
አዲስ አበባ ዩኒቨርሲቲ
Addis Ababa University

ADDIS ABABA UNIVRSITY

DEPARTMENT OF

MATHEMATICS

The undersigned here by certifies that they have read this manuscript and recommends to the school of Graduate studies its acceptance ,the title of the project is Automatic Geometric Theorem Proving by Hiwot Lemma in the requirements for the degree of master of science.

Dated : Aug 2016

Advisor : _____

Dr. Tilahun Abebaw

Examiner : _____

Dr.Berhanu Bekele

_____

Dr.Yibeltal Y.

TABLE OF CONTENT

ACKNOWLEDGMENT

First of all I would like to thank the Almighty GOD for his endless grace in my life .

Also I would like to express to deep gratitude and appreciation to my advisor Dr. Tilahun Abebaw for his support in providing valuable materials , suggestion and comments to this thesis and his intellectual encouragement as a whole. Additionally I would like to thank my family.

NOTATION

K	Field
K^n	n dimentional affine space
$K[x_n,\ldots,x_n]$	Set of polynomials n variabls with the cofficents from field K
$f(x_1,..,x_n)$	A polynomial with n variables
V(f_1 , . . . , f_n)	Affine Varities define by f_1, ... f_n
$I(V)$	An Ideal of V
$< f_1, \ldots, f_n >$	An ideal generated by f_1 , . . . ,f_n
$\bar{g}^G$	Polynomial g divided by the Groebner bases G
$\mathbb{Z}^n_{\geq 0}$	n – tuples of integer and each entry is greater or equal to zero
$\mathbb{R}$	Set of Real number
$\perp$	Perpendicular
C	Strict inclusion
$\in$	Element
■	End of the proof

ABSTRACT

For several decades algebraic method have been successfully used in automated deduction in Geometry objects in Euclidean geometry are relations between them are expressed as polynomials and algebraic method e.g.Groebner bases are used over that set of polynomials we describe aformalization of an algorithm that accepts a term representation of a geometry construction and returns a corresponding set of polynomials our furtherwork will be to use the method of Groebner bases on the generated polynomials , in order to implement a formallyverified algebraic prover for geometry .

CHAPTER ONE

INTRRODUCTION

Algebraic geometry is the study of systems of polynomial equations in one or more variables.The solutions of a system of polynomial equations from a geometric object (points , lines , curves , surfaces) called a variety;the corresponding algebraic object is an ideal.There is a close relationship between ideals and variety which reveals the intimate link between algebra and geometry.

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.

First, we will discuss some concepts from algebraic geometry and commutative algebra such as varieties, ideals and Groebner bases. Then , 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 into polynomial equations. We will apply the Groebner basis method.

Groebner besis were first discover by Bruno Buchberger in 1965, who named them after his superviser Wolfgang Groebner.They have been applied successfully in algebraic geometry and commutative algebra. The method we employed translates geometric statements in to algebraic statements.

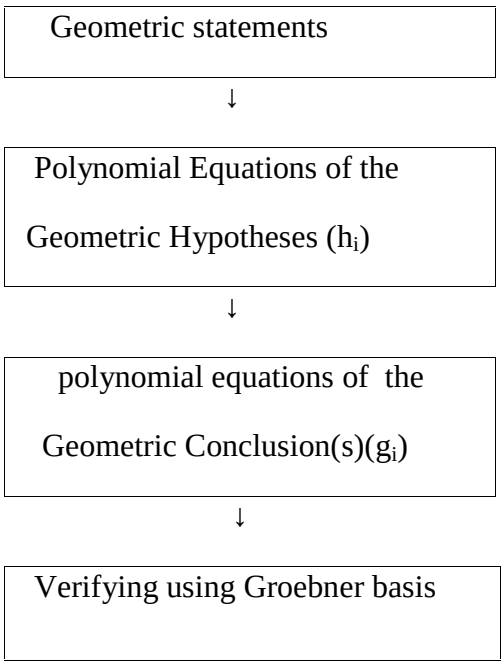
A systematic overview of approaches to Automatic Geometric Theorem Proving is as follows

1 . Algebraic Formulation

The translation of a geometric statement into algebraic equations.

2 . Proof

The use of some decision procedures , in the model we are working with,to determine the validity of the theorem.



This thesis is organized around these items.

CHAPTER TWO

PRELIMINARIES

In this chapter we will introduce some of the basic concepts which can be used for an implementation of this thesis, that is , to prove generally the Automatic geometric theorem .

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

Our aim is to prove a geometric theorem algebraically by applying the above mentioned concepts. We will change the geometric statements into polynomial equations by using the concepts of slope of lines and distance formula.

First we begin with some basic concepts.From the many references that we have used for this work , we took most of the preliminary parts from [1]

2.1. Polynomials and Affine Varieties

Definition 2.1.1 A **monomial** in the variables $x_1, x_2, \dots, x_n$ 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 $\alpha_1 + \alpha_2 + \cdots + \alpha_n$

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

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

Definition 2.1.2 A **polynomial** f in $x_1, x_2, \ldots, x_n$ with coefficients in a field k is a finite linear combination of monomials. We write a polynomial f in the form

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

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

Example 2.1.3 $f = \sqrt{2}x^2yz^3 + {}^3/_4 xy^2 + 3xyz - z^4$ is a polynomial in $\mathbb{R}[x, y, z]$

Definition 2.1.4 Given a field k and a positive integer n, we define the n-dimensional affine space over k to be the set

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

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 $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ gives a function $f: k^n \to k$, define for a given $(a_1, \ldots, a_n) \in k^n$, 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 $f(a_1, \ldots, a_n) \in k$. This enables us to link algebra and geometry.

Definition 2.1.5 Let k be a field, and let $f_1, f_2, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$, then we set $V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n: f_i(a_1, \ldots, a_n) = 0 \text{ for all } 1 \leq i \leq s\}$.

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

$f_1(x_1, \dots, x_n) = \cdots = f_s(x_1, \dots, x_n) = 0$

Examples 2.1.6

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. hyperbolas) are affine varieties.
iii. Graphs of polynomial functions are affine varieties. In this case the graph of a polynomial $y = f(x)$ is given by $V(y - f(x))$ as a variety.

2.2. Ideals

In this section we will discuss on the ideals of the polynomial ring $k[x_1, \dots, x_n]$ in n variables .

Definition 2.2.1 A subset $I \subset k[x_1, \dots, x_n]$ is said to be an **ideal of** $K[x_1, \dots, x_n]$ if it satisfies the following .

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 to see how ideals are related with affine varieties .The real importance of ideals is to give us a language for computions in affine varieties

Lamma 2.2.2 Let $f_1, \dots, f_s$ be polynomials in $k[x_1, \dots, x_n]$. Then we set

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

$\langle f_1, \dots, f_s \rangle$ is an ideal of $k[x_1, \dots, x_n]$ and it is called $\langle f_1, \dots, f_s \rangle$ 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

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

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

Lemma 2.2.3 *Let $V \subset k^n$ be an affine variety.* We set

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

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

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

Hence $I(V)$ is an ideal of V.

■

2.3. Monomial ordering and monomial ideals

Definition 2.3.1 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 $Z_{\geq 0}^n$ 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 $\gamma \in Z_{\geq 0}^n$, then $\alpha + \gamma > \beta + \gamma$.

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

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

Definition 2.3.2 (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.

For monomials x^α *and* x^β

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

Example 2.3.3

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 ordering.

Definition 2.3.4 (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 2.3.5

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 2.3.6 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 $multideg(f) = max(\alpha \in \mathbb{Z}_{\geq 0}^n : a_\alpha \neq 0)$, the maximum is taken with respect to $>$.

ii. The leading coefficient of f is $LC(f) = a_{multideg(f)} \in k$

iii. The leading monomial of f is $LM(f) = x^{multideg(f)}$ (With coefficient *1*)

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

Example 2.3.7 Let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$ and let $>$ denote the *lex order*. Then, $multideg(f) = (3,0,0)$

$$LC(f) = -5$$

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

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

Lemma 2.3.8 Let $f, g \in k[x_1, \dots, x_n]$ be non-zero polynomials. Then

i. $multideg(fg) = multideg(f) + multideg(g)$

ii. If $f + g \neq 0$, *then* $multideg(f + g) \leq max(multideg(f) + multieg(g))$. If in addition, $multideg(f) \neq multideg(g)$, then equality occurs.

***Proof**: See* [1]

Definition 2.3.9 An ideal $I \subset k[x_1, ..., x_n]$ 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 $h_\alpha \in k[x_1, .., x_n]$. In this case, we write $I = \langle x^\alpha : \alpha \in A \rangle$

Lemma 2.3.10 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 $h_i \in k[x_1, .., x_n]$ 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 2.3.11 (***Division Algorithm in*** $k[x_1, ..., x_n]$)

Fix a monomial order > on $\mathbb{Z}_{\geq 0}^n$, and let $F = (f_1, ..., f_n)$ be an ordered s-tuple of polynomials in $k[x_1, .., x_n]$. Then every $f \in k[x_1, ..., x_n]$ can be written as

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

where $a_i, r \in k[x_1, .., x_n]$ and either $r = 0$ or r is a linear combination ,with coefficient in k,

of monomials, none of which is divisible by any of $LT(f_1), LT(f_2), ..., LT(f_s)$.

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

$$multideg(f) \geq multideg(a_i f_i)$$

Proof : *See* [1]

Example 2.3.12. Let us divide $f = x^2y + xy^2 + y^2$ by $f_1 = y^2 - 1$ and $f_2 = xy - 1$. Use *lex order* with $x > y$. Then,

$$a_1 = x + 1$$

$$a_2 = x$$

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

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

2.4. The Hilbert Basis Theorem and Groebner Bases of Ideals

Definition 2.4.1 Let $I \subset k[x_1, \ldots, x_n]$ be a non zero ideal of $k[x_1, \ldots, x_n]$

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

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

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

Let $= \langle f_1, \ldots, f_s \rangle$. Then $\langle LT(f_1), LT(f_2), \ldots, LT(f_s) \rangle$ 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

$\langle LT(f_1), LT(f_2), \ldots, LT(f_s)\rangle \subset \langle LT(I)\rangle$. 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 2.3.10, x^2 is not an element of $< LT(f_1), LT(f_2) >$.

Proposition 2.4.2 Let $I \subset k[x_1, \ldots, x_n]$ be an ideal.

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

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

Theorem 2.4.3. (Hilbert basis theorem):

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

Proof See [1]

Definition 2.4.4 Fix a monomial order. A finite subset $G = \{g_1, \ldots, g_t\}$ of an ideal I is said to be a Groebner basis (or standard basis) if

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

Equivalently, but more informally, a set $\{g_1, \ldots, g_t\} \subset I$ is a Groebner basis of I if and only if the leading term of any element of I is divisible by one of the $LT(g_i)$ $i = 1, 2 \ldots s$.

Corollary 2.4.5 Fix a monomial order. Then every ideal $I \subset k[x_1, \ldots, x_n]$ other than $\{0\}$ has a Groebner basis. Furthermore any Groebner basis for an ideal I is a basis of I.

Proof See [1]

Definition 2.4.6 Let $I \subset k[x_1, \dots, x_n]$ be an ideal. We will denote by $V(I)$ the set

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

Remark 2.4.7 If $I = \langle f_1, \dots, f_s \rangle$, then $V(I) = V(f_1, \dots, f_s)$

2.5 Some Properties of Groebner bases

Proposition 2.5.1 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 2.5.2 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 2.5.3 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.

Example 2.5.4 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,

$x^5y = (x^3 + xy)(x^2y - y^2) + 0.(x^4y^2 - y^2) + xy^3$ and no term of $x\,y^3$,which is xy^3 in this case ,is divisible by LT $(x^2y - y^2)$ and LT ($x^4y^2 - y^2$).

Definition 2.5.5 Let $f, g \in k[x_1, \dots, x_n]$ be non zero polynomials

a. If $multideg(f) = \alpha$, $multideg(g) = \beta$, 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)

Exampie 2.5.6 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 $\gamma = (4,2)$ and $S(f,g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g = x.f - (1/3) \cdot y \cdot g = -x^3y^3 + x^2 - (1/3)y^3$

Observe that on *S*- polynomial $S(f,g)$ of is "designed" to produce cancellation of leading terms.

Lemma 2.5.7 Suppose we have a sum $\sum_{i=}^{s} c_i f_i$, where $c_i \in k$ and $multideg(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$, for all i. If $multideg(\sum_{i=}^{s} c_i f_i) < \delta$. Then $\sum_{i=}^{s} c_i f_i$ 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 ***See*** [1]

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

***Theorem* 2.5.8** 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 See [1]

2.6. 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 we can construct a Groebner basis for I. let's see this by the following example

***Example* 2.6.1** 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

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

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

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

$S(f_2,f_3) = (x^2y-2y^2+x)-(-y)(-x^2) = -2y^2+x$, 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

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

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

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

Output: a Groebner basis $G = \langle g_1, \ldots, g_t\rangle$ 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 2.6.3 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 for I. ■

Definition 2.6.4 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 2.6.3 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 2.6.1. 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 2.6.3, 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, $\widetilde{f_3} = x^2$, $\widetilde{f_4} = xy$, $\widetilde{f_5} = y^2 - (1/2)x$ is a minimal Groebner basis for I.

Unfortunately, a given ideal may have many minimal Groebner bases. For example, in the ideal I considered above $\widetilde{f_3} = x^2 + axy$, $\widetilde{f_4} = xy$, $\widetilde{f_5} = y^2 - (1/2)x$ is also a minimal Groebner basis, where $a \in k$ is any constant.

Definition 2.6.5 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.

2.7. Some 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 us see this by giving an example

Example 2.7.1 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 2.4.7, 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 into 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.

2.8. Hilbert's Nullstellensatz theorem and radical ideals

Given a variety $V \subset K^n$, Recall that $I(V) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \text{ for all } x \in V\}$ the set of all polynomials vanishing on V. And for ideal $I \subset k[x_1, \ldots, x_n]$, 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 $f_1, \ldots, f_s \in I$ such that $I = \langle f_1, \ldots, f_s \rangle$ and in Remark 1.4.7, we have seen that $V(I)$ is the set of common roots of these polynomials.

Theorem 2.8.1 **(Hilbert's Nullstellensatz)**

Let k be an algebraically closed field. If $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ such that

$f \in I(V(f_1, \ldots, f_s))$, then there exists an integer $m \geq 1$ such that

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

Proof See [1]

Lemma 2.8.2 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 $\big(f(x)\big)^m$

This implies $f(x) = 0$

Hence, $f \in I(V)$ ■

Definition 2.8.3 An ideal I is radical, if $f^m \in I$ for some integer $m \geq 1$, then $f \in I$.

By Lemma 2.8.2, $I(V)$ is a radical

Definition 2.8.4 Let $I \subset k[x_1, \ldots, x_n]$ be an ideal. Then **radical** of I, denoted $\sqrt{I}$, is the set

$$\{f \in K[x_1, \ldots, x_n] : f^m \in I \text{ for some integer } m \geq 1\}$$

Remark 2.8.5

i. The ideal $I \subset \sqrt{I}$, since $f \in I \Rightarrow f^1 \in I$ and hence $f \in \sqrt{I}$.

ii. If I is an ideal in $k[x_1, \ldots, x_n]$, then $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$

iii. The radical of an ideal is an ideal.

Theorem 2.8.6 **(The Strong Nullstellensatz Theorem)**

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

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

Proof If $f \in \sqrt{I}$, then $f^m \in I$, for some $m \geq 1$ and f^m Vanishes on V(I).

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

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.

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

■

Proposition 2.8.7 (Radical Ideal Membership) Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$ be an ideal of $K[x_1, \ldots, x_n]$. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal

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

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

Proof See **[1]**

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

Example 2.8.8. 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 THREE

GEOMETRIC THEOREMS PROVING USING GROEBNER BASIS

3.1. 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 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 $g_i = f_1 h_1 + \cdots + f_n h_n$, for some $f_1, \ldots, f_n$.

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.

3.2. 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 3.2.1 A geometric theorem is said to be *admissible* if both its hypotheses and its conclusions admit translation into polynomial equations.

Let $u_1, \ldots, u_m$ be the independent variable and $x_1, \ldots, x_n$ 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. So we will write thehypotheses as

$$h_1(u_1, \ldots, u_m, x_1, \ldots, x_n) = 0$$

$$\vdots$$

$$h_n(u_1, \ldots, u_m, x_1, \ldots, x_n) = 0$$

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 defined by $h_1, h_2, \ldots, h_n$ be

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

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

Let the variety be

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

and, let the ideal be

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

Definition 3.2.2 The conclusion g follows strictly from the hypotheses $h_1, \ldots, h_n$ if $g \in I(V) \subset k[u_1, \ldots, u_m, x_1, \ldots, x_n]$ where $V = V(h_1, \ldots, h_n)$.

Proposition3.2.3 If $g \in \sqrt{\langle h_1, \ldots, h_n \rangle} = \{f \in k[u_1, \ldots, u_m, x_1, \ldots, x_n] : f^s \in < h_1, \ldots, h_n >$ for some $s\}$, then g follows strictly from $h_1, \ldots, h_n$.

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

Now for each $\in V$,

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

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

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

Remark 3.2.4 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 $\mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n, y]$. Then the radical membership proposition implies that

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

Proposition 3.2.5 The conclusion g follows generically from $h_1, \dots h_n$ if there exists a nonzero polynomial $c(u_1, \dots, u_n) \in K[u_1, \dots, u_m]$ such that

$$cg \in \sqrt{I}$$

where $I = \langle h_1, \dots, h_n \rangle$ and $h_i \in K[u_1, \dots, u_m, x_1, \dots, x_n]$.

Proof see [1]

Corollary 3.2.6 In the situation of above proposition the following are equivalent:

i) There is a nonzero polynomial $c \in \mathbb{R}[u_1, \dots, u_m]$ such that $cg \in \sqrt{I}$.
ii) $g \in \sqrt{I}$, where $I = \langle h_1, \dots, h_n \rangle \in R[u_1, \dots, u_m, x_1, \dots, x_n, y]$.
iii) $\{1\}$ is the reduced Groebner basis of the ideal $\langle h_1, \dots, h_n, 1 - yg \rangle \subset R[u_1, \dots, u_m, x_1, \dots, x_n, y]$

Proof See [1]

3.3. Translation of geometric statements into Polynomials

Our main objective in this chapter is to translate a given statement in geometry in the form of polynomial equations and prove then with ideal membership . First let us state some of the geometric statements that can be expressed by polynomial equations .This are given in the following proposition.

Proposition 3.3.1 let A, B, C, D, E, F be points in the plane. Each of the following geometric statements can be expressed by one or more polynomial equation .

is parall .
is perpen .

B is equa
with center A and r
is the midp of $\overline{AB}$.
ae acute an ABC is equal to the acut DEF.
bisects th ABC

can be transl nto polynom A, B, C, D
$\overline{AB}$ be parall $\overline{CD}$ as showr

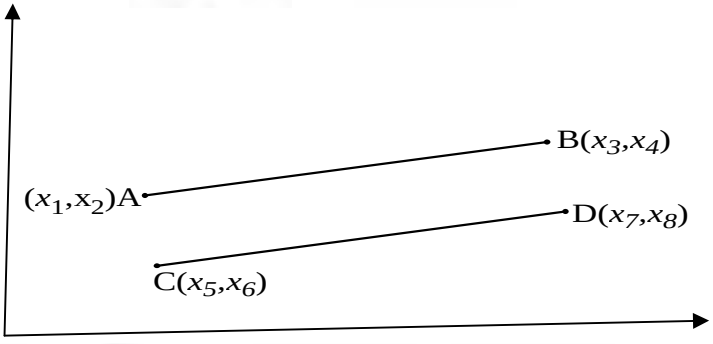


Figure 2.1: pa allel lines

$\overline{AB}$ is paralle $\overline{CD}$, Slope of $\overline{AB}$ = Slope $\overline{CD}$

$$\frac{x_4-x_2}{x_3-x_1}=\frac{x_8-x_6}{x_7-x_5}$$

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.

3.3.3 Perpendicular lines

Suppose $\overline{AB}$ *and* $\overline{CD}$ be two nonhorizontal and nonvertical linesegments. $\overline{AB}$ is perpendicular to $\overline{CD}$ as in the figure below

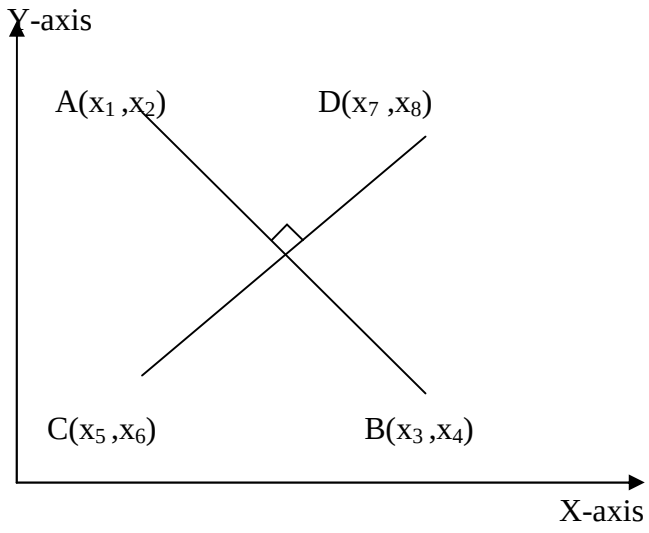


Figure 2.2: perpendicular lines

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

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

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

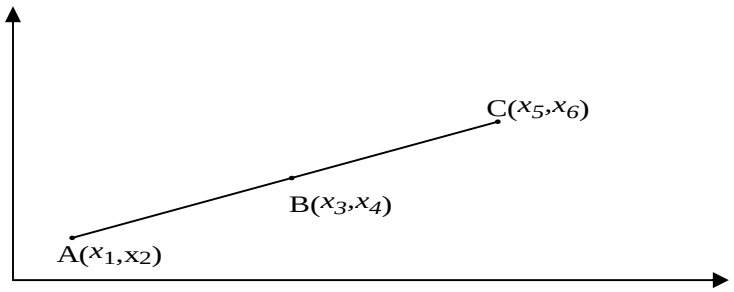
$$x_4-x_2)(x_8-x_6) = \quad x_3-x_1)(x_7-x_5)]$$

g distributive property and collecting to the left gives,

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

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

A, B, C be co



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

$$\frac{x_4-x_2}{x_3-x_1} = \frac{x_6-x_2}{x_5-x_1}$$

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

ıg and collect ıg to the eft si e gives

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

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

C lies o A and AB as showr

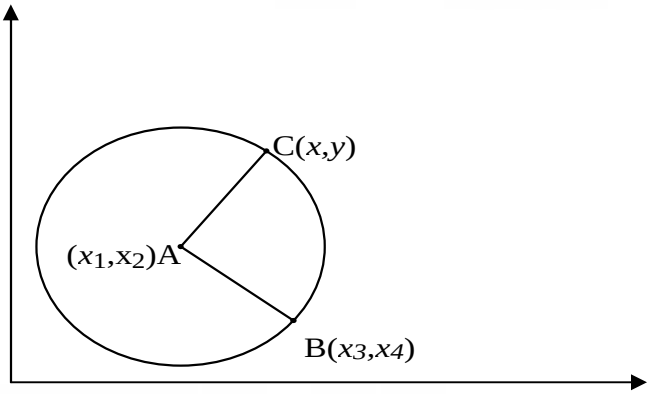


Figure 2.4: C cle

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

C lies o rcle, then $AC = AB$.

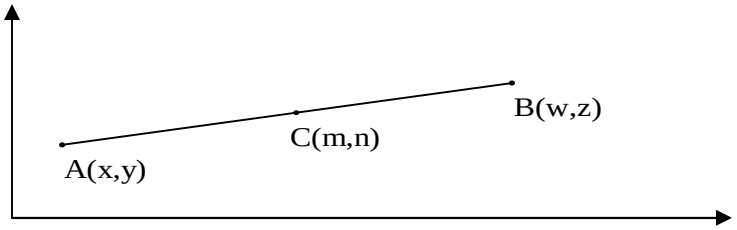
$$\sqrt{(x - x_1)^2 + \ \overline{y - x_2)^2} = \sqrt{(x_3 - x_1)^2 + (x_4 - x_2)^2}$$

ides gives $x - x_1)^2 + y - x_2)^2 = x_3 - x_1)^2 + x_4 - x_2)^2$

nplies $(x - x_1)^2 + (y - x_2)^2 - (x_3 - x_1)^2 - (x_4 - x_2)^2 =$

$$x - x_1)^2 + y - x_2)^2 - x_3 - x_1)^2 - x_4 - x_2)^2 =$$

C be the $\overline{AB}$ as in the



re 2.5: midpoint

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

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

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

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

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

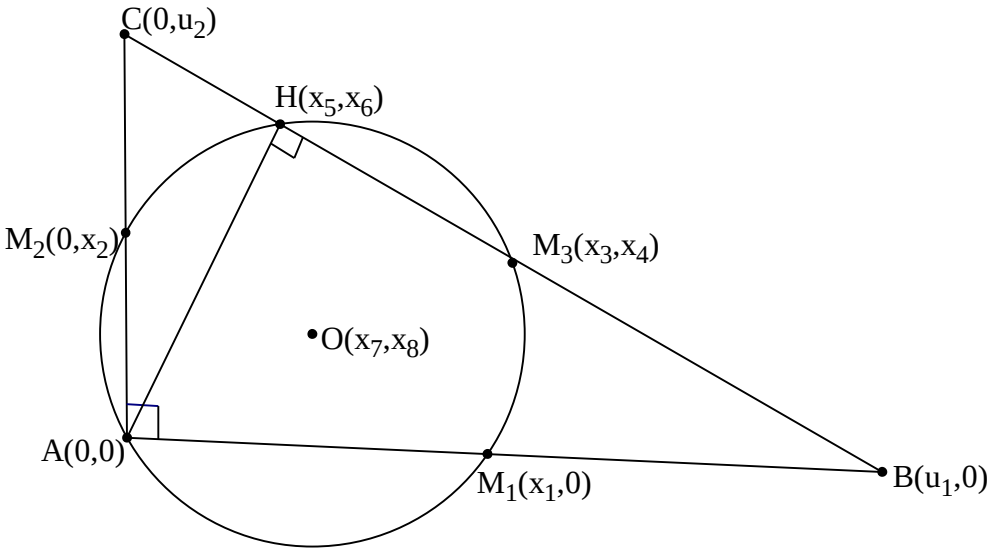
seen t at, we ca trans sys is

ing $k[u_1, .. u_m, x_1, .. x_n]$. 1, . . n

1, .

ABC be right triang th rigl A. Th

A to $\overline{BC}$



n is ac , we b / con

A at ( )) an B at $(u_1,0)$ $u_1 \neq$ CAB is a right ang

$C=(0,u_2)$ $u_2 \neq$

$M_1=(x_1,0),\ M_2=(0,x_2)$ *and* $M_3=(x_3,x_4)$ u_i's

as the x_i's e de... u_i's

$M_1, M_2,$; M_3 a

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

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:

$$AH \perp BC \text{ implies } h_5 = x_5u_1 - x_6u_2 = 0 \qquad (2)$$

$$B, H, C \text{ are collinear implies } h_6 = x_5u_2 + x_6u_1 - u_1u_2 = 0$$

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 2.2.3, we have two additional hypotheses,

$$\begin{aligned} &M_1O = M_2O \text{ implies } h_7 = (x_1 - x_7)^2 + x_8^2 - x_7^2 - (x_8 - x_2)^2 = 0 \\ &M_1O = M_3O \text{ implies } h_8 = (x_1 - x_7)^2 + x_8^2 - (x_3 - x_7)^2 - (x_4 - x_8)^2 = 0 \end{aligned} \qquad (3)$$

Now, our conclusion (we want to show) is $HO = M_1O$, which takes the form

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

Now what we want to show is that g *vanishes whenever* $h_1, \ldots, h_8$ *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: $G = \{f_1, f_2 \dots, f_8\}$, where

$$f_1 = x_1 - {}^{u_1}/_{2}$$

$$f_2 = x_2 - {}^{u_2}/_{2}$$

$$f_3 = x_3 - {}^{u_1}/_{2}$$

$$f_4 = x_4 - {}^{u_2}/_{2}$$

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

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

$$f_7 = x_7 - {}^{u_1}/_{4}$$

$$f_8 = x_8 - {}^{u_2}/_{4}$$

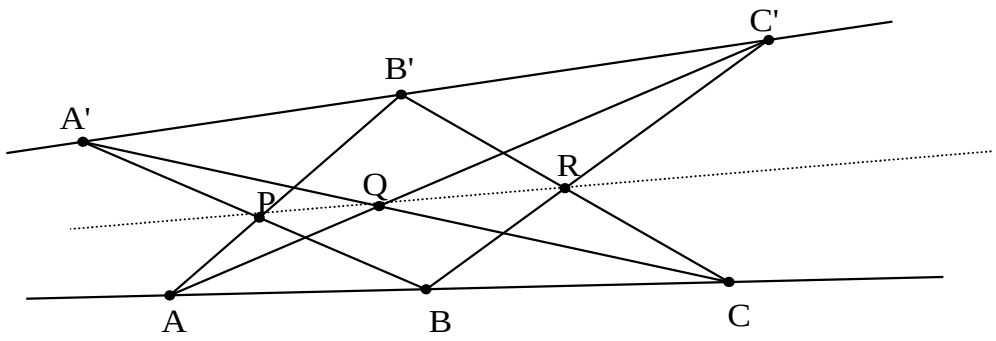
The conclusion (equation 4) reduces to zero on division by this Groebner basis. That is,

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

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. ■

Theorem 2.4.2 Let A, B, C and A', B', C' be tw ear poi s. An $P = \overline{AB'} \cap$ $\overline{A'B}$,$Q = \overline{AC'} \cap \overline{A'C}$, and $R = \overline{BC'} \cap \overline{B'C}$. Tl P, Q an R ar



Proof To make the transla easier, let the ordinates of th oints be as follows:$A = (0,0)$, $B = (u_1, 0)$, $C = (u_2, 0)$ $A' = (u_3, u_4)$ $B' = (u_5, u_6)$ $C' = (u_7, x_1)$, $P = (x_2, x_3)$ $Q = (x_4, x_5), R = (x_6, x_7)$. C' is pa $A, B\ A', B'$, so is x_1. We translate

$A', B',$ and C' are c , then usin

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

impli s, $\frac{u_6 - u_4}{u_5 - u_3} = \frac{x_1 - u_4}{u_7 - u_3}$

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

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

A, P an B' are

Slope of $\overline{AP}$ = 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

Slope of $\overline{BA'}$ = 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

Slope of $\overline{AQ}$ = 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

Slope of $\overline{CQ}$ = 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

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

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

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

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

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

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

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

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

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 is that g to vanishes whenever $h_1, \ldots, h_7$ do or g in the radical I = $(h_1, \ldots, h_7)$.

For the ideal I = $< h_1, \ldots, h_7 >$,computing a Groebner basis G of the ideal I gives us:

G = $\{ f_1, \ldots, f_6 \}$, where

$$f_1 = x_5 u_7 - x_1 x_4$$

$$f_2 = (x_1 - x_7)u_1 + x_7 u_7 - x_1 x_6$$

$$f_3 = (x_1 x_3 - x_3 x_7)u_3 - x_7 u_4 u_7 + (-x_1 x_2 + x_1 x_6 + x_2 x_7)u_4 + x_3 x_7 u_7 - x_1 x_3 x_6$$

$$f_4 = (-x_1 x_2 x_5 + x_1 x_3 x_4 - x_1 x_4 x_7 + x_1 x_5 x_6 + x_2 x_5 x_7 - x_3 x_4 x_7)u_4 + x_1 x_3 x_5 - x_3 x_5 x_7$$

$$f_5 = (-x_1 x_2 x_5 + x_1 x_3 x_4 + x_2 x_5 x_7 - x_3 x_5 x_6)u_6^2 - x_3 x_5 x_7 u_6 u_7 + x_1 x_3 x_5 x_6 u_6$$

$$f_6 = x_1 x_2 x_5^2 - x_1 x_2 x_5 x_7 - x_1 x_3 x_4 x_5 + x_1 x_3 x_5 x_6 + x_1 x_4 x_5 x_7 - x_1 x_5^2 x_6 - x_2 x_5^2$$

But using computer algebra system the division of the conclusion g by the Groebner basis G gives nonzero.

That is $\bar{g}^G \neq 0$

$$This\ impilies\ g \notin I$$

Let $g_2 = 1 - yg$ and let $\tilde{I} = < h_1, \ldots, h_7, g_2 >$ then computing the Groebner basis for $\tilde{I}$ the reduced Groebner basis {1}.

Then by the above Remark 2.2.4 this implies g $\in \sqrt{< h_1, \ldots, h_7 >}$

Hence g follows generically from the hypotheses . Hence g holds whenever

$h_1, \ldots, h_7$ hold.

■

3.4.3. Orthocenter theorem

The main result of our work is the following .We want to prove that the alttitudes of a given triangle are concurrent that is they pass through the same point.

Theorem 2.4.3. The altitudes of a triangle ΔABC all meet in a single point,H,called the orthocenter.

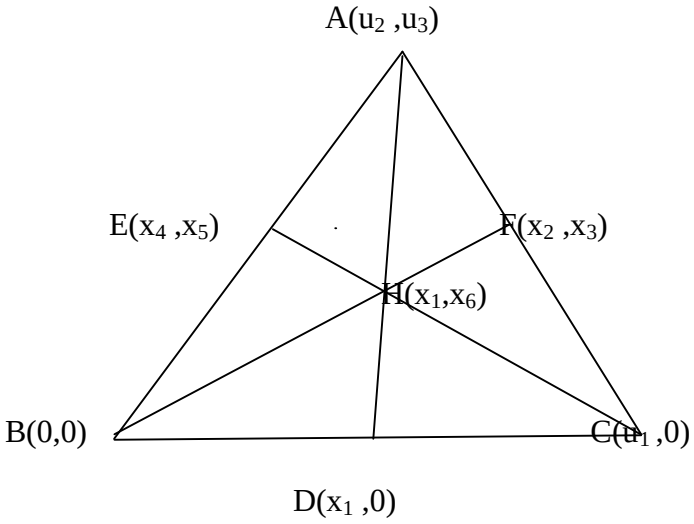


Figure 2.8:Orthocenter theorem

Proof First we construct the triangle in the coordinat plane by letting A=(u_2,u_3) B=(0,0) C=(u_1,0).

Next we construct the altitudes of ΔABC . Let $D = (x_1, 0)$, $E = (x_4, x_4)$ and $F = (x_2, x_3)$ be points such that $\overline{AD}$, $\overline{BF}$, $\overline{CE}$ are altitudes from A ,B , C respectively .Then we must have B ,D ,C ; B, E, A and C, F, A are collinear . Also, we must have $AD \perp BC$; $CE \perp AB$ and $BF \perp AC$. This yields the following hypotheses . Labling the polynomial as h_1, h_2, h_3, h_4, h_5

$$\begin{aligned} h_1 &= u_1(x_1 - u_2) = 0 \\ h_2 &= x_2(u_2 - u_1) + x_3u_3 = 0 \\ h_3 &= x_3(u_2 - u_1) - u_3(x_2 - u_1) = 0 \\ h_4 &= u_2(x_4 - u_1) + u_3x_5 = 0 \\ h_5 &= x_5u_2 - u_3x_4 = 0 \end{aligned} \qquad (1)$$

Now, we want to conclude that all three altitudes meet at a single point H . Hence we construct the point $H(x_1, x_6)$ shoud be the intersection of $\overline{AD}$, $\overline{BF}$, $\overline{CE}$. The additional hypotheses that C ,H ,E, are collinear yielding the following equations. Which we call h_6 .

$$h_6 = x_6(x_4 - u_1) - x_5(x_1 - u_1) = 0 \qquad (2)$$

Finally ,our conclusion becomes B ,H , F are collinear ,since all the three altitudes meet at H.

Hence,we get the equation call this polynomial g .

$$g = x_6x_2 - x_3x_1$$

Now what we want to show is that g vanishes whenever $h_1, \ldots, h_6$ do, or g is the in radical $(h_1, \ldots, h_6)$ our hypothesis are the six polynomials from (1) and (2).

Let $I = < h_1 , \dots , h_6 >$, computing a Groebner basis G for the ideal I ,with lex order which yields

$G = \{f_1 , \dots . f_{19}\}$, where

$f_1 = x_6 u_1 u_3^2 - u_1^2 u_2 u_3 + u_1 u_2^2 u_3$

$f_2 = x_5 u_2^2 + x_5 u_3^2 - u_1 u_2 u_3$

$f_3 = x_5 x_6 u_1 u_3 - x_5 u_1^2 u_2 - x_5 u_1 u_3^2 + u_1^2 u_2 u_3$

$f_4 = x_5 x_6 u_1 u_2 + x_5 u_1^2 u_2^2 - x_5 u_1 u_2 u_3 - x_6 u_1^2 u_3$

$f_5 = x_4 u_3 - x_5 u_2$

$f_6 = x_4 u_3 + x_5 u_3 - u_1 u_2$

$f_7 = x_4 x_6 u_1 + x_5 u_1^2 - x_5 u_1 u_2 - x_6 u_1^2$

$f_8 = x_3 u_1^2 - 2 x_3 u_1 u_2 + x_3 u_2^2 + x_3 u_3^2 - u_1^2 u_2 + u_1 u_2 u_3$

$f_9 = x_3 x_6 u_3^2 + x_3 x_6 u_3^4 - x_3 u_1 u_2^3 u_3 - x_3 u_1 u_2 u_3^3 + x_3 u_2^4 u_3 + x_3 u_2^2 u_3^3$

$f_{10} = x_3 x_6 u_1 u_2 u_3 - x_3 x_6 u_2^2 u_3 - x_3 x_6 u_3^3 + x_3 u_1 u_2 u_3^2 - u_1^2 u_2^2 u_3 + u_1 u_2^3 u_3$

$f_{11} = x_3 x_5 x_6 u_1 + x_3 x_5 u_1 u_2 - x_3 x_6 u_1 u_3 - x_5 u_1^2 u_2 - x_5 u_1 u_3^2 + u_1^2 u_2 u_3$

$f_{12} = x_3 x_4^2 u_1 + x_3 x_5^2 u_1 + 2 x_3 x_5 u_1 u_3 - 3 x_3 u_1 u_2^2 + 2 x_3 u_2^3 + 2 x_3 u_2 u_3^2 - x_5 u_1^2 u_2 - x_5 u_1 u_2^2 - u_1^2 u_2 u_3 + 2 u_1 u_2^2 u_3$

$f_{13} = x_2 u_3 + x_3 u_1 - x_3 u_2 - u_1 u_3$

$f_{14} = x_2 u_1 - x_2 u_2 - x_3 u_3$

$f_{15} = x_2 x_5 u_2 + x_3 x_4 u_1 + x_3 x_5 u_3 - x_3 u_1 u_2 - x_5 u_1 u_2$

$f_{16} = x_1 u_1 - u_1 u_2$

$f_{17} = x_1 x_5 - x_4 x_6 - x_1 u_1 + x_6 u_1$

$f_{18} = x_1 x_3 u_2^2 + x_1 x_3 u_3^2 - x_3 u_2^3 - x_3 u_2 u_3^2$

$f_{19} = x_1 x_2 u_2 + x_1 x_2 u_3 - x_2 u_2^2 - x_3 u_2 u_3$

But the division of the conclusion g by this Groebner basis is different from zero.

That is $\overline{g}^{G} \neq 0$

$Impilies \quad g \notin I$

This is due to so called degenerate case.For exampie , if A coincides with B , the coordinates of E are undefined . So $u_1 \neq 0$ and $u_3 \neq 0$.

In section 3 .2. 5 above we have use Groebner basis to automatically drive degenerate case.

Finally computing a Groebner basis for $< h_1 , \ldots , h_6 , 1 - ygu_1u_3 >$ the computition can be carried out completely over the field yielding the reduced Groebner basis {1} .

$$This\ impilies \quad g \in \sqrt{I}$$

So ,the conclusion of this Theorem g follows generically from the hypotheses $(h_1 , \ldots , h_6)$ That is g holds whenever $h_1 , \ldots , h_n$ hold.

This meams point H is an intersection point to all the three altitudes of ΔABC .

■

References

1. David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms an introduction to computational algebraic geometry and commutative algebra,2nd Edition, Undergraduate texts in mathematics.* Springer-Verlag, New York , NY, 1997.
2. David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer, University of California, 2004
3. Joran Elias , *Automatic Geometric Theorem Proving* , TMME ,vol.3,no.1,University of Montana 2006
4. KenMadlener BSC thesis, *Automatic Geometric Theorem Proving*, Radbound University, oct 7, 2008
5. Roozemond 2J008- Bachelor project, *Automatic Geometic Theorem Proving* ,Eindhoven University of Technology, *9th* July 2003.
6. Samuel Nartey, *Automatic Geometric Theorem Proving*, African Institute for Mathematical Sciences (AIMS), University of Stellenbosch, 2007
7. T.W. Hungerford, *Algebra*, Springer-Verlag, 1978

.