2009

Geometric theorem proving using the Groebner basis algorithm

Karla Friné Rivas

Geometric Theorem Proving Using The Groebner Basis Algorithm

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

Karla Friné Rivas

December 2009

Geometric Theorem Proving Using The Groebner Basis Algorithm

A Thesis

Presented to the

Faculty of

California State University,

San Bernardino

by

Karla Friné Rivas

December 2009

Approved by:

[redacted]

Dr. Laura Wallace, Committee Chair

12-3-09

Date

[redacted]

Dr. John Sarli, Committee Member

[redacted]

Dr. Jim Okon, Committee Member

[redacted]

Dr. Peter Williams, Chair,
Department of Mathematics

[redacted]

Dr. Joseph Chavez
Graduate Coordinator,
Department of Mathematics

Abstract

One important aspect of algebraic geometry is the study of affine varieties. Affine varieties are curves, surfaces, and higher dimensional objects that are defined by polynomial equations. It is this connection between geometry and algebra that can be used to prove geometric theorems algebraically. In particular, an algebraic method known as the Groebner Basis Algorithm can confirm or reject a conjecture in Euclidean geometry. The purpose of this project is to study ideals in polynomial rings and affine varieties in order to establish a connection between these two different concepts. Doing so will lead to an in depth examination of Groebner bases. Once this has been defined, steps will be outlined that will enable the application of the Groebner Basis Algorithm to geometric problems.

Acknowledgements

My journey at CSUSB over the last six years has been long but very rewarding. I would like to take a moment to thank everyone that made my time at this school memorable. First of all, I want to thank my committee members Dr. Okon and Dr. Sarli for their input and help with my thesis. In addition, Dr. Dunn and Dr. Stanton for helping me with all of my LaTex questions. A very special thank you to Stefan Johnson for helping me typeset the multivariable long division problems found in my thesis. Thanks again for your hard work and for a job well done because I would not have been able to figure this out before the deadline! However, completing this project would not have been possible without my advisor Dr. Laura Wallace. Dr. Wallace, I just wanted to thank you for all of your help throughout this entire time. You were patient and willing to explain things more than once so that I could understand what I was doing. Thank you for always encouraging me every step of the way because there were several times when I didn't think that I would ever finish. I am so glad that I had this opportunity to work with you because I really had a lot of fun. I also wanted to acknowledge Dr. Joseph Chavez for his guidance during my time in the Master's program. It didn't matter whether it was a question about math or TA stuff, but with your help I was able to resolve whatever issue I was facing. But just so you know, I still don't like block walking.

The second group of people that I would like to thank are my family and friends. I would not have returned to school to pursue another degree without all of your support and encouragement either. No matter if I was tired, irritated, or frustrated I could always count on you to cheer me up and tell me everything would be ok. Anyone who is a math student knows that it's impossible to successfully complete the Master's program alone. During my time at CSUSB, I had the honor and privilege of working and meeting people who are very dear to me. So I just wanted to say that I feel extremely fortunate that our paths crossed. Thank you everyone!

Table of Contents

List of Figures

Chapter 1

Introduction

Algebraic geometry makes a connection to topics discussed in abstract algebra to problems studied in geometry. Concepts of algebraic geometry have been applied to fields in computer science such as robotics and artificial intelligence. The main focus of study in algebraic geometry is affine varieties. Affine varieties are the solutions to systems of polynomial equations. These affine varieties represent curves, surfaces, and higher dimensional objects that are defined by polynomial equations. The polynomial equations that are studied are not restricted to one variable. The terms of these polynomials can be composed of a finite number of variables. One of the important applications of algebraic geometry that this project will focus on is to prove geometric theorems algebraically. The hypothesis and conclusion of the theorem will be translated into a system of equations and it will be shown that if the system for the hypothesis has a solution, then the system for the conclusion has a solution. The algebraic method that will be discussed in this project is the Groebner Bases algorithm.

In order to successfully complete this project we need to be able to properly define and understand Groebner bases. A Groebner basis is a generating set of an ideal of polynomials with some nice and useful properties. These properties will be discussed in the project in more detail. Ideals and affine varieties are critical to the understanding of the Groebner Bases Algorithm that we wish to use to prove theorems in Euclidean geometry. Affine varieties are determined by ideals generated by polynomials, so in order to understand affine varieties we will need concepts from algebra. We have to study ideals in polynomial rings over a field k. Ideals are important because they will provide us with a way to compute an affine variety. For instance, if we can change the basis of the ideal of polynomials we are working with to a Groebner basis, then it will be easier to determine the variety. This is important because we would like to be able to solve systems of polynomial equations of any degree with any number of variables.

The goal of this project will be to present several theorems proven in Euclidean geometry using the Groebner Bases Algorithm. The first example we will examine is the proof showing that the diagonals of a parallelogram intersect at a point that bisects both of the diagonals. In addition, we will look at a proof for the Circle Theorem of Apollonius. The Circle Theorem of Apollonius is named after the Greek mathematician Apollonius. Apollonius wrote extensively on conic sections and he is credited with naming some of the conic sections. He also came up with an alternative way to define a circle. Usually, we think of a circle as the set of all points that are the same distance from a given point. Apollonius proved that a circle is the set of all points in the plane that have a specified ratio of distances to two fixed points. [Sma98] These two examples will illustrate how theorems proven in Euclidean geometry can be represented and verified by solving a system of polynomial equations.

Chapter 2

Geometry and Algebra

2.1 Polynomials and Affine Space

To use the Groebner Basis Algorithm, we will need to solve systems of polynomial equations of any degree with any number of variables. In order to do so, we need to define the polynomials we will be working with. The polynomials we will encounter throughout the course of this project contain more than one or two variables. These polynomials will have coefficients from a field k and n variables. We begin by defining a monomial because each term in any polynomial is a monomial.

Definition 2.1. A *monomial* in $x_1, \ldots, x_n$ is a product of the form

$$x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

where all of the exponents $\alpha_1, \ldots, \alpha_n$ are nonnegative integers. The **total degree** of this monomial is the sum $\alpha_1 + \cdots + \alpha_n$.

Now that we have discussed monomials, we can now define a polynomial in $k[x_1, x_2, ..., x_n]$. We can simplify the notation for a monomial in the following manner. We can rewrite $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ as x^α where $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$, an n-tuple of positive integers. The second question we need to ask ourselves is how will we determine the degree of a monomial? The degree of the monomial will be denoted $|\alpha|$ where $|\alpha| = \alpha_1 + \alpha_2 + ... + \alpha_n$.

Definition 2.2. A **polynomial** f in $x_1, \ldots, x_n$ with coefficients in k is a finite linear combination (with coefficients in k) of monomials. We will write 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 $\alpha = (\alpha_1, \ldots, \alpha_n)$. The set of all polynomials in $x_1, \ldots, x_n$ with coefficients in k is denoted $k[x_1, \ldots, x_n]$.

The definition that follows will introduce the basic terminology that will be used when working with polynomials with multivariable terms.

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

(i) We call a_α the **coefficient** of the monomial x^α.

(ii) If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a **term** of f.

(iii) The **total degree** of f, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient a_α is nonzero.

We will apply the definitions and terminology previously discussed to an example. Consider, the polynomial $f = 7x^4yz^2 - \frac{4}{3}x^2y^5 + xyz^3 - 10x^4 + 2xyz$. Notice that $f \in \mathbb{R}[x, y, z]$. The polynomial f has 5 terms. The coefficients of f are 7, $-\frac{4}{3}$, 1, -10, and 2. The total degree of f is 7. Unlike polynomials of only one variable, this example illustrates a problem present in multivariable polynomials. There are two terms $7x^4yz^2$ and $-\frac{4}{3}x^2y^5$ in f that have a total degree of 7. Ordering the terms of these polynomials will be examined further in Chapter 3.

It is extremely important to note that $k[x_1, x_2, ..., x_n]$ is not a polynomial field, but a polynomial ring. By taking two arbitrary polynomials f and g from $k[x_1, x_2, ..., x_n]$, we have $f + g \in k[x_1, x_2, ..., x_n]$ and $f \cdot g \in k[x_1, x_2, ..., x_n]$. Furthermore, it can be shown that the associative, commutative, distributive, multiplicative and additive identities, and additive inverse conditions for a field are satisfied. However, it is not always possible to find a multiplicative inverse when working in $k[x_1, x_2, ..., x_n]$. For example, let $f = x + y$ and $g = \frac{1}{x+y}$. Although $f \cdot g = 1$, only the polynomial f is an element of $\mathbb{R}[x, y]$. Unfortunately, g is not an element of $\mathbb{R}[x, y]$ because it is not a polynomial (as stated in Definition 2.2). Consequently, $k[x_1, x_2, ..., x_n]$ is a commutative ring and not a field.

Next, we will look at affine space.

Definition 2.4. Given a field k and a positive integer n, we define the n-dimensional **affine space** over k to be the set

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

When $k = \mathbb{R}$, we get one of the most common examples of an affine space, $\mathbb{R}^n$. This space is used throughout many courses in the study of mathematics.

2.2 Affine Varieties

Affine varieties are the most important focus of algebraic geometry. We will start this section by defining an affine variety.

Definition 2.5. Let k be a field, and let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set

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

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

An affine variety $\mathbf{V}(f_1, \ldots, f_s)$ is a collection of n-tuples that are solutions to a system of equations. More specifically, we are interested in solving the system $f_1(x_1, x_2, \ldots, x_n) = 0$, $f_2(x_1, x_2, \ldots, x_n) = 0$, $\ldots$, $f_n(x_1, x_2, \ldots, x_n) = 0$.

Next, we will look at some examples of affine varieties in $\mathbb{R}^2$ to become more comfortable with this topic. By working in $\mathbb{R}^2$ it will be easier to understand affine varieties because we will be able to visualize them when they are drawn in the Cartesian plane.

Example 1. Take for instance, $\mathbf{V}(2x + y - 1, 3x - y + 2)$. We would like to find the set of points $(x, y) \in \mathbb{R}^2$ such that $2x + y - 1 = 0$ and $3x - y + 2 = 0$. The equations $f_1(x, y) = 2x + y - 1$ and $f_2(x, y) = 3x - y + 2$ are linear. Therefore, there are three possible outcomes when we graph this system in the plane $\mathbb{R}^2$. If the two lines are the same, then there are an infinite amount of solutions to the system. On the other hand, if the two lines are parallel, the lines will never intersect so there would be no solutions. Thus, the variety would be empty. Lastly, the two lines drawn in the plane can intersect at a single point. This is exactly what happens with the given variety above. One can quickly solve this system by using substitution or the elimination method to determine that $\mathbf{V}(2x + y - 1, 3x - y + 2) = \{(-\frac{1}{5}, \frac{7}{5})\}$.

Example 2. Another example of an affine variety from $\mathbb{R}^2$ is $\mathbf{V}(x^2 + y^2 - 1)$. To find the set of $(x, y) \in \mathbb{R}^2$, we need to solve the equation $x^2 + y^2 - 1 = 0$. Adding 1 to both sides of the equation results in the equation $x^2 + y^2 = 1$. This is the equation of a circle centered at the origin with a radius of one. Therefore, the variety $\mathbf{V}(x^2 + y^2 - 1)$ has an infinite number of solutions including $(1, 0)$, $(\frac{\sqrt{3}}{2}, \frac{1}{2})$, $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$, $(\frac{1}{2}, \frac{\sqrt{3}}{2})$, and $(0, 1)$.

Example 3. The last example of an affine variety that we will study from $\mathbb{R}^2$ is the four leaf rose. The four leaf rose is defined by the polar equation $r = \sin(2\theta)$. We would like to show that this polar equation gives an affine variety.

The affine variety is $\mathbf{V}((x^2 + y^2)^3 - 4x^2y^2) = \{(a, b) \in \mathbb{R}^2 \mid (a^2 + b^2)^3 - 4a^2b^2 = 0\}$.

The rose is $\mathrm{R} = \{(x, y) \mid x = r\cos\theta,\ y = r\sin\theta,\ r^2 = x^2 + y^2,\ r = \sin(2\theta)\}$.

We will first show that the rose is contained in the affine variety $\mathbf{V}((x^2 + y^2)^3 - 4x^2y^2)$.

Show $\mathrm{R} \subseteq \mathbf{V}$.

Let $(x, y) \in \mathrm{R}$. We would like to show that $(x, y) \in \mathbf{V}$. We have

$$\begin{aligned}
(x^2 + y^2)^3 - 4x^2y^2 &= (r^2)^3 - 4(r\cos\theta)^2(r\sin\theta)^2 \\
&= r^6 - 4(r\cos\theta)^2(r\sin\theta)^2 \\
&= r^6 - 4(r^2\cos^2\theta)(r^2\sin^2\theta) \\
&= r^6 - 4r^4\cos^2\theta\sin^2\theta \\
&= r^6 - r^4(2\cos\theta\sin\theta)(2\cos\theta\sin\theta) \\
&= r^6 - r^4(\sin(2\theta))(\sin(2\theta)) \\
&= r^6 - r^4(r)(r) \\
&= r^6 - r^6 \\
&= 0.
\end{aligned}$$

Thus, $(x, y) \in \mathbf{V}$ and $r = \sin(2\theta)$ is contained in $\mathbf{V}((x^2 + y^2)^3 - 4x^2y^2)$. The second part of this problem is to show that $\mathbf{V}$ is contained in the four leaf rose $r = \sin(2\theta)$.

Show $\mathbf{V} \subseteq \mathrm{R}$.

Let $(a, b) \in \mathbf{V}$. We want to show that $(a, b) \in \mathrm{R}$. Since $(a, b) \in \mathbf{V}$, we know $(a^2 + b^2)^3 -$

$4a^2b^2 = 0$. So we get

$$\begin{aligned}
(a^2+b^2)^3 - 4a^2b^2 &= 0 \\
(a^2+b^2)^3 &= 4a^2b^2 \\
(r^2)^3 &= 4(r\cos\theta)^2(r\sin\theta)^2 \\
r^6 &= 4r^4\cos^2\theta\sin^2\theta \\
r^2 &= 4\cos^2\theta\sin^2\theta \\
r &= \pm\, 2\cos\theta\sin\theta \\
r &= \pm\, \sin(2\theta).
\end{aligned}$$

Therefore, since R $\subseteq$ **V** and **V** $\subseteq$ R, we have shown that the four leaf rose is the affine variety $\mathbf{V}((x^2+y^2)^3 - 4x^2y^2)$.

After examining several examples of affine varieties in $\mathbb{R}^2$, we want to look at some properties of affine varieties.

Lemma 2.6. *If V, $W \subset k^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.*

Proof. For both of these proofs we will let V $= \mathbf{V}(f_1, f_2, \ldots, f_s)$ and W $= \mathbf{V}(g_1, g_2, \ldots, g_t)$. We want to show that $V \cup W = \mathbf{V}(f_ig_j \mid 1 \leq i \leq s,\ 1 \leq j \leq t)$.

($\Longrightarrow$) Show $V \cup W \subset \mathbf{V}(f_ig_j)$.

Let $(a_1, a_2, \ldots, a_n) \in V \cup W$. This implies that $(a_1, a_2, \ldots, a_n) \in V$ or $(a_1, a_2, \ldots, a_n) \in W$. If $(a_1, a_2, \ldots, a_n) \in V$, then $f_1(a_1, a_2, \ldots, a_n) = 0$, $f_2(a_1, a_2, \ldots, a_n) = 0$, $\ldots$, $f_s(a_1, a_2, \ldots, a_n) = 0$. So $f_i(a_1, a_2, \ldots, a_n)g_1(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s$, $f_i(a_1, a_2, \ldots, a_n)g_2(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s$, $\ldots$, and finally $f_i(a_1, a_2, \ldots, a_n)g_t(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s$. So, V $\subset \mathbf{V}(f_ig_j)$.

Similarly, if $(a_1, a_2, \ldots, a_n) \in W$, then $g_1(a_1, a_2, \ldots, a_n) = 0$, $g_2(a_1, a_2, \ldots, a_n) = 0$, $\ldots$, $g_t(a_1, a_2, \ldots, a_n) = 0$. So $f_1(a_1, a_2, \ldots, a_n)g_j(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$, $f_2(a_1, a_2, \ldots, a_n)g_j(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$, $\ldots$, and finally $f_s(a_1, a_2, \ldots, a_n)g_j(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$. Now, W $\subset \mathbf{V}(f_ig_j)$. Consequently, it has been shown that V $\cup$ W $\subset \mathbf{V}(f_ig_j)$.

($\Longleftarrow$) Show $\mathbf{V}(f_ig_j) \subset V \cup W$.

Let $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_ig_j)$. We want to show $(a_1, a_2, \ldots, a_n) \in V \cup W$. Since $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_ig_j)$ this implies that $f_i(a_1, a_2, \ldots, a_n)g_j(a_1, a_2, \ldots, a_n) = 0$ for all i and j. In order for the product of these two polynomials to equal zero then either

$f_i(a_1, a_2, \ldots, a_n) = 0$ or $g_j(a_1, a_2, \ldots, a_n) = 0$. Listing some of the products of $\mathbf{V}(f_i g_j)$ we get,

$$\begin{aligned} f_1(a_1, a_2, \ldots, a_n) \cdot g_j(a_1, a_2, \ldots, a_n) &= 0,\ 1 \leq j \leq t \\ f_2(a_1, a_2, \ldots, a_n) \cdot g_j(a_1, a_2, \ldots, a_n) &= 0,\ 1 \leq j \leq t \\ &\vdots \\ f_s(a_1, a_2, \ldots, a_n) \cdot g_j(a_1, a_2, \ldots, a_n) &= 0,\ 1 \leq j \leq t. \end{aligned}$$

By examining each of the products listed we notice that there are two things that can happen. One, if $f_i(a_1, a_2, \ldots, a_n) = 0$ for all i, then $g_j(a_1, a_2, \ldots, a_n)$ does not have to equal zero. Since $(a_1, a_2, \ldots, a_n)$ makes all the polynomials $f_1, f_2, \ldots, f_s$ in V equal 0, then we have shown that $(a_1, a_2, \ldots, a_n) \in$ V. On the other hand, if $f_{i_0}(a_1, a_2, \ldots, a_n) \neq 0$ for some i_0, then $g_j(a_1, a_2, \ldots, a_n)$ must equal zero for all j. So, $(a_1, a_2, \ldots, a_n)$ makes all of the polynomials g_j in W zero, and then $(a_1, a_2, \ldots, a_n) \in$ W. Due to the fact that $(a_1, a_2, \ldots, a_n) \in$ V or $(a_1, a_2, \ldots, a_n) \in$ W, we can conclude that $(a_1, a_2, \ldots, a_n) \in$ V∪W. Therefore, we have proved that $V \cup W = \mathbf{V}(f_i g_j \mid 1 \leq i \leq s,\ 1 \leq j \leq t)$.

We will next show that $V \cap W = \mathbf{V}(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$.
($\Longrightarrow$) Show that $V \cap W \subset \mathbf{V}(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$.
Let $(a_1, a_2, \ldots, a_n) \in V \cap W$. This implies that $(a_1, a_2, \ldots, a_n) \in V$ and $(a_1, a_2, \ldots, a_n) \in W$. So, $(a_1, a_2, \ldots, a_n) \in V$ means that $f_i(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq i \leq s$. Likewise, $(a_1, a_2, \ldots, a_n) \in W$ means that $g_j(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$. Thus, the n-tuple $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$ since it makes all of the equations in $\mathbf{V}$ equal to zero.
($\Longleftarrow$) Show that $\mathbf{V}(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t) \subset V \cap W$.
Assume $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$. This now implies that $f_i(a_1, a_2 \ldots, a_n) = 0$ for all $1 \leq i \leq s$ and $g_t(a_1, a_2, \ldots, a_n) = 0$ for all $1 \leq j \leq t$. So $(a_1, a_2, \ldots, a_n)$ makes all the polynomials f_i in V zero and g_j in W zero as well. Now, we can say that $(a_1, a_2, \ldots, a_n) \in$ V and $(a_1, a_2, \ldots, a_n) \in$ W. Thus, $(a_1, a_2, \ldots, a_n) \in$ V∩W. We have verified that $V \cap W = \mathbf{V}(f_1, f_2, \ldots, f_s, g_1, g_2, \ldots, g_t)$. □

In the previous lemma if V and W are affine varieties, then the union of V and W and the intersection of V and W are both affine varieties. Furthermore, it will be shown that Lemma 2.6 can also be extended to the unions and intersections of a finite number of affine varieties.

Proof. Let V_1, V_2, $\dots$, V_n be affine varieties. We want to show that $V_1 \cap V_2 \cap \dots \cap V_n$ is also an affine variety. We will show a proof by induction on n, the number of affine varieties. This is clearly true for $n = 1$ since V_1 is a variety. In the case when $n = 2$, we have $V_1 \cap V_2$ and it was proven in Lemma 2.6 that the intersection of two affine varieties is an affine variety. Next, we will assume that $V_1 \cap V_2 \cap \dots \cap V_k$ is an affine variety for k varieties. Now we must show that $V_1 \cap V_2 \cap \dots \cap V_k \cap V_{k+1}$ is an affine variety. From our previous assumption, the intersection of $V_1 \cap V_2 \cap \dots \cap V_k$ is an affine variety. We will call this variety V. Now,

$$\begin{aligned} V_1 \cap V_2 \cap \dots \cap V_k \cap V_{k+1} &= (V_1 \cap V_2 \cap \dots \cap V_k) \cap V_{k+1} \\ &= V \cap V_{k+1}. \end{aligned}$$

Notice that V and V_{k+1} are affine varieties. Applying Lemma 2.6, the intersection of two affine varieties is an affine variety. Therefore, $V_1 \cap V_2 \cap \dots \cap V_n$ is an affine variety.

Secondly, in order to show that the finite union of affine varieties is an affine variety, we will again do a proof by induction on n, the number of affine varieties. The above statement is true when $n = 1$ because V_1 is an affine variety. When $n = 2$, $V_1 \cup V_2$ is an affine variety because we have the union of two affine varieties. We will next assume that $V_1 \cup V_2 \cup \dots \cup V_k$ is an affine variety for k varieties. Now we must show that $V_1 \cup V_2 \cup \dots \cup V_k \cup V_{k+1}$ is an affine variety. By our previous assumption, the union of $V_1 \cup V_2 \cup \dots \cup V_k$ is an affine variety. We will call this variety W. So,

$$\begin{aligned} V_1 \cup V_2 \cup \dots \cup V_k \cup V_{k+1} &= (V_1 \cup V_2 \cup \dots \cup V_k) \cup V_{k+1} \\ &= W \cup V_{k+1}. \end{aligned}$$

Note that W and V_{k+1} are two affine varieties. Once again using Lemma 2.6, the union of two affine varieties is an affine variety. Consequently, $V_1 \cup V_2 \cup \dots \cup V_n$ is an affine variety. □

2.3 Ideals

One of the most important concepts from algebra that will used throughout this project are ideals. Ideals will be the key to help us find the elements from k^n that are in an affine variety.

Definition 2.7. A subset $I \subset k[x_1, \ldots, x_n]$ is an **ideal** if it satisfies:

(i) $0 \in I$.

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

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

Definition 2.8. Let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. Then we set

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

We will call $\langle f_1, \ldots, f_s \rangle$ the **ideal generated by** $f_1, \ldots, f_s$. In particular,

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

is called the **principal ideal** generated by f.

The above definition states that if a polynomial can be written as a linear combination of $f_1, f_2, \ldots, f_s$, then that polynomial is an element of $\langle f_1, f_2, \ldots, f_s \rangle$.

Lemma 2.9. *If $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, then $\langle f_1, \ldots, f_s \rangle$ is an ideal of $k[x_1, \ldots, x_n]$.*

Proof. Let $\langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, h_2, \ldots, h_s \in k[x_1, x_2, \ldots, x_n] \right\}$. We want to show that $\langle f_1, f_2, \ldots, f_s \rangle$ is an ideal. The first condition we need to show is that $0 \in \langle f_1, f_2, \ldots, f_s \rangle$. We can write $0 = 0 \cdot f_1 + 0 \cdot f_2 + \ldots + 0 \cdot f_s$, where each $0 \in k[x_1, x_2, \ldots, x_n]$. Since 0 can be written as a linear combination of the polynomials $f_1, f_2, \ldots, f_s$ belonging to $k[x_1, x_2, \ldots, x_n]$, then $0 \in \langle f_1, f_2, \ldots, f_s \rangle$.

Next, we must show that adding two arbitrary polynomials a and b from $\langle f_1, f_2, \ldots, f_s \rangle$ results in a polynomial that also belongs to $\langle f_1, f_2, \ldots, f_s \rangle$. Since $a \in \langle f_1, f_2, \ldots, f_s \rangle$ then $a = m_1 f_1 + m_2 f_2 + \ldots + m_s f_s$ where $m_1, m_2, \ldots, m_s \in k[x_1, x_2, \ldots, x_n]$. Similarly, $b \in \langle f_1, f_2, \ldots, f_s \rangle$ implies that $b = n_1 f_1 + n_2 f_2 + \ldots + n_s f_s$ where $n_1, n_2, \ldots, n_s \in k[x_1, x_2, \ldots, x_n]$. Hence,

$$\begin{aligned} a + b &= (m_1 f_1 + m_2 f_2 + \ldots + m_s f_s) + (n_1 f_1 + n_2 f_2 + \ldots + n_s f_s) \\ &= m_1 f_1 + n_1 f_1 + m_2 f_2 + n_2 f_2 + \ldots + m_s f_s + n_s f_s \\ &= (m_1 + n_1) f_1 + (m_2 + n_2) f_2 + \ldots + (m_s + n_s) f_s. \end{aligned}$$

The sum $a + b$ is a linear combination of the polynomials $f_1, f_2, \ldots, f_s$ and $m_1 + n_1$, $m_2 + n_2$, $\ldots$, $m_s + n_s \in k[x_1, x_2, \ldots, x_n]$. Thus, $a + b \in \langle f_1, f_2, \ldots, f_s \rangle$.

Finally, if $h \in k[x_1, x_2, \ldots, x_n]$ and $a \in \langle f_1, f_2, \ldots, f_s \rangle$, then we must show that $ha \in \langle f_1, f_2, \ldots, f_s \rangle$. Since $a \in \langle f_1, f_2, \ldots, f_s \rangle$, then $a = m_1 f_1 + m_2 f_2 + \ldots + m_s f_s$. Now,

$$\begin{aligned} ha &= h(m_1 f_1 + m_2 f_2 + \ldots + m_s f_s) \\ &= hm_1 f_1 + hm_2 f_2 + \ldots + hm_s f_s \\ &= (hm_1) f_1 + (hm_2) f_2 + \ldots + (hm_s) f_s. \end{aligned}$$

The product ha is a linear combination of the polynomials $f_1, f_2, \ldots, f_s$ and hm_1, hm_2, $\ldots$, hm_s are in $k[x_1, x_2, \ldots, x_n]$. So, $ha \in \langle f_1, f_2, \ldots, f_s \rangle$. By satisfying these three conditions, it has been shown that $\langle f_1, f_2, \ldots, f_s \rangle$ is an ideal. □

Proposition 2.10. *If $f_1, \ldots, f_s$ and $g_1, \ldots, g_t$ are bases of the same ideal in $k[x_1, \ldots, x_n]$, so that $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.*

Proof. Assume that $\langle f_1, f_2, \ldots, f_s \rangle = \langle g_1, g_2, \ldots, g_t \rangle$. We want to show that $\mathrm{V}(f_1, f_2, \ldots, f_s) = \mathrm{V}(g_1, g_2, \ldots, g_t)$. Let $(a_1, a_2, \ldots, a_n) \in \mathrm{V}(f_1, f_2, \ldots, f_s)$. Since $(a_1, a_2, \ldots, a_n) \in \mathrm{V}(f_1, f_2, \ldots, f_s)$ we know that $f_1(a_1, a_2, \ldots, a_n) = 0$, $f_2(a_1, a_2, \ldots, a_n) = 0$, $\ldots$, $f_s(a_1, a_2, \ldots, a_n) = 0$. In order for $(a_1, a_2, \ldots, a_n)$ to be an element of $\mathrm{V}(g_1, g_2, \ldots, g_t)$, we have to show that $g_1(a_1, a_2, \ldots, a_n) = 0$, $g_2(a_1, a_2, \ldots, a_n) = 0$, $\ldots$, $g_t(a_1, a_2, \ldots, a_n) = 0$. The polynomials $g_1, g_2, \ldots, g_t$ are elements in the ideal $\langle g_1, g_2, \ldots, g_t \rangle$. Consequently, $g_1, g_2, \ldots, g_t$ are also elements in the ideal $\langle f_1, f_2, \ldots, f_s \rangle$ because from our initial assumption $\langle f_1, f_2, \ldots, f_s \rangle = \langle g_1, g_2, \ldots, g_t \rangle$. Now that $g_1, g_2, \ldots, g_t \in \langle f_1, f_2, \ldots, f_s \rangle$ we can write each g_i for $1 \leq i \leq t$ as a linear combination of $f_1, f_2, \ldots, f_s$. Hence, $g_i = b_{i_1} f_1 + b_{i_2} f_2 + \ldots + b_{i_s} f_s$, where $b_{i_1}, b_{i_2}, \ldots, b_{i_s} \in k[x_1, x_2, \ldots, x_n]$. If we evaluate each g_i by $(a_1, a_2, \ldots, a_n)$ we get,

$$\begin{aligned} g_i(a_1, a_2, \ldots, a_n) &= b_{i_1}(a_1, a_2, \ldots, a_n) f_1(a_1, a_2, \ldots, a_n) + \ldots \\ &\quad + b_{i_s}(a_1, a_2, \ldots, a_n) f_s(a_1, a_2, \ldots, a_n) \\ &= b_{i_1}(a_1, a_2, \ldots, a_n) \cdot 0 + \ldots + b_{i_s}(a_1, a_2, \ldots, a_n) \cdot 0 \\ &= 0. \end{aligned}$$

So, $g_i(a_1, a_2, \ldots a_n) = 0$ for all $1 \leq i \leq t$. As a result, $(a_1, a_2, \ldots, a_n) \in \mathrm{V}(g_1, g_2, \ldots, g_t)$. It has been shown that if $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, then $\mathrm{V}(f_1, \ldots, f_s) = \mathrm{V}(g_1, \ldots, g_t)$. □

With the help of the division algorithm, it will be possible to determine the form of every ideal in the polynomial ring $k[x]$.

Corollary 2.11. *If k is a field, then every ideal of $k[x]$ can be written in the form $\langle f\rangle$ for some $f \in k[x]$. Furthermore, f is unique up to multiplication by a nonzero constant in k. In other words, $k[x]$ is a principal ideal domain (PID).*

Proof. Let the ideal $I \subset k[x]$. If $I = \{0\}$, then $I = \langle 0\rangle$. Since the only element in I is zero, zero is clearly an element of $\langle 0\rangle$. Looking at the converse, $\langle 0\rangle = g \cdot 0$ where $g \in k[x]$. Regardless of the polynomial chosen from the ring, the product will always be zero. Thus, $I = \langle 0\rangle$. Suppose I is a nonzero ideal. Assume f is a nonzero polynomial of minimal degree such that $f \in I$. Let $g \in \langle f\rangle$. We want the polynomial $g \in I$. If $g \in \langle f\rangle$, then $g = h \cdot f$ where $h \in k[x]$. Now the product $hf \in I$ because $h \in k[x]$, $f \in I$ and I is an ideal. So $g \in I$ and $\langle f\rangle \subset I$. We continue by proving that $I \subset \langle f\rangle$. Let $g \in I$. We would like to show that $g \in \langle f\rangle$. By the Division Algorithm $g = qf + r$ where $r = 0$ or $\deg(r) < \deg(f)$. If the remainder $r \neq 0$, then $\deg(r) < \deg(f)$. Now, $r = g - qf$. In this equation, $g \in I$ and the product $qf \in I$ because $q \in k[x]$, $f \in I$, and I is an ideal. Consequently, this would make $r \in I$. This is a contradiction because r is an element of I that has lesser degree than f. By our assumption, f is supposed to be a polynomial of smallest degree in I. Therefore, $r = 0$ which makes $g = qf \in \langle f\rangle$ and $I \subset \langle f\rangle$. So, for some $f \in k[x]$ an ideal I in $k[x]$ has the form $I = \langle f\rangle$.

We next turn our attention to prove that f is unique. Assume $\langle f\rangle = \langle g\rangle$. Because $f \in \langle g\rangle$ then $f = hg$ for $h \in k[x]$. Examining the degrees of the polynomials f, g, and h we see that $\deg(f) = \deg(h) + \deg(g)$. So $\deg(f) \geq \deg(g)$. Similarly, $g \in \langle f\rangle$ means that $g = hf$ for $h \in k[x]$. In this case, $\deg(g) = \deg(h) + \deg(f)$ so that $\deg(f) \leq \deg(g)$. Hence, $\deg(f) = \deg(g)$. If the $\deg(f) = \deg(g)$, then the equation $\deg(f) = \deg(h) + \deg(g)$ implies that the $\deg(h)$ is zero. Then h must be a nonzero constant. □

An ideal generated by one element from the ring is called a *principal ideal.* As a result of Corollary 2.11, the polynomial ring $k[x]$ is a *principal ideal domain* or PID for short.

Definition 2.12. Let $V \subset k^n$ be an affine variety. Then we set

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

The ideal of a variety consists of the polynomials in the ring $k[x_1, \ldots, x_n]$ such that all of the n-tuples belonging to V makes the polynomial zero.

Lemma 2.13. *If $V \subset k^n$ is an affine variety, then $\mathbf{I}(V) \subset k[x_1, \ldots, x_n]$ is an ideal. We will call $\mathbf{I}(V)$ the* **ideal of** *V.*

Proof. In order to prove that $\mathbf{I}(V)$ is an ideal, we will begin by showing that $0 \in \mathbf{I}(V)$. Let $(a_1, a_2, \ldots, a_n)$ be an arbitrary element from the variety V. If we take a polynomial $f \in \mathbf{I}(V)$, then $f(a_1, a_2, \ldots, a_n) = 0$ by Definition 2.12. So it has been shown that $0 \in \mathbf{I}(V)$. Now let the polynomials f and $g \in \mathbf{I}(V)$. Then $f(a_1, a_2, \ldots, a_n) = 0$ and $g(a_1, a_2, \ldots, a_n) \in \mathbf{I}(V)$. Thus,

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

Since $f + g = 0$ and $0 \in \mathbf{I}(V)$, then $f + g \in \mathbf{I}(V)$. Finally, let $f \in \mathbf{I}(V)$ and $h \in k[x_1, x_2, \ldots, x_n]$. The product

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

So, $hf \in \mathbf{I}(V)$. Therefore, we have shown that $\mathbf{I}(V)$ is an ideal. □

Lemma 2.14. *If $f_1, \ldots, f_s \in k[x_1, \ldots x_n]$, then $\langle f_1, \ldots, f_s\rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, although equality need not occur.*

Proof. Assume $f \in \langle f_1, f_2, \ldots, f_s\rangle$. If it can be shown that $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$, then $\langle f_1, f_2, \ldots, f_s\rangle \subset \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$. Since the polynomial f is an element of $\langle f_1, f_2, \ldots, f_s\rangle$ this implies that $f = h_1f_1 + h_2f_2 + \ldots + h_sf_s$ where $h_1, h_2, \ldots, h_s \in k[x_1, x_2, \ldots, x_n]$. In addition, let $(a_1, a_2, \ldots, a_n)$ be an arbitrary element of $V(f_1, f_2, \ldots, f_s)$. If we take this n-tuple and plug it into f we get

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

Due to the fact that $(a_1, a_2, \ldots a_n) \in \mathbf{V}(f_1, f_2, \ldots, f_s)$, then $f_i(a_1, a_2, \ldots, a_n) = 0$ for $1 \leq i \leq s$. As a result, the polynomial $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$. Thus, $\langle f_1, \ldots, f_s \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$.

Although it has been proven that $\langle f_1, \ldots, f_s \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, we need to examine the reasons why $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ need not be contained in $\langle f_1, \ldots, f_s \rangle$. In order to do so, we will take a look at an example from $\mathbb{R}^2$. Let $f_1 = x + 3y + 1$ and $f_2 = 2x - y - 5$ be polynomials from the ring $\mathbb{R}[x, y]$. To find the ordered pairs that belong to the $\mathbf{V}(f_1, f_2) = \mathbf{V}(x + 3y + 1, 2x - y - 5)$ we must solve the system of linear equations $x + 3y + 1 = 0$ and $2x - y - 5 = 0$. The intersection of these two lines in the plane is only at the point (2, -1). Hence, $\mathbf{V}(x + 3y + 1, 2x - y - 5) = \{(2, -1)\}$. On the other hand, if $f \in \mathbf{I}(\mathbf{V}(x + 3y + 1,\ 2x - y - 5))$ it is not guaranteed to be an element of $\langle x+3y+1,\ 2x-y-5 \rangle$. The ideal $\mathbf{I}(\mathbf{V}(x+3y+1,\ 2x-y-5)) = \{f \in \mathbb{R}[x, y] \mid f(2, -1) = 0\}$. For example, let f be the parabola $f(x, y) = x^2 - 4x - y + 3$. The parabola is an element of $\mathbf{I}(\mathbf{V}(x + 3y + 1,\ 2x - y - 5))$ because $f(2, -1) = 2^2 - 4(2) - (-1) + 3 = 0$. In order for this parabola to be an element of $\langle x + 3y + 1,\ 2x - y - 5 \rangle$, it must be a linear combination of the polynomials f_1 and f_2. Unfortunately, f cannot be written as a linear combination of $x + 3y + 1$ and $2x - y - 5$ so $f \notin \langle x + 3y + 1,\ 2x - y - 5 \rangle$. This implies that $\mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ is not contained in $\langle f_1, \ldots, f_s \rangle$. □

Chapter 3

Groebner Bases

The ultimate goal of this project is to be able to prove geometric theorems algebraically. The algebraic method that will be illustrated later is the called the Groebner Bases Algorithm. However, in order to use this algorithm we must first define and understand Groebner bases. There are two major questions that will be encountered by working with polynomials and the ideals generated by these polynomials. First, by taking an arbitrary polynomial f from $k[x_1, x_2, \ldots, x_n]$, can we determine if f is an element of the ideal $I = \langle f_1, f_2, \ldots, f_n \rangle$? In addition, is it possible to find the solutions to a system of polynomial equations, $f_1(x_1, x_2, \ldots, x_n) = 0$, $f_2(x_1, x_2, \ldots, x_n) = 0$, $\ldots$, $f_s(x_1, x_2, \ldots, x_n) = 0$? Using a concept introduced in Section 2.2, we can rephrase the previous question in the following manner. Can we find the points that belong to the affine variety $\mathbf{V}(f_1, f_2, \ldots, f_s)$? Groebner bases are the tool that will allow us to answer these questions in order to prove theorems from Euclidean geometry algebraically.

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

Since we will be working with polynomials with coefficients from a field k and whose terms are composed of n variables, we had to spend time defining these polynomials. Chapter 2 began by discussing monomials because they are the building blocks of any polynomial. We were able to define a coefficient, term, monomial and total degree for a multivariable polynomial f in $k[x_1, x_2, \ldots, x_n]$. Unfortunately, one of the topics that we did not discuss at that time was how to order the terms of a multivariable polynomial. To understand why it is important to discuss ordering a multivariable polynomial we will reexamine an example from Section 2.1. The polynomial $f(x,y,z) = 7x^4yz^2 - \frac{4}{3}x^2y^5 + xyz^3 - 10x^4 + 2xyz$ illustrates a problem that is not present in single variable polynomials. There are two terms $7x^4yz^2$ and $-\frac{4}{3}x^2y^5$ in f that have the same total degree 7. We have discovered that it is possible for a multivariable polynomial to have more than one term with the same total degree. Consequently, if we wanted to order the polynomial f in either descending or ascending order we will have a major problem. In order to use the Groebner Basis Algorithm effectively, we need to use the division algorithm for multivariable polynomials. Before using the division algorithm it is common practice to order the terms of the polynomial in descending order.

In order to arrange the terms in a polynomial from $k[x_1, x_2, \ldots, x_n]$, we will now define three possible orderings. Although there are many lexicographic orderings, in this project we will be using lex order, graded lex order, or graded reverse lex order.

Definition 3.1 (Lex Order). Let $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Definition 3.2 (Graded Lex Order). Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

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

Definition 3.3 (Graded Reverse Lex Order). Let $\alpha, \beta \in \mathbb{Z}^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ if

$$|\alpha| = \textstyle\sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i, \quad \textit{or } |\alpha| = |\beta|$$

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

To illustrate the difference between the three lex orderings defined above, we will rearrange the terms of the polynomial $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ in lex order, grlex order, and grevlex order. The variables x, y, and z will have the order $x > y > z$ unless stated otherwise. We shall begin by writing the exponents of x, y, and z in each term of the polynomial above as ordered n-tuples. The terms $2x^2y^8$, $-3x^5yz^4$, xyz^3, and $-xy^4$ will be represented by the ordered triplets $\alpha = (2,8,0)$, $\beta = (5,1,4)$, $\gamma = (1,1,3)$ and $\delta = (1,4,0)$. To place the terms in lex order we need to compare the difference between the triplets α, β, γ, and δ. The terms will be placed in descending lex order when the leftmost nonzero entry in the difference is positive. The largest term in the polynomial for this example is $-3x^5yz^4$ followed by $2x^2y^8$. To order the final 2 terms we need to compare the difference of $\gamma - \delta = (0, -3, 3)$ and $\delta - \gamma = (0, 3, -3)$. Since the leftmost nonzero entry is positive for $\delta - \gamma$, then $-xy^4$ is bigger than xyz^3. So the polynomial $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ written in lex order is $f(x, y, z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$.

Next, we will write the given polynomial in graded lex order. When using grlex order, however, the monomials are initially ordered by the total degree of each term. In case the total degrees of the terms are the same, lex order is then used to arrange the terms. Determining the total degree for each term $|\alpha| = |(2, 8, 0)| = 10$, $|\beta| = |(5, 1, 4)| = 10$, $|\gamma| = |(1, 1, 3)| = 5$, and $|\delta| = |(1, 4, 0)| = 5$. It is clear that α and β are bigger terms than γ and δ. But now we use lex order to find out if $\alpha > \beta$ or $\beta > \alpha$ and if $\gamma > \delta$ or $\delta > \gamma$. Comparing the difference between the ordered triples we can conclude that $\beta > \alpha > \delta > \gamma$. Thus, the polynomial $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ written in graded lex order is $f(x, y, z) = -3x^5yz^4 + 2x^2y^8 - xy^4 + xyz^3$.

Finally, we will conclude this example by writing the polynomial in graded reverse lex order. Similar to graded lex order the monomials will first be ordered by the total degree of each term. If the total degree between the terms happens to be equal we do not use lex order to order the terms. Instead, comparing the differences between the ordered n-tuples the larger term will have the rightmost nonzero entry be negative. As in the graded lex order, α and β are bigger than γ and δ. Comparing the rightmost entries in the differences, we find that $\alpha > \beta > \delta > \gamma$. Therefore, the polynomial $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$ written in graded reverse lex order is $f(x, y, z) = 2x^2y^8 - 3x^5yz^4 - xy^4 + xyz^3$.

Before we continue any further, it is necessary to introduce some additional terminology that will be used with polynomials from $k[x_1, x_2, \ldots, x_n]$.

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

(i) 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 $>$).

(ii) The **leading coefficient** of f is

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

(iii) The **leading monomial** of f is

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

(with coefficient 1).

(iv) The **leading term** of f is

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

To illustrate the use of Definition 3.4, we will give the LC(f), LM(f), LT(f), and multideg(f) for the lex order, the grlex order, and grevlex order of the polynomial $f(x,y,z) = 2x^2y^8 - 3x^5yz^4 + xyz^3 - xy^4$. Since it turns out that the lex order and the graded lex order of the polynomial f are the same, then

$$\begin{aligned} \mathrm{multideg}(f) &= (5,1,4), \\ \mathrm{LC}(f) &= -3, \\ \mathrm{LM}(f) &= x^5yz^4, \\ \mathrm{LT}(f) &= -3x^5yz^4. \end{aligned}$$

On the other hand, with respect to graded reverse lex order, we see that

$$\begin{aligned} \mathrm{multideg}(f) &= (2,8,0), \\ \mathrm{LC}(f) &= 2, \\ \mathrm{LM}(f) &= x^2y^8, \\ \mathrm{LT}(f) &= 2x^2y^8. \end{aligned}$$

3.2 A Division Algorithm in $k[x_1, x_2, \dots, x_n]$

We will now turn our focus to determine if an arbitrary polynomial f belongs to an ideal I. If we are working in the polynomial ring $k[x]$, finding out if $f \in I$ would be a simple task to accomplish by using the division algorithm since this involves polynomials of a single variable. Unfortunately, when trying to prove Euclidean geometry proofs by using algebra we will be working with polynomials from the ring $k[x_1, x_2, \ldots, x_n]$. In order to determine whether $f \in k[x_1, x_2, \ldots, x_n]$ is an element of the ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$, can we modify the division algorithm used for single variable polynomials? This means that f will be divided by the polynomials f_1, f_2, $\ldots$, f_s from $k[x_1, x_2, \ldots, x_n]$. In other words, $f = a_1 f_1 + a_2 f_2 + \ldots + a_s f_s + r$, where $a_1, a_2, \ldots, a_s$ are the quotients, f_1, f_2, $\ldots$, f_s are the divisors and r is the remainder. All of the polynomials a_i, f_i, and r are elements of $k[x_1, x_2, \ldots, x_n]$. The division algorithm for multivariable polynomials will essentially work in the same manner as for single variable polynomials. Before starting the division, we must first decide the momonial ordering that will be used on the polynomial f. Next, we want to divide the leading term of f by one of the f_i's to find the corresponding quotients a_i's and then subtracting. This process will be illustrated with the following examples.

Example 1. We will be dividing the polynomial $f = x^2y^3 + 9$ by $f_1 = xy + 1$ and $f_2 = y + 1$. We will use lex order with $x > y$. To set up the division, we will write the divisors and the quotients vertically:

$$\begin{array}{rl}
a_1 : & \\
a_2 : & \\
xy + 1 & \sqrt{\,x^2y^3 + 9 \quad} \\
y + 1 &
\end{array}$$

Both of the leading terms $\mathrm{LT}(f_1) = xy$ and $\mathrm{LT}(f_2) = y$ divide the leading term of f evenly. However, since there is more than one divisor we will use the first f_i that divides $\mathrm{LT}(f) = x^2y^3$ evenly. So the divisor f_1 will be used first. Now $xy^2 \cdot f_1 = x^2y^3 - y$ and subtracting this from f is $-xy^2 + 9$.

$$\begin{array}{rl}
a_1 : & \qquad xy^2 \\
a_2 : & \\
xy + 1 & \sqrt{\,x^2y^3 + 9 \qquad} \\
y + 1 & \underline{-(x^2y^3 + xy^2) \qquad} \\
 & \qquad\qquad -xy^2 + 9
\end{array}$$

We continue the same procedure on $-xy^2 + 9$. Again the $\mathrm{LT}(f_1) = xy$ divides the $\mathrm{LT}(-xy^2 + 9) = -xy^2$ evenly. So $-y \cdot f_1 = -xy^2 - y$ and subtracting this from $-xy^2 + 9$ is $y + 9$.

$$\begin{array}{rl}
a_1: & xy^2 - y \\
a_2: & \\
xy+1 & \sqrt{\overline{x^2y^3 + 9}} \\
y+1 & \underline{-(x^2y^3 + xy^2)} \\
 & \qquad -xy^2 + 9 \\
 & \quad \underline{-(-xy^2 - y)} \\
 & \qquad\qquad y + 9
\end{array}$$

Now notice that $\mathrm{LT}(f_1) = xy$ does not divide $\mathrm{LT}(y + 9) = y$ so we must use f_2. Thus, $1 \cdot y + 1 = y + 1$ and subtracting this from $y + 9$ results in 8.

$$\begin{array}{rl}
a_1: & xy^2 - y \\
a_2: & 1 \\
xy+1 & \sqrt{\overline{x^2y^3 + 9}} \\
y+1 & \underline{-(x^2y^3 + xy^2)} \\
 & \qquad -xy^2 + 9 \\
 & \quad \underline{-(-xy^2 - y)} \\
 & \qquad\qquad y + 9 \\
 & \qquad\quad \underline{-(y + 1)} \\
 & \qquad\qquad\quad \underline{8} \\
 & \qquad\qquad\quad 0 \quad \longrightarrow \quad 8
\end{array}$$

The algorithm has terminated at this point because the $\mathrm{LT}(f_1)$ and $\mathrm{LT}(f_2)$ cannot divide 8. Therefore, 8 is the remainder. The division completed above has shown that

$$x^2y^3 + 9 = (xy^2 - y) \cdot (xy + 1) + (1) \cdot (y + 1) + 8.$$

Example 2. In this next example we will come across a situation that does not occur when using the division algorithm for single variable polynomials. The polynomial f will be ordered using lex order where $x > y$. The polynomial $f = x^4y^2 + x^2y^3 + y^2$ will be divided by $f_1 = xy - 1$ and $f_2 = y^2 - 1$. As in Example 1, we notice that both the

$\mathrm{LT}(f_1) = xy$ and $\mathrm{LT}(f_2) = y^2$ divide the $\mathrm{LT}(f) = x^4y^2$. So $x^3y \cdot f_1 = x^4y^2 - x^3y$ and subtracting this from f results in $x^3y + x^2y^3 + y^2$.

$$\begin{array}{rl}
a_1: & x^3y \\
a_2: & \\
xy-1 & \sqrt{x^4y^2+x^2y^3+y^2} \\
y^2-1 & \underline{-(x^4y^2-x^3y)\qquad\qquad} \\
 & \qquad\qquad x^3y+x^2y^3+y^2
\end{array}$$

Next, $x^2 \cdot f_1 = x^3y - x^2$ and subtracting this from $x^3y + x^2y^3 + y^2$ yields,

$$\begin{array}{rl}
a_1: & x^3y+x^2 \\
a_2: & \\
xy-1 & \sqrt{x^4y^2+x^2y^3+y^2} \\
y^2-1 & \underline{-(x^4y^2-x^3y)\qquad\qquad} \\
 & \qquad\qquad x^3y+x^2y^3+y^2 \\
 & \qquad\quad \underline{-(x^3y-x^2)\qquad\qquad\quad} \\
 & \qquad\qquad\qquad\quad x^2y^3+x^2+y^2
\end{array}$$

Continuing with $x^2y^3 + x^2 + y^2$, the $\mathrm{LT}(f_1) = xy$ divides the $\mathrm{LT}(x^2y^3 + x^2 + y^2) = x^2y^3$ evenly. So, $xy^2 \cdot f_1 = x^2y^3 - xy^2$ and the subtracting this from $x^2y^3 + x^2 + y^2$ is

$$\begin{array}{rl}
a_1: & x^3y+x^2+xy^2 \\
a_2: & \\
xy-1 & \sqrt{x^4y^2+x^2y^3+y^2} \\
y^2-1 & \underline{-(x^4y^2-x^3y)\qquad\qquad} \\
 & \qquad\qquad x^3y+x^2y^3+y^2 \\
 & \qquad\quad \underline{-(x^3y-x^2)\qquad\qquad\quad} \\
 & \qquad\qquad\qquad\quad x^2y^3+x^2+y^2 \\
 & \qquad\qquad\quad \underline{-(x^2y^3-xy^2)\qquad\qquad} \\
 & \qquad\qquad\qquad\qquad\quad x^2+xy^2+y^2
\end{array}$$

At this point in the division we come across a problem. Neither $\mathrm{LT}(f_1) = xy$ or the $\mathrm{LT}(f_2) = y^2$ divide the $\mathrm{LT}(x^2 + xy^2 + y^2) = x^2$ evenly. In the case of a single variable polynomial this would signify that the division algorithm has terminated since the leading term of the divisor cannot divide the polynomial left after the subtraction. With multivariable polynomials, however, we can move the x^2 term to the remainder and continue dividing. Hence, $y \cdot f_1 = xy^2 - y$ and subtracting this from $xy^2 + y^2$ we get

$$\begin{array}{lrl}
a_1: & x^3y+x^2+xy^2+y & \\
a_2: & & \\
xy-1 & \sqrt{x^4y^2+x^2y^3+y^2} & \\
y^2-1 & \underline{-(x^4y^2-x^3y)} & \\
 & x^3y+x^2y^3+y^2 & \\
 & \underline{-(x^3y-x^2)} & \\
 & x^2y^3+x^2+y^2 & \\
 & \underline{-(x^2y^3-xy^2)} & \\
 & \underline{x^2+xy^2+y^2} & \\
 & xy^2+y^2 & \longrightarrow \quad x^2 \\
 & \underline{-(xy^2-y)} & \\
 & y^2+y &
\end{array}$$

Since $\mathrm{LT}(f_1)$ cannot divide $y^2 + y$ we must use the divisor f_2. So, $1 \cdot f_2 = y^2 - 1$ and subtracting from $y^2 - y$ results in

$$\begin{array}{lrl}
a_1: & x^3y+x^2+xy^2+y & \\
a_2: & 1 & \\
xy-1 & \sqrt{x^4y^2+x^2y^3+y^2} & \\
y^2-1 & \underline{-(x^4y^2-x^3y)} & \\
 & x^3y+x^2y^3+y^2 & \\
 & \underline{-(x^3y-x^2)} & \\
 & x^2y^3+x^2+y^2 & \\
 & \underline{-(x^2y^3-xy^2)} & \\
 & \underline{x^2+xy^2+y^2} & \\
 & xy^2+y^2 & \longrightarrow \quad x^2 \\
 & \underline{-(xy^2-y)} & \\
 & y^2+y & \\
 & \underline{-(y^2-1)} & \\
 & y+1 &
\end{array}$$

Unfortunately, the $\mathrm{LT}(y+1) = y$ is not divisible by the $\mathrm{LT}(f_1)$ or the $\mathrm{LT}(f_2)$. So the term y is also added to the remainder.

$$
\begin{array}{llll}
a_1: & x^3y + x^2 + xy^2 + y & & \\
a_2: & 1 & & \\
xy - 1 & \overline{\big)\, x^4y^2 + x^2y^3 + y^2} & & \\
y^2 - 1 & \underline{-(x^4y^2 - x^3y)} & & \\
 & \qquad x^3y + x^2y^3 + y^2 & & \\
 & \qquad \underline{-(x^3y - x^2)} & & \\
 & \qquad\qquad x^2y^3 + x^2 + y^2 & & \\
 & \qquad\qquad \underline{-(x^2y^3 - xy^2)} & & \\
 & \qquad\qquad\qquad \underline{x^2 + xy^2 + y^2} & & \\
 & \qquad\qquad\qquad\quad xy^2 + y^2 & \longrightarrow & x^2 \\
 & \qquad\qquad\qquad\quad \underline{-(xy^2 - y)} & & \\
 & \qquad\qquad\qquad\qquad y^2 + y & & \\
 & \qquad\qquad\qquad\qquad \underline{-(y^2 - 1)} & & \\
 & \qquad\qquad\qquad\qquad\quad \underline{y + 1} & & \\
 & \qquad\qquad\qquad\qquad\qquad 1 & \longrightarrow & x^2 + y
\end{array}
$$

The final term left from the division 1 is again not divisible by $\mathrm{LT}(f_1)$ or the $\mathrm{LT}(f_2)$ so it becomes part of the remainder.

$$\begin{array}{rrcl}
a_1: & x^3y + x^2 + xy^2 + y & & \\
a_2: & 1 & & \\
xy-1 & \sqrt{x^4y^2 + x^2y^3 + y^2} & & \\
y^2-1 & \underline{-(x^4y^2 - x^3y)} & & \\
 & x^3y + x^2y^3 + y^2 & & \\
 & \underline{-(x^3y - x^2)} & & \\
 & x^2y^3 + x^2 + y^2 & & \\
 & \underline{-(x^2y^3 - xy^2)} & & \\
 & \underline{x^2 + xy^2 + y^2} & & \\
 & xy^2 + y^2 & \longrightarrow & x^2 \\
 & \underline{-(xy^2 - y)} & & \\
 & y^2 + y & & \\
 & \underline{-(y^2 - 1)} & & \\
 & \underline{y+1} & & \\
 & \underline{1} & \longrightarrow & x^2 + y \\
 & 0 & \longrightarrow & x^2 + y + 1
\end{array}$$

Finally, the division algorithm has terminated, so that

$$x^4y^2 + x^2y^3 + y^2 = (x^3y + x^2 + xy^2 + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + (x^2 + y + 1).$$

Working through Example 2 shows the steps involved when using the division algorithm for polynomials from the ring $k[x_1, x_2, \ldots, x_n]$. We can also note something important regarding the remainder obtained from the division. Each of the terms in the remainder are not divisible by any of the leading terms of the divisors. From the two examples worked out above it appears that there are no problems with the division algorithm when it is used with multivariable polynomials. The next example will illustrate that using the division algorithm with polynomials from $k[x_1, x_2, \ldots, x_n]$ does not ensure that the remainder is unique. This is a property which the remainder has in the single variable case. It is for this reason that we need to study Groebner bases.

Example 3. In the previous example, the polynomial $f = x^4y^2 + x^2y^3 + y^2$ was divided by $f_1 = xy - 1$ and $f_2 = y^2 - 1$. The terms in f were ordered with respect to lex order with $x > y$. The only modification that will be made to the earlier division will be to change the order in which the divisors are listed. How will this affect the division from Example 2? Completing the division algorithm results in

$$\begin{array}{rrcl}
a_1: & x^4+x^2y+1 & & \\
a_2: & x & & \\
y^2-1 & \sqrt{x^4y^2+x^2y^3+y^2} & & \\
xy-1 & \underline{-(x^4y^2-x^4)} & & \\
 & \underline{x^4+x^2y^3+y^2} & & \\
 & x^2y^3+y^2 & \longrightarrow & x^4 \\
 & \underline{-(x^2y^3-x^2y)} & & \\
 & x^2y+y^2 & & \\
 & \underline{-(x^2y-x)} & & \\
 & \underline{x+y^2} & & \\
 & y^2 & \longrightarrow & x^4+x \\
 & \underline{-(y^2-1)} & & \\
 & \underline{1} & & \\
 & 0 & \longrightarrow & x^4+x+1
\end{array}$$

$$x^4y^2+x^2y^3+y^2 = (x^4+x^2y+1)\cdot(y^2-1)+x\cdot(xy-1)+(x^4+x+1)$$

Comparing the results obtained from Example 2 and Example 3 we can make the following observations about using the division algorithm with multivariable polynomials. If the order of the divisors (f_i) are changed, the quotients (a_i) and the remainders will not be the same. Furthermore, we notice that the number of steps required to complete the divison algorithm is not the same. In Example 2, it only took 5 steps to do the division as opposed to 4 steps in Example 3.

From the three examples that have been studied in this section we can formally state the division algorithm for multivariable polynomials.

Theorem 3.5 (Division Algorithm in $k[x_1, x_2, \ldots, x_n]$). *Fix a monomial order $>$ on $\mathbb{Z}^n_{\geq 0}$, and let $F = (f_1, \ldots, f_s)$ be an ordered s-tuple of polynomials in $k[x_1, \ldots, x_n]$. Then every $f \in k[x_1, \ldots, x_n]$ can be written as*

$$f = a_1f_1 + \cdots + a_sf_s + r,$$

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

$$\text{multideg}(f) \geq \text{multideg}(a_i f_i).$$

For a complete proof of the division algorithm in $k[x_1, x_2, \ldots, x_n]$ refer to pages 62 - 63 of [CLO97].

3.3 The Hilbert Basis Theorem and Groebner Bases

In the previous section, we saw that the leading terms of a polynomial are important when using the division algorithm. This is significant because in this section we will be looking at an ideal I and the ideal generated by the leading coefficients of the polynomials contained in I.

Definition 3.6. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal other than $\{0\}$.

(i) We denote by $\mathrm{LT}(I)$ the set of leading terms of elements of I. Thus,

$$\mathrm{LT}(I) = \{cx^\alpha \mid \text{there exists } f \in I \textit{ with } \mathrm{LT}(f) = cx^\alpha\}.$$

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

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 to $\langle \mathrm{LT}(I) \rangle$. In the following example it will be shown that $\langle \mathrm{LT}(I) \rangle$ can contain more elements. It can be bigger than $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s) \rangle$.

Example. Suppose $I = \langle g_1, g_2, g_3 \rangle \subset \mathbb{R}[x, y, z]$ where $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$, and $g_3 = x - yz^4$. Using lex order with $x > y > z$, we want to find a polynomial $g \in I$ but $\mathrm{LT}(g) \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle$. Let

$$\begin{aligned} g &= 1 \cdot (xy^2 - xz + y) - y \cdot (xy - z^2) + z \cdot (x - yz^4), \\ &= xy^2 - xz + y - xy^2 + yz^2 + xz - yz^5, \\ &= -yz^5 + yz^2 + y. \end{aligned}$$

Notice that $g \in I$ because it can be written as a linear combination of g_1, g_2, and g_3. So $\mathrm{LT}(g) = -yz^5 \in \langle \mathrm{LT}(I) \rangle$. Unfortunately, $\mathrm{LT}(g) = -yz^5$ is not divisible by $\mathrm{LT}(g_1) = xy^2$, $\mathrm{LT}(g_2) = xy$, or $\mathrm{LT}(g_3) = x$. So the polynomial $g \notin \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \mathrm{LT}(g_3) \rangle$.

Next, monomial ideals in $k[x_1, x_2, \ldots, x_n]$ will be defined.

Definition 3.7. An ideal $I \subset k[x_1, x_2, \ldots, x_n]$ is a **monomial ideal** if there is a subset $A \subset \mathbb{Z}^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1, x_2, \ldots, x_n]$. In this case, we write $I = \langle x^\alpha \mid \alpha \in A \subset \mathbb{Z}^n_{\geq 0} \rangle$.

One of the most important facts about monomial ideals from $k[x_1, x_2, \ldots, x_n]$ is that they are finitely generated.

Theorem 3.8 (Dickson's Lemma). *A monomial ideal $I = \langle x^\alpha \mid \alpha \in A \rangle \subset k[x_1, x_2, \ldots, x_n]$ can be written down in the form $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, where $\alpha_1, \ldots, \alpha_s \in A$. In particular, I has a finite basis.*

For a complete proof of Dickson's Lemma look at pages 69 - 70 of [CLO97].

Proposition 3.9. *Let $I \subset k[x_1, \ldots, x_n]$ be an ideal.*

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

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

Proof. (i) From Definition 3.6, $\langle \mathrm{LT}(I) \rangle = \langle cx^\alpha \mid f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha \rangle$. If $\mathrm{LT}(f) = cx^\alpha$, then $c \in k \subset k[x_1, x_2, \ldots, x_n]$. This implies that c is a nonzero constant from the field k. Consequently, the ideal $\langle cx^\alpha \mid f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha \rangle = \langle x^\alpha \mid f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha \rangle$. The polynomials generated by both of these ideals are linear combinations of the same monomial x^α. It has been shown that $\langle \mathrm{LT}(I) \rangle = \langle x^\alpha \mid f \in I \text{ with } \mathrm{LT}(f) = cx^\alpha \rangle$ is a monomial ideal as stated in Definition 3.7.

(ii) In part (i) of this proof, we showed that $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal. Combining this fact with Dickson's Lemma then $\langle \mathrm{LT}(I) \rangle$ will be generated by a finite number of monomials from polynomials in I. Hence, for $g_1, g_2, \ldots, g_t \in I$,

$$\begin{aligned}
\langle \mathrm{LT}(I) \rangle &= \langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_t) \rangle, \\
&= \langle x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_t} \rangle, \\
&= \langle c_1 x^{\alpha_1}, c_2 x^{\alpha_2}, \ldots, c_t x^{\alpha_t} \rangle \text{ where } c_1, c_2, \ldots, c_t \in k, \\
&= \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t) \rangle.
\end{aligned}$$

□

The previous example showed that $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s)\rangle$ does not equal $\langle \mathrm{LT}(I)\rangle$ since $\langle \mathrm{LT}(I)\rangle$ can contain more elements. However, it will be shown that there are polynomials belonging to ideal I for which $\langle \mathrm{LT}(f_1), \mathrm{LT}(f_2), \ldots, \mathrm{LT}(f_s)\rangle = \langle \mathrm{LT}(I)\rangle$.

Theorem 3.10. (Hilbert Basis Theorem). *Every ideal $I \subset k[x_1, \ldots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_t\rangle$ for some $g_1, \ldots, g_t \in I$.*

Proof. By part (ii) of Proposition 3.9, there are $g_1, g_2, \ldots, g_t \in I$ such that $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t)\rangle$. We must prove that $I = \langle g_1, g_2, \ldots, g_t\rangle$. We will begin by showing that $\langle g_1, g_2, \ldots, g_t\rangle \subset I$. Since each $g_1, g_2, \ldots, g_t \in I$ the polynomials that are linear combinations of elements in I also belong to I by closure. For the second part of this proof it will be shown that $I \subset \langle g_1, g_2, \ldots, g_t\rangle$. Let f be a polynomial in I, then show that f is an element of $\langle g_1, g_2, \ldots, g_t\rangle$. Due to the fact that $f \in I$, the polynomial can be divided by $g_1, g_2, \ldots, g_t$ using the division algorithm. Hence, $f = a_1g_1 + a_2g_2 + \ldots + a_tg_t + r$ where no term of r is divisible by the $\mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t)$. In order for f to be an element of $\langle g_1, g_2, \ldots, g_t\rangle$, the remainder r must be equal zero. Assume that the remainder is not zero. Solving the above equation for r, we get $r = f - a_1g_1 - a_2g_2 - \ldots - a_tg_t$. The equation for r now shows that $r \in I$ because $f \in I$ and each of the products a_ig_i for $1 \leq i \leq t$ are also in I. Since $r \in I$, this implies that $\mathrm{LT}(r) \in \langle \mathrm{LT}(I)\rangle$. Consequently, $\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t)\rangle$ because $\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1), \mathrm{LT}(g_2), \ldots, \mathrm{LT}(g_t)\rangle$. This means that $\mathrm{LT}(r)$ is divisible by some $\mathrm{LT}(g_i)$. This is clearly a contradiction because in order to be a remainder r cannot be divided by any $\mathrm{LT}(g_1)$, $\mathrm{LT}(g_2)$, $\ldots$, $\mathrm{LT}(g_t)$. So the remainder must be zero. As a result, $f = a_1g_1 + a_2g_2 + \ldots + a_tg_t$ which means that $f \in \langle g_1, g_2, \ldots, g_t\rangle$. So $I \subset \langle g_1, g_2, \ldots, g_t\rangle$. Therefore, $I = \langle g_1, g_2, \ldots, g_t\rangle$. □

We will now define what it means to be a Groebner basis. The properties of Groebner bases will be discussed in more detail in the next section. Furthermore, we will also learn how to find a Groebner basis for an ideal I.

Definition 3.11. Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is said to be a **Groebner basis** (or **standard basis**) if

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

Corollary 3.12. *Fix a monomial order. Then every ideal $I \subset k[x_1, \ldots, x_n]$ other than $\{0\}$ has a Groebner basis. Furthermore, any Groebner basis for an ideal I is a basis of I.*

As a result of the Hilbert Basis Theorem it is possible to find the variety of an ideal $I \subset k[x_1, x_2, \ldots, x_n]$.

Definition 3.13. Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. We will denote by $\mathbf{V}(I)$ the set

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

Proposition 3.14. *$\mathbf{V}(I)$ 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. By the Hilbert Basis Theorem, $I = \langle f_1, f_2, \ldots, f_s \rangle$. We shall start by showing that $\mathbf{V}(I) \subset \mathbf{V}(f_1, f_2, \ldots, f_s)$. As defined by Definition 3.13, $\mathbf{V}(I)$ is the set of all n-tuples that make all of the polynomials in I equal to zero. Let $(a_1, a_2, \ldots, a_n)$ be one of the elements from $\mathrm{V}(I)$. Since $I = \langle f_1, f_2, \ldots, f_s \rangle$, then f_1, f_2, $\ldots$, f_s are also polynomials in I. Now $f_1(a_1, a_2, \ldots, a_n) = 0$, $f_2(a_1, a_2, \ldots, a_n) = 0$, $\ldots$, $f_s(a_1, a_2, \ldots, a_n) = 0$. So, $\mathbf{V}(I) \subset \mathbf{V}(f_1, f_2, \ldots, f_s)$. Next, we will show that $\mathbf{V}(f_1, f_2, \ldots, f_s) \subset \mathbf{V}(I)$. Suppose that $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(f_1, f_2, \ldots, f_s)$ and $f \in I$. We want to show that $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. Since f is in I it can be written as a linear combination of the polynomials $f_1, f_2, \ldots, f_s$, i.e. $f = h_1 f_1 + h_2 f_2 + \ldots + h_s f_s$ where $h_i \in k[x_1, x_2, \ldots, x_n]$. So

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

Thus, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$ and $\mathbf{V}(f_1, f_2, \ldots, f_s) \subset \mathbf{V}(I)$. Therefore, $\mathbf{V}(I) = \mathbf{V}(f_1, f_2, \ldots, f_s)$. □

3.4 Properties of Groebner Bases

In the previous section it was shown that every ideal $I \subset k[x_1, x_2, \ldots, x_n]$ has a Groebner basis as long as I is a nonzero ideal. We will now take a closer look at the properties of a Groebner basis. We shall begin by examining the problem encountered by using the division algorithm with polynomials from $k[x_1, x_2, \ldots, x_n]$. In Section 3.2, the division algorithm was illustrated by dividing $x^4y^2 + x^2y^3 + y^2$ by $xy - 1$ and $y^2 - 1$. The first time the division was performed, $f_1 = xy - 1$ and $f_2 = y^2 - 1$ so that

$$x^4y^2 + x^2y^3 + y^2 = (x^3y + x^2 + xy^2 + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + (x^2 + y + 1).$$

On the other hand, the second time the division algorithm was used, we let $f_1 = y^2 - 1$ and $f_2 = xy - 1$. In other words, the order of the divisors was switched which led to the following

$$x^4y^2 + x^2y^3 + y^2 = x \cdot (xy - 1) + (x^4 + x^2y + 1) \cdot (y^2 - 1) + (x^4 + x + 1).$$

By comparing the two results we notice that both the quotients and the remainders are not the same. Using the division algorithm with multivariable polynomials illustrates a problem not present with single variable polynomials: the remainder is not unique. However, we will prove that a polynomial from $k[x_1, x_2, \ldots, x_n]$ that is divided by a Groebner basis will have a unique remainder no matter how the divisors are ordered.

Proposition 3.15. *Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then there is a unique $r \in k[x_1, \ldots, x_n]$ with the following two properties:*

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

(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 the elements of G are listed when using the division algorithm.

Proof. According to the division algorithm, we can write the polynomial $f \in k[x_1, x_2, \ldots, x_n]$ in the following manner $f = a_1g_1 + a_2g_2 + \ldots + a_tg_t + r$. One possibility is that the remainder r is zero. However, if r is not zero, then it is a linear combination of monomials that are not divisible by any of $\mathrm{LT}(g_1)$, $\mathrm{LT}(g_2)$, $\ldots$, $\mathrm{LT}(g_t)$. Hence, condition (i) has been satisfied by the division algorithm in $k[x_1, x_2, \ldots, x_n]$. By letting $g = a_1g_1 + a_2g_2 + \ldots + a_tg_t$ in the equation for f, we get $f = g + r$ as stated in condition (ii). Notice that $g \in I$ because g is a linear combination of the polynomials g_1, g_2, $\ldots$, g_t. Finally, we must prove that the remainder is unique regardless of the order of the divisors used. Suppose that $f = g + r = g' + r'$ where g, r, g', and r' each satisfy conditions (i) and (ii) above. By rearranging the equation, $r - r' = g' - g \in I$. If the remainders r and r' are not the same, then $\text{LT}(r - r') \in \langle \text{LT}(I) \rangle$ since $r - r' \in I$. However, this implies that $\text{LT}(r - r') \in \langle \text{LT}(g_1), \text{LT}(g_2), \ldots, \text{LT}(g_t) \rangle$. Since G is a Groebner basis $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \text{LT}(g_2), \ldots, \text{LT}(g_t) \rangle$. Consequently, $\text{LT}(r - r')$ will be divisible by some $\text{LT}(g_i)$. This cannot happen because none of the monomials of r and r' are divisible by any $\text{LT}(g_i)$ as stated by condition (i). As a result, $r - r' = 0$ which means that r must equal r'. Thus, when f is divided by the polynomials $g_1, g_2, \ldots, g_t$ from a Groebner basis the remainder is unique. □

Despite the fact that it has been shown that using the division algorithm with a Groebner basis results in a unique remainder, the same cannot be said for the quotients or a_i's in $f = a_1 g_1 + a_2 g_2 + \ldots a_t g_t$. If the order of the polynomials in the basis is changed, this will result in different quotients. Let $G = \{x + z, y - z\}$ be a Groebner basis using lex order with $x > y > z$. It will be shown later in this section why the set of polynomials $G = \{x + z, y - z\}$ is a Groebner basis. We will now observe what happens when the polynomial xy is divided by G. For the first division let $f_1 = x + z$ and $f_2 = y - z$. Dividing the polynomial xy by f_1 and f_2 we get,

$$\begin{array}{rl}
a_1 : & y \\
a_2 : & -z \\
x + z & \sqrt{\overline{xy}} \\
y - z & \underline{-(xy + yz)} \\
 & \quad -yz \\
 & \quad \underline{-(-yz + z^2)} \\
 & \qquad \underline{-z^2} \\
 & \qquad 0 \quad \longrightarrow \quad -z^2
\end{array}$$

$$xy = y \cdot (x + z) - z \cdot (y - z) - z^2.$$

If the arrangement of the divisors is changed, Proposition 3.15 states that the remainder of the next division will be the same as the remainder from the previous division. The polynomial xy will be divided by $f_1 = y - z$ and $f_2 = x + z$.

$$\begin{array}{rlll}
a_1 : & x & & \\
a_2 : & z & & \\
y - z & \sqrt{xy} & & \\
x + z & \underline{-xy + xz} & & \\
 & \quad xz & & \\
 & \quad \underline{-\, xz - z^2} & & \\
 & \qquad \underline{-z^2} & & \\
 & \qquad\ 0 & \longrightarrow & -z^2
\end{array}$$

$$xy = x \cdot (y - z) + z \cdot (x + z) - z^2$$

Comparing the results from each division the remainders are both $-z^2$ as predicted. On the other hand, the quotients are different. In the first division $a_1 = y$ and $a_2 = -z$, but $a_1 = x$ and $a_2 = z$ in the second.

Corollary 3.16. *Let $G = \{g_1, \ldots, g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ and let $f \in k[x_1, \ldots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.*

Proof. If the remainder when we divide the polynomial f by G is zero, then

$$\begin{aligned} f &= a_1 g_1 + a_2 g_2 + \ldots + a_t g_t + r, \\ &= a_1 g_1 + a_2 g_2 + \ldots + a_t g_t. \end{aligned}$$

This implies that the polynomial f is a linear combination of g_1, g_2, $\ldots$, g_t, so $f \in I$. If it is given that $f \in I$, then $f = f + 0$. Thus, the remainder is zero when f is divided by the Groebner basis G. □

With the help of Corollary 3.16, there is now an algorithm available that will help with the ideal membership problem. It will be possible to determine if a polynomial $f \in k[x_1, x_2, \ldots, x_n]$ is an element of the ideal $I = \langle f_1, f_2, \ldots, f_s \rangle$ if we have a Groebner basis for I. When we have a Groebner basis, finding the remainder when f is divided by G will tell us whether $f \in I$. We shall next introduce some notation for this remainder.

Definition 3.17. We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, \ldots, f_s)$. If F is a Groebner basis for $\langle f_1, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order) by Proposition 3.15.

In the example worked at the beginning of this section with $F = (x+z, y-z) \subset \mathbb{R}[x, y, z]$, the remainder or $\overline{xy}^F = -z^2$.

At the beginning of Section 3.3, we looked at the given ideal $I = \langle g_1, g_2, g_3 \rangle = \langle xy^2 - xz + y, xy - z^2, x - yz^4 \rangle$. The polynomial $g = -yz^5 + yz^2 + y$ is an element of I since it is a linear combination of g_1, g_2, and g_3. Consequently, the $\text{LT}(g) = -yz^5 \in \langle \text{LT}(I) \rangle$. But $-yz^5 \notin \langle \text{LT}(g_1), \text{LT}(g_2), \text{LT}(g_3) \rangle$ since it is not divisible by any of the $\text{LT}(g_i)$. As a result, the set $\{xy^2 - xz + y, xy - z^2, x - yz^4\}$ is not a Groebner basis. So how does something like this occur? By taking a closer look at the linear combination used to find the polynomial g we can make an interesting observation. In the computation, the largest terms of the polynomial xy^2 and xz are cancelled. The smaller terms that are left over $-yz^5$, yz^2 and y are not divisible by $\text{LT}(g_1)$, $\text{LT}(g_2)$, or the $\text{LT}(g_3)$. Thus, if the linear combination of the elements in a basis generates polynomials that have had the largest terms cancelled, then that polynomial will never belong to the ideal generated by the $\text{LT}(g_i)$. So, the basis cannot be called a Groebner basis. To better examine the effect of this cancellation, we will define S-polynomials.

Definition 3.18. Let $f, g \in k[x_1, \ldots, x_n]$ be nonzero polynomials.

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

(ii) The **S − polynomial** of f and g is the combination

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

(Note that we are inverting the leading coefficients here as well.)

For instance, let us compute $S(f, g)$ using lex order for $f = 4x^2z - 7y^2$ and $g = xyz^2 + 3xz^4$ in $\mathbb{R}[x, y, z]$. The $\text{multideg}(f) = \alpha$ and $\text{multideg}(g) = \beta$. So, $\alpha = (2, 0, 1)$ and $\beta = (1, 1, 2)$. Using α and β, we can now find $\gamma = (\gamma_1, \gamma_2, \gamma_3)$. By comparing the corresponding elements in the ordered triplets α and β we get,

$$\begin{aligned}
\gamma_1 &= \max(\alpha_1, \beta_1) \\
&= \max(2, 1) \\
&= 2 \\
\gamma_2 &= \max(\alpha_2, \beta_2) \\
&= \max(0, 1) \\
&= 1 \\
\gamma_3 &= \max(\alpha_3, \beta_3) \\
&= \max(1, 2) \\
&= 2.
\end{aligned}$$

Since $\gamma = (2, 1, 2)$, the least common multiple $x^\gamma = x^2yz^2$. To compute the S-polynomial,

$$\begin{aligned}
S(f, g) &= \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g \\
&= \frac{x^2yz^2}{4x^2z} \cdot (4x^2z - 7y^2) - \frac{x^2yz^2}{xyz^2} \cdot (xyz^2 + 3xz^4) \\
&= x^2yz^2 - \frac{7}{4}y^3z - x^2yz^2 - 3x^2z^4 \\
&= -3x^2z^4 - \frac{7}{4}y^3z.
\end{aligned}$$

From our computations above, it is important to note that the S-polynomial results in the cancellation of leading terms.

Theorem 3.19. *Let I be a polynomial ideal. Then a basis $G = \{g_1, \ldots, g_t\}$ 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.*

For a complete proof of Theorem 3.19 please refer to pages 82 - 84 of [CLO97].

The theorem above is referred to as Buchberger's S-pair criterion. With this theorem it will now be possible and much easier to determine if a given basis really is a Groebner basis. This criterion will enable us to generate an algorithm in order to find a Groebner basis. Earlier it was stated that the set $G = \{x + z, y - z\}$ is a Groebner basis. Using Buchberger's S-pair criterion it will be shown that G is a Groebner basis for lex order where $x > y > z$. We shall start by computing the S-polynomial $S(g_1, g_2)$.

Let $\alpha = \text{multideg}(g_1) = (1,0,0)$ and $\beta = \text{multideg}(g_2) = (0,1,0)$. Comparing the corresponding elements in the ordered triplets α and β then $\gamma = (\gamma_1, \gamma_2, \gamma_3)$ is

$$\begin{aligned} \gamma_1 &= \max(\alpha_1, \beta_1) \\ &= \max(1,0) \\ &= 1 \\ \gamma_2 &= \max(\alpha_2, \beta_2) \\ &= \max(0,1) \\ &= 1 \\ \gamma_3 &= \max(\alpha_3, \beta_3) \\ &= \max(0,0) \\ &= 0. \end{aligned}$$

So the least common multiple $x^\gamma = xy$. To compute the S-polynomial,

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

If we can verify that $\overline{xz+yz}^G$ is zero, then G is a Groebner basis for $I = \langle x+z, y-z \rangle$. By the division algorithm,

$$\begin{array}{rl} a_1: & z \\ a_2: & z \\ x+z & \sqrt{xz+yz} \\ y-z & \underline{-(xz+z^2)} \\ & \qquad yz - z^2 \\ & \qquad \underline{-(yz-z^2)} \\ & \qquad\qquad 0 \end{array}$$

$$xz + yz = z(x+z) + z(y-z) + 0.$$

Therefore, G is a Groebner basis for the ideal I.

3.5 Buchberger's Algorithm

In the previous sections of Chapter 3 a lot of time was spent defining a Groebner basis and studying the properties of a Groebner basis. It was also shown that every nonzero ideal has a Groebner basis. The only question that has yet to be answered is how do we construct a Groebner basis? If the ideal I is a subset of the polynomial ring $k[x_1, x_2, \ldots, x_n]$, how can we make a Groebner basis for I? To help answer this question we will take a look at the following example. Suppose the ideal $I = \langle g_1, g_2 \rangle$ where $g_1 = x^2y - 1$ and $g_2 = xy^2 - x$. In order for $\{g_1, g_2\}$ to be a Groebner basis we must add more polynomials to the given set. To help determine the polynomials that should be added to the basis we will make use of S-polynomials. To compute $S(g_1, g_2)$, $\alpha = (2,1)$, $\beta = (1,2)$, $\gamma = (2,2)$ making the least common multiple $x^\gamma = x^2y^2$. So

$$\begin{aligned}
S(g_1, g_2) &= \frac{x^2y^2}{x^2y} \cdot (x^2y - 1) - \frac{x^2y^2}{xy^2} \cdot (xy^2 - x) \\
&= y(x^2y - 1) - x(xy^2 - x) \\
&= x^2y^2 - y - x^2y^2 + x^2 \\
&= x^2 - y.
\end{aligned}$$

Dividing $S(g_1, g_2)$ by the set $G = \{x^2y - 1, xy^2 - x\}$

$$\begin{array}{rl}
a_1 : & 0 \\
a_2 : & 0 \\
x^2y - 1 & \sqrt{\,x^2 - y} \\
xy^2 - x & \quad \underline{\quad 0} \\
 & \quad x^2 - y
\end{array}$$

The division shows that $\overline{S(g_1, g_2)}^G = x^2 - y$. Since the remainder is not zero we will call this polynomial $g_3 = x^2 - y$ and add it to the the set G. Now we will check to see if $G = \{x^2y - 1, xy^2 - x, x^2 - y\}$ is a Groebner basis. Using Theorem 3.19, if $\overline{S(g_i, g_j)}^G = 0$ for all $i \neq j$, then G is a Groebner basis. Since $S(g_1, g_2) = g_3$ then $\overline{S(g_1, g_2)}^G = 0$. To compute $S(g_1, g_3)$, $\alpha = (2,1)$, $\beta = (2,0)$, $\gamma = (2,1)$ making the LCM $x^\gamma = x^2y$. So

$$\begin{aligned} S(g_1, g_3) &= \frac{x^2y}{x^2y} \cdot (x^2y - 1) - \frac{x^2y}{x^2} \cdot (x^2 - y) \\ &= 1(x^2y - 1) - y(x^2 - y) \\ &= x^2y - 1 - x^2y + y^2 \\ &= y^2 - 1. \end{aligned}$$

Dividing $S(g_1, g_3)$ by the set $G = \{x^2y - 1, xy^2 - x, x^2 - y\}$

$$\begin{array}{rl} a_1 : & 0 \\ a_2 : & 0 \\ a_3 : & 0 \\ \cline{2-2} x^2y - 1 & \big) \; y^2 - 1 \\ xy^2 - x & \qquad\quad 0 \\ \cline{2-2} x^2 - y & \; y^2 - 1 \end{array}$$

The division shows that $\overline{S(g_1, g_3)}^G = y^2 - 1$. Since the remainder is not zero we will call this polynomial $g_4 = y^2 - 1$ and add it to the the set G. Now we will repeat the same process to determine if $G = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1\}$ is a Groebner basis. Notice that $\overline{S(g_1, g_2)}^G = \overline{S(g_1, g_3)}^G = 0$. To compute $S(g_1, g_4)$, $\alpha = (2,1)$, $\beta = (0,2)$, $\gamma = (2,2)$ making the LCM $x^\gamma = x^2y^2$. So

$$\begin{aligned} S(g_1, g_4) &= \frac{x^2y^2}{x^2y} \cdot (x^2y - 1) - \frac{x^2y^2}{y^2} \cdot (y^2 - 1) \\ &= y(x^2y - 1) - x^2(y^2 - 1) \\ &= x^2y^2 - y - x^2y^2 + x^2 \\ &= x^2 - y. \end{aligned}$$

Unfortunately, $\overline{S(g_1, g_4)}^G = x^2 - y$ but this remainder equals g_3, so there is nothing new to add to the basis G. To compute $S(g_2, g_3)$, $\alpha = (1,2)$, $\beta = (2,0)$, $\gamma = (2,2)$ making the LCM $x^\gamma = x^2y^2$. So

$$\begin{aligned} S(g_2, g_3) &= \frac{x^2y^2}{xy^2} \cdot (xy^2 - x) - \frac{x^2y^2}{x^2} \cdot (x^2 - y) \\ &= x(xy^2 - x) - y^2(x^2 - y) \\ &= x^2y^2 - x^2 - x^2y^2 + y^3 \\ &= -x^2 + y^3. \end{aligned}$$

Dividing $S(g_2, g_3)$ by the set $G = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1\}$

$$\begin{array}{rl}
a_1: & 0 \\
a_2: & 0 \\
a_3: & -1 \\
a_4: & y \\ \cline{2-2}
x^2y-1 & \big) \; -x^2 + y^3 \\
xy^2-x & -(-x^2+y) \\ \cline{2-2}
x^2-y & \qquad y^3 - y \\
y^2-1 & \quad -(y^3-y) \\ \cline{2-2}
 & \qquad\quad 0
\end{array}$$

The division shows that $\overline{S(g_2, g_3)}^G = 0$ so the set G remains unchanged. To compute $S(g_2, g_4)$, $\alpha = (1, 2)$, $\beta = (0, 2)$, $\gamma = (1, 2)$ making the LCM $x^\gamma = xy^2$. So

$$\begin{aligned}
S(g_2, g_4) &= \frac{xy^2}{xy^2} \cdot (xy^2 - x) - \frac{xy^2}{y^2} \cdot (y^2 - 1) \\
&= 1(xy^2 - x) - x(y^2 - 1) \\
&= xy^2 - x - xy^2 + x \\
&= 0.
\end{aligned}$$

Dividing $S(g_2, g_4)$ by G is still zero therefore G will not change. To compute $S(g_3, g_4)$, $\alpha = (2, 0)$, $\beta = (0, 2)$, $\gamma = (2, 2)$ making the LCM $x^\gamma = x^2y^2$. So

$$\begin{aligned}
S(g_3, g_4) &= \frac{x^2y^2}{x^2} \cdot (x^2 - y) - \frac{x^2y^2}{y^2} \cdot (y^2 - 1) \\
&= y^2(x^2 - y) - x^2(y^2 - 1) \\
&= x^2y^2 - y^3 - x^2y^2 + x^2 \\
&= x^2 - y^3.
\end{aligned}$$

Dividing $S(g_3, g_4)$ by the set $G = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1\}$

$$\begin{array}{rl}
a_1 : & 0\\
a_2 : & 0\\
a_3 : & 1\\
a_4 : & -y\\
x^2y-1 & \sqrt{\;x^2-y^3}\\
xy^2-x & \underline{-(x^2-y)\quad}\\
x^2-y & \qquad -y^3+y\\
y^2-1 & \underline{\quad -(-y^3+y)}\\
 & \qquad\qquad 0
\end{array}$$

The division shows that $\overline{S(g_3,g_4)}^G = 0$ so the set G stays the same. It has been shown that for the set $G = \{x^2y-1, xy^2-x, x^2-y, y^2-1\}$, $\overline{S(g_i,g_j)}^G = 0$ for all combinations in which $i \neq j$. Therefore, we may call G a Groebner basis. A formal definition of the algorithm used above to compute a Groebner basis is detailed below.

Theorem 3.20. *Let $I = \langle f_1,\dots,f_s\rangle \neq \{0\}$ be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following algorithm:*
Let $F_n = \{f_1,\dots,f_s\}$.
Step 1: For each pair $\{f_i,f_j\}$ in F_n where $i \neq j$ compute the S-polynomial $S(f_i,f_j)$.
Step 2: Take the S-polynomial previously computed and let $S = \overline{S(f_i,f_j)}^{F_n}$.
Step 3: If $S \neq 0$, then S must be added to the set so that $F_{n+1} = F_n \cup \{S\}$. Whenever $S = 0$ there is nothing new to add to the basis.
Now steps 1 - 3 are repeated until the set $F_{n+1} = F_n$ for some n.

One important note needs to be made regarding the use of the algorithm above to find a Groebner basis. Computing a Groebner basis with Theorem 3.20 often leads to a set of polynomials that is bigger than it needs to be. These extra generators can be removed from the computed basis and the remaining set of polynomials will still be a Groebner basis.

Lemma 3.21. *Let G be a Groebner basis for the polynomial ideal I. Let $p \in G$ be a polynomial such that $\mathrm{LT}(p) \in \langle \mathrm{LT}(G-\{p\})\rangle$. Then $G-\{p\}$ is also a Groebner basis for I.*

Proof. Let $G = \{g_1, g_2, \ldots, g_s, p\}$ be a Groebner basis for I. Then $\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle$. We would like to prove that $G-\{p\}$ is also a Groebner basis for I, $\langle \mathrm{LT}(G-\{p\})\rangle = \langle \mathrm{LT}(I)\rangle$. In other words, $\langle \mathrm{LT}(G-\{p\})\rangle = \langle \mathrm{LT}(G)\rangle$. First, it will be shown that $\langle \mathrm{LT}(G-\{p\})\rangle \subset \langle \mathrm{LT}(G)\rangle$. Suppose that $g \in \langle \mathrm{LT}(G-\{p\})\rangle$. Then the polynomial g can be written in the following manner

$$\begin{aligned} g &= h_1\mathrm{LT}(g_1) + h_2\mathrm{LT}(g_2) + \ldots + h_s\mathrm{LT}(g_s), \\ &= h_1\mathrm{LT}(g_1) + h_2\mathrm{LT}(g_2) + \ldots + h_s\mathrm{LT}(g_s) + 0 \cdot \mathrm{LT}(p). \end{aligned}$$

Since g is a linear combination of the elements in $\langle \mathrm{LT}(G)\rangle$ then $g \in \langle \mathrm{LT}(G)\rangle$. Next, we must show that $\langle \mathrm{LT}(G)\rangle \subset \langle \mathrm{LT}(G-\{p\})\rangle$. Assume that $g \in \langle \mathrm{LT}(G)\rangle$. Consequently, g can be written as the linear combination $g = h_1\mathrm{LT}(g_1) + h_2\mathrm{LT}(g_2) + \ldots + h_s\mathrm{LT}(g_s) + h\mathrm{LT}(p)$. Notice that every $\mathrm{LT}(g_i)$ is an element of $\mathrm{LT}(G-\{p\})$. Furthermore, from our hypothesis $\mathrm{LT}(p) \in \langle \mathrm{LT}(G-\{p\})\rangle$. As a result, each product listed in the linear combination is an element of $\langle \mathrm{LT}(G-\{p\})\rangle$ and by closure $g \in \langle \mathrm{LT}(G-\{p\})\rangle$. Thus, $\langle \mathrm{LT}(G-\{p\})\rangle = \langle \mathrm{LT}(G)\rangle$, so $G-\{p\}$ is also a Groebner basis for the ideal I. □

So how do we determine which generators are extra and should be removed from the Groebner basis? A generator that is a linear combination of the remaining polynomials in the basis is not needed. This new basis will be called a reduced Groebner basis.

Definition 3.22. 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 $\langle \mathrm{LT}(G-\{p\})\rangle$.

Now we shall reexamine the Groebner basis $G = \{x^2y-1, xy^2-x, x^2-y, y^2-1\}$ that was computed earlier. Let $g_1 = x^2y-1$, $g_2 = xy^2-x$, $g_3 = x^2-y$, and $g_4 = y^2-1$. Taking a closer look at the generator $g_2 = xy^2 - x = x(y^2-1) = x \cdot g_4$. Since it was shown g_2 is a multiple of g_4 it can be removed from the set so that $G = \{x^2y-1, x^2-y, y^2-1\}$. In addition, we can make an interesting observation about the polynomial g_1 and the set

G using the division algorithm. Dividing g_1 by $x^2 - y$ and $y^2 - 1$ we see that

$$\begin{array}{rr}
a_1 : & y \qquad\quad \\
a_2 : & 1 \qquad\quad \\
x^2 - y & \sqrt{\; x^2y - 1 \;} \quad \\
y^2 - 1 & -(x^2y - y^2) \quad \\
\cline{2-2}
 & y^2 - 1 \\
 & -(y^2 - 1) \\
\cline{2-2}
 & 0 \;\;
\end{array}$$

$$\begin{aligned}
g_1 &= x^2y - 1, \\
&= y(x^2 - y) + 1(y^2 - 1) + 0, \\
&= y \cdot g_3 + 1 \cdot g_4.
\end{aligned}$$

So g_1 must also be eliminated from the set G. Finally, the reduced Groebner basis that has been computed for the set is $G = \{x^2 - y, y^2 - 1\}$.

Chapter 4

The Algebra-Geometry Connection

The goal of this project is to be able to prove geometric theorems algebraically. To accomplish this, time was spent discussing and defining concepts from geometry and algebra that would be needed. We have discussed affine varieties, ideals, and Groebner bases. However, we have not yet established a connection between each of these concepts. This chapter will be devoted to explaining the relationship between the algebraic and geometric concepts previously mentioned. We shall be able to bridge the gap between these ideas by proving Hilbert's Nullstellensatz Theorem.

4.1 Hilbert's Nullstellensatz

The most important connection that we want to establish is between varieties and ideals of polynomials. Basically, if we have a variety can it be converted to an ideal? Likewise, if we have an ideal can it be changed to an affine variety? It turns out that there exist two maps that will show that this is possible. Earlier we learned about the ideal of a variety, $\mathbf{I}(V) = \{f \in k[x_1, x_2, \ldots, x_n] \mid f(x) = 0 \text{ for all } x \in V\}$. The only polynomials that will belong to I are the those that vanish for each n-tuple that is an element of V. So there is a map from an affine variety to an ideal. On the other hand, when we are given an ideal from the polynomial ring $k[x_1, x_2, \ldots, x_n]$, the variety of an ideal is $\mathbf{V}(I) = \{(a_1, a_2, \ldots, a_n) \in k^n \mid f(a_1, a_2, \ldots, a_n) = 0 \text{ for all } f \in I\}$. So is $\mathbf{V}(I)$ an affine variety? The answer to this question is yes. By combining the Hilbert Basis Theorem (Theorem 3.10) which states that $I = \langle f_1, f_2, \dots, f_s \rangle$ and Proposition 3.14, $\mathbf{V}(I)$ is an affine variety. Thus, there is also a map from ideals to affine varieties.

It is important to note that there is the possibility that different ideals will result in the same variety. Let us look at the polynomials $x - 1$ and $x^2 - 2x + 1$ from the ring $\mathbb{R}[x]$. Suppose $I_1 = \langle x - 1 \rangle$ and $I_2 = \langle x^2 - 2x + 1 \rangle$. The ideal $\langle x^2 - 2x + 1 \rangle \subset \langle x - 1 \rangle$. If $p \in \langle x^2 - 2x + 1 \rangle$ it can be written as follows $p = f(x^2 - 2x + 1)$ where $f \in \mathbb{R}[x]$. Now, $p = f(x-1)(x-1)$ and $f(x-1) \in \mathbb{R}[x]$. Thus, $p \in \langle x - 1 \rangle$ and $\langle x^2 - 2x + 1 \rangle \subset \langle x - 1 \rangle$. On the other hand, the element $x - 1$ from $\langle x - 1 \rangle$ is not contained in $\langle x^2 - 2x + 1 \rangle$ so $\langle x - 1 \rangle \not\subset \langle x^2 - 2x + 1 \rangle$. We have confirmed that $\langle x - 1 \rangle \neq \langle x^2 - 2x + 1 \rangle$ so we can be sure that we are working with two different ideals. The variety $\mathbf{V}(I_1) = \{a \in \mathbb{R} \mid f(a) = 0$ for all $f \in I_1\}$. The only value that makes the polynomial $x - 1 = 0$ is 1. For the next variety $\mathbf{V}(I_2) = \{b \in \mathbb{R} \mid g(b) = 0$ for all $g \in I_2\}$. The only element from $\mathbb{R}$ that makes $x^2 - 2x + 1 = 0$ is also 1. Consequently, since $I_1 \neq I_2$ resulted in $\mathbf{V}(I_1) = \mathbf{V}(I_2) = \{1\}$, the map $\mathbf{V}$ is not one-to-one. This creates a problem that needs to be eliminated. If we have an ideal that generates the entire polynomial ring and a variety is computed on this ideal, then the variety should produce the empty set. We do not want other varieties of ideals from the ring $k[x_1, x_2, \dots, x_n]$ to also generate the empty set. To illustrate this problem let us look at the polynomials $1+x^2+y^2$ and $1+x^2+y^4$ from the ring $\mathbb{R}[x,y]$. Let $I_1 = \langle 1+x^2+y^2 \rangle$ and $I_2 = \langle 1+x^2+y^4 \rangle$. The variety $\mathbf{V}(I_1) = \{(a_1, a_2) \in \mathbb{R}^2 \mid f(a_1, a_2) = 0$ for all $f \in I_1\}$. The only ordered pairs that make the polynomial $1 + x^2 + y^2 = 0$ are $(i, 0)$, $(-i, 0)$, $(0, i)$, and $(0, -i)$. Unfortunately, these four ordered pairs are not elements from $\mathbb{R}^2$, so $\mathbf{V}(I_1) = \emptyset$. The next variety $\mathbf{V}(I_2) = \{(b_1, b_2) \in \mathbb{R}^2 \mid g(b_1, b_2) = 0$ for all $g \in I_2\}$. The ordered pairs that make $1 + x^2 + y^4 = 0$ are $(i, 0)$ and $(-i, 0)$. But again we encounter the same problem when we computed $\mathbf{V}(I_1) : (i, 0) \notin \mathbb{R}^2$ and $(-i, 0) \notin \mathbb{R}^2$. Thus, $\mathbf{V}(I_2) = \emptyset$. Note that the field $\mathbb{R}$ is not algebraically closed because the roots found came from $\mathbb{C}$ and not from $\mathbb{R}$. If there are different ideals that generate the empty variety can we resolve this issue by working with a field that is algebraically closed? Let us first take a look at the single variable case.

Theorem 4.1. *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. Every ideal $I = \langle f \rangle$ for some $f \in k[x]$ since $k[x]$ is a PID by Corollary 2.11.

Suppose $f \in k[x]$ is a nonconstant polynomial, then $\mathbf{V}(I) = \{a \in k \mid g(a) = 0$ for all $g \in I\}$. We will be able to find the roots of f from the field k since it is algebraically closed. So $\mathbf{V}(I) \neq \emptyset$. However, if $f \in k[x]$ is a constant, then the $\mathbf{V}(I) = \emptyset$. An element from the ideal $I = \langle f \rangle$ is $g \cdot f$ where $g \in k[x]$. Because f is a constant element from the polynomial ring $k[x]$, there exists an element $g = \frac{1}{f}$, the multiplicative inverse of f, that also belongs to $k[x]$. Hence, $g \cdot f = \frac{1}{f} \cdot f = 1$. This means that 1 is an element of the ideal I so $g \in I$ for all $g \in k[x]$. This makes $I = k[x]$, which is the entire polynomial ring. If $I = k[x]$, then it will not be possible to find a common solution to the system of equations $f_1(x) = 0$, $f_2(x) = 0$, $\ldots$, for all f_i's in $k[x]$. Therefore, taking the variety of the entire polynomial ring $\mathbf{V}(I)$ is empty. □

By studying the single variable case, we were able to determine that when k is an algebraically closed field, computing the variety of the whole polynomial ring $k[x]$ will be the empty set. This finding can also be applied to a ring $k[x_1, x_2, \ldots, x_n]$ that is made up of multivariable polynomials.

Theorem 4.2 (The Weak Nullstellensatz). *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 $I = k[x_1, x_2, \ldots, x_n]$.*

For a detailed proof of The Weak Nullstellensatz refer to pages 168 - 169 of [CLO97].

The Weak Nullstellensatz is an important tool that will be used to determine whether a system of polynomials will have any common solutions. In order to determine if the variety $\mathbf{V}(f_1, f_2, \ldots, f_s) = \emptyset$ for $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$ we must satisfy two conditions. First, the field k must be algebraically closed. Second, we must determine if 1 is an element of the ideal generated by $f_1, f_2, \ldots, f_s$. This can be done by induction on n noting that the case $n = 1$ was proved above. So the Weak Nullstellensatz allows us to generate the following consistency algorithm. If we have polynomials $f_1, f_2, \ldots, f_s \in \mathbb{C}[x_1, x_2, \ldots, x_n]$, we compute a reduced Groebner basis of the ideal they generate with respect to any ordering. If this basis is $\{1\}$, the polynomials have no common zero in $\mathbb{C}^n$; if the basis is not $\{1\}$, they must have a common zero. Note that the algorithm works over any algebraically closed field. [CLO97]

Despite the fact that the Weak Nullstellensatz tells us whether a system of equations has a solution, there is still a flaw present between the maps of ideals and varieties. Adding the restriction that k must be an algebraically closed field does not make the correspondence between ideals and varieties one-to-one. Earlier we computed the varieties of the ideals $I_1 = \langle x-1 \rangle$ and $I_2 = \langle x^2-2x+1 \rangle$ where $x-1$ and $x^2-2x+1 \in \mathbb{R}[x]$. Let us compute the varieties of I_1 and I_2 once again where $x-1$ and x^2-2x+1 are polynomials from an algebraically closed field $\mathbb{C}[x]$. The ideals $I_1 \neq I_2$ both generate the variety $\mathbf{V}(I_1) = \mathbf{V}(I_2) = \{1\}$. Note that $x^2 - 2x + 1 = (x-1)^2$. The Hilbert Nullstellensatz states that, over an algebraically closed field, this is the only reason that different ideals can give the same variety: if a polynomial f vanishes at all points of some variety $\mathbf{V}(I)$, then some power of f must belong to I. [CLO97]

Theorem 4.3 (Hilbert's Nullstellensatz). *Let k be an algebraically closed field. If f, $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ are such that $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, then there exists an integer $m \geq 1$ such that*

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

(and conversely).

Proof. Since the polynomial $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$, then for all $(a_1, a_2, \ldots, a_n) \in \mathbf{V}$, $f(a_1, a_2, \ldots, a_n) = 0$. We would like to show that $f^m \in \langle f_1, f_2, \ldots, f_s \rangle$ for some $m \geq 1$. In other words that $f^m = A_1 f_1 + A_2 f_2 + \ldots + A_s f_s$ for $m \geq 1$ and the polynomials $A_1, A_2, \ldots, A_s$ are from the ring $k[x_1, x_2, \ldots, x_n]$. To begin, we will use a trick to help us complete the proof for this theorem. Let the ideal $\tilde{I} = \langle f_1, f_2, \ldots, f_s, 1 - yf \rangle \subset k[x_1, x_2, \ldots, x_n, y]$. The polynomials $f_1, f_2, \ldots, f_s$ are still from $k[x_1, x_2, \ldots, x_n]$. Our goal is to show that $\tilde{I} = k[x_1, x_2, \ldots, x_n, y]$. In order to do this we must show that $\mathbf{V}(\tilde{I}) = \emptyset$. Let $(a_1, a_2, \ldots, a_n, a_{n+1}) \in k^{n+1}$. There are now two possible scenarios, the n-tuple is a common zero or it is not. First, suppose the n-tuple $(a_1, a_2, \ldots, a_n)$ is a common zero of the polynomials $f_1, f_2, \ldots, f_s$. If this occurs, then $f(a_1, a_2, \ldots, a_n) = 0$ since $f \in \mathbf{I}(\mathbf{V}(f_1, f_2, \ldots, f_s))$ and so f will also disappear at the n-tuples that make $f_1, f_2, \ldots, f_s$ vanish.

Assume that $(a_1, a_2, \ldots, a_n, a_{n+1}) \in \mathbf{V}(\tilde{I})$ and also let $g \in \tilde{I}$. This means that $g(a_1,\, a_2,\, \ldots,\, a_n,\, a_{n+1})$ must equal zero. The polynomial g can be written as follows, $g = g_1(x_1, x_2, \ldots, x_n, y) f_1(x_1, x_2, \ldots, x_n) + g_2(x_1, x_2, \ldots, x_n, y) f_2(x_1, x_2, \ldots, x_n) + \ldots + g_s(x_1, x_2, \ldots, x_n, y) f_s(x_1, x_2, \ldots, x_n) + g_{s+1}(x_1, x_2, \ldots, x_n, y)(1 - yf(x_1, x_2, \ldots, x_n))$.

Evaluating g at the n-tuple $(a_1, a_2, \ldots, a_n, a_{n+1})$ we get,

$$\begin{aligned} g(a_1, a_2, \ldots, a_n, a_{n+1}) &= g_1(a_1, a_2, \ldots, a_n, a_{n+1})f_1(a_1, a_2, \ldots, a_n) \\ &\quad + g_2(a_1, a_2, \ldots, a_n, a_{n+1})f_2(a_1, a_2, \ldots, a_n) + \ldots \\ &\quad + g_s(a_1, a_2, \ldots, a_n, a_{n+1})f_s(a_1, a_2, \ldots, a_n) \\ &\quad + g_{s+1}(a_1, a_2, \ldots, a_n, a_{n+1})(1 - a_{n+1}f(a_1, a_2, \ldots, a_n)). \end{aligned}$$

Continuing the computation,

$$\begin{aligned} g(a_1, \ldots, a_{n+1}) &= g_1(a_1, a_2, \ldots, a_n, a_{n+1}) \cdot 0 + \ldots + g_s(a_1, a_2, \ldots, a_n, a_{n+1}) \cdot 0 \\ &\quad + g_{s+1}(a_1, a_2, \ldots, a_n, a_{n+1})(1 - a_{n+1} \cdot 0) \\ &= 0 + 0 + \ldots + 0 + g_{s+1}(a_1, a_2, \ldots, a_n, a_{n+1}) \\ &= g_{s+1}(a_1, a_2, \ldots, a_n, a_{n+1}). \end{aligned}$$

This is clearly a contradiction because the final result of $g_{s+1}(a_1, a_2, \ldots, a_n, a_{n+1})$ is not zero as we expected. So, $(a_1, a_2, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$.

On the other hand, there is the possibility that $(a_1, a_2, \ldots, a_n)$ is not a common zero of the polynomials $f_1, f_2, \ldots, f_s$. This means that $f_i(a_1, a_2, \ldots, a_n) \neq 0$ for some i from $1 \leq i \leq s$. When one more coordinate, a_{n+1}, is added to the original n-tuple $f_i(a_1, a_2, \ldots, a_n, a_{n+1}) \neq 0$. We have again showed that $(a_1, a_2, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$. Therefore, the variety $\mathbf{V}(\tilde{I})$ is the empty set.

It is extremely important that we have a variety that is empty because using the Weak Nullstellensatz we can conclude that 1 is an element of the ideal $\tilde{I}$. Since $1 \in \tilde{I}$ then $1 = p_1(x_1, x_2, \ldots, x_n, y)f_1(x_1, x_2, \ldots, x_n) + p_2(x_1, x_2, \ldots, x_n, y)f_2(x_1, x_2, \ldots, x_n) + \ldots + p_s(x_1, x_2, \ldots, x_n, y)f_s(x_1, x_2, \ldots, x_n) + p(x_1, x_2, \ldots, x_n, y)(1 - yf(x_1, x_2, \ldots, x_n))$ where $p_1, \ldots, p_s, p$ are elements from $k[x_1, x_2, \ldots, x_n, y]$. Letting $y = \frac{1}{f(x_1, x_2, \ldots, x_n)}$ results in $1 = p_1(x_1, x_2, \ldots, x_n, \frac{1}{f})f_1(x_1, x_2, \ldots, x_n) + p_2(x_1, x_2, \ldots, x_n, \frac{1}{f})f_2(x_1, x_2, \ldots, x_n) + \ldots + p_s(x_1, x_2, \ldots, x_n, \frac{1}{f})f_s(x_1, x_2, \ldots, x_n) + p(x_1, x_2, \ldots, x_n, \frac{1}{f})(1 - \frac{1}{f} \cdot f)$. The final product in the previous equation is now zero so that $1 = p_1(x_1, x_2, \ldots, x_n, \frac{1}{f})f_1(x_1, x_2, \ldots, x_n) + p_2(x_1, x_2, \ldots, x_n, \frac{1}{f})f_2(x_1, x_2, \ldots, x_n) + \ldots + p_s(x_1, x_2, \ldots, x_n, \frac{1}{f})f_s(x_1, x_2, \ldots, x_n)$. We can multiply both sides of this equation by f^m making sure to use a value for m that will clear all of the denominators present. This will result in $f^m = A_1 f_1 + A_2 f_2 + \ldots A_s f_s$ where $A_1, A_2, \ldots, A_s \in k[x_1, x_2, \ldots, x_n]$. □

4.2 Radical Ideals and the Ideal-Variety Correspondence

We have yet to find a suitable correspondence between ideals and varieties because we discovered a problem with the mappings that exist. In order to successfully make a connection between algebra and geometry we have to find a way to eliminate this issue. In this section, we will take Hilbert's Nullstellensatz and make improvements that will ultimately allow us to reach our goal.

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

Proof. Let x be an arbitrary element of V. We are given that $f^m \in \mathbf{I}(V)$. Then $(f(x))^m = 0$. However, the only way that this equation can equal zero is when $f(x) = 0$. If $f(x) = 0$, this implies that $f \in \mathbf{I}(V)$ since the polynomial f disappears for $x \in V$. □

This lemma is useful to establish an important property of ideals of varieties. If a power of a polynomial belongs to the ideal of a variety, then the polynomial itself is also an element of that ideal. This property will be formally defined next.

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

Using Definition 4.5, Lemma 4.4 can now be restated as follows: The ideal $\mathbf{I}(V)$ is a radical ideal.

Throughout Section 4.1, time was spent examining in detail the maps between affine varieties and ideals. It was observed that two different ideals can generate the same variety. Consequently, the map $\mathbf{V}$ is not one-to-one. Hilbert's Nullstellensatz Theorem was able to pinpoint the reason why different ideals can result in the same variety. When an ideal contains some power of a polynomial f^m, but the original polynomial f is not in the ideal, the map $\mathbf{V}$ will never be one-to-one. Stating this conclusion differently, this problem will occur when the ideal I is not a radical ideal. This is exactly what happened with the example in the previous section with the two ideals $I_1 = \langle x-1 \rangle$ and $I_2 = \langle x^2-2x+1 \rangle$. Let $f = x-1$. Notice that a power of f, $f^2 = (x-1)^2 = x^2-2x+1$ is in the ideal $\langle x^2-2x+1 \rangle$. Unfortunately, the original polynomial $f = x-1$ is not an element of $\langle x^2-2x+1 \rangle$, i.e. $\langle x^2-2x+1 \rangle$ is not a radical ideal. Consequently, computing the variety of these two different ideals led to the same result $\mathbf{V}(I_1) = \mathbf{V}(I_2) = \{1\}$. Perhaps it will be possible to have a map from ideals to an affine variety that is one-to-one with the help of radical ideals. In order to accomplish this, we must be able to find the radical of a given ideal.

Definition 4.6. 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. *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. We will begin by showing that the ideal I is contained in $\sqrt{I}$. It will be shown that when $f \in I$, then $f \in \sqrt{I}$. If we assume that $f \in I$ this implies that $f^1 \in I$. Since a power (greater than or equal to 1) of f is in the ideal I, f is also an element of $\sqrt{I}$. Thus, $I \subset \sqrt{I}$.

Next, we will prove that $\sqrt{I}$ is an ideal in $k[x_1, x_2, \ldots, x_n]$. In order to show that this set is an ideal, zero must be an element of $\sqrt{I}$. Due to the fact that I is an ideal, $0 \in I$ by definition. This automatically makes 0 an element of $\sqrt{I}$ since $I \subset \sqrt{I}$. Assume that f and g are both elements of $\sqrt{I}$. The second condition that must be satisfied is that $f+g \in \sqrt{I}$. The only way that $f+g$ can be in $\sqrt{I}$ is if $(f+g)^p \in I$ for some $p \geq 1$. Expanding this product results in $(f+g)^p = a_1 f^p + a_2 f^{p-1} g^1 + a_3 f^{p-2} g^2 + \ldots + a_{q-1} f g^{p-1} + a_q g^p$. From our assumption, $f \in \sqrt{I}$ and $g \in \sqrt{I}$ implies that $f^m \in I$ and $g^n \in I$ for some $m, n \geq 1$. We must find the appropriate value for p that will ensure that $(f+g)^p$ is also an element of I. Let $p = m+n-1$. Rewriting the previous expansion of $(f+g)^p$,

$$\begin{aligned}
(f+g)^{m+n-1} &= a_1 f^{m+n-1} + a_2 f^{m+n-2} g + a_3 f^{m+n-3} g^2 + \ldots + a_q f^m g^{n-1} \\
&\quad + a_{q+1} f^{m-1} g^n + a_{q+2} f^{m-2} g^{n+1} + \ldots + a g^{m+n-1}, \\
&= a_1 f^m f^{n-1} + a_2 f^m f^{n-2} g + a_3 f^m f^{n-3} g^2 + \ldots + a_q f^m g^{n-1} \\
&\quad + a_{q+1} f^{m-1} g^n + a_{q+2} f^{m-2} g^n g + \ldots + a g^n g^{m-1}.
\end{aligned}$$

The first group of the terms in the expansion $a_1 f^{m+n-1}$, $a_2 f^{m+n-2} g$, $a_3 f^{m+n-3} g^2$ up to $a_q f^m g^{n-1}$ all contain a factor of f^m in their products. In the second part of the polynomial, the terms $a_{q+1} f^{m-1} g^n$, $a_{q+2} f^{m-2} g^{n+1}$ through $a g^{m+n-1}$ do not contain f^m. Instead, these products contain a factor of g^n. So by individually looking at all of the terms in the expansion of $(f+g)^p$ it has been shown that each one is an element of I because they all contain f^m or g^n. Thus, by closure, $a_1 f^p + a_2 f^{p-1} g^1 + a_3 f^{p-2} g^2 + \ldots + a_{n-1} f g^{p-1} + a_n g^p \in I$. Now, we can conclude that $f+g \in \sqrt{I}$. The third criteria that remains to be shown is that the product $hf \in \sqrt{I}$ for $h \in k[x_1, x_2, \ldots, x_n]$ and $f \in \sqrt{I}$. To show that $hf \in \sqrt{I}$, a power of this product must be an element of I. From our assumption $f \in \sqrt{I}$ implies that $f^m \in I$ for some $m \geq 1$. Now, $(hf)^m = h^m f^m$ where $f^m \in I$ and $h^m \in k[x_1, x_2, \ldots, x_n]$. Therefore, $(hf)^m \in I$ and $hf \in \sqrt{I}$. We have now proven that $\sqrt{I}$ is an ideal in $k[x_1, x_2, \ldots, x_n]$.

Finally, we will prove that $\sqrt{I}$ is a radical ideal. In order to call $\sqrt{I}$ a radical ideal it must be shown than when $f^m \in \sqrt{I}$, then $f \in \sqrt{I}$. If $f^m \in \sqrt{I}$, then $(f^m)^n \in I$ for some $n \geq 1$. Now, $f^{mn} \in I$ implies that $f \in \sqrt{I}$ since $mn \geq 1$. Therefore, $\sqrt{I}$ is a radical ideal. □

Lemma 4.8. *If I is radical, then $\sqrt{I} = I$.*

Proof. Assume I is radical. This implies that if $f^m \in I$ for some $m \geq 1$, then $f \in I$. In order to show that $\sqrt{I} = I$ when I is radical we must show that $I \subset \sqrt{I}$ and $\sqrt{I} \subset I$. It is clear from the proof for Lemma 4.7 that $I \subset \sqrt{I}$. To finish we will now show that $\sqrt{I} \subset I$. Let $f \in \sqrt{I}$. Show that $f \in I$. Since $f \in \sqrt{I}$ this means that $f^m \in I$ for some $m \geq 1$. Therefore, $f \in I$ because we are given that I is radical. □

With the introduction of radical ideals we can improve upon Hilbert's Nullstellensatz Theorem. This will allow us to transition between geometric and algebraic concepts more easily.

Theorem 4.9 (The Strong Nullstellensatz). *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. First, we will show that $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$. Let $f \in \sqrt{I}$. Show that $f \in \mathbf{I}(\mathbf{V}(I))$. If the polynomial $f \in \sqrt{I}$, then $f^m \in I$ for some $m \geq 1$. Since $f^m \in I$ this implies that f^m vanishes on $\mathbf{V}(I)$. Now let $(a_1, a_2, \ldots, a_n)$ be an arbitrary element of $\mathbf{V}(I)$. Taking $f^m \in I$ and evaluating it at $(a_1, a_2, \ldots, a_n)$,

$$\begin{aligned} f^m(a_1, a_2, \ldots, a_n) &= 0 \text{ for all } (a_1, a_2, \ldots, a_n) \in V, \\ (f(a_1, a_2, \ldots, a_n))^m &= 0 \text{ since } f^m(a_1, a_2, \ldots, a_n) = (f(a_1, a_2, \ldots, a_n))^m. \end{aligned}$$

However, $(f(a_1, a_2, \ldots, a_n))^m$ can only equal zero when $f(a_1, a_2, \ldots, a_n) = 0$. In other words, the polynomial f will disappear when it is evaluated by any n-tuple from $\mathbf{V}$. Consequently, this makes $f \in \mathbf{I}(\mathbf{V}(I))$ and $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$.

We will finish this proof by showing that $\mathbf{I}(\mathbf{V}(I)) \subset \sqrt{I}$. Let $f \in \mathbf{I}(\mathbf{V}(I))$. This implies that $f(a_1, a_2, \ldots, a_n) = 0$ for $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. From Hilbert's Nullstellensatz since k is an algebraically closed field and $f \in \mathbf{I}(\mathbf{V}(I))$, then there exists an integer $m \geq 1$ such that $f^m \in I$. Hence, $f \in \sqrt{I}$ and $\mathbf{I}(\mathbf{V}(I)) \subset \sqrt{I}$. □

Theorem 4.10 (The Ideal-Variety Correspondence). *Let k be an arbitrary field.*

(i) *The maps*

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

and

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

are inclusion-reversing, i.e., if $I_1 \subset I_2$ are ideals, then $\mathbf{V}(I_1) \supset \mathbf{V}(I_2)$ and, similarly, if $V_1 \subset V_2$ are varieties, then $\mathbf{I}(V_1) \supset \mathbf{I}(V_2)$. Furthermore, for any variety V, we have

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

so that $\mathbf{I}$ is always one-to-one. Note that $\mathbf{I}(\mathbf{V}(I)) \neq I$.

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

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

and

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

are inclusion-reversing bijections which are inverses of each other. In other words, $\mathbf{I}(\mathbf{V}(I)) = I$ and $\mathbf{V}(\mathbf{I}(V)) = V$.

Proof. (i) It will be shown that both of the maps $\mathbf{V}$ and $\mathbf{I}$ are inclusion-reversing. We will start by looking at the map $\mathbf{V}$. If $I_1 \subset I_2$ are ideals, then $\mathbf{V}(I_2) \subset \mathbf{V}(I_1)$. Let $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I_2)$. If $f \in I_2$, then $f(a_1, a_2, \ldots, a_n) = 0$. We would like to show that $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I_1)$. Let the polynomial $f \in I_1$. Then $f \in I_2$ since the ideal

$I_1 \subset I_2$. Now that the polynomial f is also an element of I_2, then evaluating f by the n-tuple $(a_1, a_2, \ldots, a_n)$ results in $f(a_1, a_2, \ldots, a_n) = 0$. Thus, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I_1)$ and $\mathbf{V}(I_2) \subset \mathbf{V}(I_1)$.

Next, we turn our attention to the mapping I. If $V_1 \subset V_2$ are varieties, then $\mathbf{I}(V_2) \subset \mathbf{I}(V_1)$. Let $f \in \mathbf{I}(V_2)$. Then $f(a_1, a_2, \ldots, a_n) = 0$ for all $(a_1, a_2, \ldots, a_n) \in V_2$. In order to show that $f \in \mathbf{I}(V_1)$ then $f(a_1, a_2, \ldots, a_n) = 0$ for all $(a_1, a_2, \ldots, a_n) \in V_1$. Assume that the n-tuple $(a_1, a_2, \ldots, a_n) \in V_1$. Now $(a_1, a_2, \ldots, a_n) \in V_2$ because from our given $V_1 \subset V_2$. Consequently, $f(a_1, a_2, \ldots, a_n) = 0$ and $\mathbf{I}(V_2) \subset \mathbf{I}(V_1)$.

To finalize the proof of part (i), it will be shown that $\mathbf{V}(\mathbf{I}(V)) = V$ when $V = V(f_1, f_2, \ldots, f_s)$. Show that $V \subset \mathbf{V}(\mathbf{I}(V)$. Let $(a_1, a_2, \ldots, a_n) \in V$. Then for a polynomial $f \in \mathbf{I}(V)$, $f(a_1, a_2, \ldots, a_n) = 0$. Thus, $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(\mathbf{I}(V))$ because it is an n-tuple which makes a polynomial from $\mathbf{I}(V)$ zero. So the set V is contained in $\mathbf{V}(\mathbf{I}(V))$. To finish we will illustrate that $\mathbf{V}(\mathbf{I}(V)) \subset V$. Each of the polynomials $f_1, f_2, \ldots, f_s \in \mathbf{I}(V)$ since V contains the n-tuples that make those polynomials vanish. As a result, $\langle f_1, f_2, \ldots, f_s \rangle \subset \mathbf{I}(V)$. Furthermore, $\langle f_1, f_2, \ldots, f_s \rangle \subset \mathbf{I}(V)$ are two ideals so applying the map $\mathbf{V}$ we get $\mathbf{V}(\mathbf{I}(V)) \subset \mathbf{V}(\langle f_1, f_2, \ldots, f_s \rangle) = V$. The map $\mathbf{V}$ was shown to be inclusion-reversing. We have successfully proved that $\mathbf{V}(\mathbf{I}(V)) = V$ and I is one-to-one.

(ii) The ideal $\mathbf{I}(V)$ is a radical ideal. The map $\mathbf{I}$ takes an affine variety to a radical ideal. In part (i) of this proof it was shown that $\mathbf{V}(\mathbf{I}(V)) = V$. We must prove that $\mathbf{I}(\mathbf{V}(I)) = I$ when I is a radical ideal. Since k is an algebraically closed field, the strong Nullstellensatzs states that $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. When the ideal I is radical, then from Lemma 4.8 we know that $\sqrt{I} = I$. Combining this with the strong Nullstellensatz yields what we wanted to prove that $\mathbf{I}(\mathbf{V}(I)) = I$. It has clearly been shown that the maps $\mathbf{I}$ and $\mathbf{V}$ are inverses of one another. Consequently, both of the maps between radical ideals and varieties are one-to-one and onto. □

We will now turn our attention to the radical membership problem. If we are given that the polynomial $f \in k[x_1, x_2, \ldots, x_n]$, is there an algorithm that will determine whether $f \in \sqrt{I}$? In order for f to be an element of the radical of I, f^m must be in the ideal I for some $m \geq 1$. At this point we would have to check if $f^m \in I$ for each $m > 0$ and stop when we find such an m. Unfortunately, this method is inefficient because the power of m that will make $f^m \in I$ may be ridiculously large. Furthermore, there is also the chance that $f \notin \sqrt{I}$ which is information that this algorithm would not provide. However, it is possible to find an algorithm to see if $f \in \sqrt{I}$ by using the proof of Hilbert's Nullstellensatz (Theorem 4.3).

Proposition 4.11 (Radical Membership). *Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y]$ (in which case, $\tilde{I} = k[x_1, \ldots, x_n, y]$.)*

Proof. Suppose $1 \in \tilde{I}$. Referring back to the proof of Theorem 4.3 it was shown that when $1 \in \tilde{I}$, then $f^m \in I$ for some integer $m \geq 1$. So now the polynomial $f \in \sqrt{I}$. For the second part of this proof assume that $f \in \sqrt{I}$. This assumption implies that $f^m \in I$ for some $m \geq 1$. Thus, $f^m \in \tilde{I}$ since $I \subset \tilde{I}$. Furthermore, $1 - yf$ is also an element of the ideal $\tilde{I}$. We can write the element 1 in the following manner, $1 = y^m f^m + (1 - y^m f^m)$. The term $y^m f^m \in \tilde{I}$ since $y^m \in k[x_1, \ldots, x_n, y]$ and $f^m \in \tilde{I}$. We must show that the expression $1 - y^m f^m$ is also an element from $\tilde{I}$ so that $1 \in \tilde{I}$ by closure. This expression can be factored into $1 - y^m f^m = (1 - yf)(1 + yf + y^2 f^2 + \ldots + y^{m-2} f^{m-2} + y^{m-1} f^{m-1})$. Notice that $1 - yf \in \tilde{I}$ and $1 + yf + y^2 f^2 + \ldots + y^{m-2} f^{m-2} + y^{m-1} f^{m-1} \in k[x_1, \ldots, x_n, y]$ and so $1 - y^m f^m \in \tilde{I}$ since $\tilde{I}$ is an ideal. As a result, $1 \in \tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle$ and the proof is complete. □

4.3 Products of Ideals

In this section we turn our attention to operations on ideals. Since ideals are algebraic objects there exist algebraic operations that can be defined on them. There are three operations that can be performed on ideals: sum, product, and intersection. The operations on ideals are binary. In other words, if we take two given ideals and we find the sum, product, or intersection the result will be another ideal. However, for what we hope to achieve in this project the focus will mainly be on the product of ideals.

Definition 4.12. If I and J are two ideals in $k[x_1, x_2, \ldots, x_n]$, then their **product**, denoted $I \cdot J$, is defined to be the ideal generated by all polynomials $f \cdot g$ where $f \in I$ and $g \in J$. Thus, the product $I \cdot J$ of I and J is the set

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

Lemma 4.13. *If I and J are two ideals in $k[x_1, x_2, \ldots, x_n]$, then $I \cdot J = \{f_1g_1 + \ldots + f_rg_r \mid f_1, \ldots, f_r \in I, g_1, \ldots, g_r \in J\}$ is an ideal in $k[x_1, x_2, \ldots, x_n]$.*

Proof. We would like to show that the set $I \cdot J$ is an ideal. First, it must be shown that $0 \in I \cdot J$. Both I and J are ideals so $0 \in I$ and also $0 \in J$. Thus, $0 = 0 \cdot 0 \in I \cdot J$ because zero is a product of an element from I and an element from J. If $h_1 \in I \cdot J$ and $h_2 \in I \cdot J$, then the sum $h_1 + h_2 \in I \cdot J$. If $h_1 \in I \cdot J$, then $h_1 = f_1g_1 + f_2g_2 + \ldots + f_rg_r$ where $f_i \in I$ and $g_i \in J$ for $1 \leq i \leq r$. In addition, $h_2 \in I \cdot J$ means that $h_2 = f_1'g_1' + f_2'g_2' + \ldots + f_s'g_s'$ where $f_j' \in I$ and $g_j' \in J$ for $1 \leq j \leq s$. Looking at the sum of h_1 and h_2,

$$\begin{aligned} h_1 + h_2 &= (f_1g_1 + f_2g_2 + \ldots + f_rg_r) + (f_1'g_1' + f_2'g_2' + \ldots + f_s'g_s'), \\ &= f_1g_1 + f_2g_2 + \ldots + f_rg_r + f_1'g_1' + f_2'g_2' + \ldots + f_s'g_s'. \end{aligned}$$

The sum $h_1 + h_2$ is clearly an element of $I \cdot J$ because it satisfies Definition 4.12. Every term in the equation above is a product of an element from I and an element from the ideal J. Finally, if $p \in k[x_1, x_2, \ldots, x_n]$ and $f \in I \cdot J$, then $pf \in I \cdot J$. The polynomial $f \in I \cdot J$ implies that $f = f_1g_1 + f_2g_2 + \ldots + f_rg_r$ where $f_i \in I$ and $g_i \in J$. The product of f and p would now be

$$\begin{aligned} p \cdot f &= p(f_1g_1 + f_2g_2 + \ldots + f_rg_r), \\ &= pf_1g_1 + pf_2g_2 + \ldots + pf_rg_r, \\ &= (pf_1)g_1 + (pf_2)g_2 + \ldots + (pf_r)g_r. \end{aligned}$$

Notice that the product of pf_i for $1 \leq i \leq r$ in each term is an element of the ideal I because $p \in k[x_1, x_2, \ldots, x_n]$ and $f_i \in I$. Now the product of pf satisfies the conditions of Definition 4.12 because $pf_i \in I$ and $g_i \in J$ for $1 \leq i \leq r$. Consequently, $pf \in I \cdot J$ and the set $I \cdot J$ is an ideal. □

When the specific generators for two ideals I and J are not known, Definition 4.12 can be used to help us see how an element from the set $I \cdot J$ is written. However, the proposition that follows illustrates how to write polynomials from $I \cdot J$ when the generators for I and the generators for J are known.

Proposition 4.14. *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:*

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

Proof. We shall begin by showing that $I \cdot J \subset \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. From the previous definition an element from $I \cdot J$ has the form $m_1 n_1 + m_2 n_2 + \ldots + m_r n_r$ where $m_i \in I$ and $n_i \in J$ for $1 \leq i \leq r$. Since each $m_i \in I$ then $m_i = a_1 f_1 + a_2 f_2 + \ldots + a_r f_r$ with $a_i \in k[x_1, x_2, \ldots, x_n]$ and $f_1, f_2, \ldots, f_r \in I$. Similarly, every $n_i \in J$ so each of these polynomials can be rewritten as follows $n_i = b_1 g_1 + b_2 g_2 + \ldots + b_r g_r$ where $b_i \in k[x_1, x_2, \ldots, x_n]$ and $g_1, g_2, \ldots, g_r \in J$. Taking a closer look at each product of $m_i n_i$,

$$\begin{aligned} m_i n_i &= (a_1 f_1 + a_2 f_2 + \ldots + a_r f_r)(b_1 g_1 + b_2 g_2 + \ldots b_r g_r), \\ &= a_1 f_1 b_1 g_1 + a_1 f_1 b_2 g_2 + \ldots + a_1 f_1 b_r g_r + a_2 f_2 b_1 g_1 + a_2 f_2 b_2 g_2 + \ldots + a_2 f_2 b_r g_r \\ &\quad + \ldots + a_r f_r b_r g_r, \\ &= (a_1 b_1) f_1 g_1 + (a_1 b_2) f_1 g_2 + \ldots + (a_1 b_r) f_1 g_r + (a_2 b_1) f_2 g_1 + (a_2 b_2) f_2 g_2 + \ldots \\ &\quad + (a_2 b_r) f_2 g_r + \ldots + (a_r b_r) f_r g_r. \end{aligned}$$

For every term in the equation above $a_i b_j \in k[x_1, x_2, \ldots, x_n]$ by closure and $f_i \in I$ and $g_j \in J$. Thus, $I \cdot J \subset \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. This proof will be concluded by showing that $\langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle \subset I \cdot J$. Let w be an element from the ideal $\langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. Now, $w = \sum p_{ij} f_i g_j$ with the polynomials $p_{ij} \in k[x_1, x_2, \ldots, x_n]$. The terms in the summation are all products of elements from I and J since $p_{ij} f_i \in I$ and $g_j \in J$. As a result, $\langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle \subset I \cdot J$. We have successfully proven that $I \cdot J = \langle f_i g_j \mid 1 \leq i \leq r,\ 1 \leq j \leq s \rangle$. □

The next theorem will show that there exists a connection with the products of ideals and taking the union of varieties.

Theorem 4.15. *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. This proof will start by showing that $\mathbf{V}(I \cdot J) \subset \mathbf{V}(I) \cup \mathbf{V}(J)$. Suppose $x \in \mathbf{V}(I \cdot J)$. We must show that $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Since $x \in \mathbf{V}(I \cdot J)$, $p(x) = 0$ for all $p \in I \cdot J$. In particular, suppose $p = fg$ where $f \in I$ and $g \in J$. Evaluating the polynomial p by the n-tuple x we get $p(x) = (fg)(x) = f(x)g(x) = 0$. At this point we now come across two possible cases. First, in order for $p(x) = 0$, the equation above implies that $g(x) = 0$ for all $g \in J$ and $f(x)$ does not necessarily have to equal zero. This now means that $x \in \mathbf{V}(J)$ because it made all of the polynomials from the ideal J disappear. The second possibility is that $g(x) \neq 0$ for some $g \in J$. Examining the product of $p(x) = f(x)g(x) = 0$ once more, then $f(x)$ must equal zero for all $f \in I$ to maintain a zero result. Thus, $x \in \mathbf{V}(I)$.

It has been shown that $x \in \mathbf{V}(I)$ or $x \in \mathbf{V}(J)$ which is exactly what it means to be in $\mathbf{V}(I) \cup \mathbf{V}(J)$.

Next, we will illustrate that $\mathbf{V}(I) \cup \mathbf{V}(J) \subset \mathbf{V}(I \cdot J)$. Let $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Then we must show that $x \in \mathbf{V}(I \cdot J)$. In other words that $p(x) = 0$ for all $p \in I \cdot J$. If $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$, then $x \in \mathbf{V}(I)$ or $x \in \mathbf{V}(J)$. By Definition 4.12, the polynomial $p \in I \cdot J$ can be written as follows $p = f_1g_1 + f_2g_2 + \ldots + f_rg_r$ where $f_i \in I$ and $g_i \in J$. When $x \in \mathbf{V}(I)$ any polynomial from I evaluated at x will vanish. Therefore, substituting x into p,

$$\begin{aligned} p(x) &= (f_1g_1)(x) + (f_2g_2)(x) + \ldots + (f_rg_r)(x), \\ &= f_1(x)g_1(x) + f_2(x)g_2(x) + \ldots + f_r(x)g_r(x), \\ &= 0 \cdot g_1(x) + 0 \cdot g_2(x) + \ldots + 0 \cdot g_r(x), \\ &= 0. \end{aligned}$$

Likewise, $x \in \mathbf{V}(J)$ makes all of the polynomials belonging to J disappear. In the equations above all the polynomials $g_j \in J$ evaluated at x would all equal zero. Once again this makes $p(x) = 0$. Thus, evaluating any polynomial p from $I \cdot J$ by x yields a product of zero. As a result, $x \in \mathbf{V}(I \cdot J)$, $\mathbf{V}(I) \cup \mathbf{V}(J) \subset \mathbf{V}(I \cdot J)$, and finally $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J)$. □

4.4 Irreducible Varieties and Prime Ideals

When affine varieties were introduced in Section 2.2, it was shown that the union of two varieties is a variety. Furthermore, this finding was extended to the union of a finite number of varieties. We proved by induction on n, the number of finite varieties, that the union of $V_1 \cup V_2 \cup \ldots \cup V_n$ is also a variety. In abstract algebra the topic of irreducible elements was studied by looking at polynomials. Let $k[x]$ represent the ring of polynomials whose coefficients are from the field k. A polynomial $p \in k[x]$ is called irreducible over k if it is non-constant and cannot be factored into the product of two or more non-constant polynomials from the ring $k[x]$. For this project we need to apply this algebraic concept to affine varieties which are geometric objects. Irreducible varieties will be defined below.

Definition 4.16. An affine variety $V \subset k^n$ 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 will also reexamine and define algebraic concepts that have been studied in polynomial rings of a single variable to rings involving multivariable polynomials.

Definition 4.17. An ideal $I \subset k[x_1, x_2, \ldots, x_n]$ 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 $g \in I$.

The following theorem will prove that there exists a connection between irreducible varieties and prime ideals.

Proposition 4.18. *Let $V \subset k^n$ be an affine variety. Then V is irreducible if and only if $\mathbf{I}(V)$ is a prime ideal.*

Proof. Assume V is irreducible and $fg \in \mathbf{I}(V)$. We want to show that $\mathbf{I}(V)$ is a prime ideal. In other words that $f \in \mathbf{I}(V)$ or $g \in \mathbf{I}(V)$. Suppose that $V_1 = V \cap V(f)$ and $V_2 = V \cap V(g)$. The sets V_1 and V_2 are varieties because we know from Lemma 2.6 that the intersection of two varieties is a variety. Now, $V = V_1 \cup V_2$. Since V is irreducible by definition $V = V_1$ or $V = V_2$. If $V = V_1$, then $V = V_1 = V \cap V(f)$. This now implies that $f(x) = 0$ for all $x \in V$. Since f disappears when it is evaluated by all of the elements in V then $f \in \mathbf{I}(V)$. Similarly, if $V = V_2$, then $V = V_2 = V \cap V(g)$. This now implies that $g(x) = 0$ for all $x \in V$. Thus, in this case the polynomial g is an element of $\mathbf{I}(V)$. Since it has been shown that $f \in \mathbf{I}(V)$ or $g \in \mathbf{I}(V)$, we can conclude that $\mathbf{I}(V)$ is a prime ideal when V is irreducible.

To conclude, we will now prove that when $\mathbf{I}(V)$ is a prime ideal the variety V is irreducible. Let $V = V_1 \cup V_2$ and $V \neq V_1$. In order to show that $V = V_2$ we must have $\mathbf{I}(V) = \mathbf{I}(V_2)$. From our assumption, $V = V_1 \cup V_2$ implies that $V_2 \subset V$. Since $V_2 \subset V$ then $\mathbf{I}(V) \subset \mathbf{I}(V_2)$ by the Ideal-Variety Correspondence. We now turn our attention to the other inclusion $\mathbf{I}(V_2) \subset \mathbf{I}(V)$. We assumed that $V \neq V_1$ hence $V_1 \subsetneq V$ and $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$. So there exists a polynomial $f \in \mathbf{I}(V_1)$ such that $f \notin \mathbf{I}(V)$. Pick $f \in \mathbf{I}(V_1) - \mathbf{I}(V)$. Let $g \in \mathbf{I}(V_2)$. To demonstrate that $g \in \mathbf{I}(V)$ we want $fg \in \mathbf{I}(V)$. In other words, $(fg)(a) = 0$ for all $a \in V$. If the element $a \in V$, then $a \in V_1 \cup V_2$ because $V = V_1 \cup V_2$. Due to the fact that $a \in V_1 \cup V_2$ there are two possibilities, either $a \in V_1$ or $a \in V_2$. When $a \in V_1$, then $f(a) = 0$ since $f \in \mathbf{I}(V_1)$. Consequently, $(fg)(a) = f(a)g(a) = 0 \cdot g(a) = 0$. On the other hand, when $a \in V_2$ then $g(a) = 0$ since $g \in \mathbf{I}(V_2)$. So the product of

$(fg)(a) = f(a)g(a) = f(a) \cdot 0 = 0$. Notice that evaluating fg by all of the elements from the variety V results in a product of zero. Thus, $fg \in \mathbf{I}(V)$. By combining our initial assumption that the ideal $\mathbf{I}(V)$ is prime and $fg \in \mathbf{I}(V)$ then $f \in \mathbf{I}(V)$ or $g \in \mathbf{I}(V)$. However, $f \notin \mathbf{I}(V)$ implies that $g \in \mathbf{I}(V)$. Since $g \in \mathbf{I}(V_2)$ and $g \in \mathbf{I}(V)$ then $\mathbf{I}(V_2) \subset \mathbf{I}(V)$. It has successfully been shown that $\mathbf{I}(V_2) \subset \mathbf{I}(V)$ and $\mathbf{I}(V) \subset \mathbf{I}(V_2)$ so we can conclude that $\mathbf{I}(V_2) = \mathbf{I}(V)$. It was previously established that the map $\mathbf{I}$ is one-to-one so $V = V_2$ and finally V is an irreducible variety. □

Proposition 4.19. *Every prime ideal is radical.*

Proof. Given that $I \subset k[x_1, x_2, \ldots, x_n]$ is a prime ideal we want to prove that I is radical. In other words, we must show that if $f^m \in I$ for some $m \geq 1$, then $f \in I$. This will be proven by induction on finite products. In the case when $m = 2$, suppose we have $f^2 = f \cdot f \in I$. Since I is prime, by Definition 4.17 this makes $f \in I$. Next, we will assume that when $f^m \in I$ for some $m \geq 1$, then $f \in I$. If $f^{m+1} \in I$, then $f^{m+1} = f^m \cdot f \in I$. Again, because I is prime this implies that $f^m \in I$ or $f \in I$. From the previous assumption, when $f^m \in I$, then $f \in I$. If $f^m \notin I$, this implies that $f \in I$. In either case, $f \in I$. As a result, I is a radical ideal. □

Now that we know that every prime ideal is a radical ideal we can combine this fact with the ideal variety correspondence to get the following corollary.

Corollary 4.20. *When k is algebraically closed, the functions* $\mathbf{V}$ *and* $\mathbf{I}$ *induce a one-to-one correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, x_2, \ldots, x_n]$.*

Some other concepts covered in abstract algebra will be defined next.

Definition 4.21. An ideal $I \subset k[x_1, x_2, \ldots, x_n]$ is said to be **maximal** if $I \neq k[x_1, x_2, \ldots, x_n]$ and any ideal J containing I is such that either $J = I$ or $J = k[x_1, x_2, \ldots, x_n]$.

Definition 4.22. An ideal $I \subset k[x_1, x_2, \ldots, x_n]$ is called **proper** if I is not equal to $k[x_1, x_2, \ldots, x_n]$.

Therefore, an ideal that is maximal is also proper. We will now show that an ideal of the form $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ is maximal.

Proposition 4.23. *If k is any field, an ideal $I \subset [x_1, x_2, \ldots, x_n]$ of the form $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$, where $a_1, \ldots, a_n \in k$, is maximal.*

Proof. In order to show that $I = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n\rangle$ is a maximal ideal we must show that $I \neq k[x_1, x_2, \ldots, x_n]$ and any ideal J containing I is such that $J = I$ or $J = k[x_1, x_2, \ldots, x_n]$. Let $I \subsetneq J$. Then we can find a polynomial f such that $f \in J$ but $f \notin I$. Using the division algorithm f can be written in the following form $f = A_1(x_1 - a_1) + A_2(x_2 - a_2) + \ldots + A_n(x_n - a_n) + b$ where $b \in k$. Notice that in the previous equation $A_1(x_1 - a_1) + A_2(x_2 - a_2) + \ldots + A_n(x_n - a_n) \in I$. However, we know that since $f \notin I$ the remainder b cannot equal zero. If the remainder is zero, this would make $f \in I$ which contradicts our original assumption about f. Furthermore, $A_1(x_1 - a_1) + A_2(x_2 - a_2) + \ldots + A_n(x_n - a_n) \in I$ implies that $A_1(x_1 - a_1) + A_2(x_2 - a_2) + \ldots + A_n(x_n - a_n) \in J$ because $I \subsetneq J$. Since $f \in J$ rewriting the equation for f above yields $b = f - (A_1(x_1 - a_1) + A_2(x_2 - a_2) + \ldots + A_n(x_n - a_n))$. Now $b \in J$ by closure since J is an ideal. The element $b \in J$ has a multiplicative inverse since $b \neq 0$ and $b \in k$ where k is a field. Thus, $b \cdot \frac{1}{b} = 1 \in J$. Now that 1 is in the ideal J this implies that $J = k[x_1, x_2, \ldots, x_n]$. Therefore, $I = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n\rangle$ is a maximal ideal. □

Proposition 4.24. *If k is any field, a maximal ideal in $k[x_1, x_2, \ldots, x_n]$ is prime.*

Proof. Suppose I is a maximal ideal which is not prime. Let $fg \in I$ where $f \notin I$ and $g \notin I$. Since I is maximal, then the ideal $\langle f\rangle + I = I$ or $\langle f\rangle + I = k[x_1, x_2, \ldots, x_n]$. Assume $\langle f\rangle + I = k[x_1, x_2, \ldots, x_n]$. If $\langle f\rangle + I = k[x_1, x_2, \ldots, x_n]$, then $1 \in \langle f\rangle + I$. Now, $1 = cf + h$ where $c \in k[x_1, x_2, \ldots, x_n]$ and $h \in I$. Multiplying $1 = cf + h$ through by g we get the equation $g = cfg + hg$. Notice that the term $cfg \in I$ because $c \in k[x_1, x_2, \ldots, x_n]$, $fg \in I$, and I is an ideal. In addition, $hg \in I$ because $h \in I$ and $g \in k[x_1, x_2, \ldots, x_n]$. Thus, by closure $g \in I$. However, this is a contradiction to our assumption $g \notin I$. Therefore, $1 \notin \langle f\rangle + I$ so $\langle f\rangle + I \neq k[x_1, x_2, \ldots, x_n]$. Also, if $\langle f\rangle + I = I$, then $f \in I$, a contradiction. As a result, I must be prime. □

Theorem 4.25. *If k is an algebraically closed field, then every maximal ideal of $k[x_1, x_2, \ldots, x_n]$ is of the form $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ for some $a_1, \ldots, a_n \in k$.*

Proof. Suppose $I \subset k[x_1, x_2, \ldots, x_n]$ is a maximal ideal. Since I is maximal we know that $I \neq k[x_1, x_2, \ldots, x_n]$. From the Weak Nullstellensatz when k is an algebraically closed field and $\mathbf{V}(I) = \emptyset$, then $I = k[x_1, x_2, \ldots, x_n]$. So because I is not the entire polynomial ring $\mathbf{V}(I) \neq \emptyset$. The variety of I is not empty so there exists an n-tuple

$(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$. Thus, every $f \in I$ evaluated at $(a_1, a_2, \ldots, a_n)$ will be zero. This will make all of these polynomials elements of $\mathbf{I}(\{(a_1, a_2, \ldots, a_n)\})$. It has been shown that when $f \in I$, then $f \in \mathbf{I}(\{(a_1, a_2, \ldots, a_n)\})$. So the ideal $I \subset \mathbf{I}(\{(a_1, a_2, \ldots, a_n)\})$. We will show that $\mathbf{I}(\{(a_1, a_2, \ldots, a_n)\}) = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. First, we will look at $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle \subset \mathbf{I}(\{(a_1, a_2, \ldots, a_n)\})$. Let $f \in \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. Then $f(x_1, x_2, \ldots, x_n) = p_1(x_1 - a_1) + p_2(x_2 - a_2) + \ldots + p_n(x_n - a_n)$ where $p_i \in k[x_1, x_2, \ldots, x_n]$ for $1 \leq i \leq n$. Evaluating the polynomial f by the n-tuple $(a_1, a_2, \ldots, a_n)$ results in

$$\begin{aligned} f(a_1, a_2, \ldots, a_n) &= p_1(a_1 - a_1) + p_2(a_2 - a_2) + \ldots + p_n(a_n - a_n), \\ &= p_1 \cdot 0 + p_2 \cdot 0 + \ldots + p_n \cdot 0, \\ &= 0. \end{aligned}$$

Thus, f vanishes on $(a_1, a_2, \ldots, a_n)$. So $f \in \mathbf{I}(\{(a_1, a_2, \ldots, a_n)\})$. Next, it will be shown that $\mathbf{I}(\{(a_1, a_2, \ldots, a_n)\}) \subset \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. Suppose $f \in \mathbf{I}(\{(a_1, a_2, \ldots, a_n)\})$. This implies that $f(a_1, a_2, \ldots, a_n) = 0$. Now using the division algorithm, $f(x_1, \ldots, x_n) = (x_1 - a_1)g_1 + (x_2 - a_2)g_2 + \ldots + (x_n - a_n)g_n + r$ where $r \in k$. We would like to show that $r = 0$. Using the fact that $f(a_1, a_2, \ldots, a_n) = 0$ then

$$\begin{aligned} 0 &= f(a_1, a_2, \ldots, a_n), \\ 0 &= (a_1 - a_1)g_1 + (a_2 - a_2)g_2 + \ldots + (a_n - a_n)g_n + r, \\ 0 &= 0 \cdot g_1 + 0 \cdot g_2 + \ldots + 0 \cdot g_n + r, \\ 0 &= r. \end{aligned}$$

Therefore, $f \in \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$ so $\mathbf{I}(\{(a_1, a_2, \ldots, a_n)\}) \subset \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. We have proven that $\mathbf{I}(\{(a_1, a_2, \ldots, a_n)\}) = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. The statement $I \subset \mathbf{I}(\{(a_1, a_2, \ldots, a_n)\})$ can be rewritten as follows $I \subset \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. Furthermore, by Proposition 4.23, an ideal of the form $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$ is maximal. In other words, $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$ is proper. So $I \subset \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle \neq k[x_1, x_2, \ldots, x_n]$. The ideal I is also maximal so this implies that $I = \langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$. □

Chapter 5

Application of The Groebner Basis Algorithm

Throughout the first four chapters of this project much time was spent covering a variety of concepts that are critical to our understanding of the Groebner Basis Algorithm. We first looked at defining polynomials from the ring $k[x_1, x_2, \ldots, x_n]$. Next, affine varieties were introduced. Once the definition of an affine variety was presented, two operations that can be applied to them were examined. It is possible to take the union and the intersection of a finite number of varieties. From algebra the concept of ideals (prime, maximal, and radical) is thoroughly studied as well. When the necessary concepts from geometry and algebra were properly discussed, the focus turned to establish a connection between affine varieties and ideals that is one-to-one and onto. Without this mapping it would not be possible to prove geometric theorems using the Groebner Basis Algorithm which is an algebraic approach. In this chapter, two applications of the Groebner Basis Algorithm will be presented. The following proposition will be an important step in the Groebner Basis Algorithm.

Proposition 5.1. *Suppose $h_1, h_2, \ldots, h_n, g \in k[x_1, x_2, \ldots, x_t]$. If $g \in \sqrt{\langle h_1, h_2, \ldots, h_n \rangle}$, then $g \in \mathbf{I}(V)$ i.e. if $h_i(a_1, a_2, \ldots, a_t) = 0$ for $1 \leq i \leq n$, then $g(a_1, a_2, \ldots, a_t) = 0$.*

Proof. Let $g \in \sqrt{\langle h_1, h_2, \ldots, h_n \rangle}$ and $h_i(a_1, a_2, \ldots, a_t) = 0$ for $1 \leq i \leq n$. When $g \in \sqrt{\langle h_1, h_2, \ldots, h_n \rangle}$, then $g^s \in \langle h_1, h_2, \ldots, h_n \rangle$ for some $s \geq 1$. So $g^s \in \langle h_1, h_2, \ldots, h_n \rangle$ implies that $g^s = (p_1 h_1 + p_2 h_2 + \ldots + p_n h_n)^s$ where $p_1, p_2, \ldots, p_n \in k[x_1, x_2, \ldots, x_t]$.

Substituting $(a_1, a_2, \ldots, a_t)$ into g^s,

$$\begin{aligned} g^s(a_1, \ldots, a_t) &= (p_1(a_1, \ldots, a_t)h_1(a_1, \ldots, a_t) + p_2(a_1, \ldots, a_t)h_2(a_1, \ldots, a_t) \\ &\quad + \ldots + p_n(a_1, \ldots, a_t)h_n(a_1, \ldots, a_t))^s, \\ &= (p_1(a_1, \ldots, a_t) \cdot 0 + p_2(a_1, \ldots, a_t) \cdot 0 + \ldots + p_n(a_1, \ldots, a_t) \cdot 0)^s, \\ &= 0. \end{aligned}$$

In other words, a power of g vanishes when it is evaluated by $(a_1, a_2, \ldots, a_t)$. However, g^s can only disappear at $(a_1, a_2, \ldots, a_t)$ when $g(a_1, a_2, \ldots, a_t) = 0$. Since the polynomial g is a linear combination of the h_i's, then g will vanish at the same values as the h_i. Hence, g follows from $h_1, h_2, \ldots, h_n$. □

5.1 Problem 1: Diagonals of a Parallelogram

In this section, we shall begin by proving the following theorem using the Groebner basis technique.

Theorem 5.2. *Two diagonals of any parallelogram intersect at a point which bisects both of the diagonals.*

In this problem, we will show that the hypothesis and the conclusion of the theorem above can be written as polynomials by using Cartesian coordinates. The parallelogram can be placed anywhere in the plane or we can choose to place the parallelogram at coordinates that will make it easier to work with. To begin this problem, we will place the vertex A of the parallelogram at the origin $(0,0)$. The second vertex of the parallelogram B will be placed randomly on the x-axis and it will have coordinates $(u_1, 0)$. The third vertex of the parallelogram C can be placed anywhere in the plane and it will have coordinates (u_2, u_3). However, $u_3 \neq 0$ because there would be no parallelogram if the third vertex was on the side $\overline{AB}$. The coordinates for the final vertex D (x_1, x_2) are determined by the placement of vertices A, B, and C. The intersection of the diagonals $\overline{AD}$ and $\overline{BC}$ will be labeled N and have coordinates (x_3, x_4). The parallelogram we have constructed is pictured below.

The hypothesis of Theorem 5.1 is that $ABCD$ is a parallelogram with diagonals $\overline{AD}$ and $\overline{BC}$. We will next convert this hypothesis into polynomials (labeled h_i) using

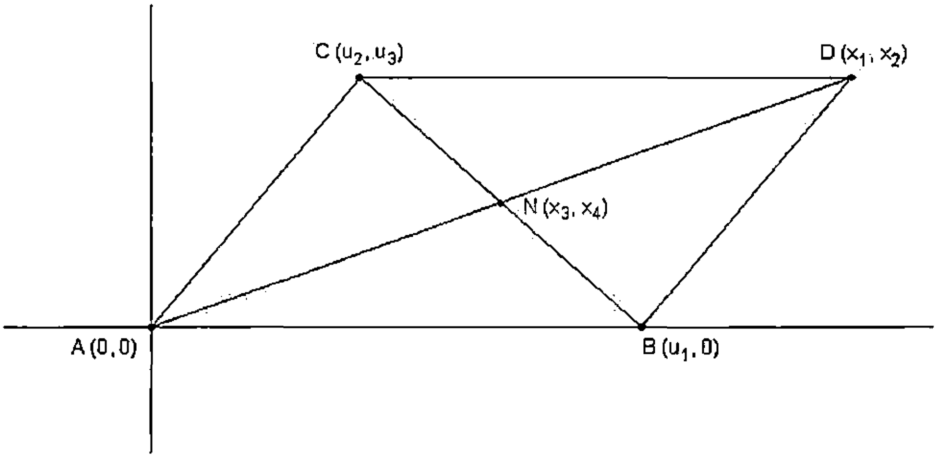

Figure 5.1: Parallelogram $ABCD$ in the Cartesian plane.

the above picture. The figure $ABCD$ is a parallelogram implies that $\overline{AB} \parallel \overline{CD}$ and $\overline{AC} \parallel \overline{BD}$. Also, $\overline{AB} = \overline{CD}$ and $\overline{AC} = \overline{BD}$.

$\overline{AB} \parallel \overline{CD}$ means that the slope of $\overline{AB}$ = the slope of $\overline{CD}$, so

$$\begin{aligned}
\frac{0-0}{u_1-0} &= \frac{x_2-u_3}{x_1-u_2} \\
0 &= \frac{x_2-u_3}{x_1-u_2} \\
x_2-u_3 &= 0.
\end{aligned}$$

Now let $h_1 = x_2 - u_3$.
$\overline{AC} \parallel \overline{BD}$ means that the slope of $\overline{AC}$ = the slope of $\overline{BD}$, so

$$\begin{aligned}
\frac{u_3-0}{u_2-0} &= \frac{x_2-0}{x_1-u_1} \\
\frac{u_3}{u_2} &= \frac{x_2}{x_1-u_1} \\
\frac{u_3}{u_2} - \frac{x_2}{x_1-u_1} &= 0 \\
u_3(x_1-u_1) - x_2u_2 &= 0.
\end{aligned}$$

Therefore, let $h_2 = u_3(x_1 - u_1) - x_2u_2$.
If N is the intersection of the diagonals, then N lies on $\overline{AD}$ and $\overline{BC}$. We can conclude

that the points A, D, and N are collinear so the slope of $\overline{AN}$ = the slope of $\overline{AD}$, so

$$\begin{aligned}
\frac{x_4-0}{x_3-0} &= \frac{u_3-0}{x_1-0} \\
\frac{x_4}{x_3} &= \frac{u_3}{x_1} \\
\frac{x_4}{x_3}-\frac{u_3}{x_1} &= 0 \\
x_1x_4 - x_3u_3 &= 0.
\end{aligned}$$

Then let $h_3 = x_1x_4 - x_3u_3$.

Similarly, the points B, C, and N are also collinear so the slope of $\overline{BN}$ = the slope of $\overline{BC}$, so

$$\begin{aligned}
\frac{0-x_4}{u_1-x_3} &= \frac{0-u_3}{u_1-u_2} \\
\frac{-x_4}{u_1-x_3} &= \frac{-u_3}{u_1-u_2} \\
\frac{x_4}{u_1-x_3}-\frac{u_3}{u_1-u_2} &= 0 \\
x_4(u_1-u_2)-u_3(u_1-x_3) &= 0.
\end{aligned}$$

Hence, let $h_4 = x_4(u_1-u_2) - u_3(u_1-x_3)$.

From the computations above we get four algebraic hypotheses: $h_1 = 0$, $h_2 = 0$, $h_3 = 0$, and $h_4 = 0$. The conclusion of this problem is that the point N bisects the diagonals of the parallelogram $ABCD$. In other words, $\overline{AN} = \overline{ND}$ and $\overline{BN} = \overline{NC}$. Both of these statements can be converted into polynomials (labeled g_i) by using the distance formula as follows

$$\begin{aligned}
\overline{AN} &= \overline{ND} \\
\sqrt{(x_4-0)^2+(x_3-0)^2} &= \sqrt{(u_3-x_4)^2+(x_1-x_3)^2} \\
\sqrt{x_4{}^2+x_3{}^2} &= \sqrt{(u_3-x_4)^2+(x_1-x_3)^2} \\
x_4{}^2+x_3{}^2 &= (u_3-x_4)^2+(x_1-x_3)^2 \\
x_4{}^2+x_3{}^2 &= x_2{}^2-2x_2x_4+x_4{}^2+x_1{}^2-2x_1x_3+x_3{}^2 \\
x_2{}^2-2x_2x_4+x_1{}^2-2x_1x_3 &= 0
\end{aligned}$$

and

$$\begin{aligned}
\overline{BN} &= \overline{NC} \\
\sqrt{(0-x_4)^2+(u_1-x_3)^2} &= \sqrt{(x_4-u_3)^2+(x_3-u_2)^2} \\
\sqrt{{x_4}^2+(u_1-x_3)^2} &= \sqrt{(x_4-u_3)^2+(x_3-u_2)^2} \\
{x_4}^2+(u_1-x_3)^2 &= (x_4-u_3)^2+(x_3-u_2)^2 \\
{x_4}^2+{u_1}^2-2u_1x_3+{x_3}^2 &= {x_4}^2-2u_3x_4+{u_3}^2+{x_3}^2-2x_3u_2+{u_2}^2 \\
-{u_1}^2+2u_1x_3-2u_3x_4+{u_3}^2-2x_3u_2+{u_2}^2 &= 0.
\end{aligned}$$

We get the following two polynomials $g_1 = {x_2}^2 - 2x_2x_4 + {x_1}^2 - 2x_1x_3$ and $g_2 = -{u_1}^2 + 2u_1x_3 - 2u_3x_4 + {u_3}^2 - 2x_3u_2 + {u_2}^2$. Our next step is to show that the conclusions $g_i = 0$ hold when the hypotheses $h_i = 0$ holds. We have a variety $V = V(h_1, h_2, h_3, h_4)$. We want to show that g_i vanishes for the same values as h_1, h_2, h_3, and h_4.

Let $I = \langle h_1, h_2, h_3, h_4\rangle$. According to the Groebner basis technique, we can use the radical membership test to determine whether $g_1 \in \sqrt{\langle h_1, h_2, h_3, h_4\rangle}$. The conclusion will follow from h_1, h_2, h_3, and h_4 if $1 \in \tilde{I} = \langle h_1, h_2, h_3, h_4, 1 - yg_1\rangle$. Unfortunately, computing a Groebner basis with Maple for $\langle h_1, h_2, h_3, h_4, 1 - yg_1\rangle$ did not result in a basis of $\{1\}$. This is a major problem because using Euclidean geometry it can be easily shown that this theorem is true. Since figure $ABCD$ is a parallelogram $\overline{AB} \parallel \overline{CD}$. Also, $\overline{AB} = \overline{CD}$ because the parallel sides in a parallelogram have equal length. Now, $\angle BAN \cong \angle NDC$ because when parallel lines are cut by a transversal alternate interior angles are congruent. Likewise, $\angle NBA \cong \angle NCD$ because they are also alternate interior angles. Consequently, $\triangle ANB \cong \triangle DNC$ by ASA. As a result, this makes $\overline{AN} = \overline{ND}$ and $\overline{BN} = \overline{NC}$ since corresponding parts of congruent figures are congruent. To see why the radical membership test failed, a Groebner basis will be computed for I in $\mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$ using lex order where $x_1 > x_2 > x_3 > x_4 > u_1 > u_2 > u_3$. With the help of Maple, the polynomials computed for the Groebner basis of $\langle h_1, h_2, h_3, h_4\rangle$ are listed below

$$\begin{aligned}
f_1 &= x_1x_4 + x_4u_1 - x_4u_2 - u_1u_3,\\
f_2 &= x_1u_3 - u_1u_3 - u_2u_3,\\
f_3 &= x_2 - u_3,\\
f_4 &= x_3u_3 + x_4u_1 - x_4u_2 - u_1u_3,\\
f_5 &= x_4u_1^2 - x_4u_1u_2 - \frac{1}{2}u_1^2u_3 + \frac{1}{2}u_1u_2u_3,\\
f_6 &= x_4u_1u_3 - \frac{1}{2}u_1u_3^2.
\end{aligned}$$

Since $\langle h_1, h_2, h_3, h_4\rangle = \langle f_1, f_2, f_3, f_4, f_5, f_6\rangle$ by Proposition 2.10 then $V(h_1, h_2, h_3, h_4) = V(f_1, f_2, f_3, f_4, f_5, f_6)$. However, the variety $V(f_1, f_2, f_3, f_4, f_5, f_6)$ can be decomposed further because the polynomial $f_2 = x_1u_3 - u_1u_3 - u_2u_3 = (x_1 - u_1 - u_2)u_3$ is factorable. So the variety

$$\begin{aligned}
V &= V(h_1, h_2, h_3, h_4),\\
&= V(f_1, (x_1 - u_1 - u_2)u_3, f_3, f_4, f_5, f_6),\\
&= V(f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6) \cup V(f_1, u_3, f_3, f_4, f_5, f_6).
\end{aligned}$$

Now computing the Groebner Basis for $V(f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6)$ results in

$$\begin{aligned}
p_1 &= x_1 - u_1 - u_2,\\
p_2 &= x_2 - u_3,\\
p_3 &= 2x_3u_3 - 2x_4u_2 - u_1u_3 = x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3,\\
p_4 &= 2x_4u_1 - u_1u_3 = x_4u_1 - \frac{1}{2}u_1u_3.
\end{aligned}$$

Computing the Groebner Basis for $V(f_1, u_3, f_3, f_4, f_5, f_6)$ yields

$$\begin{aligned}
o_1 &= x_1x_4,\\
o_2 &= x_2,\\
o_3 &= x_4u_1 - x_4u_2,\\
o_4 &= u_3.
\end{aligned}$$

So,

$$\begin{aligned} V &= V(f_1, x_1 - u_1 - u_2, f_3, f_4, f_5, f_6) \cup V(f_1, u_3, f_3, f_4, f_5, f_6), \\ &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4u_1 - \frac{1}{2}u_1u_3) \cup \\ &\quad V(x_1x_4, x_2, x_4u_1 - x_4u_2, u_3). \end{aligned}$$

The variety $V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4u_1 - \frac{1}{2}u_1u_3)$ is reducible since $x_4u_1 - \frac{1}{2}u_1u_3 = (x_4 - \frac{1}{2}u_3)u_1$. Continuing from before,

$$\begin{aligned} V &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4u_1 - \frac{1}{2}u_1u_3) \cup \\ &\quad V(x_1x_4, x_2, x_4u_1 - x_4u_2, u_3), \\ &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4 - \frac{1}{2}u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1) \cup \\ &\quad V(x_1x_4, x_2, x_4u_1 - x_4u_2, u_3). \end{aligned}$$

Furthermore, in $V(x_1x_4, x_2, x_4u_1 - x_4u_2, u_3)$ the product of x_1x_4 can be split into $V(x_1, x_2, x_4u_1 - x_4u_2, u_3) \cup V(x_4, x_2, x_4u_1 - x_4u_2, u_3)$. So,

$$\begin{aligned} V &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4 - \frac{1}{2}u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1) \cup \\ &\quad V(x_1x_4, x_2, x_4u_1 - x_4u_2, u_3), \\ &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4 - \frac{1}{2}u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1) \cup \\ &\quad V(x_1, x_2, x_4u_1 - x_4u_2, u_3) \cup V(x_4, x_2, x_4u_1 - x_4u_2, u_3). \end{aligned}$$

Notice also that for the last two varieties above $x_4u_1 - x_4u_2 = (u_1 - u_2)x_4$ is factorable so that,

$$\begin{aligned} V &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4 - \frac{1}{2}u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1) \cup \\ &\quad V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_1, x_2, x_4, u_3) \cup \\ &\quad V(x_2, x_4, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3). \end{aligned}$$

Also, we can make an important observation about the ideals $\langle x_1, x_2, x_4, u_3\rangle$, $\langle x_2, x_4, u_1 - u_2, u_3\rangle$ and $\langle x_2, x_4, u_3\rangle$. In particular, $\langle x_2, x_4, u_3\rangle \subset \langle x_1, x_2, x_4, u_3\rangle$ so by the Ideal-Variety Correspondence $V(x_1, x_2, x_4, u_3) \subset V(x_2, x_4, u_3)$. In addition, $\langle x_2, x_4, u_3\rangle \subset \langle x_2, x_4, u_1 - u_2, u_3\rangle$, then $V(x_2, x_4, u_1 - u_2, u_3) \subset V(x_2, x_4, u_3)$. The variety V can be rewritten as follows,

$$\begin{aligned} V &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4 - \frac{1}{2}u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1) \cup \\ &\quad V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3). \end{aligned}$$

Computing the Groebner basis for $V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, x_4 - \frac{1}{2}u_3)$ leads to the following polynomials

$$\begin{aligned} q_1 &= x_1 - u_1 - u_2, \\ q_2 &= x_2 - u_3, \\ q_3 &= 2x_3u_3 - u_1u_3 - u_2u_3 = x_3u_3 - \frac{1}{2}u_1u_3 - \frac{1}{2}u_2u_3, \\ q_4 &= 2x_4 - u_3 = x_4 - \frac{1}{2}u_3. \end{aligned}$$

Now,

$$\begin{aligned} V &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - \frac{1}{2}u_1u_3 - \frac{1}{2}u_2u_3, x_4 - \frac{1}{2}u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1) \cup \\ &\quad V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3). \end{aligned}$$

The variety $V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - \frac{1}{2}u_1u_3 - \frac{1}{2}u_2u_3, x_4 - \frac{1}{2}u_3)$ can be further split into $V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{1}{2}u_1 - \frac{1}{2}u_2, x_4 - \frac{1}{2}u_3) \cup V(x_1 - u_1 - u_2, x_2 - u_3, u_3, x_4 - \frac{1}{2}u_3)$. Then,

$$\begin{aligned} V &= V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{1}{2}u_1 - \frac{1}{2}u_2, x_4 - \frac{1}{2}u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_4 - \frac{1}{2}u_3, u_3) \cup \\ &\quad V(x_1 - u_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1) \cup \\ &\quad V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3). \end{aligned}$$

The Groebner basis for $V(x_1 - u_1 - u_2, x_2 -- u_3, x_3u_3 - x_4u_2 - \frac{1}{2}u_1u_3, u_1)$ is made up of the following polynomials,

$$\begin{aligned}
r_1 &= x_1 - u_2,\\
r_2 &= x_2 - u_3,\\
r_3 &= x_3u_3 - x_4u_2,\\
r_4 &= u_1.
\end{aligned}$$

So,

$$\begin{aligned}
V \;=\; & V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{1}{2}u_1 - \frac{1}{2}u_2, x_4 - \frac{1}{2}u_3) \cup\\
& V(x_1 - u_1 - u_2, x_2 - u_3, x_4 - \frac{1}{2}u_3, u_3) \cup\\
& V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1) \cup\\
& V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3).
\end{aligned}$$

The Groebner basis for $V(x_1 - u_1 - u_2, x_2 - u_3, x_4 - \frac{1}{2}u_3, u_3)$ is

$$\begin{aligned}
t_1 &= x_1 - u_1 - u_2,\\
t_2 &= x_2,\\
t_3 &= x_4,\\
t_4 &= u_3.
\end{aligned}$$

As a result,

$$\begin{aligned}
V \;=\; & V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{1}{2}u_1 - \frac{1}{2}u_2, x_4 - \frac{1}{2}u_3) \cup\\
& V(x_1 - u_1 - u_2, x_2, x_4, u_3) \cup\\
& V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1) \cup\\
& V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3).
\end{aligned}$$

In the union of the varieties listed above $V(x_1 - u_1 - u_2, x_2, x_4, u_3) \subset V(x_2, x_4, u_3)$ since $\langle x_2, x_4, u_3\rangle \subset \langle x_1 - u_1 - u_2, x_2, x_4, u_3\rangle$. And finally the variety

$$\begin{aligned}
V \;=\; & V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}) \cup\\
& V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1) \cup\\
& V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3).
\end{aligned}$$

The varieties that are left are all irreducible components of V. The varieties $V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1)$, $V(x_1, x_2, u_1 - u_2, u_3)$, and $V(x_2, x_4, u_3)$ represent the degenerate cases for the parallelogram problem. In the varieties $V(x_1, x_2, u_1 - u_2, u_3)$ and $V(x_2, x_4, u_3)$, the arbitrary variable $u_3 = 0$. This would make vertex C a point on $\overline{AB}$. Similarly, $u_1 = 0$ in $V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1)$ makes vertex B at the same location as vertex A. Consequently, in these cases the figure $ABCD$ would not be a parallelogram. This is why the first attempt at using the radical membership test failed. As a result, these varieties must be removed and it will be shown that the polynomials g_1 and g_2 disappear for the same values as $V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2})$. To conclude this problem we need to show that g_1 and $g_2 \in \sqrt{\langle x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}\rangle}$. By using the radical membership test if $1 \in \langle x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}, 1 - yg_1\rangle$, then $g_1 \in \sqrt{\langle x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}\rangle}$. Computing a Groebner basis for $x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}, 1 - yg_1$ with Maple resulted in a basis of $\{1\}$. Therefore, g_1 vanishes on $V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2})$. Similarly, if $1 \in \langle x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}, 1 - yg_2\rangle$, then $g_2 \in \sqrt{\langle x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}\rangle}$. Computing a Groebner basis for $x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}, 1 - yg_2$ with Maple again resulted in a basis of $\{1\}$. So the conclusion g_2 also vanishes on $V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2})$. Hence, $\overline{AN} = \overline{ND}$ and $\overline{BN} = \overline{NC}$ so the diagonals of any parallelogram intersect at a point that bisects one another.

Although we successfully proved that the diagonals of a parallelogram bisect each other, we need to take a moment to make some important observations about using the Groebner basis technique. Notice that we began to use the Groebner basis technique without taking into account that there are several degenerate cases that can occur. If the figure $ABCD$ is not a parallelogram, then it would not be possible to prove the stated theorem. When the variety V contained polynomials that were factorable it became necessary to split the variety into a union $V' \cup U$. In this union V' represents the irreducible nondegenerate portion of V and U represents the degenerate cases. To do this, we computed a Groebner basis. Along the way there were varieties that were absorbed into others and eventually we determined that $V = V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}) \cup V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1) \cup V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3)$. So for this example, $V' = V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2})$ and $U = V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1) \cup V(x_1, x_2, u_1 - u_2, u_3) \cup V(x_2, x_4, u_3)$. Despite the fact that we never mentioned degenerate cases in the beginning of the problem, computing a finite union of irreducible varieties led to the identification and exclusion of these problem cases represented by the varieties $V(x_1 - u_2, x_2 - u_3, x_3u_3 - x_4u_2, u_1)$, $V(x_1, x_2, u_1 - u_2, u_3)$, and $V(x_2, x_4, u_3)$. It is for this reason that we only check to see if g_1 and $g_2 \in \mathbf{I}(V') = \mathbf{I}(V(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1+u_2}{2}, x_4 - \frac{u_3}{2}))$.

Finally, we can outline the steps involved in using the Groebner Basis Algorithm (GBA) below:

- Sketch a picture of the problem. Depending on the construction label all vertices, intersections, or any other necessary points. We would like to make a distinction between independent and dependent x and y-coordinates for the points in the figure. Any coordinate labeled u_i is an arbitrary variable. However, coordinates labeled x_i are dependent on the location of other points in the figure.

- Determine the polynomials that represent the hypotheses and the conclusion(s) by using the labeled figure.

- To show whether the conclusion follows from the hypotheses using Proposition 5.1, determine if $g \in \sqrt{\langle h_1, h_2, \ldots, h_n \rangle}$ using the following radical membership test: $g \in \sqrt{\langle h_1, h_2, \ldots, h_n \rangle}$ if and only if $\{1\}$ is the reduced Groebner basis of the ideal $\langle h_1, h_2, \ldots, h_n, 1 - yg \rangle \subset k[x_1, x_2, \ldots, x_n, y]$.

- If the basis of $\langle h_1, h_2, \ldots, h_n, 1 - yg \rangle$ is not $\{1\}$ (due to possible degenerate cases), compute a reduced Groebner basis for the ideal generated by all of the hypotheses to get a finite union of irreducible varieties $V' \cup U$ as described earlier. Then show that g vanishes on the resulting variety V' that does not represent a degenerate case.

5.2 Problem 2: The Circle Theorem of Apollonius

We will now illustrate a second example of using the Groebner Basis Algorithm by proving the Circle Theorem of Apollonius.

Theorem 5.3 (The Circle Theorem of Apollonius). *Let $\triangle ABC$ be a right triangle in the plane, with right angle at A. The foot of the altitude drawn from A to $\overline{BC}$ and the three noncollinear midpoints of $\triangle ABC$ all lie on the same circle.*

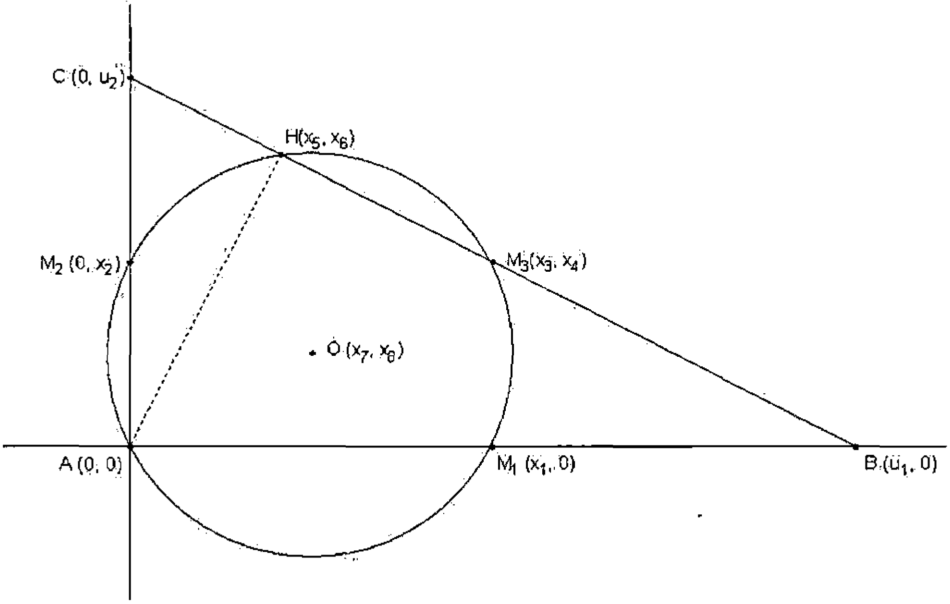

Figure 5.2: Circle centered a O containing points M_1, M_2, M_3, and H.

We will begin by placing $\triangle ABC$ on the Cartesian plane as illustrated above. As defined by the theorem, the right angle will be at vertex A. We will place vertex A at the origin $(0,0)$. The second vertex B of $\triangle ABC$ will be placed randomly on the x-axis and it will have coordinates $(u_1, 0)$. The final vertex C will also be placed randomly on the y-axis and it will have coordinates $(0, u_2)$. The coordinates for the three noncollinear midpoints of sides $\overline{AB}$, $\overline{BC}$, and $\overline{AC}$ will all be determined by the placement of vertices B and C. The midpoint of $\overline{AB}$ will have coordinates $(x_1, 0)$ and be labeled M_1. The midpoint of $\overline{AC}$ will have coordinates $(0, x_2)$ and be labeled M_2. The midpoint of $\overline{BC}$ will have coordinates (x_3, x_4) and will be labeled M_3. The altitude $\overline{AH}$ will be drawn from vertex A to $\overline{BC}$. The foot of this altitude, point H, will have coordinates (x_5, x_6). The objective of this theorem is to prove that points M_1, M_2, M_3, and H all lie on the same circle. Thus, the final point that needs to be defined for this example is the center of this circle. The center will be labeled point O and have coordinates (x_7, x_8).

Note that the circle also passes through the vertex A, the foot of the other two altitudes. It turns out that the circle in Figure 5.2 is a special case of the 9-point circle theorem often studied in an advanced Euclidean geometry course. Since $\triangle ABC$ is a right triangle we instead have a 5-point circle. It is important to point out that there are degenerate cases that are possible in attempting to prove this theorem. The first case occurs when both $u_1 = 0$ and $u_2 = 0$. When $u_1 = 0$ then vertex B is at the same location as vertex A. Similarly, if $u_2 = 0$, then vertex C is also at the same location as vertex A. Now, with $A = B = C$ there is no longer a right triangle. Consequently, this makes the location of M_1, M_2, M_3, and H also at vertex A. Since $A = B = C = M_1 = M_2 = M_3 = H$, there is only a single point in the plane. Thus, we can find an infinite number of circles that pass through this single point. On the other hand, suppose $u_1 \neq 0$ and $u_2 = 0$. If $u_2 = 0$, then vertex C is at the same location as vertex A. Furthermore, this will make $M_2 = A = C$. Once again there is no right triangle but we have a line segment from A to B. In addition, $M_3 = M_1$ and $H = A$. Just like in the previous scenario, we can find an infinite number of circles passing through the points M_1, M_2, M_3, and H. However, in order to prove this geometric theorem, we will assume that the points A, B, and C are three distinct vertices that form a right triangle in the plane to avoid the previously described degenerate cases.

Using the picture above we will convert the hypothesis of the theorem into polynomial equations. We will use the midpoint formula to write the first four hypotheses of this theorem. Computing the midpoint of $\overline{AB}$, we get:

$$\begin{aligned} M_1 &= \left(\frac{u_1+0}{2}, \frac{0+0}{2}\right) \\ (x_1, 0) &= \left(\frac{u_1}{2}, 0\right) \\ x_1 &= \frac{u_1}{2} \\ x_1 - \frac{u_1}{2} &= 0. \end{aligned}$$

So, with $h_1 = 2x_1 - u_1$ the first hypothesis translates algebraically as $h_1 = 0$. Similarly, computing the midpoint of $\overline{AC}$, we get:

$$\begin{aligned} M_2 &= \left(\frac{0+0}{2}, \frac{u_2+0}{2}\right) \\ (0, x_2) &= \left(0, \frac{u_2}{2}\right) \\ x_2 &= \frac{u_2}{2} \\ x_2 - \frac{u_2}{2} &= 0. \end{aligned}$$

The second hypothesis is $h_2 = 2x_2 - u_2 = 0$.

Finally, computing the midpoint of $\overline{BC}$, we get:

$$\begin{aligned}
M_3 &= \left(\frac{0+u_1}{2}, \frac{0+u_2}{2}\right) \\
(x_3, x_4) &= \left(\frac{u_1}{2}, \frac{u_2}{2}\right) \\
x_3 &= \frac{u_1}{2} \\
x_3 - \frac{u_1}{2} &= 0 \\
x_4 &= \frac{u_2}{2} \\
x_4 - \frac{u_2}{2} &= 0.
\end{aligned}$$

The computation above generates the third and fourth hypotheses: $h_3 = 2x_3 - u_1 = 0$ and $h_4 = 2x_4 - u_2 = 0$.

The construction of point H with coordinates (x_5, x_6) at the foot of the intersection of $\overline{AH}$ and $\overline{BC}$ results in two more hypotheses. Since $\overline{AH}$ is an altitude of $\triangle ABC$, $\overline{AH}$ is perpendicular to side $\overline{BC}$. Since $\overline{AH} \perp \overline{BC}$, the product of the slope of $\overline{AH}$ and the slope of $\overline{BC}$ is -1. This translates into the following:

$$\begin{aligned}
\frac{x_6 - 0}{x_5 - 0} \cdot \frac{0 - u_2}{u_1 - 0} &= -1, \\
\frac{x_6}{x_5} \cdot \frac{-u_2}{u_1} &= -1, \\
\frac{-x_6 u_2}{x_5 u_1} &= -1, \\
-x_6 u_2 &= -x_5 u_1.
\end{aligned}$$

The fifth hypotheses is then $h_5 = x_5 u_1 - x_6 u_2 = 0$.

Now, points B, H, and C are also collinear so the slope of $\overline{BH} = \overline{BC}$. Thus, we have the following:

$$\begin{aligned}
\frac{0 - x_6}{u_1 - x_5} &= \frac{0 - u_2}{u_1 - 0} \\
\frac{-x_6}{u_1 - x_5} &= \frac{-u_2}{u_1} \\
-x_6 u_1 &= -u_2(u_1 - x_5) \\
-x_6 u_1 &= -u_1 u_2 + x_5 u_2
\end{aligned}$$

The sixth hypotheses is $h_6 = x_6 u_1 - u_1 u_2 + x_5 u_2 = 0$.

The points M_1, M_2 and M_3 are three noncollinear points in our figure. So we know that three noncollinear points lie on the circumscribed circle of the triangle they form. The center of this circle is point $O(x_7, x_8)$. Using the distance formula, we can derive two additional hypotheses. Since $\overline{M_1O}$ and $\overline{M_2O}$ are both radii, then

$$\begin{aligned}\sqrt{(x_1-x_7)^2+(0-x_8)^2} &= \sqrt{(x_7-0)^2+(x_8-x_2)^2}\\ (x_1-x_7)^2+x_8^2 &= x_7^2+(x_8-x_2)^2.\end{aligned}$$

The seventh hypotheses then becomes $h_7 = (x_1-x_7)^2+x_8^2-x_7^2-(x_8-x_2)^2 = 0$. Similarly, since $\overline{M_1O} = \overline{M_3O}$, we have

$$(x_1-x_7)^2+x_8^2 = (x_4-x_8)^2+(x_3-x_7)^2.$$

The eighth and final hypotheses is $h_8 = (x_1-x_7)^2+x_8^2-(x_3-x_7)^2-(x_4-x_8)^2 = 0$. In this example, we would like to show that point H also lies on the circle centered at O containing points $M_1, M_2,$ and M_3. Thus, our conclusion is that $\overline{HO} = \overline{M_1O}$, or

$$(x_1-x_7)^2+x_8^2 = (x_5-x_7)^2+(x_6-x_8)^2$$

So, the conclusion, expressed algebraically, is $g = (x_1-x_7)^2+x_8^2-(x_5-x_7)^2-(x_6-x_8)^2 = 0$.

Now, $g \in \sqrt{\langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8\rangle}$ if and only if $1 \in \langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8, 1-yg\rangle$ in the ring $\mathbb{R}[u_1, u_2, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$. Computing the basis did not result in a basis of $\{1\}$ like we had hoped. Since the radical membership test failed, we can begin to compute the Groebner basis for the ideal $\langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8\rangle$ in the ring $\mathbb{R}[u_1, u_2, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$ using lex order with $x_1 > x_2 > x_3 > x_4 >$

$x_5 > x_6 > x_7 > x_8 > u_1 > u_2$. Using Maple the Groebner basis is the following:

$$\begin{aligned}
p_1 &= 2x_1 - u_1 = 2\left(x_1 - \frac{u_1}{2}\right), \\
p_2 &= 2x_2 - u_2 = 2\left(x_2 - \frac{u_2}{2}\right), \\
p_3 &= 2x_3 - u_1 = 2\left(x_3 - \frac{u_1}{2}\right), \\
p_4 &= 2x_4 - u_2 = 2\left(x_4 - \frac{u_2}{2}\right), \\
p_5 &= x_5u_1 - x_6u_2, \\
p_6 &= x_5u_2 + x_6u_1 - u_1u_2, \\
p_7 &= 4x_6x_7u_2 - x_6u_1u_2 = 4x_6u_2\left(x_7 - \frac{u_1}{4}\right), \\
p_8 &= 4x_6x_8u_1 - x_6u_1u_2 = 4x_6u_1\left(x_8 - \frac{u_2}{4}\right), \\
p_9 &= x_6u_1^2 + x_6u_2^2 - u_1^2u_2, \\
&= x_6(u_1^2 + u_2^2) - u_1^2u_2, \\
&= (u_1^2 + u_2^2)\left(x_6 - \frac{u_1^2u_2}{u_1^2 + u_2^2}\right), \\
p_{10} &= 4x_7u_1 - u_1^2 = 4u_1\left(x_7 - \frac{u_1}{4}\right), \\
p_{11} &= 4x_8u_2 - u_2^2 = 4u_2\left(x_8 - \frac{u_2}{4}\right).
\end{aligned}$$

Unfortunately, this is not a reduced Groebner basis. Notice that some of the listed polynomials are multiples or linear combinations of one another. Take for instance, a linear combination of the polynomials p_5 and p_6

$$\begin{aligned}
u_1p_5 + u_2p_6 &= u_1(x_5u_1 - x_6u_2) + u_2(x_5u_2 + x_6u_1 - u_1u_2), \\
&= x_5u_1^2 - x_6u_1u_2 + x_5u_2^2 + x_6u_1u_2 - u_1u_2^2, \\
&= x_5u_1^2 + x_5u_2^2 - u_1u_2^2, \\
&= x_5(u_1^2 + u_2^2) - u_1u_2^2, \\
&= (u_1^2 + u_2^2)\left(x_5 - \frac{u_1u_2^2}{u_1^2 + u_2^2}\right).
\end{aligned}$$

Thus, we can eliminate them from the basis. Once this has been accomplished it will result in the reduced Groebner basis shown below

$$\begin{aligned} f_1 &= x_1 - \frac{u_1}{2}, \\ f_2 &= x_2 - \frac{u_2}{2}, \\ f_3 &= x_3 - \frac{u_1}{2}, \\ f_4 &= x_4 - \frac{u_2}{2}, \\ f_5 &= x_5 - \frac{u_1 u_2^2}{u_1^2 + u_2^2}, \\ f_6 &= x_6 - \frac{u_1^2 u_2}{u_1^2 + u_2^2}, \\ f_7 &= x_7 - \frac{u_1}{4}, \\ f_8 &= x_8 - \frac{u_2}{4}. \end{aligned}$$

Notice that by computing the Groebner basis in the ring $\mathbb{R}[u_1, u_2, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$ it took longer to produce the desired basis. In the computations above, we see that trying to generate a finite union of irreducible varieties can be a quite a challenge. The reason why this task is so difficult is because of the degenerate cases. Fortunately, there is a way to modify the Groebner Basis Algorithm so that we can prove any geometric theorem excluding all degenerate cases that occur. Throughout the parallelogram example all of the computations for the Groebner basis were done in the ring $\mathbb{R}[u_1, u_2, u_3, x_1, x_2, x_3, x_4]$. Recall that the u_i represent elements that are independent or arbitrarily chosen, and these elements should be nonzero if we want to avoid degenerate cases. So, will computing a basis in the ring $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$ (or making the independent variables part of the coefficients) make things simpler? Yes, we can modify Proposition 5.1 because it is too strict since it does not take into account that there are degenerate cases.

Proposition 5.4. *If $g \in \sqrt{\langle h_1, h_2, \ldots, h_n\rangle}$ in $k(u_1, u_2, \ldots, u_i)[x_1, x_2, \ldots, x_j]$, then $g \in$ $\mathrm{I}(V')$ and g follows from $h_1, h_2, \ldots, h_n$.*

To illustrate what will happen with this modification, we will redo the parallelogram example by working in the ring $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4]$. So, $g_1 \in \sqrt{\langle h_1, h_2, h_3, h_4\rangle}$ if and only if $1 \in \langle h_1, h_2, h_3, h_4, 1 - yg_1\rangle$ in the ring $\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4, y]$. In addition, $g_2 \in \sqrt{\langle h_1, h_2, h_3, h_4\rangle}$ if and only if $1 \in \langle h_1, h_2, h_3, h_4, 1 - yg_2\rangle$ in the ring

$\mathbb{R}(u_1, u_2, u_3)[x_1, x_2, x_3, x_4, y]$. Using Maple once again to compute a Groebner basis, we find that in both cases the basis is $\{1\}$. Thus, by the radical membership test and Proposition 5.4 the conclusions g_1 and g_2 follow from the hypotheses h_1, h_2, h_3 and h_4. Using this approach to verify a geometric theorem is much easier due to the fact that we do not have to know the decomposition of the variety V. It eliminates the time consuming task of having to find and exclude any degenerate cases.

Returning to the circle theorem, if we had made the initial computation in the ring $\mathbb{R}(u_1, u_2)[x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$, Maple would have generated the reduced Groebner basis containing the polynomials f_1, f_2, f_3, f_4, f_5, f_6, f_7, and f_8. It would not have been necessary to factor and reduce the polynomials p_i for $1 \leq i \leq 11$ generated by computing the basis in $\mathbb{R}[u_1, u_2, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$ as shown earlier. By working in the ring $\mathbb{R}(u_1, u_2)[x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8]$ in the all of the f_i's listed above each of the terms that come after the minus sign are coefficients from the field $\mathbb{R}$. Consequently, the ideal $\langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8 \rangle$ is of the form $\langle x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \rangle$ with $a_1, a_2, \ldots, a_n \in k$ (k is a field) is maximal. When an ideal is maximal in $k[x_1, x_2, \ldots, x_n]$, then the ideal is prime which now implies that $V(f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8)$ is irreducible so it cannot be decomposed any further. As a result, we can use Proposition 5.1 and the radical membership test to determine whether $g \in \sqrt{\langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8 \rangle}$. In order for this to occur, we must show that $1 \in \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, 1 - yg \rangle$. Using Maple one more time to compute the Groebner basis of $\langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, 1 - yg \rangle$ resulted in a basis of $\{1\}$. Therefore, the conclusion $g \in \sqrt{\langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8 \rangle}$. Hence, g follows from the hypotheses h_i for $1 \leq i \leq 8$. Consequently, this makes the point H lie on the same circle passing through the three noncollinear points M_1, M_2, and M_3.

However, it is interesting to note that for this problem there is an alternative to using the radical membership test. The reason why we have consistently used the radical membership test is because it is time consuming to determine if the conclusion g is an element of a particular ideal. By using the division algorithm for multivariable polynomials, we can easily determine whether the polynomial $g \in \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8 \rangle$. It turns out that our conclusion $g = (x_1 - x_7)^2 + x_8^2 - (x_5 - x_7)^2 - (x_6 - x_8)^2$ has a remainder of 0 when it is divided by the Groebner basis $f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8$. In other words, the conclusion can be written as a linear combination of the polynomials in our Groebner basis as follows,

$$\begin{aligned} g &= \left(-x_1 + 2x_7 - \frac{u_1}{2}\right) \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 0 \cdot f_4 + \left(x_5 - 2x_7 + \frac{u_1 u_2^2}{u_1^2 + u_2^2}\right) \cdot f_5 \\ &\quad + \left(x_6 - 2x_8 + \frac{u_1^2 u_2}{u_1^2 + u_2^2}\right) \cdot f_6 + \left(\frac{u_1^3 - u_1 u_2^2}{u_1^2 + u_2^2}\right) \cdot f_7 + \left(\frac{-2u_1^2 u_2}{u_1^2 + u_2^2}\right) \cdot f_8, \\ &= \left(-x_1 + 2x_7 - \frac{u_1}{2}\right)\left(x_1 - \frac{u_1}{2}\right) + 0 \cdot \left(x_2 - \frac{u_2}{2}\right) + 0 \cdot \left(x_3 - \frac{u_1}{2}\right) + 0 \cdot \left(x_4 - \frac{u_2}{2}\right) \\ &\quad + \left(x_5 - 2x_7 + \frac{u_1 u_2^2}{u_1^2 + u_2^2}\right)\left(x_5 - \frac{u_1 u_2^2}{u_1^2 + u_2^2}\right) + \left(x_6 - 2x_8 + \frac{u_1^2 u_2}{u_1^2 + u_2^2}\right)\left(x_6 - \frac{u_1^2 u_2}{u_1^2 + u_2^2}\right) \\ &\quad + \left(\frac{u_1^3 - u_1 u_2^2}{u_1^2 + u_2^2}\right)\left(x_7 - \frac{u_1}{4}\right) + \left(\frac{-2u_1^2 u_2}{u_1^2 + u_2^2}\right)\left(x_8 - \frac{u_2}{4}\right), \\ &= -x_1^2 + 2x_1 x_7 - u_1 x_7 + \frac{u_1^2}{4} + x_5^2 - 2x_5 x_7 + \frac{2u_1 u_2^2}{u_1^2 + u_2^2} x_7 - \frac{u_1^2 u_2^4}{(u_1^2 + u_2^2)^2} + x_6^2 - 2x_6 x_8 \\ &\quad + \frac{2u_1^2 u_2}{u_1^2 + u_2^2} x_8 - \frac{u_1^4 u_2^2}{(u_1^2 + u_2^2)^2} + \frac{u_1^3 - u_1 u_2^2}{u_1^2 + u_2^2} x_7 - \frac{u_1^4 - u_1^2 u_2^2}{4(u_1^2 + u_2^2)} - \frac{2u_1^2 u_2}{u_1^2 + u_2^2} x_8 + \frac{u_1^2 u_2^2}{2(u_1^2 + u_2^2)}. \end{aligned}$$

Collecting like terms in the equation above,

$$\frac{-u_1^2 u_2^4}{(u_1^2 + u_2^2)^2} - \frac{u_1^4 u_2^2}{(u_1^2 + u_2^2)^2} = \frac{-u_1^2 u_2^4 - u_1^4 u_2^2}{(u_1^2 + u_2^2)^2} = \frac{-u_1^2 u_2^2 (u_2^2 + u_1^2)}{(u_1^2 + u_2^2)^2} = -\frac{u_1^2 u_2^2}{u_1^2 + u_2^2}.$$

Continuing to combine like terms,

$$\frac{u_1^2}{4} - \frac{u_1^4 - u_1^2 u_2^2}{4(u_1^2 + u_2^2)} + \frac{u_1^2 u_2^2}{2(u_1^2 + u_2^2)} = \frac{u_1^4 + u_1^2 u_2^2 - u_1^4 + u_1^2 u_2^2 + 2u_1^2 u_2^2}{4(u_1^2 + u_2^2)} = \frac{4u_1^2 u_2^2}{4(u_1^2 + u_2^2)} = \frac{u_1^2 u_2^2}{u_1^2 + u_2^2}.$$

Furthermore,

$$\frac{2u_1 u_2^2}{u_1^2 + u_2^2} x_7 + \frac{u_1^3 - u_1 u_2^2}{u_1^2 + u_2^2} x_7 = \frac{u_1^3 + u_1 u_2^2}{u_1^2 + u_2^2} x_7 = \frac{u_1(u_1^2 + u_2^2)}{u_1^2 + u_2^2} x_7 = u_1 x_7.$$

As a result, the equation for g becomes,

$$\begin{aligned} g &= -x_1^2 + 2x_1 x_7 - u_1 x_7 + x_5^2 - 2x_5 x_7 + x_6^2 - 2x_6 x_8 - \frac{u_1^2 u_2^2}{u_1^2 + u_2^2} + \frac{u_1^2 u_2^2}{u_1^2 + u_2^2} + u_1 x_7, \\ &= -x_1^2 + 2x_1 x_7 + x_5^2 - 2x_5 x_7 + x_6^2 - 2x_6 x_8. \end{aligned}$$

This is exactly what the polynomial g equals when $(x_1 - x_7)^2 + x_8^2 - (x_5 - x_7)^2 - (x_6 - x_8)^2$ is multiplied out. Consequently, $g \in \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8 \rangle$. Since $\langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8 \rangle = \langle f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8 \rangle$, this will also make $g \in \langle h_1, h_2, h_3, h_4, h_5, h_6, h_7, h_8 \rangle$. Hence, g will vanish for the same values that make all of the h_i for $1 \leq i \leq 8$ zero. Therefore, g follows from the hypotheses. The point H is once again on the circle containing the three noncollinear points M_1, M_2, and M_3.

From our experiences with the previous two theorems, we can now modify and make improvements to the Groebner Basis Algorithm as follows:

- Sketch a picture of the problem. Depending on the construction label all vertices, intersections, or any other necessary points. We would like to make a distinction between independent and dependent x and y-coordinates for the points in the figure. Any coordinate labeled u_i is an arbitrary variable. However, coordinates labeled x_i are dependent on the location of other points in the figure.

- Determine the polynomials that represent the hypotheses and the conclusion(s) by using the labeled figure.

- To show whether the conclusion follows from the hypotheses using Proposition 5.1, determine if $g \in \sqrt{\langle h_1, h_2, \ldots, h_n \rangle}$ using the following radical membership test: $g \in \sqrt{\langle h_1, h_2, \ldots, h_n \rangle}$ if and only if $\{1\}$ is the reduced Groebner basis of the ideal $\langle h_1, h_2, \ldots, h_n, 1 - yg \rangle \subset k[x_1, x_2, \ldots, x_n, y]$.

- If $\{1\}$ is not a reduced Groebner basis of $\langle h_1, h_2, \ldots, h_n, 1 - yg \rangle$, compute a reduced Groebner basis for the ideal generated by all of the hypotheses in the ring $k(u_1, \ldots, u_i)[x_1, \ldots, x_j]$. Apply the radical membership test to determine if 1 is an element of the ideal generated by $\langle f_1, f_2, \ldots, f_t, 1 - yg \rangle$ where the f's are polynomials from the Groebner basis (in the ring $k(u_1, \ldots, u_i)[x_1, \ldots, x_j, y]$).

Chapter 6

Conclusion

From both of the examples presented in Chapter 5, we learned how to apply the Groebner Basis Algorithm to geometric theorems. In order to begin using the GBA, it is important to write the hypotheses and the conclusion(s) in polynomial form. Since the polynomials that represent the hypotheses and conclusions are multivariable polynomials from the ring $k[x_1, x_2, \ldots, x_n]$, it is extremely difficult to directly solve the system of equations generated by these polynomials. Instead, the GBA shifts the focus to the ideals that generate the polynomials and the varieties of these ideals. This approach will make it easier to reach the final goal. This process will ultimately show that the values which make the hypotheses zero also make the conclusion(s) vanish. As a result, we will have successfully proven the geometric theorem we happen to be studying.

Furthermore, there were some important concerns that were raised by using the Groebner Basis Algorithm to prove geometric theorems. First, would the GBA be able to take into account the degenerate cases that can occur in these theorems? The answer to this question is yes! Recall for a moment what happened in the diagonals of a parallelogram problem. In order for the figure drawn in the plane to be called a parallelogram, the location of the four vertices is critical. For example, the figure would not be a parallelogram if two distinct vertices shared the same location. The variety V was split into the union of a finite number of irreducible varieties. Once this was achieved, the varieties that represented the degenerate cases were quickly identified and excluded. The final step of the algorithm was to then apply the radical membership test to show that the conclusion followed from the hypotheses. However, the parallelogram problem highlighted one drawback when using the GBA. The process to end up with a union of irreducible varieties can be long and time consuming. Fortunately, we later discovered that by working in the ring $k(u_1, u_2, \ldots, u_i)[x_1, x_2, \ldots, x_j]$ eliminated the need to know the decomposition for a given variety in order to remove any degenerate cases. Consequently, we were able to adjust and improve the steps used to apply the Groebner Basis Algorithm.

When a Groebner basis is computed for the hypotheses, it is sometimes possible to show that the conclusion is an element of the ideal generated by the Groebner basis. At this point, we can use the division algorithm for multivariable polynomials to determine the remainder. If the remainder is zero, then the conclusion can be written as a linear combination of all of the polynomials in the Groebner basis. Hence, the conclusion would be an element of the ideal generated by the Groebner basis and there would be no need to resort to the radical membership test. This scenario was illustrated with the Circle Theorem of Apollonius.

One of the more interesting aspects of this project is that concepts studied in algebraic geometry have been applied to computer science. The first application to computer science is in the field of robotics. It is possible to describe the movement of a robot arm using varieties. The goal is take a robot arm and enable the robot to perform a task by writing a program that can control and plan the movements of the robot. For instance, the robot might be provided with mechanisms for grasping objects or with tools to carry out a given task. The second application is to researchers working in artificial intelligence and geometric modeling. This project shows that we are able to use an algorithmic method to prove statements in Euclidean geometry. This is important because programs have been written that have successfully proven or disproven conjectured relationships between, or theorems about, plane geometric objects. [CLO97]

Bibliography

[CLO97] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[Sma98] James R. Smart. *Modern Geometries.* Brooks/Cole Publishing, California, fifth edition, 1998.