ADDIS ABABA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

DEPARTMENT OF MATHEMATICS

GRADUTE SEMINAR REPORT

ON

GROEBNER BASES

(Submitted in partial fulfillment of M.Sc.Degree in Mathematics)

Compiled by : Kebede Alemu

June,2010

Addis Ababa

Table of contents

Contentes	Page
Acknowledgments	ii
Intoduction	1
CHAPTER ONE	2
1.1 Polynomials and Affine Space	2
1.2 *Affine Varieties*	*4*
1.3 Parameterization of Affine Varieties	*9*
1.4 Ideals	14
CHAPTER TWO	18
2.1 Introduction	18
2.2 Ordering on The Monomials in K $[x_1,x_2,---x_n]$	21
2.3 A Division Algorithm in K $[x_1,\ldots,x_n]$	24
2.4 Monomial Ideals and Dickson's Lemma	26
2.5 The Hilbert Basis Theorem and Groebner Bases	28
2.6 Properties of Groebner Bases	31
2.7 Buchberger's Algorithm	36
2.8 *First Applications of Groebner Bases*	*39*
References	42

ACKNOWLEDGMENTS

First and above all I thank the almighty God for his provision and protection in all aspects of my life.

Next, I would like to express my heart felt apperciation to my advisor Dr. Tilahun Abebaw for his constructive comments, suggestions, valuable advices and generous hospitality in preparing the report.

I am also grateful to the department of Mathematics for providing departmental facilities.

Introduction

The theory of Grőbner basis is a corner stone of computer algebra which has also found (often unexpected) applications to a wide spectrum of areas in science and engineering .All major computer algebra systems offer Grőbner basis functionalities and powerful stand alone implementation are also available.

Grőbner bases for ideals in polynomial rings were introduced in 1965 G.C by B. Buchberger and named by him in honour of W. Grobner (1899- 1980), Buchberger thesis advisor .The closely related concept of standard bases for ideals in power series rings was discovered independently in 1964 by H.Hisonaka. As we see later in the seminar report ,Buchburger also developed the fundamental algorithm for working with Groebner bases .We use the English form "Groebner basis'' since this is how the command is spelled in some computer algebra systems.

CHAPTER ONE

Geometry, Algebra, and Algorithms.

Introduction:-

In this chapter we introduce some of the basic themes of this seminar report. The geometry we are interested in concerns affine varieties which are curves and surfaces (and higher dimensional objects) defined by polynomial equations. To understand **affine** varieties we need some algebra, and in particular, we need ideals in the polynomial ring $K[x_1,x_2, \dots ,x_n]$.

1.1 Polynomials and Affine space.

To link algebra and geometry, we study polynomials over a field. One reason that fields are important is that linear algebra works over any field. Thus even if the linear algebra course restricted the scalars to lie in $\mathbb{R}$ or$\mathbb{C}$, most of the theorems and techniques apply to an arbitrary field K. The most commonly used fields are:-

- The rational numbers $\mathbb{Q}$ the field for most of computer examples.
- The real numbers$\mathbb{R}$, the field for drawing pictures of curves and surfaces.
- The complex numbers$\mathbb{C}$, the field for proving many of our theorems.

Definition1.1.1:- A monomial in $x_1,\dots,x_n$ is a product of the form $x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$, where all of the exponents $\alpha_1, \alpha_2,\dots, \alpha_n$ are non negative integers. The total degree of this monomial is the sum $\alpha_1+ \alpha_2 +\dots+\alpha_n$.

We can simplify the notation for monomials as follows. Let $\alpha = (\alpha_1, \alpha_2,\dots, \alpha_n)$ be an n-tuple of non negative integers .Then we set $x^{\alpha}= x_1^{\alpha_1} x_2^{\alpha_2}\dots x_n^{\alpha_n}$ and when $\alpha = (0, 0, \dots ,0)$ note that $x^{\alpha} = 1$ .We also denote $|\alpha| = \alpha_1+ \alpha_2 +\dots+\alpha_n$, denote the total degree of the monomial x^{α}.

Definition1.1.2:- A polynomial f in $x_1, x_2,\dots,x_n$ with coefficient in K is a finite linear combination (with coefficient in K) of monomials. We write a polynomial of in the form

$f =\sum_{\alpha} a_{\alpha}x^{\alpha}$ $a_{\alpha}\epsilon$ K, where the sum is over a finite number of n-tuple, $\alpha = (\alpha_1, \alpha_2,\dots, \alpha_n)$. The set of all polynomial in $x_1,\dots,x_n$ with coefficients in K is denoted $K[x_1,\dots,x_n]$.

When dealing with polynomials in a small number of variables, we will usually dispense with subject subscripts. Thus, polynomials in one, two and three variables lie in K[x] ,K[x, y] and K[x, y, z] respectively.

***Example 1.1.1*:-** $f= 2x^3y^2z + \frac{3}{2} y^3z^3 - 3xyz + y^2$ is a polynomial in $\mathbb{Q}$ [x, y, z].

Notation : - We usually use the letters f,g,h,p,q,r to refer the polynomials .

***Definition1.1.3*:-**Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a polynomial in $K[x_1,x_2,...,x_n]$.

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 non zero.

***Example 1.1.2*:-** The polynomial $f = 2x^3y^2z + \frac{3}{2} y^3z^3 - 3xyz + y^2$ has four terms and a total degree six.

Note that there are two terms of maximal total degree which is something that cannot happen for a polynomial of one variable. In chapter 2, we will discuss how to order the terms of polynomial.

The sum and product of two polynomials is again a polynomial .We say that a polynomial f divides a polynomial g provided that g = fh for some $h \in K[x_1,...,x_n]$. One can show that under addition and multiplication $K[x_1,.,.,x_n]$ satisfies all of the field axioms except for the existence of a multiplication inverses. (Because, for example $\frac{1}{x}$ is not a polynomial). Such a mathematical structure is called a commutative ring.

***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 $K^n= \{ (a_1,a_2,\ldots,a_n) : a_1,a_2,\ldots,a_n \in K \}$.

***Example 1.1.3*:-** For an affine space, consider the case $K=\mathbb{R}$ here we get the familiar space $\mathbb{R}^n$ from calculus and linear algebra. In general we call $K^1=K$ the affine line and K^2 the affine plane.

Let us next see how polynomials are related to affine space .The key idea is that a polynomial $f= \sum_{\alpha} a_{\alpha} x^{\alpha} \in K [x_1,x_2,..., x_n]$ gives a function $f : K^n \rightarrow K$ defined as follows. Given $(a_1,a_2,...,a_n) \in K^n$. Replace every x_i by a_i in the expression for f. Since all of the

coefficients also lie in k, this operation gives an element f $(a_1,..., a_n) \in K$ .The ability to regard a polynomial as a function is what makes it possible to link algebra and geometry.

This dual nature of polynomials has some unexpected consequences. For example, the question "is f =0?" now has two potential meanings.

1) Is f the zero polynomial? Which means that all of its coefficients a_α are zero ,or
2) Is f the zero function? which means that $f(a_1,a_2,., a_n) =0$ for all $(a_1,a_2,..., a_n) \in K^n$
   The surprising fact is that these two statements are not equivalent in general.

Example 1.1.4:- Consider the set consists of two elements 0 and 1 .We see that this can be made into a field where 1+1 =0. This field is usually called F_2 .Now consider the polynomial $x^2-x = x(x-1) \in F_2 [x]$. Since this polynomial vanishes at 0 and 1, we have found non-zero polynomial which gives the zero function on the affine space F_2.

1.2 Affine Varieties

We can now define the basic geometric object of the seminar.

Definition 1.2.1:- Let K be a field, and let $f_1,...,f_s$ be a polynomials in $K[x_1,x_2,...,x_n]$ Then we set $V(f_1,f_2,..., f_s) = \{ (a_1,a_2, ..., a_n) \in K^n : f_i (a_1,a_2,..., a_n) =0$ for all$1 \leq i \leq s\}$.

We call $V (f_1,f_2,...,f_s)$ the affine variety defined by $f_1,...,f_s$.

Thus ,an affine variety $V(f_1,f_2,..., f_s) \subseteq K^n$ is the set of all solutions of the system of equations $f_1 (x_1,..., x_n) = ...= f_s(x_1,x_2 ,..., x_n) = 0$.

***Notation*: -** We use the letters V, W, etc to denote affine varieties.

Example1.2.1:- Consider the plane $\mathbb{R}^2$ with the variety $V (x^2+y^2 -1)$ which is the circle of radius 1 centered at the origin.

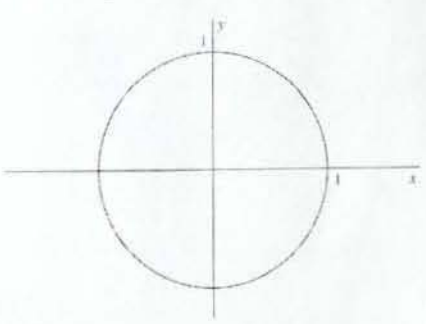


Figure 1

The conic sections studied in analytic geometry (circles, ellipses, parabolas and hyperbolas) are affine varieties. Likewise, graphs of polynomial functions are affine varieties [the graph of y= f(x) is v(y-f(x)]. Although not as obvious, graphs of rational functions are also affine varieties.

Example1. ***2.2*** Consider the graph of $y = \frac{x^3-1}{x}$:

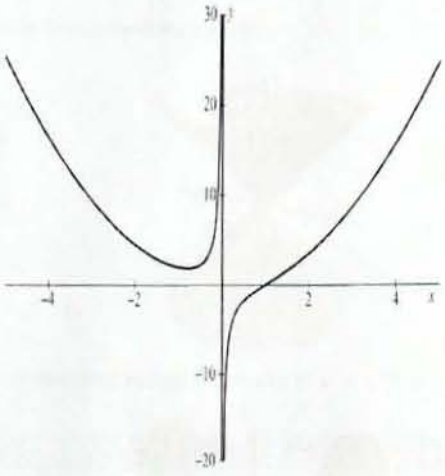
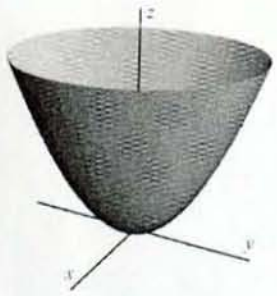


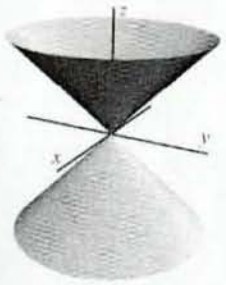
Figure 2

It is easy to check that this is affine varieties V $(xy - x^3+1)$.

Next let look 3-dimensional space $\mathbb{R}^3$. A nice affine varieties, is given by paraboloid of revolution V $(z-x^2-y^2)$,which obtained by rotating the parabola $z = x^2$ about the z- axis .This gives as the following picture.



You may also be familiar with the cone $\mathbf{V}(z^2 - x^2 - y^2)$:



A much more complicated surface is given by $\mathbf{V}(x^2 - y^2z^2 + z^3)$:

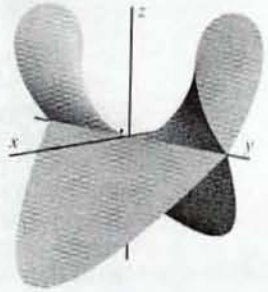
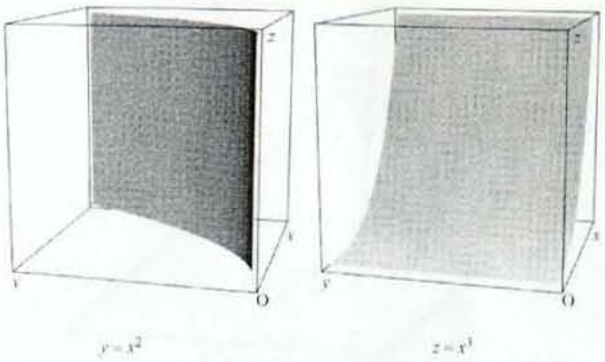


Figure 3

Example1.2.3:- A curve in $\mathbb{R}^3$ is the twisted cubic which is the variety $V(y-x^2, z-x^3)$. For simplicity we confine ourselves to the portion that lies in the first octant. To begin, we draw the surfaces $y = x^2$ and $z = x^3$ separately.



Then their intersection gives the twisted cubic:

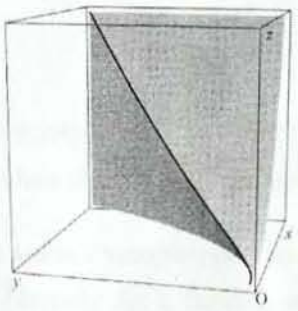


Figure 4

Notice that when we had one equation in $\mathbb{R}^2$, we got a curve, which is a one dimensional object. A similar situation happens in $\mathbb{R}^3$, usually gives a surface which has dimension two. Again dimension drops by one .But now consider the twisted cubic, here two equations in $\mathbb{R}^3$ gives a curve, so that dimension drops by two. Since each equation imposes an extra constraint intuition suggests that each equation drops the dimension by one. Thus if we started in $\mathbb{R}^4$, one would hope that an affine variety defined by two equations would be a surface. Unfortunately the notation of dimension is more subtle than indicated by the above examples. To illustrate this consider the variety V(x z, y z) .One can easily check that the equation

x z = y z =0 define the union of the (x, y) -plane and the z-axis.

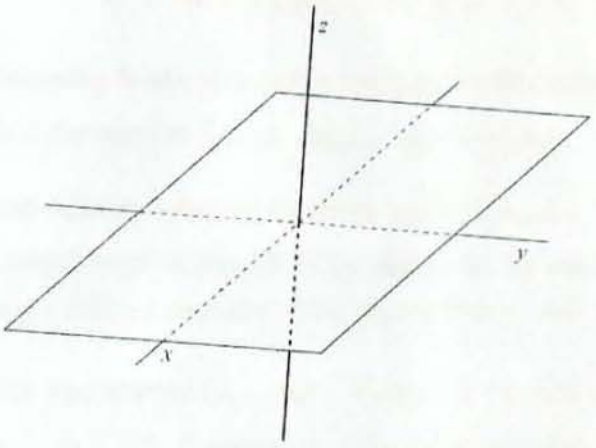


Figure 5

Hence, this variety consists of two pieces which have different dimensions and one of the pieces (the plane) has the "wrong" dimension according to the above intuition.

We next give some examples of varieties in higher dimensions .A familiar case comes from linear algebra .Namely fix a field k, and consider a system of m linear equations in n-unknowns $x_1,\ldots,x_n$ with coefficients in K:

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n &= b_i \qquad (1)\\ &\vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n &= b_m \end{aligned}$$

The solutions of these equations form an affine variety, in K^n, which we call a linear variety .Thus lines and planes are a linear varieties and there are examples of arbitrary large dimension.

Linear varieties relate nicely to our discussion of dimension, Namely, if $V \subseteq K^n$ is the linear variety defined by (1) , then V need not have dimension n-m, even though V is defined by m equations. In fact when V is nonempty, linear algebra tells us that V has dimension n-r, where r is the rank of the matrix (a_{ij}). So for linear varieties, the dimension is determined by number of independent equations.

***Lemma 1.2.1*:-** If $V, W \subseteq K^n$ are affine varieties then so are VUW and $V \cap W$.

Proof: - Suppose that $V= V(f_1,\ldots,f_s)$ and $W=V(g_1,g_2,\ldots, g_t)$

Then we claim that $V \cap W = V(f_1,\ldots,f_s,g_1,g_2,\ldots,g_t)$ and

$$V \cup W = V(f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t).$$

The first equality is trivial to prove being in $V \cap W$ means that both $f_1,\ldots,f_s$ and $g_1,g_2,\ldots, g_t$ vanish, which is the same as $f_1,\ldots,f_s$, $g_1,\ldots\ldots g_t$ vanishing.

The second equality takes a little more work, If $(a_1,a_2,\ldots,an) \in V$ then all of the f_i's vanish at this point ,which implies that all of the f_ig_j's also vanish at $(a_1,\ldots,a_n)$,Thus ,$V \subseteq V(f_ig_j)$ and $W \subseteq V(f_ig_j)$ follows similarly. This proves that $V \cup W \subseteq V(f_ig_j)$.

On the other way choose $(a_1,\ldots,a_n) \in V(f_ig_j)$. If this lies in V then we are done, and if not, then $f_{io}(a_1, a_2,\ldots,a_n) \neq 0$ for some io. Since $f_{io}g_j$ vanishes at $(a_1, a_2,\ldots,a_n)$ for all j, the g_j's must vanish at this point, proving that $(a_1, a_2, \ldots, a_n) \in W$. This shows that $V(f_ig_j) \subseteq V \cup W$.

This lemma implies that finite intersections and unions of affine varieties are again affine varieties. Concerning unions, consider the union of the (x, y) plane and the z-axis in affine three space. By the above formula we have $V(z) \cup V(x, y) = V(zx, zy)$.

Note: As for intersections the twisted cubic was given as the intersection of two surfaces.

The examples given in this section lead to some intersecting questions concerning affine varieties. Suppose that we have $f_1,\ldots,f_s \in K[x_1,x_2,\ldots, x_n]$. Then,

- (Consistency) can we determine if $V(f_1,\ldots,f_s) \neq \emptyset$,i.e. do the equations $f_1=\ldots=f_s= 0$ have a common solution ?
- (Finiteness) can we determine if $V(f_1,\ldots,f_s)$ is finite and if so, can we find all of the solutions explicitly?
- (Dimension) can we determine the "dimension" of $V(f_1,\ldots,f_s)$?
  The answer to these questions is yes, although care must be taken in choosing the field K that we work over.

1.3 Parameterization of Affine Varieties

In this section, we discuss the problem of describing the points of an affine variety $V(f_1,\ldots,f_s)$ .This reduces to asking whether this is a way to " write down " the solution of the system of polynomial equation $f_1=\ldots= f_s= 0$ when there are finitely many solutions, the goal is simply to list them all. What do we do when there are infinitely many? As we will see, this question leads to the notion of parameterizing an affine variety.

Example 1.3.1:- Let the field be $\mathbb{R}$ and consider the system of equations

$$x+ y+ z =1$$

$$x+ 2y- z =3 \qquad (3.1)$$

Geometrically this represents the line in $\mathbb{R}^3$ which is the intersection of the planes $x+ y+ z =1$ and $x+2y-z = 3$. It follows that there are infinitely many solutions.

To describe the solutions, we use row operations on equations 3.1 to obtain the equivalent equations $x+3z = -1$

$$y- 2z = 2$$

Letting $z=t$, where t is arbitrary, this implies that all solutions of 3.1 are given by

$$x = -1-3t$$

$$y= 2+2t \qquad (3.2)$$

$$z= t$$

As t varies over $\mathbb{R}$, we call t a parameter, and (3.2) is thus ,a parametrization of solution of (3.1).

Example 1.3.2:- To see if the idea of parameterizing solutions can be applied to other affine varieties let us look at the example of the unit circle

$$x^2+y^2=1 \quad (3.3)$$

A common way to parameterize the circle is using trigonometric functions.

$$x= \cos (t)$$

$$y= \sin (t)$$

There is also a more algebraic way to parameterize this circle

$$x= \frac{1-t^2}{1+t^2}$$

$$y= \frac{2t}{1+t^2} \qquad (3.4)$$

We should check that the points defined by these equations lie on the circle (3.3)

Note:- This parameterization does not describe the whole circle, since $x= \frac{1-t^2}{1+t^2}$

Can never equal -1, the point (-1, 0) is not covered.

Notice that equations (3.4) involve quotients of polynomials. These are examples of rational functions, before we can say what it means to parameterize a variety. We need to define the general notion of rational function.

Definition1.3.1:- Let K be a field. A rational function in $t_1,t_2,\ldots,t_m$ with coefficients in K is a quotient $\frac{f}{g}$ of two polynomials f, g ϵ $K[\ t_1,\ldots,t_m\ ]$, where g is not the zero polynomial . Furthermore, two rational functions $\frac{f}{g}$ and $\frac{h}{k}$ are equal, provided that kf =gh in $K[\ t_1,\ldots,t_m]$. Finally, the set of all rational functions in $t_1,\ldots,t_m$ with coefficients in K is denoted

$$K\ (t_1,\ldots,t_m).$$

It is not difficult to show that addition and multiplication of rational function are well defined and that $K\ (t_1,\ldots,t_m)$ is a field.

Now suppose that we are given a variety $V=V\ (f_1,\ldots,f_s) \subseteq K^n$ .Then a rational parametric representation of V consists of rational functions $r_1,\ldots,r_n \ \epsilon\ K\ (t_1,\ldots,t_m)$ such that the points given by

$$x_1 = r_1\ (\ t_1,\ldots,t_m)$$

$$x_2 = r_2\ (t_1,\ldots,t_m)$$

$$\vdots$$

$$x_n=r_n\ (t_1,\ldots,t_m) \quad \text{lie in V.}$$

In many situations, we have a parameterization of a variety V, where $r_1,\ldots,r_n$ are polynomials rather than rational functions.

This is what we call a polynomial parametric representation of V.

By contrast, the original defining equations $f_1=\ldots=\ f_s\ =\ 0$ of V are called an implicit representation of V. In our previous examples, note that equations (3.1) and (3.3) are implicit representations of varieties, whereas (3.2) and (3.4) are parametric, It is useful to have an implicit representation of variety.

Example 1.3.3:- Suppose we want to know whether or not the point (1, 2,-1) is on the surface

$V(x^2-y^2z^2+z^3)$, we use the parametric representation given by;

$$x = t(u^2-t^2)$$

$$y = u \qquad (3.5)$$

$$z = u^2-t^2$$

then, to decide this question, we would need to solve the equations

$$1= t(u^2-t^2)$$

$$2= u \qquad (3.6)$$

$$-1= u^2-t^2$$

for t and u .On the other hand ,if we have the implicit representation $x^2-y^2z^2+ z^3 =0$, then it is simply a matter of plugging into this equation.

Since $1^2-2^2(-1)^2 + (-1)^3 = 1-4-1=-4 \neq 0$. It shows that (1, 2,-1) is not on the surface [and, consequently, equation (3.6) have no solution].

The desirability of having both types of representation leads to the following two questions:

- (parameterization) Does every affine variety have a rational parametric representation?

- (Implicitization) Given a parametric representation of an affine variety can we find the defining equations (i.e. can we find an implicit representation)?

-The answer to the first question is no. In fact most affine varieties cannot be parameterized in the sense described here.

- The situation for the second question is much nicer that the answer is always yes.

Example1.3.4:- Let us look at an example of how implicitization works. Consider the parametric representation. $x= 1+t \qquad (3.7)$

$$y=1+t^2$$

This describes a curve in the plane, but at this point, we cannot be sure that it lies on an affine variety. To find the equation we are looking for, notice that we can solve the first equation for t to obtain t= x-1.

Substituting that the parametric equation yields $y=1+(x-1)^2 = x^2-2x+2$.

It follows that the parametric equations (3.7) describe the affine variety.

Note:- The basic strategy in the above example is to eliminate the variable t ,so that we were left with an equation involving only x and y. We will next discuss on how geometry can be used to parameterize varieties.

Example 1.3.5:- Consider the unit circle $x^2 + y^2 =1$ which was parameterize in (3. 4) via

$$x=\frac{1-t^2}{1+t^2}$$

$$y=\frac{2t}{1+t^2}$$

To see where this parameterization comes from, notice that each non vertical line through

(-1,0) will intersect the circle in a unit point (x, y).

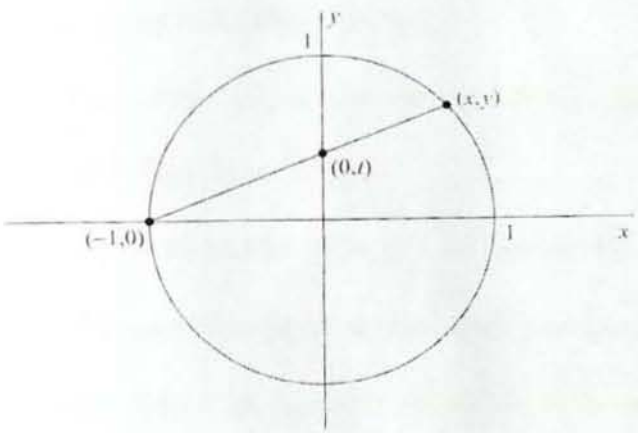


Figure 6

Each non vertical line also meets the y- axis, and this point (0, t) in the above picture.

This gives us a geometric parameterization of a circle. Given t, draw the line connecting

(-1, 0) to (0,t) and let (x, y) be the point where the line meets $x^2+y^2 =1$. Notice that the previous sentences really gives a parameterization, as t runs from $-\infty$ to corresponding points (x, y) traverses all of the circle except for the point (-1,0) .

It remains to find explicit formulas for x and y in terms of t, to do this considers the slope of the line in the above picture. We can compute the slope in two ways. Using either the points

(-1,0) and (0,t) or the points (-1,0) and (x, y) .This gives us the equation $\frac{t-0}{0-(-1)} = \frac{y-0}{x-(-1)}$

Which simplifies to become $t = \frac{y}{x+1}$

Thus $y=t(x+1)$. If we substitute this in to $x^2+y^2=1$, we get $x^2+t^2(x+1)^2=1$ which gives the quadratic equation.$(1+t^2)x^2+2t^2x+t^2-1=0$. (3.8)

This equation gives the x-coordinates of where the lines meet the circle and it is quadratic since there are two points of intersection one of the points is-1.So that x+1 is a factor of (3.8). It is now easy to find the other factor, and we can rewrite (3.8), as $(x+1)((1+t^2)x-(1-t^2))=0$. Since the x-coordinate we want is given by the second factor, we obtain $x = \frac{1-t^2}{1+t^2}$

Furthermore, $y = t(x+1)$ easily leads to $y = \frac{2t}{1+t^2}$

1.4 Ideals

The goal of this section is to introduce some naturally occurring ideals and to see how ideals relate to affine varieties. The real importance of ideals is that they give us a language for computing with affine varieties.

Definition 1.4.1:- A nonempty subset $I \subseteq K(x_1,....,x_n)$ is an ideal if it satisfies:

i) If $f, g \in I$ then $f + g \in I$

ii) If $f \in I$ and $h \in K[x_1,x_2,...,x_n]$, then $hf \in I$.

The first natural example of an ideal is the ideal generated by a finite number of polynomials.

Definition 1.4.2 :-Let $f_1,....,f_s$ be polynomial in $K[x_1,...., x_n]$.Then we set

$$(f_1,...,f_s) = \{\sum_{i=1}^{s} h_i f_i : h_1,....,h_s \in K[x_1,...,x_n]\}.$$

Lemma 1.4.1 :- If $f_1,..., f_s \in K[x_1,...,x_n]$, then $(f_1,...,f_s)$ is an ideal of $K[x_1,...,x_n]$. We call $(f_1,...,f_s)$ the ideal generated by $f_1,...,f_s$.

Proof:- .

First $0 \in (f_1,...,f_s)$ since $0 = \sum_{i=1}^{s} 0.f_i$ Next suppose that $f = \sum_{i=1}^{s} p_i f_i$ and $g = \sum_{i=1}^{s} q_i f_i$ and let $h \in K[x_1,...,x_n]$, then the equations. $f+g = \sum_{i=1}^{s} (p_i + q_i) f_i$ and $hf = \sum_{i=1}^{s} (hp_i) f_i$ complete the proof that $(f_1,...,f_s)$ is an ideal.

The ideal $(f_1,...,f_s)$ has a nice interpretation in terms of equations.

Example 1.4.1:-Given $f_1,...,f_s \in K[x_1,x_2,...,x_n]$ we get the system of equations.

$$f_1 = 0$$

$$f_2 = 0$$

$$\vdots$$

$$f_s = 0$$

From these equations, one can derive others using algebra. If we multiply the first equation by $h_1 \in K[x_1,x_2,...,x_n]$,the second by $h_2 \in K[x_1,x_2,...,x_n]$, etc and then add resulting equations, we obtain $h_1f_1+h_2f_2+....+h_sf_s = 0$ which is a consequence of our original systems.

Note: - The left hand side of this equation is exactly an element of the ideal $(f_1,...,f_s)$ .Thus we can think of $(f_1,...,f_s)$ as consisting of all "polynomial consequences" of the equations

$$f_1 = f_2 = ... = f_s = 0.$$

To see what this means in practice consider the example 3.4 of section 3, where we took

$$x = 1+t$$

$$y = 1+t^2$$

And eliminated t to obtain $y= x^2-2x+2$ Let us redo this example using the above ideas .we start by writing the equations as $x-1-t =0$

$$y-1-t^2 =0 \qquad (4.1)$$

To cancel the t-terms, we multiply the first equation by x-1+t and the second by -1.

$$(x-1)^2 - t^2 = 0$$

$$-y+ 1+t^2 = 0,$$

And then add to obtain $(x-1)^2 - y+1 = x^2-2x+2-y =0$ in terms of the ideal generated by equations (4.1) , we can write this as $x^2-2x+2-y = (x-1+t)(x-1-t)+(-1)(y-1-t^2) \in \langle x-1-t, y-1-t^2 \rangle$

Similarly, any other 'polynomial consequence' of (4.l) leads to an element of the ideal.

There is a nice analogy with linear algebra that can be made here .The definition of an ideal is similar to the definition of a subspace, both have to be closed under addition and multiplication, except that for a subspace we multiply by scalars, where as for an ideal, we multiply by polynomials.

Note :-1.The ideal generated by polynomials $f_1,\ldots,f_s$ is similar to the span of a finite number of vectors $v_1,\ldots,v_s$. In each case ,one takes linear combinations using field coefficients for the span and polynomial coefficients for the ideal generator.

2. A given ideal may have many different bases. In chapter 2 we will show an especially useful type of basis called Groebner basis.

Definition 1.4.3:- Let $V \subseteq K^n$ be an affine variety, then we set

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

Lemma 1.4.2:- If $V \subseteq K^n$ be an affine variety, then $I(V) \subseteq K[x_1,\ldots,x_n]$ is an ideal, we call I(V) the ideal of V.

Proof: It is obvious that $0 \in I(V)$ since the zero polynomial vanishes on all of the K^n and so in particular, it vanishes on V. Next suppose that $f,g \in I(V)$ and $h \in K[x_1,\ldots,x_n]$ .Let $(a_1,\ldots,a_n)$ be an arbitrary point of V. Then $f(a_1,\ldots,a_n)+g(a_1,\ldots,a_n) = 0 + 0 = 0$

$$\Rightarrow f + g \in I(V) \text{ and}$$

$$h(a_1,\ldots,a_n)\ f(a_1,\ldots,a_n) = h(a_1,\ldots,a_n).0 = 0$$

$$\Rightarrow hf \in I(V)$$

and it follows that I (V) is an ideal.

Example 1.4.2:-For the ideal of a variety, consider the variety $\{(0, 0)\}$ consists of the origin in K^2. Then, its ideal $I(\{(0,0)\})$ consists of all polynomials that vanishes at the origin ,and we claim that $I(\{(0,0)\}) = (x,y)$ one direction of the proof is trivial, for any polynomial of the form $A(x, y)x + B(x, y)y$ obviously vanishes at the origin. Going the other way suppose that $f=\sum_{i,j} a_{ij} x^i y^j$ vanishes at the origin .Then $a_{00} = f(0, 0) = 0$ and, consequently,

$$f = a_{00}+\sum_{i,j\neq 0,0} a_{ij} x^i y^j$$

$$0+\left(\sum_{i,j,i=0} a_{ij} x^{i-1} y^j\right)x+\left(\sum_{j>0} a_{oj} y^{j-1}\right)y \in \langle x, y \rangle.$$

Our claim is now proved.

Example 1.4.3:-Consider the case when V is all of K^n. Then $I(K^n)$ consists of polynomials that vanish everywhere, and hence we have $I(K^n) = 0$ when K is infinite.

Remark: - Here '' 0'' denotes the zero polynomial in $K[x_1,\ldots,x_n]$.

Proposition 1.4.3:- Let V and W be an affine varieties in K^n . Then

i. $V \subseteq W$ if and only if $I(V) \supseteq I(W)$
ii. $V = W$ if and only if $I(V) = I(W)$

Proof : Since (ii) is an immediate consequence of (i) ,we prove (i) first suppose that $V \subseteq W$ .Then any polynomial vanishing on W must vanish on V ,which proves $I(W) \subseteq I(V)$, Next assume that $I(W) \subseteq I(V)$. We know that W is variety defined by some polynomials $g_1,...,g_t \in K[x_1,...,x_n]$, then $g_1,...,g_t \in I(W) \subseteq I(V)$,and hence the g_i's vanish on V. Since W consists of all common zeros of the g_i's it follows that $V \subseteq W$.

CHAPTER TWO

Groebner Bases

2.1 Introduction

In Chapter One we have seen how the algebra of polynomial rings $K[x_1,\ldots,x_n]$ and the geometry of affine algebraic varieties are linked. In this chapter we study the method of Groebner bases which will allow us solving problems about polynomial ideals in an algorithmic or computational fashion. In chapter 1, we posed many problems concerning the algebra of polynomial ideals and the geometry of affine varieties. In this chapter we will focus on three of these problems.

a) The ideal description problem:- Does every ideal $I \subseteq K[x_1,x_2,\ldots,x_n]$ have a finite generating set? In other words, can we write $I = (f_1,f_2,\ldots,f_s)$ for some $f_i \in K[x_1,x_2,\ldots,x_n]$?

b) The ideal member ship problem:- Given $f \in K[x_1,\ldots,x_n]$ and an ideal $I = (f_1,f_2,\ldots,f_s)$, determine if $f \in I$. Geometrically, this is closely related to the problem of determining whether $V(f_1,\ldots,f_s)$ lies on the variety $V(f)$.

c) The problem of solving polynomial equations:- Find all common solutions in k^n of a system of polynomial equations $f_1(x_1,\ldots,x_n) = \ldots. = f_s(x_1,x_2,\ldots x_n)= 0$. Of course this is the same as asking for the points in the affine variety $V(f_1,\ldots,f_s)$.

The main example we have seen is the ideal of a variety, I (V). It will be useful to know these ideal have finite descriptions. On the other hand if we allow infinitely many variables to appear in our polynomials, then the answer to (a) is no.

To begin our study of Groebner bases, let us consider some special cases in which we have seen algorithmic techniques to solve the problems given above.

Example 2.1.1:- When $n = 1$, the ideal description problem $I \subseteq K[x]$, showed that $I= (g)$ for some $g \in K[x]$. So ideals have an especially simple description in this case.

We also know that the solution of the ideal member ship problem follows easily from the division algorithm. Given $f \in K[x]$ to check whether $f \in I= (g)$, we divide g in to f: $f = q.g+r$ where $q,r \in k[x]$ and $r = 0$ or $\deg(r) < \deg(g)$. Then $f \in I$ iff $r = 0$. Thus, we have an algorithmic test for ideal member ship in the case $n=1$.

Example 2.1.2:-Let n (the number of variables) be arbitrary, and consider the problem solving a system of polynomial equations:

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1n}x_n + b_1 &= 0 \\ &\vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n + b_m &= 0 \end{aligned} \qquad (2.1)$$

where each polynomial is linear (total degree=1)

For example, consider the system

$$\begin{aligned} 2x_1 + 3x_2 - x_3 &= 0 \\ x_1 + x_2 - 1 &= 0 \\ x_1 + x_3 - 3 &= 0 \end{aligned} \qquad (2.2)$$

Use row reduce the matrix of the system to reduced row echelon form

$$\begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & -1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

The form of this matrix shows that x_3 is free variable, and setting $x_3 = t$

(Any element k), we have $x_1 = -t+3$

$x_2 = t-2$

$x_3 = t$

These are parametric equations for a line L in K^3. The original system of equations (2.2) presents L as an affine variety.

In general case, one performs row operations on the matrix of (2.1).

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} & -b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & -b_m \end{pmatrix}$$

Until it is in reduced row echelon form (where the first non-zero entry on each row is 1, and all other entries in the column containing a leading 1 are 0).

Example 2.1.3:- Once again, take n arbitrary, and consider the sub set V of K^n parameterized by

$$\begin{aligned} x_1 &= a_{11}t_1 + \ldots + a_{1m}t_m + b_1, \\ &\vdots \end{aligned} \qquad (2.3)$$

$$x_n = a_{n1}t_1 + \ldots + a_{nm}t_m + b_n$$

We see that V is an affine linear subspace of K^n since V is the image of the mapping

F: $K^m \rightarrow K^n$ defined by

$$F(t_1,\ldots,t_m) = (a_{11}t_1 + \ldots + a_{1m}t_m + b_1, \ldots, a_{n1}t_1 + \ldots + a_{nm}t_m + b_n).$$

This is a linear mapping, followed by a translation. Let us consider the implicitization problem in this case. In other words, we seek a system of linear equations [as in (2.1)] whose solutions are the points of V.

Example 2.1.4:- consider the affine linear subspace $V \subseteq K^4$ defined by

$$x_1 = t_1 + t_2 + 1,$$

$$x_2 = t_1 - t_2 + 3,$$

$$x_3 = 2t_1 - 2,$$

$$x_4 = t_1 + t_2 - 3$$

We rewrite the equations by subtracting the x_i terms from both sides and apply the row reduction algorithm to the corresponding matrix.

$$\begin{pmatrix} 1 & 1 & -1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & -1 & 0 & 0 & -3 \\ 2 & 0 & 0 & 0 & -1 & 0 & 2 \\ 1 & 2 & 0 & 0 & 0 & -1 & 3 \end{pmatrix}$$

where the coefficients of the x; have been placed after the coefficients of the t; in each row. We obtain the reduced row echelon form.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & \frac{-1}{2} & 0 & 1 \\ 0 & 1 & 0 & 0 & \frac{1}{4} & \frac{-1}{2} & 1 \\ 0 & 0 & 1 & 0 & \frac{-1}{4} & \frac{-1}{2} & 3 \\ 0 & 0 & 0 & 1 & \frac{-3}{4} & \frac{1}{2} & 3 \end{pmatrix}$$

Because the entries in the first two columns of rows 3 and 4 are zero, the last two rows of this matrix correspond to the following two equations with no t_j terms.

$$x_1 - (\tfrac{1}{4})\, x_3 - (\tfrac{1}{2})\, x_4 - 3 = 0$$

$$x_2-(\tfrac{3}{4})\,x_3+(\tfrac{1}{2})\,x_4-3=0$$

Note:- This system is also in reduced row echelon form. These two equations define V in K^4.

The same method can be applied to find implicit equations for any affine linear sub space V given parametrically as in (2.3) one computes the reduced row echelon form of (2.3) and the rows involving only $x_1, \ldots, x_n$ given the equations for V. We, thus, have an algorithmic solution to the implicitization problem in this case.

2.2 Ordering On The Monomials in k $[x_1,x_2,\ldots,x_n]$

There are many different ways to define ordering on $z^n_{\geq o}$. For our purposes, most of these orderings will not be useful, however, since we will want our ordering to be "compatible" with the algebraic structure of polynomial rings.

Definition 2.2.1:- A monomial ordering on $K[x_1,\ldots,x_n]$ is any relation $>$ on $z^n_{\geq 0}$, or equivalently, any relation on the set of monomials $x^{\alpha}, \alpha \in z^n_{\geq 0}$ satisfying.

i. $>$ is a total (or linear) ordering on $z^n_{\geq o}$.
ii. If $\alpha > \beta$ and $\gamma \in z^n_{\geq 0}$, then $\alpha+\gamma > \beta+\gamma$
iii. $>$ is a well ordering on $z^n_{\geq 0}$. This means that every non empty subset of $z^n_{\geq 0}$ has a smallest element under $>$.

The following lemma will help us understand what the well ordering condition of part (iii) of the definition means.

Lemma 2.2.1:- An order relation $>$ on $z^n_{\geq 0}$ is a well ordering if and only if every strictly decreasing sequence in $z^n_{\geq 0}$; $\alpha(1) > \alpha(2) > \alpha(3) > \ldots$ eventually terminates.

Proof: We prove this in contra positive form : $>$ is not a well ordering if and only if there is an infinite strictly decreasing sequence in $z^n_{\geq 0}$.

If $>$ is not a well ordering, then some nonempty subset $S \subseteq z^n_{\geq 0}$ has no least element. Now pick $\alpha(1) \in S$. Since $\alpha(1)$ is not the least element, we can find $\alpha(1) > \alpha(2)$ in S. Then $\alpha(2)$ is also not the least element. So, there is $\alpha(2) > \alpha(3)$ in S. Continuing this way, we get an infinite strictly decreasing sequence $\alpha(1) > \alpha(2) > \alpha(3) > \ldots$

Conversely, given such an infinite sequence, then $\{\alpha(1), \alpha(2), \ldots\}$ is non empty subset of $z^n_{\geq 0}$ with no least element, and thus, $>$ is not a well ordering.

Definition 2.2.2 (Lexicographic order):- Let $\alpha=\alpha_1...\alpha_n$ and $\beta=(\beta_1,...,\beta_n)\in z^n{}_{\geq 0}$. we say $\propto >_{lex} \beta$ if, in the vector difference $\propto - \beta \in z^n{}_{\geq 0}$, the left most non zero entry $z^n{}_{\geq 0}$ is positive. We write $x^{\alpha} >_{lex} x^{\beta}$ if $\propto >_{lex} \beta$.

Example 2.2.1

a) $(1,2,0) >_{lex} (0,3,4)$ Since $\propto - \beta = (1,-1,-4)$

b) $(3,2,4) >_{lex} (3,2,1)$ Since $\propto - \beta = (0,0,3)$

c) The variables $x_1,\ldots,x_n$ are ordered in the usual way by the lex ordering $(1,0,\ldots,0) >_{lex} \ldots >_{lex} (0,0,\ldots,0,1)$. So $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

In practice when we work with polynomials in two or more variables we call the variables x, y, z rather than x_1, x_2, x_3. We also assume that the alphabetical order x>y>z on the variables is used to define the lexicographic ordering unless we explicitly say otherwise.

Lex order is analogous to the ordering of words used in the dictionaries hence the name. We can view the entries of an n-tuple $\propto \in z^n{}_{\geq 0}$ as analogous of the letters in a word. The letters are ordered alphabetically a > b >... > y > z.

Remark:- In the general case of n variables, there are n! lex order. For the lex order with x>y>z, we have $x >_{lex} y^5 z^3$.

Definition 2.2.3 (Graded lex order) Let $\propto, \beta, \in Z^n{}_{\geq}o$ we say $\propto > g_{rlex} \beta$ if $|\propto| = \sum_{i=1}^{n} \propto_i > |\beta| = \sum_{i=1}^{n} \beta_i$, or $|\propto| = |\beta|$ and $\propto >_{lex} \beta$.

Note: - We see that grlex orders by total degree first, then "breaks ties" using lex order.

Example 2.2.3

a) $(1,2,3) >_{grlex} (3,2,0)$ Since $|(1,2,3)| = 6 > |(4,2,3)| = 5$

b) $(1,2,4,) >_{grlex} (1,1,5)$ Since $|(1,2,4)| = |(1,15)|$ and $(1,2,4) >_{lex} (1,1,5)$

c) The variables are ordered according to the lex order. i.e $x_1 >_{grlex} \text{---} >_{grlex} x_n$.

Remark:- There are n! grlex orders of n variables; depending on how the variables are ordered.

Definition 2.2.4 (Graded Reverse lex order) Let $\propto, \beta, \in z^n{}_{\geq}o$. We say $\propto >_{grevlex} \beta$ if $|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$, or $|\alpha| = |\beta|$, and the right most non zero entry of $\propto - \beta, \in Z^n{}_{\geq 0}$ is negative.

Note: - Like grlex, grevlex orders by total degree but it "breaks ties" in a different way.

Example 2.2.4

a) $(4,7,1) >_{grevlex} (4,2,3)$ since $|(4,7,1)|= 12 >|(1,1,5)|= 9$.

b) $(1,5,2) >_{grevlex} (4,1,3)$ since $|(1,5,2)|=|(4,1,3)|$ and $(1,5,2)-(4,1,3)= (-3,4,-1)$

Note: - Also that lex and grevlex give the same ordering on the variables.

That is $(1,0,\ldots,0) >_{grevlex} \ldots >_{gevlex}(0,\ldots,0,1)$ Or $x_1 >_{grevlex} \ldots >_{servlex} x_n$.

To explain the relation between grlex and grevlex, note that both use total degree in the same way. To break a tie grlex use lex orders so that is looks at the left most (or largest) variable and favors the larger power. In contrast, when graded revlex finds the same total degree, it looks at the right most (or smallest) variable and favors the smaller power.

Remark: - There are n! grevlex ordering corresponding to how the n variables are ordered.

We end this section with a discussion of how a monomial ordering can be applied to polynomials. If $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ is a polynomial in $K[x_1,\ldots,x_n]$ and we have selected monomial ordering>, then we can order the monomials of f in an unambiguous way with respect to >.

Example 2.2.5 Let $f = 4xy^2z+4z^2-5x^3+7x^2z^2 \in K[x,y,z]$.

Then:

a) with respect to the lex order, we would reorder the terms of f in decreasing order as

$f = -5x^3+7x^2z^2+4xy^2z+4z^2$.

b) with respect to the grlex, we would have $f = 7x^2z^2+4xy^2z-5x^3+4z^2$.

c) with respect to the grevlex, we would have $f = 4xy^2z+7x^2z^2-5x^3+4z^2$.

Definition2.2.5 Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a non zero polynomial in $K[x_1,\ldots,x_n]$ and let > be a monomial order.

i. The multi degree of f is multi deg(f) = max $(\alpha \in Z^n_{\geq 0}: a_{\alpha} \neq 0)$
(The maximum is taken with respect to >).

ii. The leading coefficient of f is LC (f) = $a_{\text{multi deg(f)}} \in K$.

iii. The leading monomial of f is LM(f) = $x^{\text{multi deg(f)}}$ (with coefficient 1)

iv. The leading term of f is LT (f) = LC (f). LM (f).

To illustrate, let $f = 4xy^2z+3z^2-5x^3+7x^2z^2$ as before and let > denote the lex order. Then we have Multi deg (f) = (3, 0, 0), LM (f) = x^3, LC (f) = -5, LT (f) = $-5x^3$.

2.3 A Division Algorithm in $K[x_1,\ldots,x_n]$

The aim of this sub topic is to divide $f \in K[x_1,\cdots,x_n]$ by $f_1,\ldots,f_s \in K[x_1,\cdots,x_n]$. As we will see, this means expressing f in the form $f = a_1f_1+\ldots+a_sf_s+ r$, where the "quotients" $a_1,\ldots,a_s$ and remainder r lie in $K[x_1,\ldots,x_n]$.

Example 2.3.1:- We first divide $f = xy^2+1$ by $f_1 = xy+1$ and $f_2 = y+1$, using lex order with x>y. We want to employ the same scheme as for division of one variable polynomials, the difference being that there are now several divisors and quotients. Listing the divisors f_1, f_2 and the quotients a_1, a_2 vertically, we have the following set up.

$a_1=$

$a_2 =$

$$\begin{array}{l} xy+1 \overline{)\sqrt{xy^2+1}} \\ y+1 \end{array}$$

The leading terms LT (f_1) =xy and LT (f_2) = y both divide the leading term LT (f)= xy^2. Since f_1 is listed first, we will use it. Thus, we divide xy in to xy^2, leaving y, and then subtract y. f_1 from f.

$a_1=y$

$a_2=$

$$\begin{array}{l} xy+1 \overline{)\begin{array}{l}\sqrt{xy^2+1} \\ \sqrt{xy^2+y} \\ \hline -y+1\end{array}} \\ y+1 \end{array}$$

Now we repeat the same process on –y+1. This time we must use f_2 since LT(f_1)= xy does not divide LT(-y+1). We obtain

$a_1 = y$

$a_2 = -1$

$$\begin{array}{l} xy+1 \overline{)\begin{array}{l}\sqrt{xy^2+1} \\ \sqrt{xy^2+y} \\ \hline -y+1 \\ -y-1 \\ \hline 2\end{array}} \\ y+1 \end{array}$$

Since LT (f_1) and LT (f_2) do not divide 2, the remainder is r=2 and we are done.

Thus we have written $f=xy^2+1$ in the form

$$xy^2+1= y\,(xy+1)+(-1).(y+1)+2.$$

Example 2.3.2 Divide $f=x^2y+xy^2+y^2$ by $f_1=xy-1$ and $f_2=y^2-1$

$a_1 = x+ y$

$a_2 =$

$$\begin{array}{r|l} xy+1 & \sqrt{x^2y+xy^2+y^2} \\ & x^2y-x \\ \hline y+1 & xy^2+x+y^2 \\ & xy^2-y \\ \hline & x+y^2+y \end{array}$$

By using lex order x > y, the first two steps of the algorithm go as usual.

Note that neither LT (f_1) = xy nor LT (f_2) = y^2 divides LT ($x+y^2+y$) = x. However, $x+y^2+y$ is not the remainder since LT (f_2) divides y^2. Thus, if we move x to the remainder, we can continue dividing. (This is something that never happens in the one variable case: Once the leading term of the divisor no longer divides the leading term of what is left under the radical, the algorithm terminates).

Then we continue dividing by creating remainder column units the intermediate dividend is zero.

$a_1 = x+ y$ r

$a_2 = 1$

$$\begin{array}{r|l} xy-1 & \sqrt{x^2y+xy^2+y^2} \\ & x^2y-x \\ \hline x^2-1 & xy^2+x+y^2 \\ & xy^2-y \\ \hline & x+y^2+y \\ & y^2+y-x \\ \hline & y^2-1 \\ & 1-x+y \\ \hline & 0-x+y+1 \end{array}$$

Thus, the remainder is x+y+1, and we obtain

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

Example 2.3.3:- Let $f_1= xy+1, f_2= y^2-1 \in k\,[x, y]$ with the lex order dividing $f = xy^2-xby$

$F = (f_1,f_2)$ the result is $xy^2-x = y.(xy+1)+0.(y^2-1)+(-x-y)$ with $F= (f_2,f_1)$, however, we have

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

The second calculation shows that $f \in (f_1, f_2)$. Then the first calculation shows that even if $f \in (f_1, f_2)$ if is still possible to obtain none zero remainder on division by $F= GCD(f_1, f_2)$.

2.4 Monomial Ideals and Dickson's Lemma

In this sub topic, we consider the ideal description problem of section 1 for the special case of monomial ideals.

Definition 2.4.1:- An ideal $I \subseteq K[x_1,\ldots,x_n]$ is a monomial ideal if there is a sub set $A \subseteq Z^n_{\geq o}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$, where $h_\alpha \in K[x_1,\ldots,x_n]$ In this case, we write $I= (x^\alpha : \alpha \in A)$. An example of monomial ideal is given by; $I=(x^4y^2, x^3y^4, x^2y^5) \subseteq K[x,y]$.

Lemma 2.4.1:- Let $I=(x^\alpha : \alpha \in A)$, 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 $\alpha \in A$.

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

Note: - x^β is divisible by x^α exactly when $x^\beta = x^\alpha . x^\gamma$ for some $\gamma \in z^n_{\geq o}$. This is equivalent to $\beta = \alpha + \gamma$. Thus the set $\alpha + Z^n_{\geq o} = \{\alpha + \gamma = \gamma \in z^n_{\geq 0}\}$ consists of the exponents of all monomials divisible by x^α.

This observation and lemma 2.4.1 allows us to draw pictures of the monomials in a given monomial ideal. For example If $I= (x^4y^2, x^3y^4, x^2y^5)$, then the exponents of the monomials in I form the set.

$$((4,2)+ z^2_{\geq o}) \cup ((3,4)+ z^2_{\geq o} > \cup ((2,5)+ z^2_{\geq o})$$

We can visualize this set as the union of the integer points in three translated copies of the first quadrant in the picture.

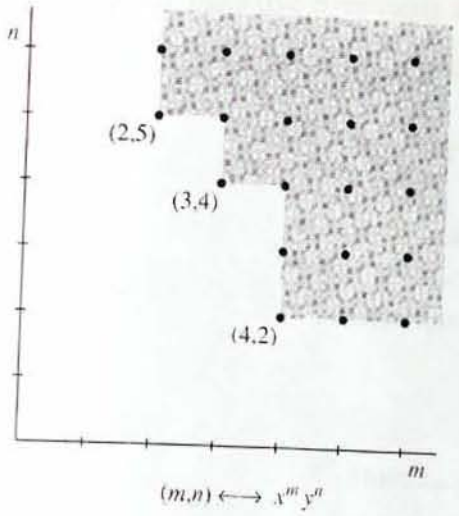


Figure 7

Theorem 2.4.2 (Dickson's Lemma):- A monomial ideal $I=\langle x^{\alpha} : \alpha \in A\rangle \subseteq K[x_1,\ldots,x_n]$ can be written down in the form $I=\langle x^{\alpha(1)},\ldots, x^{\alpha(s)}\rangle$,where $\alpha(1),\ldots,\alpha(s) \in A$. In particular, I has finite basis.

Proof: (By induction on n, the number of variables) (If n=1, then I is generated by the monomials $x_1^{(\alpha)}$, where $\alpha \in A \subseteq Z_{\geq 0}$. Let β be the smallest element of $A \subseteq Z_{\geq 0}$. Then, $\beta \leq \alpha$ for all $\alpha \in A$. So that x_1^{β} divides all other generators x_1^{α}. From here, $I = \langle x_1^{\beta}\rangle$ follows easily.

Now assume that n>1 and that the theorem is true for n-1. We will write the variables as $x_1,\ldots,x_{n-1},y$. so that monomials in $K[x_1,\ldots,x_{n-1},y]$ can be written as $x^{\alpha}y^m$, where;

$\alpha=(\alpha_1,\ldots \alpha_{n-1}) \in Z^{n-1}_{\geq 0}$ and $m \in Z^{n}_{\geq 0}$.

Suppose that $I \subseteq K[x_1 \cdots, x_{n-1}, y]$ is a monomial ideal. To find generators for I, let J be the ideal in $k[x_1 \cdots, x_{n-1}]$ generated by the monomials x^{α} for which $x^{\alpha}y^m \in I$ for some $m \geq 0$. Since J is a monomial ideal in $K[x_1 \cdots, x_{n-1}]$ our inductive hypothesis implies that finitely many of the $x^{\alpha' s}$ generate J, say $J=\langle x^{\alpha(1)},\ldots, x^{\alpha(s)}\rangle$. The ideal J can be understood as the "projection" of I in to $K[x_1 \cdots, x_{n-1}]$. For each i between 1and s, the definition of J tells us that $x^{\alpha(i)}y^{m_i} \in I$ for some $m_i \geq o$. Let m be the largest of m_i. Then for each k between 0and m-1, consider the ideal $J_k \subseteq K[x_1 \cdots, x_{n-1}]$ generated by the monomials x^{β} such that $x^{\beta}y^k \in I$. One can think of J_k as the "slice" of I generated by monomials containing y exactly to the k^{th}

power. Using our inductive hypothesis again, J_k has finite generating set of monomials, say $J_k = \langle x^{\alpha_1(1)}, \ldots, x^{\alpha_1(s_k)} \rangle$. We claim that I is generated by the monomials in the following list.

$$\text{from } J: x^{\alpha(1)}y^m, \ldots, x^{\alpha(s)}y^m,$$

$$\text{from } J_0: x^{\alpha_0(1)}, \ldots, x^{\alpha_0(s_0)},$$

$$\text{from } J_1: x^{\alpha_1(1)}y, \ldots; x^{\alpha_1 s_1}y,$$

$$\vdots$$

$$\text{From } J_{m-1} x^{\alpha_{m-1}(1)}y^{m-1}, \ldots, x^{\alpha_{m-1}(s_{m-1})}y^{m-1}.$$

First note that every monomial in I is divisible by one on the list. To see why, let $y^p \in I$. If $p \geq m$, then, $x^{\alpha}y^p$ is divisible by some $x^{\alpha(i)}y^m$ by the construction of J. On the other hand, if $p \leq m-1$, then $x^{\alpha}y^p$ is divisible by some $x^{\alpha_p(i)}y^p$ by the construction of J_p. It follows from lemma 2.4.1 that the above monomials generate an ideal having the same monomials as I. This forces the ideals to the same, and our claim is proved.

To complete the proof of the theorem, we need to show that the finite set of generators can be chosen from a given set of generators for the ideals. If we switch back to writing the variables as $x_1, \ldots, x_n$, then our monomial ideal is $I = \langle x^{\alpha} : \alpha \in A \rangle \subseteq K[x_1, \ldots, x_{n-1}]$ we need to show that I is generated by finitely many of the x^{α}'s, *where* $\alpha \in A$. We know that

$I = \langle x^{\beta(1)}, \ldots, x^{\beta(s)} \rangle$ for some monomials $x^{\beta(i)}$ in I since $x^{\beta(i)} \in I = \langle x^{\alpha} = \alpha \in A \rangle$. Lemma 2.4.1 tells us that each $x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ for some $\alpha(i) \in A$. From here, it is easy to show that $I = \langle x^{\alpha(i)}, \ldots, x^{\alpha(s)} \rangle$. This completes the proof.

2.5 The Hilbert Basis Theorem and Groebner Bases

In this sub topic we give a complete solution of the ideal description problem. Our treatment will also lead to ideal bases with "good" properties relative to division algorithms.

Definition 2.5.1 Let $I \subseteq K[x_1, \ldots, x_n]$ an ideal other than $\{0\}$.

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

(ii) We denote by <LT (I)> the ideal generated by the elements of LT (I).

Example 2.5.1 Let $I = (f_1,f_2)$, where $f_1=x^3-2xy$ and $f_2 = x^2y-2y^2+x$, and use the grlex ordering on monomials in $K[x,y]$. Then $x.(x^2y-2y^2+x)-y.(x^3-2xy) = x^2$ so that $x^2 \in I$, thus,

$x^2 = LT(x^2) \in (LT(I))$. However x^2 is not divisible by $LT(f_1) = x^3$ or $LT(f_2) = x^2y$, so that,

$x^2 \notin (LT(f_1),LT(f_2))$ by Lemma 2.4.1

Proposition 2.5.1:- Let $I \subseteq K[x_1,\ldots,x_n]$ be an ideal

(i)$(LT(I))$ is a monomial ideal

(ii)There are $g_1,\ldots,g_t \in I$ such that $(LT(I)) = (LT(g_1),\ldots,LT(g_t))$.

Proof:

i) The leading monomials LM (g) of elements $g \in I-\{0\}$ generate the monomial ideal $(LM(g) = g \in I-\{0\})$. Since LM (g) and LT (g) differ by non-zero constant, this ideals equals $(LT(g): g \in I-\{0\}) = (LT(I))$. Thus LT (I) is a monomial.

ii) Since $<LT(I)>$ is generated by the monomials LM(g) for $g \in I-\{0\}$ Dickson's lemma tells us that $<LT(I)> = <LM(g_1),\ldots, LM(g_t)>$ for finitely many $g_1,\ldots,g_t \in I$. Since LM (g_i) differs from $LT(g_i)$ by a non zero constant, it follows that$<LT(I)>=<LT(g_i),\ldots,LT(g_t)>$. This completes the proof.

Theorem 2.5.2 (Hilbert Basis Theorem):- Every ideal $I \subseteq K[x_1,\ldots,x_n]$ has a finite generating set. That is, $I=<g_1,\ldots,g_t>$ for some $g_1,\ldots,g_t \in I$.

Proof: If $I = \{0\}$,we take our generating set to be $\{0\}$ which is certainly finite. If I contains some non-zero polynomial, then generating set, $g_1,\ldots,g_t$ for I can be constructed as follows, by proposition 2.5.1 there are $g_1,\ldots,g_t \in I$ such that $<(LT(I)> = <LT(g_1),\ldots,LT(g_t)>$. We claim that $I = <g_1,\ldots,g_t>$.

It is clear that $<g_1,\ldots, g_t> \subseteq I$ Since each $g_i \in I$. Conversely let $f \in I$ be any polynomial. If we apply the division algorithm from section 2.3 to divide f by $<g_1,\ldots,g_t>$ then we get an expression of the form $f=a_1g_1+\ldots+a_tg_t+ r$ where no term of r is divisible by any of $LT(g_1),\ldots,LT(g_t)$. We claim that $r = 0$. To see this, note that $r = f-a_1g_1- \ldots-a_tg_t \in I$.

If $r \neq 0$, then $LT(r) \in <LT(I)> = <LT(g_1),\ldots,LT(g_t)>$. And by lemma 2.4.1 of sub topic 4 it follows that LT(r) must be divisible by some $LT(g_i)$. This contradicts what it means to be remainder, and consequently, r must be zero. Thus $f= a_1g_1+\ldots+a_tg_t+0 \in <g_1,\ldots,g_t>$, which shows that $I \subseteq <g_1,\ldots,g_t>$. This completes the proof.

In addition to answering the ideal description question, the basis $\{g_1,g_2,\ldots,g_t\}$ used in the proof of theorem 2.5.2 has the special property that $\langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$.

As we saw in example 2.5.1 not all bases of an ideal behave this way. We give these special bases the following name.

Definition 2.5.2 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 $\langle LT(g_1),\ldots,LT(g_t)\rangle = \langle LT(I)\rangle$.

Equivalently, but more informally, a set $\{g_1,\ldots,g_t\} \subseteq I$ is a Groebner basis of I if and only if the leading term of any element of I is divisible by one of the $LT(g_i)$.

Corollary 2.5.3 Fix a monomial order. Then every ideal $I \subseteq K[x_1,\ldots,x_n]$ other than $\{0\}$ has a Groebner basis. Furthermore, any Groebner basis for an ideal I is a basis of I.

Proof: Given a non-zero ideal, the set $G = \{g_1,\ldots,g_t\}$ constructed in the proof of theorem 2.5.2 is a Groebner basis by definition. For the second claim, note that if $\langle LT(I)\rangle = \langle LT(g_1),\ldots, LT(g_t)\rangle$, then the argument given in theorem 2.5.2 shows that $I=\langle g_1,\ldots,g_t\rangle$. So that G is a basis for I.

Example 2.5.2 Consider the ideal I from example 2.5.1 which had the basis;

$\{f_1,f_2\}= \{x^3-2xy,x^2y-2y^2+x\}$ then$\{f_1,f_2\}$ is not a Groebner basis for I with respect to grlex order. Since we saw in example 2.5.1 that $x^2 \in \langle LT(I)\rangle$, but $x^2 \notin \langle LT(f_1), LT(f_2)\rangle$.

Theorem 2.5.4 (The ascending chain condition):- Let $I_1\subseteq I_2\subseteq I_3\subseteq\ldots$ be an ascending chain of ideals in $K[x_1,\ldots,x_n]$, then there exists an $N\geq 1$ such that $I_N = I_{N+1} = I_{N+2} = \ldots$

Proof: Given the ascending chain $I_1\subseteq I_2\subseteq I_3\subseteq\ldots$, consider the set $I= \bigcup_{i=1}^{\infty} I_i$. We begin by showing that I is also an ideal in $k[x_1,\ldots,x_n]$. First, $0\in I$since $0\in I$, for every i. Next, if $f,g \in I$, then, by definition, $f\in I_i$, and $g\in I_i$, for some i and j (possibly different). However, since the ideals I_i form an ascending chain, if we relabel so that $i \leq j$, then both f and g are in I_j. Since I_j is an ideal, the sum $f+g \in I_j$, hence, $\in I$. Similarly, if $f \in I$ and $r \in K[x_1,\ldots,x_n]$, then $f \in I_i$ for some i, and $r.f \in I_i \subseteq I$. Hence, I is an ideal.

By the Hilbert basis theorem the ideal I must have finite generating set: $I = \langle f_1, \ldots,f_s\rangle$. But each of the generators is contained in some one of the I_j, say $f_i \in I_{j_i}$, for some ji, i= 1,…,s. We take N to be the maximum of the Ji. Then by the definition of an ascending chain $f_i \in I_N$ for all i, hence we have $I = \langle f_1,\ldots,f_s\rangle \subseteq I_N\subseteq I_{N+1}\subseteq\ldots\subseteq I$. As a result the ascending chain stabilizes with I_N. All the sub sequent ideal in the chain are equal.

Our second consequence of the Hilbert basis theorem will be geometric. Up to this point, we have considered affine varieties as the sets of solutions of specific finite sets of polynomial equations:

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

The Hilbert basis theorem shows that in fact, it also makes sense to speak of the affine variety defined by an ideal $I \subseteq K[x_1,\ldots,x_n]$.

Definition 2.5.3:- Let $I \subseteq K[x_1,\ldots,x_n]$ be an ideal. We denote by V(I) the set $V(I) = \{(a_1,\ldots, a_n) \in K^n : f(a_1,\ldots,a_n) = 0 \text{ for all } f \in I\}$.

Even though a non-zero ideal I always contains infinitely many different problems, the set V(I) can still be defined by a finite set of polynomial equations.

Proposition 2.5.5:-V (I) is an affine variety. In particular, if $I = \langle f_1,\ldots,f_s\rangle$, then

$V(I) = V(f_1,\ldots,f_s)$.

Proof: By the Hilbert basis theorem, $I = \langle f_1,\ldots,f_s\rangle$ for some finite generating set. We claim that $V(I) = V\langle f_1,\ldots,f_s\rangle$. First since the $f_i \in I$, if $f(a_1,\ldots,a_n) = 0$ for all $f \in I$, then $f_i(a_1,\ldots,a_n) = 0$, So $V(I) \subseteq V(f_1,\ldots,f_s)$. On the other hand, let $(a_1,\ldots,a_n) \in V(f_1,\ldots,f_s)$ and let $f \in I$. Since $I = \langle f_1,\ldots,f_s\rangle$, we can write $f = \sum_{i=1}^{s} h_i f_i$

For some $h_i \in k[x_1,\ldots,x_n]$, but then $f(a_1,\ldots,a_n) = \sum_{i=1}^{s} h_i(a_1,\ldots,a_n)\, f_i(a_1,\ldots a_n)$

$$= \sum h_i\,(a_1,\ldots,a_n).0 = 0$$

Thus, $V(f_1,\ldots,f_s) \subseteq V(I)$ and hence they are equal.

The most important consequence of this proposition is that varieties are determined by ideals. For instance in chapter1, we proved that $V(f_1, \ldots,f_s) = V(g_1,\ldots,g_t)$ whenever

$$\langle f_1,\ldots,f_s\rangle = \langle g_1,\ldots,g_t\rangle.$$

2.6 Properties of Groebner Bases

In this subtopic, first we prove that the remainder is uniquely determined when we divide by a Groebner basis.

Proposition 2.6.1 Let G= $\{g_1,\ldots,g_t\}$ be a Groebner basis for an ideal $I \subseteq K[x_1,\ldots,x_n]$ and let $f \in K[x_1,\ldots,x_n]$. Then there is a unique $r \in K[x_1,\ldots,x_n]$ with the following two properties:

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

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

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

Proof: The division algorithm gives $f = a_1g_1+\ldots+a_tg_t + r$, where r satisfies (i). We can also satisfy (ii) by setting $g=a_1g_1+\text{---}+a_tg_t \in I$. This proves the existence of r.

To prove uniqueness suppose that $f = g+ r = g' + r'$ satisfy(i) and(ii).Then $r-r'=g'-g \in I$, so that if $r \neq r'$, then $LT(r-r') \in \langle LT(I)\rangle = \langle LT(g_1),\ldots,LT(g_t)\rangle$. By lemma 2.4.1 of section 4, it follows that LT(r-r') is divisible by some LT (g_i). This is impossible since no term of r,r'is divisible by one of $LT(g_1),\ldots,LT(g_t)$. Thus r-r' must be zero, and uniqueness is proved. The final part of the proposition follows from the uniqueness of r.

Corollary 2.6.2 Let G = $\{g_1,\ldots,g_t\}$ be a Groebner basis for an ideal $I \subseteq K[x_1,\ldots,x_n]$ and let

$f \in K[x_1,\ldots,x_n]$.Then $f \in I$ if and only if the remainder on division of f by G is Zero.

Proof: If the remainder is zero, then, we have already observed that $f \in I$. Conversely given $f \in I$, then $f = f + 0$ satisfies the two conditions of proposition 2.6.1. It follows that 0 is the remainder of f on division by G.

Definition 2.6.1 We 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 2.6.1. For instance, with $F = (x^2y-y^2,x^4y^2-y^2) \subseteq K[x,y]$, using the lex order, we have $\overline{x^5y}^F = xy^3$.

Since the division algorithm yields $x^5y = (x^3+xy)(x^2y-y^2) +0.(x^4y^2-y^2)+ xy^3$.

Definition 2.6.2:- Let $f, g \in K[x_1,\ldots,x_n]$ be non zero polynomials.

(i) If multi deg (f)=α and multi deg(g)=β, 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 LM(f) and LM(g), written x^γ = LCM (LM(f), LM(g)).

(ii) The **S-polynomial** of f and g is the combination $S(f,g)=\frac{x^\gamma}{LT(f)}\cdot f - \frac{x^\gamma}{LT(g)}\cdot g$

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

Example 2.6.1 Let $f = x^3y^2-x^2y^3+x$ and $g = 3x^4y+y^2$ in $\mathbb{R}[x, y]$ with the grlex order. Then $\gamma = (4,2)$ and

$$S(f,g) = \frac{x^4y^2}{x^3y^2}.f - \frac{x^4y^2}{3x^4y}.g$$

$$= x.f - (\frac{1}{3}).y.g$$

$$= -x^3y^3+x^2 - (\frac{1}{3})y^3$$

An S- polynomial S (f,g) is "designed" to produce cancellation of leading terms.

Lemma 2.6.3:- Suppose we have a sum $\sum_{i=1}^{s} c_i f_i$ where $c_i \in K$ and multideg $(f_i) = \delta \in Z^n_{\geq 0}$ for all i. If multideg $(\sum_{i=1}^{s} c_i f_i) < \delta$, then $\sum_{i=1}^{s} c_i f_i$ is a linear combination, with coefficients in K, of the S-polynomials $S(f_i,f_k)$ for $1 \leq j, k \leq s$. Furthermore, each $S(f_i,f_k)$ has multidegree $< \delta$.

Proof: Let d_i=LC (f_i) so that c_id_i is the leading coefficient of c_if_i. Since the c_if_i have multi degree δ and their sum has strictly smaller multi degree, it follows that $\sum_{i=1}^{s} c_i d_i = 0$.

Define $p_i = \frac{f_i}{d_i}$ and note that p_i has leading coefficient 1. Consider the telescoping sum $\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i = c_1d_1(p_1-p_2)+(c_1d_1+\ldots+(c_1d_1+\ldots+c_{s-1},d_{s-1})(p_{s-1}-p_s)+(c_1d_1+\ldots+c_sd_s)p_s$.

By assumption, LT (fi) = $d_i x^{\delta}$, which implies that the least common multiple of LM (f_i) and LM (f_j) is x^{δ}, Thus

$$S(f_jf_k) = \frac{x^{\delta}}{LT(f_i)} f_i - \frac{x^{\delta}}{LT(f_k)} f_k = \frac{x^{\delta}}{d_jx^{\delta}} f_j - \frac{x^{\delta}}{d_kx^{\delta}} f_k = p_j - p_k \qquad (6.1)$$

Using this equation and $\sum_{i=1}^{s} c_i d_i = 0$ the above telescoping sum becomes:

$$\sum_{i=1}^{s} c_i f_i = c_1d_1S(f_1,f_2)+(c_1d_1+c_2d_2)S(f_2,f_3)+\ldots+(c_1d_1+\text{---}+c_{s-1}d_{s-1})S(f_{s-1},f_s),$$

which is sum of desired form. Since p_j and p_k have multidegree δ and leading coefficient 1, the difference $p_j - p_k$ has multidegree $< \delta$. By equation (6.1) the same is true of $S(f_j, f_k)$, and the lemma is proved.

Theorem 2.6.4 (Buchberger's criterion):- Let I be 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.

Proof: ($\Rightarrow$) If G is a Groebner basis, then since $S(g_i, g_j) \in I$, the remainder on division by G is zero by Corollary 2.6.2

($\Leftarrow$) Let $f \in I$ be a non-zero polynomial, we must show that if the s-polynomials all have zero remainders on division by G, then $LT(f) \in LT(g_1)\ldots LT(g_t)$. Before giving the details, let us out line the strategy of the proof.

Given $f \in I = \langle g_1,\ldots,g_t\rangle$ there are polynomials $h_i \in K[x_1,\ldots,x_n]$ such that

$$f = \sum_{i=1}^{t} h_i g_i \qquad (6.2)$$

From Lemma 2.2.3 it follows that:

$$\text{multideg}(f) < \max(\text{multideg}(h_i g_i)) \qquad (6.3)$$

If equality does not occur, then some cancellation must occur among the leading terms of

(6.2). Lemma 2.6.3 will enable us to rewrite this in terms of S-polynomials. Then our assumption that S-polynomials have zero remainders will allow us to replace the S-polynomials by expressions that involve less cancellation. Thus we will get an expression for f that has less cancellation of leading terms. Continuing in this way, we will eventually find an expression (6.2) for f where equality occurs in (6.3). Then multideg (f) = multideg $(h_i g_i)$ for some i, and it will follow that LT (f) is divisible by LT (g_i). This will show that $LT(f) \in \langle LT(g_1),\ldots,LT(g_t)\rangle$, which is what we want to prove.

We now give the details of the proof. Given an expression (6.2) for f, let $m(i) = \text{multideg}(h_i g_i)$, and define $\delta = \max(m(1),\ldots,m(t))$. Then inequality (6.3) becomes $\text{multideg}(f) \leq \delta$.

Now consider all possible ways that f can be written in the form (6.2). For each such expression, we get a possible different δ. Since a monomial order is a well ordering, we can select an expression (6.2) for f such that δ is minimal.

We will show that once this minimal δ is chosen, we have multideg (f) = δ. Then equality occurs in (6.3), and as we observed, it follows that $LT(f) \in \langle LT(g_1),\ldots,LT(g_t)\rangle$. This will prove the theorem.

It remains to show multideg (f) = δ. We will prove this by contradiction. Equality can fail only when multideg (f) < δ. To isolate the terms of multidegree δ, let us write f in the following form:

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)=\delta} h_i g_i \qquad (6.4)$$

$$= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)} h_i g_i$$

The monomials appearing in the second and third sums on the second line all have multi degree < δ. Thus the assumption multideg (f) < δ means that the first sum also has multi degree < δ.

Let LT (h_i) = $c_i x^{\alpha(i)}$. Then the first sum $\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)<\delta} c_i x^{\alpha(i)} g_i$ has exactly the form described in lemma 2.6.3 implies that this sum is a linear combination of the S-polynomials $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$. However,

$$S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) = \frac{x^{\delta}}{x^{\alpha(j)} LT(g_j)} x^{\alpha(j)} g_j - \frac{x^{\delta}}{x^{\alpha(k)} LT(g_k)} x^{\alpha(k)} g_k$$

$$= x^{\delta - \gamma_{jk}} S(g_j, g_k)$$

Where $x^{\gamma_{jk}}$ = LCM (LM (g_j), LM (g_k)). Thus there are constants $c_{jk} \in k$ such that

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{j,k} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k) \qquad (6.5)$$

The next step is to use our hypothesis that the remainder of $S(g_j, g_k)$ on division by $g_1, \ldots, g_t$ is zero. Using the division algorithm, this means that each s-polynomial can be written in the form.

$$S(g_i, g_k) = \sum a_{ijk} g_i \qquad (6.6)$$

Where $a_{ijk} \in k[x_1, \ldots, x_n]$. The division algorithm also tells us that

$$\text{Multideg } (a_{ijk} g_i) \leq \text{multideg } (S(g_j, g_k)) \qquad (6.7)$$

For all i,j,k. Intuitively this says that when the remainder is zero, we can find an expression for $s(g_j, g_k)$ in terms of G where the leading terms do not all cancel.

To exploit this, multiply the expression for S (g_j,g_k) by $x^{\delta - \gamma_{jk}}$ to obtain.

$$x^{\delta - \gamma_{jk}} S(g_j, g_k) = \sum_{i=1}^{s} b_{ijk} g_i,$$

Where $b_{ijk} = x^{\delta-\gamma_{jk}} a_{ijk}$. Then (6.7) and lemma 2.6.3 imply that multideg $(b_{ijk}\, g_i) \leq$ multideg $(x^{\delta-\gamma_{jk}} S(g_j, g_k) < \delta$. (6.8)

If we substitute the above expression for $x^{\delta-\gamma_{jk}} S(g_j,g_k)$ in to (6.5) we get an equation.

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j g_k) = \sum_{j,k} c_{jk}\left(\sum_i b_{ijk} g_i\right) = \sum_i \bar{h}_i g_i$$

Which by (6.8) has the property that for all i,

$$\text{multi deg}\,(\bar{h}_i g_i) < \delta.$$

For the final step in the proof, substitute $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i h_i g_i$ in to equation (6.4) to Obtain an expression for f as a polynomial combination of the g_i's where all terms have multi degree $< \delta$.This contradicts the minimality of δ and complete the proof of the theorem.

Remark: - Theorem 2.6.4 sometimes called "Buchberger's S-pair criterion" and is one of the key results about Groebner bases.

Example 2.6.2 (An example how to use theorem 2.6.4):- Consider the ideal $I = \langle y-x^2, z-x^3\rangle$ of the twisted cubic in $\mathbb{R}^3$. We claim that $G = \{y-x^2, z-x^3\}$ is a Groebner basis for lex order with $y > z > x$. To prove this, consider the S-polynomial.

$$S(y-x^2, z-x^3) = \frac{yz}{y}(y-x^2) - \frac{yz}{z}(z-x^3) = -zx^2 + yx^3.$$

Using the division algorithm, one finds,

$$-zx^2+yx^3 = x^3.(y-x^2) + (-x^2).(z-x^3) + 0$$

So that $\overline{s(y-x^2, z-x^3)}^{G} = 0$. Thus, by theorem (2.6.4), G is Groebner basis for I. We can also check that G is not Groebner basis for lex order $x > y > z$.

2.7 Buchberger's Algorithm

In this section we turn to the question given an ideal $I \subseteq K[x_1,\ldots,x_n]$, how can we actually construct a Groebner basis for I?

Example2.7.1 Consider the ring K[x,y] with grlex order, and let

$I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Recall that $\{f_1, f_2\}$ is not a Groebner basis for I since $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

To produce a Groebner basis, one natural idea is to try first to extend the original generating set to a Groebner basis by adding more polynomials in I. In one sense, this adds nothing new, and even introduces an element of redundancy. However, the extra information we get form a Groebner basis more than makes up for this. We have $S(f_1, f_2) = -x^2 \in I$, and its remainder on division by $F = (f_1, f_2)$ is $-x^2$, which is non zero. Hence we should include that reminder in our generating set, as a new generator $f_3 = -x^2$. If we set $F = (f_1, f_2, f_3)$, we can use theorem 2.6.4 to test if this new set is a Groebner basis for I. We compute $S(f_1, f_2) = f_3$, so

$$\overline{S(f_1, f_2)}^F = 0$$

$$S(f_1, f_3) = (x^3 - 2xy) - (-x)(-x^2) = -2xy, \text{ but}$$

$$\overline{S(f_1, f_3)}^F = -2xy \neq 0$$

Hence we must add $f_4 = -2xy$ to our generating set. If we let $F = (f_1, f_2, f_3, f_4)$ then $\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0$

$$S(f_1, f_4) = y(x^3 - 2xy) - \left(\frac{-1}{2}\right)x^2(-2xy) = -2xy^2 = yf_4, \text{ so}$$

$$\overline{s(f_1, f_4)}^F = 0$$

$$S(f_2, f_3) = (x^2y - 2y^2 + x) - (-y)(-x^2) = -2y^2 + x, \text{ but}$$

$\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0$. Thus we must add $f_5 = -2y^2 + x$ to our generating set.

Setting $F = \{f_1, f_2, f_3, f_4, f_5\}$, one can compute that $\overline{S(f_i, f_j)}^F = 0$ for all $1 \leq i \leq j \leq 5$.

By theorem 2.6.4 it follows that a grlex Groebner basis for I is given by

$$\{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x\}.$$

The above example suggests that in general, one should try to extend a basis F to a Groebner basis by successively adding non-zero remainders $\overline{S(f_i, f_{i+1})}^F$ to F. This idea is natural consequence of the S-pair criterion from section 2.6.

Lemma 2.7.1 Let G be a Groebner basis for the polynomial ideal I. let p ∈ G be a polynomial such that

LT (p) ∈ <LT (G- {p}) > .Then G- {p} is also a Groebner basis for I.

Proof: We know that < LT (G)> = <LT (I)>. If LT (p) ∈ < LT (G- {p}) >, then

<LT (G- {p})> = < LT (G)>. By definition ,it follows that G - {p} is also a Groebner basis for I.

By adjusting constants to make all leading coefficient 1 and removing any p with LT (p)∈ <LT (G- {p}) > from G we arrive at what we will call a **minimal** Groebner basis.

Definition 2.7.1:- A **minimal Groebner basis** for a polynomial ideal I is a Groebner basis G for I such that:

i) LC (p) = 1 for all p ∈ G

ii) For all p ∈G, LT (p) ∈ < LT (G- {p}) >.

Definition 2.7.2:- A **reduced Groebner basis** for a polynomial ideal I is a Groebner basis G for I such that

i) LC (p) = 1 for all p ∈ G

ii) For all p ∈ G no monomial of P lies in <LT (G-{p}) >

Many computer algebra systems implement a version of Buchberger's algorithm for computing Groebner basis. These systems always compute a Groebner bases whose elements in a reduced Groebner basis.

To conclude this section, we will indicate briefly some of the concentrations between Buchberger's algorithm and the row reduction (Gaussian elimination) algorithm for systems of linear equations. The interesting fact here is that the row reduction algorithm is essentially a special case of the general algorithm we have discussed. For the concreteness, we discuss the special case corresponding to the system of linear equations.

$$3x-6y-2z = 0$$

$$2x-4y+4w = 0$$

$$x-2y-z-w = 0$$

If we use the row operations on the coefficient matrix to put it in row echelon form (which means that the leading 1's have been identified) then we get the matrix

$$\begin{pmatrix} 1 & -2 & -1 & -1 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad (7.1)$$

this leads to the matrix,

$$\begin{pmatrix} 1 & -2 & 0 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad (7.2)$$

To translate these computations into algebra, let I be the ideal

$I = \langle 3x-6y-2z, 2x-4y+4w, x-2y-z-w \rangle \subseteq K[x, y, z, w]$ corresponding to the original system of equations we use lex order with $x > y > z > w$,the linear forms determined by the row echelon matrix in (7.1) given a minimal Groebner basis.

$I = \langle x-2y-z-w, z+3w \rangle$ and we will also check that the reduced row echelon matrix in (7.2) gives the reduced Groebner basis $I = \langle x-2y+2w, z+3w \rangle$.

Recall from linear algebra that every matrix can be put in reduced row echelon form in a unique way.

This can be viewed as a special case of the uniqueness of a reduced Groebner basis.

2.8 First Applications of Groebner Bases

In section 2.1 we posed three problems concerning ideals and varieties .The first was the ideal description problem. Which was solved by the Hilbert basis theorem on section 2.5?

Let us now consider the two remaining problems and see to what extent we can solve them using Groebner basis.

The Ideal membership problem

If we combine Groebner basis with the division algorithm, we get the following ideal member ship algorithm: given an ideal $I = \langle f_1, \ldots, f_s \rangle$, we can decide whether a given polynomial f lies in I as follows. First, using an algorithm similar to theorem 2.7.1 finds a Groebner bases $G = g_1, \ldots, g_t$ for I then corollary 2.6.2 implies that $f \in I$ iff $\overline{f}^{G} = 0$.

Example 2.8 .1 Let $I = < f_1,f_2> = < xz -y^2,x^3-z^2 > \in \mathbb{C}$ (x,y,z) and use grlex order .

Let $f= -4x^2 y^2z^2+y^6+3z^5$. We want to know if $f \in I$.

The generating set given is not a Groebner basis of I, because LT (I) also contains polynomials such as $LT (S(f_1,f_2)) = LT (-x^2y^2+z^3)= x^2y^2$ that are not in the ideal

$$<LT (f_1), LT (f_2)>= < xz,x^3>.$$

Hence we begin by computing a Groebner basis for I .Using a computer algorithm system, we find a Groebner bases

$$G = (f_1,f_2,f_3 ,f_4 ,f_5) = (x z-y^2,x^3-z^2,x^2y^2 -z^3,xy^4-z^4,y^6-z^5).$$

We may now test polynomials for membership in I . For example dividing f above by G , we find $f= (-4xy^2z-4y^4)f_1+0f_2+0f_3+0f_4+(-3)f_5+0$. Since the remainder is zero, we have $f \in I$.

For another example consider $f=xy-5z^2+x$. Even without completely computing the remainder on division by G. We can see from the form of the elements in G that $f \notin I$. The reason is that LT (f) = xy is clearly not in the ideal $< LT (G)> = < xz,x^3,x^2y^2,xy^4,y^6>$ hence $\overline{f}^G \neq 0$, to that $f \notin I$ .This last observation illustrates the way the properties of an ideal are reversed by the form of the elements of a Groebner basis.

The problem of solving polynomial equations

Next we will investigate how the Groebner basis technique can be applied to solve system of polynomial equations in several variables. Let us begin by looking at some specific example

Example2.8.2 *Consider* the equations

$$\begin{aligned} x^2 +y^2+z^2 &= 1 \\ x^2+z^2 &= y \\ x &= z \end{aligned} \qquad (8.1)$$

In $\mathbb{C}^3$, these equations determine $I = < x^2+y^2+z^2-1,x^2+z^2-y,x-z> \subseteq \mathbb{C}(x,y,z)$ and we want to find all points in V(I) , we can compute V(I) using any basis of I .So let us see what happens when we use a Groebner basis.

Though we have no compelling reason as of yet to do so, we will compute a Groebner basis on I with respect to the lex order. The basis is

$$g_1 = x\text{-}z$$

$$g_2 = -y+2z^2$$

$$g_3 = z^4 + (\tfrac{1}{2})\, z^2 - (\tfrac{1}{4})$$

If we examined these polynomials closely, we find something remarkable. First the polynomial g_3 depends on z alone and its roots can be found by first using quadratic formula to solve for z^2, then taking square root, $z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5}-1}$. This gives us four values of z. Next when these values of z are substituted in the equations of $g_2 = 0$ and $g_1 = 0$ those two questions can be solved uniquely for y and x respectively. Thus, there are four solutions all together of $g_1 = g_2 = g_3 = 0$, two real and two complex. Since V (I) = V (g_1, g_2, g_3), we have found all solutions of the original equation (8.1).

To summarize our findings in this section, we have seen that Groebner basis and a division algorithm give a complete solution of the ideal membership problem. Furthermore, we have seen ways to produce solutions of system of polynomial equations and to produce equations of parametrically given subsets of affine space. The examples given earlier depended on the fact that Groebner bases when computed using lex order, seem to eliminate variables in a very nice fashion.

REFERENCES

[1]. David Cox John Little Donal O'Shea, *IDEALS, VARAITIES, AND ALGORITHMS, An Introduction to Computational Algebraic Geometry and Commutative Algebra*, USA 2007.

[2]. Louis Halle Rowen, Graduate Algebra: Commutative view, USA 2006.

[3].Paul B. Garrett ABSTRACT ALGEBRA, University of Minnesota Minneapolis, USA 2008

[4]. R.Y. SHARP, Steps in Commutative Algebra, Cambridge University Press 2000.

[5]. Werner Greub Linear Algebra, USA 1981.