

## Lehigh University Lehigh Preserve

---

### Theses and Dissertations

---

1-1-1982

# Real closed fields.

Hassan Abdull Yousef

Follow this and additional works at: <http://preserve.lehigh.edu/etd>

 Part of the [Mathematics Commons](#)

---

### Recommended Citation

Yousef, Hassan Abdull, "Real closed fields." (1982). *Theses and Dissertations*. Paper 2325.

This Thesis is brought to you for free and open access by Lehigh Preserve. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Lehigh Preserve. For more information, please contact [preserve@lehigh.edu](mailto:preserve@lehigh.edu).

REAL CLOSED FIELDS

by

Hassan Abdull Raheem Deeb Yousef

A Thesis

Presented to the Graduate Committee

of Lehigh University

in Candidacy for the Degree of

Master of Science

in

Mathematics

Lehigh University

1982

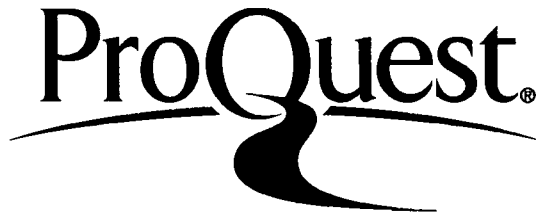
ProQuest Number: EP76601

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



ProQuest EP76601

Published by ProQuest LLC (2015). Copyright of the Dissertation is held by the Author.


All rights reserved.

This work is protected against unauthorized copying under Title 17, United States Code  
Microform Edition © ProQuest LLC.

ProQuest LLC.  
789 East Eisenhower Parkway  
P.O. Box 1346  
Ann Arbor, MI 48106 - 1346

This thesis is accepted and approved in partial fulfillment of the requirements for the degree of Master of Science.

August 30, 1982  
(Date)

Professor in Charge 

Chairman of Department

To the memory of my father.

## ACKNOWLEDGEMENT

I wish to express my appreciation to my advisor, Professor E. F. Assmus, for his constant encouragement and advice during the preparation of my thesis.

I would like to thank Bir Zeit University for its support in the form of a scholarship while I have been attending Lehigh University. Thanks also to America Mideast Educational and Training Services and Student Aid International for sponsoring my.

I would like to thank Jeanne Loosbrock for the time she spent typing the manuscript.

My special thanks to my parents and my wife for their patience, constant encouragement, love, faith and understanding.

## TABLE OF CONTENTS

	<u>Page</u>
Certificate of Approval	ii
Acknowledgement	iv
Table of Contents	v
Abstract	1
Introduction	2
1. Ordered Fields and Formally Real Fields	5
2. Real Closed Fields	12
3. Sturm's Theorem	18
4. Extension Theorems for Formally Real Fields	25
5. Real Closure for Formally Real Fields	27
6. Real Algebraic Numbers	31
7. Positive Definite Rational Functions	34
8. Formalized Euclidean Algorithm and Sturm's Theorem	42
9. Elimination Procedures. Resultants	50
10. The Decision Method for an Algebraic Curve	59
11. Bibliography	67
12. Vita	68

## ABSTRACT

The theory of formally real fields was introduced by Artin and Schreier in 1926. Artin and Schreier noticed that in the field of real numbers the only relation of the form  $\sum_{i=1}^n x_i^2 = 0$  is the trivial one  $0+0+\dots+0$ ; this observation led Artin and Schreier to call any such field formally real.

In this thesis I consider the development of the theory of formally real fields from its beginning in 1926 up to the results of Tarski. I treat its application to the solution of Hilbert's 17th problem (which was solved by Artin using the theory) and to the solution in a real closed field of a system of equations, inequations and inequalities in several variables.



## INTRODUCTION

In this thesis I consider the theory of formally real fields developed by Artin and Schreier in 1926. Artin and Schreier noticed that the only relations of the form  $\sum_1^n \alpha_i^2 = 0$  in the field of real numbers are the trivial ones  $0+0+\dots+0 = 0$ ; this observation led them to call any field with this property "formally real." The formally real fields were characterized by the fact that  $-1$  is not a sum of squares of elements in the field. The deeper properties of formally real fields concern real closed fields which are the formally real fields maximal in their algebraic closure. Real closed fields were characterized by Artin and Schreier as those fields of finite degree under their algebraic closure; this degree is 2 and the algebraic closure can be obtained by the adjunction of  $\sqrt{-1}$ .

If  $F$  is a real closed field, then it can be ordered, the positive elements being the squares in  $F$ . Any formally real field can be ordered since it can be imbedded in a real closure. The classical application of the Artin-Schreier theory is to the problem of determining which elements of a given field are representable as sums of squares of elements of that field. For finite algebraic extensions of the rationals the problem has a simple solution which is due to Hilbert and Landau. The

solution says that if  $K$  is a finite-dimensional extension field of the rationals and if  $f_1, f_2, \dots, f_r$  ( $r > 0$ ) are the different isomorphisms of  $K/Q$  into the field of algebraic numbers, then an element  $a \neq 0$  of  $K$  is a sum of squares in  $K$  if and only if  $f_i(a) > 0$  for  $i = 1, 2, \dots, r$ . The theory of formally real fields led Artin and Schreier to the solution of Hilbert's 17th problem, which says that if  $Q$  is a rational function of  $n$  variables with rational coefficients such that  $Q(x_1, \dots, x_n) \geq 0$  for all real  $(x_1, \dots, x_n)$  for which  $Q$  is defined, then  $Q$  is necessarily a sum of squares of rational functions with rational coefficients.

After Artin came Abraham Robinson. He gave another derivation of Artin's main theorems and obtained various improvements and generalizations of Artin's results in 1955.

The most important development of the theory of formally real fields subsequent to the original work of Artin and Schreier is the metamathematical principle due to Tarski which asserts that any elementary statement of algebra which is valid for one real closed field is valid for every real closed field. This is based on an algorithm for deciding the solvability in a real closed field of a finite system of polynomial equations and inequalities with rational coefficients, such a decision method was given originally by Tarski. We are including

an alternative one due to Seidenberg.

In my thesis I introduce the theory of formally real fields starting in §1 with ordered fields, formally real fields, and the characterization that  $F$  is formally real if and only if  $-1$  is not a sum of squares in  $F$ . In §2 I introduce real closed fields developing their properties. In §3 I introduce a classical result, Sturm's theorem. Before Sturm's theorem was known there were several ways to estimate the roots of an equation  $f(x) = 0$ , but the question of finding the exact number of real roots was open and it was not until 1836 that this question was solved completely by Sturm (his solution was announced in 1829 and was first published in 1835). In §3 we derive Sturm's theorem following rather closely Weber's exposition in his *Lehrbuch der Algebra* (1898) Vol. 1, pp. 301-313. In §4 and §5 we shall consider the theorem on the existence of formally real fields and of real closed algebraic extensions of given formally real field. We conclude that a field can be ordered if and only if it is formally real. In §6 we consider the real algebraic numbers which are the real closure of the rationals. We give a proof of the theorem on the number of distinct ordering of a finite-dimensional extension of the rationals and we apply this theorem to obtain the theorem of Hilbert and Landau which gives a necessary and sufficient condi-

tion that an element of this field is a sum of squares of elements of the field. In §7 we consider the positive definite rational functions and give Artin's theorem which solves Hilbert's 17th Problem. In §8 we shall show that we can obtain a version of Sturm's theorem for any equation whose coefficients are parameters that take on values in a real closed field. This will be based on a parametrized version of the Euclidean algorithm for determining the greatest common division of polynomials. In §9 we consider the theory of elimination of variables in systems of equations and inequations with coefficients in any field, and in the last section, §10, we give a method due to Seidenberg for deciding the solvability of  $f(x,y) = 0$  in a real closed field and an extension of the decision procedure for  $f(x,y) = 0$  restricted by  $g(x) \neq 0$ .

## 1. Ordered Fields and Formally Real Fields

Definition 1.1. An ordered field is a field  $F$  together with a subset  $P$  such that we have the following: (i)  $0 \notin P$ ; (ii) if  $x \in F$  then either  $x \in P$  or  $x=0$  or  $-x \in P$ ; and, finally, (iii)  $P$  is closed under addition and multiplication (i.e.  $x, y \in P \Rightarrow xy \in P$  and  $x+y \in P$ ).

Remarks: (i) Since any field contains at least two elements we have that  $P \neq \emptyset$ . (ii) If we define  $N = \{-x/x \in P\}$  then from (ii) above if  $x \in F$  then  $x \in P$  or  $x=0$  or  $x \in N$  and  $P \cap N = \emptyset$  (if  $x \in P \cap N$  then  $-x \in P \cap N$  so  $x+(-x) = 0 \in P$ , a contradiction). Also,  $0 \notin N$  so  $F$  is the disjoint union of  $N, \{0\}, P$ . (iii) We can define an order relation in the ordered field  $(F, P)$  as follows:  $a > b$  if  $a-b \in P$ . Then for any  $x, y \in F$  we have that one and only one of the following holds: either  $x > y$  or  $x=y$  or  $y > x$ , where  $x-y \in P$  or  $x-y=0$  or  $-(x-y) = y-x \in P$ , respectively. We note also that the relation  $(>)$  in any ordered field  $(F, P)$  satisfies the following properties:

- (1)  $x > 0 \Rightarrow x^{-1} > 0$ .
- (2)  $x > y \Rightarrow x+z > y+z$  for every  $z \in F$ .
- (3)  $x > y \Rightarrow xz > yz$  for every  $z \in P$ .
- (4)  $x > y \Rightarrow -y > -x$
- (5)  $x > y, y > z \Rightarrow x > z$  where  $x, y, z \in F$ .
- (6)  $x \in F, x \neq 0 \Rightarrow x^2 \in P$ .
- (7)  $x > y > 0 \Rightarrow y^{-1} > x^{-1} > 0$ .

Proof:

- (1) Otherwise  $x^{-1} < 0$  and  $-x^{-1} > 0$ , which implies that  $(x)(-x^{-1}) = -1 > 0$ , a contradiction with (6) below.
- (2) This follows from  $(x+z) - (y+z) = x-y > 0$
- (3) This follows from  $xz - yz = z(x-y) > 0$  since  $z > 0$  and  $x-y > 0$ .
- (4)  $-y - (-x) = x-y > 0$  so  $-y > -x$ .
- (5) Since  $x-y > 0, y-z > 0$ , then  $x-z = (x-y) + (y-z) > 0$ .
- (6)  $x \in F, x \neq 0$  implies  $x^2 = x \cdot x = (-x)(-x) \in P$ , since either  $x \in P$  or  $-x \in P$  and  $P$  is closed under multiplication.
- (7) If  $x > y > 0$ , then if  $x^{-1} > y^{-1}$  this implies that  $x^{-1} - y^{-1} > 0$  and since  $xy > 0$  so  $xy(x^{-1} - y^{-1}) = y - x > 0$  hence  $y > x$ , a contradiction.

Now  $1 = 1^2 > 0$  by (6) and if we have  $x_1, \dots, x_n$ , not all of them are zero, then  $\sum_{i=1}^n x_i^2 > 0$ , so we conclude  $1^2 + 1^2 + \dots + 1^2 = 1 + 1 + \dots + 1 > 0$ . which means that any ordered field must be of characteristic zero.

Note: If we are given a field  $F$  and a relation  $>$  on  $F$  satisfying the following properties:

- (i) For  $a, b \in F$  then one and only one of the following holds:  $a > b, a = b, b > a$ .
- (ii)  $a > b, b > c$  implies  $a > c, a, b, c \in F$ .
- (iii)  $a > b$  implies  $a + c > b + c$  and  $ad > bd$  for every  $c, d \in F$  and  $d > 0$ .

Then by defining  $\mathbb{R} \subseteq F$  by  $P = \{x \in F / x > 0\}$  we can conclude that  $(F, P)$  is an ordered field. Moreover, the relation

> defined by this ordered field is the same as the relation we started with, and this can be seen by direct verification of the conditions in the definition of an ordered field.

If we define  $|x| = x$  when  $x \geq 0$  or  $x=0$  and  $|x| = -x$  otherwise, then we can see that we have the triangle inequality  $|a+b| \leq |a|+|b|$   $a, b \in F$  and  $|ab| = |a||b|$   $a, b \in F$ . The proofs are very easy taking into consideration the cases  $a \geq 0, b \geq 0$ , or  $a \geq 0, b < 0$ , or  $a < 0, b \geq 0$ , or  $a < 0, b < 0$ .

Note: If  $(F, P)$  is an ordered field and  $F'$  is a subfield of  $F$ , then by defining  $P' = P \cap F'$  we have that  $(F', P')$  is an ordered field. The ordering of  $F'$  is called the induced ordering.

Deductions:

(1)  $-1 \neq \sum_{i=1}^n x_i^2$  in any ordered field  $(F, P)$  where  $x_i \in F$  otherwise  $1^2 + \sum_{i=1}^n x_i^2 = 1 + (-1) = 0$  which contradict what we proved before, that  $\sum_{i=1}^n x_i^2 > 0$  if not all  $x_i$  are zero. In particular  $-1 \neq a^2$  where  $a \in F$ .

(2) Any ordered field  $(F, P)$  is dense in itself, that is for every  $a, b \in F$   $a < b$  there exists  $c \in F$  such that  $a < c < b$  (i.e.  $c = \frac{a+b}{2}$ ).

Definition 1.2. Let  $(F, P)$  and  $(F', P')$  be two ordered fields. An order isomorphism is a field isomorphism  $f: F \rightarrow F'$  such that  $f(P) \subset P'$ .

From this definition we conclude that if  $f$  is an order isomorphism then  $f(P) = P'$  since if  $x \in P$  then  $-x \in P$

and  $f(-x) = -f(x) \in P$  which implies  $f(N) \subset N'$  and, since  $f$  is bijective,  $f(P) = P'$ . We say that a field  $F$  is orderable if we can find a subset  $P$  of  $F$  such that  $(F, P)$  is an ordered field. Since in any ordered field  $-1 \neq a^2$ , i.e.,  $\sqrt{-1} \notin F$ ,  $\mathbb{C}$ , the field of complex numbers, cannot be ordered.

Examples: (1)(Veblen) If  $F$  is a field such that  $-1$  is not a square in  $F$  and the sum of two non-squares in  $F$  is a non-square, then  $F$  can be ordered in one and only one way.

Proof: If we let  $P = \{a \in F / a \neq 0 \text{ and } a \text{ is a square in } F\}$  then  $(F, P)$  is an ordered field since

(i)  $0 \in P$  by definition.

(ii) Let  $a \in F$  with  $a \neq 0$ . Then we must show  $a \in P$  or  $-a \in P$ .

If  $a$  is a square in  $F$ , then  $a \in P$ ; otherwise  $-a$  is a square in  $F$  because, if not, then  $a$  is not a square and  $-a$  is not a square implies  $a + (-a) = 0$  is a non-square in  $F$ , a contradiction. So either  $a \in P$  or  $-a \in P$ .

(iii) If  $a, b \in P$  then  $-b \notin P$  and if  $a + b \notin P$  then  $(a + b) + (-b) = a \in P$ , a contradiction; also  $ab \in P$  since  $a = x^2$ ,  $b = y^2$  then  $ab = x^2 y^2 = (xy)^2 \in P$ , so  $(F, P)$  is ordered field. This ordered field is unique since if  $(F, P')$  is another ordering then  $P = P'$  since (1)  $P \subset P'$  because  $P$  consists of squares and all squares are in  $P'$ ; (2)  $P' \subset P$  because



if  $a \in P'$  and  $a \notin P$  then  $-a \in P \subset P'$  which implies  $a + (-a) = 0 \in P'$ , a contradiction.

(2) In any ordering of  $Z$ ,  $1, 1+1, \dots$  all must be positive. Since these numbers and their negatives together with  $0$  exhaust all  $Z$ , we see that  $Z$  has only its natural order. From this we conclude also the rationals  $Q$  have only their natural order: I claim that if  $\frac{a}{b} \in Q$  then  $\frac{a}{b} > 0$  is equivalent to  $ab > 0$  since  $\frac{a}{b} > 0$  implies  $(\frac{a}{b})(b^2) = ab > 0$  and conversely  $ab > 0$  implies  $\frac{a}{b} = (ab)(\frac{1}{b^2}) > 0$ . Since  $Z$  has but one order, so does  $Q$ .

(3) There are two orderings for  $Q(\sqrt{2})$ , first by considering  $Q(\sqrt{2}) \subset R$  and giving  $Q(\sqrt{2})$  the induced ordering, and also by considering the isomorphism  $\phi: Q(\sqrt{2})$  into  $R$  such that  $\phi(a+b\sqrt{2}) = a-b\sqrt{2}$  we can define the second order from the fact that the image of  $\phi$  is a subfield of  $R$ . So  $a+b\sqrt{2}$  is positive if and only if  $\phi(a+b\sqrt{2}) > 0$  in  $R$  is an order.

(4) If  $F$  is an ordered field,  $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$ , and  $M = \max\{1, |a_1| + \dots + |a_n|\}$ , then  $|u| > M$  implies  $|f(u)| > 0$ . To prove this we see that

$$|f(u)| = |u^n + a_1 u^{n-1} + \dots + a_n| \geq |u|^n - |a_1 u^{n-1} + \dots + a_n|$$

$$\geq |u|^n - (|a_1| |u|^{n-1} + \dots + |a_n|) \dots$$

(1)

If  $M=1$ , then  $|u| > M$  means  $u = 1+k, k > 0$  then (1) implies

$$|f(u)| \geq (1+k)^n - (|a_1| (1+k)^{n-1} + \dots + |a_n| (1+k)^n)$$

$$= (1+k)^n (1 - (|a_1| + \dots + |a_n|)) > 0$$

If  $M = |a_1| + \dots + |a_n|$ , then  $|u| > M$  means  $|u| = |a_1| + \dots + |a_n| + \ell$ , ( $\ell > 0$ ), so (1) implies  $|f(u)| \geq (|a_1| + \dots + |a_n| + \ell)^n - |a_1| + \dots + |a_n| + \ell)^{n-1} + \dots + |a_n| (|a_1| + \dots + |a_n| + \ell)^{n-1} = (|a_1| + \dots + |a_n| + \ell)^{n-1} \cdot \ell > 0$ .

This property implies that the roots of  $f(x)$  in  $F$  are contained in the interval  $[-M, M]$ .

We know that if  $(F, P)$  is an ordered field and if  $x_1, \dots, x_n \in F$  are not all zero, then  $\sum_{i=1}^n x_i^2 \neq 0$ . The converse is obvious and we are led to the following definition.

Definition 1.3. A field  $F$  is called formally real if  $\sum_{i=1}^n x_i^2 = 0$  implies  $x_i = 0$   $i = 1, \dots, n$ .

Remark:  $F$  is formally real if  $-1$  is not a sum of squares in  $F$ .

Proof: Assume that  $-1 = \sum_{i=1}^n x_i^2$ . Then  $1^2 + \sum_{i=1}^n x_i^2 = 0$ , and  $F$  is not formally real. On the other hand, if  $F$  is not formally real, then there are  $x_1, \dots, x_n \in F$ , not all zero, with  $x_1^2 + \dots + x_n^2 = 0$ . Assume  $x_1 \neq 0$ . If we multiply by  $(x_1^{-1})^2$   $(x_1^{-1}x_2)^2 + \dots + (x_1^{-1}x_n)^2 = -1$ . So  $-1$  is a sum of squares.

Definition 1.4. For  $F$  any field let  $\Sigma(F)$  be the set of all sums of squares of elements of  $F$ .

We notice that  $1 \in \Sigma(F)$  and  $\Sigma(F)$  is closed under addition and multiplication and if  $a \in \Sigma(F)$  then  $a^{-1} \in \Sigma(F)$  since  $a^{-1} = (a^{-1})^2 \cdot a$ .

Thus we can state the previous result for formally real fields as:  $F$  is formally real iff  $-1 \notin \Sigma(F)$ .

Property: If  $F$  is not formally real and not of characteristic 2 then  $\Sigma(F) = F$ .

Proof: We can write  $a \in F$  as  $a = (\frac{1+a}{2})^2 + (-1)(\frac{1-a}{2})^2$  since  $-1 \in \Sigma(F)$  and  $\Sigma(F)$  is closed under addition and multiplication.

Corollary: In any finite field any element is a sum of squares.

Fact: If  $F$  is a formally real field and  $t$  is any transcendental then  $F(t)$  is formally real.

Proof: If  $-1 = \sum_{i=1}^n \phi_i(t)^2$  where  $\phi_i(t) \in F(t)$  then if we substitute  $t=1$  we have  $-1 = \sum_{i=1}^n \phi_i(1)^2$  which is contradiction of the formal reality of  $F$  since  $\phi_i(1) \in F$ .

## 2. Real Closed Fields

Definition 2.1. A field  $F$  is called real closed if  $F$  is formally real and no proper algebraic extension of  $F$  is formally real.

Theorem 2.1. Let  $F$  be a real closed field then if  $x \in F$  either  $x$  is a square in  $F$  or  $-x$  is a square.

Proof: Assume  $x \in F$  and  $x$  is not a square. Then  $\sqrt{x} \notin F$  and  $F(\sqrt{x})$  is proper algebraic extension of  $F$ . So  $F(\sqrt{x})$  is not formally real.  $-1 = \sum_{i=1}^n (a_i + b_i \sqrt{x})^2$   $a_i, b_i \in F$  or  
 $-1 = \sum_{i=1}^n a_i^2 + 2\sqrt{x} \sum_{i=1}^n a_i b_i + x \sum_{i=1}^n b_i^2$ . Now  $\sum_{i=1}^n a_i b_i = 0$  since otherwise  $\sqrt{x} \in F$ . So  $-1 = \sum_{i=1}^n a_i^2 + x \sum_{i=1}^n b_i^2$ ; also,  $\sum_{i=1}^n b_i^2 \neq 0$

since otherwise  $-1 = \sum_1^n a_i^2$ . Therefore  
 $-x = (1 + \sum a_i^2)(\sum b_i^2)^{-1}$  and  $-x \in \Sigma(F)$  by the properties of  
 $\Sigma(f)$ .  $-1 \notin \Sigma(F)$  implies  $x \notin \Sigma(F)$  since otherwise  $x^{-1} \in \Sigma(F)$   
and  $(x^{-1})(-x) = -1 \in \Sigma(F)$ , an impossibility. Therefore  
 $x \notin \Sigma(F)$  and we have proved that  $x$  not a square implies  
 $x \notin \Sigma(F)$  which is equivalent to  $x \in \Sigma(F)$  implies  $x$  is a  
square, we proved  $x$  not a square implies  $-x \in \Sigma(F)$ , so  
 $x$  is a square or  $-x$  is a square.

Theorem 2.2. Any real closed field can be ordered in one  
and only one way and any automorphism of such a field is  
an order automorphism.

Proof: Let  $P = \{x/x \text{ is a square in } F, x \neq 0\}$  then we can  
check easily that  $(F, P)$  is an ordered field since  $0 \notin P$   
from definition and if  $x \in F$  by the last theorem either  $x$   
is a square or  $-x$  is a square so  $x \in P$  or  $-x \in P$  and finally  
if  $x, y \in P$  (i.e. squares) then  $xy \in P$  and  $x+y \in P$  since if  
 $x+y \notin P$  then  $-(x+y)$  is a square and so  $(-x-y)+(y) = -x$   
is a square which is a contradiction since we have as-  
sumed already that  $x$  is a square.

The ordering is unique since if  $(F, P')$  is another or-  
der then  $x \in P$  implies  $x = a^2$  so  $x \in P'$  and  $P \subset P'$ . On the other  
hand, if  $P' \not\subset P$  then let  $x \in P', x \notin P$ . Then  $-x$  is a square  
so  $-x \in P$  and  $x + (-x) = 0 \in P'$ , a contradiction so  $P = P'$   
and the ordering is unique.

Theorem 2.3. Let  $F$  be a real closed field then every polynomial of odd degree with coefficients in  $F$  has a root belonging to  $F$ .

Proof: We use induction. If  $n=1$  the assertion is trivial. Assume  $f(x)$  is of degree  $n>1$  and assume that the theorem is true for all polynomials of odd degree  $<n$ . If  $f(x)$  is reducible then one of its factors has odd degree  $<n$ , so has a root in  $F$ . If  $f(x)$  is irreducible then let  $K = F(\theta)$  where  $f(\theta) = 0$ . Then  $K$  is not formally real so  $-1 = \sum_{i=1}^n \phi_i^2(\theta)$  where  $\phi_i(x) \in F(x)$  of degree  $\leq n-1$  and so we have  $-1 + f(x)g(x) = \sum_{i=1}^n \phi_i(x)^2$  and since degree of  $\sum_{i=1}^n \phi_i(x)^2 \leq 2(n-1) = 2n-2$  and degree of  $f(x) = n$  which is odd then degree  $g(x) < n$  and is odd so by induction there exists  $a \in F$ , such that  $g(a) = 0$  which implies  $-1 = \sum_{i=1}^n \phi_i(a)^2$ , a contradiction So  $f(x)$  has a root in  $F$ .

Theorem 2.4. If  $F$  is a real closed field then  $F(\sqrt{-1})$  is algebraically closed

Proof: We note first that  $\phi: F(\sqrt{-1}) \rightarrow F(\sqrt{-1})$  such that  $\phi(a+b\sqrt{-1}) = a-b\sqrt{-1}$  is an automorphism of  $F(\sqrt{-1})$  and what we want to prove is that if  $f(x) \in F(\sqrt{-1})[X]$  then  $f(x)$  has a root in  $F(\sqrt{-1})$ . Now if  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in F(\sqrt{-1})[x]$ , set  $\bar{f}(x) = \overline{a_n x^n + a_{n-1} x^{n-1} + \dots + a_0}$  then  $(f\bar{f})(x) \in F(x)$  since  $f(x)\bar{f}(x) = b_{2n} x^{2n} + b_{2n-1} x^{2n-1} + \dots + b_0$  where

$$b_k = a_k \bar{a}_0 + a_{k-1} \bar{a}_1 + \dots + a_0 \bar{a}_k$$

$$= (a_k \bar{a}_0 + \overline{a_k \bar{a}_0}) + \dots + (a_{\frac{k+1}{2}} \bar{a}_{\frac{k-1}{2}}) \text{ if } k \text{ is odd}$$

and  $b_k = (a_k \bar{a}_0 + \overline{a_k \bar{a}_0}) + \dots + (a_k \bar{a}_k + \overline{a_k \bar{a}_k})$  if  $k$  is even.

Thus  $b_k \in F$ , and  $f\bar{f} \in F(x)$ . Now if  $f(x)$  has a root in  $F(\sqrt{-1})$  then also  $f\bar{f}$  has a root and the converse is true so it is sufficient to show that if  $f \in F[X]$  then  $f$  has a root in  $F(\sqrt{-1})$ . First we notice that any element  $a$  of  $F(\sqrt{-1})$  has a square root in  $F(\sqrt{-1})$ , since if  $a > 0$  then  $a = b^2$ ,  $b \in F$  since  $F$  is real closed and if  $a < 0$  then  $-a = b^2$ ,  $b \in F$  so  $a = (\sqrt{-1}b)^2$ . Now suppose  $a = x + iy$  where  $i = \sqrt{-1}$  then  $(x + iy) = (c + di)^2$  is equivalent to  $c^2 - d^2 = x$  and  $2cd = y$ . Since  $y \neq 0$  we can multiply  $x + iy$  by  $\frac{2}{y}$  which has a square root in  $F(\sqrt{-1})$ . Thus we can assume that  $y = 2$ .

So we have  $c^2 - y^2 = x$  and  $cd = 1$  or  $d = c^{-1}$ . The first equation is  $c^2 - c^{-2} = x$  so  $c^4 - xc^2 - 1 = 0$  or  $c^2 = \frac{x + \sqrt{x^2 + 4}}{2}$  and we notice that  $x^2 + 4 < 0$  also  $x + \sqrt{x^2 + 4} < 0$ , since otherwise this will give  $4 < 0$  which is a contradiction. So  $c^2 = \frac{1}{2}(x + \sqrt{x^2 + 4})$  has a solution in  $F$ . So  $c, d = c^{-1}$  is a solution. This means that there exists no  $E$  such that  $[E:F] = 2$ , since any element in  $F$  has a square root. Now let  $f(x) \in F[X]$ . Let  $E$  be a splitting field of  $f(x) (x^2 + 1)$  which contains  $F(\sqrt{-1})$ .  $E$  is Galois over  $F$ . Let  $G$  be the Galois group and  $|G| = 2^e m$  where  $m$  is odd. By Sylow's theorem  $G$  has a subgroup of order  $2^e$ , say  $H$ . If  $K$  is the corresponding subfield of  $E/F$  then

we have  $[E:K] = 2^e$  and  $[K:F] = m$  since  $F$  has no proper odd-dimensional extension since every polynomial of odd degree has a root. So  $m=1$  and  $K=F$  so  $[E:F] = 2^e$  this implies that  $G=H$  and this group is solvable if  $e>1$  so  $E$  contains a subfield  $L$  which contains  $F(\sqrt{-1})$  such that  $[L:F(\sqrt{-1})] = 2$  but there is no  $L$  over  $F(\sqrt{-1})$  such that  $[L:F(\sqrt{-1})] = 2$  since any element has a square root in  $F(\sqrt{-1})$ .

Corollary: Every polynomial in  $F[x]$  where  $F$  is real closed splits into factors of the first or second degree.

Using the algebraic closure of  $F$  we can prove easily some of the facts about continuous and differentiable real functions, for example.

Theorem 2.5. Let  $F$  be a real closed field. Let  $f(x) \in F[x]$  and let  $a < b$  such that  $f(a)f(b) < 0$ . Then there exists  $a < c < b$  such that  $f(c) = 0$ .

Proof:  $f(x) = (x-a_1)(x-a_2)\dots(x-a_r)g_1(x)\dots g_s(x)$  where  $g_i(x) = x^2 + c_i x + d_i$  and  $c_i^2 < 4d_i$  then  $g_i(x) = (x + \frac{c_i}{2})^2 + \frac{1}{4}(4d_i - c_i^2)$ , so  $g_i(u) > 0$  for all  $u$ . Now if  $a, b < a_i$  for every  $i$  then

$$f(a)f(b) = \prod_{i,j} (a-a_i)(b-a_i)g_j(a)g_j(b) > 0. \quad \text{Also if } a, b > a_i$$

for every  $i$ , then  $f(a)f(b) > 0$ . Therefore there is  $a_k$  with  $a < a_k < b$ . But  $f(a_k) = 0$  and the theorem is proved. If we define  $f'(x) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \dots + a_1$  where  $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$  then it is easy to see that

for  $f(x), g(x) \in F[x]$  then  $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$  and we can use induction to prove that if  $f(x) = f_1(x)f_2(x)\dots f_k(x)$  then  $f'(x) = f_1'(x)f_2(x)\dots f_k(x) + f_1(x)f_2'(x)\dots f_k(x) + \dots + f_1(x)f_2(x)\dots f_k'(x)$ .

Theorem 2.6. (Rolle's theorem for polynomials) If  $f(a) = 0 = f(b)$  and  $a < b$  then there is  $c$  such that  $a < c < b$  and  $f'(c) = 0$ .

Proof: As before,  $f(x)$  can be written as

$f(x) = (x-a_1)\dots(x-a_r) g_1(x)\dots g_s(x)$  where  $g_1(x)$  are irreducible of degree two. Then using the formula for the derivative we can write  $f'(x)$  as

$$f'(x) = (x-a_2)\dots(x-a_r)g_1(x)\dots g_s(x) + \dots + (x-a_1)\dots$$

$(x-a_r)g_1(x)\dots g_s'(x)$ . We can assume that  $a = a_k, b = a_\ell$  where  $a_k, a_\ell \in \{a_1, \dots, a_r\}$  and no root of  $f(x)$  between  $a$  and  $b$ . Since  $g_1(u) > 0$  for every  $u$  then  $f'(a)f'(b) > 0$ . So by theorem 2.5 for  $f'(x)$  we conclude that there is  $c$  such that  $a < c < b$  with  $f'(c) = 0$ .

Now we can state the converse of theorem 2.4.

Theorem 2.7: If  $F$  is an ordered field and  $F(\sqrt{-1})$  is algebraically closed then  $F$  is a real closed field.

Proof: We want to show first that  $-1 \notin \Sigma(F)$  for this implies that  $F$  is formally real. Now, since  $F(\sqrt{-1})$  is algebraically closed the irreducible polynomials in  $F[x]$  are of



the first or second degree. Let  $a, b \in F$  arbitrary and consider  $g(x) = (x^2 - a) + b^2 = (x^2 - a - bi)(x^2 - a - bi)$ , where  $i = \sqrt{-1}$ .  
 $g(x) = (x - (a + bi)^{\frac{1}{2}})(x + (a + bi)^{\frac{1}{2}})(x - (a - bi)^{\frac{1}{2}})(x + (a - bi)^{\frac{1}{2}})$ .  
 Since  $g(x) \in F[x]$  and has no root in  $F$  it factors into two quadratic factors. The one divisible by  $(x - (a + bi)^{\frac{1}{2}})$  cannot be  $(x - (a + bi)^{\frac{1}{2}})(x + (a + bi)^{\frac{1}{2}})$  for this will imply that  $a + b_i \in F$  so it must be either  $(x - (a + bi)^{\frac{1}{2}})(x + (a - bi)^{\frac{1}{2}})$  or  $(x - (a + bi)^{\frac{1}{2}})(x - (a - bi)^{\frac{1}{2}})$ . In both cases this implies that  $(a^2 + b^2)^{\frac{1}{2}} \in F$  so the sum of two squares in  $F$  is a square in  $F$  and in general the sum of squares is a square. Since  $-1$  is not a square so  $-1$  is not a sum of squares which means that  $F$  is formally real. Any proper algebraic extension of  $F$  must be isomorphic to  $F(\sqrt{-1})$  so not formally real. This implies that  $F$  is a real closed field.

Remarks. (1) Theorems 2.4 and 2.7 give a characterization of real closed fields: An ordered field is real closed if  $F(\sqrt{-1})$  is algebraically closed.

(2) There is another characterization of real closed fields and this is often given as a definition: An ordered field  $F$  is real closed iff (i) positive elements of  $F$  have square roots in  $F$  and (ii) any polynomial with odd degree with coefficients in  $F$  has a root in  $F$ .

### 3. Sturm's Theorem

The main object of this section is to give a method for determining the exact number of roots of a polynomial

in a real closed field. We start with the following definition.

Definition 3.1: Let  $f(x) \in F[x]$  where  $F$  is a real closed field, a sequence of polynomials:  $f_0(x) = f(x), f_1(x), \dots, f_s(x)$  is called a Sturm sequence for  $f(x)$  for the closed interval  $[a, b]$  if  $f_i(x) \in F[x]$   $0 \leq i \leq s$  such that

- (1)  $f_s(x)$  has no roots in  $[a, b]$ .
- (2)  $f_0(a)f_0(b) \neq 0$ .
- (3) If  $f_i(c) = 0$  for  $c \in [a, b]$  then  $f_{i-1}(c)f_{i+1}(c) < 0$   $0 < i < s$ .
- (4) If  $f(c) = 0$  for  $c \in [a, b]$  then there exists  $c_1 < c$  and  $c < c_2$  such that  $f_0(x)f_1(x) < 0$  for  $x \in [c_1, c]$  and  $f_0(x)f_1(x) > 0$  for  $x \in [c, c_2]$ .

Definition 3.2: By the number of variations in sign of an  $r$ -tuple of non-zero elements  $\{c_1, c_2, \dots, c_r\}$ , of an ordered field we mean the number of indices  $i$ ,  $1 \leq i \leq r-1$  such that  $c_i c_{i+1} < 0$ .

If  $A = \{c_1, \dots, c_r\}$  is an arbitrary  $r$ -tuple of an ordered field then the number of variations in sign of  $A$  is equal to the number of variations in sign of  $A'$  obtained by dropping the zero elements. For example, if  $A = \{-2, 0, 5, 10, \frac{1}{2}, 0, -5\}$  then the number of variations in sign of  $A$  is the same as the number of variations in sign of  $A' = \{-2, 5, 10, \frac{1}{2}, -5\}$  which is equal to 2.

Theorem 3.1: Let  $f(x)$  be a polynomial of positive degree

with coefficients in a real closed field  $F$ . If  $f_0(x) = f(x), f_1(x), \dots, f_s(x)$  is a Sturm sequence for  $f(x)$  for the interval  $[a, b]$ , then the number of distinct roots of  $f(x)$  in  $[a, b]$  is  $V_a - V_b$ , where  $V_c$  is the number of variations in sign of the sequence  $\{f_0(c), f_1(c), \dots, f_s(c)\}$ .

Proof: The interval  $[a, b]$  is divided into sub-intervals by the roots of  $f_i(x)$ ,  $0 \leq i \leq s$ . If  $a = x_0 < x_1 < \dots < x_n = b$  are these points, let  $c \in (x_0, x_1)$ , so there is no root for  $f_j(x)$ ,  $0 \leq j \leq s$  in the interval  $(x_0, c)$ . By the intermediate value theorem  $f_j(x_0)f_j(c) \geq 0$ . So if none of  $f_j(x_0) = 0$  then  $f_j(x_0)f_j(c) > 0$  which means that  $V_{x_0} = V_c$ . Now assume  $k$ ,  $0 < k < s$  such that  $f_k(x_0) = 0$  then  $f_{k-1}(x_0)f_{k+1}(x_0) < 0$  by property (3) of the definition of Sturm's theorem.

Since  $f_{k-1}$  and  $f_{k+1}$  have no roots in the interval  $(x_0, c)$ , therefore,  $f_{k-1}(x_0)f_{k-1}(c) > 0$  and  $f_{k+1}(x_0)f_{k+1}(c) > 0$ . This implies that  $f_{k-1}(c)$ ,  $f_k(c)$ ,  $f_{k+1}(c)$ , and  $f_{k-1}(x_0)$ ,  $0$ ,  $f_{k+1}(x_0)$  each contributes one variation in sign to  $V_c$  and  $V_{x_0}$ , respectively. Taking into consideration all  $k$ ,  $0 < k < s$  we conclude that  $V_{x_0} = V_c$ . The same argument applies if  $c \in (x_{s-1}, x_s)$ . Next let  $c \in (x_{i-1}, x_i)$ ,  $d \in (x_i, x_{i+1})$ .

(1) If  $f(x_i) \neq 0$  then

(i) either  $f_k(x_i) \neq 0$   $0 < k < s$  which implies that  $f_k$  has no roots in the interval  $(c, d)$  so  $f_k(c)f_k(d) > 0$ , so  $f_k(c), f_k(d)$  have the same sign.

(ii) or  $f_k(x_i) = 0$  for some  $0 < k < s$  so  $f_{k-1}(x_i)f_{k+1}(x_i) < 0$  which implies that  $f_{k-1}$  and  $f_{k+1}$  have no roots

in  $[c, d]$ . So  $f_{k-1}(c)f_{k-1}(d) > 0$  and  $f_{k+1}(c)f_{k+1}(d) > 0$ , which implies  $f_{k-1}(c), f_k(c), f_{k+1}(c)$  and  $f_{k-1}(d), f_k(d), f_{k+1}(d)$  each contributes one variation in sign to  $V_c$  and  $V_d$ . From (i) and (ii) and taking into account all  $k$  we have  $V_c = V_d$ .

(2) If  $f(x_i) = 0$  then  $f_0(c)f_1(c) < 0$ ,  $f_0(d)f_1(d) > 0$  which implies that  $f_0(c), f_1(c)$  has one variation in sign more than  $f_0(d), f_1(d)$ . The argument used before shows that  $f_{j-1}(c), f_j(c), f_{j+1}(c)$  and  $f_{j-1}(d), f_j(d), f_{j+1}(d)$  have the same number of variation in sign if  $j > 1$ . Now if  $a_i \in (x_{i-1}, x_i)$  then  $V_a - V_b = (V_a - V_{a_i}) + \sum_1^{n-1} (V_{a_i} - V_{a_{i+1}}) + (V_{a_n} - V_b)$  and we notice that each term is either 0 or 1 and the number of 1's is the same as the number of  $x_i$  for which  $f(x_i) = 0$ .

The construction of a Sturm sequence for any polynomial  $f(x)$  is very easy. We can construct it in the following way:

Let  $f(x) \in F[x]$ ,  $F$  real closed. We define  $f_i(x)$   $0 \leq i \leq s$  as follows:  $f_0(x) = f(x)$ ,  $f_1(x) = f'(x)$  and

$$f_{i-1}(x) = q_i(x) f_i(x) - f_{i+1}(x) \quad 1 \leq i \leq s$$

$$f_{s-1}(x) = q_s(x) f_s(x) \quad (\text{i.e. } f_{s+1}(x) = 0).$$

We shall call  $f_0(x), \dots, f_s(x)$  the standard sequence for  $f(x)$ .

Example: Let  $f(x) = x^3 - 7x - 7$ ,  $f'(x) = 3x^2 - 7$ . Then since  $x^3 - 7x - 7 = (\frac{1}{3}x)(3x^2 - 7) - (\frac{14}{3}x + 7)$  and  $(3x^2 - 7) = (\frac{9}{14}x - \frac{27}{28})(\frac{14}{3}x + 7) - (+\frac{1}{2})$ , we have  $f_0(x) = x^3 - 7x - 7$ ,  $f_1(x) = 3x - 7$ ,  $f_2(x) = \frac{14}{3}x + 7$ ,  $f_3(x) = +\frac{1}{2}$  is the standard sequence for  $f(x)$ . If we define  $g_i(x) = f_i(x)f_s^{-1}(x)$  then we can show that  $g_0(x), g_1(x), \dots, g_s(x)$  is a Sturm sequence for  $g_0(x)$  for the interval  $[a, b]$  where  $g_0(a) \neq 0$ ,  $g_0(b) \neq 0$ .

Proof: First we note that  $f_s(x)$  is the greatest common divisor of  $f(x)$  and  $f'(x)$ . Next we see that  $g_s(x) = 1$  so  $g_s(x) \neq 0$  for every  $x$  which is condition (1). Since  $g_0(a)g_0(b) \neq 0$  condition (2) is satisfied. Next assume  $g_k(c) = 0$   $0 < k < s$  then dividing the relation  $f_{i-1} = q_i f_i - f_{i+1}$  by  $f_s$  we have  $g_{i-1} = q_i g_i - g_{i+1}$ , so if  $g_k(c) = 0$  then  $g_{k-1}(c) = -g_{k+1}(c)$  which implies  $g_{k-1}(c)g_{k+1}(c) \leq 0$ . If  $g_{k-1}(c) = 0$  then  $g_{k+1}(c) = 0$  which implies  $g_{k-1}(c) = g_k(c) = \dots = g_s(c) = 0$ , a contradiction. So  $g_{k-1}(c)g_{k+1}(c) < 0$  and condition (3) is satisfied. Finally, if  $g_0(c) = 0$  then  $f(x) = (x-c)^e h(x)$   $e > 0$  and  $h(c) \neq 0$ , then  $f'(x) = (x-c)^e h'(x) + e(x-c)^{e-1} h(x)$  and also  $f_s(x) = (x-c)^{e-1} k(x)$ ,  $k(c) \neq 0$  so  $h(x) = k(x)l(x)$  where  $l(c) \neq 0$  and  $h'(x) = k(x)m(x)$  these give  $g_0(x) = (x-c)l(x)$ ,  $l(c) \neq 0$ ,  $g_1(x) = (x-c)m(x) + el(x)$  and then  $g_1(c) = el(c) \neq 0$ . Since  $g_1(c) \neq 0$  we choose  $[c_1, c_2]$  such that  $g_1(x)l(x) > 0$  in  $[c_1, c_2]$ . So  $g_0(x)g_1(x) = (x-c)g_1(x)l(x)$  has the same sign as  $x-c$  in  $[c_1, c_2]$ , so  $g_0(x)g_1(x) < 0$  if

$x \in [c_1, c]$  and  $g_0(x)g_1(x) > 0$  if  $x \in [c, c_2]$  which is condition (4) of the definition of Sturm's theorem.

We note that if  $f(x)$  has no multiple roots in  $[a, b]$  then the greatest common divisor of  $f(x)$  and  $f'(x)$  is 1 then the sequence  $\{f_0(x), f_1(x), \dots\}$  differs from  $\{g_0(x), g_1(x), \dots\}$  by a non-zero multiplier so the sequence  $\{f_0(x), f_1(x), \dots\}$  is a Sturm sequence. But if  $f(x)$  contains a multiple root in the interval  $[a, b]$  then the sequence  $\{f_0(x), f_1(x), \dots\}$  will not be a Sturm sequence. But still we can use the standard sequence for determining the number of roots of  $f(x)$  in  $[a, b]$ . We have the following theorem.

Theorem 3.2. Let  $f(x) \in F[x]$ ,  $F$  a real closed field, and let  $\{f_0(x) = f(x), f_1(x) = f'(x), \dots, f_s(x)\}$  be the standard sequence for  $f(x)$  in the interval  $[a, b]$  where  $f(a) \neq 0$ ,  $f(b) \neq 0$ . Then the number of distinct roots of  $f(x)$  in  $[a, b]$  is  $V_a - V_b$ .

Proof: If  $g_i(x) = f_i(x)f_s^{-1}(x)$  then  $f(x)$  and  $g_0(x)$  have the same number of roots, and  $g_0(x)$  has only simple roots, so they have the same number of distinct roots. Since the sequence  $g_0(x), g_1(x), \dots$  is a Sturm sequence for  $g(x)$  in  $[a, b]$ , the number of roots of  $g_0(x)$  is  $V_a(g) - V_b(g)$ . Since  $f_i(c) = g_i(c)f_s^{-1}(c)$ , and  $f_s(a), f_s(b) \neq 0$  so  $V_a(g) = V_a$  and  $V_b(g) = V_b$  and  $V_a - V_b$  is the number of distinct roots for  $f(x)$ .

Remarks: (1) We have seen before that the roots of  $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$  lie between  $-M$  and  $M$  where  $M = \max\{1, |a_1| + \dots + |a_n|\}$ .

Set  $k = 1 + |a_1| + \dots + |a_n|$ . If  $\{f_0(x), \dots, f_s(x)\}$  is the standard sequence for  $f(x)$  then the number of roots is  $V_{-k} - V_k$ . Using  $|a_i| < 1 + a_i^2$ ,  $1 + |a_1| + \dots + |a_n| < 1 + |a_1| + \dots + |a_n| < 1 + (1 + a_1^2) + \dots + (1 + a_n^2) = (1+n) + (a_1^2 + \dots + a_n^2)$ , and if  $\ell = (n+1) + \sum_{i=1}^n a_i^2$  then the number of distinct roots of  $f(x)$  is  $V_{-\ell} - V_\ell$ .

(2) If we wish to apply Sturm's theorem for determining the total number of roots of  $f(x) \in F[x]$ , the limits  $a$  and  $b$  must be respectively so small and so large that there are no more roots for either  $x < a$  or  $x > b$ . It suffices to take  $a = -M$  and  $b = M$ . However, it is still more convenient to choose  $a$  and  $b$  so that all polynomials of Sturm's chain have no more zeros for  $x < a$  or for  $x > b$ . Then their signs are determined by the signs of their leading coefficients:  $a_0 x^m + a_1 x^{m-1} + \dots$  has the sign of  $a_0$  for very large  $x$  and that of  $(-1)^m a_0$  for very small  $x < 0$ . In this method we may disregard the question as to how large  $a$  and  $b$  have to be. We merely compute the leading coefficient  $a_0$  and degrees  $m$  of Sturm's polynomials.

Examples: (1) We have seen before that the standard sequence for  $f(x) = x^3 - 7x - 7$  is  $x^3 - 7x - 7$ ,  $3x^2 - 7$ ,  $\frac{14}{3}x + 7$ ,  $+\frac{1}{2}$  so the number of distinct roots of  $f(x)$  in the interval  $[-2, 1]$  is  $V_{-2} - V_1 = 3 - 1 = 2$ .

(2). If  $f(x) = x^4 + 12x^2 + 5x - 9$  then  $f'(x) = 4x^3 + 24x + 5$ , and from the following equations

$$(x^4 + 12x^2 + 5x - 9) = (\frac{1}{4}x)(4x^3 + 24x + 5) - (-6x^2 - \frac{15}{4}x + 9)$$

$$\text{and } (-6x - \frac{15}{4}x + 9) = (\frac{96}{505}x - \frac{1419}{5(101)^2}) (\frac{-505}{16}x - \frac{5}{4}) - (\frac{4x \cdot 1419}{5(101)^2} - 9)$$

we have the standard sequence for  $f(x)$  defined by

$$f_0(x) = x^4 + 12x^2 + 5x - 9, \quad f_1(x) = 4x^3 + 24x + 5.$$

$$f_2(x) = -\frac{405}{16}x - \frac{5}{4} \text{ and } f_3(x) = K = -\frac{1419}{(101)^2} - 9.$$

By remark (2), if we choose  $a$ , a very small negative number, and  $b$ , a very large positive number, then  $f_0(a) > 0$ ,  $f_1(a) < 0$ ,  $f_2(a) > 0$ ,  $f_3(a) < 0$ . They have the same sign as  $1, 4, -\frac{405}{16}, -K$ , respectively, and  $f_0(b) > 0$ ,  $f_1(b) > 0$ ,  $f_2(b) < 0$ ,  $f_3(b) < 0$ . They have the same sign as  $(-1)^4(1), (-1)^3(4), (-1)(-\frac{405}{16}), -K$ , respectively. So  $V_a - V_b = 3 - 1 = 2$  which is the total number of distinct roots of  $f(x)$  in  $\mathbb{R}$ .

#### 4. Extension Theorems for Formally Real Fields

The question of existence of formally real fields can be answered by the following theorems.

Theorem 4.1: If  $F$  is an ordered field then the field  $K$  that we obtain by adjoining to  $F$  all square roots of positive elements of  $F$  is formally real.

Proof: If we have a relation of the form  $-1 = \sum_{k=1}^n b_k^2$  in  $K$  then the  $b_k$  are contained in a finite dimensional extension of the form  $F(\sqrt{c_1}, \sqrt{c_2}, \dots, \sqrt{c_r})$  where the  $c_i$ 's are positive elements in  $F$ . So it is sufficient to prove that



every subfield of  $K$  of the form  $F(\sqrt{c_1}, \dots, \sqrt{c_r})$  is formally real. We prove this by induction on  $r$ . We want to show a strong result that if  $\sum_1^n a_i b_k^2 = 0$  where  $a_i \in F$ ,  $b_k \in K$ ,  $a_i > 0$  then the  $b_k$  are zeros. We see this is true for  $F$ . Next assume that it is true for subfields of indicated form with dimensionality less than  $r$ , so if  $\sum_1^n a_i b_k^2 = 0$  then the  $b_k$  are contained in  $L = F(\sqrt{c_1}, \dots, \sqrt{c_r}) \supseteq F(c_1, \dots, c_{r-1}) = M$ , we can write  $b_k = x_i + y_i \sqrt{c_r}$ . So  $0 = \sum_1^n a_i (x_i + y_i \sqrt{c_r})^2$  implies  $0 = \sum_1^n a_i x_i^2 + c_r \sum_1^n a_i y_i^2 + 2(\sum_1^n a_i x_i y_i)(\sqrt{c_r})$ . Since  $\sqrt{c_r} \notin M$ , then  $\sum_1^n a_i x_i y_i = 0$ ,  $\sum_1^n a_i x_i^2 + c_r \sum_1^n a_i y_i^2 = 0$ , since  $a_i > 0$  and  $a_i c_r > 0$  then  $x_i = 0, y_i = 0$  by the induction hypothesis and so  $b_k = 0$  for every  $k$ .

The field of real numbers is a real closed field. Is there any other real closed field? In fact, we have the following constructive theorem.

Theorem 4.2: Let  $F$  be a formally real field and let  $K$  be an algebraic closure of  $F$  then  $K$  contains a real closed field containing  $F$ .

Proof: Let  $\phi$  be the collection of all formally real subfields of  $K$  containing  $F$ ,  $\phi$  is not empty since it contains  $F$ . Now the union of any chain  $\{L_k\}$  of formally real fields is formally real for otherwise  $-1 = \sum_1^n a_i^2$  holds in the union then the elements  $a_i \in L_{k_i}$  for some  $k_i$ , a contradiction with the formal reality of  $L_{k_i}$ . So the set  $\phi$  forms an inductive set and contains a maximal

element, say  $E$ .  $E$  is real closed, since if  $E$  is not real closed then it contains an algebraic extension which is formally real, but since  $E$  is a maximal element this can not happen, since this real closed field is a subset of  $K$  and will contain  $E$ .

Corollary 1. From theorems (4.1) and (4.2) we have that any ordered field has a real closed algebraic extension.

Corollary 2. Any formally real field can be ordered.

Proof: Let  $F$  be a formally real field, then  $F$  has a real closed algebraic extension so it can be ordered by the unique ordering of this real closed field.

We can come to the conclusion that a field can be ordered if and only if it is formally real.

## 5. Real Closure of Ordered Fields

We have seen that for every ordered field  $F$  there is a real closed algebraic extension. Thus we have the following.

Definition 5.1: Let  $F$  be an ordered field, a field  $K$  is called a real algebraic closure of  $F$  if and only if (1)  $K$  is real closed; (2)  $K$  is algebraic over  $F$ ; (3) the order in  $K$  is an extension of that of  $F$ .

Theorem 5.1: Let  $F$  be an ordered field, then  $F$  has a real closure. If  $F_1, F_2$  are two ordered fields with real closures  $K_1$  and  $K_2$ , respectively, then any order isomorphism of  $F_1$  onto  $F_2$  can be extended to a unique isomorphism of

$K_1$  onto  $K_2$ . In particular, the only automorphism of  $K_1$  which leaves the elements of  $F$  fixed is the identity.

Proof: Corollary 1 to theorem 4.1 and 4.2 gives the existence. For the second part assume that  $F_1, F_2$  are two ordered fields with the real closure  $K_1$  and  $K_2$ , respectively. Let  $x \mapsto \bar{x}$  be an order isomorphism of  $F_1$  onto  $F_2$ . We want to define an extension of this mapping into one between  $K_1$  and  $K_2$ . Now we observe that if  $f(x) \in F[x]$  then  $f(x)$  and its image  $\bar{f}(x)$  have the same number of roots, since by Sturm's theorem we can find  $M$  such that the roots of  $f(x)$  are in  $[-M, M]$  and the number of these roots in  $K_1$  is  $V_{-M} - V_M$ . Since the standard sequence of  $f(x)$  are contained in  $F_1[x]$ , all of this carries over  $\bar{f}(x)$  and  $F_2$ , so the number of roots of  $\bar{f}(x)$  in  $F_2[x]$  is the same as the number of roots of  $f(x)$  in  $F_1[x]$ . Next we observe that if we are given a set  $A = \{a_1, a_2, \dots, a_n\} \subset K_1$  then there exists a subfield  $L$  of  $K_1/F_1$  and an isomorphism  $f$  of  $L_1$  into  $K_2$  such that if  $a_1 < a_2 < \dots < a_n$  then  $f(x) = x, x \in F_1$ , and  $f(a_1) < f(a_2) < \dots < f(a_n)$  for this. Let  $f(x) \in F[x]$  be such that it contains among its roots  $a_1, \dots, a_n$  and  $\sqrt{a_{i+1} - a_i} \quad 1 \leq i \leq n-1, (\sqrt{a_{i+1} - a_i} \in K_1$  since  $a_{i+1} - a_i > 0$  and  $K_1$  is real closed). Let  $L_1$  be the subfield of  $K_1$  generated by the roots of  $f(x)$  in  $K_1$ , then  $L_1 = F_1(\theta)$ . If  $g(x)$  is the minimum polynomial for  $\theta$  then  $\bar{g}(x)$  has a root  $\bar{\theta}$  in  $K_2$  and we have an isomorphism  $f$

from  $L$  into  $F_2(\bar{\theta})$  such that  $f(x) = x$  if  $x \in F_1$  and  $f(\theta) = \bar{\theta}$ . So  $f(a_{i+1}) - f(a_i) = f(a_{i+1} - a_i) = f(b_i)^2$  for  $b_i \in K_1$   
 $b_i = \sqrt{a_{i+1} - a_i}$  so  $f(b_i^2) = f(b_i)^2$  so in  $F_2(\bar{\theta}_1)$  so we have  
 $f(a_1) < f(a_2) < \dots < f(a_n)$  as required.

Now we can define the extended isomorphism between  $K_1$  and  $K_2$  as follows: If  $a \in K_1$ , let  $f(x)$  be the minimum polynomial of  $a$  in  $F_1$ , let the roots of  $f(x)$  in  $K_1$  be  $a_1 < a_2 < \dots < a_s$ . The function  $\bar{f}(x) \in F_2[x]$  has exactly  $s$  roots,  $a_1', a_2', \dots, a_s'$  in  $K_2$  and if  $a = a_k$  we define  $g(a) = a_k'$ . This mapping is well-defined since if  $a \in K_1$  it cannot have two minimum polynomials and so  $g(a)$  is defined uniquely and it is obvious that  $g(x) = \bar{x}$ , for every  $x \in F$  since the minimum polynomial in this case is just  $x - a$  for every  $a \in F$ , which has one root  $a \in F$ , and this is mapped into  $\bar{a} \in F_2$ .  $g$  is obvious one to one and onto.

It remains to be shown that  $g$  is an isomorphism of  $K_1$  onto  $K_2$ , so let  $a, b \in K_1$ . We have to show that  $g(a+b) = g(a) + g(b)$  and  $g(ab) = g(a)g(b)$ , so let  $A \subset K$ , such that  $A$  contains the roots of the minimum polynomials of  $a, b, a+b, ab$ . So there exists a subfield  $L_1 \supset A$  of  $K_1/F_1$  and an isomorphism  $f$  of  $L_1$  into  $K_2$  extending  $x \rightarrow \bar{x}$  and preserving the order of elements in  $A$ . Then if  $h(x)$  is the minimum polynomial of  $a$  over  $F_1$  and the roots of  $h(x)$  are  $b_1 < b_2 < \dots < b_s$ ,  $b_i \in A$  then  $f(b_1) < f(b_2) < \dots < f(b_s)$ , and since  $\bar{g}(f(b_i)) = 0$ . So from the definition of  $g$  we have  $g(b_i) = f(b_i)$  and so  $g(a) = f(a), g(b) = g(b)$ , also

from  $L$  into  $F_2(\bar{\theta})$  such that  $f(x) = x$  if  $x \in F_1$  and  $f(\theta) = \bar{\theta}$ . So  $f(a_{i+1}) - f(a_i) = f(a_{i+1} - a_i) = f(b_i)^2$  for  $b_i \in K_1$   
 $b_i = \sqrt{a_{i+1} - a_i}$  so  $f(b_i^2) = f(b_i)^2$  so in  $F_2(\bar{\theta}_1)$  so we have  
 $f(a_1) < f(a_2) < \dots < f(a_n)$  as required.

Now we can define the extended isomorphism between  $K_1$  and  $K_2$  as follows: If  $a \in K_1$ , let  $f(x)$  be the minimum polynomial of  $a$  in  $F_1$ , let the roots of  $f(x)$  in  $K_1$  be  $a_1 < a_2 < \dots < a_s$ . The function  $\bar{f}(x) \in F_2[x]$  has exactly  $s$  roots,  $a_1', a_2', \dots, a_s'$  in  $K_2$  and if  $a = a_k$  we define  $g(a) = a_k'$ . This mapping is well-defined since if  $a \in K_1$  it cannot have two minimum polynomials and so  $g(a)$  is defined uniquely and it is obvious that  $g(x) = \bar{x}$ , for every  $x \in F$  since the minimum polynomial in this case is just  $x - a$  for every  $a \in F$ , which has one root  $a \in F$ , and this is mapped into  $\bar{a} \in F_2$ .  $g$  is obvious one to one and onto.

It remains to be shown that  $g$  is an isomorphism of  $K_1$  onto  $K_2$ , so let  $a, b \in K_1$ . We have to show that  $g(a+b) = g(a) + g(b)$  and  $g(ab) = g(a)g(b)$ , so let  $A \subset K_1$ , such that  $A$  contains the roots of the minimum polynomials of  $a, b, a+b, ab$ . So there exists a subfield  $L_1 \supset A$  of  $K_1/F_1$  and an isomorphism  $f$  of  $L_1$  into  $K_2$  extending  $x \rightarrow \bar{x}$  and preserving the order of elements in  $A$ . Then if  $h(x)$  is the minimum polynomial of  $a$  over  $F_1$  and the roots of  $h(x)$  are  $b_1 < b_2 < \dots < b_s$ ,  $b_i \in A$  then  $f(b_1) < f(b_2) < \dots < f(b_s)$ , and since  $\bar{g}(f(b_i)) = 0$ . So from the definition of  $g$  we have  $g(b_i) = f(b_i)$  and so  $g(a) = f(a), g(b) = f(b)$ , also

$g(a+b) = f(a+b)$ ,  $g(ab) = f(ab)$  so  $g$  is isomorphism since  $f$  is an isomorphism.

$g$  is unique since if  $g'$  is another order isomorphism extending that  $x \rightarrow \bar{x}$  of  $F_1$  onto  $F_2$  then if  $a \in K$ , and  $b_1 < b_2 < \dots < b_s$  are the roots of the minimum polynomial  $h(x)$  of  $a$  then  $g'(b_1) < g'(b_2) < \dots < g'(b_s)$  and so  $g'(a) = g(a)$ .

If  $K$  and  $K'$  are two real closure for  $F$  then the identity isomorphism of  $F$  can be extended to an isomorphism of  $K$  onto  $K'$  fixing the elements of  $F$ , and since this is unique we see that  $K, K'$  are equivalent.

If  $g$  is an automorphism of  $K$  leaving the elements of  $F$  fixed, and since the identity of  $K$  is an isomorphism so by uniqueness,  $g$  must be the identity. This theorem means that if  $K$  is an ordered field with one ordering then all the real closures are isomorphic under the isomorphism fixing the elements of  $K$ . For example, the field of rational numbers  $Q$  has only one order so any two real closed fields over  $Q$  are isomorphic under an isomorphism which leaves the element of  $Q$  unchanged. On the other hand, if  $K$  is an ordered field with  $n$  different orderings then each gives rise to a real closure and no two of them are isomorphic, because if  $L_1, L_2$  are two real closure with distinct orderings  $>_1, >_2$  of  $K$ , respectively, then for some  $a \in K$   $a >_1 0$  and  $a <_2 0$  so  $a$  is a square in  $L_1$  and not in  $L_2$ .

An example:  $Q(\sqrt{2})$  has two distinct orderings and therefore we have two non-isomorphic real closures of  $Q(\sqrt{2})$ .

## 6. Real Algebraic Numbers

We know that the field of rational numbers has only one ordering. As already mentioned,  $Q$  has a real closure and this is determined up to isomorphism. If  $K$  is the real closure of  $Q$  then  $K(i) = S$  is algebraically closed. We call  $K$  the field of real algebraic numbers and  $S$  the field of algebraic numbers.

Theorem 6.1: Let  $L$  be a finite dimensional extension field of the field of rational numbers. Then the number of distinct ordering of  $L$  is the same as the number of isomorphisms of  $L$  into the field  $K$  of real algebraic numbers.

Proof: Suppose  $L = Q(\theta)$  and  $f(x)$  is the minimum polynomial of  $\theta$ . Let  $\{\theta_1, \dots, \theta_2, \dots, \theta_n\}$  be the set of distinct roots of  $f(x)$  in  $S$ . We have  $n$  distinct isomorphisms of  $L$  into  $S$ . If  $\{\theta_1, \dots, \theta_r\}$  are the roots of  $f(x)$  contained in  $K$  then these roots are called the real conjugates of  $\theta$ . We have the isomorphism  $f_i$  of  $L$  into  $K$  such that  $f_i(\theta) = \theta_i$   $1 \leq i \leq r$ . Now  $Q(\theta_i)$  is a subset of the real closed field, so it has the induced order and this order can be used to define an ordering of  $L$  as follows: If  $P \in L$  then  $P > 0$  if  $f_i(P) > 0$  and it is easy to see that this is an ordering of  $L$ . If  $L$  has a certain order then

this order has a real algebraic closure  $K'$ .  $K'$  is a real closure of  $Q$  since  $L$  is algebraic over  $Q$ , so by theorem 5.1  $K'$  and  $K$  are isomorphic and the restriction of  $K$  coincide with one of the mappings  $f_i$ . If  $f_i, f_j$  have the same ordering of  $L$  then we have an isomorphism of  $Q(\theta_i)$  onto  $Q(\theta_j)$  such that  $\theta_i \rightarrow \theta_j$ . Since  $K$  is a real algebraic closure of both  $Q(\theta_i)$  and  $Q(\theta_j)$  this can be extended to an automorphism of  $K$  such that  $a \rightarrow a$  for every  $a \in Q$  and this is the identity according to theorem 5.1 so  $\theta_i = \theta_j$ .

Definition 6.1: Let  $F$  be a field.  $p \in F$  is called totally positive if and only if  $p > 0$  under any ordering of  $F$ . If  $F$  has no ordering then  $p \in F$  is totally positive for every  $p$ . In particular, any element of a field which is not formally real is totally positive since this field is not orderable.

Theorem 6.2: Let  $F$  be a field.  $p \in F$  is totally positive if and only if  $p$  is a sum of squares of elements of  $F$ .

Proof: If  $p$  is a sum of squares of elements  $F$  then  $p > 0$  under any ordering of  $F$  so  $p$  is totally positive. If  $p$  is not a sum of squares and if  $S$  is an algebraic closure of  $F$  we consider the family of subfields of  $S/F$  such that  $p$  is not a sum of squares. This collection is not empty since it contains  $F$ . Also this collection is inductive so it has a maximal element  $K$ .  $K$  is formally real, otherwise every element of  $K$  is a sum of squares and we are assuming  $p$  is not a sum of squares.



$-p$  is a square in  $K$  since if  $-p$  is not a square then  $K(\sqrt{-p}) \supset K$  properly and so  $p$  is a sum of square in this field since  $K$  is maximal of those for which  $p$  is not a sum of squares. So  $p = \sum_{i=1}^n (a_i + b_i \sqrt{-p})^2$   $a_i, b_i \in K$  and so  $p = \sum a_i^2 + 2\sqrt{-p} \sum a_i b_i - p \sum b_i^2$ .  $\sqrt{-p} \notin K$  implies  $\sum a_i b_i = 0$ , so  $p = (\sum a_i^2)(1 + \sum b_i^2)^{-1}$  where  $1 + \sum b_i^2 \neq 0$  since otherwise  $K$  is not formally real. This means that  $p$  is a sum of squares in  $K$  which contradicts the choice of  $K$ . This gives  $-p = k^2$  and so  $-p > 0$  which implies  $p < 0$  in every ordering so  $p$  is not totally positive. This result and theorem 6.1 on the form of ordering of a finite dimensional extension field of the rationals imply the following theorem which is due to Hilbert and Landau.

Theorem 6.3: Let  $L$  be a finite dimensional extension field of the rationals and let  $f_1, f_2, \dots, f_r$  ( $r > 0$ ) be the different isomorphisms of  $L$  into the field of real algebraic numbers. Let  $p \in L$ ,  $p \neq 0$  then  $p$  is a sum of squares in  $L$  if and only if  $f_i(p) > 0$  for  $i=1, 2, \dots, r$ .

## 7. Positive Definite Rational Functions

One of the problems proposed by Hilbert in his address to the 1900 Paris Congress of Mathematics, known as Hilbert's 17th Problem, asks the following question: If  $Q$  is a rational function in  $n$  variables with rational coefficients such that  $Q(k_1, \dots, k_n) \geq 0$  for every  $k_1, \dots, k_n$ , where all  $k_i$  are real, is  $Q$  a sum of squares of rational functions with rational coefficients? By a rational function we mean a mapping  $(k_1, \dots, k_n) \rightarrow Q(k_1, \dots, k_n)$  such that  $Q(x_1, \dots, x_n)$  is a rational expression in indeterminants  $x_i$  with rational coefficients.

In 1927 Artin gave a positive answer to Hilbert's question and proved a more general theorem.

Theorem 7.1: (Artin) Let  $K$  be a subfield of the field  $\mathbb{R}$  of ordinary real numbers.

Let  $Q$  be a rational function with coefficients in  $K$  which is rationally definite in the sense that  $Q(k_1, \dots, k_n) \geq 0$  for all rationals  $(k_i)$  where  $Q$  is defined. Then  $Q$  is a sum of squares of rational functions with coefficients in  $K$ . Since  $K(x_1, \dots, x_n)$  is a formally real field for  $x_1, \dots, x_n$  transcendental-indeterminants as we have seen then (by theorem 6.2)  $Q \in K(x_1, \dots, x_n)$  is a sum of squares of elements in  $K(x_1, \dots, x_n)$  if and only if  $Q \geq 0$  in every ordering of  $K(x_1, \dots, x_n)$ . Theorem (7.1) will follow if we prove that if  $Q \neq 0$  is rationally definite,

then  $Q > 0$  in every ordering of  $K(x_i)$  and this follows from the following.

Theorem 7.2: Let  $K$  be a field of real numbers and let  $K(x_1, \dots, x_n)$  be the field of rational expressions in  $n$  indeterminates  $x_i$ , with rational coefficients. Let  $f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n) \in K(x_i)$  where  $K(x_1, \dots, x_n)$  has an order which is an extension of the order of  $K$ . Then there is a rational  $n$ -tuple  $(a_1, \dots, a_n)$  such that for every  $j, 1 \leq j \leq k$   $f_j(x_1, \dots, x_n)$  is defined at  $(a_1, \dots, a_n)$  and has the same sign as  $f_k(a_1, \dots, a_n)$  (i.e.  $f_k(x_1, \dots, x_n) \underset{<}{\geq} 0$  according as  $f_k(a_1, \dots, a_n) \underset{<}{\geq} 0$ ).

Suppose this theorem is proved. Let  $K$  be as in theorem (7.1) and  $Q \neq 0$  be an element of  $K(x_i)$  which is not a sum of squares then  $Q < 0$  for some ordering of  $K(x_i)$  and since the order of  $K(x_i)$  is an extension of the unique order of  $K$  then by this theorem there is  $n$ -tuple  $(a_1, \dots, a_n)$  of elements of  $K$  such that  $Q(a_1, \dots, a_n) < 0$ , a contradiction.

To prove the theorem we use induction on the number of  $x$ 's. If  $n=0$  the result is obvious since in this case  $K(x_i)=K$  and the functions  $f_i$ 's are constants. We assume the result is true for  $K(x_1, \dots, x_n)$  and we want to show that it is true for  $K(x_1, \dots, x_n, y)$  where  $y$  is another indeterminate. To prove this we need definition and two lemmas.

Definition: Let  $F_1(x_i, y), \dots, F_k(x_i, y) \in K(x_i)[y]$  then we call a property  $p$  of this set of polynomials in  $y$  to be rationally specializable if there exists a set of elements  $k_1(x_i), \dots, k_h(x_i) \in K(x_i)$  such that if  $(a_1, \dots, a_n)$  is any rational  $n$ -tuple for which  $k_1(a_i), \dots, k_h(a_i)$  are defined and have the same sign as  $k_1(x_i), \dots, k_h(x_i)$ , respectively, then the set of polynomials  $F(a_i, y), \dots, F_k(a_i, y)$  has the property  $P$ .

Lemma 1: The property that  $F(x_i, y) = y^{m+\phi_1(x_i, y)}y^{m-1} + \dots + \phi_m(x_i)$  has precisely  $r$  roots in the real closure of  $K(x_i)$  is rationally specializable.

Proof: What we have to show is that there is  $k_1, \dots, k_h$  in  $K(x_i)$  such that if  $(a_1, \dots, a_n)$  is any rational  $n$ -tuple such that  $k_i$  are defined for  $(a_1, \dots, a_n)$   $1 \leq i \leq h$  and have the same sign as  $k_i(x_i)$  then the function  $F(a_i, y)$  has  $r$  roots in the real closure of  $K$  which is the real algebraic numbers. Let  $F_0(x_i, y) = F(x_i, y)$  and  $F_1, \dots, F_s$  be the standard sequence for  $F(x_i, y)$  as a polynomial in  $K(x_i)[y]$ , and if  $h(x_i) = (m+1) + \sum_1^m \phi_i(x_i)^2$  then by Sturm's theorem the  $r$  roots of  $F(x_i, y)$  in the real closure of  $K(x_i)$  are in  $(-h, h)$  and  $r$  is the difference in the variation in sign of the two sequences  $F_0(x_i, -h), F_1(x_i, -h), \dots, F_s(x_i, -h)$  and  $F_0(x_i, +h), F_1(x_i, +h), \dots, F_s(x_i, +h)$ . If  $(a_1, \dots, a_n)$  is any rational  $n$ -tuple such that the non-zero coefficients of the standard sequence  $F_j(a_i, x)$  and

the quotients  $Q_j$  are defined and not zero then  $F_0(a_i, y), \dots, F_s(a_i, y)$  is the standard sequence for  $F(a_i, y)$ . Now let  $k_1(x_i), \dots, k_h(x_i)$  be a subset of  $K(x_i)$  consisting of the coefficients of  $F_j(x_i)$  of the standard sequence  $F(x_i, y)$  and of the quotients  $Q_j$  and the elements  $F_j(x_i, -h(x_1, \dots, x_n)), F_j(x_i, h(x_1, \dots, x_n)) \ 0 \leq j \leq s$ . Then from Sturm's theorem if  $(a_1, \dots, a_n)$  is any rational  $n$ -tuple for which  $k_i(x_i)$  are defined and  $k_i(a_1, \dots, a_n)$  has the same sign as  $k_i(x_1, \dots, x_n) \ 1 \leq i \leq h$  then  $F(a_i, y)$  is defined and has  $r$  roots in the real algebraic numbers. Moreover, if we refer to the bound in Sturm's theorem all the roots of  $F(a_i, y)$  are in  $(-h(a_1, \dots, a_n), h(a_1, \dots, a_n))$ . Thus the number of roots is exactly  $r$ .

Lemma 2: Let  $\{F_1(x_i, y), \dots, F_t(x_i, y)\}$  be a sequence of polynomials in  $K(x_i)[y]$  and assume that the leading coefficients are 1. The property that  $F_j(x_i, y)$  has a root  $p_j$  in the real closure  $P$  of  $K(x_i)$  and  $p_1 < p_2 < \dots < p_t$  is rationally specializable.

Proof: Since  $p_{i+1} - p_i > 0 \ 1 \leq i \leq t-1$  then  $(p_{i+1} - p_i)^{\frac{1}{2}} \in P$ . Let  $A$  be an algebraic extension field generated by the elements  $p_i$  and  $(p_{i+1} - p_i)^{\frac{1}{2}}$  and assume that  $A = K(\theta)$  with  $g(x_i, y)$  the minimum polynomial of  $\theta$ . Then  $p_i = k_i(x_i, \theta)$  and  $(p_{i+1} - p_i)^{\frac{1}{2}} = \ell_i(x_i, \theta)$  where  $\phi_i(x_i, y), \ell_i(x_i, y) \in K(x_i, y)$ . Since  $p_i$  is a root for  $F_i(x_i, y)$ ,  $F_i(x_i, \phi_i(x_i, y))$  has  $\theta$  as a root and since  $g(x_i, y)$  is the minimum polynomial of  $\theta$  so we have

$$F_k(x_i, \phi_k(x_i', y)) = G_k(x_i, y) g(x_i, y) \quad (1)$$

From the relations  $p_{i+1} - p_i = \ell_i^2(x_i, \theta)$  we have

$p_{i+1}(x_i, \theta) - p_i(x_i, \theta) - \ell_i^2(x_i, \theta) = 0$ . This means that the polynomial  $p_{i+1}(x_i, y) - p_i(x_i, y) - \ell_i^2(x_i, y) = 0$  has  $\theta$  as a root and since  $g(x_i, y)$  is the minimum polynomial for  $\theta$  so

$$p_{i+1}(x_i, y) - p_i(x_i, y) - \ell_i^2(x_i, y) = H_i(x_i, y)g(x_i, y) \quad 1 \leq i \leq t-1 \quad (2)$$

Also since  $\ell_i(x_i, \theta) \neq 0$  it has an inverse  $m_i(x_i, \theta)$  in  $A$  and since  $\ell_i(x_i, \theta) m_i(x_i, \theta) - 1 = 0$  so  $\theta$  is a root of the polynomial  $\ell_i(x_i, y) m_i(x_i, y) - 1 = 0$ . This implies that  $\ell_j(x_i, y) m_j(x_i, y) - 1 = K_j(x_i, y)g(x_i, y) \quad 1 \leq j \leq t-1 \quad (3)$

Now let  $\{k_i(x_i)\}$  be a finite subset of  $K(x_i)$  consisting of the coefficients of polynomials in  $y$  of equations (1) and (2) and (3) and a set of elements given in Lemma 1 to insure that  $g(a_i, y)$  has a real root  $c$  since  $g(x_i, y)$  has a root  $\theta$ ; if the  $a_i$  are chosen such that every  $k_n(a_i)$  is defined and has the same sign as  $k_n(x_i)$  then substituting  $c$  for  $y$  in every polynomial appearing in (1), (2) and (3) is possible. Now substituting  $y=c$  in (1) then  $F_k(a_i, y)$  has a root  $b_k = \phi_k(a_i, c)$ . Substituting  $y = c$  in (2) we have  $b_{i+1} - b_i = \phi_{i+1}(a_i, c) - \phi_i(a_i, c) = \ell_i^2(a_i, c) \geq 0$  and from (3)  $\ell_j(a_i, c) m_j(a_i, c) = 1$  so  $\ell_j(a_i, c) \neq 0$ . Hence  $b_{i+1} - b_i > 0$ , so  $F_j(a_i, y)$  has the roots  $b_j$  with  $b_1 < b_2 < \dots < b_t$ .

Proof of Theorem 7.2: Let  $P'$  be a real closure of  $K(x_i, y)$  and  $p$  a real closure of  $K(x_i)$  contained in  $P'$ . Assume that the theorem holds for  $K(x_1, \dots, x_n)$ . So we have to show that it holds for  $K(x_1, \dots, x_n, y)$  where  $y$  is an additional indeterminate. Let  $F_k(x_i, y)$  be a family of elements of  $K(x_i, y)$ . We have to show that there is  $(a_1, \dots, a_n, b)$  such that  $F_k(a_i, b)$  is defined and has the same sign as  $F_k(x_i, y)$ , for every  $k$ .

Let  $F_k(x_i, y) = F(x_i, y)$  be an arbitrary element of the given set. Write  $F(x_i, y) = \phi(x_1, \dots, x_n) P_1(x_i, y)^{e_1} \dots P_h(x_i, y)^{e_h}$  where  $\phi(x_1, \dots, x_n) \in K(x_i)$  and  $P_j(x_i, y) \in K(x_i)[y]$  are irreducible with leading coefficients 1 with  $e_j > 0$ . Then if  $(a_1, \dots, a_n, b)$  has the property that  $\phi(a_i), P_j(a_i, b)$  are defined and have the same sign as  $\phi(x_i), P_j(x_i, y)$  then  $F(a_1, \dots, a_n, b)$  is defined and has the same sign as  $F(x_i, \dots, x_n, y)$ . So we can consider the family of elements  $F_k(x_i, y)$  given, to be a finite set of elements of  $\phi(x_i)$  and irreducible polynomials in  $K(x_i)[y]$  with leading coefficients 1. Next assume that  $p_1 < p_2 < \dots < p_t$  are the roots in  $P$  of the new set. We can form a sequence  $F_1, \dots, F_t$  from this set such that  $F_j$  has the root  $p_j$   $1 \leq j \leq t$ . Since the  $F$ 's are irreducible and of characteristic 0, the roots of each  $F$  in the set are distinct. Since the  $F$ 's are relatively prime then  $G(x_i, y) = F_1(x_i, y) \dots F_t(x_i, y)$  has distinct roots.

By Lemma 1, there exists  $k_1, \dots, k_h \in K(x_i)$  such that if  $(a_1, \dots, a_n)$  is a rational  $n$ -tuple such that  $k_n(a_i)$  is defined and has the same sign as  $k_n(x_i)$   $1 \leq n \leq h$ , then  $G(a_i, y)$  has  $t$  distinct real roots. By Lemma 2, there exist elements  $k_{h+1}, \dots, k_s \in K(x_i)$  such that if  $(a_1, \dots, a_n)$  is a rational  $n$ -tuple for which  $k_m(a_i)$  is defined and has the same sign as  $k_m(x_i)$ ,  $h+1 \leq m \leq s$  then  $F_j(a_i, y)$  is defined and has a real root  $b_j$  with  $b_1 < b_2 < \dots < b_t$   $1 \leq j \leq t$ . Now we add to  $\{k_1, \dots, k_s\}$  all the  $\phi$ 's of the new constructed set and the discriminant  $d$  of  $G(x_i, y)$  which is different from zero since  $G(x_i, y)$  has distinct roots. By the induction hypothesis there exists rationals  $a_1, \dots, a_n$  such that the conditions on  $k_i$   $1 \leq i \leq s$ ,  $d$  and the  $\phi$ 's are satisfied, since they are elements of  $K(x_1, \dots, x_n)$ . In  $P[y]$  we have

$$F_j(x_i, y) = (y-p_{j1})(y-p_{j2}) \dots (y-p_{jt_j}) Q_1(y) \dots Q_{j_s_j}(y) \quad (4)$$

where  $Q_i$ 's are quadratic polynomials with leading coefficients 1, and  $\{j_1, \dots, j_t\} \subset \{1, 2, \dots, t\}$ . In the field of real numbers and by the choice of  $a_i$  we have

$$F_j(a_i, y) = (y-b_{j1}) \dots (y-b_{jt_j}) S_1(y) \dots S_{s_j}(y) \dots \quad (5)$$

$S_k(y)$  is irreducible with leading coefficients 1,  $1 \leq k \leq s_j$ . Since  $y$  is transcendental over  $K(x_i)$  and the  $p_i$ 's are algebraic over  $K(x_i)$ . So  $y \neq p_i$ , and so  $y$  belongs to one



of the following intervals in  $P'$   $(-\infty, p_1), (p_1, p_2), \dots, (p_t, \infty)$ . Also we notice that  $Q(y) > 0$  in  $P'$  and  $S(b) > 0$ , since they are irreducible quadratics. So from (4) and (5) if  $y \in (p_k, p_{k+1})$  and  $b \in (b_k, b_{k+1})$  then  $F_j(x_i, y)$  and  $F_j(a_i, b)$  have the same sign and this holds for every  $j$ . Since we can find a rational in any open interval, the theorem is proved.

## 8. Formalized Euclidean Algorithm and Sturm's Theorem

The object of this section is to use Sturm's theorem for equations whose coefficients are parameters that take values in a real closed field. This will depend on a parametrized version of the Euclidean algorithm for determining the greatest common divisor of polynomials that we are going to discuss.

In the last few sections we shall determine a method for testing the solvability, in a real closed field, of a finite system of polynomial equations, inequations and inequalities whose coefficients are parameters that take values in the real closed field. The main result, Tarski's theorem, states that given such a system we can find in a finite number of steps a finite system of polynomial equations, inequations and inequalities in the coefficients of the given system, such that the given system has a solution in the real closed field if and only if one of the derived systems is satisfied by the coefficients of the given system.

Example 1: Let  $f(x) = x^3 + px + q$ ,  $P \neq 0$  and  $p$  and  $q$  parameters that may assume any real number.  $f'(x) = 3x^2 + p$ . From the equations  $(x^3 + px + q) = (\frac{1}{3}x)(3x^2 + p) - (\frac{-2p}{3}x - q)$  and  $(3x^2 + p) = (\frac{-2p}{3}x + \frac{27q}{4p})(\frac{-2p}{3}x - q) - (\frac{-4p^3 - 27q^2}{4p^2})$  we get  $x^3 + px + q$ ,  $3x^2 + p$ ,  $\frac{-2p}{3}x - q$ ,  $\frac{-4p^3 - 27q^2}{4p^2}$  as the standard sequence and

if  $p \neq 0$  as asserted this sequence is equivalent to  $x^3+px+q$ ,  $3x^2+p$ ,  $-2px-3q$ ,  $-4p^3-27q^2$  which is a Sturm sequence and we notice that  $-4p^3-27q^2$  is the discriminant  $d$ . Now we can use Sturm's theorem to show that  $f$  has a single root or three roots according as  $d < 0$  or  $d > 0$ .

If  $d < 0$  we can choose  $k$  so large that all the roots of  $f(x)$  are in  $[-k, k]$  and moreover the roots of  $f_i(x)$  of the Sturm's sequence are in  $[-k, k]$  so the sign of  $f_i(k)$  is the same as the sign of the leading coefficient of  $f_i$  and the sign of  $f_i(-k)$  is the same as the sign of  $(-1)^m a_m$  where  $f_i(x) = a_m x^m + \dots + a_0$ . So if  $d < 0$  then  $x^3+px+q$ ,  $3x^2+p$ ,  $-2px-3q$ ,  $d$  has the corresponding signs  $+$ ,  $+$ , the sign of  $-2p$ ,  $-$  if  $x=k$  and the sign  $(-1)^3$ ,  $(-1)^2$ ,  $(-1)$  the sign of  $-2p$ ,  $-$  if  $x=-k$ . So  $V_{-k} - V_k = 2 - 1 = 1$  if  $-2p > 0$ , also  $V_{-k} - V_k = 2 - 1$  if  $2p < 0$ . If  $d > 0$  we observe that  $V_{-k} - V_k = 3 - 0$  since  $p$  has to be negative.

Example 2.  $f(x) = x^4 + qx^2 + rx + S$ . We see that if  $L = 8qs - 2q^3 - r^2$  and  $d = 4(4s + \frac{q}{3})^3 - 27(\frac{8}{3}qs - r^2 - \frac{2}{27}q^3)$  ( $d$  is the discriminant of  $f$ ), by the same method as in the previous example we can prove that if  $d < 0$  then the number of real roots of  $f$  is two and if  $d > 0$ ,  $q < 0$ ,  $L > 0$  then  $f$  has four distinct roots and if  $d > 0$ , and either  $q \geq 0$  or  $L \leq 0$  then  $f$  has no real roots. Moreover, Tarski's method shows that if the coefficients of  $f(x)$  satisfy one of the following systems:

- (i)  $d < 0$
- (ii)  $d > 0, q < c, L > 0$
- (iii)  $d = 0, r \neq 0$
- (iv)  $d = 0, r = 0, q < 0$

then  $f(x)$  has a root in the real closed field.

Now for  $A = K[t_1, \dots, t_r]$  where  $K = \mathbb{Z}$  or  $\mathbb{Z}/(p)$ ,  $p$  a prime, let  $F(t_1, \dots, t_r, x), G(t_1, \dots, t_r, x) \in A[x]$  so  $F(t_1, \dots, t_r, x) = u_n x^n + u_{n-1} x^{n-1} + \dots + u_0$  and  $G(t_1, \dots, t_r, x) = v_m x^m + v_{m-1} x^{m-1} + \dots + v_0$  where  $u_i, v_i \in K[t_1, \dots, t_r]$ . We assume  $G(t_i, x) \neq 0$  and we take a section of  $G$ , say  $G_k(t_i, x) = v_k x^k + \dots + v_0$ , where  $v_k(t_1, \dots, t_r) \neq 0$  and  $k \leq m$  then by the division algorithm we can write  $(v_k(t_i))^{e_k} F(t_i, x) = Q_k(t_i, x) G_k(t_i, x) - R_k(t_i, x)$  where  $e_k$  is an integer and is the larger of 0 and  $n - k + 1$ . For the application of Sturm's theorem we need  $e_k$  to be even. So we choose  $e_k = 0$  if  $n < k$  or the smallest even integer  $\geq n - k + 1$ . By the division algorithm this factorization is unique.

If  $R$  is an extension field of  $K$  then if  $(c_1, \dots, c_r) \in K^{(r)}$  either  $v_k(c_i) = 0$  for every  $k, 0 \leq k \leq m$  and so  $G(c_i, x) = 0$  or there exists  $k, 0 < k \leq m$  such that  $v_k(c_i) \neq 0, v_j(c_i) = 0, j > k$  and so  $G(c_i, x) = v_k(c_i) x^k + \dots + v_0(c_i)$ . So  $G(c_i, x) = G_k(c_i, x)$ , and  $(v_k(c_i))^{e_k} F(c_i, x) = Q(c_i, x) G(c_i, x) - R_k(c_i, x)$ . Now since  $v_k(c_i, x) \neq 0$  and  $\deg R_k(c_i, x) < \deg G(c_i, x)$ .  $Q_k(c_i, x)$  and  $-R_k(c_i, x)$  differ

by a non-zero multiplier  $(v_k(c_i))^{-e_k}$  from the quotient and remainder when dividing  $F(c_i, x)$  by  $G(c_i, x)$ . We introduce the following set of systems of relations in  $A = K[t_1, \dots, t_r]$ . If  $G(t_i, x) = v_m x^m + \dots + v_0 \neq 0$  then  $T_{-\infty} = \{v_0=0, v_1=0, \dots, v_m=0\}$ .  $T_k = \{v_k \neq 0, v_j=0 \text{ } k < j \leq m\}$  if  $v_k(t_i) \neq 0$ . For example, if  $G(p, q, x) = (p+q)x^3 + px + q$  then  $v_0=q, v_1=p, v_2=0, v_3=p+q$  and  $T_{-\infty} = \{p+q=0, p=0, q=0\}$   $T_0 = \{q \neq 0, p=0, p+q=0\}$   $T_1 = \{p \neq 0, p+q=0\}$  and  $T_3 = \{p+q \neq 0\}$ .

We observe that if  $\theta = \{T_{-\infty}, T_k\}$  then  $\theta$  defines a cover for  $A = K[t_1, \dots, t_r]$  in the following sense: if  $F$  is a field extension of  $K$  and if we define  $T_k(F) = \{(c_1, \dots, c_r) \in F^{(r)} / (c_1, \dots, c_r)\}$  satisfies the relations in  $T_k\}$  then  $F^{(r)} = \cup T_k(F)$ , note that  $(c_1, \dots, c_r) \in T_k(F)$  if and only if  $G(c_i, x)$  is of degree  $k$ . So it is obvious that for every  $(c_1, \dots, c_r) \in F^r$ ,  $G(c_i, x)$  has a degree  $0 < k \leq m$  or  $G(c_i, x) = 0$ . In any field  $F$  a system of equations  $l_1 \neq 0, \dots, l_h \neq 0$  is equivalent to a single equation  $l_1 \cdot l_2 \dots l_h \neq 0$  and if  $F$  is a real closed field a system of equations  $l_1 = 0, \dots, l_h = 0$  is equivalent to a single equation  $l_1^2 + \dots + l_h^2 = 0$ , so if we add to  $T_k$  the trivial equation  $0=0$  and the inequation  $1 \neq 0$  we can assume that each  $T_k$  consists of one equation and one inequation, if we are dealing with a real closed field.

Assume  $C = \{S_1, \dots, S_t\}$  is a cover of  $A$  and  $T$  is a finite set of equations and a single inequation determined

by elements of  $A$ , if we define  $T^{(j)}$   $1 \leq j \leq t$  to be the set having the equations of  $T$  and  $S_j$  and the inequation which is the product of the inequations of  $T$  and  $S_j$ , then we see that  $T^{(j)}(F) = S_j(F) \cap T(F)$  and since  $\cup S_j(F) = F^{(r)}$  so  $T(F) = \cup T^{(j)}(F)$ . If we have

$C = \{T_1, T_2, \dots, T_\ell\}$  is a cover of  $A$  then  $\{T_1^{(1)}, T_1^{(2)}, \dots, T_1^{(3)}, T_2, \dots, T_\ell\}$  is a cover which is a refinement of the first one.

Definition 8.1: If  $f(x), g(x) \in R[x]$

where  $R$  is a field then by the

Euclidean algorithm we can determine

a greatest common division of  $f, g$  by constructing a sequence of polynomials  $f_i(x)$   $0 \leq i \leq s$  such that  $f_0(x) = f(x)$ ,  $f_1(x) = f'(x)$  and  $f_{i-1}(x) = q_i(x)f_i(x) - f_{i+1}(x)$ ,  $f_{s+1}(x) = 0$ . We shall call the sequence  $f_i(x)$  the Euclidean sequence for  $f(x)$ , and  $g(x)$ .

If  $g=0$  then the Euclidean sequence for  $f, 0$  by definition is  $f, 0, 0$ .

Theorem 8.1: Let  $F, G \neq 0 \in A[x]$ . Then we can construct

in a finite number of steps a cover  $C = \{S_1, \dots, S_h\}$

which is a refinement of the cover determined by the coefficients of  $G$ , and sequences of polynomials  $F_{j_0} =$

$F, F_{j_1}, \dots, F_{j_{k_j}} \in A[x]$   $1 \leq j \leq h$  such that for any field extension  $F$  of  $K$  and any  $(c_1, \dots, c_r) \in S_j(F)$  the terms of the

sequence  $F_{j_0}(c_i, x), F_{j_1}(c_i, x), \dots, F_{j_{k_j}}(c_i, x), F_{j_{k_j+1}}(c_i, x)$   
 $= 0$  differ by a non-zero multiplier from those of the  
 Euclidean sequence of  $F(c_i, x), G(c_i, x)$  and the multipliers  
 are positive if  $F$  is real closed.

Proof: If  $C = \{T_{-\infty}, T_k\}$  and if  $k \neq -\infty$  we determine  $Q_k$  and  
 $-R_k$  by dividing  $F$  by  $G_k = v_k x^k + \dots + v_0$  by the Euclidean  
 algorithm if  $-R_k = 0$  then  $F_{k_0} = F, F_{k_1} = G_k$  and  $F_{k_2} = 0$  satis-  
 fies the stated condition.

If  $-R_k \neq 0$  then from  $F = Q_k G_k - R_k$  we see that the  
 sum of degree of  $Q_k$  and  $-R_k$  is less than that of  $F$  and  $G_k$ ,  
 so using induction we can assume the result for  $Q_k$  and  
 $-R_k$ . So we can assume that we have a cover  $C_k = \{S_{k_1},$   
 $S_{k_2}, \dots, S_{k_\ell}\}$  and sequences of polynomials  $F_{k_\ell 0}, F_{k_\ell 1}, \dots,$   
 $F_{k_\ell s_{k_\ell}}$  satisfies the stated conditions of the theorem.  
 If we refine the cover  $C = \{T_{-\infty}, T_k\}$  by defining  $T_k^{(j)}$  to  
 be the set of equations of  $T_k$  and  $S_{k_j}$  and of the inequa-  
 tion which is the product of the inequations of  $T_k$  and  
 $S_{k_j}$  then with each  $T_k^j$  we associate the sequence of func-  
 tions  $F_{k_j 0}, F_{k_j 1}, \dots, F_{k_j s_{k_j}}$ . For the term  $T_{-\infty}$  we associate  
 the sequence  $\{F, 0, 0\}$  then  $C$  with this sequence satisfies  
 the conditions stated in the theorem.

Example: Let  $F(p, q, x) = x^3 + qx + q$  and  $G(p, q, x) = F'(p, q, x)$   
 $= 3x^2 + p$ . Now  $v_0 = p, v_1 = 0, v_2 = 3$ , so  $P_{-\infty} = \{P=0, 3=0\}$  and  
 $T_0 = \{P \neq 0, 3=0\}, T_2 = \{3 \neq 0, 0=0\}$  and we have  
 $C = \{\{P=0, 3=0\}, \{P \neq 0, 3=0\}, \{3 \neq 0, 0=0\}\}$ . Since  $3 \neq 0$  cannot

hold  $T_{-\infty}(F) = \phi$  and  $T_0(F) = \phi$  and we have  $C = \{\{3 \neq 0, 0 = 0\}\} = \{\{1 \neq 0, 0 = 0\}\}$ . Now we consider  $F$  and  $G_2 = 3x^2 + p$ . When we divide  $F$  by  $G_2$  we have  $-R_2 = -(6px + 9q)$ . Since  $-R \neq 0$  we consider the pair of functions  $F = G_2 = 3x^2 + p$  and  $G = -R = (-6px - 9q)$ . We have  $C' = \{T_{-\infty}, T_1, T_0\} = \{\{p=0, q=0, 1 \neq 0\}, \{p \neq 0, 0=0\}, \{q \neq 0, p=0\}\}$ .  $p_1 \neq 0$  in  $T_1$  so when dividing  $F = 3x^2 + p$  by  $G_1 = -6px - 9q$  we have  $-R = -9(4p^3 + 27q^2)$ . For  $T_1$  we have the cover  $d_1 = \{T_{-\infty}, T_0\}$  corresponding to  $G(p, q, x) = -9(4p^3 + 27q^2)$  which is  $\{\{4p^3 + 27q^2 = 0, 1 \neq 0\}, \{4p^3 + 27q^2 \neq 0, 0 = 0\}\}$  with correspondence sequences of polynomials  $3x^2 + p, -6px - 9q, 0$  and  $3x^2 + p, -6px - 9q, 4p^3 + 27q^2, 0$ .

For  $T_0$  we have  $p = 0, q \neq 0$ , so  $F = 3x^2 + p$  and  $G_0 = -9q$ , and when we divide  $F$  by  $G_0$  we have remainder 0, so we have the refinement of  $C$  into  $C'$  such that

$$C' = \{T_{-\infty}, T_1^{(1)}, T_1^{(2)}, T_0\} \\ = \{\{p=0, q=0, 1 \neq 0\}, \{p \neq 0, 4p^3 + 27q^2 = 0\}, \{p(4p^3 + 27q^2 \neq 0, 0 = 0\}, \\ \{q \neq 0, p = 0\}\}$$

where  $\{T_1^{(1)}, T_1^{(2)}\}$  is the refinement of  $T_1$  by the cover  $C_1$  and the corresponding sequences are

$$\text{for } T_{-\infty}: x^3 + px + q, 3x^2 + p, 0.$$

$$\text{for } T_1^{(1)}: x^3 + px + q, 3x^2 + p, -6px - 9q, 0.$$

$$\text{for } T_1^{(2)}: x^3 + px + q, 3x^2 + p, -6px - 9q, -9(4p^3 + 27q^2), 0$$

$$\text{for } T_0: x^3 + px + q, 3x^2 + p, -9q, 0.$$

We can now state the parameterized version of Sturm's theorem.



Theorem 8.2: Let  $F(t_i, x) = u_n x^n + u_{n-1} x^{n-1} + \dots + u_0 \in A[x]$  where  $u_j(t_i) \in A = Z[t_1, \dots, t_r]$ , the  $t_i$ , and  $x$  indeterminants. Then we can determine in a finite number of steps a finite set of polynomial relations of the form  $C=0$ .  $C \neq 0$ ,  $C \neq 0$  where  $C \in A$  such that for any real closed field  $R$  the statement  $F(c_i, x) = 0$  for  $c_i \in R$  has a solution is equivalent to the validity for  $t_i = c_i$  of every relation in any  $T_k$ .

Proof: Let  $G(t_i, x) = F'(t_i, x) = nu_n x^{n-1} + (n-1)u_{n-1} x^{n-1} + \dots + u_1$ . If  $G = 0$  then  $F(t_i, x) = u_0 \in A$  and the result of the theorem is trivial. If  $G(t_i, x) \neq 0$  so we can apply theorem 8.2 to obtain a cover  $d = \{S_j\}$  and sequences of polynomials  $F_{j_1}, \dots, F_{j_{s_j}} \in A[x]$  such that if  $(c_1, \dots, c_r) \in S_j(R)$  then  $F_{j_1}(c_i), \dots, F_{j_{s_j}}(c_i)$  differ by a non-zero multiplies from the standard sequence for  $F(c_i, x)$ . If we take one of these  $S_j$  and assume  $(c_1, \dots, c_r) \in S_j(R)$  then either  $u_n(c_i) = \dots = u_1(c_i) = 0$  or there is  $1 \leq m \leq n$  such that  $u_m(c_i) \neq 0$  and  $u_j(c_i) = 0$   $m < j \leq n$ , then the roots of  $F(c_i, x) = 0$  are in the interval  $(-k, k)$  when  $k = (m+1) + \sum_0^{m-1} u_j(c_1, \dots, c_r)^2 u_m(c_1, \dots, c_r)^{-2}$ . Since the terms of the sequence  $F_{j_0}(c_i, x), \dots, F_{j_{s_j}}(c_i, x)$  are positive multiples of those of the standard sequence for  $F_{j_0}(c_i, x)$  it follows that  $F(c_i, x)$  has a root if and only if  $F_{j_0}(c_i, -k), \dots, F_{j_{s_j}}(c_i, -k)$  exceeds those of  $F_{j_0}(c_i, k), \dots, F_{j_{s_j}}(c_i, k)$ . We now write  $g_{jk}(t_1, \dots, t_r) = u_m^{2nk}$

$F_k(t_i, m+1 + \sum_0^{m-1} u_j u_m^{-2})$  and  $h_{jk}(t_1, \dots, t_r) = u_m^{2n_k} F_{jk}(t_i,$   
 $-(m+1) - \sum_0^{m-1} u_j^2 u_m^{-2})$ .  $n_k$  is the degree in  $x$  of  $f_{jk}$  so

$g_{jk}(c_i), h_{jk}(c_i)$  differ from  $F_{jk}(c_i, k), F_{jk}(c_i, -k)$  by positive multipliers. So for  $(c_1, \dots, c_r) \in S_j(R)$   $F(c_i, x) = 0$  has a root if the number of variation in sign of  $h_{j_0}(c_i), \dots, h_{j_{s_j}}(c_i)$  exceeds that of  $g_{j_0}(c_i), g_{j_1}(c_i), \dots, g_{j_{s_j}}(c_i)$ , so we consider all possible orderings  $g_{j_0} \geq 0, g_{j_k} \geq 0, g_{j_s} \geq 0, h_{j_0} \leq 0, h_{j_k} \geq 0, h_{j_s} \geq 0$   $1 < k < j_{s-1}$  and we form all possible collections of  $g$ 's and  $h$ 's such that the number of variation of  $h$ 's sequences exceeds that of  $g$  and we obtain a collection of relation for  $T_k$  and we do this for all the other elements of the cover. We can still apply this theorem for the existence of roots of  $F(t_i, x) = 0$  in  $(-c, c)$ . Just replace  $k$  by  $c$  and we obtain a corresponding collection  $\{T_1, \dots, T_s\}$ . Each consists of a finite set of relations of the form  $C=0, C>0, C \neq 0, C \in A$ .

## 9. Elimination Procedures Resultants

We need to generalize theorem 8.2 to a system of equations, inequations, and inequalities with several unknowns. Before this we need the following:

Lemma 9.1: Let  $f_i(x)$   $1 \leq i \leq m, g(x) \in F[x]$ ,  $F$  is a field and let  $d(x)$  be the greatest common divisor of the  $f_i(x)$  then there is a  $p$  in some extension field of  $F$  such that  $f_i(p) = 0, 1 \leq i \leq m$  and  $g(p) \neq 0$  if and only if either all

$f_i(x) = 0$  and  $g(x) \neq 0$  or  $d(x) \neq 0$  and  $d(x)$  is not a factor of  $g(x)$   $\deg d(x)$ .

Proof: If  $f_i(x) = 0$  for every  $i$  and  $g(x) \neq 0$  then the result is obvious. Since we can choose  $p$  not a root of  $g(x)$  since  $g(x)$  has a finite number of roots then  $f_i(p) = 0$  and  $g(p) \neq 0$ . Assume that not all  $f_i(x) = 0$   $1 \leq i \leq m$  then there is a greatest common divisor  $d(x)$  of  $f_i(x)$  and  $d(x) \neq 0$  for all  $i$  in some extension field of  $F$  if and only if  $d(p) = 0$ . So if some  $f_i(x) \neq 0$   $1 \leq i \leq m$  then the statement of the theorem holds if and only if  $d(x)$  is of positive degree and there is an irreducible factor of  $d(x)$  which is not a factor of  $g(x)$ , for if this is true and  $p(x)$  is such a factor and  $\theta$  is a root of  $p(x)$  then  $d(\theta) = 0$  and  $f_i(\theta) = 0$ ,  $g(\theta) \neq 0$ . On the other hand, if  $d(x) = 1$ , then  $f_i(x) = 0$   $1 \leq i \leq m$  has no solution. If every irreducible factor of  $d(x)$  is a factor of  $g(x)$  then if  $d(p) = 0$  in some extension field then  $g(p) = 0$  since  $p(x)/g(x)$  where  $p(p) = 0$  and  $p(x)$  is an irreducible factor of  $d(x)$  and also no solution of  $f_i(x) = 0, g(x) \neq 0$  exists. Since  $d(x) = 1$  or every irreducible factor of  $d(x)$  divides  $g(x)$  is equivalent to  $d(x) / g(x)^{\deg d(x)}$

Remark: Since  $g_1(x) \neq 0, g_2(x) \neq 0, \dots, g_s(x) \neq 0$  is equivalent to  $g(x) \neq 0$  where  $g(x) = \prod_1^s g_i(x)$  then Lemma (9.1) can be stated more generally with  $g_1(p) \neq 0, \dots, g_s(p) \neq 0$  substituted for  $g(p) \neq 0$ .

Lemma 9.2: Let  $F(t_i, x), G(t_i, x), \dots, H(t_i, x) \in A[x]$  where  $A = K[t_1, \dots, t_r]$  and  $K = \mathbb{Z}$  or  $\mathbb{Z}/(p)$ .  $p$  is a prime then we can find in a finite number of steps a cover  $C = \{S_1, \dots, S_h\}$  and for each  $S_k$  a polynomial  $D_k(t_i, x) \in A[x]$  such that for any extension field  $F$  of  $K$  and any  $(c_1, \dots, c_r) \in F^{(r)}$  such that  $(c_1, \dots, c_r) \in S_k(R)$  then  $D_k(c_i, x)$  is a greatest common divisor of  $F(c_i, x), G(c_i, x), \dots, H(c_i, x)$ .

Proof: If every polynomial is zero then the result is trivial and if the number of polynomials is one it is also obvious since  $D_1(t_i, x) = F(t_i, x)$  works. If we have two polynomials  $F(t_i, x), G(t_i, x)$  then by theorem 8.1 the result follows immediately. So we use induction and assume that the result is true for polynomials  $F_1(t_i, x), F_2(t_i, x), \dots, F_n(t_i, x)$ . Assume we have  $F_{n+1}(t_i, x)$  in addition then we can assume that we have a cover  $C' = \{T_1, \dots, T_s\}$  and polynomials  $E_k(t_i, x)$  satisfying the stated condition for  $F_1, \dots, F_n$ . We can apply theorem 8.1 to each pair,  $E_k(t_i, x)$  and  $F_{n+1}(t_i, x)$ , and obtain a cover  $C_i = \{S_{k\ell}\}$  and corresponding polynomials  $E_{k\ell}$  such that  $(c_1, \dots, c_r) \in S_{k\ell}$ .  $E_{k\ell}(c_i, x)$  is a greatest common divisor of  $E_k(c_i, x)$  and  $F_{n+1}(c_i, x)$ , hence a greatest common divisor of  $F_1, \dots, F_n$ . Now we refine the cover  $C'$  by replacing each  $T_k$  by  $T_k^{(1)}, T_k^{(2)}, \dots$  determined by the cover  $C_k$  and so we have the cover  $C = \{T_k^\ell\}$  and the corresponding  $E_{k\ell}$  satisfying the theorem.

Theorem 9.1: Let  $K = \mathbb{Z}$  or  $\mathbb{Z}/(p)$ ,  $p$  is prime and let  $A = K[t_1, \dots, t_t]$  and  $B = A[x_1, \dots, x_n]$ ,  $x_i, t_i$  indeterminants. Then if  $F_1, \dots, F_m, G \in B$ , one can determine in a finite number of steps a finite collection  $\{T_1, T_2, \dots, T_s\}$  where  $T_j = \{f_{j1}, f_{j2}, \dots, f_{jm}, g_j\} \subset A$  such that if  $F$  is an extension field of  $K$  and  $(c_1, \dots, c_r) \in F^{(r)}$  then the system of equations and inequations  $F_1(c_1, \dots, c_r, x_1, \dots, x_n) = 0$ ,  $F_2(c_1, \dots, c_r, x_1, \dots, x_n) = 0, \dots, F_m(c_1, \dots, c_r, x_1, \dots, x_n) = 0$ ,  $G(c_1, \dots, c_r, x_1, \dots, x_n) \neq 0 \dots (1)$ , has a solution in some extension field  $E$  of  $F$  if and only if the system of equations and inequation  $f_{j1}(c_1, \dots, c_r) = 0, \dots, f_{jm}(c_1, \dots, c_r) = 0$ ,  $g_j(c_1, \dots, c_r) \neq 0$  is solvable for some  $1 \leq j \leq s \dots (2)$ .

Proof: Assume that  $n=1$ , then there is a cover  $C = \{S_j\}$  and, for each  $S_j$ , a polynomial  $D_j(t_i, x) \in A[x]$  such that if  $(c_1, \dots, c_r) \in S_j(F)$  then  $D_j(c_1, \dots, c_r, x)$  is a greatest common divisor of  $F_1(c_i, x), \dots, F_m(c_i, x)$ , and such that for every  $(c_1, \dots, c_r) \in S_j(F)$  either  $D_j(c_i, x) = 0$  or  $D_j(c_i, x) \neq 0$  for every  $(c_1, \dots, c_r) \in S_j(F)$  and in this case there is  $R_j(t_i, x) \in A[x]$  such that for  $(c_1, \dots, c_r) \in S_j(F)$ ,  $R_j(c_i, x)$  differs by a non-zero multiplier in  $F$  from the remainder when dividing  $G(c_i, x) x^{\deg_x D_j}$  by  $D_j(c_i, x)$ .

This follows from Lemma (9.2) since we can construct a cover  $C = \{T_k\}$  and polynomials  $D_k(t_i, x)$  such that for  $(c_1, \dots, c_r) \in T_k(F)$ ,  $D_k(c_i, x)$  is a greatest common divisor

of  $F_1(c_i, x), \dots, F_m(c_i, x)$ , and for each  $D_k(t_i, x) \neq 0$  there is a cover  $C_k = \{S_{k\ell}\}$  such that for  $(c_1, \dots, c_r) \in S_{k\ell}(F)$  either  $D_k(c_i, x) = 0$  or for all  $(c_1, \dots, c_r) \in S_{k\ell}(F)$ ,  $D_k(c_i, x) \neq 0$  then we can apply division algorithm to find polynomials  $R_{k\ell}(t_i, x) \in A[x]$  such that  $(c_1, \dots, c_r) \in S_{k\ell}(F)$  then  $R_{k\ell}(c_i, x)$  differ by non-zero multiplier from the remainder on dividing  $G(c_i, x)$  by  $D_j(c_i, x)$  and finally we refine the cover  $T = \{T_k\}$  by substituting each  $T_k$  by  $\{T_k^{(1)}, T_k^{(2)}, \dots\}$  defined by the cover  $\{S_{k\ell}\}$ . So we have the cover  $C = \{S_j\}$  and polynomials  $D_j$ .

Next we consider all  $(c_1, \dots, c_r) \in S_j(F)$  and we begin to find for which  $(c_1, \dots, c_r)$  the system (1) has a solution, first if  $D_j(c_1, \dots, c_r) = 0$  then (1) has a solution if  $G(c_i, x) \neq 0$  by Lemma (1) and so if the coefficients of a power of  $x$  in  $G(c_i, x)$  is not zero. If  $D_j(c_i, x) \neq 0$  then a solution for (1) exists in some extension field of  $F$  if and only if  $R_j(t_i, x) \neq 0$  since by Lemma 1 we need  $D_j(c_i, x)$  is not a factor of  $G(c_i, x)$  and so this is true if some coefficient of a power of  $x$  in  $R_j(t_i, x)$  is not zero. We see also that the two cases  $G(t_i, x) = 0$  and  $R_j(t_i, x) = 0$  implies that (1) has no solution. So by excluding these two cases we can obtain the system (2) by multiplying the inequations defining  $S_j$  by a non-zero coefficient of  $G(t_i, x)$  if  $D_j(c_i, x) = 0$  and by a non-zero coefficient of  $R_j(t_i, x)$  if  $D_j(c_i, x) \neq 0$  so this

inequation together with the equations defining  $S_j$  forms one of the system (2) and doing this for all  $S_j$  we obtain the system (2).

Now we proceed by induction on  $n$  and we assume  $n > 1$  so we can consider  $t_1, t_2, \dots, t_r, x_1, \dots, x_{n-1}$  as parameters and apply the previous result to obtain a finite set  $C = \{A_j\}$  where  $A_j$  consists of polynomial equations and inequation with coefficients in  $K$  in the indeterminant  $t_1, \dots, t_r, x_1, \dots, x_{n-1}$  satisfying the conditions for one unknown  $x_n$ . Then using the induction hypothesis we can assume that for each  $A_j$  we have a finite number of systems of polynomial equations and an inequation with coefficients in  $K$  in the indeterminant  $t_1, \dots, t_r$ , if  $M_1, \dots, M_s$  are the systems obtained then this satisfied the conditions of the system (1), for if  $(c_1, \dots, c_r) \in F^{(r)}$  has the property that (1) has a solution  $(p_1, \dots, p_r)$  in some extension field  $E$  of  $F$  then  $(c_1, \dots, c_r, p_1, \dots, p_{n-1}) \in E^{n+r-1}$  has the property that for this choice of  $(t_1, \dots, t_r, x_1, \dots, x_{n-1})$  (1) has the solution  $p_n$  so  $(c_1, \dots, c_r, p_1, \dots, p_n)$  satisfies one of the systems  $p_j$  and consequently one of  $M_k$ . Conversely, if  $(c_1, \dots, c_r), c_i \in F$  satisfies one of the systems  $M_k$ , then there exists  $p_i$  in an extension field  $E$  of  $F$  such that one of the systems is solvable for  $p_1, \dots, p_{n-1}$  in  $E$  so there is an extension field  $E'$  of  $E$  and consequently of  $F$  such that  $(p_1, \dots, p_n)$  is a solution

for (1) for  $t_i = c_i$  and so  $M_k$  are the required systems.

Next we have the following criterion for the existence of a common factor of positive degree of two polynomials.

Theorem 9.2. Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  and  $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$  where  $n \geq 0$ ,  $m \geq 0$  and put

$$\text{Res}(f, g) = \begin{vmatrix} a_n & a_{n-1} & \dots & \dots & \dots & a_0 & \dots & \dots & \dots & \dots & \dots \\ 0 & a_n & a_{n-1} & \dots & \dots & \dots & a_0 & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & a_n & a_{n-1} & \dots & \dots & \dots & \dots & a_0 \\ b_m & b_{m-1} & \dots & \dots & \dots & \dots & \dots & b_0 & \dots & \dots & \dots \\ 0 & b_m & b_{m-1} & \dots & \dots & \dots & \dots & \dots & b_0 & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & b_m & b_{m-1} & \dots & \dots & \dots & \dots & \dots & b_0 \end{vmatrix} \begin{matrix} m \text{ rows} \\ n \text{ rows} \end{matrix}$$

Then  $\text{Res}(f, g) = 0$  if and only if  $a_n = 0 = b_m$  or  $f(x)$  and  $g(x)$  have a common factor of positive degree.

Proof: If  $a_n = 0 = b_m$  then the first column of the determinant is zero so  $\text{Res}(f, g) = 0$ .

Next assume that  $f(x)$  and  $g(x)$  have a common factor  $h(x)$  of positive degree and either  $a_n \neq 0$  or  $b_m \neq 0$ , then by symmetry if  $a_n \neq 0$  then we can write  $f(x) = f_1(x)h(x)$  and  $g(x) = g_1(x)h(x)$  and  $f_1(x) \neq 0$ , and if  $\text{degree } h(x) = k$  then  $\text{deg } f_1(x) = n - k$ ; if  $g(x) = 0$  then  $g_1(x) = 0$  or from



the equation,  $f(x)g_1(x) = g(x)f_1(x)$  we conclude that  $\deg g_1(x) \leq m-1$ . In any case, we can write  $f_1(x) = -c_{n-1}x^{n-1} - c_{n-2}x^{n-2} - \dots - c_0$ ,  $g_1(x) = d_{m-1}x^{m-1} + \dots + d_0$  and some  $c_i \neq 0$  since  $f_1(x) \neq 0$ , we can substitute for  $fg_1 = gh_1$  and we have

$$(a_n x^{n-1} + \dots + a_0)(d_{m-1} x^{m-1} + \dots + d_0) + (b_m x^m + \dots + b_0) \\ (c_{n-1} x^{n-1} + \dots + c_0) = 0 \dots \quad (4)$$

If we equate the coefficients of the  $x$ 's we get a system of equations  $a_n d_{m-1} + b_m c_{n-1} = 0$

$$a_n d_{m-2} + a_{n-1} d_{m-1} + b_m c_{n-2} + b_{m-1} c_{m-2} = 0 \dots \quad (5) \\ a_0 d_0 + b_0 c_0 = 0$$

We can consider this system as a linear equation in the  $c$ 's and  $d$ 's in the order  $d_{m-1}, d_{m-2}, \dots, d_0, c_{n-1}, \dots, c_0$ , since this system has a non-trivial solution since not all the  $c$ 's and  $d$ 's are zeros so the determinant of the coefficient matrix =  $\text{Res}(f, g) = 0$ . Conversely assume  $\text{Res}(f, g) = 0$  then from equations (4) and (5) we conclude that there exist  $f_1(x)$  and  $g_1(x)$  such that  $f(x)g_1(x) = g(x)f_1(x)$  and  $\deg f_1 \leq n-1, \deg g_1 \leq m-1$  and not both  $f_1$  and  $g_1$  are zero. If we assume  $f_1 \neq 0$  then if  $g_1(x) = 0$  we have  $fg_1 = gf_1$  implies that  $g = 0$  so  $b_m = 0$ . Hence either  $a_n = 0$  or  $f(x)$  is a non-zero common factor of  $f$  and  $g$ . If  $f_1 \neq 0$  and  $g_1 \neq 0$  then either  $g = 0$  and hence  $b_m = 0$  and so either  $a_n = b_m = 0$  or there is a common

factor of positive degree of  $f(x)$  and  $g(x)$ . Finally, if  $f_1(x) \neq 0$ ,  $g_1(x) \neq 0$  and  $g(x) \neq 0$  then either  $a_n = b_m = 0$  or  $a_n \neq 0$  or  $a_n \neq 0$  and in this case  $\deg f_1(x) \leq n-1$  and from  $f(x)g_1(x) = g(x)f_1(x)$  and factoring both sides into irreducible factors we see that one of the irreducible factors of  $f(x)$  must divide one of the irreducible factors of  $g(x)$  and conversely. So  $f(x)$  and  $g(x)$  have a common factor of positive degree.

Remark: In theorem 9.1 the system of equations and inequation of the form (1) is solvable if and only if the following system involving one more indeterminate  $x_{i+1}$  is solvable.

$F_1(c_1, \dots, c_r, x_1, \dots, x_n) = \dots = F_m(c_1, \dots, c_r, x_1, \dots, x_n) = 0$  and  $x_{n+1} G(c_1, \dots, c_r, x_1, \dots, x_n) - 1 = 0$ . Since  $x_{n+1} G(c_1, \dots, c_r, x_1, \dots, x_n) - 1 = 0$  is equivalent to  $G(c_1, \dots, c_r, x_1, \dots, x_n) \neq 0$ , by this case we get rid of the inequation in the theorem and consider only a system of equations.

## 10. The Decision Method for an Algebraic Curve.

This section will give a method due to A. Seidenberg for deciding whether or not an equation  $f(x,y) = 0$ ,  $f(x,y) \in R[x,y]$  has a real root,  $R$  a real closed field. This will depend on the simple fact that if  $f(x,y) = 0$  has a real root, then it has a root nearest the origin and this root is also a solution of  $g(x,y) = x(\frac{\partial f}{\partial y}) - y(\frac{\partial f}{\partial x}) = 0$ . If  $(a,b)$  is such a solution, then  $a$  is a root of  $h(x)$  where  $h(x)$  is the resultant of  $f(x,y)$  and  $g(x,y)$  as polynomials in  $y$ . These two results are codified in the following two lemmas.

Lemma 1: Let  $f(x,y) \in R[x,y]$ ,  $R$  a real closed field,  $x, y$  indeterminates. Then if  $f(x,y) = 0$  has a solution in  $R$ , it has a solution  $(a,b)$  nearest the origin.

Proof: We consider the intersection of  $f(x,y) = 0$  with  $x^2 - y^2 = c^2, c \in R$ . Our hypothesis implies that we have a non-empty intersection since there is a solution  $(a,b)$  of  $f(x,y) = 0, (a,b)$  is a solution for  $x^2 + y^2 = ((a^2 + b^2)^{\frac{1}{2}})$ . Now let  $S = \{c \in R / f(x,y) = 0 \text{ meets } x^2 + y^2 = c^2, c > 0\}$ . We first show that  $S$  is the same as the set of  $c > 0$  such that  $g(c,x)$  has a root in  $[-c, c]$  where  $g(t,x)$  is the resultant with respect to  $y$  of  $f(x,y)$ , and  $x^2 - y^2 - t^2$  as polynomials in  $R[t, x, y]$ .

If  $c \in S$  and  $(a,b)$  is a point of intersection of  $x^2 + y^2 = c^2$  and  $f(x,y) = 0$ , then  $f(a,y)$  and  $y^2 + a^2 - c^2$

10. The Decision Method for an Algebraic Curve.

This section will give a method due to A. Seidenberg for deciding whether or not an equation  $f(x,y) = 0$ ,  $f(x,y) \in R[x,y]$  has a real root,  $R$  a real closed field. This will depend on the simple fact that if  $f(x,y) = 0$  has a real root, then it has a root nearest the origin and this root is also a solution of  $g(x,y) = x(\frac{\partial f}{\partial y}) - y(\frac{\partial f}{\partial x}) = 0$ . If  $(a,b)$  is such a solution, then  $a$  is a root of  $h(x)$  where  $h(x)$  is the resultant of  $f(x,y)$  and  $g(x,y)$  as polynomials in  $y$ . These two results are codified in the following two lemmas.

Lemma 1: Let  $f(x,y) \in R[x,y]$ ,  $R$  a real closed field,  $x,y$  indeterminates. Then if  $f(x,y) = 0$  has a solution in  $R$ , it has a solution  $(a,b)$  nearest the origin.

Proof: We consider the intersection of  $f(x,y) = 0$  with  $x^2 - y^2 = c^2$ ,  $c \in R$ . Our hypothesis implies that we have a non-empty intersection since there is a solution  $(a,b)$  of  $f(x,y) = 0$ ,  $(a,b)$  is a solution for  $x^2 + y^2 = ((a^2 + b^2)^{\frac{1}{2}})^2$ . Now let  $S = \{c \in R / f(x,y) = 0 \text{ meets } x^2 + y^2 = c^2, c > 0\}$ . We first show that  $S$  is the same as the set of  $c > 0$  such that  $g(c,x)$  has a root in  $[-c,c]$  where  $g(t,x)$  is the resultant with respect to  $y$  of  $f(x,y)$ , and  $x^2 - y^2 - t^2$  as polynomials in  $R[t,x,y]$ .

If  $c \in S$  and  $(a,b)$  is a point of intersection of  $x^2 + y^2 = c^2$  and  $f(x,y) = 0$ , then  $f(a,y)$  and  $y^2 + a^2 - c^2$

have a common factor. Therefore  $g(c,a) = 0$ ; hence  $g(c,x)$  has a root  $a$ , with  $-c \leq a \leq c$ . On the other hand, if  $c > 0$  such that  $g(c,x)$  has a root  $a$  with  $-c \leq a \leq c$  then  $y^2 + a^2 - c^2$  and  $f(a,y)$  have a common factor of positive degree by the theorem or resultants. Since the factors of  $y^2 + a^2 - c^2 = 0$  are  $y \pm b$  where  $b = (c^2 - a^2)^{\frac{1}{2}}$  then  $(a,b)$  or  $(a,-b)$  is a point of intersection of  $f(x,y) = 0$  and  $x^2 + y^2 = c^2$ , hence  $c \in S$ .

If  $S'$  is that subset of  $S$  consisting of that  $c \in \mathbb{R}$  such that  $g(c,x)$  has a root in the open interval  $(-c,c)$  then by the remark on theorem 8.2 we see that  $S'$  is the union of a finite number of sets defined by finite systems of polynomial equations  $p(c) = 0$ , inequations  $q(c) > 0$  and inequalities  $r(c) > 0$  where  $p(t)$ ,  $q(t)$  and  $r(t) \in \mathbb{R}[t]$ .

If we look at the loci in  $\mathbb{R}$  of  $p(t) = 0$ ,  $q(t) \neq 0$ ,  $r(t) > 0$  we see that the set of points  $c$  such that  $c > 0$ ,  $p(c) = 0$ ,  $q(c) \neq 0$ ,  $r(c) > 0$  is the union of a finite number of open sets which might be open, closed, half open, single point or extend to  $\infty$ . So  $S'$  is a subset of  $\mathbb{R}$  of this form and since  $q(c, \bar{c}) = 0$  is either a finite set or all of  $\mathbb{R}$  then  $S$  has the same structure as  $S'$ . Now if we show that the complement of  $S$  in the non-negative real numbers is the union of open intervals then  $S$  is the union of a finite number of closed intervals so it has a minimum element. Let  $d \notin S$  then  $g(d,x) - d \leq x \leq d$  has no solution. Write  $g(t,x)$  as a polynomial in  $x$  and  $(t-d), g(t,x) = g_0(x)$

$+ g_1(x)(t-d) + \dots + g_m(x)(t-d)^m$  then  $g_0(u) \neq 0$ ,  $-d \leq u \leq d$   
 and so there exists  $d' > d$  such that  $g_0(u) \neq 0$   $-d' \leq u \leq d'$ .  
 Then there are  $b > 0$  and  $B > 0$  such that  $|g_0(u)| \geq b$ ,  $|g_i(u)| \leq B$   
 $u \in [-d', d']$  by the fact that  $g_i(u)$  are polynomials on  
 closed intervals and hence bounded. Then if  $|c-d|$   
 $< \frac{1}{2}$ ,  $|c-d| < \frac{b}{4B}$  and  $u \in [-d', d']$ ,  $|g(c, u)| \geq |g_0(u)| - |g_1(u)(c-d)$   
 $+ \dots + g_m(u)(c-d)^m| \geq b - 2B|c-d| > b - \frac{b}{2} = \frac{b}{2}$ .  
 If  $c > 0$  is such that  $|c-d| < \frac{1}{2}$ ,  $|c-d| < \frac{b}{4B}$ ,  $c \leq d'$  then  $c$  is in  
 the complement of  $S$ . This means that if  $d \in S$  then there  
 is an open interval containing  $d$  such that this interval  
 is in the complement of  $S$ . So  $S$  is the union of closed  
 intervals as required.

Definition: A point  $(a, b)$  on the curve  $C: f(x, y) = 0$  is  
 called a simple point if  $((\frac{\partial f}{\partial x})_{(a,b)}, (\frac{\partial f}{\partial y})_{(a,b)}) \neq (0, 0)$ .  
 In this case the normal vector to  $C$  at  $(a, b)$  is  $((\frac{\partial f}{\partial x})_{(a,b)}$   
 $(\frac{\partial f}{\partial y})_{(a,b)})$  and the tangent line to the curve at  $(a, b)$  has  
 the equation  $(\frac{\partial f}{\partial x})_{(a,b)}(x-a) + (\frac{\partial f}{\partial y})_{(a,b)}(y-b) = 0$ . Let  $(a, b)$  be  
 a point on  $C: f(x, y) = 0$  nearest the origin. We want to  
 show that  $b(\frac{\partial f}{\partial x})_{(a,b)} - a(\frac{\partial f}{\partial y})_{(a,b)} = 0$ . If  $(a, b) = (0, 0)$   
 or  $(a, b)$  is not a simple point then this is obvious  
 otherwise the equation we want to prove says that the  
 vector joining the origin to  $(a, b)$  and the normal vector  
 to  $C$  at  $(a, b)$  are linearly dependent or  $C$  and the circle  
 with center at the origin and radius  $(a^2 + b^2)^{\frac{1}{2}}$  has the  
 same tangent line at  $(a, b)$ . If this is not the case then

the tangent to the curve C at (a,b) would contain interior points to the circle and C doesn't since (a,b) is nearest point of C to (0,0). The following lemma shows that this is impossible.

Lemma 2: Let p be a point of intersection of a circle and a curve C.  $f(x,y) = 0$ . Assume p is a simple point of C and the tangent at p to C contains points interior to the circle. Then C itself contains points interior to the circle.

Proof: By suitable choice of axis we may assume that  $p = (0,0)$  then  $f(0,0) = 0$ . And if we choose the x-axis to be the tangent to the curve C at p then  $(\frac{\partial f}{\partial x})(0,0) = 0$  and we may assume  $(\frac{\partial f}{\partial y})(0,0) = 1$ . We note that the center of the circle is not on the y axis so we may denote it as (a,b) with  $a \neq 0$ . Then we have  $f(x,y) = f(0,0) + (\frac{\partial f}{\partial x})(0,0)x + \frac{1}{2!} (\frac{\partial^2 f}{\partial y^2})(0,0)y^2 + 2(\frac{\partial^2 f}{\partial x \partial y})(0,0)xy + (\frac{\partial^2 f}{\partial x^2})(0,0)x^2 + \dots$  and this can be written as  $f(x,y) = y(1+h(x,y)) + g(x)$  since  $(\frac{\partial f}{\partial y})(0,0) = 1$  and from this equation  $h(0,0)=0$  and  $g(x)$  is a polynomial divisible by  $x^2$ . Since  $h(0,0)=0$  we may choose  $d>0$  such that  $|h(x,y)| \leq \frac{1}{2}$  if  $|x| \leq d, |y| \leq d$  so  $\frac{1}{2} \leq 1+h(x,y) \leq \frac{3}{2}$  and  $\frac{d}{2} \leq d(1+h(x,d)) \leq \frac{3d}{2}$  and  $-\frac{3d}{2} \leq -d(1+h(x,-d)) \leq -\frac{d}{2}$   $-d \leq x \leq d$ .

Since  $g(0) = 0$  there exists a  $d', 0 < d' < d$  such that  $f(x,d) = d(1+h(x,d)) + g(x) > 0$  and  $f(x,-d) < 0$  if  $-d' \leq x \leq d'$ . So by the mean value theorem for every  $x_0, |x_0| \leq d'$  there

exists  $y_0 \in [-d, d]$  such that  $f(x_0, y_0) = 0$  and hence

$$y_0 = -g(x_0)(1+h(x_0, y_0))^{-1} \text{ and } (a-x_0)^2 + (b-y_0)^2 = (a-x_0)^2 + (b-y_0)^2 + (a-x_0)^2 + (b + \frac{g(x_0)}{1+h(x_0, y_0)})^2$$

$$= a^2 + b^2 - 2ax_0 + x_0^2 + \frac{2bg(x_0)}{1+h(x_0, y_0)} + \frac{g(x_0)^2}{(1+h(x_0, y_0))^2}$$

Since  $g(x_0)$  is divisible by  $x_0^2$ , if we chose  $x_0$  small so that  $a - x_0$  is positive then  $(a-x_0)^2 + (b-y_0)^2 \leq a^2 + b^2$

and this means that  $(a, b)$  is a point interior to the

circle. We have seen that if  $C: f(x, y) = 0$  has a solution in  $\mathbb{R}^2$  then  $C: f(x, y) = 0$  and  $D: y \frac{\partial f}{\partial y} - x \frac{\partial f}{\partial x} = 0$  have a common point and more generally if  $C: f(x, y) = 0$  has a solution in  $\mathbb{R}^2$  and  $(0, 0)$  is replaced by  $(c, d)$  then  $C$  and  $D:$

$(y-d) \frac{f}{x} - (x-a) \frac{\partial f}{\partial y} = 0$  have a common point. We shall use

this fact to obtain Seidenberg method for deciding the solvability of  $f(x, y) = 0$  in  $\mathbb{R}^2$ . First let  $f(x, y) \in \mathbb{R}[x, y]$ .

Using the Euclidean algorithm we can determine a greatest common divisor of the coefficients of  $y$  of  $f(x, y)$  and if  $d(x)$  is the greatest common divisor we can write

$f(x, y) = d(x)f_1(x, y)$  where  $f_1(x, y)$  is not divisible by a polynomial in  $x$ . If  $f(x, y) = 0$  is solvable in  $\mathbb{R}^2$  then either  $d(x)$  is solvable or  $f_1(x, y)$  is solvable and the

converse is also true. This means that we can reduce our problem to that of primitive one in  $\mathbb{R}[x, y]$  as polynomials in  $y$  since  $d(x) = 0$  can be decided by Sturm's theorem.



Next if  $f(x,y) \in R[x,y]$  is a primitive polynomial in  $y$  we can determine by Euclidean algorithm a greatest common divisor of  $f(x,y)$  and  $\frac{\partial f}{\partial y} f(x,y)$  in  $R(x)[y]$  and we can write that as  $u(x) v(x)^{-1} d(x,y)$  where  $R(x)$  is the field of fractions of  $R[x]$  and  $d(x,y)$  is  $y$  primitive then we see that  $g(x,y) = f(x,y) d(x,y)^{-1}$  has the same roots as  $f(x,y)$  and no multiple roots exist and the solvability of  $f(x,y) = 0$  is equivalent to that of  $g(x,y) = 0$  for the same reason. So we notice that this reduces the problem to polynomials which are  $y$  primitive with no multiple factors of positive  $y$  degree and this means that  $f(x,y)$  and  $(\frac{\partial}{\partial y})(f(x,y))$  has no common factor of positive  $y$  degree in  $R(x)[y]$ . Consider  $f(x,y)$  and the polynomial defined by  $g(t,x,y) = y\frac{\partial f}{\partial y} - (x-t)\frac{\partial f}{\partial y}$  and let  $h(t,x)$  be their resultant as polynomials in  $y$ . Now  $h(t,x) \neq 0$ . Otherwise  $h(c,x) = 0$  for every  $c \in R$ , which means that  $f(x,y)$  and  $g(c,x,y)$  have a common factor of positive degree in  $y$  and since we have a finite number of factors of  $f(x,y)$  this means that there is  $c_1 \neq c_2$  such that  $g(c_1,x,y)$ ,  $g(c_2,x,y)$  and  $f(x,y)$  have a common factor which implies that we have  $f(x,y)$  and  $\frac{\partial f}{\partial y} = (c_1 - c_2)^{-1} [g(c_1,x,y) - g(c_2,x,y)]$  have a non-trivial common factor, a contradiction with the choice of  $f(x,y)$ ; hence  $h(t,x) \neq 0$ . Let  $c$  be chosen such that  $h(x) = h(c,x) \neq 0$  and write  $g(x,y) = g(c,x,y) = y(\frac{\partial f}{\partial y}) - (x-c)(\frac{\partial f}{\partial y})$ . We see that

these two polynomials have no common factor of positive degree in  $y$  since  $h(x) \neq 0$  and since  $f(x,y)$  is primitive  $y$  polynomial so they have no common factor in  $x$  alone. Since we have seen that if  $f(x,y) = 0$  has a root in  $\mathbb{R}^2$  then also  $f(x,y) = 0$  and  $g(x,y) = y \frac{\partial f}{\partial x} - (x-c) \frac{\partial f}{\partial y} = 0$  has a common point in  $\mathbb{R}^2$  and this means that if  $(a,b)$  is such a point then  $f(a,y)$  and  $g(a,y)$  have the common factor  $y-b$  which implies that  $h(a) = 0$  so  $h(x) = 0$  has a solution. In fact this result is convertible also so if  $h(x)$  has a root  $a$  then  $f(x,y)$  and  $g(x,y)$  have a common factor. This can be proved provided that we choose the generators  $x,y$  of  $\mathbb{R}[x,y]$  suitably. So the main result we have is that  $f(x,y) = 0$  has a root in  $\mathbb{R}^2$  equivalent to that  $h(x)$  which is the resultant of  $f(x,y)$  and  $g(x,y) = y \frac{\partial f}{\partial x} - (x-c) \frac{\partial f}{\partial y}$  has a root and this can be decided by Sturm's theorem. There is an extension of this procedure to the case of  $f(x,y) = 0$  restricted by  $g(x) \neq 0$ . We can assume as before that  $f(x,y)$  is  $y$  primitive as a polynomial in  $y$  and we assume that  $\text{degree } g(x) > 0$ , otherwise it is trivial case since  $g(x)$  will be a constant. So let  $t(y)$  be the resultant of  $f(x,y)$  and  $g(x)$  as polynomials in  $x$ ,  $t(y) \neq 0$  since  $f(x,y)$  is primitive  $y$  polynomial. Let  $c \in \mathbb{R}$  be chosen such that  $t(c) \neq 0$  and we replace  $f(x,y)$  by  $f_1(x,y) = f(x,y+c)$ . Now  $f(x,y) = 0$ ,  $g(x) \neq 0$  is solvable if and only if the system

$f_1(x,y) = 0, g(x) \neq 0$  is solvable, we notice that the resultant with respect to  $x$  of  $f_1(x,y)$  and  $g(x)$  is  $t(y+c)$  and this is different from 0 for  $y = 0$  so  $f_1(x,0)$  and  $g(x)$  have no common factor in  $R[x]$ . If we put  $f_2(x,y) = f_1(x,g(x)y)$  then  $f_1(x,y) = 0, g(x) \neq 0$  is solvable in  $R$  if and only if  $f_2(x,g(x)y)$  is solvable in  $R$ , since if  $(a,b)$  is a solution of the first system then  $f_2(a,g(a^{-1}b)) = f_1(a,b) = 0$ . On the other hand, if  $F_2(a,c) = f_1(a,g(a)c) = 0$  then  $g(a) \neq 0$ . Otherwise, if  $g(a) = 0$  then  $g(x)$  and  $f_1(x,0)$  have a common factor  $(x-a)$ , a contradiction with the fact that  $f(x,0), g(x)$  have no common factor. Now if  $b = g(a)c$  then  $(a,b)$  satisfies  $f_1(x,y) = 0, g(x) \neq 0$ . So this case, which is the solvability of  $f_1(x,y) = 0, g(x) \neq 0$ , turns out to be a problem of deciding the solvability by Sturm's theorem of their resultant and the problem of solvability of  $f(x,y) = 0, g(x) \neq 0$  is reduced to the problem of solvability of  $h(x) \in R[x]$ .

## BIBLIOGRAPHY

1. N. Jacobson, Basic Algebra 1, 1974, W. H. Freeman and Company.
2. N. Jacobson, Lectures in Abstract Algebra, Vol. III, 1964.
3. B. L. Van der Waerden, Modern Algebra, Vol. I, 1948, Frederick Ungar Publishing Co.
4. P. M. Cohn, Algebra, Vol. II, 1977, John Wiley And Sons Ltd.
5. S. Lang and J. Tate, The Collected Papers of Emil Artin, 1965, Addison-Wesley Publishing Company.
6. A. Robinson, "On Ordered Fields and Definite Functions," *Mathematische Annalen* 130 (1955) pp. 267-271 and pp. 405-409.
7. P. Erdos, L. Gillman and M. Hersiksen, "An isomorphism theorem for real closed fields," *Annals of Math* 61 (1955) pp. 542-554.
8. S. Lang, "The theory of real places," *Annals of Math* 57 (1953) pp. 378-391.
9. G. Kreisel, "The mathematical significance of consistency proofs," *J. Symbolic Logic* 23 (1958) pp. 155-182.
10. A. Seidenberg, "A new decision method for elementary algebra," *Annals of Math* 60 (1954) pp. 365-374.

## VITA

Hassan Yousef was born in Beit Ligia, Jordan, on December 16, 1954. He finished his elementary and secondary education in Jordan and graduated with high honors from Hashemia Secondary School in 1972. He entered the University of Jordan in October 1972 under the sponsorship of the Ministry of Education of Jordan, and received a B.Sc. degree in Mathematics in June 1976.

During the period 1976-1980 Mr. Hassan was a teacher of high school employed by the Ministry of Education. During the year 1980-1981 he was an academic assistant employed by Bir-Zeit University in Jordan. In August 1981 he entered the Graduate School of Lehigh University under the sponsorship of Bir-Zeit University.