ADDIS ABABA UNIVERSITY

School of Graduate Studies
Department of Mathematics

GRADUATE SEMINAR REPORT

ON

Elimination Theory

(SUBMITTED IN PARTIAL FULFILMENT OF THE M.Sc. DEGREE IN MATHEMATICS)

By: Tsegaye Mamo

May, 2010
Addis Ababa

Acknowledgment

I am extremely thankful to my adviser Dr. Tilahun Abebaw, an instructor in Addis Ababa University Mathematics Department, for his helpful suggestions, material support, and constructive comments in preparing this seminar report.

Also I would like to express my deep appreciation to the Department of Mathematics in supplying the necessary materials and computer typing for preparation of this seminar report.

My deep heart also felt thanks to all my families and friends for their cooperation on my way of preparing this paper.

Table of Contents

CHAPTER 1

Preliminaries

1.1 Polynomials of One variable

Definition 1.1.1 Given a non-zero polynomial $f \in K[x]$, let

$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m$ where $a_i \in K$ and $a_0 \neq 0$. [Thus m=deg (f)]

Then we say that, $a_0 x^m$ is the leading term of f, written LT (f) $= a_0 x^m$.

Example f(x) $= 2x^3 - 4x + 3$, then LT (f) $= 2x^3$, deg (f) $= 3$

Note: If f and g are non zero polynomials, then

$\deg(f) \leq \deg(g)$ if and only if LT (f) divides LT (g)

Proposition 1.1.2. (The Division Algorithm)

Let K be a field and let g be a non-zero polynomial in $k[x]$ .Then every $f \in k[x]$ can be written as $f = gq + r$ Where $q, r \in k[x]$, and either $r = 0$ or $\deg(r) < \deg(g)$.Furthermore, q and r are unique.

Proof: We first prove Existence of q, r .If deg (g)>deg (f) then we set $q = 0$ and $r = f$ .Otherwise, deg (f) $\geq$deg (g) .Let $f = a_0 + \cdots + a_m X^m$, where $a_m \neq 0$, and $g = b_0 + \cdots + b_n X^n$, where $b_n \neq 0$

Define the integer $d = m - n \geq 0$ .We will use induction in d.

Let $d = 0$, then m = n. We set $q = a_m / b_m$ and $r = f - qg$ .Notice that q is well – defined because $b_m \neq 0$ and that the coefficients of X^m in r vanishes ,whence $\deg(r) < m = \deg(g)$.

Induction step: Now we assume that this is true whenever d<k and let d = k, so that m= n + k. Let $f_1 = f - (a_m/b_n)X^{m-n}g$. Notice that $\deg f_1 < \deg f$, whence by induction there exists q_1, r with $\deg r < \deg g$ and $f_1 = q_1 g + r$.Therefore

$$f = f_1 + \frac{a_m}{b_n} X^{m-n} q = \left(q_1 + \frac{a_m}{b_n} X^{m-n} \right) g + r ,$$

Whence define $q = q_1 + (a_m/b_n)X^{m-n}$ and the result is true for d= k.

Suppose that $f = qg + r = Qg + R$,with $\deg r < \deg g$ and $\deg R < \deg g$.

Rearranging , we have $R-r=(q-Q)g$,whence g divides $R-r$.Since $\deg(R-r)<\deg g$, this can only happen if $R-r=0$,whence $R=r$.In this case $g(q-Q)=0$,which since $g\neq 0$ implies that $q-Q=0$ or , equivalently ,that $Q=q$.

The polynomial q and r in the statement of the theorem are called the quotient and remainder, respectively.

Finally we prove uniqueness. Proving the proposition is to show that q and r are unique. So suppose that $f=qg+r=q'g+r'$ $f=qg+r=q'g+r'$ where both r and r' have degree less than g (unless one or both are 0). If r$\neq r'$, then deg (r'-r) < deg (g).

On the other hand, since $(q-q')g=r'-r$.....(1). We would have $q-q'\neq 0$, and consequently, $\deg(r-r')=\deg((q-q')g)=\deg(q-q')+\deg(g)\geq\deg(g)$.

This contradiction forces $r'=r$ and then (1) shows that $q'=q$.

Corollary 1.1.3. If k is a field and $f\in k[x]$ is a non -zero polynomial, then f has at most deg (f) roots in k.

Proof: We will use induction on $m=\deg(f)$.

When $m=0$, f is a non -zero constant, and the corollary is obviously true.

Now assume that the corollary holds for all polynomials of degree $m-1$, and let f have degree m.

If f has no roots in k, then we are done. So suppose a is a root in k. If we divide f by x-a, then proposition 1.1.2 tells us that $f=q(x-a)+r$, where $r\in k$, since $x-a$, has degree one.

To determine r, evaluate both sides at $x=a$, which gives

$0=f(a)=q(a)(a-a)+r=r.$

It follows that $f=q(x-a)$. Note also that q has degree $m-1$. We claim that any root of f other than a is also a root of q. To see this, let $b\neq a$ be a root of f.

Then $0=f(b)=q(b)(b-a)$ implies that $q(b)=0$ since k is a field. Since q has at most $m-1$ roots by our inductive assumption f has at most m roots in k.

Corollary 1.1.4 If k is a field, then every idea of $k[x]$can be written in the form $< f >$ for some $f \in k[x]$. Further more f is unique up to multiplication by a non-zero constant in k.

Proof: Take an ideal I $\subseteq$k[x]. If I = {0}, then we are done since I= < 0 >. Other wise let f be a non- zero polynomial of minimum degree contained in I. we claim that < f > = I. The inclusion $< f > \subseteq I$ is obvious since I is an ideal .Going the other way take $g \in I$. By division algorithm, we have $g = qf + r$ where either r = 0 or deg(r) <deg (f).Since I is an ideal, $qf \in I$ and, thus, $r = g - qf \in I$.*If* $r \neq 0$, then deg(r) <deg (f), which would contradict our choice of f. Thus r = 0 so that $g = qf \in < f >$. This implies $I \subseteq < f >$.

Thus I = < f >

To show uniqueness, suppose that $< f >=< g >$. Then $f \in < g >$ implies that $f = hg$ for some polynomial h$\in$k[x]. Thus, deg (f) = deg (h) +deg (g)..... (2), so that $\deg(f) \geq \deg(g)$.

The same argument with f and g interchanged shows $\deg(g) \geq \deg(f)$, and it follows that deg (f) = deg (g).

Then (2) implies that deg (h) = 0, so that h is non-zero constant.

In general an ideal generated by one element is called a principal ideal. K[x] is a principal ideal domain, abbreviated PID.

The prove of Corollary1.1.4 tells us that the generator of an ideal in k[x] is the non-zero polynomial of minimum degree contained in the ideal.

Definition 1.1.5:-A greatest common divisor of polynomials $f, g \in k[x]$ is a polynomial h such that

i. h divides f and g

ii. If p is another polynomial which divides f and g, then p divides h. when h has these properties, we write h = GCD (f, g).

Proposition 1.1.6 let $f, g \in k[x]$ then:

i .GCD (f, g) exists and is unique up to multiplication by a non-zero constant in k.

ii .GCD (f, g) is a generator of the ideal $< f, g >$.

Proof. Considers the ideal $< f, g >$. Since every ideal of k[x] is principal (corollary 1.1.4), there exists h∈k[x] such that, <f, g >= <h>. We claim that h is the GCD of f, g.

To see this, first note that h divides f and g since $f, g \in < h >$. Thus, the first part of Definition 1.1.5 is satisfied.

Next suppose that $p \in k[x]$ divides f, g. This means that f = Cp and g =Dp for some $C, D \in k[x]$. Since $h \in < f, g >$, there are A, B such that $Af + Bg = h$. Substituting, we obtain $h = Af + Bg = ACp + BDp = (AC + BD)p$ which shows that p divides h. Thus, h = GCD (f, g).

This proves the existence of the GCD. To prove uniqueness, suppose that h' was another GCD of f and g. Then by the second part of Definition 1.1.5, h and h' would each divide the other. This easily implies that h is a non-zero constant multiple of h'.

Thus part (i) of the corollary is proved, and part (ii) follows by the way we found h in the above.

There is a classic algorithm, known as the Euclidean Algorithm, which computes the GCD of two polynomials in $k[x]$.

Example 1.1.7: Compute the GCD of $x^4 - 1$ and $x^6 - 1$.

Solution First, we use the division algorithm:

$x^4 - 1 = 0\,(x^6 - 1) + x^4 - 1$

$x^6 - 1 = x^2(\,x^4 - 1) + x^2 - 1$

$x^4 - 1 = (x^2 - 1)\,(x^2 + 1) + 0$

Then by Euclidean Algorithm, we have

GCD $(x^6 - 1, x^4 - 1)$ =GCD $(x^4 - 1, x^6 - 1)$ = GCD $(x^4 - 1, x^2 - 1)$

=GCD $(x^2 - 1, 0) = x^2 - 1$

Note that this GCD computation answers our earlier question of finding a generator for the ideal $<x^6-1\ ,\ x^4-1>$.

Namely, proposition1.1.6 and GCD $(x^4-1, x^6-1) = x^2$-1 imply that

$<x^4-1, x^6-1> = <x^2\text{-}1>$

Definition 1.1.8. A greatest common divisor of polynomials $f_1, f_2, ..., f_s \in \mathrm{K}[x]$ is a polynomial h such that

i. h divides $f_1, f_2, ..., f_s$.

ii. If p is another polynomial which divides $f_1, f_2, ..., f_s$, then p divides h.

iii. When h has these properties, we writer

$h = GCD(f_1, ..., f_s)$.

Proposition 1.1.9 Let $f_1, f_2, ..., f_s \in \mathrm{K}[x]$, where $s \geq 2$. Then:

i. $GCD(f_1, f_2, ..., f_s)$ exists and is unique up to a multiplication by a non-zero constant in k.

ii. $GCD(f_1, f_2, ..., f_s)$ is a generator of the ideal $< f_1, f_2, ..., f_s >$.

iii. If $s \geq 3$, then $GCD(f_1, f_2, ..., f_s) = GCD(f_1, GCD(f_2, f_3, ..., f_s))$.

Proof. The prove of part (i) and (ii) are similar to the proofs given in Proposition1.1.6.

To prove part (iii), let h = GCD $(f_2, f_3, ..., f_s)$, then <f, h> $= < f_1, f_2, ..., f_s >$

By part ii of this proposition we see that

$<GCD(f_1, h)> = <GCD(f_1, f_2, ..., f_s)>$.Then GCD $(f_1,$ h) =GCD $(f_1, f_2, ..., f_s)$ follows from the uniqueness part of Corollary 1.1.4.

For example, suppose that we wanted to compute the GCD of four polynomials f_1, f_2, f_3, f_4. Using part (iii) of the proposition twice, we obtain

GCD (f_1, f_2, f_3, f_4) =GCD $(f_1, GCD(f_2, f_3, f_4))$

$= GCD(f_1, GCD(f_2, GCD(f_3, f_4)))$

Then if we use the Euclidean Algorithm three times, we get the GCD of f_1, f_2, f_3, f_4.

Example 1.1.10 Compute the GCD of x^3-3x+2, x^4-1, x^6-1

Solution. Consider the ideal $<x^3-3x+2, x^4-1, x^6-1> \in$ k[x]

We know that GCD (x^3-3x+2, x^4-1, x^6-1)

= GCD $((x^3-3x+2, GCD(x^4-4, x^6-1))$

$= GCD(x^3-3x+2, x-1^2)$

= x-1

Therefore GCD $(x^3-3x+2, x^4-1, x^6-1) = x-1$

It follows that $<x^3-3x+2, x^4-1, x^6-1>=<$x-1$>$

1.2. Polynomials of n-variables

Definition 1.2.1. A monomial in, $x_1, x_2, ..., x_n$, is a product of the form $x_1^{\alpha_1}.x_2^{\alpha_2}....x_n^{\alpha_n}$, where all of the exponents $\alpha_1, \alpha_2, ..., \alpha_n$, are non-negative integers. The total degree of this monomial is the sum $\alpha_1+\alpha_2+...+\alpha_n$.

We can simplify the notion for monomials as follows: let $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ be an n- tuple of non-negative integer's .Then we set $x^\alpha = x_1^{\alpha_1}.x_2^{\alpha_2}....x_n^{\alpha_n}$. When $\alpha = (0,0,...,0)$, note that $x^\alpha = 1$. We also let $|\alpha| = \alpha_1+\alpha_2+...+\alpha_n$ denote the total degree of the monomial x^α.

Definition 1.2.2: A polynomial f in $x_1, x_2, ..., x_n$, with coefficients in k is a linear combination (with coefficients in k) of monomials. We will write a polynomial f in the form $f = \sum_\alpha a_\alpha x^\alpha, a_\alpha \in k$ .Where the sum is over a finite number of n-tuples $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$.

The set of all polynomials in $x_1, x_2, ..., x_n$, with coefficients in k is denoted by $k[x_1, x_2, ..., x_n]$.

Example 1.2.3 $f = 2x^3y^2z^2 + \frac{3}{2}y^3z^3 - 3xyz + y^2$ polynomial in $\mathbb{Q}$ [x, y, z].

We will usually use the letters f, g, p, q, r to refer to polynomials.

Definition 1.2.4. 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 1.2.5 $f = 2x^3y^2z^2 + \frac{3}{2}y^3z^3 - 3xyz + y^2$ f has four terms and total degree six.

Note. i. The sum and product of two polynomial is again a polynomial.

ii. We say that a polynomial f divides a polynomial g provided that $g = fh$ for some h$\in k[x_1, x_2, ..., x_n]$.

1.3. Affine Space and Affine Varieties

Definition 1.3.1. Given a field k and a positive integer n, we define the n-dimensional affine space over k to be the set

$$k^n = \{(a_1, a_2, ..., a_n): a_1, a_2, ..., a_n \in \mathrm{k}\}.$$

Example 1.3.2 For an example of affine space, $\mathbb{R}^n$.

In general k=k^1 the affine line.

k= k^2 the affine plane.

Proposition 1.3.3. (Fundamental Theorem of Algebra)

Every non-constant polynomial $f \in \mathbb{C}[x]$ has a root in $\mathbb{C}$.

We say that a field k is algebraically closed if every non-constant polynomial in k[x] has a root in k.

Thus $\mathbb{R}$ is not algebraically closed (Since $x^2 + 1$ has no root in $\mathbb{R}$)

$\mathbb{C}$ is algebraically closed.

Definition 1.3.4. Let k be a field, and let $f_1, f_2, ..., f_s$, be 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 $f_1, f_2, ..., f_s$.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 $f_1(x_1, ..., x_n) = ... = f_s(x_1, ..., x_n) = 0$.

We will use the letters v, w, etc to denote affine varieties.

Definition 1.3.5: Let k be a field. A rational function in $t_1,t_2,...,t_m$ with coefficients in k is a quotient $\frac{f}{g}$ of two polynomials $f,g\in k[t_1,t_2,...,t_m]$, where g is not the zero polynomial. The set of all rational functions in $t_1,t_2,...,t_m$ with coefficients in k is denoted $k(t_1,t_2,...,t_m)$.

Note.1. Two rational functions f/g and h/k are equal provided that $kf = gh$ in $k(t_1,t_2,...,t_m)$.

2. $k(t_1,t_2,...,t_m)$ is a field.

1.4. Ideals

Definition 1.4.1: A subset $I\subseteq k[x_1,x_2,...,x_n]$ is an ideal if it satisfies

i. $0\in I$.

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

iii. If $f\in I\ and\ h\in k[x_1,...,x_n], then\ fh\in I$.

Definition 1.4.2: Let $f_1,f_2,...,f_s$ be polynomials in $k[x_1,x_2,...,x_n]$.Then we set

$$<f_1,f_2,...,f_s>=\{\sum_{i=1}^{s}h_if_i : h_1,...,h_s\in k[x_1,x_2,...,x_n]\}.$$

Lemma 1.4.3. If $f_1,f_2,...,f_s\in$ k $[x_1,x_2,...,x_n]$, then $<f_1,f_2,...,f_s>$ is an ideal of $k[x_1,x_2,...,x_n]$.We will call $<f_1,f_2,...,f_s>$ the ideal generated by $f_1,f_2,...,f_s$.

Proof first $0\in<f_1,f_2,...,f_s>$. Since $0=\sum_{i=1}^{s}0f_i$.

Suppose that $f=\sum_{i=1}^{s}p_if_i$ and $g=\sum_{i=1}^{s}q_if_i$ and let $h\in k[x_1,x_2,...,x_n]$

Then the equation

$$f+g=\sum_{i=1}^{s}(p_i+q_i)f_i \Rightarrow f+g\in I$$

$$hf=\sum_{i=1}^{s}(hp_i)f_i \Rightarrow hf\in I.$$

Thus $<f_1,f_2,...,f_s>$ is an ideal of $k[x_1,x_2,...,x_n]$.

Definition 1.4.4: Let $V \subseteq k^n$ be an affine variety. Then we set

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

Lemma 1.4.5: If $V \subseteq k^n$ is an affine variety, then $I(V) \subseteq k[x_1, x_2, ..., x_n]$ 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 k^n, and so, in particular on V.

Suppose that, $f, g \in I(V)$ and $h \in k[x_1, x_2, ..., x_n]$.

Let $(a_1, a_2, ..., a_n)$ be an arbitrary point of V. Then

$f(a_1, a_2, ..., a_n)) + g(a_1, a_2, ..., a_n) = 0+0 = 0$ thus $f + g \in I(V)$

$h(a_1, a_2, ..., a_n)\ f(a_1, a_2, ..., a_n) = h(a_1, a_2, ..., a_n).0 = 0$. Thus $hf \in I(V)$.

Thus, I (V) is an ideal of $k[x_1, x_2, ..., x_n]$.

Lemma 1.4.6: If $f_1, f_2, ..., f_s \in k[x_1, x_2, ..., x_n]$,then

$< f_1, f_2, ..., f_s > \subseteq I(V(f_1, f_2, ..., f_s))$, although equality need not occur.

Proof: Let $f \in < f_1, f_2, ..., f_s >$ which means that $f = \sum_{i=1}^{s} h_i f_i$ for some polynomial $h_1, h_2, ..., h_s \in k[x_1, x_2, ..., x_n]$.

Since $f_1, f_2, ..., f_s$ vanish on $V(f_1, f_2, ..., f_s)$ so must $\sum_{i=1}^{s} h_i f_i$.

Thus f vanishes on $V(f_1, f_2, ..., f_s)$, which proves $f \in I(V(f_1, f_2, ..., f_s))$.

Thus $< f_1, f_2, ..., f_s > \subseteq I(V(f_1, f_2, ..., f_s))$.

1.5. Ordering on the monomials in $k[x_1, x_2, ..., x_n]$.

Definition 1.5.1. A monomial ordering on $k[x_1, x_2, ..., x_n]$ 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 $Z^n_{\geq 0}$ (i.e. our ordering be linear or total ordering means, that for every pair of monomials x^α and x^β exactly one of the three statements $x^\alpha > x^\beta$, $x^\alpha = x^\beta$ $x^\beta > x^\alpha$, should be true).

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 >.

Definition 1.5.2. (Lexicographic order (lex))

Let $\alpha = (\alpha_1, \alpha_2, ..., \alpha_n)$ and $\beta = (\beta_1, \beta_2, ..., \beta_n) \in Z^n_{\geq 0}$.

We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in Z^n$, the left most non-zero entry is positive .we will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Example 1.5.3: a. (1, 2, 0)$>_{lex}$ (0, 3, 4), Since $\alpha - \beta$ = (1,-1,-4).

b. (3, 2, 4) $>_{lex}$ (3, 2, 1), since $\alpha - \beta$ = (0, 0, 3).

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

$$x_1 >_{lex} x_2 >_{lex} x_3 >_{lex} \dots >_{lex} x_n.$$

Defintion 1.5.4. (Graded lex order) (grlex order)

Let $\alpha, \beta \in Z^n_{\geq 0}$. We say $\alpha >_{grlex} \beta$ if

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

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

Example 1.5.5: a. (1, 2, 3) $>_{grlex}$ (3, 2, 0) since $|(1,2,3)| = 6 > |(3,2,0)| = 5$

b. (1, 2, 4) $>_{grlex}$ (1, 1, 5) since $|(1,2,4)| = |(1,1,5)| = 5$ and

(1, 2, 4) $>_{lex}$ (1, 1, 5)

c. The variables are ordered according to the lex order i.e.

$$x_1 >_{grlex} x_2 >_{grlex} x_3 >_{grlex} \dots >_{grlex} x_n$$

Definition 1.5.6. (Graded reverse lex order).

Let $\alpha, \beta \in Z^n_{\geq 0}$. We say $\alpha >_{grevlex} \beta$ 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 $\alpha - \beta \in Z^n$ is negative. Like grlex, grevlex orders by total degree, but it "breaks ties" in different way.

Example 1.5.7.

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

b. $(1, 5, 2) >_{grevlex} (4, 1, 3)$ since $|(1,5,2)| = |(4,3,1)| = 8$ and

$$(1, 5, 2) - (4, 1, 3) = (-3, 4, -1).$$

c. Grevlex gives the same on the variables. That is

$$(1, 0, \ldots, 0) >_{grevlex} \cdots >_{grevlex} (0, 0, \ldots, 1) \text{ or}$$

$$x_1 >_{grevlex} x_2 >_{grevlex} \cdots >_{grevlex} x_n .$$

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 order, so that it looks at the left most (or largest) variable and favors the larger power.

In contrast, when grevlex finds the same total degree, it looks at the right most (or smallest) variable and favors the smaller power.

Example 1.5.8: $x^5yz >_{grlex} x^4yz^2$ since both monomials have total degree 7 and $x^5yz >_{lex} x^4yz^2$, but for a different reason: x^5yz is larger because the smaller variable z appears to a smaller power.

As with lex and grlex, there are n! grevex orderings corresponding to how the n variables are ordered.

Example 1.5.9: 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 order, we would have $f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2$.

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

Definition 1.5.10: Let $f = \sum_{\alpha} a_\alpha x^\alpha$ be a non-zero polynomial in $k[x_1, x_2, \ldots, x_n]$ and let > be a monomial order

i. The multidegree of f is

multideg (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) $= a_{multi\deg(f)} \in k$.

iii. The leading monomial of f is

LM (f) $= x^{multi\deg(f)}$ (with coefficient 1).

iv. The leading term of f is

LT (f) = LC (f). LM (f).

Example 1.5.11: let f = $4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ as before and let > denote the lex order. Then f = $-5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$

multideg (f) = (3, 0, 0)

LC (f) =-5

LM (f) = x^3

LT (f) =$-5x^3$

Definition 1.5.12: An ideal $I \subseteq k[x_1, x_2, ..., x_n]$ is a monomial ideal if there is a subset $A \subseteq Z^n_{\geq 0}$ (possibly infinite) such that I consists of all polynomials which are finite sums of the form $\sum_{\alpha \in A} h_\alpha x^\alpha$,where $h_\alpha \in k[x_1, x_2, ..., x_n]$. In this case, we write $I = \langle x^\alpha : \alpha \in A \rangle$.

Example 1.5.13: An example of monomial ideal is given by

$$I = \left\langle x^4y^2, x^3y^4, x^2y^5 \right\rangle \subseteq k[x, y].$$

Lemma 1.5.14: Let $I = \langle x^\alpha : \alpha \in A \rangle$ 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 $\alpha \in A$.

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, $x^\beta \in I$ then $x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, where $h_i \in k[x_1, x_2, ..., x_n]$ 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 that x^β is divisible by x^α exactly when $x^\beta = x^\alpha x^\gamma$ for some $\gamma \in Z^n_{\geq 0}$.This is

$\alpha + Z^n_{\geq 0} = \{\alpha + \gamma : \gamma \in Z^n_{\geq 0}\}$ consists of the exponents of all monomials divisible by x^α.

Lemma 1.5.15: let I be a monomial ideal and let $f \in k[x_1, x_2, ..., x_n]$, 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.

1.6. Groebner bases and properties of Groebner Bases

Definition 1.6.1: Let $I \subseteq k[x_1, x_2, ..., x_n]$ be an ideal other than $\{0\}$.

i. We denote by LT (I) the set of leading terms of elements of I. Thus,

LT (I) $= \{c\,x^\alpha$: there exists f$\in$ I with LT (f) $= c\,x^\alpha\}$.

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

If we are given a finite generating set for I, say $I = < f_1, f_2, ..., f_s >$, then

$< LT(f_1), LT(f_2), ..., LT(f_s) >$ and $< LT(I) >$ may be different ideals. It is true that $LT(f_i) \in LT(I) \subseteq < LT(I) >$ by definition, which implies

$< LT(f_1), ..., LT(f_s) > \subseteq < LT(I) >$ .However $< LT(I) >$ can be strictly larger.

Example 1.6.2: Let I=$< f_1, f_2 >$, where $f_1 = x^3$-2xy and $f_2 = x^2y$-2 y^2+x and use the grlex ordering on monomials in k[x, y]. Then

x^2 = x (x^2y-2 y^2+x)–y (x^3-2xy) .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 1.5.14.

Definition 1.6.3: Fix a monomial order. A finite subset $G = \{g_1, g_2, ..., g_t\}$ of an ideal I is said to be a Groebner basis (or standard basis) if

$< LT(g_1), ..., LT(g_t) = < LT(I) >$.Equivalently, but more informally, a set $\{g_1, g_2, ..., g_t\} \subseteq I$ 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 1.6.4. Fix a monomial order. Then every ideal $I \subseteq k[x_1, x_2, ..., x_n]$ other than $\{0\}$ has a Groebner basis. Further more, any Groebner basis for an ideal I is a basis of I.

Proposition 1.6.5. V (I) is an affine variety. In particular, if $I =< f_1, f_2, ..., f_s >$, then $V(I) = V(f_1, f_2, ..., f_s)$.

Proof: $I =< f_1, f_2, ..., f_s >$ for some finite generating set.

We claim that $V(I) = V(f_1, f_2, ..., f_s)$.

First, since $f_i \in$ I, if f $(a_1, a_2, ..., a_n) = 0$ for all f$\in$ I then,

$f_i(a_1, a_2, ..., a_n) = 0$, so V (I) $\subseteq V(f_1, f_2, ..., f_s)$ ..... (1)

On the other hand, let $(a_1, a_2, ..., a_n) \in V(f_1, f_2, ..., f_s)$ and let f$\in$ I.

Since $I =< f_1, f_2, ..., f_s >$ we can write

$$f = \sum_{i=1}^{s} h_i f_i \quad \text{for some } h_i \in k[x_1, x_2, ..., x_n].$$

But then f $(a_1, a_2, ..., a_n) = \sum_{i=1}^{s} h_i(a_1, ..., a_n) f_i(a_1, ..., a_n)$.

$$\sum_{i=1}^{s} h_i(a_1, ..., a_n).0 = 0$$

Thus, $V(f_1, f_2, ..., f_s) \subseteq$ V (I) ..... (2)

Thus from (1) and (2) $V(f_1, f_2, ..., f_s)$=V (I).

Note: The most important consequence of this proposition is that varieties are determined by ideals.

CHAPTER –TWO

2.1. ELIMINATION THEORY

This chapter will study systematic methods for eliminating variables from systems of polynomial equations. The basic strategy of Elimination Theory will be given in two main theorems: the Elimination Theorems and the Extension Theorem. We will prove these results using Groebner bases and the classic theory of resultants.

The Elimination and Extension Theorems

To get a sense of how elimination works, let us look at an example

Example 2.1.1 Solve the system of equations in $\mathbb{C}^3$.

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

Solution. If we let I be the ideal

$$I=\langle\ x^2 + y^2 + z^2 - 1, x^2 + y^2 - y\ ,\ x\text{-}z\ \rangle \ldots\ldots\ldots (2)$$

We want to find all points in V(I) .Proposition 1.6.5 implies that we can compute V(I) using Groebner basis of I.

Then a Groebner basis for I with respect to lex order is given by the three polynomials

$g_1 = x\text{-}z$

$g_2 = -y+2z^2 \ldots\ldots\ldots\ldots (3)$

$g_3 = z^4 + \frac{1}{2}z^2 - \frac{1}{4}$

It follows that equation (1) and (3) have the same solutions. However, since $g_3 = z^4 + \frac{1}{2}z^2 - \frac{1}{4}$ involves only z, we see that the possible z's are $z = \pm\frac{1}{2}\sqrt{\pm\sqrt{5}-1}$ (i.e. its roots can be found by first using the quadratic formula to solve for z^2 then, taking square roots).

This gives us four values of z (Namely $\pm\frac{1}{2}\sqrt{\sqrt{5}-1}$, $\pm\frac{1}{2}\sqrt{-\sqrt{5}-1}$)

Substituting these values in to $g_2 = -y+2z^2$, we can determine the possible y's.

From $g_2 = 0 \quad \Rightarrow -y+2z^2 = 0$

$\Rightarrow \quad y = 2z^2$

If $z = \frac{1}{2}\sqrt{\sqrt{5}-1}$ then $y = 2z^2 \qquad \Rightarrow y = \frac{\sqrt{5}-1}{2}$

If $z = -\frac{1}{2}\sqrt{\sqrt{5}-1}$ then $y = 2z^2 \qquad \Rightarrow y = \frac{\sqrt{5}-1}{2}$

If $z = \frac{1}{2}\sqrt{-\sqrt{5}-1}$ then $y = 2z^2 \qquad \Rightarrow y = \frac{-\sqrt{5}-1}{2}$

If $z = -\frac{1}{2}\sqrt{-\sqrt{5}-1}$ then $y = 2z^2 \qquad \Rightarrow y = \frac{-\sqrt{5}-1}{2}$

Then finally substitute the values of y and z in $g_1 = x-z$ gives the corresponding values of x.

i.e. $g_1 = 0 \Rightarrow x = z$

In this way, one can check that equation (1) have exactly four solutions that is the solution of the equation are

$$(\frac{1}{2}\sqrt{\sqrt{5}-1}, \frac{\sqrt{5}-1}{2}, \frac{1}{2}\sqrt{\sqrt{5}-1}) ,(-\frac{1}{2}\sqrt{\sqrt{5}-1}, \frac{\sqrt{5}-1}{2}, -\frac{1}{2}\sqrt{\sqrt{5}-1}) ,$$

$$(\frac{1}{2}\sqrt{-\sqrt{5}-1}, \frac{-\sqrt{5}-1}{2}, \frac{1}{2}\sqrt{-\sqrt{5}-1}) , (-\frac{1}{2}\sqrt{-\sqrt{5}-1}, \frac{-\sqrt{5}-1}{2}, -\frac{1}{2}\sqrt{-\sqrt{5}-1})$$

Since V (I) =V (g_1, g_2, g_3) . We have found all solutions of the original equation (two real and two complex solutions).

What enabled us to find these solutions? There were two things that made our success possible.

(Elimination step)

We could find $g_3 = z^4 + \frac{1}{2}z^2 - \frac{1}{4} = 0$ of our original equations which involved only z, i.e, we eliminate x and y from the system of equations.

(Extension step) once we solved the simpler equation $g_3 = 0$ to determine the values of z, we could extend these solutions to solutions of the original equations.

Definition 2.1.2 Given $I =< f_1, f_2, ..., f_s > \subseteq k[x_1, ..., x_n]$ ℓ^{th} elimination ideal I_ℓ is the ideal of $k[x_{\ell+1}, ..., x_n]$ defined by $I_\ell = I \cap k[x_{\ell+1}, ..., x_n]$.

Thus, I_ℓ consists of all consequences of $f_1 = ... = f_s = 0$ which eliminate the variables $x_1, x_2, ..., x_\ell$.

Note: 1. I_ℓ is an ideal of k $[x_{\ell+1}, ..., x_n]$.

2. I=I_0 is the 0^{th} elimination ideal.

3. Different orderings of the variables lead to different elimination ideals.

Theorem 2.1.3: (The Elimination Theorem)

Let $I \subseteq k[x_1, x_2, ..., x_n]$ be an ideal and let G be a Groebner basis of I with respect to lex order where $x_1 > x_2 > ... > x_n$ .Then, for every $0 \le \ell \le n$, the set

G_ℓ=G$\cap$k $[x_{\ell+1}, ..., x_n]$ is a Groebner basis of the ℓ^{th} elimination ideal I_ℓ.

Proof: Fix ℓ between 0 and n. Since $G_\ell \subseteq I_\ell$ by construction, it suffice to show that $< LT(I_\ell) >=< LT(G_\ell) >$ by definition of Groebner basis.

One inclusion is obvious (i.e. $< LT(G_\ell) > \subseteq < LT(I_\ell) >$).

To prove the other inclusion $< LT(I_\ell) > \subseteq < LT(G_\ell) >$ we need only show that the leading term LT (f), for an arbitrary f$\in I_\ell$, is divisible by LT (g) for some g$\in G_\ell$.

To prove this, note that f$\in$I which tells us that LT (f) is divisible by LT (g) for some g$\in$G since G is a Groebner basis of I. Since f$\in I_\ell$, this means that LT (g) involves only the variables $x_{\ell+1}, ..., x_n$ .Now comes the crucial observation: Since we are using lex order with $x_1 > x_2 > ... > x_n$,any monomial involving $x_1, x_2, \ldots, x_\ell$ is greater than all monomials in $k[x_{\ell+1}, ..., x_n]$,so that $LT(g) \in k[x_{\ell+1}, ..., x_n]$ implies $g \in k[x_{\ell+1}, ..., x_n]$ .This shows that g$\in G_\ell$.

Thus $< LT(I_\ell) > \subseteq < LT(G_\ell) >$.

There for $< LT(I_\ell) =< LT(G_\ell) >$ thee for

There for G_ℓ is a Groebner basis of I_ℓ .

Example 2.1.4: Consider the system of equations.

$x^2+y+z=1$

$x+y^2+z=1$.....(1)

$x+y+z^2=1$

If we let I be the ideal

$I=<x^2+y+z-1, x+y^2+z-1, x+y+z^2-1>$..... (2)

Then a Groebner basis for I with respect to lex order is given by the four polynomials

$g_1 = x+y+z^2-1$

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

$g_3 = 2yz^2+z^4-z^2$ ..... (3)

$g_4 = z^6-4z^4+4z^3-z^2$

It follows that equation (1) and (3) have the same solutions. Thus it follows from the Elimination Theorem that

$I_1 = I \cap \mathbb{C}[y, z] = < y^2-y-z^2+z, 2yz^2+z^4-z^2, z^6-4z^4+4z^3-z^2>$ (the first elimination ideal)

$I_2 = I \cap \mathbb{C}[z] = < z^6-4z^4+4z^3-z^2>$ (second elimination ideal).

The elimination theorem shows that a Groebner basis for lex order eliminates not only the first variable, but also the first two variables, the first three variables and so on.

Theorem 2.1.5 (The Extension Theorem)

Let $I = < f_1, f_2, ..., f_s > \subseteq \mathbb{C}[x_1, x_2, ..., x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \le i \le s$, write f_i in the form $f_i = g_i(x_2, ..., x_n)x_1^{N_i}$ + terms in which x_1 has degree $< N_i$, where $N_i \ge 0$ and $g_i \in \mathbb{C}[x_2, ..., x_n]$ is non-zero. Suppose that we have a partial solution $(a_2, ..., a_n) \in V(I_1)$. If $(a_2, ..., a_n) \notin V(g_1, ..., g_s)$, then there exists $a_1 \in \mathbb{C}$ such that $(a_1, a_2, ..., a_n) \in V(I)$.

The prove of this theorem uses resultants and will be given in Chapter 3.

Suppose that we have an ideal $I \subseteq k[x_1, x_2, ..., x_n]$.

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

To describe points of V (I), the basis idea is to build up solutions one coordinate at a time .Fix some ℓ between 1 and n.

This gives us the elimination ideal I_ℓ, and we will call a solution $(a_{\ell+1},...,a_n) \in V$ (I_ℓ) a partial solution of the original system of equations. To extend $(a_{\ell+1},...,a_n)$ to a complete solution in V (I), we first need to add one more coordinate to the solution. This means finding a_ℓ so that $(a_\ell, a_{\ell+1},...,a_n)$ lies in the variety V ($I_{\ell-1}$) of the next elimination ideal. More concretely, suppose that $I_{\ell-1} = < g_1,..., g_r >$ in k $[x_\ell, x_{\ell+1},...,x_n]$ .Then we want to find solutions $x_\ell = a_\ell$ of the equations

$g_1(a_\ell, a_{\ell+1},...,a_n) = ... = g_s(a_\ell, a_{\ell+1},...,a_n) = 0.$

Here we are dealing with polynomials of one variable x_ℓ , and it follows that the possible a_ℓ 's are just the roots of the GCD of the above r polynomials.

Example 2.1.6 Solve the system of equations

$$x^2+y+z=1$$
$$x+y^2+z=1 \quad \text{.....(1)}$$
$$x+y+z^2=1$$

If we let I be the ideal

$$I = <x^2+y+z-1,\ x+y^2+z-1,\ x+y+z^2-1> \quad \text{..... (2)}$$

Then a Groebner basis for I with respect to lex order is given by the four polynomials

$g_1 = x+y+z^2-1$

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

$g_3 = 2yz^2+z^4-z^2$ ..... (3)

$g_4 = z^6-4z^4+4z^3-z^2$

If follows that equations (1) and (3) have the same solutions. How ever, since

$g_4 = z^6-4z^4+4z^3-z^2 = z^2(z-1)^2(z^2+2z-1)$ involves only z. we see that the possible z's are 0, 1 and $-1 \pm \sqrt{2}$. Substituting these values in to

$g_2 = y^2-y-z^2+z=0$ and $g_3 = 2yz^2+z^4-z^2=0$

We can determine the possible y's.

If z = 0, g_2 = (y, 0) = y^2-y and g_3 =(y, 0) = 0

Therefore GCD (g_2 =(y, 0), g_3 =(y, 0)) =GCD (y^2-y, 0) = y^2-y.

Then the solution of g_2 = g_3 = 0 is the

GCD (g_2 = (y, 0), g_3 = (y, 0)) =GCD (y^2-y, 0) = y^2-y = 0

Thus y^2-y = 0 $\Rightarrow$ y = 0 and y=1

If z =1 g_2 = (y, 1) = y^2-y, g_3 = (y, 1) = y

Then the solution of g_2 = g_3 = 0 is the GCD (g_2 = (y, 1), g_3 = (y, 1)) =

GCD (y^2-y, y) = y $\Rightarrow g_2 = g_3 = 0$

$\Rightarrow$y = 0

Similarly when z=-1 $\pm \sqrt{2}$, then the value of y are y = -1 $\pm \sqrt{2}$.

Then finally substitute the above values of y and z in g_1 =x +y+ z^2 -1= 0

Gives the corresponding values of x.

In this way g_1 = 0 $\Rightarrow$ x = -y- z^2 +1 .Thus

If y=0, z = 0 then x =1

If y = 0, z =1, then x = 0

If y =1, z = 0, then x = 0.

If y = -1+$\sqrt{2}$, z =-1+$\sqrt{2}$, then x =-1+$\sqrt{2}$.

If y =-1-$\sqrt{2}$, z =-1-$\sqrt{2}$, then x =-1-$\sqrt{2}$.

Thus, equations (1) have five solutions:

(1,0,0),(0,1,0),(0,0,1),(-1+$\sqrt{2}$,-1+$\sqrt{2}$,-1+$\sqrt{2}$) and (-1-$\sqrt{2}$,-1-$\sqrt{2}$,-1-$\sqrt{2}$).

Example 2.1.7 Solve the system of equations

$x^2 + y^2 + z^2 = 4$

$x^2 + 2y^2 = 5$

$xz = 1$

Let $I = < x^2 + y^2 + z^2 - 1, x^2 - 2y^2 - 5, xz - 1 >$

Then a Groebner basis for I with respect to lex order is given by the three polynomials

$g_1 = 2z^3 - 3z + x$

$g_2 = -1 + y^2 - z^2$

$g_3 = 1 + 2z^4 - 3z^2$

From Groebner basis the solution in $\mathbb{C}^3$ are finite. The last polynomial depends on z (it is a generator of the second elimination ideal)

$I_2 = I \cap \mathbb{C}[z]$ and factor nicely in $\mathbb{Q}[z] \therefore 2z^4 - 3z^2 + 1 = (z-1)(z+1)(2z^2 - 1)$. Thus we have four possible z-values $z = \pm 1, \pm\frac{1}{\sqrt{2}}$. By the Extension Theorem, the first elimination ideal $I_1 = I \cap \mathbb{C}[y, z]$ is generated by $g_2 = y^2 - z^2 - 1$, $g_3 = 1 + 2z^4 - 3z^2$

Since the coefficient of y^2 in the first elimination ideal is non zero constant, every partial solution in $V(I_2)$ extended to a solution in $V(I_1)$. There are eight such points in all. To find them, we substitute a root of the last equation for z and solve the resulting equation for y, for instance substitute (z =1 in Groebner basis) will produce $[-1 + x, y^2 - 2, 0]$. So in particular, $y = \pm\sqrt{2}$. In addition since the coefficients of x in g_1 is non zero constant, then we can extend each partial solution in $V(I_1)$ (uniquely) to a point to $V(I)$. For this value of z, we have x =1.cary out the same procedure for the other values of z as well you should find that eight solutions

$$(1, \pm\sqrt{2}, 1), (-1, \pm\sqrt{2}, -1), (\sqrt{2}, \pm\frac{\sqrt{6}}{2}, \frac{1}{\sqrt{2}}), (-\sqrt{2}, \pm\frac{\sqrt{6}}{2}, -\frac{1}{\sqrt{2}})$$

Note: Observe that the theorem is stated only for the field k = $\mathbb{C}$.

To see why $\mathbb{C}$ is important, assume that k = $\mathbb{R}$.

Consider the equations. $x^2 = y$, $x^2 = z$.....*

Eliminating x gives y = z, so that we get the partial solutions (a, a), for all a $\in \mathbb{R}$. Since the leading coefficients of x in x^2-y and x^2-z never vanish, the extension theorem guarantees that (a, a) extends, provided we work over $\mathbb{C}$. Over $\mathbb{R}$, the situation is different. Here x^2= a has no real solutions when a is negative, so that

the only those partial solutions with a≥0 extended to real solutions of (*). This shows that the extension theorem is false over $\mathbb{R}$.

Example 2.1.8: consider the equation $\begin{matrix} xy = 1 \\ xz = 1 \end{matrix}$

Here $I =< xy-1, xz-1 >$ and an easy application of the Elimination Theorem shows that $I_1 =< y-z >$ (the first elimination ideal)

Eliminating x gives $y = z$, so that we get the partial solutions (y, z) = (a, a) all $a \in \mathbb{R}$.

The only one that dose not extended is (0, 0), which is the partial solution where the leading coefficients y and z of x vanish.

The extension theorem tells us that the extension step can fail only when the leading coefficients vanish simultaneously.

Thus the partial solutions are given by (a, a), and these all extended to complete solutions $(\frac{1}{a}, a, a)$ except for the partial solution (0, 0).

Finally, we should mention that the variety $V(g_1,...,g_s)$ where the leading coefficients vanish depends on the basis $\{f_1, f_2,..., f_s\}$ of I. Changing to a different basis may cause $V(g_1,...,g_s)$ to change.

Corollary 2.1.9 Let $I =< f_1, f_2,..., f_s > \subseteq \mathbb{C}[x_1,...,x_n]$ and assume that for some i,

f_i is of the form $f_i = cx_1^N + terms\ in\ which\ x_1\ has\ degree < N$,

Where $c \in \mathbb{C}$ is non-zero and N>0. If I_1 is the first elimination ideal of I and $(a_2,...,a_n) \in V(I_1)$, then there is $a_1 \in \mathbb{C}$ so that $(a_1, a_2,..., a_n) \in V(I))$.

Proof. This follows immediately from the Extension Theorem: since $g_i = c \neq 0$ implies

$V(g_1,...,g_s) = \phi$.

We have $(a_2,...,a_n) \notin V(g_1,...,g_s)$ V (for all partial solutions.

Note: The Extension Theorem is stated only for the case of eliminating the first variable x_1, it can be used when eliminating any number of variables.

Exmple 2.1.10. Consider the equations

$$x^2 + y^2 + z^2 = 1$$
$$xyz = 1 \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

A Groebner basis for $I = < x^2 + y^2 + z^2 - 1, xyz - 1 >$ with respect to lex order is:

$$g_1 = y^4 z^2 + y^2 z^4 - y^2 z^2 + 1$$

$$g_2 = x + y^3 z + yz^3 - yz$$

By the elimination theorem, we obtain

$$I_1 = \mathrm{I} \cap \mathbb{C}[\mathrm{y}, \mathrm{z}] = < g_1 >$$

$$I_2 = \mathrm{I} \cap \mathbb{C}[\mathrm{z}] = \{0\}.$$

Since $I_2 = \{0\}$, we have V (I_2) = $\mathbb{C}$ and, thus, every c$\in$ $\mathbb{C}$ is a partial solution. So we ask:

Which partial solutions $c \in \mathbb{C} = V(I_2)$ extended to (a, b, c) $\in$ V (I)?

The ideal is to extend c one coordinate at a time: first to (b, c), then to (a, b, c). To control which solutions extended, we will use extension theorem at each step. The crucial observation is that I_2 is the first elimination ideal of I_1. Thus, we will use the extension once to go c$\in$ V (I_2) to (b, c) $\in$ V (I_1), and second time to go to (a ,b , c) $\in$ V (I).

To start, we apply the extension theorem to go from I_2 to $I_1 = < g_1 >$. The coefficient of y^4 in g_1 is z^2 so that c$\in$ V (I_2) extents to (b, c) whenever $c \neq 0$. Note that $g_1 = 0$ has no solution when c = 0. The next step is to go from I_1 to I; that is, to find a so that

$(a, b, c) \in V(I)$.If we substitute (y, z) = (b, c) in to (1), we get two equations in x and, it is not obvious that there is a common solution x = a. This is where the extension theorem shows its power. The leading coefficients of x in $x^2 + y^2 + z^2 - 1$ and xyz-1 are 1 and yz respectively. Since 1 never vanishes, the extension theorem guaranties that a is always exists. We have thus proved that all partial solutions $c \neq 0$ extended to V (I).

CHAPTER -3

Unique Factorization and Resultant

The main task remaining in chapter two is to prove the Extension theorem .this will require that we learn some new algebraic tools concerning unique factorization and resultants. Both of these will be used in 3.3 when we prove the Extension Theorem.

3.1 Irreducible polynomial and unique factorization

Definition 3.1.1. Let k be a field. A polynomial $f \in k[x_1, x_2, ..., x_n]$ is irreducible over k if f is non constant and is not the product of two non constant polynomials in $k[x_1, x_2, ..., x_n]$.

Note: The concept of irreducibility depends on the field.

Example 3.1.2: let $f = x^2 + 1$ is irreducible over $\mathbb{Q}$ and $\mathbb{R}$, but over $\mathbb{C}$, we have $x^2 + 1 = (x+i)(x-i)$.

Proposition 3.1.3: Every non constant polynomial $f \in k[x_1, x_2, ..., x_n]$ can be written as a product of polynomials which are irreducible over k.

Proof. If f is irreducible over k, then we are done.Otherwise, we can write $f = gh$, where $g, h \in k[x_1, x_2, ..., x_n]$ are non constant.

Note that the total degrees of g and h are less than the total degree of f. Now apply this process to g and h: if either fails to be irreducible over k, we factor it in to non constant factors. Since the total degree drops each time we factor, this process can be repeated at most finitely many times. Thus f must be a product of irreducible.

Theorem 3.1.4 Let $f \in k[x_1, x_2, ..., x_n]$ be irreducible over k and suppose that f divides the product gh, where $g, h \in k[x_1, x_2, ..., x_n]$. Then f divides g or h.

Proof. We will use induction on the number of variables.

When n =1, we can use the GCD theory.

If f divides gh, then consider p = GCD (f, g)

If p is non constant, then f must be a constant multiple of p since f is irreducible, and it follows that f divides g.

On the other hand, if p is constant, we can assume p =1, and then we can find

A and B$\in k[x_1]$ such that $Af + Bg = 1$

If we multiply this by h, we get

$h = Afh + Bgh$

Since f divides gh, f is a factor of $Afh + Bgh$, and thus, f divides h .This proves the case n =1

Now assume that the theorem is true for n -1. We first discuss the special case where the irreducible polynomial dose not involves x_1:

1. $u \in k[x_2,...,x_n]$ irreducible, u divides $gh \in k[x_1, x_2,...,x_n] \Rightarrow$ u divides g or h.

To prove this, write $g = \sum_{i=0}^{\ell} a_i x_1^{\ i}$ and $h = \sum_{i=0}^{m} b_i x_1^{\ i}$, where $a_i, b_i \in k[x_2,...,x_n]$.

If u divides every a_i, then u divides g, and similarly for h. Hence, if u divides neither, we can find i, j $\geq$ 0 such that u divides neither a_i nor b_i. We will assume that i and j are the smallest subscripts with this property. Then consider $c_{i+j} = (a_0 b_{i+j} + a_1 b_{i+j-1} + ... + a_{i-1} b_{j+1}) + a_{ij} + (a_{i+1} b_{j-1} + ... + a_{i+j} b_0)$. By the way we chose i, u divides every term inside the first set of parentheses and, by the choice of j, the same is true for the second set of parentheses. But u divides neither a_i nor b_j, and since u is irreducible, our inductive assumption implies that u dose not divide $a_i b_j$.

Since u divides all other terms of c_{i+j}, it can not divide c_{i+j}. Thus c_{i+j} is the coefficient of $x_1^{\ i+j}$ in gh, and, hence u can not divide gh. This contradiction complete the proof of (1)

Now given (1), we can treat the general case .Suppose that f divides gh. If f doesn't involve x_1, then we are done by (1). So assume that f is non constant in x_1 . We will use the ring $k(x_2,...,x_n)[x_1]$, which is a polynomial ring in one variable over the field $k(x_2,...,x_n)$. Remember that elements of $k(x_2,...,x_n)$ are quotients of polynomials in $k(x_2,...,x_n)$. We can regard k $(x_1,\ldots,x_n)$ as lying in side $k(x_2,...,x_n)[x_1]$ .The strategy will be to work in the larger ring, where we

know the theorem to be true, and then pass back to the smaller ring $k[x_1, x_2, ..., x_n]$.

We claim that f is still irreducible when regarded as an element of $k(x_2, ..., x_n)[x_1]$.To see why, suppose we had a factorization of f in the larger ring, say $f = AB$. Here, A and B are polynomials in x_1 with coefficients in $k(x_2, ..., x_n)$. To prove that f is irreducible here, we must show that A or B has degree 0 in x_1. Let $d \in k[x_2, ..., x_n]$ be the product of all denominators in A and B. Then $\widetilde{A} = dA$ and $\widetilde{B} = dB$ are in $k[x_1, x_2, ..., x_n]$, and $d^2 f = \widetilde{A}\widetilde{B}$.....(2) in $k[x_1, x_2, ..., x_n]$. By Proposition3.1.3, we can write d^2 as a product of irreducible factors in $k[x_2, ..., x_n]$, and, by (1), each of these divides $\widetilde{A}$ or $\widetilde{B}$. We can cancel such a factor from both sides of (2), and after we have cancelled all of the factors, we are left with

f= $\widetilde{A}_1 \widetilde{B}_1$ in $k[x_1, x_2, ..., x_n]$.

Since f is irreducible in $k[x_1, x_2, ..., x_n]$, this implies that $\widetilde{A}_1$ or $\widetilde{B}_1$ is constant. Now these polynomials were obtained from the original A, B by multiplying and dividing by various elements of $k[x_2, ..., x_n]$. This shows that either A or B dose not involve x_1, and our claim follows.

Now that f is irreducible in $k(x_2, ..., x_n)[x_1]$, we know by the n =1 case of the theorem that f divides g or h in $k(x_2, ..., x_n)[x_1]$.Say $g = Af$ for some

A$\in k(x_2, ..., x_n)[x_1]$. If we clear denominator, we can write

$dg = \widetilde{A}f$.....(3) in $k[x_1, x_2, ..., x_n]$, where d$\in k[x_1, x_2, ..., x_n]$. By (1), every irreducible factor of d divides $\widetilde{A}$ or f. The latter is impossible since f is irreducible and has a positive degree in x_1. But each time an irreducible factor divides $\widetilde{A}$, we can cancel it from both sides of (3). When all the cancellation is done, we see that f divides g in $k[x_1, x_2, ..., x_n]$.

Corollary 3.1.5. Suppose that $f, g \in k[x_1, x_2, ..., x_n]$ have positive degree in x_1. Then f and g have a common factor in $k[x_1, x_2, ..., x_n]$ of positive degree in x_1 if and only if they have a common factor in $k(x_2, ..., x_n)[x_1]$.

Proof. If f and g have a common factor h in $k[x_1, x_2, ..., x_n]$ of positive degree in x_1, then they certainly, have a common factor in the larger ring $k(x_2, ..., x_n)[x_1]$. Going the other way, suppose that f and g have a common factor

h$\in k(x_2, ..., x_n)[x_1]$. Then

$f = \tilde{h}\tilde{f}_1$, $\tilde{f}_1 \in k(x_2, ..., x_n)[x_1]$.

g=$\tilde{h}\,\tilde{g}_1$, $\tilde{g}_1 \in k(x_2, ..., x_n)[x_1]$.

Now $\tilde{h}$, $\tilde{f}_1$ and $\tilde{g}_1$ may have denominators that are polynomials in $k[x_2, ..., x_n]$. Letting $d \in k[x_2, ..., x_n]$ be a common denominator of these polynomials, we get h=d$\tilde{h}$, f_1 =d$\tilde{f}_1$ and g_1=d$\tilde{g}_1$, in $k[x_1, x_2, ..., x_n]$. If we multiply each side of the above equations by d^2, we obtain $d^2 f = hf_1$, $d^2 g = hg_1$, in $k[x_1, x_2, ..., x_n]$.

Now let h_1 be an irreducible factor of h of positive degree in x_1. Since $\tilde{h} = \frac{h}{d}$ has positive degree in x_1, such an h_1 must exist. Then h_1 divides $d^2 f$, so that it divides d^2 or f by Theorem3.1.4. The former is impossible because $d^2 \in k[x_2, ..., x_n]$, and hence h_1 must divide f in $k[x_1, x_2, ..., x_n]$. A similar argument shows that h_1 divides g, and thus h_1 is the required common factor.

Theorem 3.1.6: Every non constant $f \in k[x_1, x_2, ..., x_n]$ can be written as a product $f = f_1 f_2 ... f_r$ of irreducible over k. Further, if $f = g_1 g_2 g_3 ... g_s$ is another factorization in to irreducible over k, then $r = s$ and the g_i's can be permuted so that each of f_i constant multiple of g_i.

Proof. Suppose $g_1 g_2 .... g_s = f_1 f_2 .... f_r$ then there exist i such that g_i divide f_i (By Theorem 3.1.4). Since f_i is irreducible then f_i is a constant multiple of g_i . Similarly for all i there exists g_i such that f_i is a constant multiple of g_i.

Since $\deg(f) = \deg(f_1) + ... + \deg(f_r) = \deg(g_1) + ...\deg(g_s)$, then $r = s$.

3.2. Resultants

Resultants play an important role in elimination theory and we want to know whether two polynomials, f, g $\in$k[x] have a common factor, finally we will study the resultant of two polynomials in $k[x_1, x_2, ..., x_n]$, and we will then use resultants to prove the extension theorem.

We find a common factor by using factoring f and g in to irreducible. Unfortunately, factoring can be a time consuming process. A more efficient method would be to compute the GCD of f and g using the Euclidean Algorithm. A drawback is that the Euclidean Algorithm requires division in the field k. As we will see later, this is something we want to avoid when doing elimination. So is there a way of determining whether a common factor exists with out doing any division in k.

Lemma 3.2.1: Let $f, g \in k[x]$ be polynomial of degree $\ell > 0$ and $m > 0$, respectively. Then f and g have a common factor if and only if there are polynomials $A, B \in k[x]$ such that:

i. A and B are not both zero

ii. A has degree at most m-1 and B has degree at most ℓ-1

iii. $Af + Bg = 0$

Proof: First, assume that f and g have a common factor $h \in k[x]$. Then $f = hf_1$, and $g = hg_1$, where $f_1, g_1 \in k[x]$. Note that f_1 has degree at most ℓ-1 and similarly $\deg(g_1) \le m-1$. Then $g_1 f + (-f_1)\, g = g_1 h f_1 - f_1\, h g_1 = 0$, and thus $A = g_1$ and $B = -f_1$ have the required properties.

Conversely, suppose that A and B have the above three properties. By (i), we may assume $B \neq 0$. If f and g have no common factor, then their GCD is 1, so we can find polynomials $\tilde{A}, \tilde{B} \in$k[x] such that $\tilde{A} f + \tilde{B} g = 1$

Now multiply by B and use Bg = -Af

$$B = (\tilde{A}f + \tilde{B}g)B = \tilde{A}fB + \tilde{B}gB = \tilde{A}fB - \tilde{B}Af = (\tilde{A}B - \tilde{B}A)f$$

Since B is non-zero, this equation shows that B has degree at least ℓ, which contradicts (iii).

Hence, there must be a common factor of positive degree.

Note: The answer given by lemma3.2.1. May not seem very satisfactory, for we still need to decide whether the required A and B exists. Remarkably, we can use linear algebra to answer this last question. The idea is turn Af +Bg = 0 in to a system of linear equations. Write

$$A = c_0 x^{m-1} + \ldots + c_{m-1}$$

$$B = d_0 x^{\ell-1} + \ldots + d_{\ell-1}$$

Where for now we will regard the $\ell + m$ coefficients $c_0, c_1, \ldots, c_{m-1}, d_0, d_1, \ldots, d_{\ell-1}$ as unknowns. Our goal it to find c_i, $d_i \in$ k, not all zero, so that the equation

$$Af + Bg = 0 \ldots\ldots\ldots\ldots\ldots\ldots (4) \text{ holds}$$

Note that this will automatically give us A and B as required in lemma3.2.5.

To get a system of linear equations, let us also write out f and g:

$$f = a_0 x^{\ell} + a_1 x^{\ell-1} + \ldots + a_{\ell}, \quad a_0 \neq 0$$

$g = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$, $b_0 \neq 0$, Where $a_i, b_i \in k$. If we substitute these formulas for f, g, A and B into equation (4) and compare the coefficients of powers of x, then we get the following system of linear equations with unknowns c_i and d_i and coefficients a_i, b_i in k.

$$\begin{aligned}
a_0c_0 \quad &+ \quad b_0d_0 \quad &&= 0 \ \textit{coefficient of } x^{\ell+m-1} \\
a_1c_0 + a_0c_1 \quad &+ \quad b_1d_0 + b_0d_1 \quad &&= 0 \ \textit{coefficient of } x^{\ell+m-2} \\
&\quad \vdots \quad &&\vdots \\
&\quad \vdots \quad &&\vdots \qquad \ldots\ldots\ldots\ldots (5) \\
&\quad \vdots \quad &&\vdots \\
a_{\ell}c_{m-1} \quad &+ \quad b_m d_{\ell-1} \quad &&= 0 \ \textit{coefficient of } x^0
\end{aligned}$$

Since there are $\ell + m$ linear equations and $\ell + m$ unknown, we know from linear algebra that there is a non -zero solution if and only if the coefficient matrix has zero determinant.

Definition 3.2.2: Given polynomials $f, g \in k[x]$ of positive degree, write them in the form

$$f = a_0 x^{\ell} + a_1 x^{\ell-1} + \ldots + a_{\ell} \quad , a_0 \neq 0$$

$$g = b_0 x^{m} + b_1 x^{m-1} + \ldots + b_m \quad , b_0 \neq 0$$

Then the Sylvester matrix of f and g with respect to x, denoted $Syl(f,g,x)$ is the coefficient matrix of the system of equations given in (5). Thus $Syl(f,g,x)$ is the following $(\ell + m)$ x $(\ell + m)$ matrix.

$$\mathrm{Syl}(f,g,x) = \underbrace{\begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ddots & & b_2 & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}}_{m \text{ columns}} \quad \underbrace{\qquad\qquad}_{l \text{ columns}}$$

Where the empty spaces are filled by zeros. The resultant of f and g with respect to x, denoted $\mathrm{Re}\,s(f,g,x)$, is the determinant of the Sylvester matrix. Thus

$$\mathrm{Re}\,s(f,g,x) = \det(Syl(f,g,x)).$$

Note: A polynomial is called an integer polynomial provided that all of its coefficients are integers.

Proposition 3.2.3: Given $f, g \in k[x]$ of positive degree, the resultant $\mathrm{Re}\,s(f,g,x) \in k$ is an integer polynomial in the coefficients of f and g. Further more, f and g have a common factor in $k[x]$ if and only if $\mathrm{Re}\,s(f,g,x) = 0$.

Proof: The standard formula for the determinant of an s× s matrix A=$(a_{ij})_{\ell \le i,j \le s}$ is

$\det(A) = \sum_{\substack{\sigma \text{ a permutation} \\ \text{of } \{1,2,\ldots,s\}}} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \ldots a_{j\sigma(j)}$,Where $\operatorname{sgn}(\sigma)$ is +1 if σ inter changes an even number of pairs of elements of {1,2,3,...,s} and -1 if σ interchanges an odd number of pairs. This shows that the determinant is an integer polynomial (in fact the coefficients are ± 1) in its entries, and the first statement of the proposition then follows immediately from the definition of resultant.

The second statement is just as easy to prove: the resultant is zero $\Leftrightarrow$

The coefficient matrix of equations (5) has zero determinants $\Leftrightarrow$ equation (5) have a non-zero solution. We observed earlier that this is equivalent to the existence of A and B as in Lemma3.2.1, and then Lemma3.2.1: completes the proof of the proposition.

Example 3.2.4: If $f = 2x^2 + 3x + 1$ and $g(x) = 7x^2 + x + 3$ have a common factor in $Q[x]$. One computes that

$$\operatorname{Res}(f,g,x) = \det\begin{pmatrix} 2 & 0 & 7 & 0 \\ 3 & 2 & 1 & 7 \\ 1 & 3 & 3 & 1 \\ 0 & 1 & 0 & 3 \end{pmatrix} = 153 \neq 0 .$$

So that there is no common factor.

Example 3.2.5

$$f(x) = x^3 - 3x^2 + 5x - 3$$
$$g(x) = 2x^2 - 7x + 5$$

$$\operatorname{Res}(f,g,x) = \begin{vmatrix} 2 & -7 & 5 & 0 & 0 \\ 0 & 2 & -7 & 5 & 0 \\ 0 & 0 & 2 & -7 & 5 \\ 1 & -3 & 5 & -3 & 0 \\ 0 & 1 & -3 & 5 & -3 \end{vmatrix} = 0,$$ then f and g have a common factor.

Note: One disadvantage to using resultants is that large determinants are hard to compute.

Example 3.2.6: Compute the resultants of the polynomials $f = xy - 1$ and $g = x + y^2 - 4$.

Solution: Regarding f and g as polynomials in x whose coefficients are polynomials in y, we get

$$\mathrm{Re}\,s(f,g,x) = \det\begin{pmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2-4 \end{pmatrix} = y^4 - 4y^2 + 1$$

Note: More generally, if f and g are any polynomials in $k[x,y]$, in which x appears to a positive power, and then we can compute $\mathrm{Re}\,s(f,g,x)$ in the same way. Since the coefficients are polynomials in y, Proposition3.2.3 guarantees that $\mathrm{Re}\,s(f,g,x)$ is a polynomial in y. Thus given $f,g \in k[x,y]$, we can use resultant to eliminate x.

Propostion 3.2.7: Given $f,g \in k[x]$ of positive degree, there are polynomials $A,B \in k[x]$ such that $Af + Bg = \mathrm{Re}\,s(f,g,x)$.

Further more, the coefficients of A and B are integer polynomials in the coefficients of f and g.

Proof: The definition of resultant was based on the equation $Af + Bg = 0$. In this proof, we will apply the same methods to the equation $\widetilde{A}f + \widetilde{B}g = 1$ .....(6).

The reason for using $\widetilde{A}$ rather than A will soon be apparent. The proposition is trivially true if $\mathrm{Re}\,s(f,g,x) = 0$ (simply choose $A = B = 0$), so we may assume $\mathrm{Re}\,s(f,g,x) \neq 0$.

Now let $f = a_0x^\ell + a_1x^{\ell-1} + ... + a_\ell \quad , a_0 \neq 0$

$$g = b_0x^m + b_1x^{m-1} + ... + b_m \quad , b_0 \neq 0$$

$$\widetilde{A} = c_0x^{m-1} + ... + c_{m-1}$$

$$\widetilde{B} = d_0x^{\ell-1} + ... + d_{\ell-1}$$

Where the coefficients $c_0, c_1, ..., c_{m-1}, d_0, d_1, ..., d_{\ell-1}$ are unknowns in k. If we substitute these formulas in to (6) and compare coefficients of powers of x, then we get the following system of linear equations with unknowns c_i and d_i and coefficients a_i, b_i in k.

$$
\begin{aligned}
a_0c_0 \quad &+ \quad b_0d_0 \quad &&= 0 \ \textit{coefficient of } x^{t+m-1} \\
a_1c_0 + a_0c_1 \quad &+ \quad b_1d_0 + b_0d_1 \quad &&= 0 \ \textit{coefficient of } x^{t+m-2} \\
&\vdots \qquad\qquad\quad \vdots \qquad\qquad\quad \vdots \\
a_tc_{m-1} \quad &+ \quad b_md_{t-1} \quad &&= 1 \ \textit{coefficient of } x^0
\end{aligned}
\qquad \ldots\ldots\ldots\ldots (7)
$$

These equations are the same as (5) except for the 1 on the right hand side of the last equation. Thus, the coefficient matrix is the Sylvester matrix of f and g, and then

$\mathrm{Re}\,s(f,g,x) \neq 0$ guarantees that (7) has a unique solution in k.

In this situation, we can use Cramer's rule to give a formula for the unique solution. In our case, Cramer's rule gives formula for the c_i's and d_i's.

For example, the first unknown c_0 given by

$$
c_0 = \frac{1}{\mathrm{Res}(f,g,x)} \det \begin{pmatrix} 0 & & & b_0 & & \\ 0 & a_0 & & \vdots & \ddots & \\ \vdots & \vdots & \ddots & \vdots & & b_0 \\ 0 & a_t & & a_0 & b_m & \vdots \\ \vdots & & \ddots & \vdots & \ddots & \vdots \\ 1 & & & a_t & & b_m \end{pmatrix}.
$$

Since a determinant is an integer polynomial in its entries, it follows that

$$
c_0 = \frac{an\ \mathrm{int}eger\ polynomial\ in\ a_i\ , b_i}{\mathrm{Re}\,s(f,g,x)}
$$

There are similar formulas for the other c_i's and the other d_i's. Since $\widetilde{A} = c_0x^{m-1} + \ldots + c_{m-1}$, we can pull out the common denominator Res (f, g, x) and write $\widetilde{A}$ in the form $\widetilde{A} = \dfrac{1}{\mathrm{Re}\,s(f,g,x)} B$

Where B∈k[x] has the same Properties as A .since $\widetilde{A}$ and $\widetilde{B}$ satisfy $\widetilde{A}$f + $\widetilde{B}$g=1, we can multiply through by

Res (f, g, x) to obtain

$$
Af + Bg = \mathrm{Re}\,s(f,g,x)
$$

Since A and B have the required kind of coefficients, the proposition is proved.

Example 3.2.8: Let $f = xy - 1$ and $g = x + y^2 - 4$. If we regard these as a polynomials in x, then Res (f, g, x) $= y^4 - 4y^2 + 1 \neq 0$.

Thus GCF (f, g) =1, then

$$-(\frac{y}{y^4 - 4y + 1}x + \frac{1}{y^4 - 4y + 1})f + (\frac{y^2}{y^4 - 4y + 1})g = 1$$

Note that this equation takes place in k(y) [x] i.e. the coefficients are rational functions in y. This is because the GCD theory requires field coefficients.

If we want to work in k[x, y], we must clear denominator which leads to

$$-(yx+1)\,f + y^2 g = y^4 - 4y^2 + 1$$

Note If $f, g \in k[x, y]$ are any polynomials of positive degree in x, then $Res(f, g, x)$ always lies in the first elimination ideal of $< f, g >$.

3.3. Resultants and the Extension Theorem

In this section we will prove the extension Theorem using the resultants. Our first task will be to adapt the theory of resultants to the case of polynomials in n variables.

Suppose we are given $f, g \in k[x_1, x_2, ..., x_n]$ of positive degree in x_1.

We write

$$f = a_0 x^{\ell} + a_1 x^{\ell-1} + ... + a_{\ell}\ ,\ a_0 \neq 0\ .$$

$$g = b_0 x^m + b_1 x^{m-1} + ... + b_m\ ,\ b_0 \neq 0 \qquad \text{..... (a)}$$

Where $a_i, b_i \in k[x_2, ..., x_n]$, and we define the resultant of f and g with respect to x_1 to be the determinant

$$\mathrm{Res}(f,g,x_1)=\det\underbrace{\begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ & a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix}}_{m\text{ columns}\qquad\qquad t\text{ columns}}$$

Where the empty spaces are filled by zeros.

Proposition 3.3.1: Let $f,g\in k[x_1,x_2,...,x_n]$ have positive degree in x_1. Then:

i. $\mathrm{Re}s(f,g,x_1)$ is in the first elimination ideal $<f,g>\cap k[x_2,...,x_n]$.

ii. $\mathrm{Re}s(f,g,x_1)=0$ if and only if f and g have a common factor in $k[x_1,x_2,...,x_n]$ Which has positive degree in x_1 .

Proof: When we write f, g in terms of x_1, the coefficients a_i , b_i lie in $k[x_2,...,x_n]$. Since the resultant is an integer polynomial in a_i , b_i (Proposition 3.2.7), it follows that $\mathrm{Re}s(f,g,x_1)\in k[x_2,...,x_n]$. We know that $Af+Bg=\mathrm{Re}s(f,g,x_1)$, where A and B are polynomials in x_1 whose coefficients are again integer polynomials in a_i,b_i (Proposition 3.2.7). Thus A, B$\in k(x_2,...,x_n)[x_1]=k[x_1,x_2,...,x_n]$, and then the above equation implies $\mathrm{Re}s(f,g,x_1)\in<f,g>$. This proves part (i) of the proposition.

To prove the second part, we will use Proposition 3.2.3 to interpret the vanishing of the resultant in terms of common factors. In section 3.2, we worked with polynomials in one variable with coefficients in a field. Since f and g are polynomials in x_1 with coefficients in $k[x_2,...,x_n]$the field the coefficients lie in $k(x_2,...,x_n)$. The Proposition 3.2.3, applied to $f,g\in k(x_2,...,x_n)[x_1]$, tells us that $\mathrm{Re}s(f,g,x)=0$ if and only if f and g have a common factor in $k(x_2,...,x_n)[x_1]$which has positive degree in x_1. But then we can apply Corollary

3.1.5, which says that this is equivalent to having a common factor in $k[x_1, x_2, ..., x_n]$ of positive degree in x_1.

Corollary 3.3.2. If $f, g \in \mathbb{C}[x]$, then $\mathrm{Re}\, s(f, g, x) = 0$ if and only if f and g have a common root in $\mathbb{C}$.

Proposition 3.3.3: let $f, g \in \mathbb{C}[x_1, x_2, ..., x_n]$ have degree ℓ, m respectively, and let $c = (c_2, ..., c_n) \in \mathbb{C}^{n-1}$ Satisfy the following:

i. $f(x_1, c) \in \mathbb{C}[x_1]$ has degree ℓ.

ii. $g(x_1, c) \in \mathbb{C}[x_1]$ has degree $p \le m$.

Then the polynomial $h = \mathrm{Re}\, s(f, g, x_1) \in \mathbb{C}[x_2, ..., x_n]$ satisfies

$h(c) = a_0(c)^{m-p}\, \mathrm{Re}\, s(f(x_1, c), g(x_1, c), x_1)$, where a_0 is in (a)

$f = a_0 x_1^{\ell} + a_1 x_1^{\ell-1} + ... + a_\ell$, $a_0 \neq 0$.

$g = b_0 x_1^{m} + b_1 x_1^{m-1} + ... + b_m$, $b_0 \neq 0$

Proof. If we substitute $c = (c_2, ..., c_n)$ for $x_2, ..., x_n$ in the determinantal formula for $h = \mathrm{Re}\, s(f, g, x_1)$, we obtain

$$h(\mathbf{c}) = \det \begin{pmatrix} a_0(\mathbf{c}) & & & b_0(\mathbf{c}) & & \\ \vdots & \ddots & & \vdots & \ddots & \\ \vdots & & a_0(\mathbf{c}) & \vdots & & b_0(\mathbf{c}) \\ a_l(\mathbf{c}) & & \vdots & b_m(\mathbf{c}) & & \vdots \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_l(\mathbf{c}) & & & b_m(\mathbf{c}) \end{pmatrix}$$

m columns $\quad$ l columns

First suppose that g (x_1, c) has degree p = m. Then our assumptions imply that

$\mathrm{f}(x_1, \mathrm{c}) = a_0(\mathrm{c})\, x_1^{\ell} + ... + a_\ell(c)$, $a_0(c) \neq 0$

$g(x_1, c) = b_0(c) x_1^{m} + ... + b_m(c)$, $b_0(c) \neq 0$.

Hence the above determinant is the resultant of f(x_1,c) and g(x_1,c), so that h(c)=Res(f(x_1,c),g(x_1,c), x_1)

This proves the proposition when p = m. when p $\leq$ m, the above determinant is no longer the resultant of $f(x_1,c)$ and $g(x_1,c)$ (it has the wrong size). Here we get the desired resultant by repeatedly expanding by minors along the first row.

Theorem 3.3.4 (The Extension Theorem)

Let $I =< f_1, f_2,..., f_s > \subseteq \mathbb{C}[x_1,...,x_n]$ and let I_1 be the first elimination ideal of I. For each $1 \leq i \leq s$, write f_i in the form

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + terms\ in\ which\ x_1\ has\ degree < N_i, \text{ where } N_i \geq 0$$

and $g_i \in \mathbb{C}[x_2,...,x_n]$ is non-zero. Suppose that we have partial solution $(c_2,...,c_n) \in V(I_1)$. If $(c_2,...,c_n) \notin V(g_1,...,g_s)$, then there exists $c_1 \in \mathbb{C}$ such that $(c_1,...,c_n) \in V(I)$.

Proof: As above, we set $c = (c_2,...,c_n)$. Then consider the ring homomorphism $\mathbb{C}[x_1,...,x_n] \to \mathbb{C}[x_1]$ defined by $f(x_1,...,x_n) \mapsto f(x_1,c)$, since the image of I is under this homomorphism is an ideal of $\mathbb{C}[x_1]$. Since $\mathbb{C}[x_1]$ is a PID, the image of I is generated by a single polynomial $u(x_1)$. In other words, $\{f(x_1,c) : f \in I\} =< u(x_1) >$.

If u (x_1) is non-constant, then there is $c_1 \in \mathbb{C}$ such that u (c_1) = 0 by the fundamental theorem of algebra. It follows that $f(c_1,c) = 0$ for all $f \in I$. So that $(c_1,c) = (c_1,...,c_n) \in V(I)$.

Note that this argument also works if $u(x_1)$ is the zero polynomial. It remains to consider what happens when $u(x_1)$ is a non-zero constant u_0. By the above equality, there is f∈I such that $f(x_1,c) = u_0$. We will show that this case can not occur. By hypothesis, our partial solution satisfies c $\notin$ V (g_1, g_2 ,…, g_s).

Hence $g_i(c) \neq 0$ for some i. Then consider

$$h = \mathrm{Res}(f_i, f, x_1) \in \mathbb{C}[x_2,...,x_n].$$

Applying proposition 3.3.3 to f_i and f, we obtain

$$h(c) = g_0(c)^{\deg(f)}\, \mathrm{Res}(f_i(x_1,c)\ , u_0\ , x_1)$$

Since f (x_1, c) = u_0. We also have Res (f_i (x_1, c), u_0, x_1)= $u_0^{N_i}$.

Hence $h(c)=g_0(c)^{\deg(f)}u_0^{N_i} \neq 0$

However f_i, f ∈ I and proposition 3.3.1 imply that h∈ I_1, so that h(c) = 0 since $c \in V(I_1)$. This contradiction completes the proof of the Extension Theorem.

Note: For concreteness, we stated the theorem only for the complex number ℂ.

The extension Theorem is true over any algebraically closed field.

REFERENCES

1. David Cox John Little Donal O'shea, IDEALS, VARITIES, AND ALGORITHMS, An Introduction to Computational Algebraic Geometry and Commutative Algebra, USA 2007.
2. David Eisenbud , Commutative Algebra with a view toward algebraic Geometry, Springer Science + Business Media, Inc,2004
3. Paul B.Garrett: ABSTRACT ALGEBRA, Universty of Minnesota Minneapolis, USA 2008
4. W.V.D.HODGE and D.PEDOE, Methods of Algebraic Geometry Volume 1, 1968.