



***PROVING SOME GEOMETRIC THEOREMS USING
GROEBNER BASES***

AREGAWI WELDEGIORGIS AKALE.

*A Project Report submitted to Addis Ababa University faculty of Computer and
Mathematical Sciences, Department of Mathematics
in Partial fulfillment of the requirements for the Degree of Master of Science in
Mathematics.*

ADVISOR: TILAHUN ABABAW (PhD)

JANUARY, 2011

Addis Ababa-Ethiopia

Addis Ababa University
Faculty of Computer and Mathematical Sciences
Department of Mathematics

Approved by the Board of Examiners:

Department Head

Signature

Examiner

Signature

Examiner

Signature

Permission

“This is to certify that this project is compiled /a recorded of the research work done / by Aregawi Weldegiorgis in the Department of mathematics, Addis Ababa University, under my supervision. I hereby also confirm that the project can be submitted for evaluation by examiners and eventual defense.

”

Advisor’s Signature

Table of Contents	page
Declaration.....	i
Permission.....	ii
Abstract.....	iii
Acknowledgements.....	iv
Introduction.....	1
Chapter One.....	3
Preliminaries.....	3
Introduction.....	3
1.1. Polynomials and Affine Varieties.....	3
1.2. Ideals.....	5
1.3. Monomial ordering and monomial ideals.....	6
1.4. The Hilbert basis theorem and Groebner bases.....	10
1.5. Properties of Groebner bases.....	11
1.6. Buchberger’s Algorithm.....	13
1.7. Application of Groebner bases for solving polynomial equations.....	16
1.8. Hilbert’s Nullstellensatz theorem and radical ideals.....	17
Chapter Two.....	20
Proving Some Geometric Theorems Using Groebner Basis.....	20
2.1. Introduction.....	20
2.2. Admissible Geometric theorem.....	21
2.3. Examples of Translation of geometric statements into Polynomials.....	22
2.3.1. Parallel lines.....	22
2.3.2. Perpendicular lines.....	23
2.3.3. Collinear.....	24
2.3.4. Circle.....	25
2.3.5. Midpoint.....	25
2.4. Proving Translated Theorems.....	27
2.4.1. The Circle Theorem of Apollonius.....	27
2.4.2. Pappus Theorem.....	31
Reference.....	35

Abstract

Algebraic Geometry can be used to prove geometric theorems in Euclidean Plane Geometry. This can be done when the geometric theorem has the property that the hypothesis and the conclusion of the theorem can be translated into polynomial equations. Such theorems are called admissible theorems. The geometric theorems considered involve points, lines, or circles in the Euclidean Plane which have common intersection points. In this project, first we translate the hypothesis and conclusion of the theorem in to polynomial equations. Then, the method *Groebner basis* is used to answer the ideal membership problem of the ideal generated by the polynomials in the hypothesis and the polynomials in the conclusion. The geometric theorems considered are the *Theorem of Apollonius* and *Pappus Theorem* which demonstrate the applicability of our method.

Acknowledgements

First and foremost, I want to express my great thank to my advisor Dr. Tilahun Ababaw for his continuous help and advice, valuable comments on a draft version of this project.

Heartily, I would like to thank to all staffs of Mathematics Department of Addis Ababa University who thought me all the courses.

Finally, I want to thank to the Digital Library for the full access of computers.

Declaration

“I declare that this project has been composed by me and that no part of the project has formed the basis for the award of any degree, diploma, associate ship, fellowship or any other similar title to me.

_____”

Author's Signature

Introduction

Algebraic geometry is a branch of mathematics which combines techniques of abstract algebra, especially commutative algebra, with the language and the problems of geometry. It occupies a central place in modern mathematics and has multiple conceptual connections with such diverse fields as complex analysis, topology and number theory. Initially a study of systems of polynomial equations in several variables, the subject of algebraic geometry starts where equation solving leaves off, and it becomes even more important to understand the intrinsic properties of the totality of solutions of a system of equations, than to find some solution; this leads into some of the deepest waters in the whole of mathematics, both conceptually and in terms of technique.

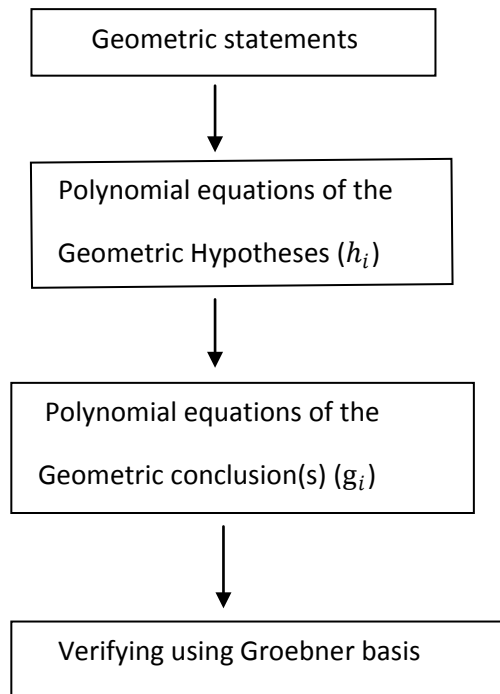
Algebraic geometry has a long history that can be said to go back to the Euclidean geometry in ancient Greece. Today, algebraic geometry is an area with geometry with connections to other areas such as commutative algebra, complex analysis, topology and number theory in mathematics, cryptography in informatics and string theory in physics.

Algebraic geometry concentrates on the abstract properties of the geometric objects by assigning them algebraic structures. The translation to algebra means that algebraic geometry is more suitable for studying geometric problems of higher complexity than other nearby fields.

In this project we will discuss algebraic methods in automatic geometric theorem proving, specifically the use of Groebner basis. Proving geometric statements algorithmically is an area of research which has particular importance in the fields of robotics and artificial intelligence.

In the first chapter, we will discuss some concepts from algebraic geometry and commutative algebra such as varieties, ideals and Groebner bases. In the second chapter, we will discuss the translation of geometric statements to algebraic statements. Next, we will see some model geometric theorems and how they can be translated in to polynomial equations. Lastly we will apply the Groebner basis method.

A systematic overview of the Automatic Geometric Theorem Proving is as follows



CHAPTER ONE

PRELIMINARIES

Introduction

In this chapter we will see the basic concepts which are very help full to prove generally the Automatic geometric theorem especially the theorem of the Circle of Apollonius and Pappus Theorem.

This chapter contains polynomials & affine varieties, ideals, monomial orderings and monomial ideals, Hilbert's basis theorem and Groebner basis, properties of Groebner bases &their applications for solving polynomial equations, Hilbert's Nullstellensatz theorem, and radical ideals.

Our aim is to prove a geometric theorem (specifically the theorem of the circle of Apollonius and Pappus Theorem) algebraically by applying the above mentioned concepts. We will change the geometric statements in to polynomial equations by using the concepts of slope of lines and distance formula.

Groebner bases were first discovered by Bruno Buchberger in 1965, who named them after his supervisor Wolfgang Groebner. They have been applied successfully in algebraic geometry and commutative algebra. The method we employed translates geometric statements into algebraic statements; we illustrate this in chapter 2.

First we begin with some basic concepts.

1.1. Polynomials and Affine Varieties

Definition 1.1.1 A monomial in x_1, x_2, \dots, x_n is a product of the form

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

where the exponents $\alpha_1, \alpha_2, \dots, \alpha_n$ are non-negative integers.

The total degree of this monomial is the sum $\alpha_1 + \alpha_2 + \dots + \alpha_n$

Let $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ be an n-tuple of non-negative integers. Then we can simplify the notation for monomials as $x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \dots \cdot x_n^{\alpha_n}$

Note that the monomial $x^\alpha = 1$ when $\alpha = (0, \dots, 0)$

Definition 1.1.2 A polynomial f in x_1, x_2, \dots, x_n with coefficients in a field k is a finite linear combination of monomials. We write a polynomial f in the form

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha}, \text{ where } a_{\alpha} \in k \text{ and } \alpha = (\alpha_1, \alpha_2, \dots, \alpha_n).$$

The set of all polynomials in x_1, x_2, \dots, x_n with coefficients in a field k is denoted by $k[x_1, \dots, x_n]$

Example 1.1.3 $f = \sqrt{2}x^2yz^3 + \frac{3}{4}xy^2 + 3xyz - z^4$ is a polynomial in $\mathbb{R}[x, y, z]$

Definition 1.1.4 For a field k and a positive integer n , we define the n -dimensional affine space over k to be the set

$$k^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in k\}$$

Consider the case of $k = \mathbb{R}$, then from calculus \mathbb{R}^1 is the number line and \mathbb{R}^2 is the coordinate plane.

In general, we call k^1 the affine line, k^2 the affine plane and so on.

Now, let us see how polynomials are related to affine space.

A polynomial $f = \sum_{\alpha} a_{\alpha} x^{\alpha} \in k[x_1, \dots, x_n]$ gives a function $f: k^n \rightarrow k$, define for a given $(a_1, \dots, a_n) \in k^n$, replace every x_i by a_i in the expression for f . Since all the coefficients lie in k , then this operation gives an element $f(a_1, \dots, a_n) \in k$. This enables us to link algebra and geometry.

Definition 1.1.5 Let k be a field, and let f_1, f_2, \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 varieties defined by f_1, f_2, \dots, f_s .

Thus an affine varieties $V(f_1, \dots, f_s) \subset k^n$ is the set of all solutions of the systems of equations $f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0$

Examples 1.1.6

- i. Let $k = \mathbb{R}$, in the plane \mathbb{R}^2 , $V(x^2 + y^2 - 1)$ which is the circle of radius 1 centered at the origin is an affine variety.
- ii. Generally conic sections studied in analytic geometry (circles, ellipses, parabolas, and hyperbolas) are affine varieties.
- iii. Graphs of polynomial functions are affine varieties. In this case the graph of

$$y = f(x) \text{ is } V(y - f(x))$$

1.2. Ideals

Definition 1.2.1 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 $hf \in I$

The goal of this section is how ideals relate with affine varieties and the real importance of ideals is to give us a language for computing with affine varieties

Definition 1.2.2 Let f_1, \dots, f_s be polynomials in $k[x_1, \dots, x_n]$. Then we set

$$\langle f_1, \dots, f_s \rangle = \{ \sum_{i=1}^s h_i f_i : h_1, \dots, h_s \in k[x_1, \dots, x_n] \}$$

Lemma 1.2.3 If $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, then $\langle f_1, \dots, f_s \rangle$ is an ideal of $k[x_1, \dots, x_n]$. We call $\langle f_1, \dots, f_s \rangle$ the ideal generated by f_1, \dots, f_s

Proof First, $0 \in \langle f_1, \dots, f_s \rangle$, since $0 = \sum_{i=1}^s 0 \cdot f_i$

Suppose that $f = \sum_{i=1}^s p_i \cdot f_i$ and $g = \sum_{i=1}^s q_i \cdot f_i$ for some $p_i, q_i \in k[x_1, \dots, x_n]$,

and let $h \in k[x_1, \dots, x_n]$, then

$$f + g = \sum_{i=1}^s (p_i + q_i) f_i \in I, \text{ since } p_i + q_i \in k[x_1, \dots, x_n]$$

$$hf = \sum_{i=1}^s (hp_i) f_i \in I, \text{ since } hp_i \in k[x_1, \dots, x_n]$$

Hence, $\langle f_1, \dots, f_s \rangle$ is an ideal of $k[x_1, \dots, x_n]$. ■

The ideal $\langle f_1, \dots, f_s \rangle$ has a nice interpretation in terms of polynomial equations.

Definition 1.2.4 Let $V \subset k^n$ be an affine variety. Then we set

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

Lemma 1.2.5 If $V \subset k^n$ is an affine variety, then $I(V) \subset k[x_1, \dots, x_n]$ 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 , in particular it vanishes on V .

Next, suppose that $f, g \in I(V)$ and $h \in k[x_1, \dots, x_n]$. let (a_1, \dots, a_n) be an arbitrary point of V .

Now, $f(a_1, \dots, a_n) + g(a_1, \dots, a_n) = 0 + 0 = 0$, then $f + g \in I(V)$

$$h(a_1, \dots, a_n)f(a_1, \dots, a_n) = h(a_1, \dots, a_n) \cdot 0 = 0. \text{ Then, } hf \in I(V)$$

Hence $I(V)$ is an ideal of V . ■

1.3. Monomial ordering and monomial ideals

Definition 1.3.1 A monomial ordering on $k[x_1, \dots, x_n]$ is any relation ' $>$ ' on $\mathbb{Z}_{\geq 0}^n$, or equivalently, any relation on the set of monomials x^α , $\alpha \in \mathbb{Z}_{\geq 0}^n$, Satisfying

- i. $>$ is a total(or linear) ordering on $\mathbb{Z}_{\geq 0}^n$. that is, for any $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$, then exactly one of the three conditions hold: $\alpha > \beta$, $\alpha = \beta$, $\alpha < \beta$
- ii. if $\alpha > \beta$ and $\gamma \in \mathbb{Z}_{\geq 0}^n$, then $\alpha + \gamma > \beta + \gamma$.
- iii. $>$ is a well-ordering on $\mathbb{Z}_{\geq 0}^n$. This means that every non empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under $>$.

The usual numerical order $\dots > m + 1 > m > \dots > 3 > 2 > 1 > 0$ is an example of monomial ordering.

Definition 1.3.2 (Lexicographic Order)

Let $\alpha = (\alpha_1, \dots, \alpha_n)$, $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. We say $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most non-zero entry is positive.

We will write $x^\alpha >_{lex} x^\beta$ if $\alpha >_{lex} \beta$.

Example 1.3.3

- 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. $(1,0, \dots, 0) >_{lex} (0,1, \dots, 0) >_{lex, \dots, >_{lex}} (0,0, \dots, 1)$

Note that the *lex order* on $\mathbb{Z}_{\geq 0}^n$ is a monomial order.

Definition 1.3.4 (Graded Lex Order)

Let $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. 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 use *lex order*.

Example 1.3.5

- i) $(1,2,3) >_{grlex} (3,2,0)$ since $|(1,2,3)| = 6 > |(3,2,0)| = 5$
- ii) $(1,2,4) >_{grlex} (1,1,5)$ since $|(1,2,4)| = |(1,1,5)|$ and $(1,2,4) >_{lex} (1,1,5)$.

Note that like *lex order*, *grlex order* is also a monomial ordering.

Definition 1.3.6 Let $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ be a non-zero polynomial in $k[x_1, \dots, x_n]$ and let $>$ be a monomial order.

- i. The multi degree of f is $\text{multideg}(f) = \max_{\{\alpha \in \mathbb{Z}_{\geq 0}^n : a_{\alpha} \neq 0\}} \alpha$, the maximum is taken with respect to $>$.
- ii. The leading coefficient of f is $LC(f) = a_{\text{multideg}(f)} \in k$
- iii. The leading monomial of f is $LM(f) = x^{\text{multideg}(f)}$ (With coefficient 1)
- iv. The leading term of f is $LT(f) = LC(f) LM(f)$

Example 1.3.7 Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ and let $>$ denote the *lex order*.

Then, $\text{multideg}(f) = (3,0,0)$

$$LC(f) = -5$$

$$LM(f) = x^3$$

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

Lemma 1.3.8 Let $f, g \in k[x_1, \dots, x_n]$ be non-zero polynomials. Then

- i. $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$
- ii. If $f + g \neq 0$, then $\text{multideg}(f + g) \leq \max(\text{multideg}(f) + \text{multideg}(g))$.

If in addition, $\text{multideg}(f) \neq \text{multideg}(g)$, then equality occurs.

Proof: [1]

Definition 1.3.9 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 $h_{\alpha} \in k[x_1, \dots, x_n]$. In this case, we write $I = \langle x^{\alpha} : \alpha \in A \rangle$

Lemma 1.3.10 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 Suppose x^{β} is a multiple of x^{α} . then by the definition of an ideal $x^{\beta} \in I$.

Conversely, let $x^{\beta} \in I$. Then $x^{\beta} = \sum_{i=1}^s h_i x^{\alpha_i}$, where $h_i \in k[x_1, \dots, x_n]$ 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^{α_i} . Hence, the left side x^{β} must have the same property. ■

Theorem 1.3.11 (Division Algorithm in $k[x_1, \dots, x_n]$)

Fix a monomial order $>$ on $\mathbb{Z}_{\geq 0}^n$, and let $F = \langle f_1, \dots, f_s \rangle$ 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 coefficient in k) of monomials, none of which is divisible by any of $LT(f_1), LT(f_2), \dots, LT(f_s)$.

We call r a remainder of f on division by F . Furthermore, if $a_i f_i \neq 0$, then we have

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

Proof [1]

Example 1.3.11. Let us divide $f = x^2 y + x y^2 + y^2$ by $f_1 = y^2 - 1$ and $f_2 = x y - 1$.

Use *lex order* with $x > y$. Then,

$$a_1 = x + 1$$

$$a_2 = x$$

$$\begin{array}{r} y^2 - 1 \quad \sqrt{\begin{array}{r} x^2 y + x y^2 + y^2 \\ x^2 y - x \end{array}} \\ \hline x y - 1 \quad \begin{array}{r} x y^2 + y^2 + x \\ \hline x y^2 - x \\ \hline y^2 + 2x \\ \hline y^2 - 1 \\ \hline 2x + 1 \end{array} \end{array}$$

Hence, $f = x^2 y + x y^2 + y^2 = (x + 1)(y^2 - 1) + x.(x y - 1) + 2x + 1$

1.4. The Hilbert basis theorem and Groebner bases

Definition 1.4.1 Let $I \subset k[x_1, \dots, x_n]$ be a non zero ideal of $k[x_1, \dots, x_n]$

- i. We denote by $LT(I)$ the set of leading terms of I . Thus

$$LT(I) = \{cx^\alpha : \text{there exists } f \in I \text{ with } LT(f) = cx^\alpha\}$$

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

Let $I = \langle f_1, \dots, f_s \rangle$. Then $\langle LT(f_1), LT(f_2), \dots, LT(f_s) \rangle$ and $\langle LT(I) \rangle$ may be different ideals. It is true by definition that $LT(f_i) \in LT(I) \subset \langle LT(I) \rangle$, which implies $\langle LT(f_1), LT(f_2), \dots, LT(f_s) \rangle \subset \langle LT(I) \rangle$. However, $\langle LT(I) \rangle$ can be strictly larger. To see this, Let $I = \langle f_1, f_2 \rangle$, where $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$, and using the *grlex ordering* on monomials in $k[x, y]$. Then

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

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

By Lemma 1.3.10, x^2 is not an element of $\langle LT(f_1), LT(f_2), \dots, LT(f_s) \rangle$

Proposition 1.4.2 Let $I \subset k[x_1, \dots, x_n]$ be an ideal.

- i. $\langle LT(I) \rangle$ is a monomial ideal.
 ii. There are $g_1, \dots, g_t \in I$ such that $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$.

Proof [1]

Theorem 1.4.3. (Hilbert basis theorem):

Every ideal $I \subset k[x_1, \dots, x_n]$ has a finite generating set. That is, $I = \langle g_1, \dots, g_t \rangle$ for some $g_1, \dots, g_t \in I$.

Definition 1.4.4 Fix a monomial order. A finite subset $G = \{g_1, \dots, g_t\}$ of an ideal I is said to be a Groebner basis (or standard basis) if

$$\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_t) \rangle$$

Equivalently, but more informally, a set $\{g_1, \dots, g_t\} \subset I$ 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 1.4.5 Fix a monomial order. Then every ideal $I \subset k[x_1, \dots, x_n]$ other than $\{0\}$ has a Groebner basis. Furthermore any Groebner basis for an ideal I is a basis of I .

Definition 1.4.6 Let $I \subset k[x_1, \dots, x_n]$ be an ideal. We will denote by $V(I)$ the set

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

Remark 1.4.7 If $I = \langle f_1, \dots, f_s \rangle$, then $V(I) = V(f_1, \dots, f_s)$

1.5. Properties of Groebner bases

Proposition 1.5.1 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 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 f by G no matter how the elements of G are listed when using the division algorithm

Corollary 1.5.2 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 the remainder is zero, then we have already observed that $f \in I$. Conversely, given $f \in I$, then $f = f + 0$ satisfies the two conditions of the above proposition. Hence 0 is the remainder of f on division by G . ■

Definition 1.5.3 We will write \overline{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 the above proposition.

Let $F = \{x^2y - y^2, x^4y^2 - y^2\} \subset k[x, y]$, using the lex order, we have, $\overline{x^5y}^F = xy^3$

Since the division algorithm yields,

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3$$

Definition 1.5.4 Let $f, g \in k[x_1, \dots, x_n]$ be non zero polynomials

- a. If $\text{multideg}(f) = \alpha$, $\text{multideg}(g) = \beta$, And 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 $x^\gamma = LCM(LM(f), LM(g))$
- b. The **S-polynomial** of f and g is the combination

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

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

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

$$\gamma = (4, 2) \text{ and } S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x \cdot f - \left(\frac{1}{3}\right) \cdot y \cdot g$$

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

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

Lemma 1.5.5 Suppose we have a sum $\sum_{i=1}^s c_i f_i$, where $c_i \in k$ and $\text{multideg}(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$, for all i . If $\text{multideg}(\sum_{i=1}^s c_i f_i) < \delta$. Then $\sum_{i=1}^s c_i f_i$ is a linear combination, with coefficients in k , of the S-polynomials $S(f_j, f_k)$ for $1 \leq j, k \leq s$. Furthermore, each $S(f_j, f_k)$ has multidegree $< \delta$.

Note: when f_1, \dots, f_s satisfy the hypothesis of the above Lemma 1.5.5; we get an equation of the form; $\sum_{i=1}^s c_i f_i = \sum_{j,k} c_{jk} S(f_j, f_k)$

Theorem 1.5.6 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

1.6. Buchberger's Algorithm

We have seen that every ideal in $k[x_1, \dots, x_n]$ other than $\{0\}$ has a Groebner basis. Now we will see for a given ideal $I \subset k[x_1, \dots, x_n]$, how can we construct a Groebner basis for I . let's see this by the following example

Example 1.6.1 Consider the ring $k[x, y]$ with the grlex order, and let $I = \langle f_1, f_2 \rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle$. Recall that $\{f_1, f_2\}$ is not a Groebner basis for I since $LT(S(f_1, f_2)) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$.

To produce a Groebner basis, one natural idea is to try first to extend the original generating set to a Groebner basis by adding more polynomials in I . Its remainder on division by $F = (f_1, f_2)$ is $-x^2$, which is non-zero. Hence, we should include this remainder in our generating set, as a new generator $f_3 = -x^2$. If we set $F = (f_1, f_2, f_3)$, we can use Theorem 1.5.6 to test if this new set is a Groebner basis for I . We compute

$$S(f_1, f_2) = f_3, \text{ so}$$

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

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

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

Hence we must add $f_4 = -2xy$ to our generating set. If we let $F = (f_1, f_2, f_3, f_4)$, then

$$\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0,$$

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

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

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

$$\overline{S(f_2, f_3)}^F = -2y^2 + x \neq 0.$$

Thus, we must also add $f_5 = -2y^2 + x$ to our generating set. Setting $\{f_1, f_2, f_3, f_4, f_5\}$, one can compute that

$$\overline{S(f_i, f_j)}^F = 0 \text{ for all } 1 \leq i \leq j \leq 5$$

By Theorem 1.5.6, it follows that a grlex Groebner basis for I is given by

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

The above example suggests that in general, one should try to extend a basis F to a Groebner basis by successively adding non-zero remainders $\overline{S(f_i, f_j)}^F$ to F .

Theorem 1.6.2 Let $I = \langle f_1, \dots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a Groebner basis for I can be constructed in a finite number of steps by the following Algorithm:

Input: $F = \langle f_1, \dots, f_s \rangle$

Output: a Groebner basis $G = \langle g_1, \dots, g_t \rangle$ for I , with $F \subset G$

$G := F$

REPEAT

$G' := G$

FOR each pair $\{p, q\}, p \neq q$ *in* G' *DO*

$$S := \overline{S(p, q)}^{G'}$$

IF $S \neq 0$, *THEN* $G := G \cup \{s\}$

UNTIL $G := G'$

Groebner bases computed using the algorithm of the above theorem are often bigger than necessary. We can eliminate some unneeded generators by using the following fact.

Lemma 1.6.3 Let G be a Groebner basis for the polynomial ideal I . Let $p \in G$ be a polynomial such that $LT(p) \in \langle LT(G - \{p\}) \rangle$. Then $G - \{p\}$ is also a Groebner basis for I .

Proof: We know that $\langle LT(G) \rangle = \langle LT(I) \rangle$. If $LT(p) \in \langle LT(G - \{p\}) \rangle$, then $\langle LT(G - \{p\}) \rangle = \langle LT(G) \rangle$. By definition it follows that $G - \{p\}$ is also a Groebner basis. ■

Definition 1.6.4 A **minimal Groebner basis** for a polynomial ideal I is a Groebner basis G for I such that:

- I. $LC(p) = 1$ for all $p \in G$.
- II. For all $p \in G$, $LT(p) \notin \langle LT(G - \{p\}) \rangle$

We can construct a minimal Groebner basis for a given non-zero ideal by applying the algorithm and then using Lemma 1.6.3 to eliminate any unneeded generators that might have been included. To illustrate this procedure, we return once again to the ideal I studied in the above Example 1.6.1. Using grlex order, we found the Groebner basis

$$f_1 = x^3 - 2xy$$

$$f_2 = x^2y - 2y^2 + x$$

$$f_3 = -x^2$$

$$f_4 = -2xy$$

$$f_5 = -2y^2 + x$$

Since some of the leading coefficients are different from 1, the first step is to multiply the generators by suitable constants to make this true. Then note that

$$LT(f_1) = x^3 = -x \cdot LT(f_3).$$

By Lemma 1.6.3, we can dispense with f_1 in the minimal Groebner basis. Similarly, since $LT(f_2) = x^2y = -(1/2)x \cdot LT(f_4)$, we can also eliminate f_2 . There are no further

cases where the leading term of a generator divides the leading term of another generator. Hence, $\tilde{f}_3 = x^2$, $\tilde{f}_4 = xy$, $\tilde{f}_5 = y^2 - (1/2)x$ is a minimal Groebner basis for I .

Unfortunately, a given ideal may have many minimal Groebner bases. For example, in the ideal I consider above $\tilde{f}_3 = x^2 + axy$, $\tilde{f}_4 = xy$, $\tilde{f}_5 = y^2 - (1/2)x$ is also a minimal Groebner basis, where $a \in k$ is any constant.

Definition 1.6.5 A **reduced Groebner basis** for a polynomial ideal I is a Groebner basis G for I such that:

- I. $LC(p) = 1$ for all $p \in G$.
- II. For all $p \in G$, no monomial of p lies in $\langle LT(G - \{p\}) \rangle$

Note: Let $I = \{0\}$ be a polynomial ideal. Then, for a given monomial ordering, I has a unique reduced Groebner basis.

1.7. Application of Groebner bases for solving polynomial equations

Next, we will see how the Groebner basis technique can be applied to solve systems of polynomial equations in several variables. Let's express this by giving an example

Example 1.7.1 Consider the equations

$$x^2 + y^2 + z^2 = 1, \quad x^2 + z^2 = y, \quad x = z \text{ in } \mathbb{C}^3.$$

These equations determine $I = \langle x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z \rangle \subset \mathbb{C}[x, y, z]$, and we want to find all points in $V(I)$. By Remark 1.4.7, we can compute $V(I)$ using any basis of I .

With respect to the *lex order*, the basis is

$$g_1 = x - z$$

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

$$g_3 = z^4 + \left(\frac{1}{2}\right)z^2 - 1/4$$

The polynomial g_3 depends on z alone, and its roots can be found by first using the quadratic formula to solve for z^2 , then, taking square roots,

$$z = \pm \frac{1}{2} \sqrt{\pm \sqrt{5} - 1}$$

This gives us four values of z . Next, when these values of z are substituted in to the equations $g_2 = 0$ and $g_1 = 0$, those two equations can be solved uniquely for y and x , respectively. Thus there are four solutions altogether of $g_1 = g_2 = g_3 = 0$, two real and two complex. Since $V(I) = V(g_1, g_2, g_3)$ by Remark 1.4.7, we have found all the solutions.

1.8. Hilbert's Nullstellensatz theorem and radical ideals.

Recall that $I(V) = \{f \in k[x_1, \dots, x_n] : f(x) = 0 \text{ for all } x \in V\}$ of all polynomials vanishing on V .

And for ideal $I \subset k[x_1, \dots, x_n]$, we can define the set

$$V(I) = \{x \in k^n : f(x) = 0 \text{ for all } f \in I\}$$

By the Hilbert's theorem $V(I)$ is an affine variety and there exists a finite set of polynomials $f_1, \dots, f_s \in I$ such that $I = \langle f_1, \dots, f_s \rangle$ and in Remark 1.4.7, we have seen that $V(I)$ is the set of common roots of these polynomials.

Theorem 1.8.1 (Hilbert's Nullstellensatz)

Let k be an algebraically closed field. If $f, f_1, \dots, f_s \in k[x_1, \dots, x_n]$ are such that $f \in I(V(f_1, \dots, f_s))$, then there exists an integer $m \geq 1$ such that

$$f^m \in \langle f_1, \dots, f_s \rangle \quad (\text{and conversely})$$

Lemma 1.8.2 Let V be a variety, if $f^m \in I(V)$, then $f \in I(V)$.

Proof. Let $x \in V$. If $f^m \in I(V)$, then $(f(x))^m = 0$

This implies $f(x) = 0$

Hence, $f \in I(V)$, Since $x \in V$ ■

Definition 1.8.3 An ideal I is radical, if $f^m \in I$ for some integer $m \geq 1$, then $f \in I$.

By Lemma 1.8.2, $I(V)$ is a radical ideal.

Definition 1.8.4 Let $I \subset k[x_1, \dots, x_n]$ be an ideal. Then radical of I , denoted \sqrt{I} , is the set

$$\{f: f^m \in I \text{ for some integer } m \geq 1\}$$

Remark

- i. The ideal $I \subset \sqrt{I}$ Since $f \in I \Rightarrow f^1 \in I$ and hence $f \in \sqrt{I}$.
- ii. The radical of an ideal is an ideal.
- iii. If I is an ideal in $k[x_1, \dots, x_n]$, then \sqrt{I} is an ideal in $k[x_1, \dots, x_n]$

Theorem 1.8.5 (The Strong Nullstellensatz Theorem)

Let k be an algebraically closed field. If I is an ideal in $k[x_1, \dots, x_n]$, then

$$I(V(I)) = \sqrt{I}.$$

Proof If $f \in \sqrt{I}$, then $f^m \in I$, for some $m \geq 1$

f^m Vanishes on $V(I)$

This implies f Vanishes on $V(I)$, which again implies $f \in I(V(I))$

$$\text{Hence, } \sqrt{I} \subset I(V(I))$$

Let $f \in I(V(I))$, by definition, f Vanishes on $V(I)$.

By Hilbert's Nullstellensatz Theorem, there exists an integer $m \geq 1$ such that

$$f^m \in I$$

This implies $f \in \sqrt{I}$

Again this implies $I(V(I)) \subset \sqrt{I}$, Since f is arbitrary.

$$\text{Hence, } I(V(I)) = \sqrt{I}. \quad \blacksquare$$

Proposition 1.8.6 (Radical Ideal Membership) Let k be an arbitrary field and let $I = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal

$$\tilde{I} = \langle f_1, \dots, f_s, 1 - yf \rangle \subset k[x_1, \dots, x_n, y]$$

(In which case, $\tilde{I} = k[x_1, \dots, x_n, y]$)

Note that if $f \in \sqrt{\langle f_1, \dots, f_s \rangle} \subset k[x_1, \dots, x_n]$ we compute a reduced Groebner basis of the ideal $\langle f_1, \dots, f_s, 1 - yf \rangle \subset k[x_1, \dots, x_n, y]$ with respect to some ordering. If the result is $\{1\}$, then $f \in \sqrt{I}$. Otherwise, $f \notin \sqrt{I}$

Example 1.8.7. Consider the ideal $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$ in $k[x, y]$

Let us test whether $f = y - x^2 + 1$ lies in \sqrt{I} . Using lex order on $k[x, y, z]$, the ideal

$\tilde{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) \rangle \subset k[x, y, z]$ has a reduced Groebner basis $\{1\}$. By Proposition 1.8.6, it implies that $f \in \sqrt{I}$.

CHAPTER TWO

PROVING SOME GEOMETRIC THEOREMS USING GROEBNER BASIS

2.1. Introduction

The idea that we will consider is that once we introduce Cartesian coordinates in the Euclidean plane geometry, the hypotheses and the conclusions of geometric theorems can be expressed as polynomial equations between the coordinates of collections of points specified in the statements.

Suppose there are two sets of polynomials, one describing the hypotheses and the other describing the conclusion. In this chapter, we will consider the class of theorems, whose algebraic formulations involve polynomial equations of the form,

hypotheses: $h_1(x) = 0, \dots, h_n(x) = 0$ and

conclusion: $g(x) = 0$, where $x = (x_1, \dots, x_n)$ are geometric entities.

The polynomials are all in x with coefficients in the geometry associated with a field k .

Proving a geometric theorem implies that

For all x , if $h_1(x) = 0, \dots, h_n(x) = 0$, then this implies $g(x) = 0$.

Now we apply the algebraic concepts written in the preliminaries. We will work in the ring $k[u_1, \dots, u_m, x_1, \dots, x_n]$.

The ‘hypothesis ideal’ $I \subset k[u_1, \dots, u_m, x_1, \dots, x_n]$ is defined as:

$$I = (h_1, \dots, h_n)$$

Suppose g_i is in I , then

$$g_i = f_1 h_1 + \dots + f_n h_n, \text{ for some } f_1, \dots, f_n.$$

So, if g_i is in I and $h_i(x) = 0$, then $g_i(x) = 0$. In practice, this implies that if the hypotheses are described by the h_i , then the conclusion holds.

Now we want to show whether $g_i \in I$. To determine whether $g_i \in I$, we calculate a Groebner basis G of I . For each g_i determine the remainder on division of g_i by G . If this remainder is zero for all i , then g_i is in I .

A Groebner basis method is an algorithmic method used to prove a conclusion that follows generically from a set of hypotheses.

2.2. Admissible Geometric theorem

When we say translation of geometric statements into polynomials, it is to mean that expressing geometrical ideas such as distance of line segment, circle, midpoint etc in algebraic form. That is, in the form of polynomial equations.

Definition 2.2.1 A geometric theorem is said to be *admissible* if both its hypotheses and its conclusions admit translation in to polynomial equations.

Let u_1, \dots, u_m be the independent variable and x_1, \dots, x_n be the dependant variables of a geometric theorem. The hypotheses and the conclusions of the theorem will be expressed as polynomials in the u_i, x_j .

When we prove a geometric theorem algebraically, we may have many conclusions. Since we can threat them one at a time, it suffices to consider the case of one conclusion.

Let the conclusion be

$$g(u_1, \dots, u_m, x_1, \dots, x_n) = 0$$

we want to deduce that g follows from h_1, \dots, h_n algebraically. We need g to vanish whenever h_1, \dots, h_n do, and this leads to the application of algebraic varieties and ideals.

Let the variety be

$$V = V(h_1, \dots, h_n) = \{a \in k^{m+n} : h_i(a) = 0 \text{ for } 1 \leq i \leq n\}$$

And, let the ideal be

$$I(V) = \{f \in k[u_1, \dots, u_m, x_1, \dots, x_n] : f(a) = 0 \text{ for all } a \in V\}.$$

Definition 2.2.2 The conclusion g follows strictly from the hypotheses h_1, \dots, h_n if $g \in I(V) \subset k[u_1, \dots, u_m, x_1, \dots, x_n]$ where $V = V(h_1, \dots, h_n)$

Proposition 2.2.3 If $g \in \sqrt{\langle h_1, \dots, h_n \rangle} = \{f \in k[u_1, \dots, u_m, x_1, \dots, x_n] : f^s \in \langle h_1, \dots, h_n \rangle \text{ for some } s\}$, then g follows strictly from h_1, \dots, h_n .

Proof The hypothesis $g \in \sqrt{\langle h_1, \dots, h_n \rangle}$ implies that $g^s \in \langle h_1, \dots, h_n \rangle$ for some s . Thus, $g^s = \sum_{i=1}^n A_i h_i$ where $A_i \in k[u_1, \dots, u_m, x_1, \dots, x_n]$

Now for each $a \in V$,

$$g^s(a) = \sum_{i=1}^n A_i(a) h_i(a) = \sum_{i=1}^n A_i(a) \cdot 0 = 0$$

Therefore $g(a) = 0$, that is, $g \in I(V)$.

Hence g must vanish whenever h_1, \dots, h_n do. ■

Remark 2.2.4 The above proposition is useful because we can test whether

$g \in \sqrt{\langle h_1, \dots, h_n \rangle}$ using the radical membership algorithm. Let $\tilde{I} = \langle h_1, \dots, h_n, 1 - yg \rangle$ in the ring $\mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$. Then the radical membership proposition implies that

$g \in \sqrt{\langle h_1, \dots, h_n \rangle}$ if and only if $\{1\}$ is the reduced Groebner basis of \tilde{I} . If this condition is satisfied, then g follows strictly from h_1, \dots, h_n .

2.3. Examples of Translation of geometric statements into Polynomials

Let us consider a few examples that show translations of geometric statements into a suitable system of algebraic equations.

2.3.1. Parallel lines

Two parallel lines can be translated into polynomial equation as follows.

Let A, B, C, D be points in the plane, and let \overline{AB} be parallel to \overline{CD} as shown in the figure below.

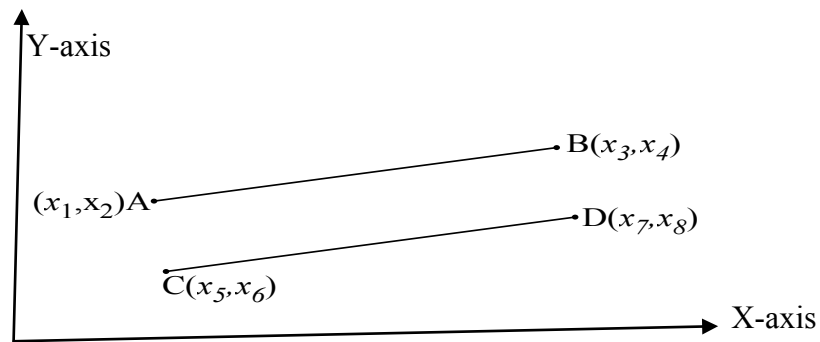


Figure 2.1: parallel lines

Since \overline{AB} is parallel to \overline{CD} , Slope of \overline{AB} = Slope of \overline{CD}

This implies that $\frac{x_4 - x_2}{x_3 - x_1} = \frac{x_8 - x_6}{x_7 - x_5}$. This is also the same as

$(x_4 - x_2)(x_7 - x_5) = (x_3 - x_1)(x_8 - x_6)$, using distributive property and collecting to the left side gives

$$x_1(x_8 - x_6) - x_2(x_7 - x_5) - x_3(x_8 - x_6) + x_4(x_7 - x_5) = 0$$

Therefore, $h = x_1(x_8 - x_6) - x_2(x_7 - x_5) - x_3(x_8 - x_6) + x_4(x_7 - x_5) = 0$ is a polynomial equation.

2.3.2. Perpendicular lines

Let \overline{AB} be perpendicular to \overline{CD} as in the figure below.

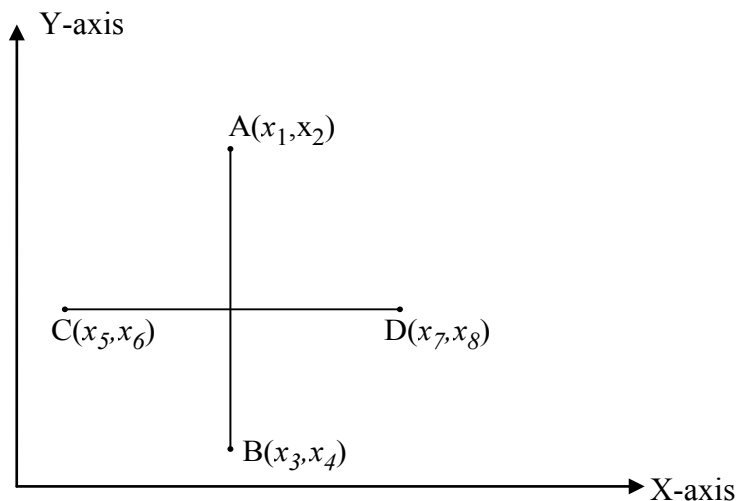


Figure 2.2: perpendicular lines

Since the product of slopes of perpendicular line segments is -1 , that is

$$(\text{Slope of } \overline{AB}) \cdot (\text{Slope of } \overline{CD}) = -1$$

$$\left(\frac{x_4-x_2}{x_3-x_1}\right) \left(\frac{x_8-x_6}{x_7-x_5}\right) = -1$$

This implies $(x_4 - x_2)(x_8 - x_6) = -[(x_3 - x_1)(x_7 - x_5)]$

Applying distributive property and collecting to the left gives,

$$-x_1(x_7 - x_5) - x_2(x_8 - x_6) + x_3(x_7 - x_5) + x_4(x_8 - x_6) = 0$$

Therefore, $h = -x_1(x_7 - x_5) - x_2(x_8 - x_6) + x_3(x_7 - x_5) + x_4(x_8 - x_6) = 0$ is a polynomial equation.

2.3.3. Collinear

Let A, B, C be collinear points in the plane as shown in the figure below.

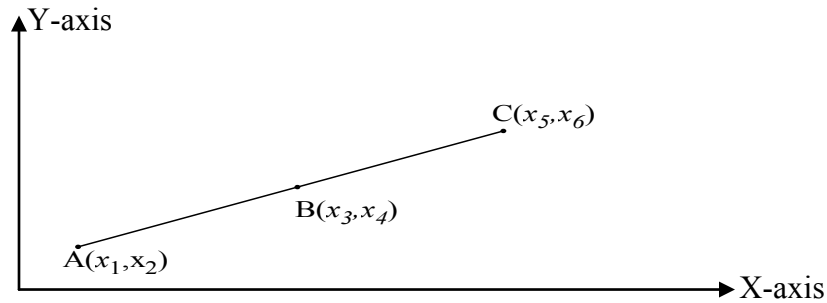


Figure 2.3: collinear points

Since A, B, C are collinear, Slope of $\overline{AB} = \text{Slope of } \overline{AC}$

This gives, $\frac{x_4-x_2}{x_3-x_1} = \frac{x_6-x_2}{x_5-x_1}$, which also the same as

$$(x_4 - x_2)(x_5 - x_1) = (x_3 - x_1)(x_6 - x_2)$$

Distributing and collecting to the left side gives

$$x_1(x_6 - x_2) - x_2(x_5 - x_1) - x_3(x_6 - x_2) + x_4(x_5 - x_1) = 0$$

Therefore, $h = x_1(x_6 - x_2) - x_2(x_5 - x_1) - x_3(x_6 - x_2) + x_4(x_5 - x_1) = 0$ is a polynomial equation.

2.3.4. Circle

Suppose C lies on the circle of center A and radius AB as shown in the following figure.

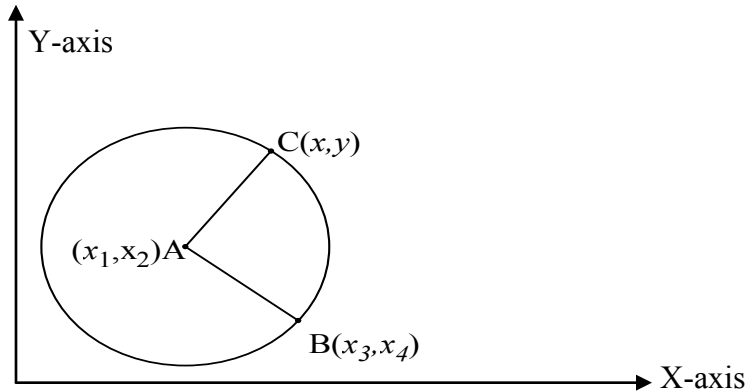


Figure 2.4: Circle

$$\text{Radius } (r) = AB = \sqrt{(x_3 - x_1)^2 + (x_4 - x_2)^2}$$

Since C lies on the circle, then $AC = AB$.

$$\text{This implies } \sqrt{(x - x_1)^2 + (y - x_2)^2} = \sqrt{(x_3 - x_1)^2 + (x_4 - x_2)^2}$$

$$\text{Squaring both sides gives } (x - x_1)^2 + (y - x_2)^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2$$

$$\text{This implies } (x - x_1)^2 + (y - x_2)^2 - (x_3 - x_1)^2 - (x_4 - x_2)^2 = 0$$

Hence, $h = (x - x_1)^2 + (y - x_2)^2 - (x_3 - x_1)^2 - (x_4 - x_2)^2 = 0$ is a polynomial

2.3.5. Midpoint

Suppose C be the midpoint of \overline{AB} as in the figure below.

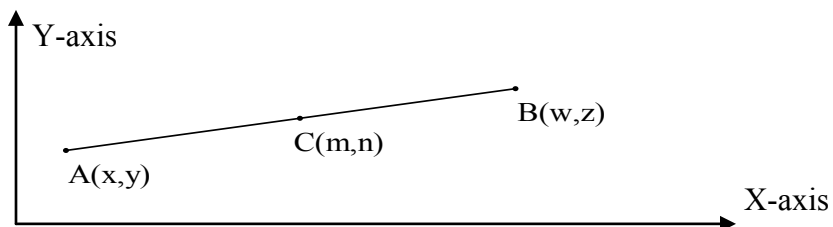


Figure 2.5: midpoint

Since C is the midpoint of \overline{AB} , then $AC = CB$.

By distance formula we have,

$$\sqrt{(m-x)^2 + (n-y)^2} = \sqrt{(w-m)^2 + (z-n)^2}.$$

Squaring both sides gives,

$$(m-x)^2 + (n-y)^2 = (w-m)^2 + (z-n)^2.$$

This implies $(m-x)^2 + (n-y)^2 - (w-m)^2 - (z-n)^2 = 0$.

Hence, $h = (m-x)^2 + (n-y)^2 - (w-m)^2 - (z-n)^2 = 0$ is a polynomial.

2.4. Proving Translated Theorems

In the above sections we have seen that, we can translate geometric statements in to systems of algebraic equations in the ring $k[u_1, \dots, u_m, x_1, \dots, x_n]$

In the following theorems, h_1, \dots, h_n denote the hypotheses and g_1, \dots, g_r the conclusions.

2.4.1. The Circle Theorem of Apollonius

Theorem 2.4.1

Let $\triangle ABC$ be right triangle in the plane, with right angle at A . The midpoints of the three sides and the foot of the altitude drawn from A to \overline{BC} all lie on one circle. (See the figure below)

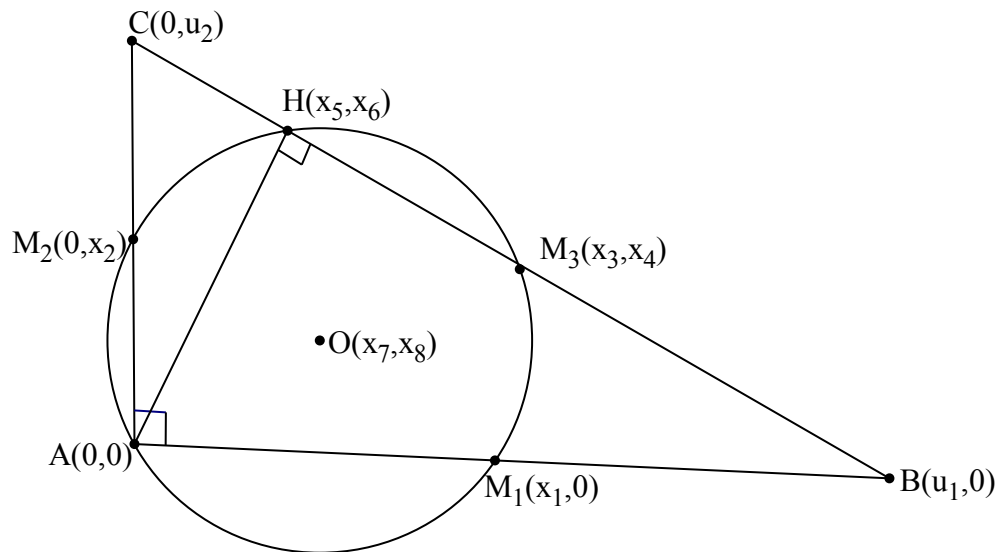


Figure 2.6: Circle Theorem of Apollonius

Proof To translate this geometrical statement to polynomial form, showing that the circle theorem is admissible, we begin by constructing the triangle.

Place A at $(0,0)$ and B at $(u_1,0)$, $u_1 \neq 0$ the hypothesis that $\angle CAB$ is a right angle tells us that $C = (0,u_2)$ and $u_2 \neq 0$

Next, we will construct the three midpoints of the sides. Suppose these points have coordinates $M_1 = (x_1, 0)$, $M_2 = (0, x_2)$ and $M_3 = (x_3, x_4)$. We use the convention that u_i 's are to be arbitrary, whereas the x_i 's are determined by the values of u_i 's.

Since M_1, M_2 , and M_3 are mid points, then by mid point formula we obtain the equations

$$\begin{aligned} h_1 &= 2x_1 - u_1 = 0 \\ h_2 &= 2x_2 - u_2 = 0 \\ h_3 &= 2x_3 - u_1 = 0 \\ h_4 &= 2x_4 - u_2 = 0 \end{aligned} \tag{1}$$

The next step is to construct the point $H = (x_5, x_6)$, the foot of the altitude drawn from A .

We have two hypotheses here:

$$AH \perp BC \text{ implies } h_5 = x_5 u_1 - x_6 u_2 = 0 \tag{2}$$

$$B, H, C \text{ are collinear implies } h_6 = x_5 u_2 + x_6 u_1 - u_1 u_2 = 0$$

Finally, we want to show that, M_1, M_2, M_3, H lie on a circle.

From Euclidean plane geometry, three non-collinear points determine a circle (the circumscribed circle of the triangle they form).

Now, our conclusion can be stated as:

If we construct the circle containing the non-collinear triple M_1, M_2, M_3 . then H also lies on this circle.

To show this, let the center of the circle O be at (x_7, x_8) . By applying the above section 2.3.3, we have two additional hypotheses,

$$M_1 O = M_2 O \text{ implies } h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \tag{3}$$

$$M_1 O = M_3 O \text{ implies } h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0$$

Now, our conclusion (we want to show) is $HO = M_1 O$, which takes the form

$$g = (x_5 - x_7)^2 + (x_6 - x_8)^2 - (x_1 - x_7)^2 - x_8^2 = 0 \quad (4)$$

Now what we want to show is that g vanishes whenever h_1, \dots, h_8 do.

Our hypotheses are the eight polynomials h_i from (1)-(3).

Let $I = \langle h_1, \dots, h_8 \rangle$, computing a Groebner basis G (using *lex order*) for the ideal I , which yields:

$$G = \{f_1, f_2, \dots, f_8\}, \text{ where}$$

$$f_1 = x_1 - u_1/2,$$

$$f_2 = x_2 - u_2/2,$$

$$f_3 = x_3 - u_1/2,$$

$$f_4 = x_4 - u_2/2,$$

$$f_5 = x_5 - \frac{u_1 u_2^2}{u_1^2 + u_2^2},$$

$$f_6 = x_6 - \frac{u_1 u_2^2}{u_1^2 + u_2^2},$$

$$f_7 = x_7 - u_1/4,$$

$$f_8 = x_8 - u_1/4,$$

The conclusion (equation 4) reduces to zero on division by this Groebner basis. That is,

$$\overline{g}^G = 0$$

Thus by Corollary 1.5.2 $g \in I = \langle h_1, \dots, h_8 \rangle$, which shows that g follows generically from h_1, \dots, h_8 . ■

Note that we must have either $u_1 \neq 0$ or $u_2 \neq 0$ in order to solve for x_5 and x_6 . The equation $u_1 = 0$ and $u_2 = 0$ describe degenerate "right triangles" in which the three vertices are not distinct, so we certainly wish to rule these cases out. It is interesting to note, however, that if either u_1 or u_2 is nonzero, the conclusion is still true. For instance, if $u_1 \neq 0$ but $u_2 = 0$, then the vertices C and A coincide. From (1) and (2), the midpoints M_1 and M_3 coincide, M_2 coincides with A , and H coincides with A as well. As a result, there is a circle (infinitely many of them in fact) containing M_1, M_2, M_3 , and H in this degenerate case.

2.4.2. Pappus Theorem

Theorem 2.4.2 Let A, B, C and A', B', C' be two sets of collinear points. And $P = \overline{AB'} \cap \overline{A'B}$, $Q = \overline{AC'} \cap \overline{A'C}$, and $R = \overline{BC'} \cap \overline{B'C}$. Then the points P, Q and R are collinear. (As shown in the figure below)

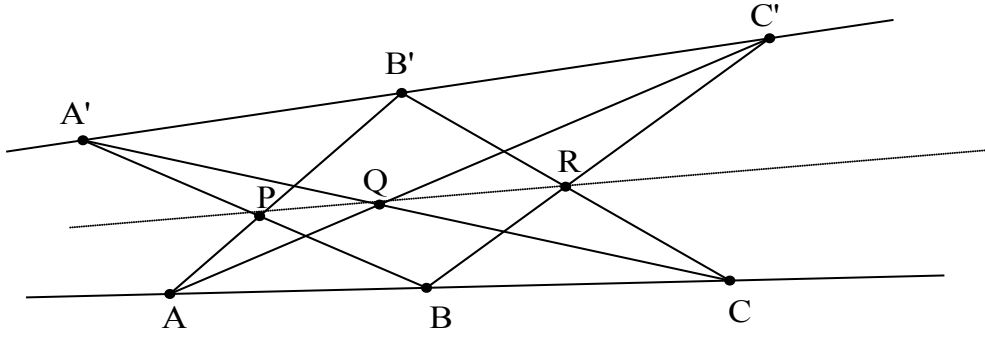


Figure 2.7: Pappus Theorem

Proof To make the translation easier, let the coordinates of the points be as follows:

$A = (0,0)$, $B = (u_1, 0)$, $C = (u_2, 0)$, $A' = (u_3, u_4)$, $B' = (u_5, u_6)$, $C' = (u_7, x_1)$,
 $P = (x_2, x_3)$, $Q = (x_4, x_5)$, $R = (x_6, x_7)$. Point C' is partially dependant on our choices of A, B, A', B' , so one of its coordinate is x_1 .

We translate the hypotheses of the theorem as follows;

Since the points A', B' , and C' are collinear, then using the slope formula, we have

$$\text{Slope of } \overline{A'B'} = \text{Slope of } \overline{A'C'}$$

$$\text{This implies, } \frac{u_6 - u_4}{u_5 - u_3} = \frac{x_1 - u_4}{u_7 - u_3}$$

$$(u_6 - u_4)(u_7 - u_3) = (x_1 - u_4)(u_7 - u_3)$$

$$h_1 = (u_6 - u_4)(u_7 - u_3) - (x_1 - u_4)(u_7 - u_3) = 0$$

The points A, P and B' are collinear, so using the slope formula, we have

$$\text{Slope of } \overline{AP} = \text{Slope of } \overline{AB'}$$

This implies, $\frac{x_3-0}{x_2-0} = \frac{u_6-0}{u_5-0}$. That is, $\frac{x_3}{x_2} = \frac{u_6}{u_5}$

$$x_3u_5 = u_6x_2$$

$$h_2 = x_3u_5 - u_6x_2 = 0$$

The points B, P and A' are collinear, so using the slope formula, we find

$$\text{Slope of } \overline{BA'} = \text{Slope of } \overline{BP}$$

This implies, $\frac{u_4-0}{u_3-u_1} = \frac{x_3-0}{x_2-u_1}$.

$$u_4(x_2 - u_1) = x_3(u_3 - u_1)$$

$$h_3 = u_4(x_2 - u_1) - x_3(u_3 - u_1) = 0$$

The points A, Q and C' are collinear, so using the slope formula, we have

$$\text{Slope of } \overline{AQ} = \text{Slope of } \overline{AC'}$$

This implies, $\frac{x_5-0}{x_4-0} = \frac{x_1-0}{u_7-0}$. That is, $\frac{x_5}{x_4} = \frac{x_1}{u_7}$.

$$x_5u_7 = x_1x_4$$

$$h_4 = x_5u_7 - x_1x_4 = 0$$

The points C, Q and A' are collinear, and using the slope formula, we find

$$\text{Slope of } \overline{CQ} = \text{Slope of } \overline{CA'}$$

This implies, $\frac{x_5-0}{x_4-u_2} = \frac{u_4-0}{u_3-u_2}$.

$$x_5(u_3 - u_2) = u_4(x_4 - u_2)$$

$$h_5 = x_5(u_3 - u_2) - u_4(x_4 - u_2) = 0$$

The points B, R and C' are collinear, and using the slope formula, we find

$$\text{Slope of } \overline{BR} = \text{Slope of } \overline{BC'}$$

$$\text{This implies, } \frac{x_7-0}{x_6-u_1} = \frac{x_1-0}{u_7-u_1}.$$

$$x_7(u_7 - u_1) = x_1(x_6 - u_1)$$

$$h_6 = x_7(u_7 - u_1) - x_1(x_6 - u_1) = 0$$

The points C, R and B' are collinear, and using the slope formula, we find

$$\text{Slope of } \overline{CR} = \text{Slope of } \overline{CB'}$$

$$\text{This implies, } \frac{x_7-0}{x_6-u_2} = \frac{u_6-0}{u_5-u_2}.$$

$$x_7(u_5 - u_2) = u_6(x_6 - u_2)$$

$$h_7 = x_7(u_5 - u_2) - u_6(x_6 - u_2) = 0$$

Now, our conclusion is that the points P, Q and R are collinear. So that using the slope formula, we have

$$\text{Slope of } \overline{PQ} = \text{Slope of } \overline{PR}$$

$$\text{This implies, } \frac{x_5-x_3}{x_4-x_2} = \frac{x_7-x_3}{x_6-x_2}$$

$$(x_5 - x_3)(x_6 - x_2) = (x_7 - x_3)(x_4 - x_2)$$

$$g = (x_5 - x_3)(x_6 - x_2) - (x_7 - x_3)(x_4 - x_2) = 0$$

Now, we want to show g is deduced from h_1, \dots, h_7 algebraically or we want g to vanish whenever h_1, \dots, h_7 do.

For the ideal $I = \langle h_1, \dots, h_7 \rangle$, computing a Groebner basis G of the ideal I gives us:

$$G = \{f_1, f_2, \dots, f_6\},$$

where $f_1 = x_5u_7 - x_1x_4$

$$f_2 = (x_1 - x_7)u_1 + x_7u_7 - x_1x_6$$

$$f_3 = (x_1x_3 - x_3x_7)u_3 - x_7u_4u_7 + (-x_1x_2 + x_1x_6 + x_2x_7)u_4 + x_3x_7u_7 - x_1x_3x_6$$

$$f_4 = (-x_1x_2x_5 + x_1x_3x_4 - x_1x_4x_7 + x_1x_5x_6 + x_2x_5x_7 - x_3x_4x_7)u_4 + x_1x_3x_5 - x_3x_5x_7$$

$$f_5 = (-x_1x_2x_5 + x_1x_3x_4 + x_2x_5x_7 - x_3x_5x_6)u_6^2 - x_3x_5x_7u_6u_7 + x_1x_3x_5x_6u_6$$

$$f_6 = x_1x_2x_5^2 - x_1x_2x_5x_7 - x_1x_3x_4x_5 + x_1x_3x_5x_6 + x_1x_4x_5x_7 - x_1x_5^2x_6 - x_2x_5^2.$$

But division of the conclusion g by the Groebner basis G gives

$$\bar{g}^G = -x_2x_5 + x_2x_7 + x_3x_4 - x_3x_6 - x_4x_7 + x_5x_6$$

This does not tell us whether g is in I or not.

Let $g_2 = 1 - yg$ and let $\tilde{I} = \langle h_1, \dots, h_7, g_2 \rangle$, then computing the Groebner basis for \tilde{I} gives us 1.

Then, by the above Remark 2.2.4 this implies $g \in \sqrt{\langle h_1, \dots, h_7 \rangle}$

Hence g holds whenever h_1, \dots, h_7 holds ■

References

1. David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms an introduction to computational algebraic geometry and commutative algebra. Undergraduate texts in mathematics.* Springer-Verlag, New York-Berlin-Paris, 1992.
2. David Cox, John Little, Donal O'Shea. *Ideals, Varieties, and Algorithms*, 2nd Edition, Springer-Verlag, New York, NY, 1997.
3. David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, University of California, 2004
4. Samuel Nartey, *Automatic Geometric Theorem Proving*, African Institute for Mathematical Sciences (AIMS), University of Stellenbosch, 2007
5. T.W. Hungerford, *Algebra*, Springer-Verlag, 1978.