GROEBNER BASES
and
MECHANICAL GEOMETRY
THEOREM PROVING

THESIS

Presented to the Graduate Council of

Southwest Texas State University

in Partial Fulfillment of

the Requirements

For the Degree

of

Masters of Science

Paul Smith Ache III

San Marcos, Texas

July, 1991

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

At this point I would like to thank Dr. Hazlewood for all his time and his quiet teaching style. His leadership has helped me grow as a student and a mathematician. I would also like to thank Dr. Thickstun and Dr. Michalk for their time and service during the writing of this paper. The Department of Mathematics also deserves my gratitude for igniting the learning bug in me and for providing me with the opportunity to continue my studies. Finally, I would like to thank my family and in particular, my father, for all their support and understanding during this time.

Paul Ache

July, 15,1991

INTRODUCTION

The idea of proving geometry theorems has been around since Euclid wrote his book *Elements* in about 300 B.C.. Traditional proofs presented in this book have changed very little in the past 2200 years. As any high school student can attest, a problem is given in which some information is known, and from this information, and usually an accompanying picture, the conclusion is derived after various exercises in logic. However, the accompanying picture can provide information that, at first glance, appears trivial. An example of "trivial" information is the ordering of three collinear points.

The development of the Cartesian coordinate system allowed for the use of algebra in proving geometry theorems. The traditional analytic proof consists of writing equations that describe a given hypothesis. A system of equations is then developed and the solutions to the system are determined. If the solutions derived from the hypothesis are also solutions for the conclusion, then the theorem is considered true. However, this approach allows for conditions for which the conclusion might not be valid. For example, in drawing a picture of a triangle, it is assumed that one vertex is not the same as another vertex. These "assumed" conditions are called *nondegenerate conditions.* According to Shang-Ching Chou in his book *Mechanical Theorem Proving*, " it was Wu Wen-Tsun who first realized the importance of non degenerate conditions in mechanical geometry theorem proving ...".[1]

It is the purpose of this paper to discuss the process of mechanical geometry proving as presented by Chou in the above cited book. In order to present this material in a logical manner, the paper is divide into four chapters. Chapter one discusses Wu's method and presents a simple example in order to point out the underlying process involved. Included in this discussion is a brief introduction to the concepts of constructive geometry, the notion of dependent and independent variables, and the general form of the hypothesis and conclusion of a given geometry statement. Chapter two presents the Algebra prerequisites necessary to determine if the given geometry statement is valid. A general background knowledge of rings, fields, ideals and polynomial rings is helpful in understanding this chapter. Chapter three presents the idea of a Groebner Basis and the concepts used when applying Groebner Basis to mechanical geometry theorem proving. Also included in this chapter is Buchberger's algorithm and his improved algorithm. Finally in this chapter the author's attempt at using MAPLE to implement the improved algorithm is presented along with a brief discussion of each of the subprocedures. The paper concludes with the theory necessary to determine the general validity of a geometry statement and an example of a theorem proved using the Groebner Basis method.

Constructive Geometry

Geometry theorems that can be proved mechanically fall into a large class of theorems known as *geometry statements of constructive type*. It should be noted that in this class there is no notion of order or length and therefore, the type of statements that can be proved

are not limited to a metric geometry. Metric statements can be used however, if the square of the length is considered.

Definition 1.1: A theorem is of constructive type if the points, lines, and circles can be constructed in a definite manner using the following constructions.

Construction 1: Taking an arbitrary point.

Construction 2: Drawing an arbitrary line.

Construction 3: Drawing an arbitrary circle.

Construction 4: Drawing a line through a given point.

Construction 5: Drawing a circle knowing its center.

Construction 6: Taking an arbitrary point on a line.

Construction 7: Taking an arbitrary point on a circle.

Construction 8: Taking the intersection of two lines.

Construction 9: Taking the intersection of a line and a circle.

Construction 10: Taking the intersection of two circles.

From these ten basic constructions it is possible to construct numerous conditions that can be used in the algebraic representation of a geometry theorem. Some of the conditions used in this paper are: points A,B, and C are collinear, line AB is parallel to line EF, line AB is perpendicular to line EF,point B is the midpoint of line AC, and the length of AC equals the length of EF. Each of these conditions can easily be represented as an equation using the coordinates of the given points as variables in the equation.

Wu's Method

In Wu's method, the particular geometric figure is drawn and each point labeled according to the selection of the parameters. Those points that are independent of the particular theorem are considered to be *independent variables*. Those points which are determined by the given hypothesis are considered to be *dependent variables*. After selecting a coordinate system, the given information is written as a series of polynomial equations. The conclusion is also written in polynomial form. Each of the hypothesis equations and the conclusion equation are polynomials in Q[u,x], where the u represents the independent variables, the x represents the dependent variables, and Q is the field of rational numbers. The hypothesis equations are usually represented as $h_1,h_2,...,h_m$ and the conclusion is usually represented by g. The set of polynomials $h_1,h_2,...,h_m$ and g is called a *geometry statement* and is represented by (S).

The next step in Wu's method is to triangulate the hypothesis. This means the equations that represent the hypothesis are arranged in an order such that each successive equation only introduces a single new dependent variable. If this is not possible, ie, one equation might introduce two variables, then a simple elimination method will clear that problem. At this point a series of equations is obtained, namely $f_1,f_2,...,f_n$, where n is the number of dependent variables. The final step is to use successive pseudo division (discussed in Chapter 2) and beginning with the conclusion reduce it with respect to f_n. The polynomial obtained in the first reduction is then reduced with respect to f_{n-1} and each resulting remainder is then reduced with respect to the next f_i concluding with a reduction

of the remainder R_2 with respect to f_1. If the final pseudo division results in zero then the theorem is *generally true* (defined in Chapter 4).

Example 1.2: Chou uses the example presented below to introduce the reader to the process of mechanical geometry proving. The theorem being considered is: The diagonals of a parallelogram bisect each other. He states that this example was " actually produced by the prover, including the selection of coordinates.".[2] Please refer to figure 1 and the discussion following to determine the specific coordinates.

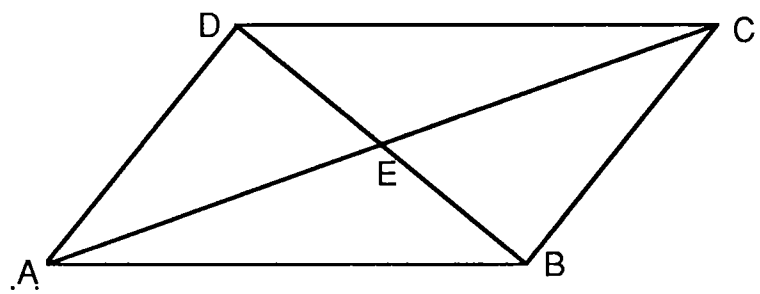

FIGURE 1

The coordinates for each point is as follows: A(0,0) is the origin. Since B can be chosen independently, it is labeled $(u_1,0)$. Likewise, point C can be chosen independently and thus, it is labeled (u_2,u_3). Point D is dependent, since the x coordinate must not be on the x-axis and the y coordinate must not be the same as that of B. Hence, it is labeled (x_2,x_1). Point E is determined by the intersection of the two diagonals and therefore, is also dependent. It is labeled (x_4,x_3).

Since there are four dependent variables, there must be four equations. These equations correspond to the following conditions. (1) AB is parallel to DC. (2) DA is parallel to CB. (3) E is on BD. And (4) E is on AC. In algebraic form the equations are:

$$h_1 = u_1x_1 - u_1u_3 = 0$$

$$h_2 = u_3x_2 - (u_2 - u_1)x_1 = 0$$

$$h_3 = x_1x_4 - (x_2 - u_1)x_3 - u_1x_1 = 0$$

$$h_4 = u_3x_4 - u_2x_3 = 0.$$

Note that h_1 introduces a single variable, as does h_2. However, h_3 introduces both x_3 and x_4. Therefore, by dividing h_4 by h_3 with respect to the variable x_4 a new equation is obtained that is only in terms of the first three variables. This equation is the new h_3, namely,

$$h_3 = (u_3x_2 - u_2x_1 - u_1u_3)x_3 + u_1u_3x_1 = 0.$$

As stated above, successive pseudo division is applied to obtain:

$$R_3 = (2u_3^2 + 2u_2^2)x_3 - u_3^3 - u_2^2u_3$$

$$R_2 = (-u_3^4 - u_2^2u_3^2)x_2 + ((u_2 - 2u_1)u_3^3 + (u_2^3 - 2u_1u_2^2)u_3)x_1 +$$

$$u_1u_3^4 + u_1u_2^2u_3^2$$

$$R_1 = (-u_1u_3^4 - u_1u_2^2u_3^2)x_1 + u_1u_3^5 + u_1u_2^2u_3^3$$

$$R_0 = 0$$

Hence, the theorem is generally true.

The *initials* I_j are the coefficients of the variables x_j in the equations h_j. They are called the *nondegenerate conditions* In this example:

$$I_1 = u_1$$

$$I_2 = u_3$$

$$I_3 = u_3x_2 - u_2x_1 - u_1u_3$$

$$I_4 = u_3$$

In order for the theorem to be generally true it must be the case that each initial not equal zero. Therefore, in this case, u_1,u_3, and $u_3x_2 - u_2x_1 - u_1u_3$ cannot be zero. The conditions that neither u_1 nor u_3 be zero indicates that points B and C cannot be on the x-axis. The third condition can be factored to show that the slope of AC cannot equal the slope of BD which indicates a normal intersection of two lines.

It is important to note that the geometry theorems that can be proved using either Wu's method or the Groebner Basis method discussed in Chapters 3 and 4 is dependent upon the parameters chosen, the equations written and the form of the conclusion. The validity of the statement is however, independent of the nondegenerate conditions, since the fact that g = 0 is not dependent upon whether or not any of the $I_j = 0$.

ALGEBRA PREREQUISITES

In reading this chapter it is assumed that the reader has an understanding of some basic concepts of Algebra. This includes a working knowledge of rings, fields, polynomial rings, ideals and extensions of fields.

THEOREM 2.1: Every ideal I of a polynomial ring A is finitely generated.

Proof: It will be enough to show that given an element $p \in A$ there exists elements b_i of A such that p is a linear combination of the b_i 's.

Let $p \in A$ such that p is reducible and call $\deg(p) = n$. Since $p \in A$, then there exists q_1, $s_1, r_1 \in A$ such that $p = q_1s_1 + r_1$. Note that $\deg(q_1) < \deg(r_1)$ and that $\deg(q_1s_1) = n$. Now, either r_1 is irreducible or not., If r_1 is irreducible then p is finitely generated. If r_1 is reducible, then there exists q_2, s_2, r_2 such that $r_1 = q_2s_2 + r_2$ and therefore, $p = q_1s_1 + q_2s_2 + r_2$. Again, note that $\deg(q_2) > \deg(r_2)$, and hence $\deg(p) \geq \deg(q_1) > \deg(r_1) \geq \deg(q_2) > \deg(r_2)$. Thus, for each polynomial r_i, the degree of the corresponding factors and remainder is less than r_i. And since the degree of any polynomial must be greater than or equal to zero, then $\deg(p) \geq \deg(q_1) \geq \deg(r_1) \geq \ldots \geq \deg(r_n) \geq 0$. Thus, p can be written as a linear combination of q_i, s_i, and r_i, ie, $p = q_1s_1 + q_2s_2 + \ldots + q_ns_n + r_n$.

Definition 2.2: A field F is said to be an *extension field* of K if K is a subfield of F.

Definition 2.3: Let F be a field and extension of some field K. An element *a* of F is said to be *algebraic over K* if *a* is a root of some non-zero polynomial in K[x]. If no polynomial exists in K[x] such that *a* is a root of that polynomial, then *a* is said to be *transcendental over K.*

Definition 2.4: Let $a_1,...a_r$ be elements in F. The *subfield* generated by K and $a_1,...a_r$ is denoted by $K(a_1,...a_r)$.

Lemma 2.5: Let F be an extension of the field K and let $a \in F$ be algebraic over K, then K(a) is the smallest extension of K that contains K and {a}, i.e., if $K \subset K$, where K' is an extension of K, and $a \in K'$, then $K(a) \subset K'$.

Proof: Let $a \in F$ be algebraic over K. Since $K \subset K'$ then $K' = (K \cup \{r_1,...r_n\})$. Either $a \in K$ or $a \notin K$. Suppose first that $a \in K$,which implies that K = K(a) and hence $K(a) \subset K'$. Now consider the case if $a \notin K$. This implies that $K(a) =(K \cup \{a\})$. And since $a \in K'$ then there exists $r_i \in \{r_1,...r_n\}$ such that $a = r_i$. Thus, $(K \cup \{a\}) \subset (K \cup \{r_1,...r_n\})$, and therefore, $K(a) \subset K'$.

Theorem 2.6: Let F be an extension of the field K and let $a \in F$ be algebraic over K, then:

(i) $K(a) = K[a]$

(ii) $K(a) \cong K[x]/(f)$ where $f \in K[x]$ is an irreducible polynomial of degree $n \geq 1$ uniquely determined by the conditions that $f(a) = 0$ and $g(a) = 0$ if and only if f divides g.

(iii) Every element in K(a) can be written uniquely in the form:

$$c_{n-1}a^{n-1} + \ldots + c_1 a + c_0$$

Proof: (ii) From the Fundamental Homomorphism Theorem, it is known that $K[a] \cong K[x]/\ker\Theta_a$ where Θ_a: $K[x] \rightarrow K$ is the mapping defined by $\Theta_a[f(x)] = f(a)$. Thus, it follows, since a is algebraic over K, that $\ker\Theta_a = (f)$ where f is the minimal, irreducible polynomial for which $f(a) = 0$. Note that $(f) \neq (0)$ since f is not the zero polynomial. Also, $(f) \neq (1)$ since the identity map is not a member of (f). Hence $K[a] \cong K[x]/(f)$. Observe that since f is irreducible, then K[x]/(f).is a field and thus, K[a] is also a field.

Now show that K[a] = K(a). Clearly, $K[a] \subset K(a)$. But, from lemma 2.5 K(a) is the smallest extension of K that contains K and a. Therefore, since $K \subset K[a]$ and K[a] contains a then $K(a) \subset K[a]$, which implies equality, ie, K[a] = K(a). Thus, by direct substitution, $K(a) \cong K[x]/(f)$.

(iii) Lastly, show that every element of K(a) can be represented uniquely in the form $c_0 + c_1 a + \ldots + c_{n-1}a^{n-1}$. Let $r \in K(a) = K[a]$. This implies, there exists a polynomial $g \in K[x]$ such that $g(a) = r$. By the division algorithm, there exists polynomials q and $s \in K[x]$ such that $g(x) = q(x)f(x) + s(x)$ and $\deg(s) < \deg(f)$. Recall that $f(a) = 0$,and therefore, $g(a) = s(a) = r$. Thus, since $\deg(s) < \deg(f)$ and $s \in K[x]$, then

$$s(a) = c_0 + c_1 a + \ldots + c_m a^m = c_0 + c_1 a + \ldots + c_{n-1}a^{n-1}$$

For uniqueness, suppose $c_0 + c_1a + ... + c_{n-1}a^{n-1} = d_0 + d_1a + ... + d_{n-1}a^{n-1}$, which implies, $c_0 - d_0 + (c_1 - d_1)a + ... + (c_{n-1} - d_{n-1})a^{n-1} = 0$.

Call $h(x) = c_0 - d_0 + (c_1 - d_1)x + ... + (c_{n-1} - d_{n-1})x^{n-1}$. Since $h(a) = 0$, then $f(x)$ is a factor of $h(x)$ and therefore, $h(x) = p(x)f(x)$ for some $p(x) \in K[x]$. Now, either $h(x) = 0$ or $h(x) \neq 0$. Suppose then, $h(x) \neq 0$. This implies that $\deg(h) = n-1$. But , $\deg(h) = \deg(f) + \deg(p)$. Recall, $\deg(f) + \deg(p) \geq \deg(f) = n$. This implies that $n-1 \geq n$, which is a contradiction. Therefore, $h(x) = 0$ and hence, $c_i - d_i = 0$ for $i = 1$ to $n-1$. Thus, $c_i = d_i$ and representation, therefore, is unique.

Theorem 2.7: If D is a U.F.D. then D[x] is also a U.F.D..

Proof: First, it must be shown that D[x] is an integral domain. So, let $p,q \in D[x]$ and suppose that $p \cdot q = 0$. Since each of p and $q \in D[x]$, then, using an alternate definition for a polynomial, $p = (a_0,a_1...,a_n)$ and $q = (b_1,b_2,...b_m)$, where the a_i's and the b_j's are the coefficients of the terms of the polynomials. Therefore, $(a_0,a_1...,a_n)\cdot(b_1,b_2,...b_m) = 0$. Recall that $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ where $c = p \cdot q = (c_1,c_2,...c_k)$ and $k = m + n$. Thus, since $p \cdot q = 0$, then $c_k = 0$ for each k. Now consider the following. Since $c_0 = a_0b_0 = 0$ then either $a_0 = 0$ or $b_0 = 0$.. Suppose then $a_0 = 0$ and $b_0 \neq 0$. Recall that $c_1 = a_0b_1 + a_1b_0 = 0$ and since $a_0 = 0$ then $a_1b_0 = 0$ which implies that $a_1 = 0$. In general therefore, $c_n = a_0b_n + a_1b_{n-1} + ... + a_nb_0 = 0$ and $a_i = 0$ for $i = 1$ to n. Thus, $p = 0$.. Similarly, if $b_0 = 0$ then $q = 0$. Hence, since either $p = 0$ or $q = 0$, then D[x] is an integral domain.

By defining a function d mapping from $D[x] - \{0\}$ into the natural numbers by $d(p) = \deg(p)$ it is clear that D[x] is a Euclidean domain and hence D[x] is a U.F.D..

Definition 2.8: A subset V of E^m is called an *algebraic set* if V is the set of all common zeros of all elements of a non-empty polynomial set S, i.e., $V=\{(a_0,a_1...,a_n) \in E^m$ $:f(a_0,a_1...,a_n) = 0$ for all $f \in S\}$. V will be denoted by V(S).

Lemma 2.9: Every algebraic set is the set of common zeros of a finite polynomial set.

Proof: Suppose I =(S), the ideal generated by a non-empty polynomial set S, then V(I) = V(S). Recalling that I has a finite generating set, I can be deonted by $(f_1,f_2,...f_n)$. Therefore,$V(S) = V(f_1,f_2,...f_n)$ and clearly, $\{f_1,f_2,...f_n\}$ is finite.

Suppose that U is a non-empty subset of E^m, and let $I = I(U) = \{f: f \in A$ and $f(a_0,a_1...,a_n) = 0$ for all $(a_0,a_1...,a_n) \in U\}$. I is the set of all polynomials for which U is an algebraic set. The following lemma defines the structure of the above set I.

Lemma 2.10: I is an ideal of A.

Proof: First, it must be shown that I is a subring of A. Recall, it is enough to show that (1) if f and g $\in$ I, then fg $\in$ I, and (2) f-g $\in$ I. Let f,g $\in$ I and consider f·g. Since f $\in$ I then $f(a_0,a_1...,a_n) = 0$ for all $(a_0,a_1...,a_n) \in U$. Likewise, $g(a_0,a_1...,a_n)$-= 0. Hence $f(a_0,a_1...,a_n)\cdot g(a_0,a_1...,a_n) = 0$ for all $(a_0,a_1...,a_n) \in U$, which implies that f·g $\in$ I. Now show that f-g $\in$ I. Since $f(a_0,a_1...,a_n) = 0$ and $g(a_0,a_1...,a_n) = 0$ then $(f-g)(a_0,a_1...,a_n) =$ 0, thus f-g$\in$ I. Therefore, I is a subring of A. To show that I is an ideal it must be shown that if f $\in$ I and r $\in$ A, then fr $\in$ I. So suppose that f$\in$ I, r$\in$ A and consider r·f. Since f$\in$ I then $f(a_0,a_1...,a_n) = 0$ Thus $r(a_0,a_1...,a_n)\cdot f(a_0,a_1...,a_n) =0$ which implies that r·f $\in$ I and hence I is an ideal.

Lemma 2.11: (i): $S \subset I(V(S))$

(ii): $U \subset V(I(U))$

(iii): $V(S) = V(I(V(S)))$

and (iv): $I(U) = I(V(I(U)))$

Proof: (i) Let $p \in S \Rightarrow p(a_1, a_2, \ldots a_m) = 0$ for all $(a_1, a_2, \ldots a_m) \in V(S) \Rightarrow p \in I(V(S))$

Thus, $S \subset I(V(S))$.

(ii): Let $a \in U \Rightarrow \exists f \in A$ s.t. $f(a) = 0 \Rightarrow a \in V(I(U))$. Thus, $U \subset V(I(U))$.

(iii): By (ii) it is known that $V(S) \subset V(I(V(S))$. Therefore, it is enough to show that $V(I(S))) \subset V(S)$. Let $a \in V(I(S))) \Rightarrow \exists f \in I(V(S))$ s.t. $f(a) = 0 \Rightarrow a \in V(S)$

$\Rightarrow V(I(S))) \subset V(S)$. Hence, $V(I(S))) = V(S)$.

(iii): By (i) it is known that $I(U) \subset I(V(I(U)))$. Therefore it is enough to show that $I(V(I(U))) \subset I(U)$. Let $p \in I(V(I(U))) \Rightarrow p(a_1, a_2, \ldots a_m) = 0$ for all $(a_1, a_2, \ldots a_m) \in V(I(U))$.

$\Rightarrow p \in I(U) \Rightarrow I(V(I(U))) \subset I(U)$. Hence, $I(V(I(U))) = I(U)$.

Lemma 2.12: Let S_1 and S_2 be two polynomial sets and let $S_1 \cdot S_2$ be the set of all products of an element of S_1 and an element of S_2, then:

(i): $V(S_1 \cup S_2) = V(S_1) \cap V(S_2)$

and (ii): $V(S_1 \cdot S_2) = V(S_1) \cup V(S_2)$.

Proof: (i): Let $a \in V(S_1 \cup S_2)$

$\Leftrightarrow f(a) = 0$ for all $f \in S_1 \cup S_2$

$\Leftrightarrow f(a) = 0 \ \forall \ f \in S_1$ and $f(a) = 0 \ \forall \ f \in S_2$

$\Leftrightarrow a \in V(S_1)$ and $a \in V(S_2)$

$\Leftrightarrow a \in V(S_1) \cap V(S_2)$

(ii): Let $a \in V(S_1 \cdot S_2) \Rightarrow f(a) = 0$ for all $f \in S_1 \cdot S_2$

$\Rightarrow \exists\, g \in S_1$ and $h \in S_2$ s.t. $f = g \cdot h$ for all $f \in S_1 \cdot S_2$

Since $f(a) = 0$ then $(g \cdot h)(a) = 0$ and hence either $g(a) = 0$ or $h(a) = 0$. If $g(a) = 0$ then $a \in V(S_1)$. If $h(a) = 0$ then $a \in V(S_2)$. Which implies $a \in V(S_1) \cup V(S_2)$ and therefore $V(S_1 \cdot S_2) \subset V(S_1) \cup V(S_2)$.

Now let $a \in V(S_1) \cup V(S_2)$. Then this implies that $a \in V(S_1)$ or $a \in V(S_2)$. If $a \in V(S_1)$, then $g(a) = 0$ for all $g \in S_1$. Likewise, If $a \in V(S_2)$, then $h(a) = 0$ for all $h \in S_2$.

Note that $S_1 \cdot S_2 = \{f = g \cdot h:\ g \in S_1,\ h \in S_2\}$. Thus, $f(a) = 0$ for all $f \in S_1 \cdot S_2$. Which implies that $a \in V(S_1 \cdot S_2)$. Therefore, $V(S_1) \cup V(S_2) \subset V(S_1 \cdot S_2)$ and equality holds.

Definition 2.13: A non-empty algebraic set is *irreducible* if it cannot be expressed as the union of two proper subsets, each of which is an algebraic set.

Theorem 2.14: Let V be a non-empty algebraic set. V is irreducible if and only if I(V) is prime.

Proof: Suppose V is irreducible and let $f \cdot g \in I(V)$. Since $f \cdot g \in I(V)$ then $[f \cdot g](a_1, a_2, \ldots a_m) = 0$ for all $(a_1, a_2, \ldots a_m) \in V$. Which implies, $f(a_1, a_2, \ldots a_m) = 0$ or $g(a_1, a_2, \ldots a_m) = 0$. And thus, either $f \in I(V)$ or $g \in I(V)$. Hence, I(V) is prime.

Now suppose that V is reducible and that I(V) is prime.. Since V is reducible then there exist sets S_1 and S_2 such that $V(I(V)) = V(S_1) \cup V(S_2) = V(S_1 \cdot S_2)$. Thus, $I(V) = S_1 \cdot S_2$. But, by supposition, I(V) is prime and therefore, V must be irreducible.

Theorem 2.15: Every algebraic set V in E^m can be uniquely expressed as a union of irreducible algebraic sets, no one containing the other. Each irreducible algebraic set is called a *component of* V.

Proof: Let V(S) be a reducible algebraic set. This implies there exists sets S_1 and S_2 such that $V(S) = V(S_1) \cup V(S_2)$. Either each set is irreducible or at least one set is reducible; suppose then that $V(S_1)$ is reducible. Since $V(S_1)$ is reducible then there exists sets S_3 and S_4 such that $V(S_1) = V(S_3) \cup V(S_4)$. Again, either of these sets may be reducible. Thus, in general, if $V(S_i)$ is reducible then it can be expressed as the union of two algebraic sets $V(S_j)$ and$V(S_k)$, ie $V(S_i) = V(S_j) \cup V(S_k)$. Hence, $V(S) = V(S_1) \cup V(S_2) \cup ... \cup V(S_n) \cup ....$ Now, show that this chain is finite.

$$V(S) = V(S_1) \cup V(S_2) \cup ... \cup V(S_n)$$

For uniquness, suppose $V(S_1) \cup V(S_2) \cup ... \cup V(S_n) = V(S) = V(R_1) \cup ... \cup V(R_m)$ and consider the following.

$$\text{Let } a \in V(S_1) \cup V(S_2) \cup .... \cup V(S_n)$$

$$\Leftrightarrow \exists\ V(S_j) \text{ s.t. } a \in V(S_j)$$

$$\Leftrightarrow f(a) = 0 \text{ for all } f \in S_j$$

$$\Leftrightarrow \exists\ f_1 \in S \text{ s.t. } f_1 \text{ is minimal}$$

$$\Leftrightarrow \exists\ R_i \text{ s.t. } f_1 \in R_i \text{ and } f_1(a) = 0$$

$$\Leftrightarrow a \in V(R_i)$$

$$\Leftrightarrow a \in V(R_1) \cup V(R_2) \cup ... \cup V(R_m)$$

Thus, $V(S_1) \cup V(S_2) \cup ... \cup V(S_n) = V(S) = V(R_1) \cup V(R_2) \cup ... \cup V(R_m)$.

Definition 2.16: The *dimension* of a prime ideal P is the transcendental degree of the quotient field of the integral domain K[x]/P over the field K. The *dimension* of an irreducible algebraic set V is the dimension of its prime ideal I(V). The *dimension* of an algebraic set V is the highest dimension of its components.

Definition 2.17: A *generic zero* of an ideal I is a zero $(a_1,a_2,...,a_n)$ of I in an extension of K such that $f \in I$ if and only if $f(a_1,a_2,...,a_n) = 0$.

Theorem 2.18: An ideal I has a generic zero in some extension K if and only if I is a prime ideal not identical to (1), i.e., $I \neq A$.

Proof:$\Rightarrow$ Suppose I has a generic zero, call it u, and consider polynomials f,g such that $(f \cdot g) \in I \Rightarrow f(u) = 0$ or $g(u) = 0$. $\Rightarrow f \in I$ or $g \in I \Rightarrow$ I is a prime ideal. And since (1) has no zeros then $I \neq (1)$.

($\Leftarrow$): A restatement of this comes from Van Der Waerden's book, *Modern Algebra volume two* on page 53 with a rough sketch of the proof given. This is the theorem that will be proved.

Theorem 2.18.5: "To every prime ideal I in K[x] s.t. $I \neq K[x]$, there exists a field $K' = K(a_1,a_2,...,a_n)$ s.t. I consists of all polynomials f of K[x] for which $f(a_1,a_2,...,a_n) = 0$."[3]

Proof: First, define a map Θ: $K[x] \rightarrow L$ where K is a subset of L such that:

(a): if $g = f \bmod(I)$ then $\Theta(g) = \Theta(f)$

(b): if $g \neq f \bmod(I)$ then $\Theta(g) \neq \Theta(f)$

and (c): if $a \in K$ then $\Theta(a) = a$

Denote $\Theta(x_i) = a_i$ for all i = 1 to n

First, show that the map is well-defined. Since I is a subset of K[x], then any element belonging to I is a polynomial in K[x], and thus, is also a member of the field K. Now, suppose g and f are polynomials in I such that $g = f \Rightarrow g - f = 0 \Rightarrow g\text{-}f \in I \Rightarrow g = f \bmod(I)$ $\Rightarrow \Theta(g) = \Theta(f)$. And further, suppose a and b are field elements belonging to I such that $a = b \bmod(I)$. But, since $I \neq A$, then $a = b$. Thus, all field elements are sent to only one place and therefore, Θ is well-defined.

To complete this arguement it will be shown that the set L is isomorphic to K[x]/I. Recall, if $g = f \bmod(I)$ then $g\text{-}f \in I$ which implies that $g + I$ and $f + I \in K[x]/I$. To do this, define a map $\prod: L \rightarrow K[x]/I$ such that $\prod[\Theta(g)] = g + I$ for all $\Theta(g) \in I$. Note that $=\prod[a] = a + I$ for all field elements in I. To show that $\prod$ is well-defined, consider $\Theta(g),\Theta(f) \in I$, such that $\Theta(g) = \Theta(f)$. Clearly, from the above definition of Θ $g = f \bmod(I)$, and hence, $g + I, f + I \in K[x]/I$ and $\prod[\Theta(g)] = \prod[\Theta(f)]$. Thus,$\prod$ is well-defined.

To show that $\prod$ is a bijection, it must be shown that $\prod$ is one-to-one and onto. To show that $\prod$ is one-to-one, suppose $g + I$ and $f + I \in K[x]/I$ such that $g+ I = f + I$ $\Rightarrow (g - f) + I = 0 \Rightarrow g - f \in I \Rightarrow g = f \bmod(I) \Rightarrow \Theta(g) = \Theta(f)$. So $\prod$ is one-to-one. Clearly,$\prod$ is onto since, if $g + I \in K[x]/I$, then $g \in K[x]$ and hence,$\prod(g) \in L$. Therefore, the map is a bijection.

Finally, define in L, an addition and multiplication that corresponds to the addition and multiplication in K[x]/i, i.e., $\prod(g) + \prod(f) = \prod(h)$ and $\prod(g)\cdot\prod(f) = \prod(k)$ where $\prod(h)$ is the inverse image of $(g + f) + I$ in L and $\prod(k) = (g \cdot f) + I$. Now, consider:

$$\prod(\Theta(g))\cdot\prod(\Theta(g))$$
$$= (g + I)\cdot(f + I)$$
$$= (g\cdot f) + I$$
$$=\prod(\Theta(g)\cdot(\Theta(f)))$$

Similarly, $\prod(\Theta(g)) + \prod(\Theta(f)) = \prod(\Theta(g) + (\Theta(f)))$. Thus, $\prod$ is an isomorphism, and hence, L is isomorphic to K[x]/I.

Now, since I is prime, then K[x]/I is an integral domain and therefore, L contains no zero divisors. Thus, the quotient field K' of L can be formed. Recall, K' = {x: $x = ab^{-1}$ where $a,b^{-1} \in L$} Now, consider the zero element in K'.

$$0 = ab^{-1}$$

$$\Rightarrow a = 0 \text{ for some } a \in L$$

$$\Rightarrow \Theta(0) = 0$$

$$\Rightarrow g(x).= 0 \text{ if and only if } g(a) = 0,$$

or, $g(a_1,a_2,...,a_n) = 0$ for some $(a_1,a_2,...,a_n) \in K'$. Thus, there exists a field K' such that any prime ideal consists of all polynomials f of K[x] for which $f(a_1,a_2,...,a_n) = 0$.

Theorem 2.19: If I is a prime ideal of K[x] such that $I \neq (1)$ and $(a_1,a_2,...,a_n)$ is a generic zero of I then, $K(a_1,a_2,...,a_n)$ is isomorphic to K[x]/I.

Proof: Define a mapping $\Gamma:K(a_1,a_2,...,a_n) \rightarrow K[x]/I$ such that $\Gamma(p(a)) = p + I$, where p(a) is the value of the polynomial evaluated at $a = a_1,a_2,...,a_n$. Note that this mapping is well-defined since if p(a) = q(a) then, p + I = q + I. To show that Γ is a bijection, .let p + I, q + I $\in$ K[x]/I such that p + I= q + I. This implies that p,q $\in$ K and that p(x) = q(x) and thus, p(a) = q(a). Hence, Γ is one to one. To show that the mapping is onto, let r $\in$ K[x]/I. This implies there exists a function f $\in$ K[x] such that r = f + I, and therefore, f(a) $\in$ K(a).

To show that Γ is a homomorphism, let f(a),g(a) $\in$ K(a) and consider the following:

$$\Gamma(f(a)) + \Gamma(g(a))$$

$$= (f + I) + (g + I)$$

$$=(f + g) + I$$

$$= \Gamma(f(a) + g(a)).$$

And likewise,

$$\Gamma(f(a)) \cdot \Gamma(g(a))$$
$$= (f + I) \cdot (g + I)$$
$$= (f \cdot g) + I$$
$$= \Gamma(f(a) \cdot g(a))$$

And thus, $K(a_1,a_2,...,a_n)$ is isomorphic to $K[x]/I$.

Definition 2.20: Let V be an irreducible algebraic set and let $P = I(V)$ be its prime ideal. Variables $v_1,v_2,...,v_s$ among the x's are *algebraically independent on* V if P does not contain a polynomial containing only those specified variables. Variables that are not algebraically independent are *algebraically dependent.*

Definition 2.21: A field K is *algebraically closed* if every polynomial f in K[x] factors into linear factors.

Theorem 2.22 (Hilbert's Nullstellensatz): Every polynomial ideal I of an algebraically closed field K, not identical to the unit ideal, has a common zero, i.e. V(I) is not empty.

Proof: Let K be algebraically closed and let $I \in K$ such that $I \neq (1)$. Clearly, if I is prime, then by theorem 2.18, V(I) is not empty. Thus, suppose I is not prime. But, by theorem 2.15, V(I) can be expressed as the union irreducible algebraic sets, $V(I_i)$ i = 1 to n. Or, $V(I) = V(I_1) \cup V(I_2) \cup ... \cup V(I_n)$. And thus, by theorem 2.14, each I_i is prime and therefore, there exists a generic zero a_i for each prime ideal I_i Hence, V(I) is not empty.

Theorem 2.23 (Alternate form of Hilbert's Nullstellensatz): For every ideal I in K[x], I(V(I)) = Radical(I), ie, every point in V(I) is a zero of f if and only if $f^n \in I$ for some integer $n > 0$.

Proof:$\Rightarrow$: Let $f \in$ Radical(I)

$\Rightarrow f^n \in I$ for some integer $n > 0$.

$\Rightarrow f^n(a) = 0$ for all $a \in V(I)$.

$\Rightarrow f(a) = 0$

$\Rightarrow$ a is a zero of f.

$\Leftarrow$: Let I be an ideal of K[x] and recall $I = (f_1,f_2,...,f_n)$. Let $f \in I$ and let $a \in V(I)$ such that $f(a) = 0$. Introduce a new variable z and consider the polynomial 1-zf. Since a is a zero of f and also of f_i, then a is not a zero of the polynomial 1-zf. Therefore, 1 can be written in as a linear combination of the f_i's and the polynomial 1-zf. Or,

$$1 = Q_1f_1 + Q_2f_2 +...+ Q_nf_n + Q(1-zf)$$

Letting $z = \frac{1}{f}$ and multiplying through by f^m for some integer $m > 0$ to clear fractions yields $f^m = P_1f_1 + P_2f_2 +...+ P_nf_n$. Thus,$f \in$ Radical(I)

Theorem 2.24: If I is a prime ideal such that $I \neq K[x]$, then V(I) is irreducible and I(V(I)) = I.

Proof: Let I be a prime ideal not K[x]. V(I) is irreducible follows from theorem 2.14. From Hilbert's Nullstellenstaz it follows that I(V(I)) = Radical(I), thus, it remains only to show that Radical(I) = I. So, let $f \in$ Radical(I) $\Leftrightarrow f^n \in$ I for some $n > 0$.$\Leftrightarrow f \in$ I since I is prime.

Pseudo Division

Let A be a commutative ring, and let f and g be polynomials in A[v], where v is a new variable. Recall that f and g may be expressed in the following manner:

$$f = a_n v^n + a_{n-1} v^{n-1} + \ldots + a_1 v^1 + a_0$$

$$g = b_k v^k + b_{k-1} v^{k-1} + \ldots + b_1 v^1 + b_0$$

Further, suppose that $k > 0$ and consider the following procedure:

Let $r = f$

Repeat the following step until $m = \deg(r,v) < k$

$r = b_k r - c_m v^{m-k}$ where c_m is the leading coefficient of r.

Since m strictly decreases with each successive step, the process terminates with a final polynomial r_0 = *pseudo division remainder*,which is denoted by prem(f,g,v). The remainder r_0 can also be expressed as $b_k^s f = qg + r_0$, where s is a non-negative integer, q is a polynomial, and $\deg(r_0,v) < \deg(g,v)$. Now suppose the following polynomials are arranged in a triangular form, i.e.,

$$f_1(u_1,\ldots,u_d,x_1)$$

$$f_1(u_1,\ldots,u_d,x_1,x_2)$$

$$\ldots$$

$$f_1(u_1,\ldots,u_d,x_1,\ldots,x_r)$$

and let $g = g(u_1,\ldots,u_d,x_1,\ldots,x_r)$, then *successive pseudo division* proceeds as follows:

$$R_{r-1} = \text{prem}(g,f_r,x_r)$$

$$R_{r-2} = \text{prem}(g,f_{r-1},x_{r-1})$$

$$R_0 = \text{prem}(g,f_1,x_1)$$

R_0 is called the *final remainder* and is denoted by $\text{prem}(g,f_1,\ldots,f_r)$.

The remainder theorem: Given $f_1,...,f_r$ and R_0 as defined above, then there exists non-negative integers $s_1,...,s_r$ and polynomials $Q_1,...,Q_r$ such that:

$$I_1^{s_1}...I_r^{s_r}g = Q_1f_1 + ... + Q_rf_r + R_0$$

where I_i is the leading coefficient of f_i for i = 1 to r (The I_i are also called the *initials*) and $\deg(R_0,x_i) < \deg(f,x_i)$

Proof: The proof will be by induction on r. For r = 1 the remainder formula reduces to the alternate form of the final remainder given above. Now suppose for $1 < j < r-1$ the remainder formula holds, ie, the expression can be written in the following manner:

$$I_1^{s_1}...I_j^{s_j}R_j = Q_1f_1 + ... + Q_jf_j + R_0$$

Performing psudeo division on R_{r-1} yields, $R_{r-1} = I_r^{s_r}g - Af_r$. By direct substitution the desired results are obtained, ie, $I_1^{s_1}...I_r^{s_r}g = Q_1f_1 + ... + Q_rf_r + R_0$.

Ascending Chains and Characteristic Sets

Let K be a field, let $y = y_1,y_2,...,y_m$ be indeterminates and fix an order on the indeterminates such that $y_1 < y_2 < ... < y_m$, letting $f \in K[y]$ and denote the following: the degree of f in y_i by $\deg(f,y_i)$; the *class* of f is the smallest integer c such that $f \in K[y_1,y_2,...,y_c]$, call it class(f). If f is in K, then class(f) = 0. If $f \in K[y_1,y_2,...,y_c]$, let lc(f) = the *leading coefficient* of f. This is also called the *initial* of f. Let lv(f) be the *leading variable* of f, and denote the leading degree of f by ld(f). A polynomial g is said to be *reduced with respect to f* if $\deg(g,y_c) < \deg(f,y_c)$ where c = class(f). If g and f are

polynomials in K[y] where c = class(f) > 0, then prem(g,f,y_c) is reduced with respect to f; this will be denoted as prem(f,g).

Definition 2.25: Let C = $f_1,f_2,...,f_r$ be a sequence of polynomials in K[y]. If either r = 1 and $f_1 \neq 1$ or if r > 0 and 0 < class(f_1) < class(f_2) < ...< class(f_r), then C is a *quasi ascending chain*. Let C be a quasi ascending chain such that class(f_1) > 0. Define prem(g,f_1,...,f_r) inductively to be prem((prem(g,f_2,...,f_r),f_1). An *ascending chain* is a quasi ascending chain in which f_i is reduced with respect to f_j for i < j. Define a partial order < in K[y] such that f < g if class(f) < class(g) or if class(f) = class(g) > 0 and ld(f) < ld(g). If neither f < g or g< f, then f and g are of the *same rank.*

Proposition 2.26: The above partial order in K[y] is well founded, i.e. there are no infinite strictly decreasing sequences of polynomials $p_1 > p_2 > ... > p_n > ....$
Proof: It is enough to show that every non-empty set of polynomials has a minimal element in that ordering. Let S be a non-empty subset of K[x]. Clearly, if there exists an element $a \in K \cap S$ then a is the minimal element. Therefore, suppose $K \cap S = \varnothing$ and let R = {f ∈ K[x] : class(f) is minimal}. This is possible since the class(f) for all f ∈ K[x] is greater than zero. Now let g be the polynomial in R such that ld(g) is least and note that g is the minimal element in S.

Definition 2.27: Let C = $f_1,f_2,...,f_r$ and C_1 = $g_1,g_2,...,g_m$ be two ascending chains. Define an ordering < on C and C_1 by C < C_1 if there is an s ≤ min(r,m) and f_i and g_i are of the same rank for i < s and that f_s < g; or m < r and f_i and g_i are of the same rank for i ≤ m.

Proposition 2.28: The above partial order is well-founded.

Proof: Again, it is enough to show that every non-empty set of ascending chains has a minimal element. Therefore, let M be a non-empty set of ascending chains and let M_1 be the set of ascending chains whose first polynomials are minimal among each ascending chains in M. If M_1 consists of ascending chains all with only one polynomial, then any one of these chains is minimal. If not, let M_2 consist of all chains in M_1 in which the second polynomial is minimal. Again, if M_2 consists of chains of two polynomials only, then one of these can be considered minimal. This process can be continued until an ascending chain is reached in at most m steps, where m is the number of polynomials in C_1.

Definition 2.29: Given a non-empty polynomial set S, let M be the set of all ascending chains formed in S. The minimal ascending chain in M is called the *characteristic set of S*.

Proposition 2.30: Let $C = f_1,f_2,...,f_r$ be a characteristic set of a polynomial set S with $0 < \text{class}(f_1)$. Let $g \neq 0$ be reduced modulo C. Then the set $S_1 = S \cup \{g\}$ has characteristic sets lower than C.

Proof: Either $\text{class}(g) \leq \text{class}(f_1)$ or not. If $\text{class}(g) \leq \text{class}(f_1)$, then g is an ascending chain lower than C. If not, then let $j = \max\{i: \text{class}(f_i) < \text{class}(g)\}$ and note that $f_1,f_2,...,f_i,g$ is an ascending chain lower than C.

Proposition 2.31: Let C be as defined above. C is a characteristic set of S if and only if S contains no non-zero polynomial reduced with respect to C.

Proof: Suppose there exists a polynomial f in S that is reduced with respect to C. From proposition 2.30,this implies, there exists an ascending chain lower than C in S, and thus, C is not a characteristic set of S. Suppose next, that C is not a characteristic set. If C is not a characteristic set , then there is an ascending chain C_1 in S that is less than C. Therefore a polynomial g can be found that is reduced with respect to C.

Theorem 2.32: Every non-empty polynomial set S has a characteristic set.

Proof: Let $f_1 \in S$ such that f_1 is of minimal rank. Either $class(f_1) = 0$ or $class(f_1) > 0$. If the $class(f_1) = 0$, then f_1 is the characteristic set. Suppose, then the $class(f_1) > 0$ and let S_1 be the set of all polynomials in S that are reduced with respect to f_1. Either S_1 is empty or not. If S_1 is empty, then f_1 is a characteristic set. If S_1 is not empty, then let f_2 be a polynomial in S_1 which is minimal and reduce S_1 with respect to f_2. Call this new set S_2. Again, consider if S_2 is empty or not. If it is empty, then the set $\{f_1,f_2\}$ is a characteristic set, if it is not empty, then choose f_3 to be minimal with respect to S_2 and repeat the above process. If S is a finite set of order m, then a characteristic set can be obtained in at most m steps. If S is infinite, then note that $class(f_1) > class(f_2) > class(f_3) > ....$ and, since this is a strictly decreasing sequence of polynomials, it must be finite. The set $R = \{f_1,f_2,...,f_n\}$ is then considered to be a characteristic set.

Proposition 2.33: Let $f_1,f_2,...,f_r$ be a characteristic set of an ideal I, then: (i) If $g \in I$, then $prem(g,f_1,f_2,...,f_r) = 0$. And, (ii) if I is prime, then $prem(g,f_1,f_2,...,f_r) = 0$ implies that $g \in I$.

Proof: (i): Let $g \in I$. Since $prem(g,f_1,f_2,...,f_r)$ is in I and is reduced with respect to $f_1,f_2,...,f_r$, then $prem(g,f_1,f_2,...,f_r) = 0$.by proposition 2.31.

(ii): Now, suppose $prem(g,f_1,f_2,...,f_r) = 0$. By the remainder formula,g can be written as a linear combination of the f_i's, ie, $c_1c_2...c_rg = a_1f_1 + a_2f_2 +... + a_rf_r$. And since each of the c_i, i = 1 to r, is nonzero and reduced with respect to $f_1,f_2,...,f_r$, then $c_i \notin I$. Hence, if I is prime, then $g \in I$.

Irreducible Ascending Chains

Suppose K is field and let $K[y_1,y_2,...,y_n]$ be a polynomial ring. Further, suppose that $C = f_1,f_2,...,f_r$ is an ascending chain not consisting of a constant. Now, consider the following numbers, $class(f_1) = d + 1$ and $m = class(f_r) = d + r$. Renaming each y_i, u_i, where $i \leq d$, and let x_i mean $lv(f_i)$ it is possible to represent C in the following form:

$$f_1(u_1,...,u_d,x_1)$$

$$f_2(u_1,...,u_d,x_1,x_2)$$

$$...$$

$$f_r(u_1,...,u_d,x_1,...,x_r)$$

Definition 2.34: An ascending chain of the form given above is called *irreducible* if each f_i is irreducible in the polynomial ring $K(u)[x_1,...,x_i]/(f_1,...,f_{i-1})$. Hence, the sequence:

$$F_0 = K(u)$$

$$F_1 = F_0[x_1]/(f_1)$$

$$...$$

$$F_r = F_{r-1}[x_r]/(f_1,...,f_{r-1})$$

is a *tower of field extensions.*

Theorem 2.35: Let $f_1,...,f_r$ be an irreducible ascending chain, g be a polynomial in $K[u,x]$ and F_r be as defined in definition 2.34. Also, let $r = prem(g,f_1,...,f_r)$ be the remainder obtained from successive pseudo division of g by $f_1,...,f_r$. The following statements are equivalent.

(i): $r = 0$

(ii): Let E be an extension field of K. If $\mu = (u_1,...,u_d,x_1,...,x_r)$ in E^{d+r} is a common zero of $f_1,...,f_r$ with $u_1,...,u_d$ transcendental over K, then $g(\mu) = 0$.

(iii): The polynomial $g \in F_r$ is zero.

(iv): There are finite non-zero polynomials $c_1,...,c_s$ in $K[u_1,...,u_d]$ such that $c_1,...,c_s g \in (f_1,...,f_r)$ in $K[u,x]$.

Lemma 2.36: For any polynomial $p = a_0 + a_1 x_k + \ldots + a_s x_k^s$ $(0 < k \leq r, 1 \leq s,$ $a_i \in K[u_1, x_1, \ldots, x_{k-1}]$ $a_s \neq 0)$ reduced with respect to $f_1, \ldots, f_r$, if μ is a zero of p, then $p = 0$.

Proof: Run induction on k. Letting $k = 1$ implies $p = a_0 + a_1 x_1 + \ldots + a_s x_1^s$ and note that all $a_j \in K[u]$. Since μ is a zero of p then $p(\mu) = a_0 + a_1 x_1 + \ldots + a_s x_1^s = 0$, and by a previous theorem this representation is unique. Since μ is transcendental over K, then each a_i, $i = 1$ to s, is zero and therefore, $p = 0$.

Now suppose for k - 1, $p = 0$ and consider $p = a_0 + a_1 x_k^{s_1} + \ldots + a_s x_k^{s_k}$ Since μ is a zero of p then $a_0 + a_1 x_k^{s_1} + \ldots + a_s x_k^{s_k} = 0$ and again, since this representation is unique, then μ is a zero for each a_i. And since a_i is reduced with respect to $f_1, \ldots, f_r$ then by the induction hypothesis, $a_i = 0$ for all i, and thus, $p = 0$.

Proof of theorem 2.35 will be as follows: (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i)

(i) $\Rightarrow$ (ii): By the remainder theorem, $I_1^{s_1} \cdot \ldots \cdot I_k^{s_k} g = Q_1 f_1 + \ldots + Q_r f_r$. Since μ is a zero of $f_1, \ldots, f_r$, then $I_1^{s_1} \cdot \ldots \cdot I_k^{s_k} g(\mu) = 0$, and since each I_i is non – zero, then $g(\mu) = 0$.

(ii) $\Rightarrow$ (iii): Since $g(\mu) = 0$ and μ is transcendental over E, then if $F_r = E$, it is immediate that g must be zero.

(iii) $\Rightarrow$ (iv): Since g is a zero in F_r, then $g \in (f_1, \ldots, f_r)$. Thus, for any non-zero polynomial c_i, $gc_i \in (f_1, \ldots, f_r)$.

(iv) $\Rightarrow$ (i) Suppose $c_1, \ldots, c_s$ are non-zero polynomials in $K[u_1, \ldots u_d]$ and consider $c_1, \ldots, c_s \cdot g$. Since each c_i is non-zero, then $c_i(\mu) \neq 0$. But, since $g(\mu) = 0$, then $g \in (f_1, \ldots, f_r)$ and from proposition 2.33, it follows that $\text{prem}(g, f_1, \ldots, f_r) = 0$.

Proposition 2.37: Let $f_1, \ldots, f_r$ be an irreducible ascending chain and let g be any polynomial. If $\text{prem}(g, f_1, \ldots, f_r) \neq 0$, then there are polynomials q and r such that

$qg - r \in (f_1,...,f_r)$ and $r \in K[u]$.

Proof: Since $prem(g,f_1,...,f_r) \neq 0$ then, by psuedo division, $\exists\ I_1^{s_1},...I_r^{s_r}$ such that

$I_1^{s_1}\cdot...\cdot I_r^{s_r}g = Q_1f_1 + ... + Q_rf_r + r_0$

$\Rightarrow I_1^{s_1}\cdot...\cdot I_r^{s_r}g - r_0 = Q_1f_1 + ... + Q_rf_r$

$\Rightarrow I_1^{s_1}\cdot...\cdot I_r^{s_r}g - r_0 \in (.f_1,...,f_r)$

And since $deg(r_0,x_i) < deg(f_i,x_i)$ for all i, then $r_0 \in K[u]$.

Theorem 2.38: Let $f_1,...,f_r$ be an ascending chain and suppose that $f_1,...,f_{k-1}$ is irreducible, but $f_1,...,f_k$ is reducible. Then there are polynomials g and h in K[u,x] reduced with respect to $f_1,...,f_r$ such that $class(g) = class(h) = class(f_k)$ and $gh \in (f_1,...,f_r)$.

Proof: Since f_k is reducible in $F_{k-1}[x]$, then there exists polynomials p and q in $F_{k-1}[x]$ such that $f_k = p\cdot q$ and $deg(p,x_k) < deg(f_k,x_k)$ and likewise, $deg(q,x_k) < deg(f_k,x_k)$. Clearly, $f_k - p\cdot q = 0$. Since the coefficients of the polynomials belong to F_{k-1} it is necessary to clear the denominators which yields a new polynomial, $r = Qf_k - p'q'$, where $p',q' \in K[u,x_1,...x_k]$ and $Q \in K[u]$. Since $Qf_k - p'q' = 0$, then $r = 0$ in $F_{k-1}[x]$, and therefore , $prem(r,f_1,...,f_{rk-1}) = 0$.

Theorem 2.39: Let $f_1,...,f_r$ be an irreducible ascending chain and let $P = \{g: g \in K[u,x]$ and $prem(g,f_1,...,f_r) = 0\}$, then:

(i): P is prime with $f_1,...,f_r$ as its characteristic set.

(ii): A generic point of $f_1,...,f_r$ is a generic zero of P.

(iii): If E is algebraically closed, then $dim(V(P)) = d$. A polynomial vanishes on V(P) if and only if $prem(g,f_1,...,f_r) = 0$.

and (iv): For any field E, if prem(g,f_1,...,f_r) = 0, then the polynomial g vanishes on V(P).

Proof: (i) and (ii): Let μ be a common zero of f_1,...,f_r . Since μ is a common zero, then $g(\mu) = 0$ for all $g \in P$. Hence, P is a prime ideal. By construction of P, there are no non-zero polynomials in P reduced with respect to f_1,...f_r , and therefore, f_1,...,f_r is a characteristic set of P.

(iii): If E is algebraically closed, then it follows from theorem 2.24 that I(V(P)) = P. Therefore, a polynomial g vanishes on V(P) if and only if prem(g,f_1,...f_r) = 0 or if $g \in$ P. Note that dim(V(P)) = dim(P) and call it d.

(iv): Since every field E has an algebraic extension, then (iv) follows immediately from (iii).

Theorem 2.40: Let P be a non-trivial prime ideal in K[u,x]. Let f_1,...f_r be a characteristic set of P, then f_1,...f_r is irreducible.

Proof: Suppose f_1,...f_r is reducible. This implies there exists an integer $k > 0$ such that f_1,...f_{k-1} is irreducible and f_1,...f_k is reducible. Theorem 2.38 implies the existence of two polynomials g and h reduced with respect to f_1,...f_r such that $gh \in (f_1,...f_r) \subset P$. Recall that P is prime, and therefore, g and h are not in P. But, this presents a contradiction and hence, since P is prime, f_1,...,f_r must be irreducible.

Ritt's Principle

Theorem 2.41: Let $S = \{ h_1,...,h_n\}$ be a finite non-empty polynomial set in $K[y_1,...,y_m]$, let I be the ideal $(h_1,...,h_n)$ in $K[y_1,...,y_m]$. There is an algorithm to obtain an ascending chain C such that either:

(i): C consists of a polynomial in $K \cap I$ or,

(ii): $C = f_1,...,f_r$ with the class$(f_1) > 0$ and such that $f_i \in I$ and

prem$(h_j,f_1,...f_r) = 0$ for all i = 1 to r and all j = 1 to n.

In either case, C is called an *extended characteristic set of S.*

Proof: Using the algorithm stated in proposition 2.28, construct a characteristic set $C_1 = f_1,...,f_r$ of S. Call S, S_1 and consider the set C_1. If C_1 consists of only one non-zero constant, then condition (i) is true. If C_1 is not as stated in condition (i), then add to S_1 all non-zero remainders of S_1 reduced with respect to C_1 and call this new set S_2. Now suppose this new set equals S_1. Recall in the construction of C_1, the polynomial f_1 is the polynomial of minimal rank in S. Also recall that each polynomial f_i i = 2 to r, in C_1 is the remainder from successive pseudo divisions of the S_i in the algorithm with respect to f_k. Thus, each f_i can be written as a linear combination of h_j for j = 1 to n, and therefore, $f_i \in I$ for all i = 1 to r. And by proposition 2.33, since C_1 is a characteristic set of $(h_1,...h_n)$, then prem$(h_j,C_1) = 0$ for all j = 1 to n.

Now suppose $S_2 \neq S_1$, then expand S_2 to a new set S_3 using the same procedure. Hence, $S_1 \subset S_2 \subset S_3 \subset ...$ with a corresponding decreasing sequence of characteristic sets, $C_1 > C_2 > C_3 > ...$, which must be finite, since the class of the corresponding polynomials is decreasing. Therefore, there exists an integer m such that C_m consists of either a non-zero constant or $C_l = C_{l+1}$. In either case, the conditions above hold.

Corollary 2.42: Let $S = \{h_1,...,h_n\}$ and suppose that case (ii) happens in theorem 2.41. Further suppose that $f_1,...,f_r$ is the extended characteristic set of S and let I_k be the initials of f_k for k = 1 to r. Letting $S_k = S \cup \{S_k\}$ and $P = \{g: g \in K[y_1,...,y_n]$ and $prem(g,f_1,...,f_r) = 0\}$, then for any extension of the field K:

(i): $V(f_1,...,f_r) - (V(I_1) \cup V(I_2) \cup ... \cup V(I_r)) \subset V(P) \subset V(S) \subset V(f_1,...,f_r)$ and

(ii): $V(S) = V(P) \cup V(S_1) \cup V(S_2) \cup ... \cup V(S_r)$

Proof: (i): Let $a \in V(f_1,...f_r) - (V(I_1) \cup V(I_2) \cup ... \cup V(I_r)) \Rightarrow$ a is a zero of V(P). Since $prem(g,f_1,...,f_r) = 0$, then $I_1^{s_1}\cdot...\cdot I_k^{s_k} g = Q_1f_1 + ... + Q_rf_r$. And since $g(a) = 0$, then $Q_1f_1(a) + Q_2f_2(a) + ... + Q_rf_r(a) = 0. \Rightarrow a \in V(S)$ since $f_i \in I$, for i = 1 to r. $\Rightarrow h_j(a) = 0. \Rightarrow$ $a \in (f_1,...,f_r)$ since $prem(h_j,f_1,...,f_r) = 0$.

(ii):Consider the following:

$V(S) = [V(S) - (V(I_1) \cup V(I_2) \cup ... \cup V(I_r))] \cup [V(S) \cap (V(I_1) \cup V(I_2) \cup ... \cup V(I_r))]$

and note that

$V(S) \cap (V(I_1) \cup V(I_2) \cup ... \cup V(I_r))$

$= (V(S) \cap V(I_1)) \cup (V(S) \cap V(I_2)) \cup ... \cup (V(S) \cap V(I_r))$

$= V(S \cup I_1) \cup V(S \cup I_2) \cup ... \cup V(S \cup I_r)$

$= V(S_1) \cup V(S_2) \cup ... \cup V(S_r)$.

Now consider $V(S) - ((V(I_1) \cup V(I_2) \cup ... \cup V(I_r))$. This set is clearly a subset of V(P). Therefore, it will be enough to show that $V(P) \subset V(S) - (V(I_1) \cup V(I_2) \cup ... \cup V(I_r))$ and hence $V(P) = V(S) - (V(I_1) \cup V(I_2) \cup ... \cup V(I_r))$ which implies (ii).

Consider the following set theory lemma.

From the given of corollary 2.42, we know that (i): $(D - C) \subset A \subset B \subset D$, (ii): $(B - C) \subset A$ and (iii): $(B - C) \cup (B \cap C) = B$. It it will be shown that $A \subset B - C$.

Let $a \in A. \Rightarrow a \in B - C$ or $a \notin B - C$. Suppose, that $a \notin B - C. \Rightarrow a \notin B$ or $a \in B \cap C$. Suppose $a \in B \cap C \Rightarrow a \in C \Rightarrow A \subset C$. From (i), either $B \subset C$, $C \subset B$, or $B = C$. Suppose that, $B \subset C, \Rightarrow (B - C) \cup (B \cap C) \subset C \Rightarrow (B \cap C) \subset C \Rightarrow B = C$. Suppose, $C \subset B \Rightarrow C \subset (B - C) \cup (B \cap C) \Rightarrow C \subset (B \cap C) \Rightarrow B = C \Rightarrow (D - B) \subset B \subset D$, which is a contradiction, thus from the second supposition it must follow that $a \notin B$. But, $A \subset B$, and hence another contradiction arises. Therefore, it must be that $a \in B - C$ and, hence, $A \subset B - C$.

Ritt's Decomposition Algorithm

Theorem 2.43: For any finite non-empty polynomial set S, there is an algorithm to decide whether ideal(S) = (1) or, in the opposite case, decompose $V(S) = V(P_1) \cup V(P_2) \cup ... \cup V(P_s)$, where P_i,i = 1 to s, is the prime ideal given by its irreducible characteristic set.

Proof (accredited to Chou's book): Let D be a dummy variable representing a set of characteristic set s and intialize D to be empty. Using Ritt's principle, construct an extended characteristic set C of S and the corresponding set S_k of S. Three cases are possible: (i) C consists of a constant in which case V(S) is empty and processing stops. (ii): The ascending chain $C = f_1,...,f_r$ is irreducible and, then from Corollary 2.42, it is known $V(S) = V(P) \cup V(S_1) \cup ... \cup V(S_r)$. Note that P_1 is the prime ideal corresponding

to the characteristic set C. From Proposition 2.30, it is known that each S_k has a characteristic set lower than C. Add C to D and repeat the process with each S_k. Or, (iii) $C = f_1,...,f_r$ is reducible, in which case there exists an integer $k > 0$ such that $f_1,...f_{k-1}$ is irreducible but f_k is reducible. Thus, there exists polynomials g and h such that g and h are reduced with respect to $f_1,...,f_r$ and $gh \in (f_1,...,f_k)$. thus, the decomposition $V(S) = V(S_1) \cup V(S_2)$ exists, where $S_1 = S_k \cup \{g\}$ and $S_2 = S_k \cup \{h\}$. Now repeat the process with each of S_1 and S_2. Since this process creates a decreasing sequence of ascending chains, the process eventually terminates with one of two cases possible: (1) D is empty. Thus, S has no common zeros in any extension of K and, therefore, by Hilbert's Nullstellensatz, ideal(S) = (1) = A, or, (2): $D = \{C_1,...,C_s\}$ and then $V(S) = V(P_1) \cup V(P_2) \cup ... \cup V(P_s)$, where P_k is the prime ideal corresponding to the characteristic set C_k.

GROEBNER BASES

Definition 3.1: Let K be a subset of $F[x_1,x_2,...,x_n]$ A polynomial g in $F[x_1,x_2,...,x_n]$ is *b-reducible* means there exists a polynomial f in K such that the leading monomial of f is a factor of some monomial, m, in g. If g is b-reducible modulo K, then a new polynomial h is formed in the following way. Rewrite g such that m is the leading monomial, i.e., $g=cm+g_1$ and note that f can be written in a similar way, ie, $f = c_1m_1+f_1$. Now let h=g-bsf where $b=\frac{c}{c_1}$ and s is a monomial such that $m=sm_1$.

Definition 3.2: The polynomial is h *in normal form* modulo K if and only if there exists no polynomial h' in K such that h is b-reducible modulo h'. The polynomial h is *a normal form* modulo K means there is a sequence of reductions $g \rightarrow h_1 \rightarrow h_2 \rightarrow ... \rightarrow h$ and h is in normal form modulo K. An algorithm S is called a *normal form algorithm* if and only if for all F and g, S(F,g) is a normal form of g modulo K.

Lemma 3.3 The following algorithm is a normal form algorithm.

h:=g

while exists $f \in K,b,s$ (as defined in defintion 3.1) $h \rightarrow f,b,s$ (which reads as h reduces modulo f)

do choose $f \in K,b,s$ such that $h \rightarrow f,b,s$ and sm_1 is maximal with respect to $<_T$ (where $<_T$ is the ordering on the monomials)

h=h-bsf

Proof: Suppose h is the output polynomial from the above algorithm. Since h is the output polynomial, then no polynomial $f \in K$ has a leading monomial that is a factor of any monomial in h. Thus, h is a normal form of g.

Lemma 3.4 For all g, K; b-reduction terminates.

Proof: Let $g \in F[x_1,...,x_n]$ and let K be a finite subset of $F[x_1,...,x_n]$. Suppose there exists a polynomial $f \in K$ such that $g \rightarrow f,b,s$. Since g reduces modulo f, then there exists a monomial m of g such that $sm_1=m$, where m_1 is the leading monomial of f. Let $p=deg(m)$. Since $sm_1=m$, then $deg(sm_1)=p$, and therefore $deg(m_1) < p$. Also note for each $2 \leq j \leq k$ $deg(m_j) \leq deg(m_1)$. By the reduction process a new polynomial h is formed,i.e.:

$$h=cm+g_0-bs(c_1m_1+f_1)$$
$$=g_0-bsf_1$$

Note that in the reduction process the term cm adds out. Thus, no term in h has degree equal to p. In fact, each term in the resulting polynomial sf_1 has degree less than p. Thus, in each step of the reduction process, the multiple term of the original polynomial is replaced by a polynomial in which each term has degree less than the original term. Recall, no term can have degree less than 0. And therefore, reduction of a single term must terminate when

the degree of the resulting polynomial has degree 0. Since the original polynomial consists of a finite number of terms and each term can only be reduced a finite number of times, then b-reduction must terminate.

Lemma 3.5 Suppose g reduces modulo K by way of the following sequence of reductions $g\ g \rightarrow g_1 \rightarrow g_2 \rightarrow \ldots \rightarrow g_k$, then $g=a_1f_1+a_2f_2+\ldots+a_{k-1}f_{k-1}+g_k$, where $a_i \in F[x_1,x_2,\ldots x_n]$ for each i and $f_i \in K$.

Proof: It will suffice to show that, for each n, $g_{n-1} = a_nf_n + g_n$

Run induction on n.

Let $n = 1$

Let $g = c_0m_0 + g_0$ where $m_0 =$ the reduction monomial.

Let $f_1 = c_1m_1 + f_{1_1}$ be the polynomial in K such that $m_0 = s_1m_1$

$$g_1 = -\frac{c_0}{c_1}(s_1f_{1_1}) + g_0$$

$$g_0 = g_1 + \frac{c_0}{c_1}(s_1f_{1_1})$$

$$g = c_0m_0 + g_1 + \frac{c_0}{c_1}(s_1f_{1_1})$$

$$= c_0(s_1m_1 + \frac{c_0s_1}{c_1} f_{1_1}) + g_1$$

$$= \frac{c_0s_1}{c_1}(c_1m_1 + f_{1_1}) + g_1$$

$$g = \frac{c_0s_1}{c_1}(f_1) + g_1$$

Thus, for $n = 1$ $g_{n-1} = a_1f_1 + g_1$

Now suppose, for all $1 \leq i \leq n$, $g_{i-1} = a_if_i + g_i$. It will be shown that

$g_n = a_{n+1}f_{n+1} + g_{n+1}$

Either a term in a_nf_n is reducible by some f in K or a term in g_{n-1} is reducible by some f in K. Therefore, suppose a_nf_n is reducible.

$$g_n = a_n f_n + g_{n-1}$$
$$= a_n(c_n m_n + f_{l_n}) + g_{n-1}$$
$$g_{n+1} = a_n c_n\left(\frac{-s_{n+1}}{c_{n+1}} f_{l_{n+1}}\right) + a_n f_{l_n} + g_{n-1}$$
$$g_{n-1} = g_{n+1} + a_n c_n\left(\frac{s_{n+1}}{c_{n+1}} f_{l_{n+1}}\right) + a_n f_{l_n} + g_{n-1}$$
$$g_n = a_n c_n m_n + a_n f_{l_n} + g_{n+1} + a_n c_n\left(\frac{s_{n+1}}{c_{n+1}} f_{l_{n+1}}\right) - a_n f_{l_n} g_n$$
$$= a_n c_n m_n + \frac{a_n c_n s_{n+1}}{c_{n+1}} f_{l_{n+1}} + g_{n+1}$$
$$= \frac{a_n c_n s_{n+1}}{c_{n+1}} f_{n+1} + g_{n+1}$$
$$= a_n c_n m_n + \frac{a_n c_n s_{n+1}}{c_{n+1}} f_{l_{n+1}} + g_{n+1}$$
$$= \frac{a_n c_n s_{n+1}}{c_{n+1}} f_{n+1} + g_{n+1}$$

Now, suppose a term in g_{n-1} is reducible by some $f \in K$. Thus,

$$g_n = a_n f_n + c_n m_n + g_{n-1}$$
$$g_{n+1} = a_n f_n + c_n\left(\frac{-s_{n+1} f_{l_{n+1}}}{c_{n+1}}\right) + g_{l_{n-1}}$$
$$g_{n-1} = g_{n+1} - a_n f_n + c_n\left(\frac{s_{n+1} f_{l_{n+1}}}{c_{n+1}}\right)$$
$$g_n = a_n f_n + c_n m_n + g_{n-1} - a_n f_n + c_n\left(\frac{s_{n+1} f_{l_{n+1}}}{c_{n+1}}\right)$$
$$= c_n s_{n+1} m_{n+1} + c_n\left(\frac{s_{n+1} f_{l_{n+1}}}{c_{n+1}}\right) + g_{n+1}$$
$$= c_n\left(\frac{s_{n+1}}{c_{n+1}}\right) f_{n+1} + g_{n+1}$$

Therefore, for any reduction, $g_{n-1} = a_n f_n + g_n$

Now consider the following reductions

$$g=a_1f_1 + g_1$$

$$g_1=a_2f_2 + g_2$$

$$g_{k-1}=a_kf_k + g_k$$

And by successive substitutions $g=a_1f_1+a_2f_2+...+a_{k-1}f_{k-1}+g_k$.

Because the choice of f is not fixed in the reduction process, it is possible to obtain two different normal forms for the same polynomial. However, there are sets for which only one set of normal forms exist. These sets, according to Buchberger, "play the crucial role for our approach to an algorithmic solution of problems in polynomial ideal theory."[4].

Definition 3.6: A set K is called a *Groebner Basis* if and only if for all g, h_1,h_2, if h_1 and h_2 are normal forms of g modulo K, then $h_1=h_2$.

The following theorem is fundamental to the application of Groebner Bases

Theorem 3.7: If G is a Groebner Basis of an ideal I in $F[x_1,x_2,...,x_n]$, then $g \in I$ if and only if the normal form of g modulo G is zero.

Proof: Let I be an ideal in $F[x_1,x_2,...,x_n]$, and let $G = \{p_1,p_2,...,p_m\}$ be a Grobner Basis of I. Let $g \in F[x_1,x_2,...,x_n]$ and consider the reduction of g modulo G. This implies that $g = a_1p_1 + a_2p_2 + ... + a_{k-1}p_{k-1} + g_k$,$\in$ where g_k is the normal form of g. Since G is a Grobner Basis, then g_k is unique.

Suppose $g_k = 0$, then $g = a_1p_1 + a_2p_2 + ... + a_{k-1}p_{k-1}$. Thus, g is the linear combination of the generating set of I and therefore, $g \in I$.

Now suppose $g \in I$ and, again consider a reduction of g modulo G. This, too, implies that $g = a_1p_1 + a_2p_2 + ... + a_{k-1}p_{k-1} + g_k$., where either $g_k = 0$ or $g_k \neq 0$. So suppose $g_k \neq 0$. Since $g \in I$, then $g = b_1p_1 + b_2p_2 + ... + b_mp_m$. Therefore, $g = a_1r_1 + a_2r_2 + ... + a_{k-1}r_{k-1} + g_k = b_1p_1 + b_2p_2 + ... + b_mp_m$. Since I is an ideal and $g \in I$, then addition is commutative and terms can, therefore, be rearranged so that $r_i = p_i$ for each i. Hence:
$g_k = (b_1 - a_1)p_1 + (b_2 - a_2)p_2 + ... + (b_{k-1} - a_{k-1})p_{k-1} + ... + b_mp_m$.
But this shows that g_k is a linear combination of the p_i's. Therefore, g_k is divisible by p_i. And thus g_k is not in normal form which contradicts the assumption. Therefore, $g_k = 0$.

Theorem 3.8: Let S be an arbitrary normal form algorithm. The following properties are equivalent:

(i) K is a Groebner Basis

(ii) For all f,g: f is congruent to g modulo K if and only if the normal form of f modulo K is congruent to the normal form of g modulo K.

Proof: Suppose K is a Groebner Basis and consider the polynomials g and h such that S(K,g) = S(K,h). From Lemma 3.6, each of g and h can be written as a linear combination of the polynomials in K plus its respective normal form. Thus, $g = a_1f_1 + a_2f_2 + ... + a_nf_n + g_n$ and $h = b_1f_1 + b_2f_2 + ... + b_nf_n + h_n$. By supposition, $h_n = g_n$, therefore, h can be rewritten as $h_n = h - b_1f_1 + b_2f_2 + ... + b_nf_n$ And then by substitution, g can be written as such: $g = a_1f_1 + a_2f_2 + ... + a_nf_n + h - (b_1f_1 + b_2f_2 + ... + b_nf_n$ Or, $g-h = (a_1-b_1)f_1 + (a_2-$

$b_2)f_2 + ... + (a_n - b_n)f_n$ Which implies that $g-h \in (K)$, and thus, h is congruent to g modulo K, since $g - h = 0$.

Now suppose statement (ii) holds and let h_1, h_2 be normal forms of g such that $h_1 = h_2$. By the supposition, h is congruent to g modulo K and therefore, K is a Groebner Basis

In the application process of Groebner Basis it is important to decide if a given set is a Groebner Basis,or if not, how to construct one from the given set. Therefore, the idea of an "S-polynomial" is introduced.

Definition 3.9: Given polynomials f_1, f_2 the corresponding S-polynomial

$(f_1, f_2) = u_1 f_1 - u_2 f_2$

where c_i = leading coefficient of f_i and u_i is such that $s_i u_i$ is the least common multiple of s_1 and s_2 and s_i is the leading monomial of f_i.(i=1,2).

Theorem 3.10: (Algorithmic characterization of a Groebner Basis)

Let S be an arbitrary normal form algorithm. The following properties are equivalent:

(i) K is a Groebner Basis

(ii) For all $f_1, f_2 \in$ K: S(K,S -polynomial(f_1, f_2)) = 0.

Proof: Suppose K is a Groebner Basis and let $f_1, f_2 \in$ K. Since the S-polynomial is a linear combination of $f_1$and f_2, then Spoly(f_1, f_2) $\in$ K. And by. lemma 3.7 a b-reduction of this polynomial yields zero.

Now suppose a normal form of S-poly(f_1,f_2) modulo K =h_1 . Further, suppose that there exists an h_2 that is also a normal form of S-poly(f_1,f_2) modulo K. From lemma 3.6, S-poly(f_1,f_2) = $a_1f_1 + a_2f_2 + \ + a_nf_n$ and S-poly(f_1,f_2) = $b_1f_1 + b_2f_2 + \ + b_nf_n + h_2$. Thus, $h_2 = (a_1 - b_1)f_1 + (a_2 - b_2)f_2 + ... + (a_n - b_n)f_n$. Since h_2 is a normal form, then no monomial term in h_2 is a multiple of the leading monomials of f_i i=1 to n. Therefore, each $(a_i - b_i) = 0$, which implies that $a_i = b_i$ for each i. And since $(a_i - b_i) = 0$ for each i, then $h_2 = 0$. Hence, $h_1 = h_2$ and K is, therefore, a Groebner Basis.

The following algorithm allows for the construction of a Groebner Basis from a given set of polynomials.

Algorithm 3.11: G:=F

B:={{f_1,f_2}: f_1,$f_2 \in$ G, $f_1 \neq f_2$}

while B $\neq \varnothing$ do

{f_1,f_2} = a pair in B

B: = B - {{f_1,f_2}}

h: = Spoly (f_1,f_2)

h' = Normal form (G,h)

If h' $\neq$ 0 then

B:= B $\cup$ {{g,h'}: g $\in$ G}

G:= G $\cup$ {h'}

The above algorithm will be referred to as S-reduction.

Theorem 3.12: S-reduction terminates.

Proof: Consider the following ideals. Let $G_1 = F = \{f_1,f_2,...,f_n\}$ and let $P_1 = \{m_1,m_2,...m_n\}$ where m_i is the leading monomial of f_i for each i. Let $G_2 = G_1 \cup \{h'\}$ as formed in the algorithm. Thus, $P_2 = P_1 \cup \{m_{h'}\}$. Therefore, in general , $P_{i+1} = P_i \cup \{m_{hi'}\}$. Clearly,$P_1 \subset P_2 \subset ... \subset P_i \subset$. ... .Now consider the sequence of ideals $(P_1),(P_2)$, ...(P_n),.... Since for each i, $P_i \subset P_{i+1}$, then $(P_i) \subset (P_{i+1})$. Thus, $(P_1) \subset (P_2) \subset ... \subset (P_n) \subset (P_{n+1}) \subset$... .Hence, by Hilbert's Theorem on ascending chains, this chain of ideals is Noetherian and, therefore, the algorithm terminates.

Definition 3.13: F is a *Reduced Groebner Basis* if and only if F is a Grobner Basis and for all $f \in F$: f is a normal form modulo F-{f} and the leading coefficient of f is one.

Theorem 3.14: Uniqueness of Reduced Groebner Basis.

If (G) = (G') and if each of G and G' is a reduced Groebner Basis, then G = G'.

Proof: Let $G'=\{g_1,g_2,...,g_m\}$, where $deg(g_i) > deg(g_{i+1})$ for i=1 to m-1, and run induction on the number of elements in G.

Base case: Let $G=\{f\}$, $f \neq 0$

Since (G)=(G'), then $f \in (G')$ and therefore $f=a_1g_1 + a_2g_2 + ...+ a_mg_m$, and since $g_i \in (G)$ for each i, then $g_i=b_if$. Thus, by direct substitution, $f=(a_1b_1 + ...+a_mb_m)f$.

Now, consider the degree of each of the following polynomials

$$deg(f) = deg(a_1) + deg(g_1),$$

$$deg(g_1) = deg(a_1) + deg(f),$$

Thus, $\deg(f) + \deg(g_1) = \deg(a_1) + \deg(b_1) + \deg(f) + \deg(g_1)$

$\Rightarrow \deg(a_1)+\deg(b_1)=0.$

Thus, $\deg(a_1) = \deg(b_1) = 0$, and therefore, $\deg(f) = \deg(g_1)$. Since $f \neq$ then $g_1 \neq 0$. Since each of G and G' is a RGB, then each of f and g_1 is monic, which implies that $c_1=1$ for each of f and g_1. Recall that $g_1 = b_1 f$, and thus, from the above statement it is clear that $b_1 = 1$. It is also clear that $\deg(a_1b_1+...+a_mb_m) = 0$ and since f is monic, then $a_1b_1+...+a_mb_m=1$. Since $b_1 = 1$, then it is also true that $a_1 = 1$, and therefore, $a_ib_i = 0$ for i = 2 to m.

Since K is a field, then either $a_i = 0$ or $b_i = 0$. If $a_i = 0$, then $a_ig_i = 0$ and if $b_i = 0$, then $g_i = 0$ and again $a_ig_i = 0$. In either case, $a_ig_i = 0$, i = 2 to m, and therefore, $f = g_1$, which implies G = G'

Now suppose that for all $1 \leq k \leq n$ $G = \{f_1,f_2,...,f_k\} = \{g_1,g_2,...,g_k\} = G'$, and consider, $G=\{f_1,f_2,...,f_{n+1}\}$ and $G'=\{g_1,g_2,...,g_m\}$ where $m \geq n+1$.

By supposition, $(G) = (f_1,f_2,...,f_{n+1}) = (g_1,g_2,...,g_m) = (G')$

$\Rightarrow (f_1,f_2,...,f_n) + (f_{n+1}) = (g_1,g_2,...,g_n) + (g_{n+1},g_{n+2},...,g_m)$

$\Rightarrow (f_1,f_2,...,f_n) + (f_{n+1}) = (f_1,f_2,...,f_n) + (g_{n+1},g_{n+2},...,g_m)$

$\Rightarrow \quad (f_{n+1}) = (g_{n+1},g_{n+2},...,g_m)$

And by the base case it follows that $g_{n+1} = f_{n+1}$ and that $g_k = 0$ for k = n+2 to m.

Algorithm 3.15: (An improved version of the Groebner Basis Algorithm)

Let G be the set of polynomials under consideration.

Let B be the set of all pairs of polynomials in G, ie ,B = $\{\{f_1,f_2\}: f_1,f_2 \in G, f_1 \neq f_2\}$,

Let R be the set of all polynomials in G which can be reduced modulo the other polynomials of G.

Let P be the set of reduced polynomials in R.

Algorithm:

R: = G ,P: = { }, G: = { }, B: = { }.

Reduceall (R,P,G,B); Newbasis (P,G,B)

while B ≠ { } *do*

$\{f_1,f_2\}$: = a pair in B whose LCM(LP(f_1,f_2)) is minimal w.r.t. $<_t$

B: = B - $\{f_1,f_2\}$

if(not Criterion1(f_1,f_2,G,B) *and*

not Criterion2(f_1,f_2)) *then*

h: = NormalForm(G,Spolynomial(f_1,f_2))

if h ≠ 0 *then*

G_0: = {g ∈ G: LP(h) ≤ LP(g)}

R: = G_0; P: ={h}; G: = G - G_0

B: =B - $\{\{f_1,f_2\}: f_1 \in G_0$ or $f_2 \in G_0\}$

Reduceall (R,P,G,B); Newbasis (P,G,B).

Subalgorithm Reduceall (transient: R,P,G,B):

while R: $\neq$ { } *do*

h: = an element in R; R: = R - {h};

h: = normalform($G \cup P$, h)

if h $\neq$ 0 *then*

G_0: = {g $\in$ G: LP(h) $\leq$LP(g)};

P_0: = {p $\in$ P: LP(h) $\leq$ LP(p)};

G: = G - G_0

P: = P - P_0

R: = $R \cup G_0 \cup P_0$

B: = B - {{f_1,f_2} $\in$ B: $f_1 \in G_0$ or $f_2 \in G_0$}

P: = $P \cup$ {h}.

Subalgorithm Newbasis (transient: P,G,B):

G: = $G \cup P$

B: = $B \cup$ {{g,p}; g $\in$ G, p $\in$ P, g $\neq$ p}

H: = G; K: = { }

while H $\neq$ { } *do*

h: = an element in H; H: = H - {h};

k: = Normalform(G - {h},h); K: = $K \cup$ {k}

G: = K.

Subalgorithm Criterion1(f_1,f_2,G,B): $\Leftrightarrow$ there exists a p $\in$ G such that

$f_1 \neq p$, $p \neq f_2$,

LP(p) $\leq_m$ LCM(LP(f_1),LP(f_2)),\

{f_1,p} not in B and {p,f_2} not in B.

Subalgorithm Criterion2(f_1,f_2): $\Leftrightarrow$

$$\text{LCM}(\text{LP}(f_1),\text{LP}(f_2)) = \text{LP}(f_1)\cdot\text{LP}(f_2).$$

Abbreviations

LP(g)	the leading power product of g.
LCM(s,t)	the least common multiple of s and t.
$s \leq_m t$	t is a multiple of s.

The two following theorems demonstrate the correctness of the algorithm.

Theorem 3.15: If $\text{LP}(f_1)\cdot\text{LP}(f_2) = \text{LCM}(\text{LP}(f_1).\text{LP}(f_2))$ then the S-polynomial (f_1,f_2) can always be reduced to zero modulo G.

Proof: Run induction on the number of terms in f_2.

Let $f_1 = a_nx^n + \ldots + a_0$ and $f_2 = b_my^m$. Recall, S-polynomial$(f_1,f_2) = u_1f_1 - \frac{c_1}{c_2}u_2f_2$. Thus, $u_1 = y^m$ and $u_2 = x^n$. Therefore:

S-poly: $= y^m(a_nx^n + \ldots + a_0) - \frac{a_n}{b_m}x^n(b_my^m)$

$= a_nx^ny^m + \ldots + a_0y^m - a_nx^ny^m$

$= a_{n-1}x^{n-1}y^m + \ldots + a_0y^m$

This polynomial will reduce modulo f_2 to zero in n steps because with each reduction the leading term will be added out. Thus, $S_n = 0$.

Now, suppose for $1 \leq i \leq m-1$, if $f_1 = a_nx^n + \ldots + a_0$ and $f_2 = b_{m-1}y^{m-1} + \ldots + b_0$, then the corresponding S-polynomial reduces to zero and let $f_1 = a_nx^n + \ldots + a_0$ and $f_2 = b_my^m + \ldots + b_0$. Forming the S-polynomial of f_1 and f_2 yields:

S-poly: $= y^m(a_nx^n + \ldots + a_0) - \frac{a_n}{b_m}x^n(b_my^m + \ldots + b_0)$

$= a_nx^{n-1}y^m + \ldots + a_0y^m - \frac{b_ma_n}{b_{m-1}}x^ny^{m-1} - \ldots - \frac{b_0a_n}{b_m}x^n$

Reducing this polynomial modulo f_2 n times yields:

$$S_n = (c_n x^n y^{m-1} + \ldots + c_0 y^{m-1}) - (d_{m-1} x^n y^{m-1} + \ldots + d_0 x^n)$$

which is in the form of an S-polynomial corresponding to a polynomial f_1 with n terms and a polynomial f_2 with m-1 terms, and thus, by the induction step, this polynomial reduces to zero.

Theorem 3.16: Let S be an arbitrary normal form algorithm. The following two statements are equivalent:

(i) F is a Groebner Basis, where $F = \{g_1,\ldots,g_n\}$.

(ii) For all $f, g \in F$ there exists $h_1,\ldots h_k \in F$ such that $f = h_1$ and $g = h_k$ and

$LCM(LP(h_1),\ldots,LP(h_k)) \leq_m LCM(LP(f),LP(g))$, and

$S(F,S\text{-polynomial}(h_i,h_{i+1})) = 0$ for i = 1 to k.

Proof: Suppose first that F is a Groebner Basis and let f and $g \in F$. By theorem 3.7, it is known that any polynomial in (F) will reduce to zero modulo F. And since $S\text{-poly}(f,g) \in (F)$, then the conditions of the theorem are met by simply letting $f = h_1$ and $g = h_2$.

Now, suppose condition (ii) is met, i.e., given for each h and $g \in F$, there exists $k \in$ {the natural numbers} and $f_1,\ldots,f_k$ such that $LCM(LP(h_1),\ldots,LP(h_k)) \leq_m LCM(LP(f),LP(g))$, and $S(F,S\text{-polynomial}(h_i,h_{i+1})) = 0$ for i = 1 to k. Note that for each $S\text{-poly}(f_i,f_{i+1})$, the $LCM(LP(f_i), LP(f_{i+1}))$ is a factor of the LCM(LP(g),LP(h)), and hence, there exists a monomial w_i such that $w_i \cdot LCM(LP(f_i), LP(f_{i+1})) = LCM(LP(g),LP(h))$. Consider the following two consecutive S-polynomials:

$$u_i f_i - v_i f_{i+1} = a_1 g_1 + \ldots + a_n g_n$$

$$u_{i+1} f_{i+1} - v_{i+1} f_{i+2} = b_1 g_1 + \ldots + b_n g_n$$

Multiplying each equation by the corresponding monomial w_i and w_{i+1} yields:

$$w_i u_i f_i - w_i v_i f_{i+1} = w_i(a_1 g_1 + \ldots + a_n g_n)$$

$$w_{i+1} u_{i+1} f_{i+1} - w_{i+1} v_{i+1} f_{i+2} = w_{i+1}(b_1 g_1 + \ldots + b_n g_n)$$

Recall that v_i is such that $v_i \cdot LP(f_{i+1}) = LCM(LP(f_i),LP(f_{i+1}))$ and that w_i is such that $w_i \cdot LCM(LP(f_i),LP(f_{i+1})) = LCM(LP(g),LP(h))$. Thus, $v_i w_i LP(f_i) = LCM(LP(g),LP(h))$ And likewise, w_{i+1} and u_{i+1} are such that $u_{i+1} w_{i+1} LP(f_i) = LCM(LP(g),LP(h))$. Therefore, $v_i w_i LP(f_i) = u_{i+1} w_{i+1} LP(f_i) = LCM(LP(g),LP(h))$, which implies that $v_i w_i(f_i) = u_{i+1} w_{i+1} LP(f_{i+1})$. Adding the two equations together yields $w_i u_i f_i - w_{i+1} v_{i+1} f_{i+2} = w_i(a_1 g_1 + \ldots + a_n g_n) + w_{i+1}(b_1 g_1 + \ldots + b_n g_n)$.

Now consider the system of equations formed by the given Spolynomials:

$$u_1 f_1 - v_1 f_2 = a_{11} g_1 + \ldots + a_{1n} g_n$$

$$u_2 f_2 - v_2 f_3 = a_{21} g_1 + \ldots + a_{2n} g_n$$

$$u_{k-1} f_{k-1} - v_{k-1} f_k = a_{k1} g_1 + \ldots + a_{kn} g_n$$

Multiplying each equation by the corresponding monomial w_i yields:

$$w_1 u_1 f_1 - w_1 v_1 f_2 = w_1(a_{11} g_1 + \ldots + a_{1n} g_n)$$

$$w_2 u_2 f_2 - w_2 v_2 f_3 = w_1(a_{21} g_1 + \ldots + a_{2n} g_n)$$

$$w_k u_{k-1} f_{k-1} - w_k v_{k-1} f_k = w_k(a_{k1} g_1 + \ldots + a_{kn} g_n)$$

And, as noted above, $w_i v_i f_{i+1} = w_{i+1} u_{i+1} f_{i+1}$ for $i = 1$ to k-1. Thus, by adding the left hand side and the right hand side, the following equation is obtained:

$$w_1 u_1 f_1 - w_k v_{k-1} f_k = (w_1 + \ldots + w_k)(c_1 g_1 + \ldots + c_n g_n)$$

Since $w_1u_1LP(f_1) = LCM(LP(g),LP(h))$ and $w_kv_{k-1}LP(f_k) = LCM(LP(g),LP(h))$, then the L.H.S. is the Spolynomial of g and h. And, clearly, since the R.H.S. is a linear combination of the generating set for ideal(F), then by theorem 3.7, it is known that this Spolynomial reduces to zero and hence, F is a Groebner Basis.

Implementation of the Improved Algorithm

The program below was written to implement Buchberger's improved algorithm for calculating a Groebner Basis for a given set of polynomials. It was written in Maple using a Macintosh IIfx. The input parameters include a set of polynomials, a list of variables, and the number zero or one. The order on the list of variables induces an ordering on the variables. For example, if the list was as follows, [x1,x2,x3,x4], then the ordering would be x1 > x2 > x3.>x4. The number 0 induces a total degree ordering on the polynomials, whereas the number 1 will induce a purely lexicographical ordering on the polynomials. The main program is listed below, followed by a list of the subroutines with a brief discussion of each.

Main Program:

```
mygrobner:=proc(POLY,X,dg): with(grobner):
  if dg=1 then DG:=plex else DG:=tdeg fi;
  R:=POLY;P:={};G:={};B:={};
  reduceall(R);newbasis(P);
  while(B<>{}) do
  smallestlcm(B);
  B:=B minus{Zee};print(Zee);
  criterion1(Zee); if ckg<>0 then next fi;
  criterion2(Zee); if ck2 = 0 then next fi;
  S:= spoly(Zee[1],Zee[2],X,DG); print(S);
```

```
h:= normalf(S,G,X,DG);print(h);if h= 0 then next fi;
fctrck(h,G);
R:=Go;P:={h};G:=G minus Go; Bminus(B);
B:=Be; reduceall(R);  newbasis(P);
od;print (G);end;
```

The first line calls for the input as a procedure in the form "mygrobner(POLY,X,dg)". "Poly" is the set of polynomials, "X" is the list of variables, and "dg" is the number 1 or 0 as described above. A call is then made to "Reduceall". This subroutine is listed below with the associated subroutines following.

Reduceall subroutine:

```
reduceall:=proc(R) F:=R;
  while (F<>{}) do
  h:=F[1]; F:= F minus {h};
  GUP:=G union P; h:=normalf(h,GUP,X,DG);  if h=0 then next
  fi;
  fctrck(h,P);Poo:=Go;Go:={};
  fctrck(h,G);G:= G minus Go;
  P:=P minus Poo;F:=F union Go;F:=F union
   Poo;Bminus(B);B:=Be;
  P:=P union {h};od;
  Poo:={};Go:={};end:
```

The subroutine "reduceall" reduces all the polynomials in the set R with respect to all other polynomials. If the reduced form of a polynomial is not zero, a call to the subroutine "fctrck" is made. In this procedure, the leading term of each polynomial in the set P is checked to see if it is a multiple of the leading term of the reduced polynomial. The procedure "fctrck" is called again to check the polynomials in the set G. The polynomials that are multiples are then removed from the sets G and P and added to the set F so they

can be further reduced. A call to the subroutine "Bminus" is then made to remove all pairs of polynomials that contain any of the polynomials removed from G.

Fctrck subroutine

```
fctrck:=proc(h,G)local j;Go:={};
  leadterm(h); hlm:=leedmon;
  leedmon:=0; for j to nops(G) do ldm:=0;
  leadterm(G[j]);ldm:=leedmon;
  if divide(ldm,hlm) =false then next else
  Go:=Go union {G[j]};fi;od;end:
```

Embedded in this subroutine is the subroutine "leadterm". This subroutine determines the leading term of a given polynomial.

Leadterm subroutine

```
leadterm:=proc(c) local el;
  el:=leadmon(c,X,DG);
  leedmon:=el[1]*el[2];end:
```

Bminus subroutine

```
Bminus:=proc(T) local eb,td; eB:={};Be:=B;
  for td to nops(Be) do
  q:=B[td];
  tee:= q intersect Go;
  if tee<>{} then eB:=eB union {q} fi;
  od;
  Be:=Be minus eB;
  end:
```

After the call to "reduceall" is made a call to the subroutine "newbasis" is made. In this subroutine a Groebner Basis is calculated using Buchburger's original algorithm. Present in this procedure is the subroutine "bset". This procedure, along with the procedure "pair"

forms the set B, which the set consisting of all pairs of polynomials in the set G. Also embedded is the subroutine "helement". This procedure reduces all polynomials in the set G with respect to all the other polynomials in the set.

Subroutine newbasis

```
newbasis:=proc(P) G:= G union P;
  bset(G,P);
  H:=G;K:={};
  helement(H);G:=K;
  end:
```

Subroutine helement

```
helement:=proc(H) local k,L; L:=H;while(L<>{}) do
  h:=L[1];L:=L minus {h};eG:=G;
  eG:=eG minus {h};
  k:=normalf(h,eG,X,DG);
  if k= 0 then next fi;
  K:=K union {k}; od;end:
```

Subroutines bset and pair:

```
bset:=proc(l,m) for k to nops(l) do
  B:=B union pair(l[k],m);od;end:

pair:=proc(l,m)local i,jt; jet[0]:={};
  for i to nops(m) do
  jt:={l,m[i]}; if nops(jt)=1 then
  next else jet[i]:=jet[i-1] union {jt};
  fi;od;end:
```

After the main program finishes, the subroutine "newbasis" a call is made to the subroutine "smallestlcm". This procedure determines the pair of polynomials in the set B

that has the smallest L.C.M. of their leading terms. Embedded in this procedure is the subroutine "least" which calculates the L.C.M. of a given pair of polynomials.

Subroutines smallestlcm and least:

```
smallestlcm:=proc(Bset) Bee:=Bset;Zee:=Bee[1];
  least(Zee);
  Bee:=Bee minus {Zee};
  frstpairlcm:=lest1;
  D1:=degree(frstpairlcm,Y);lest1:=0;
  while(Bee<>{}) do pr:=Bee[1];Bee:=Bee minus{pr};
  least(pr);
  D2:=degree(lest1,Y);
  ifD1<D2 then next else Zee:=pr;D1:=D2;fi;od;end:

least:=proc(W) trm1:=W[1];
  trm2:=W[2];
  leadterm(trm1);pptrm1:=leedmon;leedmon:=0;
  leadterm(trm2);pptrm2:=leedmon;leedmon:=0;
  lest1:=lcm(pptrm1,pptrm2);
  end:
```

The next call is to the subroutines "Criterion1" and "Criterion2". These subroutines check a given pair of polynomials to see if they meet the conditions given in Theorems 3.15 and 3.16.

Subroutines Criterion1 and Criterion2

```
criterion2:=proc(V)least(V);
  leastv:=lest1;leadterm(V[1]);pptrm1:=leedmon;
  leedmon:=0;
  leadterm(V[2]);pptrm2:=leedmon;leedmon:=0;
  pptrms:=pptrm1*pptrm2;
  if leastv=pptrms then ck2:=0 else ck2:=1 fi; end:

criterion1:=proc(V) ckg:=0;least(V);leastv:=lest1;
  fg:={};fg:=G minus{V[1],V[2]};
  for t to nops(fg) do
```

```
g1:=fg[t]; leadterm(g1);ldg1:=leedmon;
if divide(leastv,ldg1)= true then
st1:={V[1],g1};st2:={V[2],g1};
gintersect:={};g2intersect:={};
gintersect:= B intersect {st1};
if gintersect= {} then
g2intersect:= B intersect {st2};
if g2intersect={} then
ckg:=ckg+1; fi;fi;fi;od;end:
```

If either condition is met, then the program returns to the subroutine "smallestlcm" to find the next pair of polynomials to consider. If both conditions are not met, then the program forms the Spolynomial of the given pair, calculates the normalform of the Spolynomial with respect to G,performs a "fctrck" on the set G with this polynomial, and finally makes a call to "reduceall" and "newbasis". This last set of commands is performed until the set B is empty, in which case, all the pairs have been checked and the output is a Reduced Groebner Basis.

GENERIC VALIDITY OF A GEOMETRY STATEMENT

Let a geometry statement (S) be given by $u_1,...,u_d$, $x_1,...,x_r$, $h_1,...,h_n$ and g where the $u_1,...,u_d$, are the non-zero coordinates which can be arbitrarily chosen, the $x_1,...,x_r$,are the non-zero coordinates that satisfy the conditions in the theorem, the $h_1,...,h_n$ are the algebraic equations determined by the given hypothesis and g is the algebraic equation that is determined by the conclusion of the given theorem. Recall that V(S) can be decomposed into irreducible components, ie, $V(S) = V(P_1) \cup V(P_2) \cup ... \cup V(P_s) \cup V(R_1) \cup ... \cup V(R_s) \cup V(T_1) \cup ... \cup V(T_l)$ where each of the P_i, R_j, and T_k is a prime ideal and the $V(P_i) = V_1$ and $V(R_j) = V_2$ are the components on which the u's are algebraically independent. The components on which the u's are algebraically independent are called the *general component* or *components general for u.*

Definition 4.1: (S) is *generally true* if g vanishes on all non-degenerate components $V(P_i)$ of V. (S) is *not generally true* if there exists a non-degenerate component $V(P_j)$ for which $g(a) \neq 0$ for all $a \in V(P_j)$. If g vanishes on none of the non-degenerate components, then (S) is said to be *generally false.*

Definition 4.2: A polynomial in Q[u,x] is said to be a *u-polynomial* if it is non-zero and soley in Q[u].

Theorem 4.3: For a given geometry set (S) defined by $h_1 = 0$, $h_2 = 0$,..., $h_n = 0$, there is a u-polynomial s such that any conclusion is true if and only if $s \cdot g \in$ radical$(h_1,h_2,...,h_n)$.

Proof: Let $V(h_1,h_2,...,h_n) = V(P_1) \cup ... \cup V(P_s) \cup V(R_1) \cup ... \cup V(R_s)$ where $V(P_i)$ are all components general and the $V(R_j)$ are the components for which the u's are dependent. Since the u's are dependent on the $V(R_j)$, then for each j there exists a u polynomial s_j such that s_j vanishes on the $V(R_j)$. Let $s = s_1 \cdot s_2 \cdot ... \cdot s_s$.

$\Rightarrow$: Suppose g vanishes on each $V(P_i)$. Since g vanishes on each $V(P_i)$, then sg also vanishes on each $V(P_i)$. But, recall that $V(h_1,h_2,...,h_n) - V(S) \subset V(P_1) \cup V(P_2) \cup ... \cup V(P_s)$. And, thus, sg vanishes on $V(h_1,h_2,...,h_n)$ and therefore by Hilbert's nullstellensatz, $sg \in$ radical$(h_1,h_2,...,h_n)$.

$\Leftarrow$: Suppose $sg \in$ radical$(h_1,h_2,...,h_n)$. This implies that sg vanishes on $V(h_1,h_2,...,h_n)$. Thus, sg vanishes on $V(P_1) \cup ... \cup V(P_s) \cup V(R_1) \cup ... \cup V(R_s)$. But, s consists of u-polynomials only, and therefore does not vanish on $V(P_1) \cup ... \cup V(P_s)$. Since each of the $V(P_i)$ is irreducible, then g must vanish on each $V(P_i)$.

Groebner Basis Method

Let I be the ideal generated by $h_1,h_2,...,h_n$ in Q[u,x]. Let J be the ideal generated by $h_1,...,h_n$ in Q(u)[x].

Lemma 4.4: $I \subset J$.

Proof: Recall that Q[u,x] = Q[u][x] and that $Q[u] \subset Q(u)$. Thus, $Q[u,x] \subset Q(u)[x]$

Lemma 4.5: A polynomial $g \in J$ if and only if there exists a u-polynomial p such that $pg \in I$.

Proof: $\Rightarrow$: Let $g \in J$. Since I is a subset of J then either g is in I or not. Clearly, if $g \in I$, then multiplying g by any u-polynomial p will imply that $pg \in I$ Suppose then that $g \in J - I$. This implies that g consists of only variables in terms of x. However, multiplying g by a u-polynomial p will yield variables in terms of the x's and the u's and, therefore, the product

$pg \in I$.

$\Leftarrow$: Let $pg \in I$ and let p be a u-polynomial. Since $pg \in I$ then by lemma 4.4, $pg \in J$. And since p consists of u's only, then $p \in Q(u)$ and therefore, there exists a polynomial p^{-1}. Multiplying pg by p^{-1} yields the required result, ie, $g \in J$.

Theorem 4.6: A given geometry statement (S) is generally true if and only if $g \in$ Radical(J).

Proof: Suppose (S) is generally true. Then by theorem 4.3 there exists a u-polynomial p

such that pg $\in$ Radical(I). This implies there exists an integer t such that $(pg)^t \in I$. By lemma 4.5 it is known that $g^t \in J$ and hence, g $\in$ Radical(J). Now suppose g $\in$ Radical(J). This implies $g^n \in J$ for some integer n. And again, by lemma 4.5, there exists a u-polynomial p such that $pg^n \in I$ which implies that (S) is generally true.

Theorem 4.6: If g $\in$ J, then (S) is generally true.

Proof: Since J is subset of Radical(J), then if g $\in$ J, then g $\in$ Radical(J) and (S) is generally true by theorem 4.5.

Theorem 4.7: Let z be a new variable not equal to u or x. The Grobner Basis $GB(h_1,...,h_n,zg-1) = \{1\}$ in Q(u)[x,z] if and only if g $\in$ Radical(J).

Proof: Suppose g $\in$ Radical(J) and note that $h_1,...,h_n$ and zg-1 have no common zeros in any extension of Q(u). Thus, by Hilbert's nullstellensatz $(h_1,...,h_n,zg-1) = \{1\}$.

Now suppose $GB(h_1,...,h_n,zg-1) = \{1\}$. This implies there exists $p_i \in Q(u)[x,z]$ such that $p_1h_1 + ... + p_nh_n + p(zg - 1) = 1$. Letting $z = \frac{1}{g}$ and clearing fractions yields $g^n = p_1'h_1 + ... + p_n'h_n$. And, therefore, g $\in$ Radical(J).

The above theorem states that if $GB(h_1,...,h_n,zg-1) = \{1\}$, then (S) is generally true. Using this idea and theorem 4.6, a method can be introduced to show if a given geometry statement is generally true or not. This method is outlined below.

Method 4.8: Fix a purely lexicographical ordering on the monomials in Q(u)[x], ie, $x_1 < x_2 < \ldots < x_n$, then, STEP 1: Compute the grobner basis for $h_1,\ldots h_n$ in Q(u)[x] and use it to reduce g modulo $GB(h_1,\ldots h_n)$. If this reduction is zero, then $g \in J$ and the statement (S) is generally true. If step 1 fails, then appl STEP 2: Compute the grobner basis for $h_1,\ldots h_n$, and gz - 1 in Q(u)[x,z] to see if it is {1}. If it is, then (S) is generally true.

Ceva's Theorem

Giovani Ceva was an Italian mathematician and engineer of the seventeenth century. Ceva's theorem is concerned with line segments joining the vertices of a triangle with the opposite sides. These line segments are called *cevians*. Consider the triangle below in figure 2.

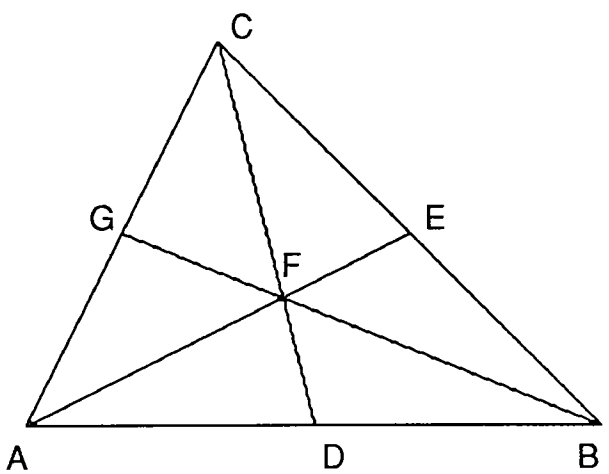

FIGURE 2

The three cevians in this figure are line segments CD, AE, and GB. Ceva's theorem presents the conclusion in the most general case. The computer was used to prove this case and also two corollaries dealing with the altitudes and the medians of a triangle. Consider first the general case as stated in Ceva's theorem.

Ceva's theorem: The three cevians of a triangle are concurrent if and only the following ratio holds:

$$\frac{AG}{GC}\frac{CE}{EB}\frac{BD}{DA} = 1$$

In setting up this problem for the computer, choosing the coordinates for the vertices and intersection was the first problem to consider. Point A was named the origin. Since both points B and C were arbitrary, then they were labeled $(u_1,0)$ and (u_2,u_3), respectively. Point D was then chosen as an arbitrary point on AB and, thus, given the coordinates $(x_1,0)$. Point E was chosen as a point on CB and since it is dependent on points C and B, it was given the coordinates (x_3,x_2). Lines lines CD and AE were then drawn and their intersection labeled F with the coordinates (x_5,x_4). Finally, line BF was drawn and extended to line AC. This intersection was labeled G and given the coordinates (x_7,x_6). This configuration gave a total of seven dependent variables requiring seven equations for calculating the Groebner Basis. The conditions that correspond to the seven equations are as follows:

1) D is not B.
2) F is not C.
3) C, F, and D are collinear
4) A, F, and E are collinear

5) C, E, and B are collinear

6) A, G, and C are collinear

7) G, F, and B are collinear

Note that the order of the conditions corresponds to the order in which the figure was drawn. Colinearity implies that the slopes are the same from , for example, C to A and from G to A. Two points not being the same corresponds to the fact that the distance between them is not zero and from these two ideas the following hypothesis equations were derived.

The order of the equations corresponds to the order of the conditions listed above.

1) $(u_1 - x_1)v_2 - 1 = 0$

2) $(x_5 - u_2)v_1 - 1 = 0$

3) $u_3(x_5 - x_1) - x_4(u_2 - x_1) = 0$

4) $x_2x_5 - x_3x_4 = 0$

5) $u_3(x_3 - u_1) - x_2(u_2 - u_1) = 0$

6) $u_3x_7 - u_2x_6 = 0$

7) $x_6(x_5 - u_1) - x_4(x_7 - u_1) = 0$

An ordering on the variables was given as the list $X = [x_1, x_2, x_3, x_4, x_5, x_6, x_7]$ which implies in MAPLE the following ordering: $x_1 > x_2 > \ldots > x_7$. This ordering was not that important as the same result was obtained when the ordering was reversed. However, it should be noted that Chou states that a particular ordering in most problems will determine the speed of calculation. A call to the Groebner package in MAPLE was then made, and the following Groebner Basis was calculated.

g :=

$$[(v1\,u1 + v2\,u2\,v1\,u1 + u1\,v2 - 1 - u1^2\,v2\,v1)\,x7 - v2\,u2^2\,v1\,u1 - v2\,u2\,u1 + v2\,u2\,v1\,u1$$

$$- v1\,u1\,u2,$$

$$- v2\,u3\,u2\,v1\,u1 - u1\,v2\,u3 + u1^2\,v2\,u3\,v1 - u3\,v1\,u1$$

$$+ (v1\,u1 + v2\,u2\,v1\,u1 + u1\,v2 - 1 - u1^2\,v2\,v1)\,x6,$$

$$x5\,v1 - u2\,v1 - 1,$$

$$- v2\,u3\,u2\,v1 - v2\,u3 + u1\,v2\,u3\,v1 - u3\,v1 + (v2\,u2\,v1 - u1\,v2\,v1 + v1)\,x4,$$

$$(v2\,u2\,v1\,u1 - u1^2\,v2\,v1 + v1\,u1 + 1)\,x3 + v2\,u2\,v1\,u1^2 - u1 - v2\,u2^2\,v1\,u1 - v2\,u2\,u1 + u1^2\,v2$$

$$- v1\,u1\,u2,$$

$$(v2\,u2\,v1\,u1^2 - u1^2\,v2\,v1 + v1\,u1 + 1)\,x2 - v2\,u3^2\,u2\,v1\,u1 - u1\,v2\,u3 + u1^2\,v2\,u3\,v1 - u3\,v1\,u1,$$

$$u1\,v2 - x1\,v2 - 1]$$

It was then necessary to determine the conclusion equation so that this equation could be reduced modulo g, the Groebner Basis. However, all equations must be equal to zero, therefore the actual conclusion was rewritten in the form given below. Note, the lengths of the line segments were tpyed in using the distance formula and then the conclusion equation was squared to clear any non-integer exponents.

$$AG := (x6^2 + x7^2)^{1/2}$$

$$GC := ((u2 - x7)^2 + (u3 - x6)^2)^{1/2}$$

$$CE := ((u3 - x2)^2 + (u2 - x3)^2)^{1/2}$$

$$EB := (x2^2 + (x3 - u1)^2)^{1/2}$$

$$DB := u1 - x1$$

$$AD := x1$$

$$c := (x6^2 + x7^2)((u3 - x2)^2 + (u2 - x3)^2)(u1 - x1)^2$$

$$- ((u2 - x7)^2 + (u3 - x6)^2)(x2^2 + (x3 - u1)^2)x1^2$$

$$F := 0$$

A call to reduce c modulo g was made and labeled F. As seen above, this reduction was zero, and hence, then theorem is generally true.

To prove the converse, the order in which te points were chosen were changed and therefore, the actual construction of the triangle was changed. However it is possible to consider figure 1 if the points labeled E and F are interchanged. Thus, with the new figure in mind, consider the following construction.

To begin, point D was chosen on AB. The line CD was then chosen and a point E was chosen such that E was not C. The line AE was then drawn and extended to intersect CB. This intersection was labeled F. The line from B to E was then drawn to determine the point G on AC; however the collinearity of G, B, and E were then used as the conclusion. From this construction the following seven conditions were determined.

1. D is not B
2. E is not C
3. E is on CD
4. F is on AE
5. F is on BC
6. G is on AC

The seventh condition refers to the the ratio stated in the theorem.

The corresponding equations are as follows.

$$h2 := (x2 - u3)\, v2 - 1$$

$$h3 := u3\,(x3 - x1) - (u2 - x1)\, x2$$

$$h4 := x5\, x2 - x4\, x3$$

$$h5 := (x5 - u1)\, u3 - (u2 - u1)\, x4$$

$$AG := (x7^{2} + x6^{2})^{1/2}$$

$$GC := ((x7 - u2)^{2} + (x6 - u3)^{2})^{1/2}$$

$$CF := ((u2 - x5)^{2} + (u3 - x4)^{2})^{1/2}$$

$$FB := ((x5 - u1)^{2} + x4^{2})^{1/2}$$

$$DB := u1 - x1$$

$$FB := ((x5 - u1)^{2} + x4^{2})^{1/2}$$

$$DB := u1 - x1$$

$$AD := x1$$

$$h7 := (x7^{2} + x6^{2})\,((u2 - x5)^{2} + (u3 - x4)^{2})\,(u1 - x1)^{2}$$

$$- ((x7 - u2)^{2} + (x6 - u3)^{2})\,((x5 - u1)^{2} + x4^{2})\,x1^{2}$$

$$h1 := (x1 - u1)\, v1 - 1$$

$$h6 := x7\, u3 - x6 - u2$$

A call was then made to form the Groebner Basis and reduce the conclusion modulo the formed set. However, in this case the reductoin was not to zero and,therefore, the second step in the proving process was used. Recall, this required that the conclusion be multiplied by a new variable, say z, and subtract 1 from it to form a new equation. This

new equation was then added to the set of hypothesis equations and then a call to form a Groebner Basis of this set was made. In this case, as can be seen below, the final reduction is equal to one and, therefore, the conclusion is true. It should be noted that in Chou's research, it was only necessary to use step one in method 4.8; however, it was necessary in this case to use step 2 and thus, the development of the theory as stated at the beginning of chapter 4 was appropriate.

• c:=(x7-u1)*x2-(x3-u1)*x6;

hyp1:={h1,h2,h3,h4,h5,h6,h7,z*c-1}:g1:=gbasis(hyp1,X,plex);

g1 := [1]

Corollary 1: The altitudes of a triangle are concurrent. Consider figure three.

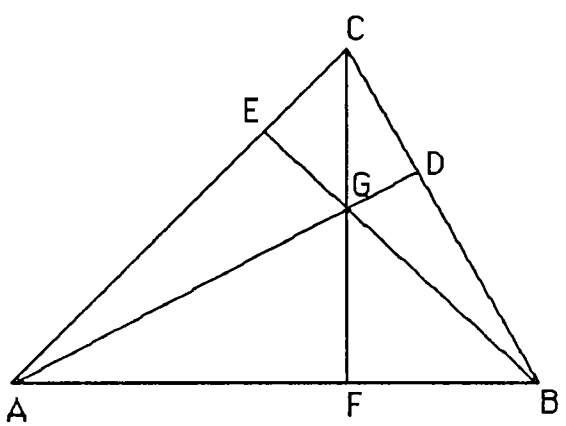

FIGURE 3

Because this corollary is dealing with right angles an appropriately chosen coordinate system will eliminate many of the dependent variables and allow for fewer equations to manipulate. Thus, by letting F be the origin points A, B, C, and G will fall on the x and y axes. A is given the coordinates $(u_1,0)$, B is given the coordinates $(u_2,0)$ and C is labeled $(0,u_3)$. The three altitudes are then drawn labeling the three intersections E, D, and F. However, the coordinates for F have been determined already leaving only D and E to be

labeled. Thus, D is labeled (x_1,x_2) and E (x_3,x_4). Since their intersection falls on the y axis, G is labeled $(0,x_5)$. This gives a total of five variables implying there must be five equations. The conditions that correspond to these five equations are: (1). A, E, and C are collinear. (2). C, D, and B are collinear. (3). AD is perpendicular to CB. (4) AC is perpendicular to EB. And (5) C, G, and F are collinear. Note that condition five is taken care of by the choice of the coordinate system which allows only four equations. These equations are:

1). $h_1 = u_3x_3 + u_1x_4 - u_1u_3 = 0$

2). $h_2 = u_3x_1 + u_2x_2 - u_2u_3 = 0$

3). $h_3 = u_2x_1 + u_3x_2 - u_1u_2 = 0$

4). $h_4 = u_1x_3 + u_3x_4 - u_1u_2 = 0$

An ordering on the variables was given as $X:=[x_1, x_2, x_3, x_4, x_5]$. Again, a call to MAPLE was made and the Groebner Basis was calculated. The resulting list is given below where g represents the Groebner Basis generated by the hypothesis. The command to the computer is listed followed by the actual output.

```
hyp:={h1,h2,h3,h4}:X:=[x1,x2,x3,x4,x5]:with(grobner):g:= gbasis(hyp,X,plex);
```

```
g :=

     2   2          2        2   2   2              2
[(u3  - u2 ) x1 - u3  u2 + u1 u2 , (u3  - u2 ) x2 - u3 u1 u2 + u2  u3,

     2   2          2        2       2   2                      2
 (u3  - u1 ) x3 - u3  u1 + u1  u2, (u3  - u1 ) x4 - u3 u1 u2 + u1  u3]
```

The conclusion is given in the following form. It is necessary to square each term so that the equation will be in polynomial form. The lengths of each segment were typed in and then the computer was used to generate the actual equation. Note that it was not necessary to expand the polynomial. Again, the commands are listed followed by the

computer's output. The last two lines of the output show the call to reduce the conclusion, given as c in this case, modulo g, the above generated Groebner Basis.

```
• AE:=(x4^2+(x3-u1)^2)^(1/2);EC:=(x3^2+(u3-x4)^2)^(1/2);
  CD:=(x1^2+(u3-x2)^2)^(1/2)
                                   2              2 1/2
                        AE := (x4  + (x3 - u1) )

                                    2              2 1/2
                        EC := (x3  + (u3 - x4) )


                                    2              2 1/2
                        CD := (x1  + (u3 - x2) )

• FB:=u2;AF:=u1;DB:=(x2^2+(x1-u2)^2)^(1/2);
                              FB := u2

                              AF := u1

                                    2              2 1/2
                        DB := (x2  + (x1 - u2) )

•

• c:=(AE*CD*FB)^2-(EC*DB*AF)^2;
          2              2     2              2    2
c := (x4  + (x3 - u1) ) (x1  + (u3 - x2) ) u2

        2              2     2              2    2
  - (x3  + (u3 - x4) ) (x2  + (x1 - u2) ) u1

• f:=normalf(c,g,X,plex);
                                 f := 0
```

Since the result is zero, then the statement is generally true.

Corollary 2: The medians of a triangle are concurrent.

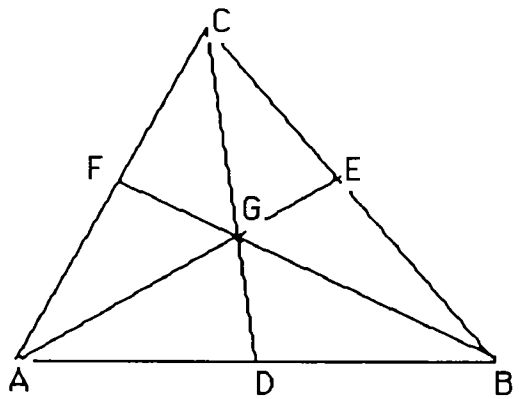

FIGURE 4

In this case, as in the most general case, point A is the origin, B is $(u_1,0)$, and C is (u_2,u_3). D is given the coordinates $(x_5,0)$, E is labeled (x_1,x_2) F is labeled (x_3,x_4), and G is labeled (x_6,x_7). Since G does not play a role in either the hypothesis or conclusion, it is not necessary to write equations involving either of these variables. The conditions then are as follows. (1). F is on AC. (2) E is on CB. (3) D is on AE, which is implied by the choice of the coordinate system and therefore no equation is needed to describe this. (4) AF = FC. (5) CE = BE. And (6) AD = BD. The equations for equality come directly from the midpoint formula, and since the points are collinear only one equation per midpoint is needed to describe this condition. Below, the entire print out for this particular problem. It should be noted that, as previously done, the given equations correlate to the stated conditions above.

```
h1:=u2*x4-u3*x3;h2:=u3*x1-u1*u3-(u2-u1)*x2;h3:=2*x4-u3;
h4:=2*x2-u3;h5:=2*x5-u1;
```

- `hyp:={h1,h2,h3,h4,h5};grob:=gbasis(hyp,X,plex);`
- `AB:=(x3^2+x4^2)^(1/2);BC:=((u2-x3)^2+(u3-x4)^2)^(1/2);AF:=x5;`
- `CD:=((u3-x2)^2+(u2-x1)^2)^(1/2);DE:=(x2^2+(u1-x1)^2)^(1/2);FE:=u1-x5;`

• c:=(AB*CD*FE)^2-(BC*DE*AF)^2;

• f:=normalf(c,grob,X,plex);

•

$$h1 := u2\ x4 - u3\ x3$$

$$h2 := u3\ x1 - u1\ u3 - (u2 - u1)\ x2$$

$$h3 := 2\ x4 - u3$$

$$h4 := 2\ x2 - u3$$

$$h5 := 2\ x5 - u1$$

hyp :=

{u3 x1 - u1 u3 - (u2 - u1) x2, 2 x4 - u3, 2 x2 - u3, 2 x5 - u1,

u2 x4 - u3 x3}

grob := [2 x1 - u1 - u2, 2 x2 - u3, 2 x3 - u2, 2 x4 - u3, 2 x5 - u1]

$$AB := (x3^2 + x4^2)^{1/2}$$

$$BC := ((u2 - x3)^2 + (u3 - x4)^2)^{1/2}$$

$$AF := x5$$

$$CD := ((u3 - x2)^2 + (u2 - x1)^2)^{1/2}$$

$$DE := (x2^2 + (u1 - x1)^2)^{1/2}$$

$$FE := u1 - x5$$

$$c := (x3^2 + x4^2)((u3 - x2)^2 + (u2 - x1)^2)(u1 - x5)^2$$

$$- ((u2 - x3)^2 + (u3 - x4)^2)(x2^2 + (u1 - x1)^2)\,x5^2$$

$$f := 0$$

ENDNOTES

1. Shang-Ching Chou , *Mechanical Geometry Theorem Proving,* (D. Reidel 1988), 5.

2. Shang-Ching.Chou, *Mechanical Geometry Theorem Proving,* (D. Reidel 1988),5-6

3. Bartel Leendert van der Waerden, *Modern Algebra,* the English Edition, (Frederick Unger, 1950), 53.

4. B. Buchberger, Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory, Chapter 6 in *Recent trends in Mulitdimensional Systems Theory,* N.K.Bose (ed.) (D. Reidel Publ. Comp. 1985), 186.

REFERENCES

1. B. Buchberger, Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory, Chapter 6
in *Recent trends in Mulitdimensional Systems Theory,* N.K.Bose (ed.) D. Reidel Publ. Comp.
1985

2. S.C.Chou, , *Mechanical Geometry Theorem Proving,* D. Reidel 1988

3. H.R. Jacobs, *Geometry,* W.H. Freeman and Co., 1987, (477-478)

4. M.B. Monagan, *MAPLE Reference Manual,* Brooks/Cole, 1988

5. B.L. Van Der Waerden, *Modern Algebra,* the English Edition, Frederick Unger, 1950.