

California State University, San Bernardino

CSUSB ScholarWorks

Theses Digitization Project

John M. Pfau Library

2000

Affine varieties, Groebner basis, and applications

Eui Won James Byun

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd-project>



Part of the [Mathematics Commons](#)

Recommended Citation

Byun, Eui Won James, "Affine varieties, Groebner basis, and applications" (2000). *Theses Digitization Project*. 1611.

<https://scholarworks.lib.csusb.edu/etd-project/1611>

This Project is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

/9590

AFFINE VARIETIES, GROEBNER BASIS, AND APPLICATIONS

A Project
Presented to the
Faculty of
California State University,
San Bernardino

In Partial Fulfillment
of the Requirements for the Degree
Master of Arts
in
Mathematics

by
Eui Won James Byun
June 2000

AFFINE VARIETIES, GROEBNER BASIS, AND APPLICATIONS

A Project

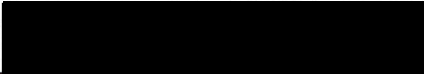
Presented to the
Faculty of
California State University,
San Bernardino

by


Eui Won James Byun

June 2000

Approved by:



Dr. Jim Okon, Chair, Mathematics

6/16/00
Date


Dr. Zahid Hasan,


Dr. John Sarli,


Dr. Terry Hallett, Graduate Coordinator


Dr. Peter Williams, Department Chair

ABSTRACT

In order to understand Groebner basis and its applications, we need to study the commutative ring $k[x_1, \dots, x_n]$ where k is field. We prove the Hilbert Basis Theorem which states that polynomials in several variables have finite spanning sets. We develop a division algorithm in $k[x_1, \dots, x_n]$, so we are able to divide polynomials in several variables by finite sets of divisors. Next we define a Groebner basis and show that it produces a unique remainder in the division algorithm. We apply Groebner basis to the problem of determining ideal membership and the problem of solving a system of polynomial equations in several variables.

ACKNOWLEDGMENTS

First, I want to thank God for giving me this chance to complete my thesis. With His wisdom and courage, I am able to complete my paper. I want to thank Dr. Jim Okon for his great knowledge and caring. He put 100% effort and more to teach me. He was very patient when I was frustrated with the topic, and he encouraged me to overcome the obstacles and triumph in this matter. I want to thank my wife who was there for me. She is my inspiration and my forever friend. Lastly, I want to thank both my committee members, Dr. Zahid Hasan and Dr. John Sarli, for their support. Thank You.

TABLE OF CONTENTS

ABSTRACT	iii
ACKNOWLEDGMENTS	iv
LIST OF GRAPHS	vi
INTRODUCTION	1
GROEBNER BASIS	4
CONCLUSION	31
REFERENCES	32

LIST OF GRAPHS

Graph 1	30
---------	-------	----

Introduction

We are studying geometry and commutative algebra. The part of geometry that we are interested in is affine varieties, which are the curves and surfaces of higher dimensions defined by polynomials. We can visualize in one dimension, two dimensions, and three dimensions, but what about n dimensions where n is greater than 4? It is hard to visualize the n -dimension space and we do not know much about this space.

In order to understand this space, we need to study ideals in the polynomial ring, $k[x_1, \dots, x_n]$ where k is a field. That is $k[x_1, \dots, x_n]$ is a ring and $fg = gf$ for all $f, g \in k[x_1, \dots, x_n]$. Further the constant polynomial $f=1$ is the identity with respect to multiplication. Thus $k[x_1, \dots, x_n]$ is a commutative ring with identity.

Now, let's look at a single variable polynomial, say $f(x) = x^8 + 2x^7 - 5x^5 + 3x^4 - x^2 + 2x$, and an ideal, $\langle x^2 \rangle$. Is this polynomial $f(x)$ in the ideal $\langle x^2 \rangle$? No, it is not because the ideal $I = \langle x^2 \rangle$ will not generate x . In the single variable case, we have a criterion for ideal membership; a polynomial $f \in I$ if and only if $x^2 | f$. On the other hand, if we have an ideal generated by x , then polynomial $f(x)$ will

be in the ideal $\langle x \rangle$ since $f(x) = (x^7 + 2x^6 - 5x^4 + 3x^3 - x + 2) \cdot x$. In a polynomial ring in one variable, we show every ideal can be generated by a single polynomial. Our main focus will be on generating sets for ideals in a polynomial ring in several variables. We will use generating sets to find an algorithm to determine whether or not a polynomial belongs to an ideal.

We will show that ideals are generated by a finite number of elements in $k[x_1, \dots, x_n]$. We begin with Dickson's Lemma, which states monomial ideals in $k[x_1, \dots, x_n]$ have a finite basis. Then we will prove the Hilbert Basis Theorem, which states that all ideals in $k[x_1, \dots, x_n]$ have a finite generating set.

Let's say we have a polynomial $f \in k[x_1, \dots, x_n]$ and an ideal $I = \langle f_1, \dots, f_s \rangle$. How can we determine if the polynomial $f \in I$? We will develop a division algorithm in $k[x_1, \dots, x_n]$ as a tool to divide polynomials in n variables by a finite basis. We will give an example to show that even though a polynomial $f \in I$, we might get a non-zero remainder when this polynomial f is divided by finite basis. To correct this problem, we will introduce the idea of a Groebner basis. We will show that when a polynomial is divided by a Groebner basis, the remainder is unique. Therefore, by applying the

division algorithm to a polynomial $f \in k[x_1, \dots, x_n]$ we can tell whether or not a polynomial belongs to an ideal generated by a Groebner basis. We will also develop an algorithm to transform an arbitrary basis into a Groebner basis. We will conclude by applying a Groebner basis to the problem of solving a system of polynomial equations in several variables. Since $V(\{f_1, \dots, f_s\}) = V(\langle f_1, \dots, f_s \rangle)$, we may replace $\{f_1, \dots, f_s\}$ with a Groebner basis and still get the same solution set. However, as we will show, if $I \cap k[x_n] \neq 0$ then the last polynomial in a Groebner basis has only one variable.

Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here. Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.

Groebner Basis

In order to understand Groebner basis, we need to introduce some terminology. Affine varieties are curves, surfaces, and higher dimensional objects defined by polynomial equations.

Definition 1. Let k be a field, and let f_1, \dots, f_s be polynomials in $k[x_1, \dots, x_n]$. Then we set

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

We call $V(f_1, \dots, f_s)$ the **affine variety** defined by f_1, \dots, f_s .

Other terminology that we need to define is an ideal in the polynomial ring $k[x_1, \dots, x_n]$.

Definition 2. A subset $I \subset k[x_1, \dots, x_n]$ 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 $h \in k[x_1, \dots, x_n]$, then $hf \in I$.

We now define an ideal generated by a finite number of polynomials.

Definition 3. Let f_1, \dots, f_s be polynomials in $k[x_1, \dots, x_n]$.

Then we set $\langle f_1, \dots, f_s \rangle = \left\{ \sum_{i=1}^s h_i f_i : h_1, \dots, h_s \in k[x_1, \dots, x_n] \right\}$. Note that this is an ideal.

We have seen polynomials with single variable before. For example, $x^5 + 7x^4 - 3x^3 + 12x^2 - 10x + 5$ is a polynomial in a single variable. Let's look how this polynomial is arranged. The polynomial is written with the highest exponent at the left and the lowest at the right. We can see this pattern because this is a single variable, and the exponents have a natural order. What if we have several variables? How are we going to arrange polynomials with several variables? We need some more definitions to describe ordering on monomials in polynomials with several variables. A total ordering is one which has the reflexive, transitive, and antisymmetric properties.

Definition 4. A **monomial ordering** on $k[x_1, \dots, x_n]$ is any relation $>$ on $Z_{\geq 0}^n$, or equivalently, any relation on the set of monomials x^α , $\alpha \in Z_{\geq 0}^n$, satisfying:

- (i) $>$ is a total (or linear) ordering on $Z_{\geq 0}^n$.
- (ii) If $\alpha > \beta$ and $\gamma \in Z_{\geq 0}^n$, then $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ is a well-ordering on $Z_{\geq 0}^n$. This means that every nonempty subset of $Z_{\geq 0}^n$ has a smallest element under $>$.

Now, we prove some lemmas that relate to monomial ordering and a well-ordering.

Lemma 1. An order relation $>$ on $Z_{\geq 0}^n$ is a well-ordering if and only if every strictly decreasing sequence in $Z_{\geq 0}^n$, $\alpha(1) > \alpha(2) > \alpha(3) > \dots$ eventually terminates.

Proof. We prove this lemma in it's contrapositive form: $>$ is not a well-ordering if and only if there is an infinite strictly decreasing sequence in $Z_{\geq 0}^n$. If $>$ is not a well-ordering, then we have some subset $T \subset Z_{\geq 0}^n$ that has no least element. Then we can choose $\alpha(1) \in T$. Since $\alpha(1)$ is not the least element in T , we have $\alpha(2)$ in T such that $\alpha(2) < \alpha(1)$. Again, $\alpha(2)$ is not the least element in T , thus we have $\alpha(3)$ in T such that $\alpha(3) < \alpha(2)$ and so on. This will give us an infinite strictly decreasing sequence of elements in T .

Conversely, with any infinite strictly decreasing sequence $\alpha(1), \alpha(2), \alpha(3), \dots$, then we have a nonempty subset $T = \{\alpha(1), \alpha(2), \alpha(3), \dots\}$ in $Z_{\geq 0}^n$ with no least element. Thus $>$ is not a well-ordering. \square

Now we will introduce more definitions needed to describe the ordering of monomials.

Definition 5. Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. We say α is greater than β in **lexicographic order** if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive. We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Example 1:

$$1) \quad (2, 3, 1) >_{lex} (1, 5, 3) \text{ since } \alpha - \beta = (1, -2, -2),$$

$$\text{therefore } x^2 y^3 z >_{lex} x y^5 z^3.$$

$$2) \quad (3, 1, 2) >_{lex} (3, 1, 1) \text{ since } \alpha - \beta = (0, 0, 1),$$

$$\text{therefore } x^3 y z^2 >_{lex} x^3 y z.$$

There are other ways to define monomial ordering.

Definition 6. Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say α is greater than β in **graded lex order**, $\alpha >_{grlex} \beta$, if $|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$ and $\alpha >_{lex} \beta$.

Notice that graded lex order starts with total degrees first, then if there is a tie then lex order applies.

Example 2:

$$1) \quad (2, 1, 4) >_{grlex} (3, 1, 1) \text{ since } |(2,1,4)| = 7 > |(3,1,1)| = 5.$$

$$2) \quad (3, 2, 2) >_{grlex} (3, 1, 3) \text{ since } |(3,2,2)| = |(3,1,3)| = 7 \text{ and}$$

$$(3,2,2) >_{lex} (3,1,3).$$

Definition 7. Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. We say α is greater than β in **graded reverse lex order**, $\alpha >_{\text{grevlex}} \beta$, if

$|\alpha| = \sum_{i=1}^n \alpha_i > |\beta| = \sum_{i=1}^n \beta_i$, or $|\alpha| = |\beta|$ and, in $\alpha - \beta \in \mathbb{Z}^n$, the right-most nonzero entry is negative.

The difference between graded lex order and graded reverse lex order is that in graded lex order the left-most nonzero coordinate of $\alpha - \beta$ is positive while in graded reverse lex order the right-most nonzero coordinate of $\alpha - \beta$ is negative.

Example 3:

- 1) $(4, 3, 2) >_{\text{grevlex}} (4, 1, 1)$ since $|(4, 3, 2)| = 9 > |(4, 1, 1)| = 6$.
- 2) $(2, 3, 4) >_{\text{grevlex}} (3, 0, 6)$ since $|(2, 3, 4)| = |(3, 0, 6)| = 9$ and $\alpha - \beta = (-1, 3, -2)$.

We now extend some definitions for polynomials in one variable to polynomials in several variables.

Definition 8. Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a nonzero polynomial in $k[x_1, \dots, x_n]$ and let $>$ be a monomial order.

- (i) the **multidegree** of f is $\text{multi deg}(f) = \max(\alpha \in \mathbb{Z}_{\geq 0}^n : a_{\alpha} \neq 0)$
(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 $LM(f) = x^{\text{multi deg}(f)}$.

(iv) The **leading term** of f is $LT(f) = LC(f) \cdot LM(f)$.

We give an example of this in three variables. Let $f(x, y, z) = 12x^5yz^2 + 4z^4 - 7x^7 + 3y^4z^3$. Using lex order, $\text{multi deg}(f) = (7, 0, 0)$, $LC(f) = -7$, $LM(f) = x^7$, and lastly $LT(f) = -7x^7$. Also, note that we have

$$\text{multi deg}(fg) = \text{multi deg}(f) + \text{multi deg}(g)$$

We define monomial ideals in $k[x_1, \dots, x_n]$.

Definition 9. An ideal $I \subset k[x_1, \dots, x_n]$ is a **monomial ideal** if there is a subset $A \subset \mathbb{Z}_{\geq 0}^n$ (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 $h_{\alpha} \in k[x_1, \dots, x_n]$ and $x^{\alpha} = x_1^{\alpha(1)} \cdot x_2^{\alpha(2)} \cdot \dots \cdot x_n^{\alpha(n)}$. In this case, we write $I = \langle x^{\alpha} : \alpha \in A \rangle$.

Lemma 2. 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 divisible by x^{α} for some $\alpha \in A$, then $x^{\beta} = cx^{\alpha}$ where $c \in k[x_1, \dots, x_n]$. Thus $x^{\beta} \in I$ by definition of ideal.

Conversely, if $x^{\beta} \in I$, then $x^{\beta} = \sum_{i=1}^r c_i x^{\alpha(i)}$ where $c_i \in k[x_1, \dots, x_n]$ and

$\alpha(i) \in A$. Let $\alpha(i_0) = \min\{\alpha(1), \dots, \alpha(r)\}$. Then we can factor $\alpha(i_0)$

from the right side of the equation,

$$\sum_{i=1}^r c_i x^{\alpha(i)} = \sum_{i=1}^r (c_i x^{\alpha(i)-\alpha(i_0)}) \cdot x^{\alpha(i_0)} . \quad \text{Therefore, we can write the}$$

equation as $x^\beta = \sum_{i=1}^r c_i (x^{\alpha(i)-\alpha(i_0)}) \cdot x^{\alpha(i_0)}$. Thus $x^{\alpha(i_0)}$ divides x^β . \square

For the case of a single variable polynomials, we know that ideals in $k[x]$ are principal. Is this true if we go on to several variables? Let's look at the polynomial ring, $k[x,y]$ in two variables.

Example 4: If k is a field, then $\langle x,y \rangle$ is not principal in $k[x,y]$.

Proof: Assume to the contrary that $\langle x,y \rangle = \langle f(x,y) \rangle$ for some $f \in k[x,y]$. This means $x \in \langle f(x,y) \rangle$ and $y \in \langle f(x,y) \rangle$. Let's look when $x \in \langle f(x,y) \rangle$. This implies that $\text{multi deg}(f(x,y))$ is either $(0,0)$ or $(1,0)$. For $y \in \langle f(x,y) \rangle$, this implies that $\text{multi deg}(f(x,y))$ has either $(0,0)$ or $(0,1)$. Thus, $\text{multi deg}(f(x,y)) = (0,0)$. This is a contradiction since $1 \notin \langle x,y \rangle$. \square

The above example shows that ideals in $k[x_1, \dots, x_n]$ need not be a principal. Next, we need to find out if these polynomials are generated by finite basis or infinite basis. Our next result, Dickson's Lemma, shows that monomial ideals are finitely generated.

Lemma 3 (Dickson's Lemma). Let $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \dots, x_n]$ be a monomial ideal. Then there exists $\alpha(1), \dots, \alpha(s) \in A$ such that it can be written in the form $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. In particular, I has a finite basis.

Proof. We will prove Dickson's Lemma by induction on the number of variables n .

Let $n=1$. In this case, I is generated by monomials x^α , where $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Let β be the smallest element of A . Because $\beta \leq \alpha$ for all $\alpha \in A$, x^β divides x^α for all α . Therefore, $I = \langle x^\beta \rangle$. Now assume monomial ideals in $n-1$ variables are finitely generated. We will write monomials in $k[x_1, \dots, x_n]$ as $x^\alpha w^\beta$ in $k[x_1, \dots, x_{n-1}, w]$ where $\alpha = (\alpha_1, \dots, \alpha_{n-1}) \in \mathbb{Z}_{\geq 0}^{n-1}$ and $\beta \in \mathbb{Z}_{\geq 0}$. Suppose $I \subset k[x_1, \dots, x_{n-1}, w]$ is a monomial ideal. Let $J = \{x^\alpha : x^\alpha w^\beta \in I \text{ for some } \beta\}$, a monomial ideal in $k[x_1, \dots, x_{n-1}]$. From our inductive hypothesis, there are finitely many generators, x^α such that $J = \langle x^{\alpha(1)}, \dots, x^{\alpha(r)} \rangle$. Let $\beta(i)$ be such that $x^{\alpha(i)} w^{\beta(i)} \in I$ and let $\beta = \max\{\beta(i)\}$. For $0 \leq k < \beta$, let $J_k = \langle x^{\alpha_k} : x^{\alpha_k} w^k \in I \rangle$, a monomial ideal in $k[x_1, \dots, x_{n-1}]$. Then by our inductive hypothesis, each J_k has a finite generating set

of monomials $B_k = \{x^{\alpha_k(1)}, \dots, x^{\alpha_k(r)}\}$. Let $B = \{x^{\alpha(1)}, \dots, x^{\alpha(r)}\} \cup \bigcup_{k=1}^{r-1} B_k$. We

claim B generates I . Let $x^a w^b \in I$. We have two cases.

Case1: If $b \geq \beta$, we have $x^a = \sum_{i=1}^n c_i x^{a-\alpha(i)} x^{\alpha(i)}$ and

$w^b = c_i w^{b-\beta(i)} w^{\beta(i)}$. Then $x^a w^b = \sum_{i=1}^n c_i x^{a-\alpha(i)} w^{b-\beta(i)} x^{\alpha(i)} w^{\beta(i)}$. Thus

$x^a w^b \in \langle B \rangle$.

Case2: If $b < \beta$, we have $x^a \in J_b$ so $x^a = \sum c_i x^{a-\alpha_b(i)} x^{\alpha_b(i)}$.

Then $x^a w^b = \sum_{i=1}^n c_i x^{a-\alpha_b(i)} x^{\alpha_b(i)} w^b$. Thus $x^a w^b \in \langle B \rangle$.

To finish the proof, we need to show that I is generated by

finitely many of the x^α 's such that $\alpha \in A$. We have shown

that $I = \langle x^{\beta(1)}, \dots, x^{\beta(s)} \rangle$ for some $x^{\beta(i)} \in I$. Using Lemma 2, for each

i , $x^{\beta(i)}$ is divisible by $x^{\alpha(i)}$ for some $\alpha(i) \in A$. Therefore,

$I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. \square

If $I = \langle f \rangle$ is an ideal in a polynomial ring $k[x]$ in one

variable, then another polynomial in one variable $g \in I$ if

and only if $f|g$. Does a similar result hold for

polynomials in several variables? We first need a division

algorithm for $k[x_1, \dots, x_n]$. Since ideals are not necessarily

principal, we must be able to "divide" a polynomial by a

finite number of polynomials. The next theorem shows that this can be done. However, the quotient and remainder are not unique.

Theorem 1 (Division Algorithm). Fix a monomial order $>$ on $Z_{\geq 0}^n$, and let $F = (f_1, \dots, f_s)$ be an ordered s -tuple of polynomials in $k[x_1, \dots, x_n]$. Then every $f \in k[x_1, \dots, x_n]$ can be written as $f = a_1 f_1 + \dots + a_s f_s + r$, where $a_i, r \in k[x_1, \dots, x_n]$, and either $r = 0$ or r is a linear combination, with coefficients in k , of monomials, none of which is divisible by any of $LT(f_1), \dots, LT(f_s)$. We will call r a remainder of f on division by F . Furthermore, if $a_i f_i \neq 0$, then we have $\text{multi deg}(f) \geq \text{multi deg}(a_i f_i)$.

Proof. Let P be a polynomial in $k[x_1, \dots, x_n]$. Fix a monomial order $>$ on $Z_{\geq 0}^n$. Let $F = (f_1, \dots, f_s)$, $f_i \in k[x_1, \dots, x_n]$. If $LT(f_i)$ does not divide $LT(P)$ for all i , then let $r_1 = LT(P)$ and $P_1 = P - r_1$. If $LT(f_i)$ divides $LT(P)$ for some i , then we let $r_1 = 0$ and $P_1 = P - a_1 \cdot f_i - r_1$ where $a_1 = \frac{LT(P)}{LT(f_i)}$. Thus we have a new polynomial P_1 . To see $\text{multi deg}(P_1) < \text{multi deg}(P)$, we look at

$\frac{LT(P)}{LT(f_i)} \cdot f_i$. The leading term of this polynomial is

$LT\left(\frac{LT(P)}{LT(f_i)} \cdot f_i\right) = \frac{LT(P)}{LT(f_i)} \cdot LT(f_i) = LT(P)$. Thus we are subtracting

$LT(P)$ from polynomial P so $\text{multideg}(P_1) < \text{multideg}(P)$. So, if we continue this process, we get $P > P_1 > P_2 > \dots > P_k$ where k is an integer with $P_k = P - \sum a_i f_i - r_k$, $r_k = 0$ or $r_k = \sum c_k$ where $c_k \in k[x_1, \dots, x_n]$ is not divisible by $LT(f_i)$ for any i . If $P_k = 0$ for some $k \in \mathbb{Z}_{\geq 0}$, then we are done because we can solve for P to get $P = \sum a_i f_i + r_k$. If $P_k \neq 0$, then there exists P_{k+1} of the form $P_{k+1} = P_k - \frac{LT(P_k)}{LT(f_i)} \cdot LT(f_i)$, or $P_{k+1} = P - \sum a_i f_i - r_{k+1}$, where $r_{k+1} = r_k + LT(P_k)$. Thus this process will eventually terminate by definition of a well-ordering. \square

Example 5: Let us divide $f = x^2y + xy^2 + y^2$ by divisors $f_1 = xy - 1$ and $f_2 = y^2 - 1$ using lex order with $x > y$. The division algorithm gives us $x^2y + xy^2 + y^2 = (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1$ with remainder $r = x + y + 1$. Now, apply the division algorithm except we switch the divisors $f_1 = y^2 - 1$ and $f_2 = xy - 1$. The result is $x^2y + xy^2 + y^2 = (x + 1) \cdot (y^2 - 1) + x \cdot (xy - 1) + 2x + 1$ with remainder $r = 2x + 1$. By just changing the order of divisors, we get different quotients and remainders. Later on, using Groebner basis, we will get a unique remainder.

The Hilbert Basis Theorem states that every ideal in $k[x_1, \dots, x_n]$ has a finite generating set.

Theorem 2 (Hilbert Basis Theorem). Every ideal $I \subset k[x_1, \dots, x_n]$ has a finite generating set. That is,

$$I = \langle g_1, \dots, g_s \rangle \text{ for some } g_1, \dots, g_s \in I.$$

Proof. First, if $I = \{0\}$ then it is certainly finitely generated. Thus the theorem is true in this case. Now assume I contains a nonzero polynomial. We will show $I = \langle g_1, \dots, g_s \rangle$ where $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$. We first prove $I \supset \langle g_1, \dots, g_s \rangle$. This is easy to show because each $g_i \in I$. Thus $\langle g_1, \dots, g_s \rangle \subset I$. Now we show $I \subset \langle g_1, \dots, g_s \rangle$. Let $P \in I$ be any polynomial in $k[x_1, \dots, x_n]$. Then divide P by $\langle g_1, \dots, g_s \rangle$ using division algorithm. Then we can write polynomial P in this way: $P = a_1 g_1 + \dots + a_t g_t + r$ where $a_i, r \in k[x_1, \dots, x_n]$ and none of $(LT(g_1), \dots, LT(g_t))$ divide r . We claim that $r = 0$. If $r \neq 0$, then $LT(r) \in \langle LT(I) \rangle$. By Lemma 2, $LT(r)$ must be divisible by some $LT(g_i)$. This contradicts the choice of r (no $LT(g_i)$ can divide $LT(r)$). Therefore $r = 0$ and $P = a_1 g_1 + \dots + a_t g_t + 0$. Thus $P \in \langle g_1, \dots, g_s \rangle$ which shows $I \subset \langle g_1, \dots, g_s \rangle$. \square

The Hilbert Basis Theorem shows that if $I \subset k[x_1, \dots, x_n]$ then $I = \langle f_1, \dots, f_s \rangle$. So, $f \in I$ if and only if $f = \sum a_i f_i$ where $a_i \in k[x_1, \dots, x_n]$. It is natural to expect that $f \in I$ if and only

if when f is divided by (f_1, \dots, f_s) . The remainder is zero.

However, this need not be the case for an arbitrary basis.

Example 6: Let's divide a polynomial, $p = xy^2 - x$, by divisors, $f_1 = xy + 1$, and $f_2 = y^2 - 1$. Let $F = (f_1, f_2)$. The result is $xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y)$, where $-x - y$ is the remainder. Now, let's switch divisors with f_2 as a first divisor. Thus, $F = (f_2, f_1)$. The result is $xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0$, where 0 is the remainder. This shows that even when $f \in \langle f_1, f_2 \rangle$, the remainder depends on the order of the divisors. The remainder may be either zero or non-zero. In order to correct this problem, we introduce the ideal of a Groebner basis.

Definition 10. Fix a monomial order. A finite subset $G = \{g_1, \dots, g_s\}$ of an ideal I is said to be a **Groebner basis** (or standard basis) if $\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle$.

The main problem in determining ideal membership is that with an arbitrary basis, the remainders in division algorithm need not be unique. The Groebner basis corrects this flaw.

Proposition 1. Let $G = (g_1, \dots, g_r)$ be a Groebner basis for an ideal $I \subset k[x_1, \dots, x_n]$ and let $f \in k[x_1, \dots, x_n]$. Then there is a unique $r \in k[x_1, \dots, x_n]$ with the following two properties:

- (i) No term of r is divisible by any of $LT(g_1), \dots, LT(g_t)$.
- (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. By the division algorithm $f = g + r$, where no term of the remainder r is divisible by $LT(g_i)$ for any i and $g = a_1 g_1 + \dots + a_t g_t \in I$. Thus $f = g + r$ satisfies the existence of g and r .

To prove the uniqueness, suppose $f = g + r = h + s$ where $g, h \in I$. Then $r - s = h - g \in I$. If $r - s \neq 0$, then $LT(r - s) \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$. By Lemma 2, $LT(r - s)$ is divisible by some $LT(g_i)$. This is not true since every term of $LT(r)$ or $LT(s)$, by definition of remainder, is not divisible by any of $LT(g_1), \dots, LT(g_t)$. Thus $r - s = 0$. \square

Corollary 1. Let $G = \{g_1, \dots, g_t\}$ be a Groebner basis for an ideal $I \subset k[x_1, \dots, x_n]$ and let $f \in k[x_1, \dots, x_n]$. Then $f \in I$ if and only if the remainder on division of f by G is zero.

Proof. If we have a remainder zero, then $f \in I$ since f can be written in as $f = a_1 g_1 + \dots + a_t g_t \in I$ by the division algorithm. Conversely, suppose $f \in I$. Then we can write f

as $f = f + 0$, which satisfies the two properties in Proposition 1. Thus 0 is the remainder of f on division by G . \square

Definition 11. We will write \bar{f}^F for the remainder on division of f by the ordered s -tuple $F = (f_1, \dots, f_s)$. If F is a Groebner basis for $\langle f_1, \dots, f_s \rangle$, then we can regard F as a set (without any particular order) by Proposition 1.

Definition 12. Let $f, g \in k[x_1, \dots, x_n]$ be nonzero polynomials.

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

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

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g. \quad (\text{Note that we are inverting the leading coefficients here as well.})$$

Lemma 4. Suppose we have a sum $\sum_{i=1}^s c_i f_i$, where $c_i \in k$ and

$\text{multi deg}(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$ for all i . If $\text{multi deg}\left(\sum_{i=1}^s c_i f_i\right) < \delta$, then $\sum_{i=1}^s c_i f_i$

is a linear combination, with coefficients in k , of the S -

polynomials $S(f_j, f_k)$ for $1 \leq j, k \leq s$. Furthermore, each $S(f_j, f_k)$ has multidegree $< \delta$.

Proof. Let $d_i = LC(f_i)$ so that $c_i d_i$ is the leading coefficient of $c_i f_i$. From the hypothesis, $\sum_{i=1}^s c_i d_i = 0$. Let $p_i = f_i / d_i$ with leading coefficient 1. Let's look at the sum

$$\sum_{i=1}^s c_i f_i = \sum_{i=1}^s c_i d_i p_i = c_1 d_1 p_1 + c_2 d_2 p_2 + \cdots + c_s d_s p_s.$$

Now consider the telescoping sum:

$$\begin{aligned} \sum_{i=1}^s c_i d_i p_i &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2) (p_2 - p_3) + (c_1 d_1 + c_2 d_2 + c_3 d_3) (p_3 - p_4) + \cdots + \\ &\quad (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) (p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s \end{aligned}$$

By assumption, $LT(f_i) = d_i x^\delta$, which implies that least common multiple of $LM(f_j)$ and $LM(f_k)$ is x^δ . So we can write S-polynomial in this way:

$$S(f_j, f_k) = \frac{x^\delta}{LT(f_j)} \cdot f_j - \frac{x^\delta}{LT(f_k)} \cdot f_k = \frac{x^\delta}{d_j x^\delta} \cdot f_j - \frac{x^\delta}{d_k x^\delta} \cdot f_k = \frac{f_j}{d_j} - \frac{f_k}{d_k} = p_j - p_k.$$

Using $S(f_j, f_k)$ and $\sum_{i=1}^s c_i d_i = 0$, we can rewrite $\sum c_i f_i$ as

$$\sum_{i=1}^s c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s).$$

We also know that p_j and p_k have multidegree δ and leading

coefficient 1, thus the difference $p_j - p_k$ has multidegree $< \delta$. Thus $S(f_j, f_k)$ has multidegree $< \delta$. \square

To see if a polynomial belongs to an ideal I in $k[x_1, \dots, x_n]$, we divide a polynomial by a Groebner basis and see if the remainder comes out to be zero or not.

Theorem 3. Let I be a polynomial ideal. Then a basis $G = \{g_1, \dots, g_t\}$ 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 $S(g_j, g_k) \in I$ for all j, k . Then the remainder when $S(g_j, g_k)$ is divided by G is zero by Corollary 1.

\Leftarrow : Let $p \in I = \langle g_1, \dots, g_t \rangle$ be a nonzero polynomial. Then we can write the polynomial p as $p = \sum_{i=1}^t h_i g_i$ where $g_i \in G$ and $h_i \in k[x_1, \dots, x_n]$. Then it follows that $\text{multideg}(p) \leq \max(\text{multideg}(h_i g_i))$.

Now, we need to show that if $\text{multideg}(p) = \text{multideg}(h_i g_i)$ for some i , then we can say $LT(p)$ is divisible by $LT(g_i)$ thus

$LT(p) \in \langle LT(g_1), \dots, LT(g_t) \rangle$. Let $m(i) = \text{multideg}(h_i g_i)$ and let

$\varepsilon = \max(m(1), \dots, m(t))$. Then we have $\text{multideg}(p) \leq \varepsilon$. Each expression

of the form $p = \sum_{i=1}^t h_i g_i$ can possibly have a different ε

depending on the choice of (h_1, \dots, h_r) . Since monomial order is

a well-ordering, we can choose an expression, $p = \sum_{i=1}^r h_i g_i$, of

the polynomial p to have ε as minimal. We will prove

$\text{multi deg}(p) = \varepsilon$ by contradiction. We write $p = \sum_{m(i)=\varepsilon} h_i g_i + \sum_{m(i)<\varepsilon} h_i g_i$

and assume $\text{multi deg}(p) < \varepsilon$. We can rewrite the polynomial p

as $p = \sum_{m(i)=\varepsilon} LT(h_i) g_i + \sum_{m(i)=\varepsilon} (h_i - LT(h_i)) g_i + \sum_{m(i)<\varepsilon} h_i g_i$. The second sum

$\sum_{m(i)=\varepsilon} (h_i - LT(h_i)) g_i$, has multidegree $< \varepsilon$ since for all i $LT(h_i)$

has been eliminated, thus both $\sum_{m(i)=\varepsilon} (h_i - LT(h_i)) g_i$ and $\sum_{m(i)<\varepsilon} h_i g_i$

have multidegree $< \varepsilon$. Let $LT(h_i) = c_i x^{\alpha(i)}$ where $c_i \in k$. Then it

follows that $\sum_{m(i)=\varepsilon} LT(h_i) g_i = \sum_{m(i)=\varepsilon} c_i x^{\alpha(i)} g_i$. Now, by using Lemma 3,

we can write $\sum_{m(i)=\varepsilon} c_i x^{\alpha(i)} g_i$ as a linear combination of S-

polynomials $S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k)$. We have

$$\begin{aligned} S(x^{\alpha(j)} g_j, x^{\alpha(k)} g_k) &= \frac{x^\varepsilon}{x^{\alpha(j)} LT(g_j)} \cdot x^{\alpha(j)} g_j - \frac{x^\varepsilon}{x^{\alpha(k)} LT(g_k)} \cdot x^{\alpha(k)} g_k = \\ x^{\varepsilon - \gamma_{jk}} \left(\frac{x^{\gamma_{jk}}}{LT(g_j)} \cdot g_j - \frac{x^{\gamma_{jk}}}{LT(g_k)} \cdot g_k \right) &= \\ x^{\varepsilon - \gamma_{jk}} \cdot \left(\frac{x^{\gamma_{jk}}}{LT(g_j)} g_j - \frac{x^{\gamma_{jk}}}{LT(g_k)} g_k \right) &= x^{\varepsilon - \gamma_{jk}} S(g_j, g_k) \end{aligned}$$

where $x^{\gamma_{jk}} = LCM(LM(g_j), LM(g_k))$. Now we can write

$$\sum_{m(i)=\varepsilon} LT(h_i)g_i = \sum_{j,k=1}^t c_{jk} x^{\varepsilon-\gamma_{jk}} S(g_j, g_k) \text{ where constant } c_{jk} \in k. \text{ Now we}$$

know that remainder of $S(g_j, g_k)$ on division by g_1, \dots, g_t is zero by the hypothesis of the theorem. By using division

algorithm, we can write $S(g_j, g_k) = \sum_{i=1}^t a_{ijk} g_i$, where $a_{ijk} \in k[x_1, \dots, x_n]$.

We can also find from the division algorithm that

$\text{multi deg}(a_{ijk} g_i) \leq \text{multi deg}(S(g_j, g_k))$ for all i, j, k . Now, multiply

$S(g_j, g_k)$ by $x^{\varepsilon-\gamma_{jk}}$ so that $x^{\varepsilon-\gamma_{jk}} \cdot S(g_j, g_k) = \sum_{i=1}^t b_{ijk} g_i$ where

$b_{ijk} = x^{\varepsilon-\gamma_{jk}} \cdot a_{ijk}$. From Lemma 3 and

$\text{multi deg}(a_{ijk} g_i) \leq \text{multi deg}(S(g_j, g_k)) < \gamma_{jk}$, we get $\text{multi deg}(b_{ijk} g_i) < \varepsilon$. By

substituting our results into the expression, $\sum_{m(i)=\varepsilon} LT(h_i)g_i$, we

get $\sum_{m(i)=\varepsilon} LT(h_i)g_i = \sum_{j,k=1}^t c_{jk} x^{\varepsilon-\gamma_{jk}} S(g_j, g_k) = \sum_{j,k=1}^t c_{jk} \left(\sum_{i=1}^t b_{ijk} g_i \right) = \sum_{i=1}^t h'_i g_i$ where

$\text{multi deg}(h'_i g_i) < \varepsilon$. Thus, if we substitute $\sum_{m(i)=\varepsilon} LT(h_i)g_i = \sum_{i=1}^t h'_i g_i$

into the expression for the polynomial p , then we get

$p = \sum_{i=1}^t h'_i g_i + \sum_{m(i)=\varepsilon} (h_i - LT(h_i)g_i) + \sum_{m(i)<\varepsilon} h_i g_i$ which implies that

$\text{multi deg}(p) < \varepsilon$. This is a contradiction to the minimality of

ε . Therefore, $\text{multideg}(p) = \varepsilon$. Thus, $LT(p)$ is divisible by $LT(g_i)$ and $LT(p) \in \langle LT(g_1), \dots, LT(g_s) \rangle$. \square

Definition 13. Given $I = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$, the l th elimination ideal I_l is the ideal of $k[x_1, \dots, x_{n-l}]$ defined by $I_l = I \cap k[x_1, \dots, x_{n-l}]$.

Theorem 4 (The Elimination Theorem). Let $I \subset k[x_1, \dots, x_n]$ be an ideal and let G be a Groebner basis of I with respect to lex order where $x_1 > x_2 > \dots > x_n$. Then, for every $0 \leq l \leq n$, the set $G_l = G \cap k[x_{l+1}, \dots, x_n]$ is a Groebner basis of the l th elimination ideal I_l .

Proof. Fix l between 0 and n . Then $G_l \subset I_l$ and we need to show $\langle LT(I_l) \rangle = \langle LT(G_l) \rangle$. Proving $\langle LT(I_l) \rangle \supset \langle LT(G_l) \rangle$ is obvious because of the construction of $G_l \subset I_l$. To prove $\langle LT(I_l) \rangle \subset \langle LT(G_l) \rangle$, let $f \in I_l$. This means that $f \in I$ also and $LT(f)$ is divisible by $LT(g)$ for some $g \in G$ since G is a Groebner basis of I . Using lex order, any monomial in $k[x_1, \dots, x_{n-l}]$ is greater than all monomials in $k[x_{l+1}, \dots, x_n]$. So $LT(g) \in k[x_{l+1}, \dots, x_n]$ implies $g \in k[x_{l+1}, \dots, x_n]$. Thus, $g \in G_l$. \square

Let's have an example of the Elimination Theorem.

Example 7: Let $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1 \rangle$. Then a Groebner basis for I with respect to lex order is

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

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

Using the Elimination Theorem, we get $I_1 = I \cap C[y, z] = \langle g_1 \rangle$ and $I_2 = I \cap C[z] = \{0\}$. Somehow, we did not get a single variable element in the Groebner basis.

Theorem 5 (The Extension Theorem): Let $I = \langle f_1, \dots, f_s \rangle \subset C[x_1, \dots, x_n]$ and let I_1 be the first elimination ideal of I . For each $1 \leq i \leq s$, write f_i in the form $f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{terms in which } x_1 \text{ has degree } < N_i$, where $N_i \geq 0$ and $g_i \in C[x_2, \dots, x_n]$ is nonzero. Suppose that we have a partial solution $(a_2, \dots, a_n) \in V(I_1)$. If $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s)$, then there exists $a_1 \in C$ such that $(a_1, a_2, \dots, a_n) \in V(I)$.

Even though we are not going to prove this theorem, we can use this theorem to state polynomials in $k[x_1, \dots, x_n]$ where the Elimination Theorem does not apply to some polynomials in $k[x_1, \dots, x_n]$. Like the example above, we can use the Extension Theorem to see if we can extend partial solutions in $V(I_2)$ to $V(I)$.

In Example 7, we did not get a single variable element in the Groebner basis. Thus we use an arbitrary number, $\chi \in C$, as a partial solution. Does this solution $\chi \in C = V(I_2)$ extend to $V(I)$? First, we substitute χ in the variable z into the

first Groebner base, g_1 , and solve for variable y . Say the solution for variable $y = \beta$. Then we substitute both χ and β into the second Groebner base, g_2 , to solve for variable x . Thus, we are extended to $V(I)$.

We will apply Groebner basis to ideal membership and the problem of solving a system of polynomial equations in several variables. We will also write algorithms for these two problems.

Example 8: First, we will look at the ideal membership. Let $I = \langle f_1, f_2 \rangle = \langle xz - y^2, x^3 - z^2 \rangle \in C[x, y, z]$ and

$F = -4x^2y^2z^2 + y^6 + 3z^5$. We like to know if $F \in I$. So, we need to find the Groebner basis for I . We used Maple 5.1 to find the Groebner basis for I . The Groebner basis for I is $(xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5)$. Using this basis, we can do the division algorithm to determine if $F \in I$. This is the algorithm for ideal membership:

with(Groebner):

```
f[1]:=x*z-y^2:f[2]:=x^3-z^2:f[3]:=x^2*y^2-z^3:f[4]:=x*y^4-
z^4:f[5]:=y^6-z^5:
```

```
P:=-4*x^2*y^2*z^2+y^6+3*z^5:n:=5:
```

```
for i from 1 to n do q[i]:=0 od:
```

```
r:=0:
```

```
while P<>0 do
```

```
LTP:=leadmon(P,plex(x,y,z))[1]*leadmon(P,plex(x,y,z))[2]:
```

```

k:=1:divoccured:=false:
while (k<=n) and (divoccured=false) do
LTfk:=leadmon(f[k],plex(x,y))[1]*leadmon(f[k],plex(x,y))[2]:
    if divide(LTP,LTfk,'d') then
        print(k,d,LTfk):
q[k]:=q[k]+d:P:=expand(P-d*f[k]):divoccured:=true:
        print(k,d,q[k],P):
    else k:=k+1: fi:od:
if divoccured=false then
    r:=r+LTP:P:=expand(P-LTP):
fi:
od:

```

After using this division algorithm, we have

$F = (-4xy^2z - 4y^4) \cdot (f_1) + 0 \cdot (f_2) + 0 \cdot (f_3) + 0 \cdot (f_4) - 3 \cdot (f_5) + 0$. Thus the remainder is 0 and therefore, $F \in I$.

We are applying the Groebner basis for the problem of solving polynomials in several variables.

Example 9: We will use Lagrange Multiplier to show the problem of solving polynomials in several variables. To find the minimum distance $d^2(x,y) = x^2 + (y-1)^2$ between a point on the parabola $y = x^2$ and the point $(0,1)$, we can apply Lagrange multipliers. We will get $2x = 2\lambda x$, $2y - 2 = -\lambda$, $x^2 = y$, thus $\lambda = 1$, $y = \frac{1}{2}$, $x = \pm \sqrt{\frac{1}{2}}$. Therefore, the minimum distance is

$$d^2\left(\pm\sqrt{\frac{1}{2}},\frac{1}{2}\right)=\left(\pm\sqrt{\frac{1}{2}}\right)^2+\left(\frac{1}{2}-1\right)^2=\frac{1}{2}+\frac{1}{4}=\frac{3}{4}.$$

What if we use the same problem except we rotate the

equation using $Ro=\frac{1}{5}\begin{pmatrix} 3 & -4 \\ 4 & 3 \end{pmatrix}$? The point (0,1) becomes

$$\frac{1}{5}\begin{pmatrix} 3 & 4 \\ -4 & 3 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix}=\begin{pmatrix} \frac{4}{5} \\ \frac{3}{5} \end{pmatrix}. \quad \text{Thus, the new point is } \left(\frac{4}{5},\frac{3}{5}\right). \quad \text{This is how}$$

we can get a rotated equation:

$$\begin{aligned} (x',y')Ro^T\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}Ro\begin{pmatrix} x' \\ y' \end{pmatrix}+(0,1)Ro\begin{pmatrix} x' \\ y' \end{pmatrix} &= 0 \\ \frac{1}{25}(x',y')\begin{pmatrix} 9 & -12 \\ -12 & 16 \end{pmatrix}\begin{pmatrix} x' \\ y' \end{pmatrix}+\frac{1}{5}(-4 \ -3)Ro\begin{pmatrix} x' \\ y' \end{pmatrix} &= 0 \end{aligned}$$

After all the calculations, we have new point $\left(\frac{4}{5},\frac{3}{5}\right)$ and the

equation $9x^2-24xy+16y^2-20x-15y=0$. Thus to find the minimum

distance $d^2(x,y)=\left(x-\frac{4}{5}\right)^2+\left(y-\frac{3}{5}\right)^2$ from a point on the parabola

$9x^2-24xy+16y^2-20x-15y=0$ to the point $\left(\frac{4}{5},\frac{3}{5}\right)$, it will be

difficult to do so and we will show why. The Lagrange multipliers for the rotated equation are

$$\begin{aligned}\frac{\partial}{\partial x}d(x,y) &= \lambda \frac{\partial}{\partial x}(9x^2 - 24xy + 16y^2 - 20x - 15y) \\ \frac{\partial}{\partial y}d(x,y) &= \lambda \frac{\partial}{\partial y}(9x^2 - 24xy + 16y^2 - 20x - 15y) \\ 0 &= 9x^2 - 24xy + 16y^2 - 20x - 15y\end{aligned}$$

when we do partial derivatives of the rotated equation, we get

$$\begin{aligned}2\left(x - \frac{4}{5}\right) &= \lambda(18x - 24y - 20) \\ 2\left(y - \frac{3}{5}\right) &= \lambda(32y - 24x - 15) \\ 0 &= 9x^2 - 24xy + 16y^2 - 20x - 15y\end{aligned}$$

That is why we can use the Groebner basis to solve this polynomial. First, we need to find the Groebner basis for this polynomial. The Groebner basis for this polynomial is

$$\begin{aligned}g_1 &= 18\lambda x - 24\lambda y - 20\lambda - 2x + \frac{8}{5} \\ g_2 &= -24\lambda x + 32\lambda y - 15\lambda - 2y + \frac{6}{5} \\ g_3 &= 9x^2 - 24xy + 16y^2 - 20x - 15y \\ g_4 &= 125\lambda + 8x + 6y - 10 \\ g_5 &= -\frac{92}{45}x - 8xy + \frac{2}{15}y - \frac{4}{9}y^2 \\ g_6 &= -\frac{460}{3}x - 365y + \frac{1250}{3}y^2 \\ g_7 &= \frac{46}{45}y + \frac{8}{3}y^2 - \frac{40}{9}y^3\end{aligned}$$

Now we can notice that g_7 has only a single variable polynomial. Thus we can solve for variable y when $g_7 = 0$.

The solution for variable y is $y=0$ or $y=\frac{3}{10}\pm\frac{2}{5}\sqrt{2}$. When

$y=0$, we get $x=0$, when $y=\frac{3}{10}+\frac{2}{5}\sqrt{2}$, we get $x=\frac{2}{5}-\frac{3}{10}\sqrt{2}$, and

when $y=\frac{3}{10}-\frac{2}{5}\sqrt{2}$, we get $x=\frac{2}{5}+\frac{3}{10}\sqrt{2}$. So we have three points

to compute into $d^2(x,y)=\left(x-\frac{4}{5}\right)^2+\left(y-\frac{3}{5}\right)^2$ and see which point

gives the minimum distance. Let $p_1=(0,0)$,

$p_2=\left(\frac{2}{5}-\frac{3}{10}\sqrt{2},\frac{3}{10}+\frac{2}{5}\sqrt{2}\right)$, and $p_3=\left(\frac{2}{5}+\frac{3}{10}\sqrt{2},\frac{3}{10}-\frac{2}{5}\sqrt{2}\right)$. The p_1

gives the distance $d(0,0)=1$, p_2 gives the distance

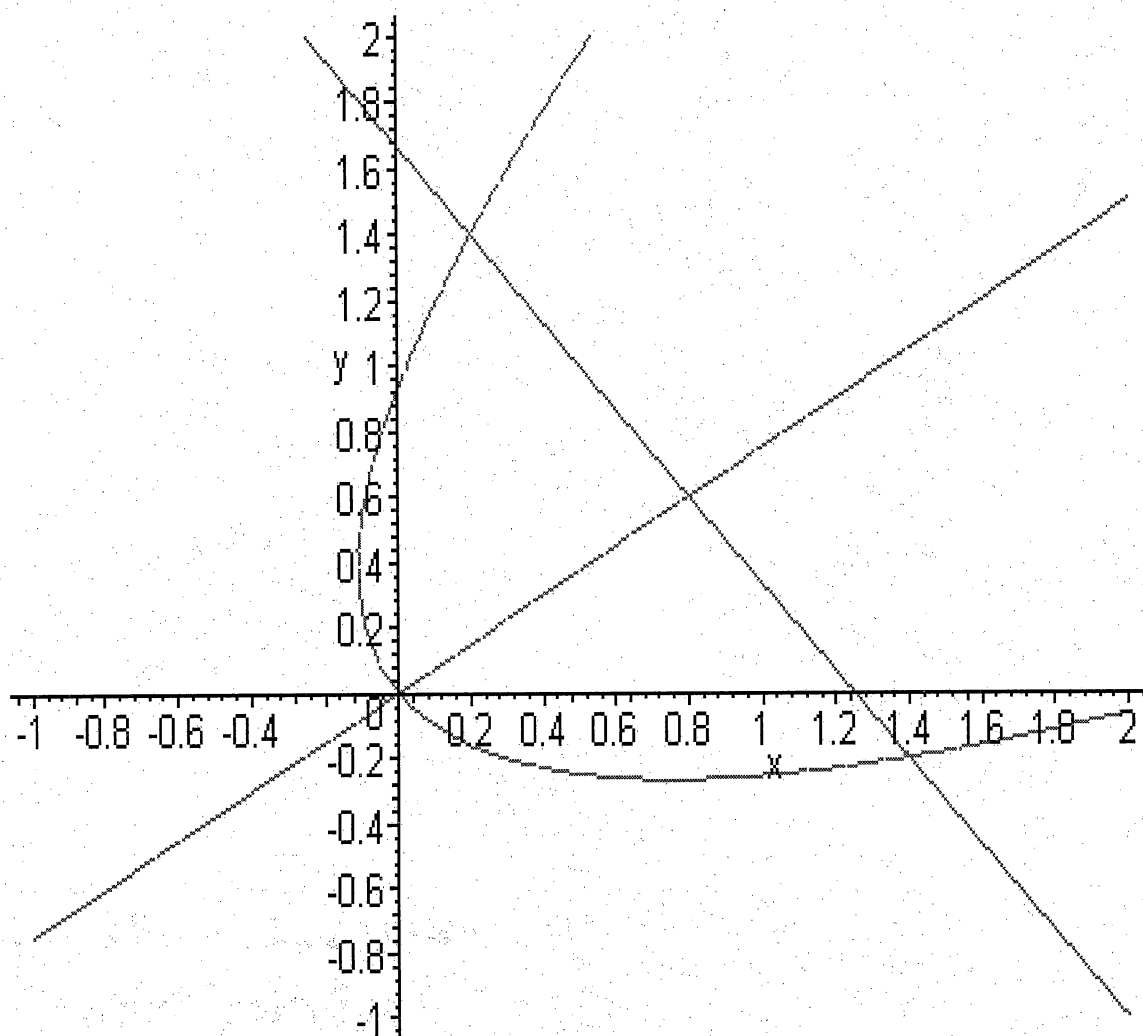
$d^2\left(\frac{2}{5}-\frac{3}{10}\sqrt{2},\frac{3}{10}+\frac{2}{5}\sqrt{2}\right)=\frac{3}{4}$, and p_3 gives the distance

$d^2\left(\frac{2}{5}+\frac{3}{10}\sqrt{2},\frac{3}{10}-\frac{2}{5}\sqrt{2}\right)=\frac{3}{4}$. Thus the minimum distance for

rotated polynomial is $\frac{3}{4}$. This is the graph of rotated

polynomial with linear equations $3x-4y=0$ and $4x+3y=5$.

Graph 1. Rotated equation with linear equations.



Conclusion

It is known that ideals in a polynomial ring in a single variable are principal. Also, there is a simple criterion for ideal membership; if $I = \langle g \rangle$ then $f \in I$ if and only if g divides f . We showed by example that ideals in a polynomial ring in several variables are not principal. However, they are finitely generated which we showed in Theorem 2, the Hilbert Basis Theorem. We developed a division algorithm for a polynomial in several variables. We showed that the quotient and the remainder needed not be unique. However, when a polynomial is divided by a Groebner basis, the remainder is unique (Theorem 3). In Theorem 3, we used this property to give a criterion for ideal membership: If $G = \{g_1, \dots, g_s\}$ is a Groebner basis and $I = \langle G \rangle$ then $f \in I$ if and only if G divides f . We then showed that if $I = \langle f_1, \dots, f_t \rangle$ has a Groebner basis, $G = \{g_1, \dots, g_s\}$, the system $f_1 = f_2 = \dots = f_t = 0$ is equivalent to $g_1 = \dots = g_s = 0$. In this second system, g_s will be a polynomial in a single variable when $I \cap k[x_n] = \{0\}$.

REFERENCES

- 1) D. Cox, J. Little, and D. O'Shea, Second Edition, Ideals, Varieties, and Algorithms, Springer-Verlag, New York Berlin Heidelberg, 1996.
- 2) D. Malik, J. Mordeson, M. Sen, Fundamentals of Abstract Algebra, New York, McGraw-Hill Companies Inc., 1997.
- 3) S. Grossman, Third Edition, Multivariable Calculus, Linear Algebra, and Differential Equations, Sanders College Publishing, San Diego, 1995.
- 4) A. Caruth, "A Concise Proof of Hilbert's Basis Theorem", *American Math. Monthly*, Volume 103, 1996, p 160-161.