AN ABSTRACT OF THE THESIS OF

Eugene A. Dixon for the Master of Science
(name of student) (degree)

in Mathematics presented on May 5, 1995
(major) (date)

Title: Grobner Bases

Abstract approved: Joe Yam

Suppose we are given a set of polynomials $g_1, ..., g_s$ and we wish to know whether another polynomial can be expressed in the form $g_1h_1 + ... + g_sh_s$ for polynomials $h_1,...,h_s$. This is often called the *ideal membership problem*. If $g_1, ..., g_s$ are polynomials in one variable, then there is really no difficulty at all. If, however, the polynomials are in n variables, then the problem becomes much more difficult.

Now suppose we have a system of polynomial equations and are looking for the solutions to $f_1(x_1, ..., x_n) = \ldots = f_s(x_1, ..., x_n) = 0$. If all the equations are linear, we can use Gaussian elimination on the matrix of coefficients and backsubstitution. The problem arises when the polynomials are nonlinear.

Both of these problems can be simplified by considering the theory of Grobner bases. The ideal membership problem can be solved for polynomials in n variables similar to the case of polynomials in one variable by using a general form of the division algorithm and a Grobner basis for the ideal. Also we can create a corresponding system of polynomial equations from any system of polynomial equations with a reduction of variables that will at least simplify the work of finding solutions to the original system.

GRÖBNER BASES

A Thesis

Presented to

the Division of Mathematics and Computer Science

EMPORIA STATE UNIVERSITY

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

by

Eugene A. Dixon

May 1995

Joe Yant

Approved for the Major Division

John O Schumann

Approved for the Graduate Council

Acknowledgement

I would like to thank Dr. Joe Yanik for introducing me to Gröbner bases, guiding me through my thesis and spending a large amount of time reading rough drafts. I would also like to thank the thesis committee, Dr. Philip Gustafson, Dr. Elizabeth Yanik, and Dr. Jorge Ballester for their time and effort. I would especially like to thank my wife, Tina, for patiently waiting by my side while writing this thesis.

Table of Contents

Introduction

Suppose we are given a set of polynomials $g_1, ..., g_s$ and we wish to know whether another polynomial can be expressed in the form $g_1h_1 + ... + g_sh_s$. This is often called the *ideal membership problem*. If $g_1, ..., g_s$ are polynomials in one variable, then the problem can be easily solved. If, however, the polynomials are in n variables, then the problem becomes much more difficult.

Now suppose we have a system of polynomial equations and are looking for the solutions to $f_1(x_1, ..., x_n) = \ldots = f_s(x_1, ..., x_n) = 0$. If all the equations are linear, we can use Gaussian elimination of the matrix of coefficients and back-substitution. The difficulty arises when the polynomials are nonlinear.

Both of these problems can be simplified by considering the theory of Gröbner bases. We will see that the ideal membership problem can be solved for polynomials in n variables in a manner similar to the case of polynomials in one variable by using a general form of the division algorithm and a different generating set for the ideal. Also we can create a corresponding system of polynomial equations from any system of polynomial equations with a reduction of variables that will at least simplify the work of finding solutions to the original system.

Chapter I
Definitions

We will now define some of the needed algebraic and geometric concepts we will be using throughout the paper. Other definitions will come as needed. Let k be a field (For example, k might be the field of real numbers or of complex numbers). All definitions here and throughout the paper are taken from *Ideals, varieties and algorithms* (See [c]).

Definition 1.1.1: A **monomial** in $x_1,...,x_n$ is a product of the form $x_1^{\alpha_1},...,x_n^{\alpha_n}$ where all exponents $\alpha_1,...,\alpha_n$ are non-negative integers. If we let $\alpha=(\alpha_1,...,\alpha_n)$ be an n-tuple of exponents, then we can write $x_1^{\alpha_1},...,x_n^{\alpha_n}$ as x^α.

A **polynomial** f in variables $x_1,...,x_n$ is a finite linear combination with coefficients in k of monomials. Polynomials can be written in the form $f=\Sigma_\alpha a_\alpha x^\alpha$ where a_α is the coefficient of the monomial x^α and where the sum of n-tuples α is finite. If a_α is not zero then $a_\alpha x^\alpha$ is called a **term** of f. The set of all polynomials in $x_1,...,x_n$ with coefficients in k is denoted $k[x_1,...,x_n]$.

We will define an ordering of the monomials of the polynomials using **lexicographic order**. Let $\alpha=(\alpha_1,...,\alpha_n)$ and $\beta=(\beta_1,...,\beta_n)$ be n-tuples of nonnegative integers. We say $\alpha>\beta$ if, in the vector difference $\alpha-\beta \in Z^n$, the left-most nonzero entry is positive. Also, $x^\alpha>x^\beta$ if $\alpha>\beta$.

Let $f=\Sigma_\alpha a_\alpha x^\alpha$ be a nonzero polynomial in $k[x_1,...,x_n]$. Then the degree of f, written **deg(f)**, is the $\max\{\alpha | a_\alpha \neq 0\}$ with respect to this lexicographic ordering. The leading coefficient of f, written **LC(f)**, is $a_{\deg(f)} \in k$. The leading monomial of f, written **LM(f)**, is $x^{\deg(f)}$. The leading term of f then is LC(f) $\cdot$ LM(f) and is written **LT(f)**.

Definition 1.1.2: With the usual addition and multiplication of polynomials, $k[x_1,\dots,x_n]$ is a commutative ring, usually called a polynomial ring. A subset I of $k[x_1,\dots,x_n]$ is called 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 $g \in k[x_1,\dots,x_n]$, then $fg \in I$.

Definition 1.1.3: Let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$. Define

$$\langle f_1,\dots,f_s \rangle = \{\Sigma\ h_i f_i \mid h_1,\dots,h_s \in k[x_1,\dots,x_n]\}.$$

We will show later in Theorem 3.1.1 that $\langle f_1,\dots,f_s \rangle$ is an ideal.

Definition 1.1.4: Given a field k and a positive integer n, we define the n-dimensional **affine space** over k to be the set $k^n = \{(a_1,\dots,a_n) \mid a_1,\dots,a_n \in k\}$. Now let $f_1,\dots,f_s$ be polynomials in $k[x_1,\dots,x_n]$. Then the **affine variety** defined by $f_1,\dots,f_s$ is the set $\mathbf{V}(f_1,\dots,f_s) = \{ (a_1,\dots,a_n) \in k^n \mid f_i(a_1,\dots,a_n)=0 \text{ for all } 1 \leq i \leq s \}$.

Definition 1.1.5: We will now give the **division algorithm** to divide a polynomial $f \in k[x_1,\dots,x_n]$ by a set of polynomials $F=\{f_1,\dots,f_s\} \subseteq k[x_1,\dots,x_n]$. We will see that f can be written as $f = q_1 f_1 + \dots + q_s f_s + r$, where $a_i, r \in k[x_1,\dots,x_n]$, and either $r = 0$ or r is a k-linear combination of monomials, none of which is divisible by any of $\mathrm{LT}(f_1),\dots,\mathrm{LT}(f_s)$.

The input will be a polynomial f and a set of polynomials $F=\{f_1,\dots,f_s\}$. The output will be the quotients after division $q_1,\dots,q_s$ and the remainder r.

```
Input: $f_1,...,f_s ,f$
Output: $q_1,...,q_s,r$

$q_1 := 0;...; q_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
        $i := 1$
        divisionoccurred := false
        WHILE $i \leq s$ AND divisionoccurred = false DO
                IF LT($f_i$) divides LT($p$) THEN
                        $q_i := q_i$ + LT($p$)/LT($f_i$)
                        $p := p$ - (LT($p$)/LT($f_i$)) $f_i$
                        divisionoccurred := true
                ELSE
                        $i := i + 1$
        IF divisionoccurred = false THEN
                $r := r$ + LT($p$)
                $p := p$ - LT($p$)
```

Example 1.1.6: To see how this algorithm works in practice, consider dividing $f= x^2y + 3xy - 2$ by the set of polynomials $F=\{x^2 + 3, xy - y\}$ all from $k[x,y]$. It will look like this:

$q_1 : y$
$q_2 : 3$

$$\begin{array}{lll} & & \underline{\quad r \quad .} \\ f_1 : x^2 + 3 & \overline{)x^2y+3xy-2} & \\ f_2 : xy - y & \underline{-x^2y - 3y} & \\ & \quad 3xy - 3y - 2 & \\ & \quad \underline{-3xy + 3y} & \\ & \qquad\qquad -2 & -2 \end{array}$$

So dividing polynomial f by polynomials $f_1 = x^2 + 3$ and $f_2 = xy - y$, we get $q_1 = y$, $q_2 = 3$ and a remainder $r = -2$. We stop at the -2 since neither the

LT(x^2+3)= x^2 nor the LT(xy - y) = xy divided -2 and hence the term -2 becomes the remainder. So we can say $f= q_1 f_1 + q_2 f_2 + r = (y)(x^2 + 3) + (3)(xy - y) - 2$. To see what happens if we change the order of the polynomials in F, we will divide f by F' = $\{xy - y, x^2 + 3\}$.

$$\begin{array}{ll}
q_1: & x+4 \\
q_2: & 0
\end{array}$$

$$\begin{array}{lll}
 & & \underline{\quad r \quad .} \\
f_1: xy - y & \overline{)x^2y+3xy-2} & \\
f_2: x^2+3 & \underline{-x^2y+xy} & \\
 & \quad 4xy - 2 & \\
 & \quad \underline{-4xy+4y} & \\
 & \qquad 4y - 2 & 4y - 2
\end{array}$$

Since neither $4y$ nor -2 is divisible by either LT(xy - y) or LT(x^2 + 3), both terms become the remainder $r = 4y - 2$. Also, $q_1 = x + 4$ and $q_2 = 0$ making f=$(x + 4)(xy - y) + (0)(x^2 + 3) + 4y - 2$. Notice the remainder in each division is different.

Chapter II

Problems and Objectives

Here we will be giving a little more insight into the ideal membership problem and solving systems of equations. We will discuss why these are problems and introduce some techniques for solving or simplifying these problems.

1. Ideal Membership problem

When working with polynomials in one variable, to check the membership of a polynomial f in an ideal I of $k[x]$, one can simply use the division algorithm and look at the remainder. We can do this since any ideal in one variable can be expressed as an ideal generated by one polynomial (see [c], Corollary 4,p.40). So $I = \langle g \rangle$ for some polynomial $g \in k[x]$. By definition, $\langle g \rangle = \{hg \mid h \in k[x]\}$. So for f to be in I, we would have to be able to write it as $f = hg$ for some polynomial $h \in k[x]$ and the generator g of I. In other words, f is in the ideal I if and only if f is divisible by g if and only if the remainder after division of f by g is zero. This works only because we are working in one variable making the remainder after division unique.

Example 2.1.1: Consider the ideal generated by $x + 1 \in k[x]$, or $\langle x + 1 \rangle$. A polynomial will be in the ideal if it can be written in the form $(x + 1)(h)$ for some polynomial h. So it is easy to show that $x^2 - 1$ is in the ideal since $x^2 - 1 = (x + 1)(x - 1) + 0$ but $2x^2 + 4$ is not since $2x^2 + 4 = (x + 1)(2x - 2) + 6$. Using the division algorithm, dividing $x^2 - 1$ by $x + 1$ yielded a zero remainder whereas dividing $2x^2 + 4$ by $x + 1$ yielded 6 as the remainder. Again this was made simple by the fact that the ideal was generated by one polynomial.

Example 2.1.2: Suppose we are working with polynomials in two variables and are considering the ideal generated by $x^2 + y^2 - 1$ and $xy - 1$, or $\langle x^2 + y^2 -1, xy - 1\rangle$. We would like to know if the polynomial $x^4 - x^2 +1$ is a member of the ideal. This will be true if we can write $x^4 - x^2 +1$ as $(x^2 + y^2 -1)h_1 + (xy - 1)h_2$ for some polynomials h_1 and h_2 in $k[x,y]$. So to see if $x^4 - x^2 +1$ is a member of the ideal, we must find h_1 and h_2 in $k[x,y]$ using the division algorithm. So we will divide x^4-x^2+1 by x^2+y^2-1 and $xy - 1$ in this order.

$q_1 :\ x^2 - y^2$
$q_2 :\ 0$

$$\begin{array}{lll}
 & & \underline{\quad r \quad .} \\
x^2 + y^2 - 1 & \overline{)x^4 - x^2 + 1} & \\
xy - 1 & -x^4 - x^2y^2 + x^2 & \\
 & \text{---------------} & \\
 & \quad -x^2y^2 + 1 & \\
 & \quad\ x^2y^2 + y^4 - y^2 & \\
 & \quad \text{-----------------} & \\
 & \qquad\quad y^4 - y^2 + 1 & y^4 - y^2 + 1
\end{array}$$

It may seem that $x^4 - x^2 +1$ is not in the ideal $\langle x^2 + y^2 -1, xy - 1\rangle$ since the remainder is $y^4 - y^2 + 1$ in the decomposition

$$x^4 - x^2 + 1 = (x^2 + y^2 -1)(x^2 - y^2) + (0)(xy-1) + y^4 - y^2 + 1$$

and not zero. Yet we can write

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

which has a zero remainder. To see this, switch the order of the divisors in the division algorithm.

$$\begin{array}{ll} q_1: & -xy\text{-}1 \\ q_2: & x^2 \end{array}$$

$$\begin{array}{llr}
 & & \underline{\quad r \quad .} \\
xy - 1 & \overline{)x^4 - x^2 + 1} & \\
x^2 + y^2 - 1 & -x^4 - x^2y^2 + x^2 & \\
 & \text{---------------} & \\
 & \quad - x^2y^2 + 1 & \\
 & \quad\ \ x^2y^2 - xy & \\
 & \quad \text{------------} & \\
 & \qquad\quad -xy + 1 & \\
 & \qquad\quad\ \ xy - 1 & \\
 & \qquad\quad \text{--------} & \\
 & \qquad\qquad\ 0 & 0
\end{array}$$

This shows that $x^4 - x^2 + 1 = (x^2 + y^2 - 1)h_1 + (xy-1)h_2$ for some h_1 and h_2 in $k[x,y]$ and hence is in the ideal $\langle x^2 + y^2 - 1, xy - 1\rangle$. This example shows what problems can arise when attempting to check ideal membership of a polynomial.

If we are working in $k[x_1,\ldots,x_n]$ with an ideal such as $\langle f_1,\ldots,f_s\rangle$, you might have to change the order of the generating set to check all possibilities of the remainder after division. Of course there are s! different orderings of $\{f_1,\ldots,f_s\}$ to check and one may still not find out for sure whether a polynomial f is in $\langle f_1,\ldots,f_s\rangle$.

Example 2.1.3: Consider the ideal $\langle x^2y - z, xy - 1\rangle$ in $k[x,y,z]$. The polynomial $yz - 1$ can be written as $(x^2y - z)(-y) + (xy - 1)(xy + 1)$ and is in the ideal $\langle x^2y - z, xy - 1\rangle$. Yet the division algorithm will give nonzero remainders after division on both orderings of the generators. This is because neither of the leading terms $\mathrm{LT}(x^2y\text{-}z)$ nor $\mathrm{LT}(xy\text{-}1)$ divide $\mathrm{LT}(yz\text{-}1)$. In fact, we would get $yz\text{-}1$ as the remainder.

Fortunately these ideals have more than one generating set of polynomial or basis. A nice property that a basis might have is a unique remainder after division of a polynomial by any ordering of the basis polynomials. Then we could say that a polynomial is in the ideal if and only if the remainder on division by the basis polynomials is zero. This is precisely the direction we will be heading. We will find a basis of an ideal called a Gröbner basis that has the equivalent of this special property.

2. Solving Systems of Equations

We will be concerned with systems of equations with finitely many solutions. The problem of solving a system of equations when each equation is linear can be solved by considering the row-reduced form of the matrix of coefficients of the system and using back-substitution. The problem becomes more difficult when the equations are nonlinear, however. Our method of attack for this problem will be to reduce the number of variables by using a different system of equations that will have the same solutions.

Example 2.2.1: For example, consider the system

$$2x^2 + 3y^2 - 11 = 0$$
$$x^2 - y^2 - 3 = 0$$

We will show later that this system corresponds to another system with the same solution set, namely the system

$$x^2 - 4 = 0$$
$$y^2 - 1 = 0$$

that has the solutions $x = 2, -2$, $y = 1, -1$.

To accomplish this goal, we will consider the **variety** determined by the equations of the system. In other words, if our system of equations is

$$f_1(x_1,\ldots,x_n) = 0$$
$$\vdots$$
$$f_s(x_1,\ldots,x_n) = 0$$

then the variety, $V(f_1,\ldots,f_s) = \{(a_1,\ldots,a_n) \in k^n \mid f_i(x_1,\ldots,x_n) = 0 \text{ for all } 1 \leq i \leq s\}$, is simply the set of points in k^n that satisfy the system of equations. If we also consider $\langle f_1,\ldots,f_s\rangle$, we will see that if $(a_1,\ldots,a_n)$ is a solution to $f_i(x_1,\ldots,x_n) = 0$ for all $1 \leq i \leq s$, then it is a solution to $g(x_1,\ldots,x_n) = 0$ for any polynomial g in $\langle f_1,\ldots,f_s\rangle$. The crucial observation is that since the ideal $\langle f_1,\ldots,f_s\rangle$ has more than one basis, the solutions to the system of equations will be solutions to more than one corresponding system of equations. The trick is finding a system of equations with the same solution set but a reduction in variables. We will see later that a special kind of basis of the ideal called a Gröbner basis corresponding to the system of equations will be the most helpful.

Chapter III
Development of Gröbner Bases

In order to fully solve the problems of ideal membership and solving systems of equations, we need to find a basis for an ideal with the desirable properties of producing a unique remainder and finding a corresponding system to a given system of equations with a reduction in the number of variables. Both problems can be simplified by the main ideas that every ideal in $k[x_1,...,x_n]$ has a finite basis and that there is a particular kind of basis that is the most helpful called a Gröbner basis. We will see that this kind of basis will have the properties we want. To do this, we will need to observe the correspondence between ideals, varieties and our particular goals.

1. Correspondence Between Ideals and Varieties

Using our definitions, we can make many observations about $\langle f_1,\ldots,f_s\rangle$, $V(f_1,\ldots,f_s)$ and how they relate to each other to help us get to the main goal of finding a basis of an ideal with the desired properties. Our first observation is this:

Theorem 3.1.1: 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: (i) $0 \in \langle f_1,\ldots,f_s\rangle$ since $0 = \Sigma\, 0 \cdot f_i$

(ii) Let f,g $\in \langle f_1,\ldots,f_s\rangle$. Then $f = \Sigma\, p_i f_i$ for some $p_i \in k[x_1,\ldots,x_n]$ and $g = \Sigma\, q_i f_i$ for some $q_i \in k[x_1,\ldots,x_n]$. Then $f+g = \Sigma\,(p_i + q_i)f_i$ which shows f+g $\in \langle f_1,\ldots,f_s\rangle$.

(iii) Let $h \in k[x_1,\ldots,x_n]$. $hf = \Sigma\,(hp_i)f_i$ which shows $hf \in \langle f_1,\ldots,f_s\rangle$.

By definition of an ideal, satisfying these three conditions completes the proof.

We will call $\langle f_1,\ldots,f_s\rangle$ the ideal generated by $f_1,\ldots,f_s$ and call $f_1,\ldots,f_s$ a basis for $\langle f_1,\ldots,f_s\rangle$. We mentioned before that a given ideal may have many different bases.

Example 3.1.2: Consider $\langle x,y\rangle$ and $\langle x+y, x-y\rangle$. These are the same ideal with different bases. To see this, first notice that a polynomial f in $\langle x,y\rangle$ must have the form $f = xh_1 + yh_2$ for some $h_1,h_2 \in k[x,y]$ that can be written in the form

$$f = (x+y)((h_1+h_2)/2) + (x-y)((h_1-h_2)/2)$$

which shows $f \in \langle x+y, x-y\rangle$. Conversely, if g $\in \langle x+y, x-y\rangle$, it has the form $g = (x+y)h_1 + (x-y)h_2$ that can be written as $g = x(h_1+h_2) + y(h_1-h_2)$ which shows g $\in \langle x,y\rangle$. So any polynomial f in $\langle x,y\rangle$ is also in $\langle x+y, x-y\rangle$ and any polynomial g in $\langle x+y, x-y\rangle$ is also in $\langle x,y\rangle$. Then $\langle x,y\rangle = \langle x+y, x-y\rangle$.

We can use this next helpful fact to show when two ideals are equal.

Lemma 3.1.3: Let $I \subseteq k[x_1,...,x_n]$ be an ideal and $f_1,...,f_s \in k[x_1,...,x_n]$. Then $f_1,...,f_s \in I$ if and only if $\langle f_1,...,f_s \rangle \subseteq I$.

proof: First, let $f_1,...,f_s \in I$. Choose a polynomial g in $\langle f_1,...,f_s \rangle$ where

$$g = f_1\, h_1 + ...+ f_s\, h_s$$

for some $h_1,...,h_s \in k[x_1,...,x_n]$. By definition, since I is an ideal then for $f_i \in I$ and $h_i \in k[x_1,...,x_n]$, $f_i\, h_i \in I$. Similarly, the sum $g = f_1\, h_1 + ...+ f_s\, h_s$ is in I. This shows $\langle f_1,...,f_s \rangle \subseteq I$.

Now let $\langle f_1,...,f_s \rangle \subseteq I$. We can write $f_i = 0\, f_1 +...+ 1\, f_i +...+ 0\, f_s$ which shows $f_1,...,f_s$ is in $\langle f_1,...,f_s \rangle$. But $\langle f_1,...,f_s \rangle \subseteq I$ making $f_1,...,f_s \in I$.

So to show two ideals, say $\langle f_1,...,f_s \rangle$ and $\langle g_1,...,g_t \rangle$ are equal, we only need to show $f_1,...,f_s \in \langle g_1,...,g_t \rangle$ and $g_1,...,g_t \in \langle f_1,...,f_s \rangle$. It is this property of the same ideal having more than one basis that will allow us to change the generating set without changing the ideal. When dealing with a system of polynomial equations, we can also change the polynomials of the system without changing the solutions. For this we will next consider the affine variety defined by a set of polynomials $f_1,...,f_s \in k[x_1,...,x_n]$.

For a system of equations, say

$$\begin{aligned} f_1(x_1,...,x_n) &= 0 \\ &\;\vdots \\ f_s(x_1,...,x_n) &= 0 \end{aligned}$$

we can think of the solutions to this system as the variety $V(f_1,...,f_s)$. This is because $V(f_1,...,f_s) = \{(a_1,...,a_n) \in k^n \mid f_i(a_1,...,a_n) = 0 \text{ for all } 1 \leq i \leq s\}$ that is the set of points in k^n where the polynomials $f_1,...,f_s$ vanish. So the variety of a set of polynomials is really the set of solutions to the system of polynomial equations.

We will see next how the variety $V(f_1,...,f_s)$ is related to the ideal $\langle f_1,...,f_s \rangle$.

Lemma 3.1.4: Let $f_1,...,f_s$ be polynomials in $k[x_1,...,x_n]$ and $(a_1,...,a_n) \in k^n$ be a point in $V(f_1,...,f)$. If $g \in \langle f_1,...,f_s \rangle$, then $g(a_1,...,a_n) = 0$.

proof: Let $g \in \langle f_1,...,f_s \rangle$. By definition, we can write $g = f_1 h_1 + ... + f_s h_s$ for some $h_1,...,h_s \in k[x_1,...,x_n]$. Then

$$\begin{aligned} g(a_1,...,a_n) &= f_1(a_1,...,a_n)\, h_1(a_1,...,a_n) + ... + f_s(a_1,...,a_n)\, h_s(a_1,...,a_n) \\ &= 0\ h_{1i} + ... + 0\ h_{si} \\ &= 0. \end{aligned}$$

This lemma shows that when dealing with a system of equations, we can consider the ideal generated by the polynomials of the system and see that any polynomial in the ideal generated by the system will vanish at any point in the variety determined by the system. We will make another important observation in the next theorem.

Theorem 3.1.5: If $f_1,...,f_s$ and $g_1,...,g_t$ are bases of the same ideal in $k[x_1,...,x_n]$ so that $\langle f_1,...,f_s \rangle = \langle g_1,...,g_t \rangle$, then $V(f_1,...,f_s) = V(g_1,...,g_t)$.

proof: Let $\langle f_1,...,f_s \rangle = \langle g_1,...,g_t \rangle$. Choose $(a_1,...,a_n) \in V(f_1,...,f_s)$. Then

$$f_1(a_1,...,a_n) = \ldots = f_s(a_1,...,a_n) = 0$$

by definition of variety. Since $\langle f_1,...,f_s \rangle = \langle g_1,...,g_t \rangle$, using Lemma 3.1.3, we know $g_i \in \langle f_1,...,f_s \rangle$. By Lemma 3.1.4, $g_i(a_1,...,a_n) = 0$. Then $(a_1,...,a_n) \in V(g_1,...,g_t)$ and so $V(f_1,...,f_s) \subseteq V(g_1,...,g_t)$. Similarly, we can show $V(g_1,...,g_t) \subseteq V(f_1,...,f_s)$. This proves $V(f_1,...,f_s) = V(g_1,...,g_t)$.

Example 3.1.6: To show $V(x + xy, y + xy, x^2, y^2) = V(x,y)$ in $k[x,y]$, we can now use Theorem 3.1.5 and simply show $\langle x + xy, y + xy, x^2, y^2 \rangle = \langle x,y \rangle$. Of course to prove this we can invoke lemma 3.1.3 and just show $x,y \in \langle x + xy, y + xy, x^2, y^2 \rangle$ and $x + xy, y + xy, x^2, y^2 \in \langle x,y \rangle$. Since we can write

$$x = (x + xy)(1 - y) + (y + xy)(0) + (x^2)(0) + (y^2)(x)$$

and

$$y = (x + xy)(0) + (y + xy)(1 - x) + (x^2)(y) + (y^2)(0),$$

then $x,y \in \langle x + xy, y + xy, x^2, y^2\rangle$. Similarly, we can write each of $x + xy, y + xy$, x^2, y^2 in the form $(x)(h_1) + (y)(h_2)$ for some $h_1,h_2 \in k[x,y]$ to show $x + xy, y + xy, x^2$, $y^2 \in \langle x,y\rangle$. Thus, $\langle x + xy, y + xy, x^2, y^2\rangle = \langle x,y\rangle$ by Lemma 3.1.3. Then by Theorem 3.1.5, $\mathrm{V}(x + xy, y + xy, x^2, y^2) = \mathrm{V}(x,y)$.

We could have looked at this problem as finding the solutions to these systems of equations,

$$\begin{array}{lcl} x + xy = 0 & & x = 0 \\ y + xy = 0 & \text{and} & y = 0 \\ x^2 = 0 & & \\ y^2 = 0 & & \end{array}$$

where the solutions are clearly $x = 0$ and $y = 0$. In other words, $\mathrm{V}(x + xy, y + xy, x^2, y^2) = \mathrm{V}(x,y) = \{(0,0)\}$.

Example 3.1.7: An example that is not so trivial is the system of equations in $k[x,y]$ that we considered earlier,

$$\begin{array}{l} 2x^2 + 3y^2 - 11 = 0 \\ \;\; x^2 - \;\; y^2 - 3 = 0. \end{array}$$

This can be thought of as the variety $\mathrm{V}(2x^2 + 3y^2 - 11,\ x^2 - y^2 - 3)$. One can show using lemma 3.1.3 that $\langle 2x^2 + 3y^2 - 11,\ x^2 - y^2 - 3\rangle = \langle x^2 - 4,\ y^2 - 1\rangle$ so that by theorem 3.1.5, $\mathrm{V}(2x^2 + 3y^2 - 11,\ x^2 - y^2 - 3) = \mathrm{V}(x^2 - 4,\ y^2 - 1)$ which corresponds to the system,

$$\begin{array}{l} x^2 = 4 \\ y^2 = 1 \end{array}$$

that has solutions $x = 2, -2$ and $y = 1, -1$ making these solutions to the original system of equations.

In these few examples, finding the solutions would not be that difficult. When working with *n* variables, however, the problem becomes more difficult. Our best alternative is to change the polynomials of the system to a new system of polynomials that may be easier to work with and with the same solution set.

2. Monomial Ideal and Ideal of Leading Terms

To get to our goal of finding a basis of an ideal with the properties that division of a polynomial f by the basis polynomials will give a unique remainder r and that $r = 0$ is equivalent to ideal membership, we need to define some additional concepts.

Definition 3.2.1: We define a **monomial ideal** to be an ideal I for which there is a subset A of Z^n such that I consists of all polynomials that are finite sums of the form $\Sigma_{\alpha \text{ of A}} h_\alpha x^\alpha$, where $h_\alpha \in k[x_1,\ldots,x_n]$ and we write $I = \langle x^\alpha : \alpha \in \text{A} \rangle$.

Definition 3.2.2: Let I be an ideal other than $\{0\}$. We denote **LT(I)** to be the set of leading terms of I so that $\text{LT}(I) = \{cx^\alpha \mid \text{there exists } f \in I \text{ with } \text{LT}(f) = cx^\alpha\}$. Then we can define **<LT(I)>** to be the ideal generated by the leading terms of I.

Example 3.2.3: An example of a monomial ideal is $\langle x^2y, xy^3 \rangle$ in $k[x,y]$. One property of a monomial ideal we can observe right away is that a monomial f is in a monomial ideal only if f is divisible by one of the monomial generators of the monomial ideal. For example, the monomial $f = x^2y^2$ is in $\langle x^2y, xy^3 \rangle$ since we can write $x^2y^2 = (x^2y)(y) + (xy^3)(0)$ whereas the monomial $g = xy$ is not since it is divisible by neither x^2y nor xy^3. This idea is stated in the next lemma.

Lemma 3.2.4: Let $I = \langle x^\alpha : \alpha \in \text{A} \rangle$ be a monomial ideal. Then a monomial x^β lies in I if and only if x^β is divisible by x^α for some $\alpha \in \text{A}$.

proof. Let x^β lie in I. Then $x^\beta = \Sigma h_i x^{\alpha(i)}$ for $h_i \in k[x_1,\ldots,x_n]$ and $\alpha(i) \in \text{A}$. But since x^β is a monomial and all of x^α are monomials, $\Sigma h_i x^{\alpha(i)}$ can only be one term of the form $x^\beta = hx^{\alpha(i)}$. This shows x^β is divisible by x^α for some $\alpha \in \text{A}$. If x^β is divisible by x^α for some $\alpha \in \text{A}$, say $x^\beta = (x^\alpha)(x^\gamma)$ for some x^γ, then clearly we can write x^β as a combination of the form $x^\beta = \Sigma h_i x^{\alpha(i)}$ for $h_i \in k[x_1,\ldots,x_n]$ and $\alpha(i) \in$ A.

Another observation we can make about a monomial ideal I is that if a polynomial f is in I then every term of f must lie in I and that f must be a combination of the monomials in I. This idea is given by the next lemma.

Lemma 3.2.5: Let I be a monomial ideal and let $f \in k[x_1,\ldots,x_n]$. Then the following are equivalent:

(i) $f \in I$.

(ii) Every term of f lies in I.

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

proof: Let $I = \langle x^\alpha : \alpha \in \mathrm{A} \rangle$ be a monomial ideal. If f is a k-linear combination of the monomials in I, we can write $f = \Sigma c_i x^{\alpha(i)}$ for $c_i \in k$ and $\alpha(i) \in$ A. Then each term of f, $c_i x^{\alpha(i)}$, is in I by lemma 3.2.4. Then clearly f is in I since we can write it as a combination of the monomial generators in I. This shows that (iii) implies (ii) which implies (i). We are left to show (i) implies (iii).

Let f be a polynomial in I. Then it has the form $f = \Sigma h_i x^{\alpha(i)}$ for $h_i \in k[x_1,\ldots,x_n]$ and $\alpha(i) \in$ A. We can write each $h_i x^{\alpha(i)}$ as a combination of monomials $h_i x^{\alpha(i)} = c_{1i} x^{\beta(1i)}\, x^{\alpha(i)} + \ldots + c_{ti} x^{\beta(ti)}\, x^{\alpha(i)}$. This shows every term of f can be written as $c\, x^\beta x^\alpha = c\, x^{(\alpha+\beta)}$ for some $c \in k$ and $\beta, \alpha \in k^n$. Thus, f is a k-linear combination of the monomials in I.

By our definition of monomial ideals, we could possibly have an infinite number of monomials that generate the ideal. With the help of Lemma 3.2.4 and Lemma 3.2.5, we can easily determine what type of polynomials are in a monomial ideal. We now an important theorem that will help us characterize monomial ideals as finitely generated ideals.

Theorem 3.2.6 (Dickson's Lemma): A monomial ideal

$$I = \langle x^{\alpha} : \alpha \in A \rangle \subseteq k[x_1,\ldots,x_n]$$

can be written in the form $I = \langle x^{\alpha(1)},\ldots,x^{\alpha(s)} \rangle$, where $\alpha(1),\ldots,\alpha(s) \in A$.

proof: See [c], p.70, for proof of Theorem 3.2.6.

Given any monomial ideal, we can find a finite basis of the ideal by Dickson's Lemma. This will become very important when trying to find a basis for any ideal.

Now consider $\langle \mathrm{LT}(I) \rangle$ for an ideal $I \subseteq k[x_1,\ldots,x_n]$. By definition, $\langle \mathrm{LT}(I) \rangle$ is the ideal of the leading terms of all the polynomials in an ideal I. (Recall that $\mathrm{LT}(f)$ is the leading term of a polynomial f.) The key here is that $\mathrm{LT}(f)$ is a monomial with a nonzero coefficient from k. So we will see by the next theorem that $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal.

Theorem 3.2.7: Let $I \subseteq k[x_1,\ldots,x_n]$ be an ideal.

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

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

proof: (i) For I to be a monomial ideal, it has to be generated by monomials. The ideal $\langle \mathrm{LT}(I) \rangle$ is generated by monomials with coefficients from k. By definition, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) \mid g \in I\text{-}\{0\} \rangle$. So to show that I is a monomial ideal, we can simply show $\langle \mathrm{LT}(g) \mid g \in I - \{0\} \rangle = \langle \mathrm{LM}(g) \mid g \in I - \{0\} \rangle$. For this, we must show

$$\mathrm{LT}(g_i) \in \langle \mathrm{LM}(g) \mid g \in I - \{0\} \rangle$$

and

$$\mathrm{LM}(g_i) \in \langle \mathrm{LT}(g) \mid g \in I - \{0\} \rangle.$$

We know $\mathrm{LT}(g_i) = \mathrm{LC}(g_i)\,\mathrm{LM}(g_i)$ which shows it is in the ideal $\langle \mathrm{LM}(g) \mid g \in I - \{0\} \rangle$. Also we can write $\mathrm{LM}(g_i) = (1/\mathrm{LC}(g_i))\,\mathrm{LT}(g_i)$ which shows it is in the ideal $\langle \mathrm{LT}(g) \mid g \in I - \{0\} \rangle$. So by Lemma 3.1.3,

$$\langle \mathrm{LT}(g) \mid g \in I - \{0\} \rangle = \langle \mathrm{LM}(g) \mid g \in I - \{0\} \rangle.$$

Because $\mathrm{LM}(g_i)$ is a monomial, $\langle \mathrm{LT}(I) \rangle$ is a monomial ideal.

(ii) Since <LT(I)> is a monomial ideal, by Theorem 3.2.6 we know it is finitely generated by monomials so that <LT(I)> = $\langle x^{\alpha(1)},\dots,x^{\alpha(t)}\rangle$, for some $\alpha \in Z^n$. Then each one of $x^{\alpha(1)},\dots,x^{\alpha(t)}$ is in <LT(I)> which implies that each of $x^{\alpha(1)},\dots,x^{\alpha(t)}$ is a leading monomial for some polynomials $g_1,\dots,g_t \in I$. Then the monomials $x^{\alpha(1)},\dots,x^{\alpha(t)}$ are of the form LM(g) for some g $\in I$. This shows <LT(I)> = <LM(g_1),...,LM(g_t)> . We saw in the previous paragraph that

$$\langle \mathrm{LM}(g) \mid g \in I - \{0\} \rangle = \langle \mathrm{LT}(g) \mid g \in I - \{0\} \rangle.$$

Then <LT(I)> = <LT(g_1),...,LT(g_t)>.

Using this theorem, there are some important observations we can make about monomial ideals. If an ideal I is a monomial ideal, by Theorem 3.2.6, it has a finite basis of monomials. Consider the monomial ideal $\langle x^{\alpha(1)},\dots,x^{\alpha(s)}\rangle$ where $x^{\alpha(1)},\dots,x^{\alpha(s)}$ are monomials. By Lemma 3.2.5, every polynomial f in $\langle x^{\alpha(1)},\dots,x^{\alpha(s)}\rangle$ will be of the form $f = c_1x^{\alpha(1)}x^{\beta(1)} + \dots + c_sx^{\alpha(s)}x^{\beta(s)}$ where $x^{\beta(1)},\dots,x^{\beta(s)}$ are monomials in $k[x_1,\dots,x_n]$ and $c_i \in k$. So to check the membership of a polynomial f in the ideal $\langle x^{\alpha(1)},\dots,x^{\alpha(s)}\rangle$, one would simply check each term of polynomial f to see if it is divisible by one of $x^{\alpha(1)},\dots,x^{\alpha(s)}$. Using the division algorithm to divide the polynomial f by $x^{\alpha(1)},\dots,x^{\alpha(s)}$, we would get a remainder of zero if $f \in \langle x^{\alpha(1)},\dots,x^{\alpha(s)}\rangle$.

Example 3.2.8: Consider the monomial ideal $\langle x^3y^2, x^2y^4, xy^5\rangle$. Let us use the division algorithm to divide $f = x^4y^2 + x^4y^4 + 2x^2y^5 + 4x^2y^4 + xy^5$ by x^3y^2, x^2y^4, and xy^5.

q_1: $x + xy^2$
q_2: $2y + 4$
q_3: 1

$$\begin{array}{lll}
 & & r \\
x^3y^2 & \big)\overline{x^4y^2 + x^4y^4 + 2x^2y^5 + 4x^2y^4 + xy^5} & \text{------------} \\
x^2y^4 & x^4y^2 & \\
xy^5 & \text{-------------------} & \\
 & \quad x^4y^4 + 2x^2y^5 + 4x^2y^4 + xy^5 & \\
 & \quad x^4y^4 & \\
 & \quad \text{-----------------------------} & \\
 & \qquad 2x^2y^5 + 4x^2y^4 + xy^5 & \\
 & \qquad 2x^2y^5 & \\
 & \qquad \text{------------------------} & \\
 & \qquad\quad 4x^2y^4 + xy^5 & \\
 & \qquad\quad 4x^2y^4 & \\
 & \qquad\quad \text{-----------------} & \\
 & \qquad\qquad xy^5 & \\
 & \qquad\qquad xy^5 & \\
 & \qquad\qquad \text{----------} & \\
 & \qquad\qquad\quad 0 & 0
\end{array}$$

We came up with a remainder of zero making

$$f = x^4y^2 + x^4y^4 + 2x^2y^5 + 4x^2y^4 + xy^5 \in \langle x^3y^2, x^2y^4, xy^5\rangle.$$

Again, each term of f is divisible by one of x^3y^2, x^2y^4 or xy^5.

Notice that in each step of the division process each term of the polynomial f was canceled out without introducing any other terms into what remained. Using any order of the divisors, one can check that the division algorithm will yield a zero remainder for this example. This is exactly the desirable property we are looking for given any ideal. We were looking for a generating set of an ideal that would return a unique remainder after division of a polynomial by the generating set of the ideal. We will see with the help of the next proposition that every monomial ideal has this property. Given an ideal, in Theorem 3.2.7 we saw the existence of $g_1,\dots,g_t \in I$ such that $\langle\mathrm{LT}(I)\rangle = \langle\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_t)\rangle$. The observation we might make that is particular for monomial ideals is that if we have a monomial ideal I, then the ideal of leading terms $\langle \mathrm{LT}(I) \rangle$ is the same as the ideal I itself.

Proposition 3.2.9: If $I \subseteq k[x_1,\dots,x_n]$ is a monomial ideal, then $\langle \mathrm{LT}(I) \rangle = I$.

proof: Using Theorem 3.2.6, Dickson's Lemma, we can write $I = \langle x^{\alpha(1)},\dots,x^{\alpha(s)} \rangle$ for some monomials $x^{\alpha(1)},\dots,x^{\alpha(s)} \in k[x_1,\dots,x_n]$. By Theorem 3.2.7, $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_t) \rangle$ for some $g_1,\dots,g_t \in k[x_1,\dots,x_n]$. By Lemma 3.2.5, each of the $\mathrm{LT}(g_1),\dots,\mathrm{LT}(g_t)$ is divisible by one of $x^{\alpha(1)},\dots,x^{\alpha(s)}$ since $g_i \in \langle x^{\alpha(1)},\dots,x^{\alpha(s)} \rangle$, a monomial ideal where every polynomial g is a k-linear combination of $x^{\alpha(1)},\dots,x^{\alpha(s)}$. This means every term of g_i is divisible by one of $x^{\alpha(1)},\dots,x^{\alpha(s)}$ including $\mathrm{LT}(g_i)$. This means $\mathrm{LT}(g_i) \in \langle x^{\alpha(1)},\dots,x^{\alpha(s)} \rangle$. This shows $\langle \mathrm{LT}(I) \rangle \subseteq I$.

Also, $x^{\alpha(i)} = \mathrm{LT}(x^{\alpha(i)})$ since it is a monomial implying $x^{\alpha(i)} \in \langle \mathrm{LT}(I) \rangle$. Then $I \subseteq \langle \mathrm{LT}(I) \rangle$. Now we have $I = \langle \mathrm{LT}(I) \rangle$.

From this theorem, we can see that if an ideal I is a monomial ideal then the ideal of leading terms $\langle \mathrm{LT}(I) \rangle$ will be the same as the ideal itself. Notice that this implies that for a monomial ideal $I = \langle g_1,\dots,g_t \rangle$ where $g_1,\dots,g_t$ are monomials, then $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1),\dots,\mathrm{LT}(g_t) \rangle$. We will see that this is exactly the property we want out of our basis of an ideal.

Also see that the leading term of any element of I is divisible by one of $x^{\alpha(1)},\dots,x^{\alpha(s)}$. We know for any polynomial f, we can consider each term of f to be divisible or not divisible by one of $x^{\alpha(1)},\dots,x^{\alpha(s)}$. If each term is divisible by one of $x^{\alpha(1)},\dots,x^{\alpha(s)}$, then $f \in \langle x^{\alpha(1)},\dots,x^{\alpha(s)} \rangle$ by definition. If there are terms of f that are not divisible by any of $x^{\alpha(1)},\dots,x^{\alpha(s)}$, then those terms will become terms of the remainder after division of f by any order of $x^{\alpha(1)},\dots,x^{\alpha(s)}$ which shows the remainder on division is unique. So for monomial ideals, we can say that a polynomial $f \in \langle x^{\alpha(1)},\dots,x^{\alpha(s)} \rangle$ if and only if the remainder after division of f by any order of $x^{\alpha(1)},\dots,x^{\alpha(s)}$ is zero.

3. Hilbert Basis Theorem and Gröbner Bases

We have not yet completely solved the ideal membership problem. We have seen that if an ideal I is a monomial ideal, we can easily check membership of a polynomial f in the ideal. One of the reasons we can do this is because we were able to find a finite basis for a monomial ideal. Let us suppose that we want to check membership of a polynomial f in any given ideal of $k[x_1,\ldots,x_n]$. If we are working with an ideal defined by an infinite number of polynomials, how can we check ideal membership? Fortunately, we will see that for any ideal, there is a finite basis.

Theorem 3.3.1(Hilbert Basis Theorem): Every ideal $I \subseteq k[x_1,\ldots,x_n]$ has a finite generating set or basis. Thus, $I = \langle g_1,\ldots,g_t \rangle$ for some $g_1,\ldots,g_t \in I$.

proof: By Theorem 3.2.7, there are polynomials $g_1,\ldots,g_t \in I$ such that $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t) \rangle$. We will show $I = \langle g_1,\ldots,g_t \rangle$.

By Lemma 3.1.3, $\langle g_1,\ldots,g_t \rangle \subseteq I$ since each of $g_1,\ldots,g_t \in I$. Now let $f \in I$. By applying the division algorithm, dividing f by $g_1,\ldots,g_t$ will give $f = a_1g_1, + \ldots + a_tg_t + r$ where every term of polynomial r is divisible by none of $\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)$. We will see that $r = 0$. We know $r = f - a_1g_1, + \ldots + a_tg_t \in I$ since $f, g_1,\ldots,g_t \in I$. Suppose r is not equal to zero. Then $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle$ since $r \in I$. But $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(\mathrm{g}_1),\ldots,\mathrm{LT}(\mathrm{g}_t) \rangle$ making $\mathrm{LT}(r) \in \langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t) \rangle$ which makes $\mathrm{LT}(r)$ divisible by one of $\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)$ by Lemma 3.2.4 (Remember $\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)$ and $\mathrm{LT}(r)$ are all monomials). This contradicts the fact that r cannot be divisible by any of $\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)$. So $r = 0$. Then $f = a_1g_1 + \ldots + a_tg_t \in \langle g_1,\ldots,g_t \rangle$ by definition making $I \subseteq \langle g_1,\ldots,g_t \rangle$. Thus $I = \langle g_1,\ldots,g_t \rangle$.(Taken from [c], Theorem 4, p.75)

So now for any ideal I, we can talk about a finite basis $g_1,\ldots,g_t$ of I. Unlike the case of a monomial ideal, however, an ideal like $\langle f_1,\ldots,f_s \rangle$ where $f_1,\ldots,f_s$ are not all monomials will not always have the property that $\langle \mathrm{LT}(f_1),\ldots,\mathrm{LT}(f_s) \rangle = \langle \mathrm{LT}(I) \rangle$.

Example 3.3.2: Consider the ideal $I = \langle x^2y - x, xy^2 + 2\rangle$. We can see that

$$f = -2x^3 - x^2 = (x^2y - x)(x^2y + x) + (xy^2 + 2)(-x^3) \in \langle x^2y - x, xy^2 + 2\rangle.$$

We know $\mathrm{LT}(-2x^3 - x^2) = -2x^3 \in \langle \mathrm{LT}(I)\rangle$ by definition. Yet, $-2x^3$ is not in the ideal $\langle \mathrm{LT}(x^2y - x), \mathrm{LT}(xy^2 + 2)\rangle = \langle x^2y, xy^2\rangle$ by Lemma 3.2.5 since $-2x^3$ is not a k-linear combination of x^2y and xy^2.

We saw that the property that $\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$ for an ideal I played a key role in showing that a basis of a monomial ideal has the desirable properties we are looking for. Then it might be in our interest to give any set of basis polynomials $g_1,\ldots,g_t \in I$ with this special property a special name.

Definition 3.3.3: A finite subset $G = \{g_1,\ldots,g_t\}$ of an ideal I that has the property that $\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$ is said to be a **Gröbner basis**.

Corollary 3.3.4: Every ideal $I \subseteq k[x_1,\ldots,x_n]$ other than $\{0\}$ has a Gröbner basis. Also, any Gröbner basis of I is a basis of I.

proof: From the proof of the Hilbert Basis theorem, we constructed a finite generating set $g_1,\ldots,g_t$ of an ideal I such that $\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$. Thus, the set $g_1,\ldots,g_t$ is a Gröbner basis of I. Since $I = \langle g_1,\ldots,g_t\rangle$, then $g_1,\ldots,g_t$ is a basis of I.

So now, using the Hilbert Basis theorem, we have found that any ideal $I \subseteq k[x_1,\ldots,x_n]$ has a finite basis of polynomials $g_1,\ldots,g_t$ with the property that $\langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle = \langle \mathrm{LT}(I)\rangle$. Now we must find how this property will help with our goals. Our goal was to find a basis of an ideal I that had the property that the remainder r on division of a polynomial f by the basis polynomials is unique. From this, we would be able to show that $f \in I$ if and only if $r = 0$.

Theorem 3.3.5: Let G = $\{g_1,...,g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1,...,x_n]$ and let $f \in k[x_1,...,x_n]$. Then there is a unique $r \in k[x_1,...,x_n]$ with the following two properties:

(i) No term of r is divisible by one of LT(g_1),...,LT(g_t).

(ii) There is a polynomial $q \in I$ such that $f = q + r$.

proof: From the division algorithm, we can divide f by $g_1,...,g_t$ to get

$$f = a_1 g_1 + ... + a_t g_t + r$$

where no term of r is divisible by one of LT(g_1),...,LT(g_t) establishing (i). Setting $q = a_1 g_1 + ... + a_t g_t$ establishes (ii). This proves existence of r.

To prove uniqueness, suppose that $f = q_1 + r_1 = q_2 + r_2$ satisfy (i) and (ii). Then $r_2 - r_1 = q_1 - q_2 \in I$, so that if r_1 is not equal to r_2, then

$$\text{LT}(r_2 - r_1) \in \langle\text{LT}(I)\rangle = \langle\text{LT}(g_1),...,\text{LT}(g_t)\rangle.$$

Then by Lemma 3.2.4, LT$(r_2 - r_1)$ is divisible by some LT(g_i). This is impossible since no term of r_1, r_2 is divisible by one of LT(g_1),...,LT(g_t). Then $r_2 - r_1 = 0$ meaning $r_2 = r_1$.(Taken from [c], Proposition 1, p.81)

Now we know that for any ideal $I \subseteq k[x_1,...,x_n]$, we can find a Gröbner basis of the ideal such that dividing a polynomial f by the basis polynomials will give a unique remainder. Next, we will see that a Gröbner basis enjoys the property that we have been looking for in a basis of an ideal.

Corollary 3.3.6: Let G = $\{g_1,...,g_t\}$ be a Gröbner basis for an ideal $I \subseteq k[x_1,...,x_n]$ and let $f \in k[x_1,...,x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.

proof: If the remainder is zero, we know we can write $f = a_1 g_1 + ... + a_t g_t$ which shows $f \in I$. If $f \in I$, by Theorem 3.3.5, we can write $f = q + r$ or specifically $f = f +$ 0 which shows the remainder is zero.

4. Buchberger's Algorithm

We know that for any ideal $I \subseteq k[x_1,\dots,x_n]$, we can find a Gröbner basis for the ideal. Just knowing the existence of a Gröbner basis will far from solve our problem of ideal membership. What we really would like to know is how to tell if a basis of an ideal is a Gröbner basis and, if it is not, how to find one.

Example 3.4.1: Consider the ideal $I = \langle x^2y\text{-}z, xy\text{-}1\rangle$ from example 2.1.3 where we showed that $f = yz\text{-}1 \in I$ yet each remainder after division by both orderings of the polynomials $x^2y\text{-}z$ and $xy\text{-}1$ was nonzero. Obviously the basis $\{x^2y\text{-}z, xy\text{-}1\}$ is not a Gröbner basis. Considering this problem very carefully, we see that neither of the leading terms $\mathrm{LT}(x^2y\text{-}z)$ nor $\mathrm{LT}(xy\text{-}1)$ divided $\mathrm{LT}(yz\text{-}1)$. Thus, we will get a nonzero remainder.

The approach we will take to solve this problem is to realize that for a basis of an ideal I, we can add any other element of I to the basis and have the same ideal. In other words, for an ideal $I = \langle f_1,\dots,f_s\rangle$ and polynomial g $\in I$, then $\langle f_1,\dots,f_s\rangle = \langle f_1,\dots,f_s,g\rangle$. This is clear by Lemma 3.1.3 since each of $f_1,\dots,f_s \in \langle f_1,\dots,f_s,g\rangle$ and each of $f_1,\dots,f_s,g \in \langle f_1,\dots,f_s\rangle$.

For the basis $\{x^2y\text{-}z, xy\text{-}1\}$, we might like to add a polynomial of $\langle x^2y\text{-}z, xy\text{-}1\rangle$ with a leading term that divides $\mathrm{LT}(yz\text{-}1)$ so that we could at least start dividing $yz\text{-}1$ by the basis so that we would not get $yz\text{-}1$ as the remainder. One way to find such a polynomial of $\langle x^2y\text{-}z, xy\text{-}1\rangle$ with such a leading term would be to take a combination of $x^2y\text{-}z$ and $xy\text{-}1$ that cancels the higher exponents in the leading terms. To do this in general, we define the following.

Definition 3.4.2: Let f,g $\in k[x_1,\dots,x_n]$ be nonzero polynomials. Let G = $(g_1,\dots,g_t)$ be an ordered t-tuple of polynomials in $k[x_1,\dots,x_n]$.

(i) If deg(f) = α and deg(g) = β, then set $\gamma = (\gamma_1,\ldots,\gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i. We will denote x^γ = LCM(LM(f),LM(g)) as the least common multiple of LM(f) and LM(g). The **S-polynomial** of f and g is the combination

$$S(f,g) = [(f\,x^\gamma)/\mathrm{LT}(f)] - [(g\,x^\gamma)/\mathrm{LT}(g)].$$

(ii) We will denote **rem(f)^G** to be the remainder on division of f by G.

Example 3.4.3: To help us with the problem above, let us compute the S-polynomial for the polynomials x^2y-z and xy-1.

$x^\gamma = \mathrm{LCM}(\mathrm{LM}(x^2y\text{-}z),\mathrm{LM}(xy\text{-}1)) = \mathrm{LCM}(x^2y,xy) = x^2y$

$\mathrm{LT}(x^2y\text{-}z) = x^2y$

$\mathrm{LT}(xy\text{-}1) = xy$

$$\begin{aligned} S(x^2y\text{-}z,xy\text{-}1) &= [(x^2y)(x^2y\text{-}z)/(x^2y) - (x^2y)(xy\text{-}1)/(xy)] \\ &= (x^2y\text{-}z) - (x)(xy\text{-}1) \\ &= x - z \end{aligned}$$

Note that the S-polynomial of f and g will always be in an ideal with f and g in the basis. This is because the S-polynomial of f and g is written in the form $S(f,g) = f\,h_1 + gh_2$ for $h_1 = x^\gamma/\mathrm{LT}(f)$ and $h_2 = -\,x^\gamma/\mathrm{LT}(g)$. (Remember that x^γ is divisible by both LT(f) and LT(g) making h_1 and $h_2 \in k[x,y,z]$).

We noted earlier that we could add a polynomial of an ideal to the basis of an ideal and have the same generating set. Applying this to the example above, let us add the polynomial x-z to the basis x^2y-z and xy-1 of the ideal $\langle x^2y\text{-}z,xy\text{-}1\rangle$. We can show that $\langle x^2y\text{-}z,xy\text{-}1\rangle = \langle x^2y\text{-}z,xy\text{-}1,x\text{-}z\rangle$ using Lemma 3.1.3 since each basis polynomial is in each ideal. Still the problem with our example is not solved since the leading term of the S-polynomial x-z does not divide the leading term of yz-1.

Example 3.4.3(cont.): We will see what happens if we compute the S-polynomial of x^2y-z and x-z and the S-polynomial of xy-1 and x-z.

For x^2y-z and x-z:

$$x^\gamma = \mathrm{LCM}(\mathrm{LM}(x^2y-z),\mathrm{LM}(x-z)) = \mathrm{LCM}(x^2y,x) = x^2y$$
$$\mathrm{LT}(x^2y-z) = x^2y$$
$$\mathrm{LT}(x-z) = x$$

$$\begin{aligned} S(x^2y-z,x-z) &= [(x^2y)(x^2y-z)/(x^2y) - (x^2y)(x-z)/(x)] \\ &= (x^2y-z) \ - \ (xy)(x-z) \\ &= xyz - z \end{aligned}$$

For xy-1 and x-z:

$$x^\gamma = \mathrm{LCM}(\mathrm{LM}(xy-1),\mathrm{LM}(x-z)) = \mathrm{LCM}(xy,x) = xy$$
$$\mathrm{LT}(xy-1) = xy$$
$$\mathrm{LT}(x-z) = x$$

$$\begin{aligned} S(xy-1,x-z) &= [(xy)(xy-1)/(xy) - (xy)(x-z)/(x)] \\ &= (xy-1) \ - \ (y)(x-z) \\ &= yz - 1 \end{aligned}$$

Since these S-polynomials are in the ideal $\langle x^2y-z,xy-1,x-z\rangle$, we can add these to the basis to get $\langle x^2y-z,xy-1,x-z\rangle = \langle x^2y-z,xy-1,x-z,xyz-z,yz-1\rangle$. Notice that in our original example we knew that the polynomial yz-1 $\in \langle x^2y-z,xy-1\rangle$ yet dividing yz-1 by the basis polynomials x^2y-z and xy-1 gave a nonzero remainder for each order of the basis.

Now that we know $\langle x^2y-z,xy-1\rangle = \langle x^2y-z,xy-1,x-z\rangle = \langle x^2y-z,xy-1,x-z,xyz-z,yz-1\rangle$ using Lemma 3.1.3, we can use the basis polynomials x^2y-z,xy-1,x-z,xyz-z and yz-1 instead in the division algorithm. Of course, since yz-1 is in the new basis we know we can divide yz-1 by at least one of the basis elements. We will see in the next theorem a criterion for when a basis of an ideal is a Gröbner basis.

Theorem 3.4.4: Let I be a polynomial ideal. Then a basis G = $\{g_1,\dots,g_t\}$ for I is a Gröbner basis for I if and only if for all pairs i not equal to j, $\mathrm{rem}(S(g_i,g_j))^G = 0$ (G in some order).

proof: See [c], Theorem 6, p.84 for the proof of Theorem 3.4.4.

Example 3.4.3(cont.): For the basis $x^2y\text{-}z,xy\text{-}1,x\text{-}z,xyz\text{-}z$ and $yz\text{-}1$ of the ideal $\langle x^2y\text{-}z,xy\text{-}1,x\text{-}z,xyz\text{-}z,yz\text{-}1\rangle$ in our example above, to see if it is a Gröbner basis, we would compute the S-polynomial for each pair of basis polynomials and check to see if the remainders after division of the S-polynomials were all *zero*. Let us do this now.

$S(x^2y\text{-}z,xy\text{-}1) = x\text{-}z$
$S(x^2y\text{-}z,x\text{-}z) = xyz\text{-}z$
$S(x^2y\text{-}z,xyz\text{-}z)= xz\text{-}z^2$
$S(x^2y\text{-}z, yz\text{-}1)= x^2\text{-}z^2$
$S(xy\text{-}1,x\text{-}z)= yz\text{-}1$
$S(xy\text{-}1, xyz\text{-}z)= 0$
$S(xy\text{-}1 , yz\text{-}1)= x\text{-}z$
$S(x\text{-}z,xyz\text{-}z)= \text{-}yz^2+z$
$S(x\text{-}z, yz\text{-}1)= x\text{-}yz^2$
$S(xyz\text{-}z, yz\text{-}1) = x\text{-}z$

Computing remainders on division of each of the S-polynomials by the basis polynomials $G = (x^2y\text{-}z,xy\text{-}1,x\text{-}z,xyz\text{-}z,yz\text{-}1)$, we will get zero as the remainder for each S-polynomial. This shows that the basis $G = (x^2y\text{-}z,xy\text{-}1,x\text{-}z,xyz\text{-}z,yz\text{-}1)$ is a Gröbner basis by Theorem 3.4.4. This idea can be formalized into an algorithm that, given a basis of an ideal *I*, will produce a Gröbner basis.

Theorem 3.4.5(Buchberger's Algorithm): Let $I = \langle f_1,\ldots,f_s\rangle$ where *I* is not {0} be a polynomial ideal. Then a Gröbner basis for *I* can be constructed in a finite number of steps by the following algorithm:

Input: $F = (f_1,\ldots,f_s)$
Output: Gröbner basis $G = (g_1,\ldots,g_t)$ for *I* with $F \subseteq G$

```
G := $F$
REPEAT
        G' := G
        FOR each pair $\{p,q\}$, $p \neq q$ in G' DO
                S := rem(S($p,q$))$^{G'}$
                IF S $\neq 0$ THEN G := G $\cup$ {S}
UNTIL G = G'
```

proof: We must show that the new ideal $\langle g_1,\ldots,g_t\rangle = I$ and G = $(g_1,\ldots,g_t)$ is a Gröbner basis of I and that the algorithm terminates.

First, through each loop in the algorithm, we are simply adding the remainders of the S-polynomials after division by the expanding set G' which at the beginning is the original basis. So each remainder is an element of I making G' = $(g_1,\ldots,g_t)$ a basis of I. This shows $I = \langle f_1,\ldots,f_s\rangle = \langle g_1,\ldots,g_t\rangle$.

Next, the algorithm terminates when G = G' making rem(S(p,q))$^{G} = 0$ for all $p,q \in$ G. By Theorem 3.4.4, G is a Gröbner basis.

Finally, through each pass in the main loop, G $\subset$G' implying that <LT(G')> $\subset$<LT(G)>. Furthermore, if G $\neq$G', then <LT(G')> is strictly smaller than <LT(G)>. To see this, suppose G$\neq$G'. Then a nonzero remainder of an S-polynomial has been added to G'. By the properties of r, none of the polynomials of G' divide the leading term of r making LT(r) not in <LT(G')>. But LT(r) is in <LT(G)>.

This shows we have an ascending chain of ideals in $k[x_1,\ldots,x_n]$. Then after a finite number of iterations, the chain will stabilize by the Ascending Chain Condition (See [v], ACC, p.117 for the theorem and proof). This says that at some point we will have <LT(G')> = <LT(G)> which implies G' = G by the above paragraph making the algorithm terminate after a finite number of iterations.

This algorithm is by no means the most efficient way to get a Gröbner basis from a basis. There are many improvements that can be made to improve the efficiency. This version is, however, one of the simplest to understand and still serves its purpose as an illustrative tool.

The main idea of the algorithm is to add polynomials of an ideal I to a basis of I in such a way as to take into consideration the remainders of the S-polynomials. Since each S-polynomial is in the ideal, then the remainder after division by the basis is in the ideal. Once we add the remainder to the basis, we are assured a zero remainder when we divide the S-polynomial by the basis. If we continue to do this for each pair of polynomials in the basis, we will eventually get a basis of the ideal that has the property that the remainder of the S-polynomial after division of the basis is zero for each pair of polynomials in the basis.

This is exactly what Buchberger's algorithm does to a basis. It computes the remainders of the S-polynomials after division of the new basis and adds the remainders if they are nonzero until finally all the remainders of the S-polynomials for every pair of polynomials in the new basis is zero.

Recall that an ideal I may have more than one basis. Then because we are simply adding polynomials to the basis to get a Gröbner basis, we can see that an ideal may have more than one Gröbner basis.

Example 3.4.6: Consider the Gröbner basis G = $(x^2y\text{-}z, xy\text{-}1, x\text{-}z, xyz\text{-}z, yz\text{-}1)$ of example 3.4.3. We will claim that G' = $(x\text{-}z, yz\text{-}1)$ is also a Gröbner basis of $I = \langle x^2y\text{-}z, xy\text{-}1, x\text{-}z, xyz\text{-}z, yz\text{-}1\rangle$. First, $x\text{-}z, yz\text{-}1 \in \langle x^2y\text{-}z, xy\text{-}1, x\text{-}z, xyz\text{-}z, yz\text{-}1\rangle$ since they are part of the basis. Also, $x^2y\text{-}z, xy\text{-}1, x\text{-}z, xyz\text{-}z, yz\text{-}1 \in \langle x\text{-}z, yz\text{-}1\rangle$ since

$$x^2y\text{-}z = (x\text{-}z)(xy+yz)+(yz\text{-}1)(z),$$

$$xy\text{-}1 = (x\text{-}z)(y)+(yz\text{-}1)(1),$$

$$xyz\text{-}z = (x\text{-}z)(yz)+(yz\text{-}1)(z)$$

and clearly $x\text{-}z$ and $yz\text{-}1$ are in the ideal. This shows

$$\langle x^2y\text{-}z, xy\text{-}1, x\text{-}z, xyz\text{-}z, yz\text{-}1\rangle = \langle x\text{-}z, yz\text{-}1\rangle$$

making G' = $(x\text{-}z, yz\text{-}1)$ a basis of I.

To show G' is a Gröbner basis, we will show that the remainder of the S-polynomial after division of the basis polynomials is zero.

$S(x-z,yz-1) = [(xyz)(x-z)/(x)] - [(xyz)(yz-1)/(yz)] = xyz - yz^2 - xyz + x = x-yz^2$.
$\text{rem}(x-yz^2)^{G'} = 0$.

This shows G' is a Gröbner basis.

Notice in example 3.4.6 that the Gröbner basis G' was the Gröbner basis G minus a few polynomials. A Gröbner basis of an ideal with the fewest number of generators would likely cut down on any computational work that might need to be done with a Gröbner basis of an ideal. The next few results will help with that goal.

Theorem 3.4.7: Let G be a Gröbner basis of a polynomial ideal I. Let $p \in$ G be a polynomial such that LT(p) $\in$ <LT(G-$\{p\}$)>. Then G-$\{p\}$ is also a Gröbner basis of I.

proof: Since G is a Gröbner basis, we know <LT(G)> = <LT(I)>. If LT(p) $\in$ <LT(G-$\{p\}$)>, then <LT(G-$\{p\}$)> = <LT(G)> by Lemma 3.1.3. This shows <LT(G-$\{p\}$)> = <LT(I)> which makes G-$\{p\}$ a Gröbner basis by definition.

This theorem shows that if any polynomial p in a Gröbner basis G can be written as a combination of the leading terms of the polynomials in G-$\{p\}$, then G-$\{p\}$ is a Gröbner basis. We can greatly reduce the number of basis polynomials using this theorem.

Example 3.4.8: Consider the ideal $I = \langle x^2y-z, xy-1, x-z, xyz-z, yz-1 \rangle$ from example 3.4.6 where $G = (x^2y-z, xy-1, x-z, xyz-z, yz-1\ )$ is a Gröbner basis. We can see that

$$\text{LT}(x^2y-z) = x^2y = (xy)(\text{LT}(x-z)),$$

$$\mathrm{LT}(xy\text{-}1) = xy = (y)(\mathrm{LT}(x\text{-}z))$$

and

$$\mathrm{LT}(xyz\text{-}z) = xyz = (x)(\mathrm{LT}(yz\text{-}1)).$$

Then we can say G' = (x-z,yz-1) is a Gröbner basis by Theorem 3.4.7. We already knew G' was a Gröbner basis, however, from example 3.4.6.

We can see that this Gröbner basis G' is more simple than G. We will give a Gröbner basis of this simplicity a name.

Definition 3.4.9: A **reduced Gröbner basis** for a polynomial ideal I is a Gröbner basis G for I such that:

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

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

Notice that the Gröbner basis G' = (x-z,yz-1) has these properties. The leading coefficients are both 1 and each monomial of each polynomial cannot be written as a combination of x and yz. We can now say the G' is a reduced Gröbner basis of the original ideal $\langle x^2y\text{-}z,xy\text{-}1\rangle = \langle x^2y\text{-}z,xy\text{-}1,x\text{-}z,xyz\text{-}z,yz\text{-}1\rangle = \langle x\text{-}z,yz\text{-}1\rangle$. Reduced Grobner bases can easily be computed on the computer program *Maple for Macintosh* (See [1], *gbasis* command in the Grobner basis package).

5. V(I) and the Elimination Theorem

Coming back to our problem of solving systems of equations in $k[x_1,\dots,x_n]$, we will see that we can use our results up to this point to show how this problem can be simplified. The idea is that for a system of equations

$$
\begin{aligned}
f_1(x_1,\dots,x_n) &= 0\\
&\ \vdots\\
f_s(x_1,\dots,x_n) &= 0
\end{aligned}
$$

we can consider the variety $V(f_1,\dots,f_s)$ as all the points in k^n that correspond to the solutions to the system of equations. Also, we can consider $I = \langle f_1,\dots,f_s\rangle \subseteq k[x_1,\dots,x_n]$ as the set of all polynomials that vanish at each point of $V(f_1,\dots,f_s)$ using Lemma 3.1.4. With this in mind, we can define the following.

Definition 3.5.3: Let $I \subseteq k[x_1,\dots,x_n]$. Define

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

Then using Theorem 3.1.5, we can state the following theorem.

Theorem 3.5.2: $V(I)$ is an affine variety. Also, if $I = \langle f_1,\dots,f_s\rangle$, then $V(I) = V(f_1,\dots,f_s)$.

proof: Since $f_i \in I$, if $f(a_1,\dots,a_n) = 0$ for all $f \in I$, then $f_i(a_1,\dots,a_n) = 0$. Then $V(I) \subseteq V(f_1,\dots,f_s)$. Also, let $(a_1,\dots,a_n) \in V(f_1,\dots,f_s)$ and let f $\in I$. Applying Lemma 3.1.4, $f(a_1,\dots,a_n) = 0$. Then $V(f_1,\dots,f_s) \subseteq V(I)$. This shows $V(I) = V(f_1,\dots,f_s)$.

We also saw that every ideal has a Gröbner basis. We will see that a nice basis we can change to is a Gröbner basis. For the variety of the system of equations, $V(f_1,\dots,f_s)$, we can consider $I = \langle f_1,\dots,f_s\rangle$. By the previous theorem, $V(I) = V(f_1,\dots,f_s)$. If we change $I = \langle f_1,\dots,f_s\rangle$ to $I = \langle g_1,\dots,g_t\rangle$ where $G = \{\, g_1,\dots,g_t\}$ is a Gröbner basis, we will get $V(I) = V(g_1,\dots,g_t)$. This variety can greatly reduce the problem of solving the original system of equations.

To help see this, we define the following.

Definition 3.5.3: Given $I = \langle f_1,\dots,f_s \rangle \subseteq k[x_1,\dots,x_n]$, the kth **elimination ideal** I_k is the ideal of $k[x_{k+1},\dots,x_n]$ defined by $I_k = I \cap k[x_{k+1},\dots,x_n]$.

Theorem 3.5.4(Elimination Theorem): Let $I \subseteq k[x_1,\dots,x_n]$ be an ideal and G be a Gröbner basis of I. Then, for every $0<k<n$, the set $G_k = G \cap k[x_{k+1},\dots,x_n]$ is a Gröbner basis of the kth elimination ideal I_k.

proof: See [c], Theorem 2, p.114 the proof of Theorem 3.5.4.

The kth elimination ideal I_k for an ideal $I = \langle f_1,\dots,f_s \rangle$ is the set of all polynomials of I that only have the last n-k-1 variables. By the Elimination Theorem, a basis for I_k can be the polynomials of a Gröbner basis that only have the last n-k-1 variables. Furthermore, if we choose these polynomials of a Gröbner basis as the basis of I_k, then these polynomials will also be a Gröbner basis.

Example 3.5.5: Consider the ideal $I = \langle x^2+y^2+z^2-1, z^2+y-x^2, 2y^2+x^2-1 \rangle$ in $k[x,y,z]$. Computing a reduced Gröbner basis for I, we get $I = \langle x^2+2z^2-1, y+3z^2-1, 9z^4-7z^2+1 \rangle$. We can easily find bases, particularly Gröbner bases, for the elimination ideals.

$I_1 = \langle y+3z^2-1, 9z^4-7z^2+1 \rangle$.
$I_2 = \langle 9z^4-7z^2+1 \rangle$.

The ideal I_1 is the set of all polynomials of $I = \langle x^2+y^2+z^2-1, z^2+y-x^2, 2y^2+x^2-1 \rangle$ that are also in $k[y,z]$. These are just the polynomials that are only in terms of y and z or where variable x is eliminated. By the Elimination Theorem, these polynomials can be generated by the polynomials $y+3z^2-1$ and $9z^4-7z^2+1$ which form a Gröbner basis.

Also, $I_2 = \langle 9z^4-7z^2+1 \rangle$ is the set of polynomials generated by the polynomial $9z^4-7z^2+1$. Any polynomial in the ideal $I = \langle x^2+y^2+z^2-1, z^2+y-x^2, 2y^2+x^2-1 \rangle$ that has z as its only variable will be of the form $(9z^4-7z^2+1)(h_1)$ for some $h_1 \in k[z]$.

Using the Elimination Theorem and given a Gröbner basis, we can find bases for the elimination ideals that contain all polynomials that eliminate the first k variables. Moreover, the bases given by the Elimination theorem are Gröbner bases. Particularly for our problem of solving systems of equations with finite solutions, we can compute the elimination ideal I_{n-1}, the last elimination ideal of $I \subseteq k[x_1,\ldots,x_n]$, to find a single polynomial is one variable. In example 3.5.5, the elimination ideal $I_2 = \langle 9z^4-7z^2+1 \rangle$ is the set of all polynomials generated by $9z^4-7z^2+1$. This is important since we want a finite number of solutions for a system of equations.

Once we consider the last elimination ideal I_{n-1}, we can extend the solutions to the elimination ideal I_{n-2}, then to I_{n-3} until we finally get to I. If the solutions to the original system of equations is finite, then in each elimination ideal, there will only be one variable to solve for.

Chapter IV

Conclusion

Our problems were determining the membership of a polynomial in an ideal and solving systems of equations. We set out to try to find a basis of an ideal with some special properties concerning the division algorithm. The properties we would like in a basis were to get a unique remainder on division of a polynomial f by the basis and to have fewer variables in certain polynomials of the basis. Using the ideas and results in the development of Gröbner bases, we will see how a Gröbner basis will help us with the ideal membership problem and solving systems of equations.

1. Ideal Membership Problem

From Corollary 3.3.6, we have a simple way of determining ideal membership of a polynomial f in an ideal I. We would use the division algorithm to divide f by a Gröbner basis of I and check the remainder. We observed earlier that given any basis of an ideal I the order of the polynomials of the basis was important. Now that we know there exists a basis of an ideal that returns a unique remainder on division and since we are only concerned with the remainder, the order of the basis in the division algorithm does not matter when using a Gröbner basis.

Example 4.1.1: Consider the ideal $I = \langle x^2 + y^2 -1, xy - 1\rangle$ from example 2.1.2. We were checking the membership of the polynomial $x^4 -x^2 + 1$ in the ideal I. By computing a Gröbner basis for I, we need only check the remainder after division of the polynomial $x^4 -x^2 + 1$ by the Gröbner basis polynomials. Using Corollary 3.3.6, polynomial $x^4 -x^2 + 1$ is in the ideal $I = \langle x^2 + y^2 -1, xy - 1\rangle$ if and only if the remainder is zero.

A Gröbner basis for $I = \langle x^2 + y^2 - 1, xy - 1\rangle$ is the set $\{x+y^3-y, y^4-y^2+1\}$. We can choose any order of the Gröbner basis polynomials to divide $x^4 - x^2 + 1$ by the polynomials $x+y^3-y$ and y^4-y^2+1. Doing the division, we get a remainder of zero which shows that $x^4 - x^2 + 1 \in I = \langle x^2 + y^2 - 1, xy - 1\rangle = \langle x+y^3-y, y^4-y^2+1\rangle$. We can now check the membership of a polynomial in any ideal I in $k[x_1,\ldots,x_n]$ by computing a Gröbner basis of I and using the division algorithm.

2. Solving Systems of Equations

If we have a system of equations in *n* variables, our strategy was to reduce the number of variables in certain equations. For the system

$$f_l(x_1,\ldots,x_n) = 0$$
$$\vdots$$
$$f_l(x_1,\ldots,x_n) = 0$$

we saw early that we can consider $V(f_1,\ldots,f_s)$ as the set of points in k^n that correspond to the solutions of the system of equations. Also, by Theorem 3.5.2, if we consider the ideal generated by the polynomials of the system $I = \langle f_1,\ldots,f_s \rangle$, then $V(I) = V(f_1,\ldots,f_s)$. By the properties of the Elimination Theorem, a good candidate for a different basis of I would be a Gröbner basis. If $G = \{g_1,\ldots,g_t\}$ is a Gröbner basis for I, then since $I = \langle g_1,\ldots,g_t \rangle$, then $V(I) = V(g_1,\ldots,g_t)$. The variety $V(g_1,\ldots,g_t)$ will correspond to the same solution set yet the polynomials of the new system will have a reduction of variables. This will help with solving the system.

Example 4.2.1: Consider the system of equations

$$\begin{aligned} x^2+y^2+z^2-1 &= 0 \\ -x^2+y+z^2 &= 0 \\ x^2+2y^2-1 &= 0 \end{aligned}$$

We saw in example 3.5.5, we can consider the ideal

$$I = \langle x^2+y^2+z^2-1, -x^2+y+z^2, x^2+2y^2-1 \rangle$$

and a Gröbner basis for I is $G = \{x^2+2z^2-1, y+3z^2-1, 9z^4-7z^2+1\}$ corresponding to the ideal $I = \langle x^2+2z^2-1, y+3z^2-1, 9z^4-7z^2+1 \rangle$.

Then the variety

$$V(x^2+y^2+z^2-1, -x^2+y+z^2, x^2+2y^2-1) = V(x^2+2z^2-1, y+3z^2-1, 9z^4-7z^2+1)$$

by Theorem 3.5.2. This variety corresponds to the system of equations

$$\begin{aligned} &x^2+2z^2-1=0\\ &y+3z^2-1=0\\ &9z^4-7z^2+1=0. \end{aligned}$$

We can solve for z in the last equation to find the ordered triple solutions for the system of equations (Using the computer program *Maple V for Macintosh*. See [m], *solve* command, p.17.)

$$\left(\frac{1}{3}\sqrt{2+\sqrt{13}},-\frac{1}{6}+\frac{1}{6}\sqrt{13},\frac{1}{6}-\frac{1}{6}\sqrt{13}\right) \quad \left(-\frac{1}{3}\sqrt{2+\sqrt{13}},-\frac{1}{6}+\frac{1}{6}\sqrt{13},\frac{1}{6}-\frac{1}{6}\sqrt{13}\right)$$

$$\left(\frac{1}{3}\sqrt{2+\sqrt{13}},-\frac{1}{6}+\frac{1}{6}\sqrt{13},-\frac{1}{6}+\frac{1}{6}\sqrt{13}\right) \quad \left(-\frac{1}{3}\sqrt{2+\sqrt{13}},-\frac{1}{6}+\frac{1}{6}\sqrt{13},-\frac{1}{6}+\frac{1}{6}\sqrt{13}\right)$$

$$\left(\frac{1}{3}\sqrt{2-\sqrt{13}},-\frac{1}{6}-\frac{1}{6}\sqrt{13},\frac{1}{6}+\frac{1}{6}\sqrt{13}\right) \quad \left(-\frac{1}{3}\sqrt{2-\sqrt{13}},-\frac{1}{6}-\frac{1}{6}\sqrt{13},\frac{1}{6}+\frac{1}{6}\sqrt{13}\right)$$

$$\left(\frac{1}{3}\sqrt{2-\sqrt{13}},-\frac{1}{6}-\frac{1}{6}\sqrt{13},-\frac{1}{6}-\frac{1}{6}\sqrt{13}\right) \quad \left(-\frac{1}{3}\sqrt{2-\sqrt{13}},-\frac{1}{6}-\frac{1}{6}\sqrt{13},-\frac{1}{6}-\frac{1}{6}\sqrt{13}\right)$$

We can think of these triples as the points in C^3 of

$$V(x^2+y^2+z^2-1,-x^2+y+z^2,x^2+2y^2-1) = V(x^2+2z^2-1,y+3z^2-1,9z^4-7z^2+1).$$

Also, each point (x,y,z) corresponds to a solution to the original system of equations. From this example, we can see that solving a system of equations can be simplified using a Gröbner basis.

References

[c] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, New York, 1991.

[l] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan, and S.W. Watt. *Maple V Library Reference Manual*. Springer-Verlag, New York, 1991.

[m] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan, and S.W. Watt. *Maple V First Leaves: A Tutorial Introduction to Maple V*. Springer-Verlag, New York, 1991.

[v] B.L. van der Waerden. *Algebra*. Springer-Verlag, New York, 1991.

I, Eugene A. Dixon, hereby submit this thesis to Emporia State University as partial fulfillment of the requirements for an advanced degree. I agree that the Library of the University may make it available for use in accordance with its regulations governing materials of this type. I further agree that quoting, photocopying, or other reproduction of this document is allowed for private study, scholarship (including teaching) and research purposes of a nonprofit nature. No copying which involves potential financial gain will be allowed without written permission of the author.

Eugene A. Dixon
Signature of Author

May 5, 1995
Date

Grobner Bases
Title of Thesis

Dary Cooper
Signature of Graduate Office Staff Member

May 12, 1995
Date Received

original