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$. In lex order the polynomial would be written as $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$.

Now we will see that lexicographic order is a monomial ordering.

**Proposition 6.5** The lex ordering on $\mathbb{Z}^n$, denoted $>_{\text{lex}}$ is a monomial ordering.

**Proof**

(i) $>_{\text{lex}}$ is a total ordering from the definition and the fact that the usual numerical order on $\mathbb{Z}^n$ is a total ordering.

(ii) If $\alpha >_{\text{lex}} \beta$, then the leftmost nonzero entry in $\alpha - \beta$, say $\alpha_k - \beta_k$, is positive. But $x^\alpha \cdot x^\gamma = x^{\alpha + \gamma}$ and $x^\beta \cdot x^\gamma = x^{\beta + \gamma}$. Then in $$(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta.$$ So the left-most nonzero entry is again $\alpha_k - \beta_k > 0$. 

30
(iii) Proof by contradiction. Assume $>_{\text{lex}}$ is not a well-ordering. Then by Lemma 6.3 there would be an infinite strictly descending sequence $\alpha(1) >_{\text{lex}} \alpha(2) >_{\text{lex}} \alpha(3) >_{\text{lex}} \cdots$ of elements in $\mathbb{Z}^n$. Consider the first entries of the vectors $\alpha(i) \in \mathbb{Z}^n$. By the definition of lex ordering, these first entries form a non-increasing sequence of nonnegative integers. Since $\mathbb{Z}$ is well-ordered, the first entries of the $\alpha(i)$ must "stabilize" eventually, i.e., there exists a $k$ such that all the first components of the $\alpha(i)$ with $i \geq k$ are equal. Beginning at $\alpha(k)$, the second and subsequent entries come into play in determining the lex order. The second entries of $\alpha(k), \alpha(k + 1), \ldots$ form a non-increasing sequence. As before, the second entries "stabilize" eventually. Since the elements $\alpha(i)$ are finite sequences, continuing in the same way we see that for some $l$, the $\alpha(l), \alpha(l + 1), \ldots$ are all equal. This contradicts the fact that $\alpha(l) >_{\text{lex}} \alpha(l + 1)$. Thus lex is a well-ordering.

In lex order, notice that a variable dominates any monomial involving only smaller variables, regardless of its total degree. Thus, for any lex order with $x > y > z$, we have $x >_{\text{lex}} y^5 z^3$. Sometimes we may want to take the total degrees of the monomials into account and order monomials of bigger degrees first. One way to do this is the graded lexicographic order ($\text{grlex}$ order).

**Definition 6.6** Let $\alpha, \beta \in \mathbb{Z}^n$. Denote $|\alpha| = \sum_{i=1}^n \alpha_i$ and $|\beta| = \sum_{i=1}^n \beta_i$. We say $\alpha >_{\text{grlex}} \beta$ if $|\alpha| > |\beta|$ or $|\alpha| = |\beta|$ and $\alpha >_{\text{lex}} \beta$. 

31
Grlex orders by total degree first, then “breaks ties” using lex order.

Returning to our example, \( f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2 \), in grlex this polynomial would be ordered \( f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2 \). This is because the only “tie” we have is \( 7x^2z^2 \) and \( 4xy^2z \). So \((2, 0, 2) >_{\text{grlex}} (1, 2, 1)\) since \(|(2, 0, 2)| = 4 = |(1, 2, 1)|\) and \((2, 0, 2) >_{\text{lex}} (1, 2, 1)\), and so \( x^2z^2 > xy^2z \).

Another, less intuitive, ordering is the graded reverse lexicographic ordering (grevlex order).

**Definition 6.7** Let \( \alpha, \beta \in \mathbb{Z}^n \) and \(|\alpha|, |\beta|\), as above. We say \( \alpha >_{\text{grevlex}} \beta \) if \(|\alpha| > |\beta|\), or \(|\alpha| = |\beta|\) and, in \( \alpha - \beta \in \mathbb{Z}^n \), the right-most entry is negative.

Grevlex orders by total degree first, like grlex, but “breaks ties” in a different way. Returning to our example, \( f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2 \), in grevlex this polynomial would be ordered \( 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2 \). This is because the only “tie” we have is \( 7x^2z^2 \) and \( 4xy^2z \). So \((1, 2, 1) >_{\text{grevlex}} (2, 0, 2)\) since \(|(1, 2, 1)| = 4 = |(2, 0, 2)|\) and \( \alpha - \beta = (-1, 2, -1) \).

From now on we use only lex ordering, so we denote it simply by >.

We recall some terminology via the last example,

\[
f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2,
\]

1. the **leading term** (LT) is \(-5x^3\)

2. the **leading monomial** (LM) is \(x^3\)

3. the **leading coefficient** (LC) is \(-5\)

4. the **multidegree** is \((3, 0, 0)\) because \(x^3 = x^3y^0z^0\)
In the multi-variable case, division did not render a unique remainder. In fact, the multi-variable division algorithm states that the remainder is either zero or a linear combination of monomials none of which are divisible by any of the leading terms of the functions.

**Theorem 6.8 (The Division Algorithm in \( k[x_1, \ldots, x_n] \))** Fix a monomial order \( > \) on \( \mathbb{Z}^n \), and let \( F = (f_1, \ldots, f_s) \) be an ordered s-tuple of polynomials in \( k[x_1, \ldots, x_n] \). Then every \( f \in k[x_1, \ldots, x_n] \) can be written as

\[ f = a_1 f_1 + \cdots + a_s f_s + r, \]

where \( a_i, r \in k[x_1, \ldots, x_n] \) and either \( r = 0 \) or \( r \) is a linear combination with coefficients in \( k \), of monomials, none of which is divisible by any \( f \in \{LT(f_1), \ldots, LT(f_s)\} \). We will call \( r \) a remainder of \( f \) on division by \( F \). Furthermore, if \( a_i f_i = 0 \), then we have

\[ \text{multideg}(f) > \text{multideg}(a_i f_i). \]

**Example 6.9** Consider dividing polynomial \( f = x^2 y + xy^2 + y^2 \) by \( f_1 = xy - 1 \) and \( f_2 = y^2 - 1 \). When we start our division using \( f_1 \) first and then dividing by \( f_2 \) we get

\[ x^2 y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + x + y^2 + y \]
\[ x^2 y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + (1) \cdot (y^2 - 1) + x + y + 1 \]

But if we divide by \( f_2 \) first and then divide by \( f_1 \) we get

\[ x^2 y + xy^2 + y^2 = (x + 1) \cdot (y^2 - 1) + x^2 y + x + 1 \]
\[ x^2 y + xy^2 + y^2 = (x = 1) \cdot (y^2 - 1) + (x) \cdot (xy - 1) + 2x + 1 \]
However, it turns out that if we have a Groebner basis of an ideal, the remainder on division of a polynomial $f$ by the elements of the Groebner basis is unique.
7 GROEBNER BASES

In this chapter we will study Groebner bases, which were introduced in 1965 by Bruno Buchberger, in honor of his thesis advisor, W. Groebner. We have already alluded to these bases in previous chapters.

In order to define and study these bases, we must first consider leading terms and how they apply to Hilbert’s Basis Theorem. Once we choose a monomial ordering each polynomial \( f \in k[x_1, \ldots, x_n] \) has a leading term, \( \text{LT}(f) \).

**Definition 7.1** Let \( I \subset k[x_1, \ldots, x_n] \) be an ideal other than \( \{0\} \), and fix a monomial ordering on the monomials of \( k[x_1, \ldots, x_n] \).

(i) We denote by \( \text{LT}(I) \) the set of leading terms of elements of \( I \). Thus
\[
\text{LT}(I) = \{ cx^\alpha \mid \exists f \in I \mid \text{LT}(f) = cx^\alpha \}.
\]

(ii) We denote by \( \langle \text{LT}(I) \rangle \) the ideal generated by the elements of the set \( \text{LT}(I) \).

If \( I = \langle f_1, \ldots, f_s \rangle \), we want to be able to compare \( \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle \) and \( \langle \text{LT}(I) \rangle \). These may be different ideals. We see that
\[
\text{LT}(f_i) \in \text{LT}(I) \subset \langle \text{LT}(I) \rangle \quad \text{which implies} \quad \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle \subset \langle \text{LT}(I) \rangle.
\]
However \( \langle \text{LT}(I) \rangle \) could be larger. Here is an example of this.

**Example 7.2** Let \( I = \langle f_1, f_2 \rangle \) where \( f_1 = x^3 - 2xy \) and \( f_2 = x^2y - 2y^2 + x \) (using grlex as our ordering). Then \( x \cdot (x^2y - 2y^2 + x) - y \cdot (x^3 - 2xy) = x^2 \), so that \( x^2 \in I \). Thus \( x^2 = \text{LT}(x^2) \in \langle \text{LT}(I) \rangle \). However \( x^2 \) is not divisible by \( \text{LT}(f_1) = x^3 \) or \( \text{LT}(f_2) = x^2y \). So by Lemma 3.6, \( x^2 \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle \).
We now want to show that \( \langle LT(I) \rangle \) is a monomial ideal so we can show it is generated by finitely many terms.

**Proposition 7.3** Let \( I \subset k[x_1, \ldots, x_n] \) be an ideal.

(i) \( \langle LT(I) \rangle \) is a monomial ideal.

(ii) There are \( g_1, \ldots, g_s \in I \) such that \( \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_2) \rangle \), i.e. \( \langle LT(I) \rangle \) has a finite basis.

**Proof**

(i) The leading monomials \( LM(g) \) of elements \( g \in I - \{0\} \) generate the monomial ideal \( \langle LM(g) \mid g \in I - \{0\} \rangle \). Since \( LM(g) \) and \( LT(g) \) differ only by multiplication of a nonzero constant, this ideal is the same as \( \langle LT(g) : g \in I - \{0\} \rangle = \langle LT(I) \rangle \). Thus \( \langle LT(I) \rangle \) is a monomial ideal.

(ii) Since \( \langle LT(I) \rangle \) is generated by the monomials \( LM(g) \) for \( g \in I - \{0\} \), Dickson’s Lemma tells us that \( \langle LT(I) \rangle = \langle LM(g_1), \ldots, LM(g_t) \rangle \) for finitely many \( g_1, \ldots, g_t \in I \). Since \( LM(g_i) \) differs from \( LT(g_i) \) by a nonzero constant, it follows that \( \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle \). \( \square \)

We now can prove using Proposition 7.3 and the division algorithm the existence of a finite generating set of every polynomial ideal.

**Theorem 7.4 (Hilbert’s Basis Theorem)** Every ideal \( I \subset k[x_1, \ldots, x_n] \) has a finite generating set. That is, \( I = \langle g_1, \ldots, g_s \rangle \) for some \( g_1, \ldots, g_s \in I \).
Proof If $I = 0$ then $\{0\}$ is an obvious finite generating set, and so $I = \langle 0 \rangle$. If $I \neq 0$ the a finite generating set $g_1, \ldots, g_s$ in $I$ can be constructed as follows: By Proposition 7.3, there are $g_1, \ldots, g_s \in I$ such that 
\[ \langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle \]
and the fact that $\langle LT(I) \rangle$ is generated by the leading monomials $LM(g)$ for $g \in I - 0$. We claim that $I = \langle g_1, \ldots, g_s \rangle$. Clearly $\langle g_1, \ldots, g_s \rangle \subset I$ since every $g_i \in I$. Conversely, let $f$ be any polynomial in $I$. Applying the multi-variable division algorithm, dividing $f$ by $\langle g_1, \ldots, g_s \rangle$ we get 
\[ f = a_1 g_1 + \cdots + a_t g_t + r \]
where no term of $r$ is divisible by any of $LT(g_1), \ldots, LT(g_s)$. We will show that $r = 0$. For, if $f = a_1 g_1 + \cdots + a_t g_t + r$ then $r = f - a_1 g_1 - \cdots - a_t g_t \in I$. Assume that $r \neq 0$, then
\[ LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle. \]
Thus $LT(r)$ is divisible by some $LT(g_i)$. But this is a contradiction to the division algorithm. Thus $r = 0$, and so $f = a_1 g_1 + \cdots + a_t g_t + 0 \in \langle g_1, \ldots, g_s \rangle$. Thus $I \subset \langle g_1, \ldots, g_s \rangle$. Since $\langle g_1, \ldots, g_s \rangle \subset I$ and $I \subset \langle g_1, \ldots, g_s \rangle$, $I = \langle g_1, \ldots, g_s \rangle$, as required. $\square$

Now the first question, the **Ideal Membership Problem**, posed in the Introduction can be answered. Given an ideal in $k[x_1, \ldots, x_n]$, can a basis be found for it? Hilbert’s Basis Theorem states every ideal has a finite generating set. In addition, the basis used in the proof of Hilbert Basis Theorem has the special property that $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$. Since this is not necessarily true for all bases of an ideal, we will give these special bases a special name, Groebner bases.
Definition 7.5 A finite subset \( G = \{ g_1, \ldots, g_s \} \) of an ideal \( I \) is said to be a Groebner basis for \( I \) if the ideal generated by the leading terms of \( g_1, \ldots, g_s \) is the ideal generated by the leading terms of all polynomials in \( I \), i.e.

\[
\langle LT(g_1), \ldots, LT(g_s) \rangle = \langle LT(I) \rangle.
\]

Thus a set \( \{ g_1, \ldots, g_s \} \in I \) is a Groebner basis of \( I \) if and only if the leading term of any element of \( I \) is divisible by one the the \( LT(g_i) \). Note that it is not immediately obvious from this definition that a Groebner basis for an ideal is indeed a basis for that ideal. The following corollary will show that this is so.

Corollary 7.6 Fix a monomial order. Then every ideal \( I \subset k[x_1, \ldots, x_n] \) other than \( \{0\} \) has a Groebner basis. Furthermore, any Groebner basis for an ideal \( I \) is a basis of \( I \).

Proof Given a nonzero ideal, the set \( G = \{ g_1, \ldots, g_s \} \) constructed in the proof of the Hilbert Basis Theorem is a Groebner basis by definition. Now we want to show any Groebner basis for an ideal \( I \) is a basis of \( I \). Suppose \( G = \{ g_1, \ldots, g_s \} \subset I \) is a Groebner basis for \( I \) such that.

\[
\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle.
\]

We want to show \( I = \langle g_1, \ldots, g_s \rangle \) so that \( G \) is a basis for \( I \). Since \( G \subset I \) and \( G = \{ g_1, \ldots, g_s \} \), then \( \{ g_1, \ldots, g_s \} \subset I \). So let \( f \in I \) be any arbitrary polynomial. Divide \( f \) by \( g_1, \ldots, g_s \) and by the division algorithm, we get \( f = a_1 + \cdots + a_sg_s + r \) where no term of \( r \) is divisible by any of the \( LT(g_1), \ldots, LT(g_s) \). Since \( f, g_1, \ldots, g_s \in I \) then \( r \in I \). Assume \( r \neq 0 \), then \( LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle \). Then by the Lemma 3.6, \( LT(r) \)
must be divisible by some \( LT(g_i) \). But this is a contradiction. So \( r = 0 \) and thus \( f = a_1 g_1 + \cdots + a_s g_s \). Thus \( I \subseteq \langle g_1, \ldots, g_s \rangle \). Therefore \( I = \langle g_1, \ldots, g_s \rangle \). \( \square \)

Although the multi-variable division algorithm does not state that there is, in general, a unique remainder, division by the elements of the Groebner basis on a polynomial does render a unique remainder, as we see in the following proposition.

**Proposition 7.7** Let \( G = \{ g_1, \ldots, g_t \} \) be a Groebner basis for an ideal \( I \subseteq k[x_1, \ldots, x_n] \) and let \( f \in k[x_1, \ldots, x_n] \). Then there is a unique \( r \in k[x_1, \ldots, x_n] \) with the following two properties:

(i) No term of \( r \) is divisible by any of \( LT(g_1), \ldots, LT(g_t) \).

(ii) There is \( g \in I \) such that \( f = g + r \).

In particular, \( r \) is the unique remainder on division of \( f \) by \( G \) no matter how the elements of \( G \) are listed when using the division algorithm.

**Proof**

(i) The division algorithm gives the existence of a polynomial \( r \) such that

\[ f = a_1 g_1 + \cdots + a_t g_t + r \text{ where no term of } r \text{ is divisible by any of } \]

\( LT(g_1), \ldots, LT(g_t) \)

(ii) To show that there exists a \( g \in I \) such that \( f = g + r \), from part (i)

\[ f = a_1 g_1 + \cdots + a_t g_t + r . \] So we set \( g = a_1 g_1 + \cdots + a_t g_t \) such that \( a_i \in I \) for all \( 1 \leq i \leq t \). Then \( f = g + r \). To prove uniqueness, let \( r \) and \( r' \) be distinct remainders such that \( f = g + r = g' + r' \) as in part (i), so that \( g \)

39
and \( g' \) are elements of the Groebner basis. Then \( r - r' = g' - g \) and since \( f, g, g' \in I \), then \( g' - g \in I \) and \( r - r' \in I \). Assume \( r \neq r' \), then

\[
\text{LT}(r - r') \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle.
\]

By Lemma 3.6, \( \text{LT}(r_1 - r_2) \) is divisible by some \( \text{LT}(g_i) \). This is a contradiction because, no term of \( r \) or \( r' \) is divisible by some \( \text{LT}(g_i) \). Thus \( r = r' \) which implies \( g = g' \). □

In order to compute a Groebner basis, Buchberger’s Algorithm will be used. But prior to proposing the algorithm, least common multiple and S-polynomial must be defined.

**Definition 7.8** Let \( f, g \in k[x_1, \ldots, x_n] \) be nonzero polynomials.

1. If \( \text{multideg}(f) = \alpha \) and \( \text{multideg}(g) = \beta \), then let \( \gamma = (\gamma_1, \ldots, \gamma_n) \), where \( \gamma_i = \text{max} (\alpha_i, \beta_i) \) for each \( i \). We call \( x^\gamma \) the least common multiple of \( \text{LM}(f) \) and \( \text{LM}(g) \), written \( x^\alpha = \text{LCM}(\text{LM}(f), \text{LM}(g)) \)

2. The **S-polynomial** of \( f \) and \( g \) is the combination

\[
S(f, g) = \left( \frac{x^\gamma}{\text{LT}(f)} \right)(f) - \left( \frac{x^\gamma}{\text{LT}(g)} \right)(g).
\]

Buchberger’s algorithm takes an arbitrary basis and transforms it into a Groebner basis.

**Proposition 7.9 (Buchberger’s Algorithm)** Let \( I = \langle f_1, \ldots, f_s \rangle \neq 0 \) be a polynomial ideal. Then a Groebner basis for \( I \) can be constructed in a finite number of steps by the following algorithm:
Input: \( F = (f_1, \ldots, f_s) \)

Output: a Groebner basis \( G = (g_1, \ldots, g_t) \) for \( I \), with \( F \subset G \)

Process:

\[
G := F
\]

REPEAT

\[
G' = G
\]

FOR each pair \( p, q, p \neq q \) in \( G' \) DO

\[
S := S(p, q)^G' \quad (\text{where } S(p, q)^G' \text{ is the remainder on division of } S(p, q) \text{ by some ordered } t\text{-tuple in } G.)
\]

IF \( S \neq 0 \) THEN \( G := G \cup \{ S \} \)

UNTIL \( G = G' \)

We now use Buchberger’s algorithm to find a Groebner Basis for a particular ideal.

**Example 7.10** Consider \( I = \langle f_1, f_2 \rangle \) where \( f_1(x, y) = x^2y - 1 \) and \( f_2(x, y) = xy^2 - x \). Calculate the S-polynomial for \( f_1 \) and \( f_2 \),

\[
S(f_1, f_2), \quad \text{where } x^\gamma = LCM(LM(f_1), LM(f_2)).
\]

Since \( f_1(x, y) = x^2y - 1 \) and \( f_2(x, y) = xy^2 - x \)

and \( LT(f_1) = x^2y = LM(f_1) \) and \( LT(f_2) = xy^2 = LM(f_2) \)

then \( x^\gamma = LCM(x^2y, xy^2) = x^2y^2 \).
The S-polynomial can now be calculated.

\[
S(f_1, f_2) = \frac{x^2 y^2}{x^2 y} \cdot (x^2 y - 1) - \frac{x^2 y^2}{xy^2} \cdot (xy^2 - x)
\]

\[
S(f_1, f_2) = y \cdot (x^2 y - 1) - x \cdot (xy^2 - x)
\]

\[
S(f_1, f_2) = x^2 y^2 - y - x^2 y^2 + x^2
\]

\[
S(f_1, f_2) = x^2 - y
\]

Clearly \( f_1(x, y) = x^2 y - 1 \) and \( f_2(x, y) = xy^2 - x \) do not divide \( x^2 - y \). So we add this third polynomial to the set that will become the Groebner basis.

\[
f_1(x, y) = x^2 y - 1, \quad f_2(x, y) = xy^2 - x, \quad f_3(x, y) = x^2 - y
\]

Continuing in the same way, \( S(f_1, f_2) = x^2 - y \) is clearly divisible by \( f_3(x, y) = x^2 - y \) but \( S(f_1, f_3) = y^3 - y \) is not divisible by any of the polynomials \( f_1, f_2, f_3 \). So we add \( S(f_1, f_3) \) as a fourth basis polynomial to the set. We now have:

\[
f_1(x, y) = x^2 y - 1, \quad f_2(x, y) = xy^2 - x, \quad f_3(x, y) = x^2 - y, \quad f_4(x, y) = y^3 - y.
\]

Now each of the polynomials, \( S(f_1, f_2), S(f_1, f_3), S(f_1, f_4), S(f_2, f_3), S(f_2, f_4), \) and \( S(f_3, f_4) \), is divisible by \( f_1, f_2, f_3, \) or by \( f_4 \). So they form a Groebner basis:

\[
G = \{x^2 y - 1, xy^2 - x, x^2 - y, y^3 - y\}.
\]

Once we have a Groebner basis, two more of our questions can be answered: Is a given function, \( g(x, y) \), a member of this ideal? How do we solve a system of equations?
The Ideal Membership Question If \( g(x, y) = x^2y - xy^2 - 1 \), we use the division algorithm and the Groebner basis that we computed to find that \( g = (1)(f_1) - (1)(f_2) + (0)(f_3) + (0)(f_4) \), and so \( g(x, y) \) is a member of the ideal.

Solutions of Systems of Equations To see how to solve a system of polynomial equations using a Groebner basis, we again look at our example, and solve the system \( f_1 = f_2 = 0 \). Notice that \( f_4(x, y) = y^3 - y \) is a polynomial in only one variable, \( y \). This is a major advantage of using Lex ordering: it gives a Groebner basis that successively eliminates the variables. So in our case:

\[
y^3 - y = y(y^2 - 1) = y(y + 1)(y - 1) = 0
\]

Thus the possible solutions for \( y \) are \(-1, 0, 1\). But we see that \( y \neq 0 \) because when we substitute 0 into \( f_1(x, y) \) we get \( x^2(0) - 1 = 0 \). Which leads to \(-1 = 0\) which is impossible. Similarly in order to get a solution in the real numbers, \( y \neq -1 \) because substituting \(-1\) into \( f_1(x, y) \) we get \( x^2(-1) - 1 = 0 \), which leads to \( x^2 = -1 \). So consider \( y = 1 \). We get the following:

\[
\begin{align*}
f_1(x, 1) &= x^2(1) - 1 = 0 \text{ which implies } x^2 = 1 \text{ which implies } x = 1 \text{ or } x = -1. \\
f_2(x, 1) &= x(1) - x = 0 \text{ which implies } x - x = 0 \text{ which is true for all real numbers.} \\
f_3(x, 1) &= x^2 - 1 = 0 \text{ which implies } x^2 = 1 \text{ which implies } x = 1 \text{ or } x = -1. \\
f_4(x, 1) &= 1^3 - 1 = 0 \text{ which implies } 1 - 1 = 0 \text{ which is true for all real numbers.}
\end{align*}
\]

So substituting \( y = 1 \) into the polynomials, we get \( f_1(x, y) = f_2(x, y) = f_3(x, y) = f_4(x, y) = 0 \), to obtain the following solutions: \((1, 1)\) and \((-1, 1)\).
Groebner bases computed using Buchberger's Algorithm are often bigger than necessary. We can eliminate some generators by using the following lemma.

Lemma 7.11 Let $G$ be a Groebner basis for the polynomial ideal $I$. Let $p \in G$ be a polynomial such that $LT(p) \in \langle LT(G) - \{p\} \rangle$. Then $G - \{p\}$ is also a Groebner basis for $I$.

Proof We know that $\langle LT(G) \rangle = \langle LT(I) \rangle$. If $LT(p) \in \langle LT(G - \{p\}) \rangle$, then $\langle LT(G - \{p\}) \rangle = \langle LT(G) \rangle$. By definition, it follows that $G - \{p\}$ is also a Groebner basis for $I$. □

By adjusting constants to make all leading coefficients 1 and removing any $p$ with $LT(p) \in \langle (G - \{p\}) \rangle$ from $G$, we arrive at what we will call a minimal Groebner basis.

Definition 7.12 A minimal Groebner basis for a polynomial ideal $I$ is a Groebner basis $G$ for $I$ such that:

(i) $LC(p) = 1$ for all $p \in G$.

(ii) For all $p \in G$, $LT(p) \notin \langle LT(G - \{p\}) \rangle$.

Even minimal bases are not unique, a given ideal may have many minimal Groebner bases. Fortunately, one minimal basis can be singled out.
**Definition 7.13** A **reduced Groebner basis** for a polynomial ideal $I$ is a Groebner basis $G$ for $I$ such that:

(i) $LC(p) = 1$ for all $p \in G$.

(ii) For all $p \in G$, no monomial of $p$ lies in $\langle LT(G - \{p\}) \rangle$.

In general, reduced Groebner bases have the following property.

**Proposition 7.14** Let $I \neq \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, $I$ has a unique reduced Groebner basis.

So determining a reduced Groebner basis will determine a unique basis.
8 HILBERT’S NULLSTELLENSATZ THEOREMS

The last topic to discuss is the relationship between an ideal and its corresponding variety. As we have seen, a variety \( V \subset k^n \) can be studied by passing to the ideal \( I(V) = \{ f \in k[x_1, \ldots, x_n] \mid f(x) = 0 \ \forall x \in V \} \) of all polynomials vanishing on \( V \). Thus we have a map

\[
\text{Affine Varieties} \quad \longrightarrow \quad \text{Ideals}
\]

\[
V \quad \longrightarrow \quad I(V)
\]

Conversely, given an ideal \( I \subset k[x_1, \ldots, x_n] \), we can define the set

\[
V(I) = \{ x \in k^n \mid f(x) = 0 \ \forall f \in I \}.
\]

The Hilbert Basis Theorem tells us that \( V(I) \) is actually an affine variety because there exists a finite set of polynomials \( f_1, \ldots, f_s \in I \) such that \( I = (f_1, \ldots, f_s) \) and \( V(I) \) is the set of common roots of these polynomials. Thus we have a map

\[
\text{Ideals} \quad \longrightarrow \quad \text{Affine Varieties}
\]

\[
I \quad \longrightarrow \quad V(I)
\]

It is important to note that different ideals can generate the same variety. For example, \( (x) \) and \( (x^2) \) are different ideals in \( k[x] \) but they have the same variety \( V(x) = V(x^2) = \{0\} \).

In another example we note that different ideals can correspond to the empty variety. This can occur if the field \( k \) is not algebraically closed. For example, consider the polynomials \( 1, 1 + x^2, \) and \( 1 + x^2 + x^4 \) in \( \mathbb{R}[x] \). All three generate different ideals, \( (1) \in \mathbb{R}[x], (1 + x^2) = \{ f(x) \mid 1 + x^2 \text{ divides } f(x) \}, \) and \( (1 + x^2 + x^4) = \{ f(x) \mid 1 + x^2 + x^4 \text{ divides } f(x) \} \) and \( 1 \notin (1 + x^2), \)
\(1 \notin (1 + x^2 + x^4)\), and \(1 + x^2 \notin (1 + x^2 + x^4)\), but each polynomial has no roots in the real numbers so the corresponding varieties are all empty. It turns out that in any polynomial ring, algebraic closure is enough to guarantee that the only ideal which represents the empty variety is the entire polynomial ring itself.

**Theorem 8.1 (The Weak Nullstellensatz)** Let \(k\) be an algebraically closed field and let \(I \subset k[x_1, \ldots, x_n]\) be an ideal satisfying \(V(I) = \emptyset\). Then \(I = k[x_1, \ldots, x_n]\).

The Hilbert Nullstellensatz states that, over an algebraically closed field, if a polynomial \(f\) vanishes at all points of some variety \(V(I)\), then some power of \(f\) must belong to \(I\). The proof of Hilbert's Nullstellensatz is interesting due to a very ingenious trick. Up to now all the work has been in the ring of polynomials \(k[x_1, \ldots, x_n]\). By expanding to the ring of polynomials in \(n + 1\) variables, polynomials \(f_1, \ldots, f_s, 1 - yf\) will be obtained. Then the arena will be expanded to the field of rational functions \(k(x_1, \ldots, x_n)\) and \(y = \frac{1}{f}\). This will return us back to our original ring of polynomials \(k[x_1, \ldots, x_n]\).

**Theorem 8.2 (Hilbert's Nullstellensatz)** Let \(k\) be an algebraically closed field. If \(f_1, \ldots, f_s \in k[x_1, \ldots, x_n]\) are such polynomials that \(f \in I(V(f_1, \ldots, f_s))\), then there exists an integer \(m \geq 1\) and polynomials \(A_1, \ldots, A_s\) such that \(f^m \in \langle f_1, \ldots, f_s \rangle\) and \(f^m = \sum_{i=1}^{s} A_i f_i\).

**Proof** Given a polynomial \(f\) which vanishes at every common zero of the polynomials \(f_1, \ldots, f_s\) we want to show that there exists an integer \(m \geq 1\) and
polynomials $A_1, \ldots, A_s$ such that $f^m = A_if_i$. To do this let $y$ be an additional variable, and consider the ideal, $I' = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$. We first show that $V(I') = \emptyset$. Let $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$.

Case (i) The point $(a_1, \ldots, a_n)$ is a common zero of $f_1, \ldots, f_s$. Then $f(a_1, \ldots, a_n) = 0$ since $f$ vanishes at every common zero of $f_1, \ldots, f_s$. Thus, at the point $(a_1, \ldots, a_n, a_{n+1})$, $1 - yf = 1 - a_{n+1}f(a_1, \ldots, a_n) = 1 - 0 \neq 0$. Thus $(a_1, \ldots, a_n, a_{n+1}) \notin V(I')$.

Case (ii) The point $(a_1, \ldots, a_n)$ is not a common zero of $f_1, \ldots, f_s$. So for some $i$, $1 \leq i \leq s$, $f(a_1, \ldots, a_n) \neq 0$. Thus considering $f_i$ as a function of $n + 1$ variables which does not depend on $a_{n+1}$, it is also true $f_i(a_1, \ldots, a_n, a_{n+1})(0) \neq 0$. Thus $(a_1, \ldots, a_n, a_{n+1}) \notin V(I')$. Since in either case $(a_1, \ldots, a_n, a_{n+1}) \in V(I')$ we see that $V(I') = \emptyset$. Now applying the Weak Nullstellensatz, $I' = k[x_1, \ldots, x_n, y]$ and $1 \in I'$. Thus

$$1 = \sum p_i(x_1, \ldots, x_n, y)f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

for some polynomials $p_i, q \in k[x_1, \ldots, x_n]$. Now let $y = \frac{1}{f(x_1, \ldots, x_n)}$. Then $1 = \sum p_i(x_1, \ldots, x_n)f_i$.

Multiplying both sides of the equation by $f^m$ where $m$ is chosen sufficiently large to clear all denominators, we obtain $f^m = A_if_i$ for some polynomials $A_i \in k[x_1, \ldots, x_n]$. Thus if $f \in I((f_1, \ldots, f_s))$ then there exists $m \geq 1$ such that $f^m \in \langle f_1, \ldots, f_s \rangle$. □

Now can we identify those ideals that consist of all polynomials which vanish on some variety $V$.  

48
Lemma 8.3 Let $V$ be a variety. If $f^m \in I(V)$, then $f \in I(V)$.

Proof Let $V$ be a variety. If $f^m \in I(V)$, then $(f(x))^m = 0$. But this is only true if $f(x) = 0 \forall x \in V$. Since $x$ was any n-tuple in $V$, $f \in I(V)$. □

Thus, if an ideal consists of all the polynomials that vanish on some variety and some power of a particular polynomial is an element of the ideal, then the particular polynomial must also be an element of the ideal.

Definition 8.4 An ideal $I$ is a radical ideal if $f^m \in I$ for any integer $m \geq 1$ implies $f \in I$.

Thus we can now state the following corollary.

Corollary 8.5 Given a variety $V$, the ideal $I(V)$ is a radical ideal.

Proof Suppose $f^m \in I(V)$ which implies $f^m(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V$. Thus $f(a_1, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V$. Thus $f \in I(V)$. □

Definition 8.6 Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. The radical of $I$, denoted $\sqrt{I}$, is the set $\{f \mid f^m \in I \mid m \in \mathbb{Z}^+\}$.

The Strong Nullstellensatz gives a precise description of the ideal of a variety of an ideal.

Theorem 8.7 (The Strong Nullstellensatz) Let $k$ be an algebraically closed field. If $I$ is an ideal in $k[x_1, \ldots, x_n]$, then $I(V(I)) = \sqrt{I}$.  

49
Proof Clearly $\sqrt{I} \subseteq \mathbf{I}(V(I))$ because $f \in \sqrt{I}$ implies $f^m \in I$ for some $m$.

Thus, $f^m$ vanishes on $V(I)$, which implies $f$ vanishes on $V(I)$. Therefore, $f \in \mathbf{I}(V(I))$. Conversely, suppose $f \in \mathbf{I}(V(I))$. Then $f$ vanishes on $V(I)$. By Hilbert’s Nullstellensatz, there exists an integer $m \geq 1$ such that $f^m \in I$. But this means $f \in \sqrt{I}$. Since $f$ was arbitrary, $\mathbf{I}(V(I)) \subseteq \sqrt{I}$.

Thus $\mathbf{I}(V(I)) = \sqrt{I}$. □

So any questions about varieties can be rephrased as an algebraic question about radical ideals and vice-versa, provided we are working over an algebraically closed field.
9 SUMMARY

The topics explored in this project present an interesting picture of close connections between algebra and geometry. A study of these connections shows how the understanding of a particular object in one area can further knowledge of the object's analogue in another.

A crucial role in this study is played by Groebner bases; these are specific kinds of finite bases of ideals in the ring of polynomials in $n$ variables over a field. Using these, we were able to find solutions of polynomial equations in more than one variable. We were also able to describe such ideals explicitly with the goal of determining ideal membership.

The close relationship between ideals and varieties is further explored in Hilbert's Nullstellensatz Theorems, which give explicit conditions under which a polynomial belongs to the ideal of a variety, and determine the structure of the ideal of the variety.
REFERENCES


