9-2019

Algebraic Methods for Proving Geometric Theorems

Lynn Redman
twokidlynn@gmail.com

Algebraic Methods for Proving Geometric Theorems

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

Lynn Kathryn Redman

September 2019

Algebraic Methods for Proving Geometric Theorems

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

---

by

Lynn Kathryn Redman

September 2019

Approved by:

Dr. Laura Wallace, Committee Chair

Dr. Davida Fischman, Committee Member

Dr. Madeleine Jetter, Committee Member

Dr. Shawnee McMurran, Chair, Department of Mathematics

Dr. Corey Dunn, Graduate Coordinator

Abstract

Algebraic geometry is the study of systems of polynomial equations in one or more variables. Thinking of polynomials as functions reveals a close connection between affine varieties, which are geometric structures, and ideals, which are algebraic objects. An affine variety is a collection of n- tuples that represents the solutions to a system of equations. An ideal is a special subset of a ring and is what provides the tools to prove geometric theorems algebraically. In this thesis, we establish that a variety depends on the ideal generated by its defining equations. The ability to change the basis of an ideal without changing the variety is a powerful tool in determining a variety. In general, the quotient and remainder on division of polynomials in more than one variable are not unique. One property of a Groebner basis is that it yields a unique remainder on division.

To prove geometric theorems algebraically, we first express the hypotheses and conclusions as polynomials. Then, with the aid of a computer, apply the Groebner Basis Algorithm to determine if the conclusion polynomial(s) vanish on the same variety as the hypotheses.

Acknowledgements

To the mathematics professors at California State University of San Bernardino who reawakened in me the joy of learning and made me keenly aware of how much mathematics I have yet to learn, my gratitude is without bound.

Specifically to Dr. Joseph Chavez whose example as a facilitator of learning inspired me to reflect upon and enhance my own teaching practices, bless you. It was his passion for teaching and learning that ignited in me a desire to study and his vote of confidence that emboldened me to pursue a graduate degree in mathematics after having spent many years on the other side of the classroom.

To my children, Greggory and Allyson, for their commitment to excellence, their integrity and their perseverance, my undying admiration. They constantly encouraged me throughout this endeavor and have grown up to be honorable people I am proud to have call me Mom. I love you more than you can imagine.

To my students who constantly challenge me to answer and ask thought provoking questions that reveal the beauty of mathematics, I am proud of you and humbled by your support of my pursuit of deeper mathematics understanding. I loved hearing them say, "You got this!" when I was on my way to take an exam.

To Dr. Madeleine Jetter and Dr. Davida Fischman who generously gave their time and wisdom to the refinement of this project, thank you.

Finally, to my thesis advisor, Dr. Laura Wallace, who patiently worked through examples, clarified tricky concepts and provided guidance and support throughout the development of this project, an enormous thank you. I treasure our chats about teaching and learning.

Table of Contents

List of Figures

Chapter 1

Introduction

Algebra and geometry are often viewed as two distinct branches of mathematics. When we find connections between these and other branches of mathematics, our understanding of mathematics is enriched. Algebraic geometry is the study of solutions of systems of polynomials in one or more variables. The solution set is a collection of ordered n-tuples, called an affine variety. Affine varieties are curves, surfaces and higher dimensional objects defined by systems of polynomial equations. "The ability to regard a polynomial as a function is what makes it possible to link algebra and geometry." [CLO15].

The goal of this thesis is to demonstrate how the hypotheses and conclusions of theorems that describe characteristics of certain geometric structures can be translated to a system of polynomial equations and how algebraic methods such as the Groebner Basis Algorithm can be applied to determine if the theorem can be confirmed or rejected. This will involve the study of polynomial rings over a field k and ideals. In particular we will determine if a polynomial is an element of a particular ideal. Given a polynomial $f \in k[x_1, x_2, \ldots, x_n]$ and an ideal generated by $f_1, f_2, \ldots, f_s$ denoted by $I = \langle f_1, f_2, \ldots, f_s \rangle$, we will explore how we can determine if $f \in I$. This is related to the geometric problem of determining whether a variety $\mathbf{V}(f)$ lies on the variety $\mathbf{V}(f_1, f_2, \ldots, f_s)$. We will show that solving a system of polynomial equations, that is, finding all common solutions in k^n of a system of polynomial equations

$$f_1(x_1, x_2, \ldots, x_n) = f_2(x_1, x_2, \ldots, x_n) = \cdots = f_s(x_1, x_2, \ldots, x_n) = 0$$

is equivalent to finding the n-tuples in the affine variety $\mathbf{V}(f_1, f_2, \ldots, f_s)$.

The thesis begins with definitions and fundamental results of the relevant al-

gebraic and geometric objects. Ideals give us the structure for computing with affine varieties. We will study the correspondence between ideals and varieties. In particular, we will explore the mappings from ideals to varieties and varieties to ideals and determine which mappings represent bijections.

When working with multivariable polynomials, we encounter difficulties that are not present when working with single variable polynomials. For example, different orderings on monomials can yield different quotients and remainders when using a division algorithm on polynomials. Deriving a convenient basis for an ideal is an important step in proving geometric theorems algebraically. We will define and study the properties of Groebner bases and demonstrate how strategic use of technology allows us to efficiently verify theorems in Euclidean geometry. Several computer programs such as *Mathematica* and *Sage* have applications that quickly perform algorithms including polynomial division and computing a Groebner basis.

The thesis culminates with proving three theorems involving triangles in the Euclidean plane using technology to implement the Groebner Basis Algorithm. The first example we will demonstrate is the proof that the three medians of a triangle meet at a single point. This point is called the centroid of the triangle. Next, we demonstrate the proof that the three altitudes of a triangle meet at a single point, called the orthocenter of the triangle. The final example demonstrates the proof that the centroid, orthocenter and circumcenter of a triangle are collinear. This line is called the Euler Line.

Chapter 2

Algebra and Geometry Preliminaries

2.1 Polynomials and Affine Space

Using the Groebner Basis Algorithm involves solving a system of polynomial equations with any degree and with any number of variables. The examples presented in this thesis will contain more than two or three variables. The coefficients will be from a field k. In this section, we define the polynomials to be studied. Since each term of a polynomial is a monomial, we begin by defining a monomial.

Definition 2.1. [CLO15] A *monomial* in $x_1, x_2, ..., x_n$ 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 the monomial is the sum $\alpha_1 + \cdots + \alpha_n$ and is denoted $|\alpha|$.

To make the definition of a polynomial in $k[x_1, x_2, ..., x_n]$ less cumbersome, we simplify the notation for the monomials as follows. Let $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ be an n-tuple of positive integers. Then we will express $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ as x^α. The total degree of the monomial, as indicated above, is $|\alpha| = \alpha_1 + \cdots + \alpha_n$. When a polynomial has fewer than five variables, we will replace the x_1, x_2, x_3, x_4 with x, y, z, w.

Definition 2.2. [CLO15] A *polynomial* f in $x_1, x_2, ..., x_n$ with coefficients in k is a finite linear combination (with coefficients in k) of monomials.

We will express a polynomial f in the form

$$f = \sum_{\alpha} a_\alpha x^\alpha, \quad a_\alpha \in k,$$

where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$. The set of all polynomials in $x_1, x_2, ..., x_n$ with coefficients in k is denoted $k[x_1, x_2, ..., x_n]$. For example, a familiar polynomial ring used in much of mathematics at the secondary level is $\mathbb{R}[x]$, the ring of polynomials over the field of real numbers.

The basic terminology we will use when working with polynomials is given in the following definition.

Definition 2.3. [CLO15] Let $f = \sum_{\alpha} a_\alpha x^\alpha$ be a polynomial in $k[x_1, x_2, \ldots, x_n]$.

1. We call a_α the *coefficient* of the monomial x_α
2. If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a *term* of f.
3. The *total degree* of f, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient a_α is nonzero.

As an example, the polynomial $f = 3x^3y^2z + \frac{5}{6}z^3 - 7x^4 + 9x^2y^4$ has four terms. The coefficients are 3, $\frac{5}{6}$, -7, and 9. Notice that $f \in \mathbb{R}[x, y, z]$. The total degree of f is 6. There are two terms of f, $3x^3y^2z$ and $9x^2y^4$, that have a total degree of 6. This presents a dilemma with ordering the terms of multivariable polynomials that is not an issue with polynomials in one variable. Ordering the terms of multivariable polynomials will be discussed further in Chapter 3.

Although the coefficients of the polynomial are from a field k the collection of polynomials $k[x_1, x_2, \ldots, x_n]$ is not a field, but is a ring called the polynomial ring over the field k. We examine the difference in the definitions below.

Definition 2.4. [CLO15] A *commutative ring with unity* consists of a set k and two binary operations denoted "$+$" and "$\cdot$" defined on k such that for all $a,\ b,\ c \in k$ the following conditions are satisfied:

(i) (closure) $a + b \in k$ and $a \cdot b \in k$.

(ii) (commutative) $a + b = b + a$ and $a \cdot b = b \cdot a$. It is the commutativity of the second binary operation "$\cdot$" that allows us to identify the ring as a commutative ring.

(iii) (associative) $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(iv) (distributive) $a \cdot (b + c) = a \cdot b + a \cdot c$.

(v) (identities) There exist members $0, 1 \in k$ such that $a + 0 = a$ and $1 \cdot a = a$. The 1 is referred to as the unit. It is with the inclusion of this element we have a ring with unity.

(vi) (additive inverses) Given $a \in k$, there is $b \in k$ such that $a + b = 0$.

Definition 2.5. [Gal17] A *field* is a commutative ring with unity for which every nonzero element $a \in k$, there is $b \in k$ such that $a \cdot b = 1$.

Consider two arbitrary polynomials f and g from $k[x_1, x_2, \ldots, x_n]$. Then $f + g$ and $f \cdot g \in k[x_1, x_2, \ldots, x_n]$. Furthermore, it can be shown that the commutative, associative, distributive, identity and additive inverse conditions are satisfied. However, it is not possible to find a multiplicative inverse for every nonzero polynomial in $k[x_1, x_2, \ldots, x_n]$. For example, let $f = x - y$. Now $f \in \mathbb{R}[x, y]$. Although we have $g = \frac{1}{x-y}$ such that $f \cdot g = 1$, $g \notin \mathbb{R}[x, y]$ since g does not satisfy the definition of a polynomial (see Definition 2.2). In fact, the only polynomials that have multiplicative inverses in $k[x_1, x_2, \ldots, x_n]$ are the constant polynomials. We conclude that $k[x_1, x_2, \ldots, x_n]$ is a commutative ring with unity, not a field. We will refer to $k[x_1, x_2, \ldots, x_n]$ as a polynomial ring.

The next topic to consider is affine space.

Definition 2.6. [CLO15] Given a field k and a positive integer n, we define the n-dimensional *affine space* over k to be the set of n-tuples with elements in a field

$$k^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in k\}.$$

When the field is $\mathbb{R}$ we recognize the affine spaces $\mathbb{R}^2$ and $\mathbb{R}^3$ from secondary mathematics courses in algebra, geometry and calculus.

Now we explore how polynomials relate to affine space. An important connection is that a polynomial $f = \sum_{\alpha} a_\alpha x^\alpha \in k[x_1, x_2, \ldots, x_n]$ gives a function that maps the n-tuple, an element of k^n to an element of k. More specifically, the function

$$f : k^n \to k$$

is defined as follows: given $(a_1, a_2, \ldots, a_n) \in k^n$, replace every x_i with a_i in the expression for f. Since all of the coefficients, $a_\alpha \in k$, this operation yields an element $f(a_1, a_2, \ldots, a_n) \in k$.

Example 1. A task in $\mathbb{R}^2$ presented in a secondary algebra class, for example, might require one to find solutions to $y = x^2$. Students would make a list of the ordered pairs such as $(0,0), (1,1), (2,4)$ that satisfy the equation. They may also represent the equation geometrically by sketching the parabolic curve that represents all solutions to the equation. We can generalize this task by expressing the equation as $f(x,y) = y - x^2$, a function that maps ordered pairs to real numbers. For example, $f(3,17) = 17 - 3^2 = 8$. The ordered pair $(3,17)$ is not a point on the parabola defined by $y = x^2$. The only ordered pairs that will be on the curve are those that are mapped to zero. Since $f(2,4) = 4 - 2^2 = 0$, the point $(2,4)$ will be on the curve. The secondary school task is a special case of this mapping in which we map n-tuples to the zero element of the field.

When we think of a polynomial as a function, the connection between algebra and geometry becomes more detectable.

2.2 Affine Varieties

The study of algebraic geometry has at its core the solution set of a system of polynomials. These solution sets are known as affine varieties. The definition and examples are the topic of this section.

Definition 2.7. [CLO15] Let k be a field, and let $f_1, f_2, \ldots, f_s$ be polynomials in $k[x_1, x_2, \ldots, x_n]$. Then we set

$$\mathbf{V}(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid f_i(a_1, a_2, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}.$$

We call $\mathbf{V}(f_1, f_2, \ldots, f_s)$ the *affine variety* defined by $f_1, f_2, \ldots, f_s$.

In other words, an affine variety is a collection of n-tuples representing the solutions to a system of equations. We are specifically interested in the n-tuples that satisfy $f_1(x_1, x_2, \ldots, x_n) = 0,\ f_2(x_1, x_2, \ldots, x_n) = 0, \ldots, f_s(x_1, x_2, \ldots, x_n) = 0$. When we have a solution to $f(x_1, x_2, \ldots, x_n) = 0$ we say f *vanishes* at $(x_1, x_2, \ldots, x_n)$.

We will continue to examine the task posed in Example 1 in the context of a variety so that we may extend the understanding of the relationship between the algebraic representation (the system of polynomials) and the geometric representation (the ordered pairs in the Cartesian Plane).

Consider $\mathbf{V}(y - x^2)$. We want to find the collection of ordered pairs $(x,y) \in \mathbb{R}^2$ such that $y - x^2 = 0$. As shown above, this is the set of points on the standard parabola

$y = x^2$ that has its vertex at the origin and is sometimes called the parent graph of parabolas. The variety contains infinitely many ordered pairs. This variety has only one polynomial but we can include any finite number of polynomials. For more complicated systems of equations, there are computer programs available to help us determine a solution set which we can interpret as a variety. Technology can also help us represent the variety geometrically, particularly if we are working in $\mathbb{R}^2$ or $\mathbb{R}^3$.

Example 2. Consider $\mathbf{V}(y-x^2,\ y-x-2)$. We want the set of ordered pairs $(x, y) \in \mathbb{R}^2$ that satisfy both equations, $y - x^2 = 0$ and $y - x - 2 = 0$. This system can be solved using substitution and yields two solutions, $(-1, 1)$ and $(2, 4)$, representing the points where the parabola and line intersect in the Cartesian Plane. So, $\mathbf{V}(y-x^2,\ y-x-2) = \{(-1,1),\ (2,4)\}$.

It is possible for a variety to be empty. In $\mathbb{R}^2$, we would have two curves that never intersect. We might also want to know if there are other polynomials that could be included in our variety from Example 2. In other words, are there other polynomials that vanish at $(-1, 1)$ and $(2, 4)$? Before considering this question, we will examine some properties of affine varieties.

Lemma 2.8. [CLO15] *If V, $W \subset k^n$ are affine varieties, then so are $V \cap W$ and $V \cup W$.*

Proof. Suppose $V = \mathbf{V}(f_1, f_2, \ldots, f_s)$ and $W = \mathbf{V}(g_1, g_2, \ldots, g_t)$. To show that the intersection of affine varieties is an affine variety, we use double inclusion to show that

$$V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t).$$

First, we will show $V \cap W \subseteq \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$. Let's assume $(a_1, a_2, \ldots, a_n) \in V \cap W$. This means that $(a_1, a_2, \ldots, a_n) \in V$ and $(a_1, a_2, \ldots, a_n) \in W$. In other words, $f_i(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s$ and $g_j(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$. So, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$.

Now, we show $\mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t) \subseteq V \cap W$. Assume $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$. This means $f_i(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s$ and $g_j(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$. In other words, the n-tuple $(a_1, a_2, \ldots, a_n) \in V$ and $(a_1, a_2, \ldots, a_n) \in W$. Thus $(a_1, a_2, \ldots, a_n) \in V \cap W$. We have shown that $V \cap W = \mathbf{V}(f_1, \ldots, f_s, g_1, \ldots, g_t)$ which implies $V \cap W$ is an affine variety.

For the second part of the lemma, the union of affine varieties is an affine variety, we will use double inclusion to show

$$V \cup W = \mathbf{V}(f_i g_j \mid 1 \leq i \leq s,\ \ 1 \leq j\ \leq t).$$

First we will show $V \cup W \subseteq \mathbf{V}(f_i g_j)$. Let's assume $(a_1, a_2, \ldots, a_n) \in V \cup W$. Then $(a_1, a_2, \ldots, a_n) \in V$ or $(a_1, a_2, \ldots, a_n) \in W$. If $(a_1, a_2, \ldots, a_n) \in V$,
then $f_i(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s$. So the product

$$\begin{aligned} f_i g_j(a_1, a_2, \ldots, a_n) &= f_i(a_1, a_2, \ldots, a_n) g_j(a_1, a_2, \ldots, a_n) \\ &= 0 \cdot g_j(a_1, a_2, \ldots, a_n) \\ &= 0 \end{aligned}$$

for all $1 \leq j \leq t$. So, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_i g_j)$. On the other hand, if $(a_1, a_2, \ldots, a_n) \in W$, then $g_j(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$. So the product

$$\begin{aligned} f_i g_j(a_1, a_2, \ldots, a_n) &= f_i(a_1, a_2, \ldots, a_n) g_j(a_1, a_2, \ldots, a_n) \\ &= f_i(a_1, a_2, \ldots, a_n) \cdot 0 \\ &= 0 \end{aligned}$$

for all $1 \leq i \leq s$. So, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_i g_j)$.

Now we show $\mathbf{V}(f_i g_j) \subseteq V \cup W$. Assume $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_i g_j)$. Then $f_i g_j(a_1, a_2, \ldots, a_n) = f_i(a_1, a_2, \ldots, a_n) g_j(a_1, a_2, \ldots, a_n) = 0$ for all i and j. If $(a_1, a_2, \ldots, a_n) \in V$, then $(a_1, a_2, \ldots, a_n) \in V \cup W$ and the proof is complete. If $(a_1, a_2, \ldots, a_n) \notin V$ then then exists some $i_0 \in \{1, \ldots, s\}$ such that $f_{i_0}(a_1, a_2, \ldots, a_n) \neq 0$. But we have, for all j, $f_{i_0}(a_1, a_2, \ldots, a_n) g_j(a_1, a_2, \ldots, a_n) = f_{i_0} g_j(a_1, a_2, \ldots, a_n) = 0$ since $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_i g_j)$. Therefore, $g_j(a_1, a_2, \ldots, a_n) = 0$ for all j. In other words, $(a_1, a_2, \ldots, a_n) \in W$, which means $(a_1, a_2, \ldots, a_n) \in V \cup W$. Thus $\mathbf{V}(f_i g_j) \subseteq V \cup W$ and $V \cup W$ is an affine variety. □

The previous lemma can be extended to state that finite intersections and finite unions of affine varieties yield affine varieties. The proof would make use of the lemma repeatedly and induction on the number of varieties. For example, suppose V, W, $X \in k^n$ are affine varieties. Let $Z = V \cup W$. Then by Lemma 2.8, $Z \in k^n$ is an affine variety. Likewise, $Z \cup X$ is an affine variety, and so forth. Hence the finite union of affine varieties is an affine variety.

Similarly, let $Y = V \cap W$. Then by Lemma 2.8, $Y \in k^n$ is an affine variety. Likewise, $Y \cap X$ is an affine variety, and so forth. Hence the finite intersection of affine varieties is an affine variety. These properties will be useful when we determine a Groebner basis for an affine variety.

2.3 Ideals

The foundational algebraic object we need in our study of varieties is an ideal, a special kind of subset that contains the zero element and is closed under addition. Ideals are also closed under multiplication of an element in the ideal by an element in the ring. Ideals will give us the structure for computing with affine varieties.

Definition 2.9. [CLO15] A subset $I \subset k[x_1, x_2, \ldots, x_n]$ 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 $h \in k[x_1, x_2, \ldots, x_n]$, then $hf \in I$.

So, an ideal of a ring is a subring that "absorbs" elements of the ring. [Gal17]

Example 3. Consider the ring of integers $\mathbb{Z}$ and the subring of even integers $2\mathbb{Z}$. Since $0 \in 2\mathbb{Z}$, the sum of two even integers is even and the product of 2 and any integer is even, we can say $2\mathbb{Z} = \langle 2 \rangle$ is an ideal of $\mathbb{Z}$ generated by the integer 2.

Next we define an ideal generated by a finite number of polynomials.

Definition 2.10. [CLO15] Let $f_1, f_2, \ldots, f_s$ be polynomials in $k[x_1, x_2, \ldots, x_n]$. Then we define

$$\langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, h_2, \ldots, h_s \in k[x_1, x_2, \ldots, x_n] \right\}.$$

We call $\langle f_1, f_2, \ldots, f_s \rangle$ the *ideal generated by* $f_1, f_2, \ldots, f_s$ and the set of defining equations, $\{f_1, f_2, \ldots, f_s\}$ is called the *basis of the ideal*. If the ideal is generated by a single element, we call it a *principal ideal*. That is,

$$\langle f \rangle = \{hf \mid h \in k[x_1, x_2, \ldots, x_n]\}$$

is called the principal ideal generated by f.

Example 4. In $\mathbb{R}[x]$, the ring of polynomials with real coefficients, the ideal, $\langle x \rangle = \{h \cdot x \mid h \in k[x_1, x_2, \ldots, x_n]\}$ is the subset of polynomials with real coefficients whose constant term is zero. The graph of these polynomials pass through the origin. Since this ideal is generated by a single polynomial, it is a principal ideal.

Example 5. Though the ring of integers is not a field, let's consider the ring of polynomials whose coefficients are integers. One ideal of this ring is the subring of polynomials with constant terms that are even integers. That is, $I = \langle x, 2\rangle = \{h_1 \cdot x + h_2 \cdot 2 \mid h_1, h_2 \in \mathbb{Z}[x_1, x_2, \ldots, x_n]\}$.

The proof of the following lemma justifies that we call $\langle f_1, f_2, \ldots, f_s\rangle$, defined above, an ideal.

Lemma 2.11. [CLO15] *If* $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$, *then* $\langle f_1, f_2, \ldots, f_s\rangle$ *is an ideal of* $k[x_1, x_2, \ldots, x_n]$.

Proof. We will verify that $\langle f_1, f_2, \ldots, f_s\rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, \ldots, h_s \in k[x_1, x_2, \ldots, x_n] \right\}$ is an ideal by showing it satisfies the conditions set forth in Definition 2.9. The first condition is satisfied by noticing that $0 \in k[x_1, x_2, \ldots, x_n]$ and $0 = \sum_{i=1}^{s} 0 \cdot f_i$. So, $0 \in \langle f_1, f_2, \ldots, f_s\rangle$. Now suppose $f, g \in I$ and $p_1, p_2, \ldots, p_s, q_1, q_2, \ldots, q_s \in k[x_1, x_2, \ldots, x_n]$ such that $f = \sum_{i=1}^{s} p_i f_i$ and $g = \sum_{i=1}^{s} q_i f_i$. Then $f + g = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i = \sum_{i=1}^{s} (p_i + q_i) f_i \in I$. Finally, for $h \in k[x_1, x_2, \ldots, x_n]$, $hf = h\sum_{i=1}^{s} p_i f_i = \sum_{i=1}^{s} (hp_i) f_i \in I$. Since all conditions are satisfied, $I = \langle f_1, f_2, \ldots, f_s\rangle$ is an ideal. □

The proof confirms that if a polynomial can be written as a linear combination of $f_1, f_2, \ldots, f_s$, then it is a member of the ideal $\langle f_1, f_2, \ldots, f_s\rangle$. This relationship is useful when comparing ideals. Let I be an ideal such that $I \subset k[x_1, x_2, \ldots, x_n]$ and let $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$. Then the following statements are equivalent:

(i) $f_1, f_2, \ldots, f_s \in I$.

(ii) $\langle f_1, f_2, \ldots, f_s\rangle \subset I$.

Suppose, for example, we want to show $\langle x, y\rangle = \langle x - y,\ x + y\rangle$. We have $x = \frac{1}{2}(x+y) + \frac{1}{2}(x-y) \in \langle x+y,\ x-y\rangle$ and $y = \frac{1}{2}(x+y) - \frac{1}{2}(x-y) \in \langle x+y,\ x-y\rangle$. Thus, $\langle x, y\rangle \subset \langle x+y,\ x-y\rangle$. Likewise, $x+y = 1\cdot x + 1\cdot y \in \langle x, y\rangle$ and $x-y = 1\cdot x - 1\cdot y \in \langle x,\ y\rangle$. Thus $\langle x + y,\ x - y\rangle \subset \langle x, y\rangle$. So $\langle x, y\rangle = \langle x + y,\ x - y\rangle$.

We further explore the role of ideals with a proposition that states a variety depends on the ideal generated by its defining equations.

Proposition 2.12. [CLO15] *If $f_1, f_2, \ldots, f_s$ and $g_1, g_2, \ldots, g_t$ are bases of the same ideal in $k[x_1, x_2, \ldots, x_n]$, so that $\langle f_1, f_2, \ldots, f_s\rangle = \langle g_1, g_2, \ldots, g_t\rangle$, then $\mathbf{V}(f_1, f_2, \ldots, f_s) = \mathbf{V}(g_1, g_2, \ldots, g_t)$.*

Proof. We have $\langle f_1, f_2, \ldots, f_s\rangle = \langle g_1, g_2, \ldots, g_t\rangle$. We will show that $\mathbf{V}(f_1, f_2, \ldots, f_s) = \mathbf{V}(g_1, g_2, \ldots, g_t)$ by double inclusion. Let the n-tuple $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_1, f_2, \ldots, f_s)$. Then $f_1(a_1, a_2, \ldots, a_n) = 0,\ f_2(a_1, a_2, \ldots, a_n) = 0, \ldots, f_s(a_1, a_2, \ldots, a_n) = 0$. In other words, for all $1 \leq i \leq s,\ f_i$ vanishes at $(a_1, a_2, \ldots, a_n)$. Consider $(h_1f_1 + h_2f_2 + \cdots + h_sf_s)(a_1, a_2, \ldots, a_n)$ for some $h_1, h_2, \ldots, h_s \in k[x_1, x_2, \ldots, x_n]$. Since $(a_1, a_2, \ldots, a_n)$ is a point where all f_i vanish, $(h_1f_1 + h_2f_2 + \cdots + h_sf_s)(a_1, a_2, \ldots, a_n) = 0$. But since $\langle f_1, f_2, \ldots, f_s\rangle = \langle g_1, g_2, \ldots, g_t\rangle$, there exist $j_1, j_2, \ldots, j_t \in k[x_1, x_2, \ldots, x_n]$ such that $h_1f_1+h_2f_2+\cdots+h_sf_s = j_1g_1+j_2g_2+\cdots+j_tg_t$. So $(j_1g_1+j_2g_2+\cdots+j_tg_t)(a_1, a_2, \ldots, a_n) = 0$. Thus $\mathbf{V}(g_1, g_2, \ldots, g_t) \subseteq \mathbf{V}(f_1, f_2, \ldots, f_s)$.

Similarly, let the n-tuple $(b_1, b_2, \ldots, b_n) \in \mathbf{V}(g_1, g_2, \ldots, g_t)$. Then for all $1 \leq i \leq t,\ g_i$ vanishes at $(b_1, b_2, \ldots, b_n)$. Consider $(j_1g_1 + j_2g_2 + \cdots + j_tg_t)(b_1, b_2, \ldots, b_n)$ for some $j_1, j_2, \ldots, j_t \in k[x_1, x_2, \ldots, x_n]$. Since $(b_1, b_2, \ldots, b_n)$ is a point where all g_i vanish $(j_1g_1 + j_2g_2 + \cdots + j_tg_t)(b_1, b_2, \ldots, b_n) = 0$. But $h_1f_1 + h_2f_2 + \cdots + h_sf_s = j_1g_1 + j_2g_2 + \cdots + j_tg_t$, so $(h_1f_1 + h_2f_2 + \cdots + h_sf_s)(b_1, b_2, \ldots, b_n) = 0$. Thus $\mathbf{V}(f_1, f_2, \ldots, f_s) \subseteq \mathbf{V}(g_1, g_2, \ldots, g_t)$. Hence, if $\langle f_1, f_2, \ldots, f_s\rangle = \langle g_1, g_2, \ldots, g_t\rangle$, then $\mathbf{V}(f_1, f_2, \ldots, f_s) = \mathbf{V}(g_1, g_2, \ldots, g_t)$. □

The ability to change the basis of an ideal without affecting the variety is a powerful tool in determining varieties.

Next we will study another class of ideals, ideals of varieties. The ideal of a variety consists of all the polynomials that vanish on a given variety.

Definition 2.13. [CLO15] Let $V \subset k^n$ be an affine variety. Then we set

$$\mathbf{I}(V) = \{f \in k[x_1, x_2, \ldots, x_n] \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } (a_1, a_2, \ldots, a_n) \in V\}.$$

The proof of the following lemma justifies that we call $\mathbf{I}(V)$ an ideal.

Lemma 2.14. [CLO15] *If $V \subset k^n$ is an affine variety, then $\mathbf{I}(V) \subset k[x_1, x_2, \ldots, x_n]$ is an ideal. We will call $\mathbf{I}(V)$ the ideal of V.*

Proof. We will show that $\mathbf{I}(V)$ satisfies the three conditions set forth in the definition of an ideal. The zero polynomial vanishes on all n-tuples, so in particular it vanishes on V. Thus $0 \in \mathbf{I}(V)$. Let $(a_1, a_2, \ldots, a_n)$ be an arbitrary element of the variety V.

Consider polynomials $f, g \in \mathbf{I}(V)$. Then by Definition 2.13, $f(a_1, a_2, \ldots, a_n) = 0$ and $g(a_1, a_2, \ldots, a_n) = 0$. So the sum,

$$\begin{aligned}(f+g)(a_1, a_2, \ldots, a_n) &= f(a_1, a_2, \ldots, a_n) + g(a_1, a_2, \ldots, a_n) \\ &= 0 + 0 \\ &= 0\end{aligned}$$

Hence, $f + g \in \mathbf{I}(V)$. Finally, let $f \in \mathbf{I}(V)$ and $h \in k[x_1, x_2, \ldots, x_n]$. Then the product

$$\begin{aligned}(hf)(a_1, a_2, \ldots, a_n) &= h(a_1, a_2, \ldots, a_n) f(a_1, a_2, \ldots, a_n) \\ &= h(a_1, a_2, \ldots, a_n) \cdot 0 \\ &= 0.\end{aligned}$$

Hence, $hf \in \mathbf{I}(V)$. Since all conditions are satisfied, $\mathbf{I}(V)$ is an ideal. □

We see that we can construct an ideal by starting with a set of polynomials and generating an ideal directly from them or we can consider the set of points on which the polynomials vanish and construct an ideal of the variety. It is natural to ask if the ideal of the variety is equivalent to the ideal generated by the polynomials. The following lemma addresses this question.

Lemma 2.15. [CLO15] *Let* $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$. *Then* $\langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$, *although equality need not occur.*

Proof. Let $f \in \langle f_1, f_2, \ldots, f_s \rangle$. Let $(a_1, a_2, \ldots, a_n)$ be an arbitrary element of $V(f_1, f_2, \ldots, f_s)$. We will show $f \in \mathbf{I}(\mathbf{V})$. If $f \in \langle f_1, f_2, \ldots, f_s \rangle$ then $f = \sum_{i=1}^{s} h_i f_i$ for some polynomials $h_1, h_2, \ldots, h_s \in k[x_1, x_2, \ldots, x_n]$. Then

$$\begin{aligned}f(a_1, a_2, \ldots, a_n) &= h_1 f_1(a_1, \ldots, a_n) + h_2 f_2(a_1, \ldots, a_n) + \cdots + h_s f_s(a_1, \ldots, a_n) \\ &= h_1(a_1, \ldots, a_n) f_1(a_1, \ldots, a_n) + h_2(a_1, \ldots, a_n) f_2(a_1, \ldots, a_n) \\ &\quad + \cdots + h_s(a_1, \ldots, a_n) f_s(a_1, \ldots, a_n) \\ &= h_1(a_1, \ldots, a_n) \cdot 0 + h_2(a_1, \ldots, a_n) \cdot 0 + \cdots + h_s(a_1, \ldots, a_n) \cdot 0 \\ &= 0.\end{aligned}$$

So, $f \in \mathbf{I}(\mathbf{V})$ and $\langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$. Now to show that equality need not occur, we present an example for which $\langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$

but $\mathbf{I}(\mathbf{V}(f_1, f_2, \cdots, f_s)) \not\subset \langle f_1, f_2, \ldots, f_s \rangle$. We use the first part of the proof. Consider $\langle x^2,\ y^2 \rangle \subseteq \mathbf{I}(\mathbf{V}(x^2,\ y^2))$. We can compute $\mathbf{I}(\mathbf{V}(x^2,\ y^2))$. Solving the equations $x^2 = 0$ and $y^2 = 0$ implies $\mathbf{V}(x^2,\ y^2) = \{(0,0)\}$, which is the origin in k^2. Then its ideal $\mathbf{I}(\{(0,0)\})$ is the set of polynomials that vanish at the origin, that is $\mathbf{I}(\mathbf{V}(x^2,\ y^2)) = \langle x,\ y \rangle$. We know $x \notin \langle x^2,\ y^2 \rangle$ since any linear combination of x^2 and y^2 will consist of monomials having total degree at least two. Hence $\langle x,\ y \rangle \not\subset \langle x^2,\ y^2 \rangle$ and so the ideals are not equal. $\square$

Chapter 3

Groebner Bases

To apply algebraic methods to solve geometric theorems such as the ones that will be presented in this thesis, we will express geometric structures as systems of polynomials $f_1(x_1, x_2, \ldots, x_n) = 0,\ f_2(x_1, x_2, \ldots, x_n) = 0, \ldots, f_s(x_1, x_2, \ldots, x_n) = 0$ and determine the solutions. This is restated geometrically as finding the n-tuples that are elements of the affine variety $\mathbf{V}(f_1, f_2, \ldots, f_s)$. We showed in the last chapter that the variety depends on the ideals generated by the defining polynomials. But we also showed that there is more than one basis for an ideal. Deriving a convenient basis is the key to solving our system. Groebner bases have the features we desire and in this chapter we define and understand the need for Groebner bases.

3.1 Orderings on the Monomials in $k[x_1, x_2, \ldots, x_n]$

We have defined the polynomials we will employ in our task of solving geometric theorems algebraically. We now turn to the dilemma mentioned in Section 2.1. When working with polynomials in more than one variable, the terms may be arranged in many ways. We define three commonly used lexicographic orderings in this section.

Definition 3.1. (Lex Order). [CLO15] Let $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Definition 3.2. (Graded Lex Order). [CLO15] Let $\alpha = (a_1, a_2, \ldots, a_n)$ and $\beta = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and } \alpha >_{lex} \beta.$$

Definition 3.3. (Graded Reverse Lex Order). [CLO15] Let $\alpha = (a_1, a_2, \ldots, a_n)$ and $\beta = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \text{ or } |\alpha| = |\beta| \text{ and the rightmost}$$

nonzero entry of $\alpha - \beta \in \mathbb{Z}^n$ is negative.

We return to our polynomial example from Section 2.1, $f(x, y, z) = 3x^3y^2z + \frac{5}{6}z^3 - 7x^4 + 9x^2y^4$ to demonstrate the difference in these three monomial orderings. The variables will have the order $x > y > z$. The orderings depend on the exponents of the monomials so we first express the exponents of each term as an n-tuple. Let $\alpha = (3, 2, 1)$ represent the term $3x^3y^2z$. We calculate the total degree of this monomial, $|\alpha| = 3 + 2 + 1 = 6$. For the term $\frac{5}{6}z^3$, we have $\beta = (0, 0, 3)$ with $|\beta| = 3$. For the term $-7x^4$, we have $\gamma = (4, 0, 0)$ and $|\gamma| = 4$. For the term $9x^2y^4$, we have $\delta = (2, 4, 0)$ and $|\delta| = 6$.

To arrange the terms in lex order, we compare the differences between the ordered triples. We look to the leftmost nonzero entry and arrange the triples in descending order based on these entries. Since the first entry in γ is larger than the first entry in the other triples, we conclude that the term $-7x^4$ will come first in the lex ordering. We see that $\delta - \alpha = (-1, 2, -1)$ but $\alpha - \delta = (1, -2, 1)$. Comparing the leftmost entries informs us that $3x^3y^2z$ is next. Since the leftmost entry of β is less than the leftmost entry of the other triples, we list the term $\frac{5}{6}z^3$ last. So, our polynomial in lex order is $f(x, y, z) = -7x^4 + 3x^3y^2z + 9x^2y^4 + \frac{5}{6}z^3$. We see that in lex order, we do not consider the total degree of the monomials. Our comparison is based only on the exponent of the first variable that has different exponents. This is the ordering one would see in a typical secondary algebra course.

In some cases, it may be advantageous to list the monomial with larger total degree first. In grlex ordering, monomials are listed in descending order by total degree. If two monomials have the same total degree, then we use lex ordering to decide which of those monomials is listed first. With our example, since $|\alpha| = |\delta| = 6$ and this total degree is greater than that of the other two monomials, we find the n-tuple differences to determine which term will hold first and second positions. The leftmost entry in $\alpha - \delta$ is 1 but the leftmost entry of $\delta - \alpha$ is -1, thus $\alpha > \delta$ in grlex ordering. Next is γ followed by β. So, in grlex order, our polynomial is $f(x, y, z) = 3x^3y^2z + 9x^2y^4 - 7x^4 + \frac{5}{6}z^3$.

Now we write our polynomial in grevlex order. As with grlex order, our first comparison is with the total degrees. However, when two or more monomials have the same total degree, we look at the rightmost nonzero entry of the n-tuple differences. As above, we need to decide if $9x^2y^4$ or $3x^3y^2z$ will be placed first. The rightmost entry in $\alpha - \delta$ is 1 and the rightmost entry of $\delta - \alpha$ is -1. According to grevlex order, $\delta > \alpha$ and our polynomial is $f(x, y, z) = 9x^2y^4 + 3x^3y^2z - 7x^4 + \frac{5}{6}z^3$. Once we have selected a monomial ordering, we can express a polynomial without ambiguity, which is especially helpful in addressing the following terminology.

Definition 3.4. [CLO15] Let $f = \sum_{\alpha} a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1, x_2, \ldots, x_n]$ and let $>$ be a monomial ordering.

1. The *multidegree* of f is

$$\text{multideg}(f) = \max(\alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha \neq 0).$$

   The maximum is taken with respect to the monomial ordering, $>$.

2. The *leading coefficient* of f is

$$\text{LC}(f) = a_{\text{multideg}(f)} \in k.$$

3. The *leading monomial* of f is

$$\text{LM}(f) = x^{\text{multideg}(f)}$$

   (with coefficient 1).

4. The *leading term* of f is

$$\text{LT}(f) = \text{LC}(f) \cdot \text{LM}(f).$$

We return again to our polynomial and illustrate the above terminology. With respect to graded lex order, $f(x, y, z) = 3x^3y^2z + 9x^2y^4 - 7x^4 + \frac{5}{6}z^3$. Then

$$\begin{aligned} \text{multideg}(f) &= (3, 2, 1), \\ \text{LC}(f) &= 3, \\ \text{LM}(f) &= x^3y^2z, \\ \text{LT}(f) &= 3x^3y^2z. \end{aligned}$$

Identifying the leading term of polynomials is necessary when we want to work systematically with a system of polynomials.

3.2 Division Algorithms

One systematic way we work with polynomials is to determine if one polynomial can be expressed as a product of other polynomials. When working with polynomials of one variable, we may use a division algorithm much like the division algorithm for integers one learns in primary school. Here we present a formal theorem describing the Division Algorithm for Integers from a Number Theory text.

Theorem 3.5. (Division Algorithm for Integers). [Bur11] *Given integers a and b, with $b \neq 0$, there exist unique integers q and r satisfying*

$$a = q \cdot b + r \qquad 0 \leq r < |b|.$$

The integers q and r are called, respectively, the *quotient* and *remainder* in the division of a by b.

Consider, for example, the integers -47 and 5. We can write $-47 = (-10)(5)+3$. We could also write $5 = (-47)(0) + 5$. We typically take the integer with the smaller absolute value as the divisor and take special notice of pairs of integers for which this division algorithm results in a remainder of zero, such as with $a = 32$ and $b = 8$. We can write $32 = 4 \cdot 8 + 0$. We say 4 and 8 are *factors* of 32 and 32 is a *multiple* of 4.

Now a division algorithm for polynomials in $k[x]$ that is analogous to the algorithm for integers is given by the following:

Theorem 3.6. (Division Algorithm for $k[x]$). [Gal17] *Let k be a field and let $f(x)$, $g(x) \in k[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $k[x]$ such that $f(x) = q(x) \cdot g(x) + r(x)$ and either $r(x) = 0$ or the degree of $r(x)$ is less than the degree of $g(x)$.*

The polynomials $q(x)$ and $r(x)$ are called the *quotient* and *remainder* in the division of $f(x)$ by $g(x)$. When the ring of coefficients of a polynomial ring is a field, we can use the long division process to determine the quotient and remainder, as shown in the examples below.

Example 6. Let $f(x) = 3x^4 + 2x^3 - x^2 - x - 6$ and $g(x) = x^2 + 1$ be polynomials in $\mathbb{R}[x]$. Then we can divide $f(x)$ by $g(x)$ as follows,

$$
\begin{array}{r|l}
 & 3x^2+2x-4 \\
\hline
x^2+1 & 3x^4+2x^3-x^2-x-6 \\
 & \underline{-3x^4\qquad -3x^2\qquad\quad} \\
 & 2x^3-4x^2-x \\
 & \underline{-2x^3\qquad\quad -2x} \\
 & -4x^2-3x-6 \\
 & \underline{4x^2\qquad\quad +4} \\
 & -3x-2
\end{array}
$$

Now we have $q(x) = 3x^2 + 2x - 4$ and $r(x) = -3x - 2$ so we can write $f(x) = 3x^4 + 2x^3 - x^2 - x - 6 = (3x^2 + 2x - 4)(x^2 + 1) + (-3x - 2)$.

With polynomials in a single variable, we note that lex, grlex and grevlex all result in the same ordering. As with integer division, we are interested in cases when polynomial division yields a remainder of zero as in the next example.

Example 7. Consider $f(x) = x^3 - 8,\ g(x) = x - 2 \in \mathbb{R}[x]$. We can divide $f(x)$ by $g(x)$ as follows,

$$
\begin{array}{r|l}
 & x^2+2x+4 \\
\hline
x-2 & x^3\qquad\quad -8 \\
 & \underline{-x^3+2x^2\qquad} \\
 & 2x^2 \\
 & \underline{-2x^2+4x} \\
 & 4x-8 \\
 & \underline{-4x+8} \\
 & 0
\end{array}
$$

We can write $x^3 - 8 = (x^2 + 2x + 4)(x - 2)$ and say $x^2 + 2x + 4$ and $x - 2$ are factors of $x^3 - 8$. Furthermore, we can say $x^3 - 8 \in \langle x - 2 \rangle$, that is, $x^3 - 8$ is in the ideal generated by $x - 2$.

An important feature of division with polynomials with one variable is that the quotient and remainder are unique. This is not generally true when we work with multivariable polynomials. We notice in the next theorem that a monomial ordering must be specified. We will see in the examples that follow that when we change monomial ordering, we may get a different remainder. We can also generate different remainders by changing the order of the divisors.

Theorem 3.7. (Division Algorithm in $k[x_1, x_2, \ldots, x_n]$). [CLO15] *Let $>$ be a monomial order on $\mathbb{Z}^n_{\geq 0}$ and let $F = (f_1, f_2, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, x_2, \ldots, x_n]$. Then every $f \in k[x_1, x_2, \ldots, x_n]$ can be written as*

$$f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r,$$

where $q_i, r \in k[x_1, x_2, \ldots, x_n]$ and either $r = 0$ or r is a linear combination with coefficients in k, of monomials, none of which is divisible by any of $\mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s)$. We call r a **remainder** *on division by F. Furthermore, if $q_i f_i \neq 0$,*

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(q_i f_i).$$

Example 8. [CLO15] In this example, posed as an exercise in the Cox, Little, O'Shea text, we demonstrate the division algorithm for multivariable polynomials. We compute the remainder on division of $f = x^7y^2 + x^3y^2 - y + 1$ by the ordered set $F = (xy^2 - x,\ x - y^3)$. These polynomials are in $\mathbb{R}[x, y]$. We will use grlex order with $x > y$. Our polynomial f is already in grlex order and our divisors in grlex order are $f_1 = xy^2 - x$ and $f_2 = -y^3 + x$. We will use the graphical representation presented in The Teaching of Mathematics Journal [Zea13].

$$\begin{aligned} (x^7y^2 + x^3y^2 - y + 1) &: (xy^2 - x) = x^6 + x^2 \\ \underline{-(x^7y^2 - x^7 + x^3y^2 - x^3)} & \\ (x^7 + x^3 - y + 1) &: (-y^3 + x) = 0 \end{aligned}$$

If either $\mathrm{LT}(f_1)$ or $\mathrm{LT}(f_2)$ divided x^7, we would repeat the procedure. When a monomial ordering is selected, the algorithm always terminates because the multidegree of f is reduced in each iteration. In this case we obtain $q_1 = x^6 + x^2$, $q_2 = 0$ and the remainder, $r = x^7 + x^3 - y + 1$ and we have $f = (x^6 + x^2)(xy^2 - x) + 0(-y^3 + x) + (x^7 + x^3 - y + 1)$.

Example 9. We will work with the same polynomial f and ordered set F from Example 8 but this time we will use lex order. The arrangement of the terms of f and f_1 remain $f = x^7y^2 + x^3y^2 - y + 1$ and $f_1 = xy^2 - x$ but f_2 changes to $f_2 = x - y^3$. We can anticipate a change early in the division procedure since $\mathrm{LT}(f_2) = x$ divides x^7 so x^7 will not become part of the remainder. The procedure with the lex ordering required 14 iterations completed by hand and resulted with $q_1 = x^6 + x^5y + x^4 + x^3y + x^2y^2 + 2x + 2y$, $q_2 = x^6 + x^5y + x^4 + x^3y + 2x + 2y$, and $r = 2y^4 - y + 1$. When working with a large number

of variables and divisors, computer programs can efficiently produce the quotients and remainders.

The significance of these examples is that when we change the orderings on the monomials, the division algorithm yields different remainders. Moreover, if we reorder the set F, we have the potential to yield different remainders. When using lex order and using the ordered set $F = (f_2, f_1)$ the procedure involved eleven iterations resulting in eleven terms in q_1 with remainder $r = -y^{26} + y^{11} - y + 1$ but using this arrangement on the set F with grlex order, we obtain the same remainder as in Example 8.

Since none of our division procedures resulted in a remainder of zero, we may be tempted to conclude $f \notin \langle f_1, f_2 \rangle$ but we have not exhausted all possible monomial orderings. Our next example shows that despite one ordering resulting in a nonzero remainder, we cannot conclude the polynomial is not a member of the ideal.

Example 10. [Zea13] We will calculate the remainder on division of $f = x^2y^3 - 2xy^2 \in \mathbb{R}[x, y]$ by the ordered set $F = (y^3 + 4,\ x^2y - 2x) \in \mathbb{R}[x, y]$. We will use lex order with $x > y$ as follows,

$$\begin{array}{r} (x^2y^3 - 2xy^2) \ : \ (y^3 + 4) = x^2 \\ \underline{-(x^2y^3 + 4x^2)} \\ -2x^2y - 4x^2 \ : \ (x^2y - 2x) = 0 \end{array}$$

So, we obtain $x^2y^3 - 2xy^2 = x^2(y^3 + 4) + 0(x^2y - 2x) - 2xy^2 - 4x^2$. Suppose, however, we reorder the divisors and take $F = (f_2, f_1)$. Then we have

$$\begin{array}{r} (x^2y^3 - 2xy^2) \ : \ (x^2y - 2x) = y^2 \\ \underline{-(x^2y^3 - 2xy^2)} \\ 0 \ : \ (y^3 + 4) = 0 \end{array}$$

This time, we obtain $x^2y^3 - 2xy^2 = y^2(x^2y - 2x) + 0(y^3 + 4) + 0$. We observe that f, f_1, f_2 are unchanged regardless of which of the three monomial orderings we selected but the two cases produced different remainders due to the change in ordering of the divisors.

Hence, we find that $f \in \langle f_1, f_2 \rangle$ despite having a nonzero remainder when dividing f by the ordered set $F = (f_1, f_2)$. The need for a uniquely defined remainder on division is one of the motivations for the definition of the Groebner basis.

3.3 The Hilbert Basis Theorem and Groebner Bases

Deciding if a polynomial is in an ideal is referred to as the Ideal Membership Problem. In polynomial rings in one variable, the division algorithm uniquely determines the remainder and a remainder of zero tells us that a polynomial is a member of an ideal. When working with multivariable polynomials, we may obtain a remainder of zero with a particular monomial ordering or divisor order and that would be sufficient to determine that the polynomial is a member of the ideal. The dilemma is there are numerous orderings. The key, then, is to choose divisors which will be generators of the ideal that uniquely determine the remainder, regardless of the order. Based on our examples, it is reasonable to expect the leading terms to play a critical role in the selection of such divisors. This set of divisors is called a Groebner basis.

Definition 3.8. [CLO15] An ideal I is a *monomial ideal* if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, x_2, \ldots, x_n]$. In this case, we write $I = \langle x^\alpha \mid \alpha \in A \subset \mathbb{Z}^n_{\geq 0} \rangle$.

In other words, a monomial ideal is an ideal generated by monomials. If a monomial x^β lies in a monomial ideal I, then x^β must be divisible by x^α for some $\alpha \in A$. If a polynomial f is a member of a monomial ideal I then each term of f lies in I and f is a linear combination of the monomials in I. Another important feature of monomial ideals in $k[x_1, x_2, \ldots, x_n]$ is that they are finitely generated.

Lemma 3.9. (Dickson's Lemma). [CLO15] *A monomial ideal $I = \langle x^\alpha \mid \alpha \in A \rangle \subset k[x_1, x_2, \ldots, x_n]$ can be written in the form $I = \langle x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_s} \rangle$, where $\alpha_1, \alpha_2, \ldots, \alpha_s \in A$. In particular, I has a finite basis.*

Definition 3.10. [CLO15] Let $I \subset k[x_1, x_2, \ldots, x_n]$ be an ideal other than $\{0\}$ and fix a monomial ordering on the monomials of $k[x_1, x_2, \ldots, x_n]$.

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

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

It is important to recognize that if the ideal I is generated by a finite set of polynomials $f_1, f_2, \ldots, f_s$, then $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s)\rangle$ does not necessarily equal $\langle \mathrm{LT}(I)\rangle$. It follows from the definition that since $\mathrm{LT}(I) \subseteq \langle \mathrm{LT}(I)\rangle$ then $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s)\rangle \subseteq \langle \mathrm{LT}(I)\rangle$. In the following example we will show that $\langle \mathrm{LT}(I)\rangle \not\subset \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s)\rangle$ by finding a member of $\langle \mathrm{LT}(I)\rangle$ that is not a member of $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s)\rangle$.

Example 11. Suppose $I = \langle f_1, f_2\rangle \subset \mathbb{R}[x, y]$ where $f_1 = 2xy^2 - x$ and $f_2 = 3x^2y - y - 1$ and use grlex ordering with $x > y$. Then

$$f_3 = 3x(2xy^2 - x) - 2y(3x^2y - y - 1) = -3x^3 + 2y^2 + 2y.$$

So, $f_3 \in I$ and $\mathrm{LT}(f_3) = -3x^3 \in \mathrm{LT}(I)$. However, since $-3x^3$ is not divisible by either $2xy^2$ or $3x^2y$, the leading terms of f_1 and f_2, nor is it a linear combination of these monomials, then $-3x^3 \notin \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2)\rangle$.

Proposition 3.11. [CLO15] *Let $I \subset k[x_1, x_2, \ldots, x_n]$ be an ideal.*

(i) *$\langle \mathrm{LT}(I)\rangle$ is a monomial ideal.*

(ii) *There are $g_1, g_2, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t)\rangle$.*

Proof. (i) By Definition 3.4, for polynomial $f = \sum_{\alpha} a_\alpha x^\alpha \in k[x_1, x_2, \ldots, x_n]$, $\mathrm{LC}(f) \in k \subset k[x_1, x_2, \ldots, x_n]$ and $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$. By Definition 3.8, the collection of leading monomials, $\mathrm{LM}(f)$ for $f \in I \setminus\{0\}$, generate the monomial ideal $\langle \mathrm{LM}(f) \mid f \in I \setminus\{0\}\rangle$ and since $\mathrm{LT}(f)$ and $\mathrm{LM}(f)$ differ only by a nonzero constant, $\langle \mathrm{LM}(f) \mid f \in I \setminus\{0\}\rangle = \langle \mathrm{LT}(f) \mid f \in I \setminus\{0\}\rangle$ which, by Definition 3.10 equals $\langle \mathrm{LT}(I)\rangle$. Thus, $\langle \mathrm{LT}(I)\rangle$ is a monomial ideal.
(ii) By part (i), $\langle \mathrm{LT}(I)\rangle$ is a monomial ideal generated by $\mathrm{LM}(f)$ for $f \in I \setminus\{0\}$. Dickson's Lemma tells us that a monomial ideal has finitely many generators. That is, monomial ideal $I = \langle x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_t}\rangle$, where $\alpha_1, \alpha_2, \ldots, \alpha_t \in A \subset \mathbb{Z}^n_{\geq 0}$. So, for $g_1, g_2, \ldots, g_t \in I$, we can write $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_t)\rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t)\rangle$. □

We have shown that monomial ideals can be finitely generated. The next theorem extends the feature to all ideals.

Theorem 3.12. (Hilbert Basis Theorem). [CLO15] *Every ideal $I \subset k[x_1, x_2, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, g_2, \ldots, g_t\rangle$ for some $g_1, g_2, \ldots, g_t \in I$.*

Proof. If $I = \{0\}$ the ideal is generated by the finite set $\{0\}$. If, however, $I \neq \{0\}$, we can specify a monomial ordering on $k[x_1, x_2, \ldots, x_n]$ and consider the ideal of leading terms of $I, \langle \mathrm{LT}(I) \rangle$. Then we can employ Proposition 3.11 to construct a finite generating set $g_1, g_2, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$.

We have $g_1, g_2, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$. We will show that $I = \langle g_1, g_2, \ldots, g_t \rangle$ by double inclusion. Since $g_i \in I$, $1 \leq i \leq t$, $\langle g_1, g_2, \ldots, g_t \rangle \subset I$. To show that $I \subset \langle g_1, g_2, \ldots, g_t \rangle$, we let f be any polynomial in the ideal and show that f is in $\langle g_1, g_2, \ldots, g_t \rangle$. Since $f \in I$, we apply the Division Algorithm for multivariable polynomials given in Theorem 3.7 and show that the remainder must be zero. Using the selected monomial ordering, dividing f by the ordered set of divisors $(g_1, g_2, \ldots, g_t)$ yields

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_t g_t + r$$

where no term of r is divisible by any of $\mathrm{LT}(g_1)$, $\mathrm{LT}(g_2)$, ..., $\mathrm{LT}(g_t)$. Suppose $r \neq 0$. Our result from the division algorithm can be written

$$r = f - a_1 g_1 - a_2 g_2 - \cdots - a_t g_t$$

which shows r is a linear combination of the members of I. So, $r \in I$ which means $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle$. We have $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle$ which implies $\mathrm{LT}(r)$ is divisible by some $\mathrm{LT}(g_i)$. This contradicts the definition of a remainder found in our division algorithm. We conclude that $r = 0$, thus

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_t g_t.$$

This means $f \in \langle g_1, g_2, \ldots, g_t \rangle$ which shows that $I \subset \langle g_1, g_2, \ldots, g_t \rangle$. It follows that $I = \langle g_1, g_2, \ldots, g_t \rangle$. □

We saw in Example 11 that in general, for an ideal generated by a finite set of polynomials $g_1, g_2, \ldots, g_t$, $\langle \mathrm{LT}(I) \rangle$ need not equal $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle$. However, in the proof of the Hilbert Basis Theorem, we constructed an ideal with this property. The type of finite generating set, or basis, used is called a Groebner basis and is our next topic.

Definition 3.13. [CLO15] Fix a monomial order. A finite subset $G = \{g_1, g_2, \ldots, g_t\}$ of an ideal I is said to be a *Groebner Basis* if

$$\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle = \langle \mathrm{LT}(I) \rangle.$$

The next corollary follows from applying the Hilbert Basis Theorem to $\langle \mathrm{LT}(I) \rangle$.

Corollary 3.14. [CLO15] *Fix a monomial order. Then every ideal $I \subset k[x_1, x_2, \ldots, x_n]$ other than $\{0\}$ has a Groebner basis. Furthermore, any Groebner basis for an ideal is a basis of I.*

Before describing additional properties of Groebner bases and describing how to obtain Groebner bases, we note another consequence, a geometric consequence, of the Hilbert Basis Theorem. We recall that affine varieties were described as solution sets of systems of polynomial equations. Specifically, from Definition 2.7,
$\mathbf{V}(f_1, f_2, \ldots, f_s) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid f_i(a_1, a_2, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}$.
The following definition and proposition allow us to think about affine varieties in the context of ideals.

Definition 3.15. [CLO15] Let $I \subset k[x_1, x_2, \ldots, x_n]$ be an ideal. We will denote by $\mathbf{V}(I)$ the set

$$\mathbf{V}(I) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

Proposition 3.16. [CLO15] *$\mathbf{V}(I)$ is an affine variety. In particular, if $I = \langle f_1, \ldots, f_s \rangle$, then $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.*

Proof. Let I be any ideal of $k[x_1, \ldots, x_n]$. Then by the Hilbert Basis Theorem, I has a finite generating set. In other words, $I = \langle f_1, \ldots, f_s \rangle$ for some $f_i \in I$. We will show $\mathbf{V}(I) = \mathbf{V}(f_1, f_2, \ldots, f_s)$ by double inclusion. By Definition 3.15, $\mathbf{V}(I)$ is the collection of n-tuples that satisfy the polynomial equations $f = 0$ for all $f \in I$ and hence satisfies the polynomial equations $f_i = 0$ for $1 \leq i \leq s$ since $f_1, \ldots, f_s \in I$. Let $(a_1, a_2, \ldots, a_n)$ be such an n-tuple. Then $f_1(a_1, a_2, \ldots, a_n) = 0$, $f_2(a_1, a_2, \ldots, a_n) = 0, \ldots,$ $f_s(a_1, a_2, \ldots, a_n) = 0$. Thus $\mathbf{V}(I) \subset \mathbf{V}(f_1, f_2, \ldots, f_s)$. To show $\mathbf{V}(f_1, f_2, \ldots, f_s) \subset \mathbf{V}(I)$, we let $(a_1, a_2, \ldots, a_n)$ be any n-tuple in $\mathbf{V}(f_1, f_2, \ldots, f_s)$ and show that $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. For any $f \in I$,

$$f = h_1 f_1 + h_2 f_2 + \cdots + h_s f_s \text{ where } h_i \in k[x_1, x_2, \ldots, x_n].$$

Since $f_1, f_2, \ldots, f_s \in I$, we have

$$\begin{aligned} f(a_1, a_2, \ldots, a_n) &= h_1(a_1, \ldots, a_n) f_1(a_1, \ldots, a_n) + \cdots + h_s(a_1, \ldots, a_n) f_s(a_1, \ldots, a_n) \\ &= h_1(a_1, \ldots, a_n) \cdot 0 + \cdots + h_s(a_1, \ldots, a_n) \cdot 0 \\ &= 0. \end{aligned}$$

Therefore, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$, which implies $\mathbf{V}(f_1, f_2, \ldots, f_s) \subset \mathbf{V}(I)$. So we conclude $\mathbf{V}(I) = \mathbf{V}(f_1, f_2, \ldots, f_s)$. □

Now we have established that varieties are determined by ideals of polynomial rings. This is an important link between algebra and geometry.

3.4 Properties of Groebner Bases

We identified the need for uniquely determined remainders as a motivation for the definition of Groebner bases in Section 3.2. Now we will explore how that definition has the quality that the division of a polynomial f by a Groebner basis G yields the same remainder regardless of the ordering on the members of the basis. We showed that every nonzero ideal has a Groebner basis, so we will be able to determine if a polynomial is a member of an ideal by dividing by a Groebner basis and checking to see if the remainder is zero. We will not need to wonder if rearranging the divisors will give us a different remainder.

Proposition 3.17. [CLO15] *Let $G = \{g_1, g_2, \ldots, g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, x_2, \ldots, x_n]$ and let $f \in k[x_1, x_2, \ldots, x_n]$. Then there is a unique $r \in k[x_1, x_2, \ldots, x_n]$ with the following two properties:*

(i) *No term of r is divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.*

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

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

Proof. For the set of divisors, $G = \{g_1, g_2, \ldots, g_t\} \subseteq k[x_1, x_2, \ldots, x_n]$, the Division Algorithm in $k[x_1, x_2, \ldots, x_n]$, states that a polynomial $f \in k[x_1, x_2, \ldots, x_n]$, can be written

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_t g_t + r$$

with r having precisely the property listed in (i) and $q_1, q_2, \ldots, q_t \in k[x_1, x_2, \ldots, x_n]$. This implies $g = q_1 g_1 + q_2 g_2 + \cdots + q_t g_t \in I$ which satisfies (ii). This proves the existence of r. We prove that r is unique by contradiction. Suppose r and r' both satisfy conditions (i) and (ii). That is $f = g + r = g' + r'$. It follows that $r - r' = g' - g \in I$ which implies, as long as r and r' are different, $\mathrm{LT}(r - r') \in \langle \mathrm{LT}(r - r') \rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle$. This means $\mathrm{LT}(r - r')$ must be divisible by some member of $\langle \mathrm{LT}(I) \rangle$. This is a contradiction. Since r and r' satisfy condition (i), no term of r or r' is divisible by any of $\mathrm{LT}(g_i), 1 \leq i \leq t$. Therefore, r and r' are not different. In other words, the remainder on division of f by G is unique. □

Although uniqueness of remainders is significant in our effort to determine if a polynomial belongs in an ideal, the quotients produced by the division algorithm need not be unique.

Example 12. [CLO15] This example is posed as an exercise in the Cox, Little, O'Shea text. We are given $G = \{x + z, y - z\}$ is a Groebner basis for $I = \langle x + z, y - z\rangle$, the ideal generated by these polynomials using lex order with $x > y > z$. We divide the polynomial $f = xy$ by the ordered set of divisors $G = (x+z, y-z)$. Then we divide with the order of the divisors reversed. First,

$$\begin{array}{rcll} (xy) & : & (x+z) & = y \\ \underline{-(xy+yz)} & & & \\ -yz & : & (y-z) & = -z \\ \underline{-(-yz+z^2)} & & & \\ -z^2 & & & \end{array}$$

The remainder is $-z^2$ so, we obtain $xy = y(x + z) - z(y - z) - z^2$.
Now reversing the order of the divisors,

$$\begin{array}{rcll} (xy) & : & (y-z) & = x \\ \underline{-(xy-xz)} & & & \\ xz & : & (x+z) & = z \\ \underline{-(xz+z^2)} & & & \\ -z^2 & & & \end{array}$$

As expected, since we are dividing by a Groebner bases, the remainder here is also $-z^2$. However, the quotients were different producing $xy = x(y - z) + z(x + z) - z^2$.

Corollary 3.18. [CLO15] *Let* $G = \{g_1, g_2, \ldots, g_t\}$ *be a Groebner basis for an ideal* $I \subset k[x_1, x_2, \ldots, x_n]$ *and let* $f \in k[x_1, x_2, \ldots, x_n]$. *Then* $f \in I$ *if and only if the remainder on division of* f *by* G *is zero.*

Proof. ($\Rightarrow$) If the remainder on division of f by G is zero, then the Division Algorithm produces

$$f = q_1g_1 + q_2g_2 + \cdots + q_tg_t + 0$$

which means f is a linear combination of $g_1, g_2, \ldots, g_t$. Therefore, $f \in I$.
($\Leftarrow$) If $f \in I$ is given, then $f = f + 0$ satisfies the two conditions of Proposition 3.17 with $r = 0$ the resulting remainder on the division of f by G. □

This corollary leads us to an algorithm for solving the Ideal Membership Problem. In other words, when we satisfy the requirement of having a Groebner basis G for the ideal I, we need only to compute a remainder on division by G to determine if $f \in I$. We will determine how Groebner bases are derived in the next section. We will use the following notation for the remainder.

Definition 3.19. [CLO15] We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, f_2, \ldots, f_s)$. If F is a Groebner basis for $\langle f_1, f_2, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order) by Proposition 3.17.

Example 13. Using our new notation, we can express the remainder $r = -z^2$ from Example 12, $\overline{xy}^G = -z^2$.

Definition 3.20. [Zea13] Let $f,\ g \in k[x_1, x_2, \ldots, x_n]$ be nonzero polynomials.

(i) If multideg$(f) = \alpha$ and multideg$(g) = \beta$, then let $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i,\ \beta_i)$ for each i. We call x^γ the *least common multiple* of LM(f) and LM(g), written $x^\gamma = \text{lcm}(\text{LM}(f), \text{LM}(g))$.

(ii) The *S-polynomial* (S stands for "syzygy", from Latin *syzygia* "conjunction", or Greek, *syzygos* "yoke together") of f and g is the combination

$$S(f,\ g) = \tfrac{x^\gamma}{\text{LT}(f)} \cdot f - \tfrac{x^\gamma}{\text{LT}(g)} \cdot g.$$

Example 14. [Zea13] Let $f = x^4yz + x^2y^3z + xz$ and $g = 2x^2y^2z + xy^2 + xz^3$ in $\mathbb{Q}[x, y, z]$ with lex ordering. We have $\alpha = (4, 1, 1)$ and $\beta = (2, 2, 1)$ so $\gamma = (4, 2, 1)$. We compute the S-polynomial as follows:

$$\begin{aligned} S(f, g) &= \frac{x^4y^2z}{x^4yz}\ f - \frac{x^4y^2z}{2x^2y^2z}\ g \\ &= yf - \frac{1}{2}x^2g \\ &= -\frac{1}{2}x^3y^2 - \frac{1}{2}x^3z^3 + x^2y^4z + xyz. \end{aligned}$$

The S-polynomial is constructed in such a way that the leading terms of the two polynomials cancel each other. This is something the division algorithm did not always produce. "Once a basis contains all the possible S-polynomials of polynomials in the ideal generating set, there are no extra polynomials in $\langle \mathrm{LT}(I) \rangle$ that are not in $\langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_s) \rangle$". [Zea13] The use of S-polynomials helps develop a criterion for determining if a basis is a Groebner basis, as described in the next theorem.

Theorem 3.21. (Buchberger's Criterion). [CLO15] *Let I be a polynomial ideal. Then a basis $G = \{g_1, g_2, \ldots, g_t\}$ for I is a Groebner basis for I if and only if for all pairs $i \neq j$, the remainder on division of $S(g_i, g_j)$ by G (listed in some order) is zero.*

Example 15. We return to the set $G = \{x + z, y - z\}$ given in Example 12 to be a Groebner basis of $I = \langle x + z, y - z \rangle$ using lex ordering $x > y > z$. Now we will prove the set is a Groebner basis using Buchberger's Criterion. We begin by computing the S-polynomial $\mathrm{S}(g_1, g_2)$. Let $\alpha = \mathrm{multideg}(g_1) = (1, 0, 0)$ and $\beta = \mathrm{multideg}(g_2) = (0, 1, 0)$. Then $\gamma = (1, 1, 0)$ and $x^\gamma = \mathrm{lcm}(g_1, g_2) = xy$. Now the S-polynomial is

$$\begin{aligned} S(g_1, g_2) &= \frac{xy}{x}(x + z) - \frac{xy}{y}(y - z) \\ &= xy + yz - xy + xz \\ &= xz + yz. \end{aligned}$$

Now we use the division algorithm to determine if $\overline{xz + yz}^G$ is zero.

$$\begin{array}{rcll} (xz + yz) & : & (x + z) & = z \\ \underline{-(xz + z^2)} & & & \\ yz - z^2 & : & (y - z) & = z \\ \underline{-(yz - z^2)} & & & \\ 0 & & & \end{array}$$

The remainder on the division of $S(g_1, g_2)$ by G is zero. Therefore, by Buchberger's Criterion, we verify that G is a Groebner basis for the ideal.

This result may lead us to believe that a Groebner basis of an ideal is simply the set of polynomials that generate that ideal. The following example demonstrates that is not the case.

Example 16. Consider the ideal $I = \langle -x^2 + y, -x^3 + z \rangle$ and use lex ordering $x > y > z$. We will show that $F = \{-x^2+y, -x^3+z\}$ is not a Groebner basis. We begin by computing the S-polynomial $\mathrm{S}(f_1, f_2)$. Let $\alpha = \mathrm{multideg}(f_1) = (2,0,0)$ and $\beta = \mathrm{multideg}(f_2) = (3,0,0)$. Then $\gamma = (3,0,0)$ and $x^\gamma = \mathrm{lcm}(f_1, f_2) = x^3$. Now the S-polynomial is

$$\begin{aligned} S(f_1, f_2) &= \frac{x^3}{-x^2}(-x^2 + y) - \frac{x^3}{-x^3}(-x^3 + z) \\ &= -x(-x^2 + y) + (-x^3 + z) \\ &= x^3 - xy - x^3 + z \\ &= -xy + z. \end{aligned}$$

Now we use the division algorithm to determine if $\overline{(-xy+z)}^F$ is zero.

$$\begin{array}{rcll} (-xy + z) & : & (-x^2 + y) & = 0 \\ \underline{-0} & & & \\ -xy + z & : & (-x^3 + z) & = 0 \\ \underline{-0} & & & \\ -xy + z & & & \end{array}$$

The remainder on division of $S(f_1, f_2)$ by F is not zero so we conclude that, with the monomial ordering specified, F is not a Groebner basis for the ideal.

If F had been a Groebner basis, we know changing the order of the divisors would not produce a different remainder. However, changing the monomial ordering on the set F can produce a different remainder as shown in the next example.

Example 17. Using the same ideal and generating set as Example 16 but specifying lex ordering $y > z > x$, we have $G = \{y - x^2, z - x^3\}$ with $\alpha = (0,1,0)$ and $\beta = (0,0,1)$. Then $\gamma = (0,1,1)$ and $x^\gamma = yz$. Now the S-polynomial is

$$\begin{aligned} S(g_1, g_2) &= \frac{yz}{y}(y - x^2) - \frac{yz}{z}(z - x^3) \\ &= z(y - x^2) - y(z - x^3) \\ &= yx^3 - zx^2. \end{aligned}$$

Now using the division algorithm,

$$\begin{array}{rcll} (yx^3 - zx^2) & : & (y - x^2) & = x^3 \\ \underline{-(yx^3 - x^5)} & & & \\ -zx^2 + x^5 & : & (z - x^3) & = -x^2 \\ \underline{-(-zx^2 + x^5)} & & & \\ 0 & & & \end{array}$$

Since $\overline{yx^3 - zx^2}^G = 0$, we conclude G is a Groebner basis for the ideal when using lex $y > z > x$ ordering.

Buchberger's Criterion allows us to check a proposed generating set to determine if it is a Groebner basis. What shall we do if it is not? Fortunately, we need not guess at random. The bi-conditional nature of the criterion suggests a practical way to construct a Groebner basis.

3.5 Buchberger's Algorithm

Although we showed that every nonzero ideal has a Groebner basis, we cannot simply take the generating set of an ideal and assume it is a Groebner basis. The division algorithm terminates when none of the LT of the divisors can divide the LT of the dividend. If we want to extend the process so the division algorithm terminates with a remainder of zero, we need additional divisors. Bruno Buchberger, an Austrian mathematician, published an algorithm in 1960 that derives these additional divisors using division on S-polynomials. Buchberger invented the name Groebner bases in honor of his thesis advisor, Wolfgang Groebner.

Theorem 3.22. (Buchberger's Algorithm). [CLO15] *Let $I = \langle f_1, f_2, \ldots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm:*
Begin with the set of polynomials defining the ideal, $F = \{f_1, f_2, \ldots, f_s\}$ and specify a monomial ordering. Then,

1) Compute the S-polynomial $S(f_i, f_j)$ for each pair $\{f_i, f_j\}$ in F, $i \neq j$.

2) Divide each nonzero S-polynomial by the generating set F.

3) If the remainder $\overline{S(f_i, f_j)}^F \neq 0$, then adjoin $\overline{S(f_i, f_j)}^F$ to the set F so

$F' = F \cup \{\overline{S(f_i, f_j)}^F\}$. *Whenever* $S = 0$ *there is nothing new to add to the basis. Repeat steps 1 - 3 until the set* $F' = F$.

Buchberger's Algorithm is demonstrated in the next example.

Example 18. Consider the ideal $I = \langle f_1, f_2 \rangle$ in $k[x, y]$ where $f_1 = x^2y^2 + xy$ and $f_2 = y^4 - y^2$. Using lex ordering with $x > y$, we compute a Groebner basis using Buchberger's Algorithm. To compute the S-polynomial $S(f_1, f_2)$, we have $\alpha = (2, 2),\ \beta = (0, 4)$ so that $x^\gamma = x^2y^4$. Now,

$$\begin{aligned} S(f_1, f_2) &= \frac{x^2y^4}{x^2y^2}(x^2y^2 + xy) - \frac{x^2y^4}{y^4}(y^4 - y^2) \\ &= x^2y^4 + xy^3 - x^2y^4 + x^2y^2 \\ &= x^2y^2 + xy^3. \end{aligned}$$

Next we divide,

$$\begin{array}{rcl} (x^2y^2 + xy^3) & : & (x^2y^2 + xy) \ = 1 \\ \underline{-(x^2y^2 + xy)} & & \\ xy^3 - xy & : & (y^4 - y^2) \quad = 0 \\ \underline{-0} & & \\ xy^3 - xy \to & & \overline{S(f_1, f_2)}^F \end{array}$$

Since $\overline{S(f_1, f_2)}^F \neq 0$, we revise our basis to include this new polynomial. We'll call it f_3 and notice the remainder on division of $S(f_1, f_2)$ by the revised set $F' = \{f_1, f_2, f_3\}$ is zero. But we now need to compute $S(f_1, f_3)$ and $S(f_2, f_3)$ to continue the algorithm. First, for $S(f_1, f_3)$ we have $\alpha = (2, 2),\ \beta = (1, 3)$. So $x^\gamma = x^2y^3$ and

$$\begin{aligned} S(f_1, f_3) &= \frac{x^2y^3}{x^2y^2}(x^2y^2 + xy) - \frac{x^2y^3}{xy^3}(xy^3 - xy) \\ &= x^2y^3 + xy^2 - x^2y^3 + x^2y \\ &= x^2y + xy^2. \end{aligned}$$

Now, we divide,

$$\begin{array}{rcl} (x^2y+xy^2) & : & (x^2y^2+xy) \;\; = 0 \\ \underline{-0} & & \\ x^2y+xy^2 & : & (y^4-y^2) \;\;\;\; = 0 \\ \underline{-0} & & \\ x^2y+xy^2 & : & (xy^3-xy) \;\; = 0 \\ \underline{-0} & & \\ x^2y+xy^2 \to & & \overline{S(f_1,f_3)}^F \end{array}$$

Since $\overline{S(f_1,f_3)}^F \neq 0$, we call it f_4 and add it to our basis. We notice the remainder on division of $S(f_1,f_3)$ by $F''=\{f_1,f_2,f_3,f_4\}$ is zero. We continue the algorithm with $S(f_2,f_3)$ which gives us $\alpha=(0,4)$ and $\beta=(1,3)$. So $x^\gamma = xy^4$ and

$$\begin{aligned} S(f_2,f_3) &= \frac{xy^4}{y^4}(y^4-y^2) - \frac{xy^4}{xy^3}(xy^3-xy) \\ &= xy^4 - xy^2 - xy^4 + xy^2 \\ &= 0. \end{aligned}$$

Since $S(f_2,f_3)=0$, we have nothing new to add to the basis. We still need to compute S-polynomials pairing $f_4 = x^2y+xy^2$ with each of $f_1 = x^2y^2+xy$, $f_2 = y^4-y^2$, and $f_3 = xy^3-xy$. First,

$$\begin{aligned} S(f_1,f_4) &= \frac{x^2y^2}{x^2y^2}(x^2y^2+xy) - \frac{x^2y^2}{x^2y}(x^2y+xy^2) \\ &= -xy^3+xy. \end{aligned}$$

We notice that $S(f_1,f_4) = -f_3$ so $\overline{S(f_1,f_4)}^F = 0$ giving us nothing new to add to the basis. Proceeding with the the next S-polynomial,

$$\begin{aligned} S(f_2,f_4) &= \frac{x^2y^4}{y^4}(y^4-y^2) - \frac{x^2y^4}{x^2y}(x^2y+xy^2) \\ &= -x^2y^2 - xy^5. \end{aligned}$$

Now we divide $S(f_2, f_4)$ by $\{f_1, f_2, f_3, f_4\}$,

$$\begin{array}{rcl} (-x^2y^2 - xy^5) & : & (x^2y^2 + xy) \ = -1 \\ \underline{-(-x^2y^2 - xy)} & & \\ -xy^5 + xy & : & (xy^3 - xy) \quad = -y^2 \\ \underline{-(-xy^5 + xy^3)} & & \\ -xy^3 + xy & : & (xy^3 - xy) \ = -1 \\ \underline{-(-xy^3 + xy)} & & \\ 0 & & \end{array}$$

Since $\overline{S(f_2, f_4)}^F = 0$, there is nothing new to add to the basis. So we continue with

$$\begin{aligned} S(f_3, f_4) &= \frac{x^2y^3}{xy^3}(xy^3 - xy) - \frac{x^2y^3}{x^2y}(x^2y + xy^2) \\ &= -x^2y - xy^4. \end{aligned}$$

Now we divide $S(f_3, f_4)$ by $\{f_1, f_2, f_3, f_4\}$,

$$\begin{array}{rcl} (-x^2y - xy^4) & : & (x^2y + xy^2) \ = -1 \\ \underline{-(-x^2y - xy^2)} & & \\ -xy^4 + xy^2 & : & (xy^3 - xy) \quad = -y \\ \underline{-(-xy^4 + xy^2)} & & \\ 0 & & \end{array}$$

Since $\overline{(f_3, f_4)}^F = 0$, the set is unchanged and there are no more S-polynomials to compute. Hence, Buchberger's Algorithm renders the Groebner basis $F = \{x^2y^2 + xy, y^4 - y^2, xy^3 - xy, x^2y + xy^2\}$ for $I = \langle x^2y^2 + xy, y^4 - y^2 \rangle$ on lex ordering with $x > y$.

Buchberger's Algorithm may render a Groebner basis that has more polynomials than necessary. These redundant generators can be eliminated and the reduced set will still be a Groebner basis.

Lemma 3.23. [CLO15] *Let G be a Groebner basis of $I \subseteq k[x_1, x_2, \ldots, x_n]$. Let $p \in G$ be a polynomial such that* LT $(p) \in \langle$ LT $(G \setminus \{p\}) \rangle$. *Then $G \setminus \{p\}$ is also a Groebner basis for I.*

Proof. Since G is a Groebner basis of I, we have $\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. Also since $\mathrm{LT}(p) \in \langle$ LT(G \{p}) $\rangle$ and is a monomial, we know $\mathrm{LT}(p)$ is divisible by $\mathrm{LT}(g_i)$ for some

$g_i \in G \setminus \{p\}$. So, by removing $\mathrm{LT}(p)$ from the set of generators, we still have a Groebner basis for I. That is $\langle \mathrm{LT}(G \setminus \{p\}) \rangle = \langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(I) \rangle$. □

The Groebner basis $G \setminus \{p\}$ will contain a minimal number of elements if all polynomials p with $\mathrm{LT}(p) \in \langle \mathrm{LT}(G \setminus \{p\}) \rangle$ are removed from G. We can further simplify the members g_i of a Groebner basis by scaling by $\frac{1}{\mathrm{LC}(g_i)}$. Below, we define a minimal Groebner basis.

Definition 3.24. [CLO15] Let $G = \{g_1, \ldots, g_s\}$ be a Groebner basis of an ideal $I \subset k[x_1, \ldots, x_n]$. Then G is a *minimal Groebner basis* if and only if for each $i = 1, 2, \ldots, s$, the polynomial g_i is monic and its leading monomial $\mathrm{LM}(g_i)$ does not divide $\mathrm{LM}(g_j)$ for any $i \neq j$.

Example 19. We return to the ideal I studied in Example 18. $I = \langle x^2y^2 + xy, y^4 - y^2 \rangle$. We produced a Groebner basis with four members,

$$\begin{aligned} g_1 &= x^2y^2 + xy \\ g_2 &= y^4 - y^2 \\ g_3 &= xy^3 - xy \\ g_4 &= x^2y + xy^2 \end{aligned}$$

The polynomials are all monic but we see that $\mathrm{LT}(g_1) = y \cdot \mathrm{LT}(g_4)$ so we can remove g_1 from the basis to obtain a minimal Groebner basis. This definition considers only the lead terms of the Groebner basis but we know the polynomials are linear combinations of the monomials in $\langle \mathrm{LT}(I) \rangle$ and so uniqueness of the minimal basis is not guaranteed. For uniqueness, we impose an additional restriction on the Groebner basis described below.

Definition 3.25. [CLO15] A *reduced Groebner basis* for a polynomial ideal I is a Groebner basis G for I such that:

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

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

So, a reduced Groebner basis verifies that the leading term of any polynomial in the basis does not divide any term of another polynomial in the basis.

Example 20. We return once more to the ideal of Example 18 and the minimal Groebner basis identified in Example 19, $G = \{y^4 - y^2, xy^3 - xy, x^2y + xy^2\}$. We can verify that

none of the leading terms $y^4,\ xy^3,\ x^2y$ divides any terms of the polynomials in G so we call G the reduced Groebner basis for I.

The Ideal Membership Problem was previously mentioned. As we apply algebraic techniques to proving geometric theorems, we will be concerned with determining if a polynomial is a member of an ideal. Suppose we are given two ideals in terms of their generators. We can determine if they are distinct ideals or the same ideal by examining the reduced Groebner basis. If the set of generators of the reduced Groebner basis for each ideal is the same, then the ideals they generate are the same. This fact alleviates ambiguity in our efforts.

Chapter 4

Algebra-Geometry Correspondence

Now that we have a method to make the study of ideals of polynomial rings more manageable, we return to the task of correlating ideals and varieties. This will enable the application of algebraic techniques to the proving of the geometric theorems to be presented in this thesis.

4.1 Hilbert's Nullstellenatz

An important relationship between ideals of polynomial rings and varieties was discovered and proven by David Hilbert in 1900. Nullstellenatz is a German word meaning theorem of zeros and will help us determine which ideals correspond to varieties.

In Section 2.3 we constructed a map from an affine variety $V \subset k^n$ to an ideal $\mathbf{I}(V)$ by defining $\mathbf{I}(V)$ to be the set of polynomials that vanish for each n-tuple in the variety. Conversely, if we have an ideal $I \subset k[x_1, x_2, \ldots, x_n]$, the variety of the ideal is the set of n-tuples that make all the polynomials in the ideal vanish. That is, $\mathbf{V}(I) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } f \in I\}$. Furthermore, Proposition 3.16 tells us that $\mathbf{V}(I)$ is an affine variety so we have a map from ideals of polynomial rings to affine varieties. These two maps give us a correspondence between ideals and varieties. It is natural to ask if the maps are one-to-one. We will show in the next example that different ideals can give the same variety so the map $I \to \mathbf{V}(I)$ is not one-to one.

Example 21. Consider the ideals $I = \langle x \rangle$ and $J = \langle x^2 \rangle \in k[x]$. Since $x \notin \langle x^2 \rangle$,

$\langle x \rangle \neq \langle x^2 \rangle$. However, $\mathbf{V}(I) = \mathbf{V}(J) = \{0\}$.

In the discussion following Example 2, we noted that a variety with more than one polynomial may be empty and that in $\mathbb{R}^2$ the graphical representation would be curves with no points in common. Consider also $V(y - x^2 - 1) \in \mathbb{R}^2$. The solutions to $y - x^2 - 1 = 0$ are $(i, 0)$ and $(-i, 0)$ but we would say $V(y - x^2 - 1) = \emptyset$ since these solutions are not in $\mathbb{R}^2$. In fact, the variety of any ideal generated by a polynomial with real coefficients that has no real roots will be empty. Our dilemma stems from the fact that we are not working in an algebraically closed field. In this section, we will study how working in an algebraically closed field eliminates the problem of having different ideals represent the empty variety. When working in an algebraically closed field, the only ideal whose corresponding variety is empty is the ideal that generates the entire ring. We begin with a lemma dealing with the one variable case when the ring is $k[x]$.

Lemma 4.1. [CLO15] *Let k be an algebraically closed field and let $I \subset k[x]$ be an ideal. Then $\mathbf{V}(I) = \emptyset$ if and only if $I = k[x]$.*

Proof. Since $k[x]$ is a principal ideal domain, any ideal in $k[x]$ can be generated by a single polynomial. That is, $I = \langle f \rangle$ for some polynomial $f \in k[x]$. The variety $\mathbf{V}(I)$ of the ideal is the set of $a \in k$ such that $f(a) = 0$. We are working with an algebraically closed field so every polynomial, except the constant polynomials, has a solution a for $f(a) = 0$. These solutions are called roots of the polynomial. Therefore, $\mathbf{V}(I) \neq \emptyset$ unless f is a nonzero constant. In the case where f is a nonzero constant, its multiplicative inverse, $g = \frac{1}{f}$ is also in k and as a result, $1 = g \cdot f \in I$. This means $p = p \cdot 1 \in I$ for all $p \in k[x]$. In other words, $I = k[x]$. Since every nonzero constant polynomial in the ring is also in the ideal and we know that a nonzero constant polynomial has no roots, the collection of polynomials in the ideal will not have a common root. So, when k is algebraically closed $I = k[x]$, the ideal that represents the entire ring, is the only ideal that yields $\mathbf{V}(I) = \emptyset$. □

This property also applies to rings of polynomials in more than one variable. As long as the coefficients come from an algebraically closed field, the only ideal of $k[x_1, x_2, \ldots, x_n]$ that yields an empty variety is the ideal that represents the entire ring. This result is precisely stated in the next theorem.

Theorem 4.2. (The Weak Nullstellenatz). [CLO15] *Let k be an algebraically closed field and let $I \subset k[x_1, x_2, \ldots, x_n]$ be an ideal. Then $\mathbf{V}(I) = \emptyset$ if and only if $I = k[x_1, x_2, \ldots, x_n]$.*

The proof uses induction on the number of variables and uses the lemma above as the base case. An important element of the proof is that $1 \in I$ if and only if $I = k[x_1, x_2, \ldots, x_n]$. If $1 \in k[x_1, x_2, \ldots, x_n]$, then $h = h \cdot 1 \in I$ for all $h \in k[x_1, x_2, \ldots, x_n]$. It follows that $I = k[x_1, x_2, \ldots, x_n]$. On the other hand, if $I = k[x_1, x_2, \ldots, x_n]$, then $1 \in k[x_1, x_2, \ldots, x_n] = I$. The remaining details of the proof are given on pages 177 - 178 of [CLO15].

To prove the geometric theorems in this thesis, we will need to show that the variety on the hypotheses and conclusions of the theorems is not empty. The polynomials that represent the hypotheses and conclusions will need to have a common zero. The Weak Nullstellensatz tells us that a variety $\mathbf{V}(f_1, f_2, \ldots, f_s) = \emptyset$ if and only if $1 \in \langle f_1, f_2, \ldots, f_s \rangle$. We saw in the last chapter that uniqueness is a feature of a reduced Groebner basis for an ideal. So we can observe that for any monomial ordering, $\{1\}$ is the only reduced Groebner basis of the ideal $\langle 1 \rangle = k[x_1, x_2, \ldots, x_n]$.

Although the Weak Nullstellensatz helps us determine if a system of polynomials with coefficients in an algebraically closed field has a solution, it does not guarantee that if there is a solution, that solution results from a unique ideal. Consider again the ideals given in Example 21. We saw that $\langle x \rangle \neq \langle x^2 \rangle$ but $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$. Now $0 \in \mathbb{C}$ and the field of complex numbers is algebraically closed. Hence, the map $I \to \mathbf{V}(I)$ is not one-to one despite working with an algebraically closed field. We can expand on this example to consider multivariable polynomials to better understand why the map is not one-to-one. Consider the ideals $\langle x, y \rangle$ and $\langle x^2, y \rangle$. Since $(x, y) \notin \langle x^2, y \rangle$, $\langle x, y \rangle \neq \langle x^2, y \rangle$. However, the variety on both these ideals is $\{(0, 0)\} \in \mathbb{C}^2$. In fact, if we consider any ideal of the form $\langle x^m, y^n \rangle$ where m and n are integers greater than one, the variety will be the same ordered pair. Thus a reason that the map fails to be one-to-one is that a power of a polynomial vanishes at the same point(s) as the original polynomial. The next theorem states that over an algebraically closed field, this is the only reason that the map fails to be one-to-one. If a polynomial f vanishes at all the points of some variety $\mathbf{V}(I)$ then the ideal must contain some power of the polynomial f.

Theorem 4.3. (Hilbert's Nullstellensatz). [CLO15] *Let k be an algebraically closed field. If $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$,* then $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$ *if and only if*

$$f^m \in \langle f_1, f_2, \ldots, f_s \rangle$$

for some $m \geq 1$.

Plan for proof. The proof of this theorem is not as straightforward as some other proofs we have examined. As such, we pause to engage in a problem solving strategy to help give some direction to the proof. We consider what we are given and what we want to show. We are given that a function is a member of an ideal. Specifically, the function is a member of an ideal of a variety. This means the function has a common zero with the other functions in the variety. We want to show that some power of the function is in the ideal generated by the functions that are in the variety. To prove this theorem we will need to introduce a power of the function f. Strategies learned in secondary algebra include raising both sides of an equation to a power and multiplying both sides of an equation by the desired power of f. To use either of these strategies, we need an equation. We know that if $f \in I$ we can write f as a linear combination of the functions in the ideal and the functions in the ring. We also must consider that we are working with the ideal of a variety and for f to be in the ideal, the variety must not be empty. We could attempt to find a solution, an n-tuple in the variety, but this may be a cumbersome process. Reflecting on the previous result, the Weak Nullstellensatz, brings to mind that it may be easier to prove a variety is empty. Clearly, if f has a common zero with the functions in the variety, $1 - f$ will not have a common zero with those functions. If we introduce a new ideal adjoining the original functions with $1 - f$, we could show that the variety on the ideal is empty. The advantage here is that we could then express 1 as a linear combination of f and the original functions. So far, we have a plan to show the variety is not empty but we have not found a way to introduce a power of f. We noted that we could multiply both sides of an equation by a power of f and this seems like a good approach since we can write an equation with 1 on one side of the equation. However, the other side of the equation would not give us what we desire. We need to have a linear combination that does not include f. Again we turn to secondary algebra and recall that multiplying by the reciprocal allows us to "cancel" an algebraic object. This leads us to introducing an extra variable that will be the multiplicative inverse of f.

To simplify the notation, a proof for the polynomial ring in two variables will be shown. The general proof is given on pages 179 - 180 in [CLO15].

Proof. For an algebraically closed field k, if $f_1, f_2, \ldots, f_s \in k[x_1, x_2]$, we want to show that given a nonzero polynomial f that vanishes at every ordered pair (a_1, a_2) for which $f_1, f_2, \ldots, f_s$ vanish there exists an integer $m \geq 1$ such that $f^m \in \langle f_1, f_2, \ldots, f_s \rangle$. For f^m to be in the ideal, there must be polynomials $A_1, A_2, \ldots, A_s \in k[x_1, x_2]$ so that f^m is a linear combination of A_i and f_i for $1 \leq i \leq s$. As described in the plan above, we

introduce a third variable x_3 and a new ideal $\tilde{I} = \langle f_1, f_2, \ldots, f_s, 1 - x_3 f \rangle \subseteq k[x_1, x_2, x_3]$. We will show $\tilde{I} = k[x_1, x_2, x_3]$. When $\tilde{I}$ is the entire ring, the variety $\mathbf{V}(\tilde{I})$ is empty. Let $(a_1, a_2, a_3) \in k^3$. There are two possibilities to consider. Either (a_1, a_2) is a common zero of $f_1, f_2, \ldots, f_s$ or it is not. We will show that in either case, $\mathbf{V}(\tilde{I}) = \emptyset$. First, if (a_1, a_2) is not a common zero of $f_1, f_2, \ldots, f_s$ there is some f_i with $1 \leq i \leq s$, such that $f_i(a_1, a_2) \neq 0$. Evaluating f_i at (a_1, a_2, a_3) does not change this result and having $f_i(a_1, a_2, a_3) \neq 0$ tells us $(a_1, a_2, a_3) \notin \mathbf{V}(\tilde{I})$. Hence, in this case, $\mathbf{V}(\tilde{I}) = \emptyset$.

Now, if (a_1, a_2) is a common zero of the polynomials $f_1, f_2, \ldots, f_s$ and we assume $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$, then $f(a_1, a_2) = 0$. For this case, we will show $\mathbf{V}(\tilde{I}) = \emptyset$ by contradiction. Suppose $(a_1, a_2, a_3) \in \mathbf{V}(\tilde{I})$. Since $1 - x_3 f \in \tilde{I}$, we expect $1 - x_3 f(a_1, a_2, a_3) = 0$. However, $1 - x_3 f(a_1, a_2, a_3) = 1 - x_3 \cdot 0 = 1$. Hence, $(a_1, a_2, a_3) \notin \mathbf{V}(\tilde{I})$ and we conclude $\mathbf{V}(\tilde{I}) = \emptyset$. Having $\mathbf{V}(\tilde{I}) = \emptyset$ allows us to apply the Weak Nullstellensatz to state $1 \in \tilde{I}$. Thus, we can write 1 as a linear combination of polynomials in $\tilde{I}$ and polynomials $p_1, p_2, \ldots, p_s, p$ in the ring $k[x_1, x_2, x_3]$ as follows:

$1 = p_1(x_1, x_2, x_3) f_1(x_1, x_2) + p_2(x_1, x_2, x_3) f_2(x_1, x_2) + \cdots + p_s(x_1, x_2, x_3) f_s(x_1, x_2) +$
$p(x_1, x_2, x_3)(1 - x_3 f(x_1, x_2))$.

Recalling from the plan for our proof that the purpose of introducing a third variable was to have the multiplicative inverse of our function, we let $x_3 = \frac{1}{f(x_1, x_2)}$ and our equation is

$1 = p_1(x_1, x_2, \frac{1}{f}) f_1(x_1, x_2) + p_2(x_1, x_2, \frac{1}{f}) f_2(x_1, x_2) + \cdots + p_s(x_1, x_2, \frac{1}{f}) f_s(x_1, x_2) +$
$p(x_1, x_2, \frac{1}{f})(1 - \frac{1}{f} \cdot f(x_1, x_2))$. Since $1 - \frac{1}{f} \cdot f(x_1, x_2) = 0$, we have

$1 = p_1(x_1, x_2, \frac{1}{f}) f_1(x_1, x_2) + p_2(x_1, x_2, \frac{1}{f}) f_2(x_1, x_2) + \cdots + p_s(x_1, x_2, \frac{1}{f}) f_s(x_1, x_2)$.

Now we can multiply both sides of the equation by f^m, where m is a positive integer large enough to clear all the denominators on the right side of the equation which gives us the desired result,

$f^m = A_1 f_1 + A_2 f_2 + \cdots + A_s f_s$ for polynomials $A_i \in k[x_1, x_2]$. □

The Nullstellensatz helps us express geometric objects with the precise language of algebra. The symbolic and numeric manipulation of algebraic objects give practical tools for applications such as the proofs included in this thesis.

4.2 Radical Ideals

As we continue to explore the connection between varieties and ideals, we consider the kinds of ideals that can be recognized as the ideal of a variety. In other words,

we want to identify those ideals that contain all the polynomials that vanish on some variety V. The following lemma reveals an important feature of such ideals.

Lemma 4.4. [CLO15] *Let V be a variety. If $f^m \in \boldsymbol{I}(V)$, then $f \in \boldsymbol{I}(V)$.*

Proof. Let V be a variety and a be an arbitrary n-tuple in V. We are assuming $f^m \in \mathbf{I}(V)$. This means that $(f(a))^m = 0$. But $(f(a))^m = 0$ only when $f(a) = 0$. Since a is an arbitrary n-tuple, then f vanishes for all $a \in \mathbf{I}(V)$. This means $f \in \mathbf{I}(V)$. □

This lemma tells us that an ideal consisting of all the polynomials that vanish on a particular variety V has the property that if some power of a polynomial is a member of the ideal, then the polynomial itself is a member of the ideal. We call such ideals *radical ideals* and provide the definition below.

Definition 4.5. [CLO15] An ideal I is a *radical ideal* if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.

This definition allows us to restate Lemma 4.4 to classify ideals of varieties as radical ideals. More precisely, for a given variety V, $\mathbf{I}(V)$ is a radical ideal.

Definition 4.6. [CLO15] Let $I \subset k[x_1, x_2, \ldots, x_n]$ be an ideal. The *radical of I*, denoted $\sqrt{I}$ is the set $\{f \mid f^m \in I \text{ for some integer } m \geq 1\}$.

Lemma 4.7. [CLO15] *If I is an ideal in $k[x_1, x_2, \ldots, x_n]$ then $\sqrt{I}$ is an ideal in $k[x_1, x_2, \ldots, x_n]$ containing I. Furthermore $\sqrt{I}$ is a radical ideal.*

Proof. To show that $I \subseteq \sqrt{I}$, consider any polynomial $f \in I$. Then $f^1 \in I$ and by Definition 4.6, $f \in \sqrt{I}$. Hence, $I \subseteq \sqrt{I}$.

To verify that $\sqrt{I}$ is an ideal, we need to show that $\sqrt{I}$ satisfies the three conditions of Definition 2.9. Since I is an ideal, $0 \in I$ and since $I \subseteq \sqrt{I}$, $0 \in \sqrt{I}$. Now suppose $f, g \in \sqrt{I}$. Then by Definition 4.6, there exist positive integers m and n such that $f^m, g^n \in I$. We need to show that $f + g \in \sqrt{I}$. Consider the binomial expansion $(f + g)^{m+n-1}$. From secondary algebra, we have that each term of the expansion has a factor $f^i g^j$ with $i + j = m + n - 1$. It follows that either $i \geq m$ or $j \geq n$ so that either f^i or g^j is in I. This means $f^i g^j \in I$ so that each term of the expansion is in I. Hence, $(f + g)^{m+n-1} \in I$ and by Definition 4.6, $f + g \in \sqrt{I}$. To satisfy the third condition, suppose $f \in \sqrt{I}$ and $h \in k[x_1, x_2, \ldots, x_n]$. Then $f^m \in I$ and $h^m \in k[x_1, x_2, \ldots, x_n]$ for some integer $m \geq 1$. We need to show $hf \in \sqrt{I}$. Since I is an ideal, $(hf)^m = h^m f^m \in I$. Hence, $hf \in \sqrt{I}$. Since all conditions are satisfied, $\sqrt{I}$ is an ideal.

Finally, to show $\sqrt{I}$ is a radical ideal, suppose $f^m \in \sqrt{I}$. Then by Definition 4.6, there is some integer $n \geq 1$ such that $(f^m)^n = f^{mn} \in I$. This implies $f \in \sqrt{I}$ since $mn \geq 1$. Hence, $\sqrt{I}$ is radical. □

With the introduction of radical ideals, the relationship between algebraic and geometric concepts can be more easily recognized in another form of Hilbert's Nullstellensatz.

Theorem 4.8. (The Strong Nullstellensatz). [CLO15] *Let k be an algebraically closed field. If I is an ideal in $k[x_1, x_2, \ldots, x_n]$, then*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Proof. Let k be an algebraically closed field and $I \subseteq k[x_1, x_2, \ldots, x_n]$ be an ideal. We will show $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ by double inclusion. First, let $f \in \sqrt{I}$ so that $f^m \in I$ for some integer $m \geq 1$. This means that f^m vanishes on $\mathbf{V}(I)$. In other words, $f^m(a_1, a_2, \ldots, a_n) = 0$ for all $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. But $f^m(a_1, a_2, \ldots, a_n) = (f(a_1, a_2, \ldots, a_n))^m$ which equals zero only when $f(a_1, a_2, \ldots, a_n) = 0$. In other words, f vanishes on $\mathbf{V}(I)$ so $f \in \mathbf{I}(\mathbf{V}(I))$ and $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$.

Conversely, let $f \in \mathbf{I}(\mathbf{V}(I))$ so that $f(a_1, a_2, \ldots, a_n) = 0$ for all $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. Since k is an algebraically closed field, we can apply Theorem 4.3 and conclude there exists some integer $m \geq 1$ such that $f^m \in I$. Hence, $f \in \sqrt{I}$ and $\mathbf{I}(\mathbf{V}(I)) \subseteq \sqrt{I}$. □

Now we re-examine the maps between ideals and varieties.

Theorem 4.9. (The Ideal-Variety Correspondence). [CLO15] *Let k be an arbitrary field.*

(i) *The maps*

$$\text{affine varieties} \xrightarrow{\mathrm{I}} \text{ideals}$$

and

$$\text{ideals} \xrightarrow{\mathrm{V}} \text{affine varieties}$$

are inclusion-reversing, i.e., if $I_1 \subseteq I_2$ are ideals, then $\boldsymbol{V}(I_1) \supseteq \boldsymbol{V}(I_2)$ and, similarly, if $V_1 \subseteq V_2$ are varieties, then $\boldsymbol{I}(V_1) \supseteq \boldsymbol{I}(V_2)$.

(ii) *For any variety V,*

$$\mathbf{V}(\mathbf{I}(V)) = V,$$

so that $\mathbf{I}$ *is always one-to-one. On the other hand, any ideal* I *satisfies*

$$\mathbf{V}(\sqrt{I}) = \mathbf{V}(I).$$

(iii) *If* k *is algebraically closed, and we restrict to radical ideals, then the maps*

$$\text{affine varieties} \xrightarrow{\text{I}} \text{radical ideals}$$

and

$$\text{radical ideals} \xrightarrow{\text{V}} \text{affine varieties}$$

are inclusion reversing bijections which are inverses of each other.

Proof. (i) First, we will show that the map $\mathbf{I}$ is inclusion reversing. That is, for varieties V_1 and V_2, we will show $V_1 \subseteq V_2$ implies $\mathbf{I}(V_2) \subseteq \mathbf{I}(V_1)$. Let $f \in \mathbf{I}(V_2)$. Then $f(a_1, \ldots, a_n) = 0$ for all n-tuples $(a_1, a_2, \ldots, a_n) \in V_2$. Since $V_1 \subseteq V_2$, $f(a_1, a_2, \ldots, a_n) = 0$ for all n-tuples in V_1. Hence, $f \in \mathbf{I}(V_1)$ and $\mathbf{I}(V_2) \subseteq \mathbf{I}(V_1)$.

Next we will show that the map $\mathbf{V}$ is inclusion reversing. For ideals I_1 and I_2 we will show $I_1 \subseteq I_2$ implies $\mathbf{V}(I_2) \subseteq \mathbf{V}(I_1)$. Consider the arbitrary n-tuple $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I_2)$. Then $f(a_1, a_2, \ldots, a_n) = 0$ for all polynomials $f \in I_2$. Since $I_1 \subseteq I_2$, the polynomials in I_1 are included in this collection of polynomials that vanish on $(a_1, a_2, \ldots, a_n)$. Hence, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ and $\mathbf{V}(I_2) \subseteq \mathbf{V}(I_1)$.

(ii) First we show that the map $\mathbf{I}$ is one-to-one by double inclusion. That is, we will show for any variety V, $\mathbf{V}(\mathbf{I}(V)) = V$. Let $V = \mathbf{V}(f_1, f_2, \ldots, f_s)$ be an affine variety and let $(a_1, a_2, \ldots, a_n) \in V$. Then for all $f \in \mathbf{I}(V)$, $f(a_1, a_2, \ldots, a_n) = 0$. This means the n-tuple $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(\mathbf{I}(V))$ and $V \subseteq \mathbf{V}(\mathbf{I}(V))$. To show the other inclusion, we note that each of the polynomials $f_1, f_2, \ldots, f_s \in \mathbf{I}(V)$ since V contains the n-tuples that make these polynomials vanish. Consequently, the ideal $\langle f_1, f_2, \ldots, f_s \rangle \subseteq \mathbf{I}(V)$. In part (i), we showed that the map $\mathbf{V}$ is inclusion reversing so when we apply the map to these ideals, we have $\mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(\langle f_1, f_2, \ldots, f_s \rangle) = V$. Hence, $\mathbf{V}(\mathbf{I}(V)) = V$ and $\mathbf{I}$ is one-to-one.

We will again use double inclusion to show $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$. We showed in the proof of Lemma 4.7 that $I \subseteq \sqrt{I}$ and by part (i) above we know the map $\mathbf{V}$ is inclusion

reversing so we have $\mathbf{V}(\sqrt{I}) \subseteq \mathbf{V}(I)$. For the other inclusion, consider an arbitrary n-tuple $a \in \mathbf{V}(I)$ and an arbitrary polynomial $f \in \sqrt{I}$. Then $f^m \in I$ for some $m \geq 1$. This means $f^m(a) = (f(a))^m = 0$ which implies $f(a) = 0$. In other words, $a \in \mathbf{V}(\sqrt{I})$ which means $\mathbf{V}(I) \subseteq \mathbf{V}(\sqrt{I})$. Hence, $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$.

(iii) We want to show that when k is an algebraically closed field and I is a radical ideal, $\mathbf{V}(\mathbf{I}(V)) = V$ and $\mathbf{I}(\mathbf{V}(I)) = I$. With Lemma 4.7 and Definition 4.5, we concluded that $\mathbf{I}(V)$ is a radical ideal and we showed in part (ii) that $\mathbf{V}(\mathbf{I}(V)) = V$. We know from the Strong Nullstellensatz $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ so we need to show that when I is radical, $\sqrt{I} = I$. We will use double inclusion to show the equality. Suppose I is radical. We showed in the proof of Lemma 4.7 that $I \subseteq \sqrt{I}$. To show the opposite inclusion, suppose that $f \in \sqrt{I}$. By Definition 4.5, there exists an integer $m \geq 1$ such that $f^m \in I$ and since I is radical, $f \in I$. Thus, $\sqrt{I} \subseteq I$. Consequently, when I is radical, $\sqrt{I} = I$ and by the Strong Nullstellensatz, for a radical ideal I, $\mathbf{I}(\mathbf{V}(I)) = I$. Hence the maps $\mathbf{I}$ and $\mathbf{V}$ are inverses of each other and define bijections between radical ideals and affine varieties. □

This result is pivotal in our effort to use algebraic methods to prove geometric theorems. We can now discuss varieties and radical ideals interchangeably when working in an algebraically closed field. We will express the hypotheses and conclusion(s) as polynomials. Then to determine if a conclusion polynomial vanishes on the same variety as the hypotheses, we will check to see if the conclusion polynomial is in the radical ideal generated by the set of hypothesis polynomials. The strategy used to prove Hilbert's Nullstellensatz is instrumental in checking for such membership as described in the next proposition.

Proposition 4.10. (Radical Membership). [CLO15] *Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then $g \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yg \rangle \subseteq k[x_1, \ldots, x_n, y]$, in which case $\tilde{I} = k[x_1, \ldots, x_n, y]$.*

Proof. Suppose $g \in \sqrt{I}$. By definition, $g^m \in I$ for some integer $m \geq 1$. Since $I \subseteq \tilde{I}$, we have $g^m \in \tilde{I}$. We also have $1 - yg \in \tilde{I}$. We want to show the polynomial 1 is a member of $\tilde{I}$. Notice that $1 = y^m g^m + (1 - y^m g^m)$ and by factoring the binomial $1 - y^m g^m$ we have

$$1 = y^m g^m + (1 - yg)(1 + yg + y^2 g^2 + \cdots + y^{m-1} g^{m-1}).$$

We already know $y^m g^m \in \tilde{I}$ since $g^m \in \tilde{I}$ and y^m is in the ring $k[x_1, x_2, \ldots, x_n, y]$. Also, since $1 - yg \in \tilde{I}$ and $(1 + yg + y^2g^2 + \cdots + y^{m-1}g^{m-1}) \in k[x_1, x_2, \ldots, x_n, y]$ we conclude that $1 - y^m g^m \in \tilde{I}$. Hence, by closure, $1 \in \tilde{I}$.

Conversely, suppose $1 \in \tilde{I}$. The proof of Hilbert's Nullstellensatz (Theorem 4.3) demonstrates that when $1 \in \tilde{I}$, g^m can be expressed as a linear combination of the polynomials in I and polynomials in the ring $k[x_1, x_2, \ldots, x_n]$. This means $g^m \in I$ and $g \in \sqrt{I}$. □

4.3 Operations on Ideals

Many natural operations on varieties correspond to natural operations on their ideals. Since ideals are algebraic objects, operations on ideals lend themselves to algorithms that can be efficiently completed with the aid of technology. This allows us to use the convenience of computer programs to work with varieties. Our primary objective in the geometric theorems to be presented in the next chapter is to determine if a conclusion polynomial vanishes on the same variety as the collection of hypothesis polynomials. The algorithm to determine radical membership plays a crucial role in our ability to use technology to complete this task.

In this section we define sums and products of ideals and show that these are also ideals. Then we show how these operations correspond to operations on varieties.

Definition 4.11. [CLO15] If I and J are ideals of the ring $k[x_1, x_2, \ldots, x_n]$, then the *sum of I and J*, denoted $I + J$, is the set

$$I + J = \{f + g \mid f \in I \text{ and } g \in J\}.$$

Proposition 4.12. [CLO15] *If I and J are ideals in $k[x_1, x_2, \ldots, x_n]$, then $I + J$ is also an ideal in $k[x_1, x_2, \ldots, x_n]$.*

Proof. To verify that $I + J$ is an ideal, we need to show that $I + J$ satisfies the three conditions of Definition 2.9. Since I and J are ideals, $0 \in I$ and $0 \in J$ so that $0 = 0 + 0 \in I + J$. Now suppose $h_1, h_2 \in I + J$. Then there exist $f_1, f_2 \in I$ and $g_1, g_2 \in J$ such that $h_1 = f_1 + g_1$ and $h_2 = f_2 + g_2$. Now $h_1 + h_2 = f_1 + g_1 + f_2 + g_2 = (f_1 + f_2) + (g_1 + g_2)$. Since I and J are ideals, $f_1 + f_2 \in I$ and $g_1 + g_2 \in J$ and by the definition of $I + J$, $h_1 + h_2 \in I + J$. To satisfy the third condition, suppose $h \in I + J$ and $p \in k[x_1, x_2, \ldots, x_n]$. Then, there exist $f \in I$ and $g \in J$ such that $h = f + g$. So, $p \cdot h = p \cdot (f + g) = p \cdot f + p \cdot g$

Since I and J are ideals, $p \cdot f \in I$ and $p \cdot g \in J$ and by the definition of $I+J$, $p \cdot h \in I+J$. Since all conditions are satisfied, $I+J$ is an ideal. □

Proposition 4.13. [CLO15] *Let $I = \langle f_1, f_2, \ldots, f_r \rangle$ and $J = \langle g_1, g_2, \ldots, g_s \rangle$. Then $I+J$ is the smallest ideal containing I and J. Furthermore, $I+J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.*

Proof. Suppose H is an ideal that contains I and J. Then H must contain all polynomials $f \in I$ and all polynomials $g \in J$. Since H is an ideal, all sums $f+g \in H$. In particular, $I+J \subseteq H$. Therefore, every ideal containing I and J contains $I+J$ and hence, $I+J$ must be the smallest ideal containing I and J.

We use double inclusion to show $I+J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. Since I and J are ideals, $0 \in I$ and $0 \in J$ so that $\langle f_1+0, f_2+0, \ldots, f_r+0,\ 0+g_1, 0+g_2, \ldots, 0+g_s \rangle = \langle f_1, f_2, \ldots, f_r, g_1, g_2, \ldots, g_s \rangle \subseteq I+J$. Now $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$ is an ideal that contains I and J so that $I+J \subseteq \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. Thus, $I+J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. □

We can generalize the equality of Proposition 4.13 as the following corollary.

Corollary 4.14. [CLO15] *If $f_1, f_2, \ldots, f_r \in k[x_1, x_2, \ldots, x_n]$, then*

$$\langle f_1, f_2, \ldots, f_r \rangle = \langle f_1 \rangle + \langle f_2 \rangle + \cdots + \langle f_r \rangle.$$

Next we consider the nature of the variety on the sum of ideals. Since the sum of two ideals must contain both ideals, the variety on the sum must include all the n-tuples where all polynomials in both ideals vanish. This collection is the intersection of the varieties of the two ideals as stated in the next theorem.

Theorem 4.15. [CLO15] *If I and J are ideals in $k[x_1, x_2, \ldots, x_n]$, then*

$$\boldsymbol{V}(I+J) = \boldsymbol{V}(I) \cap \boldsymbol{V}(J).$$

Proof. We use double inclusion to prove the equality. First, suppose the arbitrary n-tuple $a = (a_1, a_2, \ldots, a_n)$ is in $\boldsymbol{V}(I+J)$. Then $a \in \boldsymbol{V}(I)$ since $I \subseteq I+J$. Similarly, since $J \subseteq I+J$, $a \in \boldsymbol{V}(J)$. Hence, $a \in \boldsymbol{V}(I) \cap \boldsymbol{V}(J)$. Consequently, $\mathbf{V}(I+J) \subseteq \boldsymbol{V}(I) \cap \boldsymbol{V}(J)$.

Now, suppose $a \in \boldsymbol{V}(I) \cap \boldsymbol{V}(J)$. Then $a \in \boldsymbol{V}(I)$ and $a \in \boldsymbol{V}(J)$ so for all $f \in I,\ f(a) = 0$ and for all $g \in J,\ g(a) = 0$. Let h be any polynomial in $I+J$. Then there exist $f \in I$ and $g \in J$ such that $h = f+g$. Thus, $h(a) = f(a) + g(a) = 0 + 0 = 0$. Hence, $a \in \boldsymbol{V}(I+J)$. Consequently, $\boldsymbol{V}(I) \cap \boldsymbol{V}(J) \subseteq \boldsymbol{V}(I+J)$ and we conclude $\boldsymbol{V}(I+J) = \boldsymbol{V}(I) \cap \boldsymbol{V}(J)$. □

Now we explore the product of ideals and show that they correspond to the union of varieties.

Definition 4.16. [CLO15] If I and J are ideals of the ring $k[x_1, x_2, \ldots, x_n]$, then the *product of I and J*, denoted $I \cdot J$, is the set

$$I \cdot J = \{f_1 g_1 + \cdots + f_r g_r \mid f_1, \ldots, f_r \in I \text{ and } g_1, \ldots, g_r \in J,\ r \text{ a positive integer}\}.$$

Proposition 4.17. *If I and J are ideals in $k[x_1, x_2, \ldots, x_n]$ then $I \cdot J$ is also an ideal in $k[x_1, x_2, \ldots, x_n]$.*

Proof. To verify that $I \cdot J$ is an ideal, we need to show that $I \cdot J$ satisfies the three conditions of Definition 2.9. Since I and J are ideals, $0 \in I$ and $0 \in J$. So $0 = 0 \cdot 0 \in I \cdot J$ since we have a product of an element of I and an element of J. Now suppose $h_1, h_2 \in I \cdot J$. Then $h_1 = f_1 g_1 + f_2 g_2 + \cdots + f_r g_r$ where $f_i \in I$ and $g_i \in J$, $1 \leq i \leq r$. Also, $h_2 = f_1' g_1' + f_2' g_2' + \cdots + f_s' g_s'$ where $f_j' \in I$ and $g_j' \in J$, $1 \leq j \leq s$. Now the sum $h_1 + h_2 = f_1 g_1 + f_2 g_2 + \cdots + f_r g_r + f_1' g_1' + f_2' g_2' + \cdots + f_s' g_s'$ is comprised of terms that are the product of an element of I and an element of J. Thus, $h_1 + h_2 \in I \cdot J$. To satisfy the third condition, suppose $h \in I \cdot J$ and $p \in k[x_1, x_2, \ldots, x_n]$. Then $h = f_1 g_1 + f_2 g_2 + \cdots + f_r g_r$ where $f_i \in I$ and $g_i \in J$, $1 \leq i \leq r$. So, the product

$$\begin{aligned} p \cdot h &= p(f_1 g_1 + f_2 g_2 + \cdots + f_r g_r) \\ &= p f_1 g_1 + p f_2 g_2 + \cdots + p f_r g_r \\ &= (p f_1) g_1 + (p f_2) g_2 + \cdots (p f_r) g_r. \end{aligned}$$

For $1 \leq i \leq r$, each product $p f_i \in I$, since $p \in k[x_1, x_2, \ldots, x_n]$ and $f_i \in I$. Thus, each term of the product $p \cdot h$ is a product of an element from I and an element from J so that $p \cdot h \in I \cdot J$. Since all conditions are satisfied, $I \cdot J$ is an ideal. □

The product of the ideals I and J is not simply the set of products with one factor an element from I and the other factor an element from J. If we defined the product this way, we would not have a set that was closed under addition and the product $I \cdot J$ would not be an ideal. However, we can express the product $I \cdot J$ in terms of its generators when we are given the generators for both the ideals I and J.

Proposition 4.18. [CLO15] *Let $I = \langle f_1, f_2, \ldots, f_r \rangle$ and $J = \langle g_1, g_2, \ldots, g_s \rangle$. Then $I \cdot J$ is generated by the set of all products of generators of I and J:*

$$I \cdot J = \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle.$$

Proof. We use double inclusion to prove the equality. First, suppose $h \in \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. Then $h = \sum p_{ij} f_i g_j$ where $p_{ij} \in k[x_1, x_2, \ldots, x_n]$. Since each f_i is a member of the ideal I and each p_{ij} is a member of the ring, then each $p_{ij} f_i \in I$. Also, each $g_j \in J$ so that each term of the sum is a product of an element from I and an element from J which makes the sum an element of $I \cdot J$. Consequently, $\langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle \subseteq I \cdot J$. Now to show the opposite inclusion, we recall that each polynomial in $I \cdot J$ is a sum of polynomials of the form $f \cdot g$ with $f \in I$ and $g \in J$. But we can express f in terms of the generators $f_1, f_2, \ldots, f_r$ and g in terms of the generators $g_1, g_2, \ldots, g_s$. For polynomials $a_1, a_2, \ldots, a_r, b_1, b_2, \ldots, b_s \in k[x_1, x_2, \ldots, x_n]$, we have

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_r f_r \text{ and } g = b_1 g_1 + b_2 g_2 + \cdots + b_s g_s.$$

Thus, we can write products of the form $f \cdot g$ as

$$\begin{aligned} f \cdot g &= (a_1 f_1 + a_2 f_2 + \cdots + a_r f_r)(b_1 g_1 + b_2 g_2 + \cdots + b_s g_s) \\ &= a_1 f_1 b_1 g_1 + a_1 f_1 b_2 g_2 + \cdots + a_1 f_1 b_s g_s + a_2 f_2 b_1 g_1 + a_2 f_2 b_2 g_2 \\ &\quad + \cdots + a_2 f_2 b_s g_s + \cdots + a_r f_r b_s g_s \\ &= (a_1 b_1) f_1 g_1 + (a_1 b_2) f_1 g_2 + \cdots + (a_1 b_s) f_1 g_s + (a_2 b_1) f_2 g_1 + (a_2 b_2) f_2 g_2 \\ &\quad + \cdots + (a_2 b_s) f_2 g_s + \cdots + (a_r b_s) f_r g_s. \end{aligned}$$

Notice that for $1 \leq i \leq r$ and $1 \leq j \leq s$, $a_i b_j \in k[x_1, x_2, \ldots, x_n]$ so that the product $f \cdot g$ is in the ideal generated by the polynomials $f_i g_j$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. That is, products of the form $f \cdot g \in \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. Consequently, $I \cdot J \subseteq \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. Thus, $I \cdot J = \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. □

Next we consider the nature of the variety on the product of ideals. The next theorem states that the variety on the product of ideals corresponds to the union of the varieties.

Theorem 4.19. [CLO15] *If I and J are ideals in $k[x_1, x_2, \ldots, x_n]$, then*

$$\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J).$$

Proof. We use double inclusion to prove the equality. First, suppose $a = (a_1, a_2, \ldots, a_n)$ is an arbitrary n-tuple in $\mathbf{V}(I \cdot J)$. Then for all $f \in I$ and for all $g \in J$, $f(a)g(a) = 0$. We consider two possibilities, either $f(a) = 0$ for all $f \in I$ or $f(a) \neq 0$ for some $f \in I$. If $f(a) = 0$ for all $f \in I$, then $a \in \mathbf{V}(I)$. If $f(a) \neq 0$, for some $f \in I$, then we must have $g(a) = 0$ for all $g \in J$, in which case $a \in \mathbf{V}(J)$. In either case, $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$ and

$\mathbf{V}(I \cdot J) \subseteq \mathbf{V}(I) \cup \mathbf{V}(J)$. Conversely, suppose $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Then either $f(a) = 0$ for all $f \in I$ or $g(a) = 0$ for all $g \in J$. Thus, $f(a)g(a) = 0$ for all $f \in I$ and for all $g \in J$. So, for all $h \in I \cdot J$, $h(a) = 0$. This means $a \in \mathbf{V}(I \cdot J)$ and $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cdot J)$. Thus, $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J)$. □

4.4 Irreducible Varieties and Prime Ideals

We continue to explore the relationship between algebraic and geometric objects by considering one of the most fundamental topics studied in secondary algebra: how to know if an algebraic expression is in simplest form and if it is not, how to simplify it. This notion of simplifying is learned early in mathematics education. Children in primary school learning to make sense of numbers and quantities practice with money and are taught the simplest way to make change. They group types of coins and denominations of dollars so that they manage the fewest number of items. Students learn how to determine if fractions are in simplest form by checking for common factors in the numerator and denominator. This is extended to rational expressions where the numerators and denominators are polynomials that may need to be factored.

Simplifying algebraic objects is a familiar concept. In secondary geometry, we describe points, lines and planes as "undefined" objects but we need to determine what it means to simplify geometric objects. We need to know how to recognize when a geometric object is in simplest form. Specifically, we need to know how to recognize an irreducible variety. We begin this section with a definition and then take advantage of the correspondence between varieties and ideals to aid in this endeavor.

Definition 4.20. [CLO15] An affine variety $V \subseteq k^n$ is *irreducible* if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.

We notice that this definition depends on a variety being expressed as a union of two varieties. We showed in Section 2.2 that the finite union of affine varieties is an affine variety but we still do not have a clear method for decomposing a variety and proving that a variety is irreducible. Working with ideals allows us to take advantage of algebraic operations so we next explore which types of ideals correspond to irreducible varieties.

Definition 4.21. [CLO15] An ideal $I \subseteq k[x_1, x_2, \ldots, x_n]$ is *prime* if whenever $f,\ g \in k[x_1, x_2, \ldots, x_n]$ and $fg \in I$ then either $f \in I$ or $g \in I$.

Proposition 4.22. [CLO15] *Let $V \subseteq k^n$ be an affine variety. Then V is irreducible if and only if $\mathbf{I}(V)$ is a prime ideal.*

Proof. First, assume V is an irreducible variety and let $fg \in \mathbf{I}(V)$. We will show that $\mathbf{I}(V)$ is a prime ideal. Let $V_1 = V \cap V(f)$ and $V_2 = V \cap V(g)$. We showed in Section 2.2 that the intersection of two affine varieties is an affine variety so V_1 and V_2 are affine varieties. Since $fg \in \mathbf{I}(V)$, we can write $V = V_1 \cup V_2$. Since V is irreducible, either $V = V_1$ or $V = V_2$. Considering the first possibility, we would have $V = V_1 = V \cap V(f)$ which implies f vanishes on V. This means $f \in \mathbf{I}(V)$. If instead, $V = V_2$, we have $V = V \cap V(g)$ which implies g vanishes on V and $g \in \mathbf{I}(V)$. In either case, the definition of a prime ideal is satisfied.

Conversely, assume $\mathbf{I}(V)$ is a prime ideal and let $V = V_1 \cup V_2$. We will show the V is an irreducible variety. Without loss of generality, suppose $V \neq V_1$. We will use double inclusion to show $\mathbf{I}(V) = \mathbf{I}(V_2)$ so that we can conclude $V = V_2$ and satisfy the definition of an irreducible variety. Since $V = V_1 \cup V_2$, it must be true that $V_2 \subseteq V$ and by the Ideal-Variety Correspondence in Section 4.2, $\mathbf{I}(V) \subseteq \mathbf{I}(V_2)$. For the opposite inclusion, we recall $V = V_1 \cup V_2$ but that $V \neq V_1$. Hence, it must be true that $V_1 \subsetneq V$ and by the Ideal-Variety Correspondence, $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$. This means there must be some polynomial f such that $f \in \mathbf{I}(V_1)$ but $f \notin \mathbf{I}(V)$. Now let g be any polynomial in $\mathbf{I}(V_2)$ so that g vanishes on V_2. As a result, fg vanishes on V_2 and since $V = V_1 \cup V_2$, we can conclude fg vanishes on V. This means $fg \in \mathbf{I}(V)$. Our assumption is that $\mathbf{I}(V)$ is prime and according to the definition, either $f \in \mathbf{I}(V)$ or $g \in \mathbf{I}(V)$. But we chose a polynomial f that was not in $\mathbf{I}(V)$ which means $g \in \mathbf{I}(V)$. Hence, $\mathbf{I}(V_2) \subset \mathbf{I}(V)$. This proves $\mathbf{I}(V) = \mathbf{I}(V_2)$ and since the map $\mathbf{I}$ is one-to-one, $V = V_2$. We have shown that if $V = V_1 \cup V_2$ and $V \neq V_1$, then $V = V_2$ so we can conclude that V is an irreducible variety. □

We now have a way to verify that a variety is irreducible by examining the corresponding ideal. In the examples presented in this thesis, we will work with radical ideals so the following result will make the approach more direct.

Proposition 4.23. *Every prime ideal is radical.*

Proof. Let I be a prime ideal and assume $f^m \in I$ for some $m \geq 1$. We want to show that $f \in I$ which would make I a radical ideal. Suppose, on the contrary, that $f^m \in I$ but $m > 1$ so that $f \notin I$. Pick the smallest such m. We have $f \cdot f^{m-1} = f^m \in I$ and since I

is a prime ideal, either $f \in I$ or $f^{m-1} \in I$. But $f \notin I$ and by our choice of m, $f^{m-1} \notin I$. This contradiction proves that $m = 1$, so that $f \in I$. Hence, I is a radical ideal. □

Finally, we can combine the Ideal-Variety Correspondence between radical ideals and varieties to get the following corollary to Proposition 4.22.

Corollary 4.24. [CLO15] *When k is algebraically closed, the functions $\boldsymbol{I}$ and $\boldsymbol{V}$ induce a one-to-one correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, x_2, \ldots, x_n]$.*

Chapter 5

Proofs of Geometric Theorems using Algebraic Techniques

Our objective in this thesis is to demonstrate the proving of geometric theorems using algebraic methods. We will introduce Cartesian coordinates in the Euclidean plane. We can then write polynomial equations relating the coordinates of a collection of points specified in the hypotheses and conclusions of these theorems. When working with large systems of equations, having algebraic structure to represent geometric theorems enables the use of technology to efficiently verify conclusions of theorems. To use technology, however, we must have appropriate inputs and we must know how to interpret the results. A computer program can quickly perform algorithms but cannot do the planning. If we don't know what result we want, we won't know if the theorem is verified.

5.1 From Geometric Theorems to Polynomial Equations

The properties of geometric figures such lines, angles, polygons and circles are unchanged under translation and rotation in the Euclidean plane so when we introduce Cartesian coordinates, we may place the object of our theorem in any convenient location. The coordinates of some of the points will be arbitrary and others will be dependent on the arbitrary ones. It is common practice to use variables u_i to represent arbitrary values and x_i to represent coordinates determined by the arbitrary ones.

The following proposition lists the geometric statements we will use in the examples presented in this chapter.

Proposition 5.1. *Let A, B, C, D be distinct points in the plane. Then each statement*

can be expressed by one or more polynomial equations.

(i) *A, B, C are collinear.*

(ii) $\overline{AB}$ *is perpendicular to* $\overline{CD}$.

(iii) *The distance from A to B is equal to the distance from C to D:* $AB = CD$

(iv) *C is the midpoint of* $\overline{AB}$.

Proof. Let $A = (a_1, a_2),\ B = (b_1, b_2),\ C = (c_1, c_2)$ and $D = (d_1, d_2)$ be distinct points in the plane.

(i) The points A, B and C are collinear if the slopes of $\overline{AB}$ and $\overline{BC}$ are equal. Using the slope formula, we have

$$\tfrac{a_2-b_2}{a_1-b_1} = \tfrac{b_2-c_2}{b_1-c_1}$$

From this, we can obtain the polynomial equation

$$p_1 = (a_2 - b_2)(b_1 - c_1) - (a_1 - b_1)(b_2 - c_2) = 0.$$

(ii) To show $\overline{AB} \perp \overline{CD}$, we express $\overline{AB}$ as the vector $(b_1 - a_1, b_2 - a_2)$ and $\overline{CD}$ as the vector $(d_1 - c_1, d_2 - c_2)$. Then $\overline{AB} \perp \overline{CD}$ means the vectors are orthogonal. In other words, the dot product is zero. So we have

$$(b_1 - a_1, b_2 - a_2) \cdot (d_1 - c_1, d_2 - c_2) = 0$$

which gives the polynomial equation

$$p_2 = (b_1 - a_1)(d_1 - c_1) + (b_2 - a_2)(d_2 - c_2) = 0.$$

(iii) To show $AB = CD$, we use the distance formula to show $AB^2 = CD^2$.

$$AB^2 = (b_1 - a_1)^2 + (b_2 - a_2)^2$$
$$CD^2 = (d_1 - c_1)^2 + (d_2 - c_2)^2$$

Now $AB^2 = CD^2$ yields the polynomial equation

$$p_3 = (b_1 - a_1)^2 + (b_2 - a_2)^2 - (d_1 - c_1)^2 - (d_2 - c_2)^2 = 0$$

(iv) If C is the midpoint of $\overline{AB}$ then A, B and C are collinear and $AC = BC$ so we have the polynomial equations from statements (i) and (iii).

□

Other common geometric statements such as two lines are parallel, a point is on a circle, a line is tangent to a circle and a line bisects an angle can also be expressed as polynomials equations.

5.2 Example 1: The Centroid of a Triangle

In this example we will demonstrate how the Groebner Basis Algorithm can be used to prove a geometric theorem that is taken as given in many secondary geometry courses. It is expressed as a definition - that the centroid of a triangle is the point of concurrency of the three medians of the triangle.

Theorem 5.2. *Let ΔABC be a triangle in the plane. If we let M_1 be the midpoint of $\overline{BC}$, M_2 be the midpoint of $\overline{AC}$ and M_3 be the midpoint of $\overline{AB}$, then the segments $\overline{AM_1}$, $\overline{BM_2}$ and $\overline{CM_3}$ meet at a single point M, called the centroid of the triangle.*

First we will express the hypotheses and conclusion as polynomial equations. This system of equations is not unique and not all systems yield the desired results. The equations listed below are the culmination of multiple attempts and some commentary regarding why these equations are favorable is included.

The theorem is illustrated in the following figure.

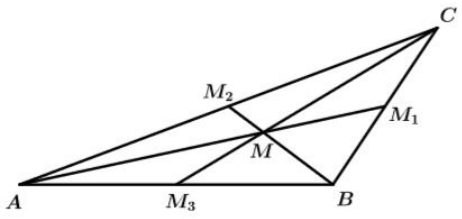

Figure 5.1: ΔABC with Medians

For convenience, we place A at the origin and align the line $\overline{AB}$ along the horizontal coordinate axis so $A = (0, 0)$ and $B = (u_1, 0)$. Let $C = (u_2, u_3)$. The coordinates of the midpoints of each side of the triangle are determined by the coordinates of the

endpoints. We have $M_1 = (x_1, x_2)$, $M_2 = (x_3, x_4)$, $M_3 = (x_5, x_6)$. The coordinates of the centroid are also completely determined so we write $M = (x_7, x_8)$. It is tempting to express the midpoints in terms of u_i as one might in a typical coordinate proof. This would not produce a complete system of polynomials needed to generate the ideal. One practical guideline in constructing the system of polynomial equations is to write a polynomial equation for each dependent coordinate. Now we can obtain polynomial equations from the hypotheses: Using the midpoint formula,

$$M_1 \text{ is the midpoint of } \overline{BC}\text{: } x_1 = \tfrac{u_1+u_2}{2} \text{ and } x_2 = \tfrac{u_3}{2}$$

produces

$$h_1 = 2x_1 - u_1 - u_2 = 0$$
$$h_2 = 2x_2 - u_3 = 0.$$

Similarly,

$$M_2 \text{ is the midpoint of } \overline{AC}\text{: } x_3 = \tfrac{u_2}{2} \text{ and } x_4 = \tfrac{u_3}{2} \text{ and}$$
$$M_3 \text{ is the midpoint of } \overline{AB}\text{: } x_5 = \tfrac{u_1}{2} \text{ and } x_6 = 0$$

produces

$$h_3 = 2x_3 - u_2 = 0$$
$$h_4 = 2x_4 - u_3 = 0$$
$$h_5 = 2x_5 - u_1 = 0$$
$$h_6 = x_6 = 0.$$

We now describe the position of M as being the point where two of the medians intersect. Our conclusion will be that the third median also contains M. Using Proposition 5.1, we can write equations to show M is on medians $\overline{AM_1}$ and $\overline{BM_2}$ as follows:

$$A, M, M_1 \text{ collinear: } \tfrac{x_8}{x_7} = \tfrac{x_2}{x_1}$$
$$B, M, M_2 \text{ collinear: } \tfrac{x_8}{x_7-u_1} = \tfrac{x_4}{x_3-u_1}.$$

Clearing the denominators we obtain two more hypothesis polynomials

$$h_7 = x_1x_8 - x_2x_7 = 0$$
$$h_8 = x_4(x_7 - u_1) - x_8(x_3 - u_1) = 0.$$

It is typical that when a hypothesis is properly translated to polynomial equations, the number of dependent variables and the number of equations is the same. We now translate our conclusion to a polynomial equation:

$$C, M, M_3 \text{ collinear: } \tfrac{x_8-u_3}{x_7-u_2} = \tfrac{x_6-u_3}{x_5-u_2}$$

produces

$$g = (x_5 - u_2)(x_8 - u_3) - (x_6 - u_3)(x_7 - u_2) = 0.$$

In this example, there is only one conclusion. If the conclusion(s) require more than one polynomial, we would make sure each conclusion polynomial g_i follows from the set of hypotheses. Our next step is to show that the conclusion $g = 0$ holds when the hypotheses $h_i = 0$ hold. The polynomial equations in the eleven variables that represent the hypotheses $h_i(u_1, u_2, u_3, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$ are equations that define a variety $V = \mathbf{V}(h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8) \subseteq \mathbb{R}^{11}$. We want to show that g vanishes whenever $h_1, h_2, \ldots, h_8$ vanish. Let $I = \langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8\rangle$. According the the Groebner Basis technique, we can use the radical membership test to determine if $g \in \sqrt{\langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8\rangle}$. The conclusion will follow from the hypotheses if $1 \in \tilde{I} = \langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, 1 - yg\rangle$. Unfortunately, computing a Groebner basis using *Sage* did not render a basis of $\{1\}$. To understand why our technique was not successful, we consider a definition.

Definition 5.3. [CLO15] Let $V = \mathbf{V}(h_1, \ldots, h_n)$. The conclusion g *follows strictly* from the hypotheses $h_1, \ldots, h_n$ if $g \in \mathbf{I}(\mathrm{V}) \subseteq \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$.

Many geometric theorems have degenerate cases that Definition 5.3 does not take into account. For instance, in Theorem 5.2, the centroid example, we cannot allow vertex C to be collinear with A and B. Another drawback of this definition is that because we are working over $\mathbb{R}$, we do not have an effective method for determining $\mathbf{I}(V)$. We will proceed with a useful way to check to see if a conclusion follows strictly from a set of hypotheses before discussing a criterion that is not as strong.

Proposition 5.4. [CLO15] *If* $g \in \sqrt{\langle h_1, \ldots, h_n\rangle}$, then g follows strictly from $h_1, \ldots, h_n$.

Proof. We are given $g \in \sqrt{\langle h_1, \ldots, h_n\rangle}$. This means $g^s \in \langle h_1, \ldots, h_n\rangle$ for some s. Thus g^s is some linear combination $\sum h_i A_i$, where polynomials A_i are in the ring $\mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$. This means g^s and, consequently, g vanish whenever $h_1, \ldots, h_n$ vanish. □

When a conclusion does not follow strictly from a set of hypotheses, possibly due to degenerate cases, we will need to decompose the variety into a finite union of irreducible varieties, as described in Chapter 4, to determine where the degenerate cases conflict with the coordinates that were designed to be arbitrary. That is, we will express the variety $V = V_1 \cup V_2 \cup \cdots \cup V_k$. This task can be simplified by recomputing the Groebner basis at each stage but it still has the potential to be rather lengthy. Furthermore, throughout the process, one must examine each polynomial to determine if its appearance in a variety conflicts with the construction of the hypotheses and the assumption that we do not have a degenerate case. We need to update our strategy so that our method determines the validity of a theorem taking into account degenerate cases that may need to be excluded.

When a polynomial equation involving one of the arbitrary coordinates u_i alone is a member of an irreducible component of the variety, this means that the function $h_i = u_i = 0$. In other words, one of the arbitrary coordinates is determined to be zero. In this case, we will exclude those components from the union since our intent was for those coordinates to be independent. Often this situation reveals a degenerate case. To help remedy this concern, we introduce another definition.

Definition 5.5. [CLO15] Let W be an irreducible variety in the affine space $\mathbb{R}^{n+m}$ with coordinates $u_1, \ldots, u_m, x_1, \ldots, x_n$. We say that the functions $u_1, \ldots, u_m$ are *algebraically independent on* W if no nonzero polynomial in the u_i alone vanishes identically on W.

Another way to state the definition is $u_1, \ldots, u_m$ are algebraically independent on W if $\mathbf{I}(W) \cap \mathbb{R}[u_1, \ldots, u_m] = \{0\}$. This allows us to strategically regroup the irreducible components of the variety so that the degenerate cases are easily identified. We express the variety as follows:

$$V = W_1 \cup \cdots \cup W_p \cup U_1 \cup \cdots \cup U_q,$$

where $u_1, \ldots, u_m$ are algebraically independent on the components W_i and are not algebraically independent on the components of U_j. Thus, U_j represent degenerate cases of the hypotheses of the theorem. So, to guarantee the coordinates u_i are indeed arbitrary in the geometric configuration being studied, we will only consider the subvariety

$$V' = W_1 \cup \cdots \cup W_p \subseteq V.$$

Since we do not want to consider how a conclusion g behaves in the degenerate cases, we adjust our definition of what it means for a conclusion to follow a set of hypotheses so that it is not as strict.

Definition 5.6. [CLO15] The conclusion g *follows generically* from the hypotheses $h_1, \ldots, h_n$ if $g \in \mathbf{I}(V') \subseteq \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, where $V' \subseteq \mathbb{R}^{m+n}$ is the union of the components of the variety $V = \mathbf{V}(h_1, \ldots, h_n)$ on which the u_i are algebraically independent.

It seems that we have simplified our task to develop a criterion that determines whether g vanishes V'. However, we will still need to decompose the original variety V which was the task we hoped to avoid. Moreover, if we successfully decomposed V into a union of irreducible varieties and identified the desired subvariety V', we would still face the challenge of computing $\mathbf{I}(V)$.

The next proposition suggests that we can determine if a conclusion follows generically from a set of hypotheses without knowing the nature of the decomposition the variety.

Proposition 5.7. [CLO15] *A conclusion g follows generically from $h_1, \ldots, h_n$ whenever there is some nonzero polynomial $c(u_1, \ldots, u_m) \in \mathbb{R}[u_1, \ldots, u_m]$ such that*

$$c \cdot g \in \sqrt{H},$$

where H is the ideal generated by the hypotheses h_i in $\mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$.

Proof. Let V_j be one of the irreducible components of V'. We are taking as given that $c \cdot g \in \sqrt{H}$. This means that $c \cdot g$ vanishes on V and thus, $c \cdot g$ vanishes on V_j. It follows that $c \cdot g$ is in the ideal $\mathbf{I}(V_j)$. Since V_j is irreducible, the ideal $\mathbf{I}(V_j)$ is a prime ideal so that $c \cdot g \in \mathbf{I}(V_j)$ implies either $c \in \mathbf{I}(V_j)$ or $g \in \mathbf{I}(V_j)$. No nonzero polynomial in u_i alone vanishes in V_j so we know $c \notin \mathbf{I}(V_j)$. We conclude that $g \in \mathbf{I}(V_j)$, satisfying the definition of what it means for g to follow generically from $h_1, \ldots, h_n$. □

Now we have reduced our task to determining if there is a nonzero polynomial c with $c \cdot g \in \sqrt{H}$. By the definition of the radical, we have $c \cdot g \in \sqrt{H}$ if and only if

$$(c \cdot g)^s = \sum_{j=1}^{n} A_j h_j$$

for some $A_j \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ and $s \geq 1$. Since c is nonzero, we can divide both sides of the equation by c^s. This yields

$$g^s = \sum_{j=1}^{n} \frac{A_j}{c^s} h_j,$$

which demonstrates that g is in the ideal $\tilde{H}$ generated by $h_1, \ldots, h_n$ over the ring $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$. In this ring, denominators depend only on the u_i. Making u_i invertible by augmenting our field of coefficients to $\mathbb{R}(u_1, \ldots, u_m)$ in effect removes the degenerate cases so that the conclusion follows generically from the hypotheses. On the other hand, if $g \in \sqrt{\tilde{H}}$, then

$$g^s = \sum_{j=1}^{n} B_j h_j,$$

where the coefficients of the B_j are in our augmented field $\mathbb{R}(u_1, \ldots, u_m)$. If we clear the denominators by multiplying both sides by c^s where c is a least common denominator for all the terms in all the B_j, we obtain

$$(c \cdot g)^s = \sum_{j=1}^{n} B'_j h_j,$$

where $B'_j \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ and c depends only on the u_i. Consequently, $c \cdot g \in \sqrt{H}$. We now have multiple ways to determine the validity of the conclusion of a theorem. The following corollary to Proposition 5.7 lists them.

Corollary 5.8. [CLO15] *The following are equivalent:*

(i) *There is a nonzero polynomial* $c \in \mathbb{R}[u_1, \ldots, u_m]$ *such that* $c \cdot g \in \sqrt{H}$.

(ii) $g \in \sqrt{\tilde{H}}$ *where* $\tilde{H}$ *is the ideal generated by the* $h_j \in \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$.

(iii) $\{1\}$ *is the reduced Groebner basis of the ideal*

$$\langle h_1, \ldots, h_n, 1 - yg \rangle \subseteq \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n, y].$$

We return now to Theorem 5.2, our example that states the three medians of a triangle are concurrent. We will apply part (iii) of Corollary 5.8 to show that $g = (x_5 - u_2)(x_8 - u_3) - (x_6 - u_3)(x_7 - u_2) = 0$ follows generically from

$$\begin{aligned} h_1 &= 2x_1 - u_1 - u_2 = 0 \\ h_2 &= 2x_2 - u_3 = 0 \\ h_3 &= 2x_3 - u_2 = 0 \\ h_4 &= 2x_4 - u_3 = 0 \\ h_5 &= 2x_5 - u_1 = 0 \end{aligned}$$

$$h_6 = x_6 = 0$$
$$h_7 = x_1x_8 - x_2x_7 = 0$$
$$h_8 = x_4(x_7 - u_1) - x_8(x_3 - u_1) = 0.$$

We use lex order and work in the ring $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, y]$. Using the computer program *Sage* to compute the Groebner basis for the ideal $\langle h_1, \ldots h_8, 1-yg\rangle$ renders the desired result $\{1\}$. Therefore, $g \in \langle h_1, \ldots, h_8\rangle$. This validates the conclusion that the polynomial g represented, the point M defined as the intersection of medians $\overline{AM_1}$ and $\overline{BM_2}$, is also on the median $\overline{CM_3}$.

Once we refined our strategy to compensate for the degenerate cases, the technology did all the tedious division work for us. Not all theorems are suitable for the proving using the techniques described above. We typically will need to be able to introduce a coordinate system. There will be some number of arbitrary coordinates, or independent variables in our construction and a collection of dependent variables. Listed below is a summary of the steps involved in the Groebner Basis Algorithm for proving suitable geometric theorems:

- Sketch the geometric object(s) involved in the theorem. Label all vertices, intersections, and other relevant points. Distinguish arbitrary coordinates using independent variables u_i from dependent variables x_i.
- Determine the polynomial equations that represent the hypotheses h_i and conclusions g_i. Expect one hypothesis equation for each dependent variable.
- With the assistance of a computer, determine if each conclusion follows strictly from the set of hypotheses by computing the reduced Groebner basis of the ideal $\langle h_1, \ldots, h_n, 1 - yg\rangle \subset \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n, y]$. If the reduced Groebner basis is $\{1\}$ then it follows from the Radical Membership Test that $g \in \sqrt{\langle h_1, \ldots, h_n\rangle}$.
- If the reduced Groebner basis rendered is something other than $\{1\}$, make the independent variables part of the field of coefficients and compute the reduced Groebner basis on the ideal $\langle h_1, \ldots, h_n, 1 - yg\rangle \subset \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n, y]$.

5.3 Example 2: The Orthocenter of a Triangle

We have described how to express a geometric theorem as a system of polynomial equations so that a computer may be utilized to validate the theorem. In this example,

and the next one, the only part of the proof that requires human reasoning is deriving the system of polynomial equations.

In secondary geometry courses, the orthocenter of a triangle is defined to be the point at which the three altitudes of a triangle intersect. Consideration is given to the seemingly contradictory notion that the center of a triangle might actually be outside of the triangle or, in the case of a right triangle, be one of the vertices, but the idea that such a point of concurrency exists is taken as given. Here we will prove that all three altitudes of a triangle are concurrent.

Theorem 5.9. *Let ΔABC be a triangle in the plane. Then the lines containing the altitudes of the triangle meet at a single point, called the orthocenter of the triangle.*

The altitude from vertex A is the line segment from A meeting the line containing the opposite side $\overline{BC}$ at a right angle. As shown in the figure below, we will call this meeting point D and notice that side $\overline{BC}$ was extended so the intersection point can be identified. The altitude from vertex B is the line segment from B meeting the line containing the opposite side $\overline{AC}$ at a right angle. In the figure below, this intersection point is labeled E. The altitude from vertex C is the line segment from C meeting the opposite side $\overline{AB}$ at a right angle. As shown below, side $\overline{AB}$ is extended and the intersection point is labeled F.

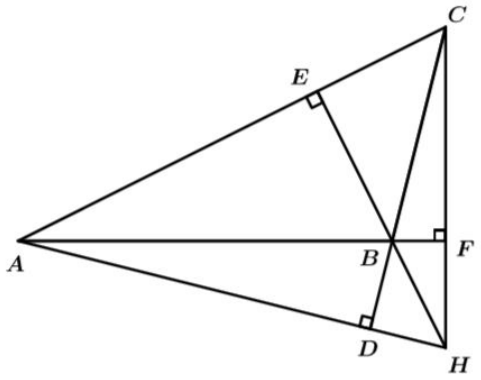

Figure 5.2: ΔABC with Altitudes

We will again place A at the origin and align $\overline{AB}$ along the horizontal coordinate axis so $A = (0, 0)$ and $B = (u_1, 0)$. Let $C = (u_2, u_3)$. The coordinates of the foot of the altitude from each vertex to the line containing the opposite side of each side of the triangle are completely determined by the vertices. We have $D = (x_1, x_2)$, $E = (x_3, x_4)$,

$F = (x_5, x_6)$. The coordinates of the orthocenter are also completely determined so we write $H = (x_7, x_8)$. Now using Proposition 5.1, we can obtain polynomial equations from the hypotheses:

$$B, D, C \text{ collinear: } \tfrac{x_2}{x_1 - u_1} = \tfrac{u_3}{u_2 - u_1}$$

produces

$$h_1 = x_2(u_2 - u_1) - u_3(x_1 - u_1) = 0.$$

Expressing the line segments as vectors, we have

$$\overline{AD} \perp \overline{BC}\text{: } AD \cdot BC = (x_1, x_2) \cdot (u_2 - u_1, u_3) = 0$$

which produces

$$h_2 = x_2 u_3 + x_1(u_2 - u_1) = 0.$$

Likewise,

$$\begin{aligned} A, E, C \text{ collinear} &: h_3 = x_4 u_2 - x_3 u_3 = 0 \\ \overline{BE} \perp \overline{AC} &: h_4 = x_4 u_3 + u_2(x_3 - u_1) = 0 \\ A, B, F \text{ collinear} &: h_5 = x_6 = 0 \\ \overline{AB} \perp \overline{CF} &: h_6 = u_2 - x_5 = 0 \end{aligned}$$

Now we identify H as the point where two of the altitudes, $\overline{AD}$ and $\overline{BE}$ intersect giving two more hypothesis polynomials:

$$\begin{aligned} A, D, H \text{ collinear} &: h_7 = x_2 x_7 - x_1 x_8 = 0 \\ B, E, H \text{ collinear} &: h_8 = x_4(x_7 - u_1) - x_8(x_3 - u_1) = 0 \end{aligned}$$

The conclusion, H is also on the altitude $\overline{CF}$ is translated

$$C, F, H \text{ collinear: } g = (x_6 - u_3)(x_7 - u_2) - (x_5 - u_2)(x_8 - u_3) = 0$$

The reduced Groebner basis for the ideal

$$\langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, 1 - yg \rangle \subset \mathbb{R}(u_1, u_2, u_3)[x_1, \ldots, x_8, y]$$

rendered by *Sage* using lex ordering is $\{1\}$ as desired so we conclude g vanishes on $V(h_1, h_2, h_2, h_4, h_5, h_6, h_7, h_8)$ which validates the conclusion that the point H is on altitude $\overline{CF}$.

5.4 Example 3: Euler's Line

We showed in Example 1 and Example 2 that the medians of a triangle are concurrent at a point we call the centroid of the triangle and the altitudes of a triangle all meet at a point we call the orthocenter of the triangle. There is another "center" of a triangle. We know that three noncollinear points always lie on a circle. These noncollinear points form a non-degenerate triangle. The center of the circle that circumscribes the triangle is called the circumcenter of the triangle. It is a famous theorem of Leonard Euler (1707-1783), a prolific contributor to many branches of mathematics, that the centroid, orthocenter and circumcenter of a triangle are collinear. The line containing the three "centers" of a triangle is called the *Euler line* of the triangle. We state the theorem below and demonstrate how encoding the hypotheses and conclusion as polynomial equations allows us to prove this geometric theorem using the Groebner Basis Algorithm.

Theorem 5.10. *Let ΔABC be a triangle in the plane. Then the circumcenter, centroid and orthocenter of the triangle are collinear.*

We begin with a sketch that uses the same points as in Examples 1 and 2.

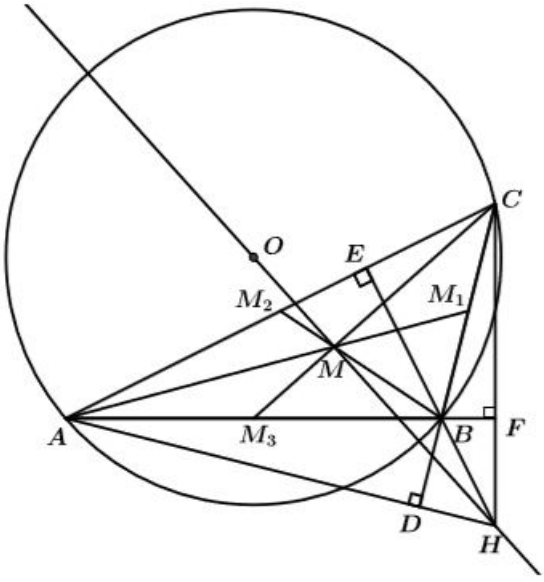

Figure 5.3: ΔABC with Euler's Line

As in the previous examples, we place A at the origin and align $\overline{AB}$ along the horizontal axis. So we have $A = (0, 0),\ B = (u_1, 0),\ C = (u_2, u_3)$. Notice that the

coordinates of $A,\ B,$ and C completely determine the coordinates of the other points. The coordinates of the midpoints are as in Example 1, $M_1 = (x_1, x_2)$, $M_2 = (x_3, x_4)$, $M_3 = (x_5, x_6)$. The coordinates of the centroid are $M = (x_7, x_8)$. Now in Example 2, we re-used coordinates $x_1, x_2, \ldots, x_8$ so we will need to reassign variables the the points $D,\ E,\ F,$ and H. Let $D = (x_9, x_{10})$, $E = (x_{11}, x_{12})$, $F = (x_{13}, x_{14})$. The coordinates of the orthocenter are $H = (x_{15}, x_{16})$. The only new point in our figure is the center O of the circle that circumscribes ΔABC. Its coordinates are also dependent on the locations of the vertices so we assign it coordinates $O = (x_{17}, x_{18})$. We already have the 16 hypothesis polynomial equations from Examples 1 and 2. We will use the distance formula to show $OA = OB$ and $OA = OC$ making O is the circumcenter of ΔABC as follows:

$$OA^2 = OB^2 : x_{17}^2 + x_{18}^2 = (x_{17} - u_1)^2 + x_{18}^2$$
$$OA^2 = OC^2 : x_{17}^2 + x_{18}^2 = (x_{17} - u_2)^2 + (x_{18} - u_3)^2.$$

The polynomial equations produced are

$$h_{17} = u_1^2 - 2x_{17}u_1 = 0$$
$$h_{18} = u_2^2 + u_3^2 - 2x_{17}u_2 - 2x_{18}u_3 = 0.$$

The conclusion that $M,\ H,$ and O are collinear is converted to a polynomial equation by showing the slopes between pairs of points are equal as follows:

$$M, H, O \text{ collinear: } \tfrac{x_{18}-x_{16}}{x_{17}-x_{15}} = \tfrac{x_{18}-x_8}{x_{17}-x_7}.$$

The polynomial equation for the conclusion is

$$g = (x_{18} - x_{16})(x_{17} - x_7) - (x_{18} - x_8)(x_{17} - x_{15}) = 0.$$

A complete list of the polynomial equations for the hypotheses is

$$
\begin{aligned}
h_1 &= 2x_1 - u_1 - u_2 = 0 \\
h_2 &= 2x_2 - u_3 = 0 \\
h_3 &= 2x_3 - u_2 = 0 \\
h_4 &= 2x_4 - u_3 = 0 \\
h_5 &= 2x_5 - u_1 = 0 \\
h_6 &= x_6 = 0 \\
h_7 &= x_1x_8 - x_2x_7 = 0 \\
h_8 &= x_4(x_7 - u_1) - x_8(x_3 - u_1) = 0 \\
h_9 &= x_{10}(u_2 - u_1) - u_3(x_9 - u_1) = 0 \\
h_{10} &= x_{10}u_3 + x_9(u_2 - u_1) = 0 \\
h_{11} &= x_{12}u_2 - x_{11}u_3 = 0 \\
h_{12} &= x_{12}u_3 + u_2(x_{11} - u_1) = 0 \\
h_{13} &= x_{14} = 0 \\
h_{14} &= u_2 - x_{13} = 0 \\
h_{15} &= x_{10}x_{15} - x_9x_{16} = 0 \\
h_{16} &= x_{12}(x_{15} - u_1) - x_{16}(x_{11} - u_1) = 0 \\
h_{17} &= u_1^2 - 2x_{17}u_1 = 0 \\
h_{18} &= u_2^2 + u_3^2 - 2x_{17}u_2 - 2x_{18}u_3 = 0.
\end{aligned}
$$

Using a computer to determine if g follows strictly from $h_1, \ldots h_{18}$, we compute a reduced Groebner basis for the ideal $\langle h_1, \ldots, h_{18}, 1 - yg \rangle \subseteq \mathbb{R}[u_1, u_2, u_3, x_1, \ldots, x_{18}, y]$. The computer does not render a Groebner basis $\{1\}$ so we check to see if g follows generically by treating the independent variables as elements of the field of coefficients. We compute the reduced Groebner basis for $\langle h_1, \ldots, h_{18}, 1 - yg \rangle \subseteq \mathbb{R}(u_1, u_2, u_3,)[x_1, \ldots, x_{18}, y]$. This time the computer renders the reduced Groebner basis $\{1\}$ which tells us that g vanishes on $V(h_1, \ldots, h_{18})$. This confirms our conclusion that the centroid, orthocenter and circumcenter of a triangle are collinear. In these examples, we had a specific conclusion we wished to validate. To demonstrate the Groebner Basis Algorithm, we chose examples appropriate for the Cartesian plane but this algorithm is not restricted to proving theorems in Euclidean space.

Chapter 6

Conclusion

There are several strategies that can be used to prove geometric theorems. Among them are proofs learned in secondary geometry that employ postulates, definitions and theorems arranged in paragraphs, two columns or flow charts to reason from the given hypothesis to the desired conclusion, proofs by geometric construction using a compass and straight edge and coordinate proofs. In this thesis, we explored the correspondence between algebra and geometry and demonstrated how the Groebner Basis Algorithm, an algebraic approach, can be used to prove geometric theorems. In particular, we explored the correspondence between varieties and ideals, specifically, radical ideals.

An important part of our study concerned the mappings from ideals to varieties and varieties to ideals. A crucial result was finding the one-to one correspondence between varieties and radical ideals. Once we expressed our hypotheses and conclusions as polynomials, this bijection allowed us to translate a variety into an ideal and make use of technology to determine if the conclusion polynomial vanished on the variety comprised of the hypothesis polynomials by determining if the conclusion polynomial was a member of the corresponding radical ideal. Translating the variety to a radical ideal is what made the use of technology possible.

Applying the Groebner Basis Algorithm made for efficient interpretation of the output from our computer application. The proof of Hilbert's Nullstellensatz revealed a convenient way to revise the ideal so that the reduced Groebner basis for the revised ideal gave us a clear decision regarding the verification of the theorem. If the output was $\{1\}$ then we concluded that the theorem was verified. We encountered a problem with the possibility of degenerate cases and resolved the issue by modifying the field of coefficients

to include the independent variables.

Throughout this thesis, we laid the foundation for the use of technology to not only assist with our proofs of geometric theorems but to carry out all of the computational tasks. The use of technology is a key component of algebraic geometry. The ability to correlate geometric concepts such as affine varieties to the algebra of polynomial rings allows us to take advantage of the algorithmic nature of computer applications to prove geometric theorems algebraically. For a mathematician, discovering the links between various branches of mathematics enhances understanding and motivates future exploration.

Bibliography

[Bur11] David M Burton. *Elementary Number Theory*. McGraw-Hill Companies, 2011.

[CLO15] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer International Publishing, 2015.

[Fro97] Ralf Froberg. *An Introduction to Grobner Bases*. John Wiley & Sons, 1997.

[Gal17] Joseph A. Gallian. *Contemporary Abstract Algebra*. Cengage Learning, 2017.

[Zea13] Samira Zeada. Polynomial division and groebner bases. *The Teaching of Mathematics*, XVI:22–28, 2013.