University of Montana

ScholarWorks at University of Montana

Graduate Student Theses, Dissertations, & Professional Papers

Graduate School

1968

Real closed fields

Yean-mei Wang Chou
The University of Montana

REAL CLOSED FIELDS

By

Yean-mei Wang Chou

B.A., National Taiwan University, 1961

B.A., University of Oregon, 1965

Presented in partial fulfillment
of the requirements for the degree of

Master of Arts

UNIVERSITY OF MONTANA

1968

Approved by:

Merle E Manis

Chairman, Board of Examiners

Fred S Honkala

Dean, Graduate School

5/29/68

Date

24-1.65

ACKNOWLEDGEMENTS

I wish to express my gratitude to those of the Mathematics Department at the University of Montana whose guidance made possible the completion of this work. I especially thank Professor Merle Manis for the encouragement, guidance and unlimited patience during the past two years. Also my sincerest thanks go to Professor William Ballard, and Mr. George Trickey for their critical readings of the manuscript and their many valuable suggestions during the period this thesis was being written. In addition I want to thank Professors William Myers and Robert Banaugh for their critical readings and helpful suggestions of parts of the manuscript.

Y. M. C.

TABLE OF CONTENTS

INTRODUCTION

This paper follows the work done by Artin and Schreier. A basic algebraic property of the field of real numbers is that the only relations of the form $\sum_{i=1}^{n} a_i^2 = 0$ which can hold in this field are the trivial ones: $0^2 + 0^2 + \dots + 0^2 = 0$. This observation led Artin and Schreier to call any field having this property formally real. Any such field can be ordered and any ordered field is formally real. Of central interest in the theory are the real closed fields which are the formally real fields maximal under algebraic extension. A real closed algebraic extension of an ordered field, whose ordering is an extension of that of the given field, is called the real closure of the ordered field.

The purpose for studying the material is to see which results of the classical theory of equations are due to the properties of the rational numbers as an ordered field, and which are due to the properties of the real numbers as an order closed field.

The main source of the material is the section on Artin and Schreier Theory in Jacobson's Lectures [5]. The approach follows the outline of DuBois's series of lectures at the University of Oregon in the summer of 1966.

Section I presents the general theory of an ordered field and an order closed field. In this section, we observe that a real closed field has a unique ordering which can be specified by the requirement that a > 0 in this field if and only if $a = b^2 \neq 0$. Also if F is real closed, $F(\sqrt{-1})$ is algebraically closed.

In Section II, we shall derive a classical result, Sturm's Theorem, which permits us to determine the exact number of distinct roots in a real closed field of a polynomial equation $f(x) = 0$. We will prove some other classical results, such as Rolle's theorem, the mean value theorem, and Budan's theorem. Most definitions and background material are adapted from [1]. The approach follows the exercises given in [5].

In Section III, we shall show that for any ordered field F, there exists a real closure which contains F, and the ordering of the real closure is an extension of that of F. Moreover, we shall see that real closures of an ordered field are equivalent and we may therefore speak of the real closure of F.

In Section IV, we shall prove the Fundamental Theorem of Algebra.

SECTION I

ORDERED FIELDS AND ORDER CLOSED FIELDS

Definition 1.1. An ordered field is a field F together with a subset P (the set of positive elements) of F such that:

(1) $0 \notin P$,

(2) if $a \in F$, then either $a \in P$, $a = 0$, or $-a \in P$,

(3) P is closed under addition and multiplication.

We shall denote the ordered field by (F, P) or F if P is understood.

Since any field has at least two elements, the subset P is not empty. Let $-P = \{-a \mid a \in P\}$. Clearly $F = P \dot{\cup} \{0\} \dot{\cup} -P$. We observe that $(-a) + (-b) = -(a + b) \in -P$ if $a, b \in P$, and $(-a)(-b) = ab \in P$ if $a, b \in P$. In particular, $(-a)(-a) = a^2 \in P$ if $a \neq 0$.

We can introduce a partial ordering in the ordered field (F, P) by defining $a > b$ if $a - b \in P$. Then if a, b are any two elements of F, we have the trichotomy: one and only one of the relations: $a > b$, $a = b$, $a < b$ holds. Thus F is linearly ordered by the relation $a > b$. If $a > b$, then $a + c > b + c$ for all $c \in F$, and if $c > 0$, $ac > bc$. Conversely, we can define an ordered field in case there is in F a linear ordering $>$ such that $a > b$ implies $a + c > b + c$, and $ac > bc$ if $c > 0$. Let P denote the set of elements $a > 0$. Then (F, P) is an ordered field in the original sense and the relation $>$ defined by (F, P) is the given ordering relation.

We will list some of the elementary properties of the ordering in an ordered field: $1 > 0$, $a > 0$ implies $a^{-1} > 0$, and $a > b > 0$ implies $b^{-1} > a^{-1} > 0$. If $a > b$, then $-a < -b$ and, if $a > b$ and $c > d$, then $a + c > b + d$. Let $|a|$ be defined as a if $a \varepsilon P$, $-a$ if $a \not\varepsilon P$, then $|a + b| \leqslant |a| + |b|$ and $|ab| = |a||b|$.

If F' is a subfield of an ordered field (F, P), then F' is ordered relative to $P' = F' \cap P$. We shall call this the induced ordering in F'. Evidently $a' > b'$ in (F', P') if and only if $a' > b'$ in (F, P). If (F, P) and (F', P') are any two ordered fields, then an isomorphism s of F into F' is called an order isomorphism if $s(P) = P'$.

<u>Note 1</u>. In any ordered field F, $a \neq 0$ implies $a^2 > 0$; hence if $a_1, a_2, \ldots, a_n$ are $\neq 0$, then $\sum_{i=1}^{n} a_i^2 > 0$. This shows that any ordered field is formally real in the sense of the following:

<u>Definition 1.2</u>. A field F is called <u>formally real</u> if the only relations of the form $\sum_{i=1}^{n} a_i^2 = 0$ in F are those for which every $a_i = 0$.

Note 2. F is formally real if and only if -1 is not a sum of squares of elements of F, and the characteristic of F is necessarily 0.

Proof: If $-1 = \sum_{i=1}^{n} a_i^2$, then $0 = -1 + 1 = \sum_{i=1}^{n} a_i^2 + 1^2$, a contradiciton. Conversely, if F is not formally real, there exists $a_i \in F$, $i = 1, \ldots, n$ such that $\sum_{i=1}^{n} a_i^2 = 0$, not all a_i's are zero. We may assume that $a_n \neq 0$. This implies $b_1^2 + b_2^2 + \ldots + b_{n-1}^2 + 1 = 0$, where $b_i = a_i/a_n$, for $i = 1, \ldots, n-1$. Then $-1 = \sum_{i=1}^{n-1} b_i^2$.

If the characteristic of F is $p \neq 0$, then $0 = 1^2 + 1^2 + \ldots + 1^2$ (p times). Thus if F has order p, then $0 \in P$, a contradiction.

Thus the only fields which have orders are of characteristic 0, so all fields considered are assumed to be of characteristic 0 unless otherwise specified. Any such field has a subfield isomorphic with the field Q of rational numbers, which we may identify with Q.

Note 3. The field of rational numbers has a unique order, i.e. the set of positive rational numbers.

Note 4. If $0 \neq a \in F$, and $a = \sum_{i=1}^{n} a_i^2$, then $a^{-1} = (a^{-1})^2 \cdot a = \sum_{i=1}^{n} (a_i a^{-1})^2$.

Definition 1.3. Let S be a subset of a field. Let $-S = \{-x \mid x \in S\}$. Then S is conic if $S \cap -S \subset \{0\}$.

Definition 1.4. Let S be a subset of a field. Then S is a preprime if :

(1) S is closed under addition and multiplication,

(2) $-1 \notin S$.

Note 5. Let S be a subset of a field F, with S closed under addition, multiplication and division. Then S is conic if and only if S is a preprime.

Proof: Suppose $-1 \in S$, then $(-1)(-1) = 1 \in S$ and since $-1 \in S$, $1 \in -S$. Hence $S \cap -S \not\subset \{0\}$, a contradiction.

Conversely, suppose $S \cap -S \not\subset \{0\}$, then there exists an x, $x \neq 0$, with $x \in S \cap -S$, i.e. $x \in S$ and $x \in -S$, $-x \in S$. Since S is closed under division, $-1 = (-x)/x \in S$, a contradiction.

Definition 1.5. A cone is a conic preprime. A division cone is a preprime closed under division.

Note 6. Division cones do not contain zero.

Lemma 1.6. If S is a cone in a field F, $0 \notin S$, then $S^* = \{x \mid xy \in S \text{ for some } y \in S\}$ is a division cone containing S.

Proof: Clearly $S \subset S^*$. If $x \in S^*$, $y \in S^*$, let $xx' = s \in S$ with $x' \in S$, $yy' = t \in S$ with $y' \in S$; then $(x + y)x'y' = sy' + x't \in S$, and $x'y' \in S$, so $x + y \in S^*$. $(xy)x'y' = st \in S$, $x'y' \in S$, so $xy \in S^*$. $y \neq 0$ since

$0 \notin S$, and $(x/y)x't = sy' \in S$, $x't \in S$, so $x/y \in S^*$.

If $S^* \cap -S^* \not\subset \{0\}$, then $-1 \in S^*$ since S^* is closed under division. Hence $-1 \cdot b = -b \in S$ for some $b \in S$, $b \neq 0$, which implies $S \cap -S \not\subset \{0\}$, a contradiction.

Theorem 1.7. (Baer, Artin - Schreier) Let D be a division cone of F. Then D contains all non-zero squares in F if and only if D is the intersection of all orders of F containing D, i.e. $D = \cap \{P \mid P \text{ an order of } F \text{ and } D \subset P\}$.

Proof: Let D be a division cone, such that $a \in F$, $a \neq 0$ implies $a^2 \in D$. Suppose $0 \neq x \in F$, $x \notin D$; we need to show there is an order P of F such that : (1) $D \subset P$, and (2) $x \notin P$.

Let $S = \{a - bx \mid a^2 + b^2 \neq 0,\ a, b \in D \cup \{0\}\}$. S is closed under addition and multiplication, since $x^2 \in D$. $0 \notin S$ since $a - bx = 0$ implies $x = ab^{-1} \in D$ ($b^{-1} \in D$ since D is a division cone). $D \subset S$, and $-x \in S$ since $-x = 0 - 1 \cdot x$ ($1 \in D$ since $1 = 1^2 \in D$). By Lemma 1.6, we know there exists a division cone S^* with $S \subset S^*$. Note that if $y \in F$, $y \neq 0$, then $y^2 \in S^*$, since $y^2 \in D \subset S \subset S^*$.

Let $Z = \{T^* \mid S^* \subset T^*,\ T^* \text{ a division cone}\}$. Z is not empty since $S^* \in Z$. Z is inductively ordered by $\subseteq$. By Zorn's Lemma, Z has maximal elements. Let P^* be maximal in Z.

Claim: P^* is an order.

Subproof: Clearly $0 \notin P^*$, since P^* is a division cone. Let $0 \neq y \in F$ and $y \notin P^*$. Let $T = \{a + by \mid a^2 + b^2 \neq 0$, a, b are in $P^* \cup \{0\}\}$. T is closed under addition and multiplication since $y^2 \in S^* \subset P^*$. Also $P^* \subset T$, and $y = 0 + 1 \cdot y \in T$. Thus $0 \in T$, otherwise applying Lemma 1.6 to T would contradict the maximality of P^*. Therefore $0 = a + by$, $a \neq 0 \neq b$, $y = -a/b$, $-y = a/b \in P^*$. So P^* is an order.

Thus P^* is an order, $D \subset P^*$ and $x \notin P^*$ since $-x \in P^*$.

Conversely, suppose $D = \cap P_\alpha$, P_α an order and $D \subset P_\alpha$ for each α. If $0 \neq x \in F$, then $x^2 \in P_\alpha$ for all α, so $x^2 \in D$.

<u>Corollary 1.8</u>. Any ordered field is formally real and any formally real field has an order.

<u>Proof</u>: By Note 1 we know that any ordered field is formally real.

Let F be a formally real field. Let $\Sigma (F) = \{\sum_{i=1}^{n} x_i^2 \mid x_i \in F \setminus \{0\}\}$. $\Sigma (F)$ is closed under addition, multiplication, and division, and $\Sigma (F) \cap -\Sigma (F) = \phi$. So $\Sigma (F)$ is a division cone. By Theorem 1.7, there exists an order in F which contains $\Sigma (F)$.

<u>Corollary 1.9</u>. F has an order if and only if $\Sigma (F) = \{\sum_{i=1}^{n} x_i^2 \mid x_i \in F \setminus \{0\}\}$ is a preprime.

<u>Proof</u>: Suppose P is an order on F. (F, P) is an ordered field. F is formally real by Corollary 1.8, and

$-1 \notin \Sigma\ (F)$ by Note 2.

Conversely, $\Sigma\ (F)$ is a division cone since it is closed under division as noted in the proof of Corollary 1.8. Thus Theorem 1.7 applies.

Corollary 1.10. Let P be an order on F, $F \subset F'$. F is a subfield of F' and F' is an ordered field. Set $\Sigma\ (F', P) = \{ \sum_{i=1}^{n} p_i x_i^2 \mid p_i \in P,\ x_i \in F' \setminus \{0\} \}$. Then $\Sigma\ (F', P)$ is the intersection of all orders of F' containing P.

Proof: Note that $\Sigma\ (F', P)$ is closed under addition, multiplication, and division. If $-1 \in \Sigma\ (F', P)$, then there are no orders of F' containing P. In this case, for all $x \in F'$, $x = ((x + 1)/2)^2 - 1 \cdot ((x - 1)/2)^2 \in \Sigma\ (F', P)$, so $\Sigma\ (F', P) = F'$ is the intersection of all orders of F' containing P. Otherwise we apply Note 5 and Theorem 1.7.

Corollary 1.11. (Artin in connection with Hilbert's 17th Problem[1]) If F is a formally real field, then the

[1] One of the problems proposed by Hilbert in his address to the 1900 Paris Congress of Mathematicians was the following:

Let Q be a rational function of n variables with rational coefficients such that $Q(a_1, a_2, \ldots, a_n) \geqslant 0$ for all real $(a_1, a_2, \ldots, a_n)$ for which Q is defined. Then is Q necessarily a sum of squares of rational functions with rational coefficients?

set S of all sums of squares of members of F is the intersection of the orders of F.

Proof: Let Q denote the field of all rational numbers, and let Q^+ denote the set of all positive rational numbers. We know that Q^+ is an order on $Q \subset F$. Since $(p/q)x^2 = pq(q^{-1}x)^2$, $S = \{ \sum_{i=1}^{n} (a_i/b_i)x_i^2 \mid a_i/b_i \in Q^+, x_i \in F\setminus\{0\}\} = \Sigma(F, Q^+)$. By Corollary 1.10, S is the intersection of all orders of F containing Q^+, hence the intersection of all orders of F.

Theorem 1.12. Let (F, P) be an ordered field and f(x) an irreducible polynomial over F. Suppose $f(a)f(b) < 0$ for some $a, b \in F$. Then:

(1) There is an order on $F[x]/(f(x))$ extending P.

(2) If $a < b$, then there is an extension field $\hat{F}$ of F with an order extending P and a $\xi \in \hat{F}$ with $a < \xi < b$ and $f(\xi) = 0$.

Proof: (1) If the theorem does not hold, there is an irreducible polynomial f of smallest degree for which it fails. Let f be such a polynomial. Assume $f(a)f(b) < 0$, and let $F^* = F[x]/(f(x))$.

We must have $0 \in \Sigma(F^*, P)$, since otherwise $\Sigma(F^*, P)$ is contained in an order. Therefore there exists $q_i(x) \in F[x]$ with $q_i(x) \notin (f(x))$ for some i, $p_i \in P$, and $h(x) \in F[x]$ such that

$\sum_{i=1}^{n} p_i q_i^2(x) = h(x)f(x)$ ....(1)

Clearly we can require that deg $q_i(x) <$ deg $f(x)$, so that deg $h(x)f(x) < 2$ deg $f(x)$, which implies deg $h(x) <$ deg $f(x)$.

If $h(t) = 0$, $t \varepsilon F$, then $\sum_{i=1}^{n} p_i q_i^2(t) = 0$, so that $q_i(t) = 0$ for each i and we can divide both sides of (1) by $(x - t)^2$. Hence we can assume $h(t) \neq 0$ for all $t \varepsilon F$. Thus $h(t)f(t) = \sum_{i=1}^{n} p_i q_i^2(t) > 0$ for all $t \varepsilon F$.

Let $h(x) = \prod_{j=1}^{\hat{n}} h_j(x)$ be a factorization of h(x) into irreducible factors.

If $h_j(x) \mid q_i(x)$ for each i (some j) we could divide out $h_j^2(x)$ in (1). So we can assume for each j, there exists an i with $q_i(x) \notin (h_j(x))$.

We know $f(a)f(b) < 0$ and $h(a)f(a) > 0$, $h(b)f(b) > 0$, thus $h(a)h(b) = \prod_{j=1}^{\hat{n}} (h_j(a)h_j(b)) < 0$, so $h_j(a)h_j(b) < 0$ for some j. Assume $j = 1$.

Now deg $h_1(x) \leqslant$ deg $h(x) <$ deg $f(x)$ so, by assumption, $F' = F[x]/(h_1(x))$ has an order extending P, so $0 \notin \Sigma\ (F', P)$.

But $\sum_{i=1}^{n} p_i q_i^2(x) = [f(x)][\prod_{j=2}^{\hat{n}} h_j(x)][h_1(x)] \varepsilon (h_1(x))$ and $q_i(x) \notin (h_1(x))$ for some i, i.e. $0 \varepsilon \Sigma\ (F', P)$, a contradiction.

(2) Let f(x) be irreducible with $f(a)f(b) < 0$. Let T be a splitting field of f(x) over F. Let $\mathcal{P} = \{(S, P_S) \mid$ S a subfield of T, P_S an order on S, $P_S \cap F = P\}$. $\mathcal{P}$ is not empty since (F, P) is in $\mathcal{P}$. It is inductively ordered by the relation defined by: $(S_1, P_{S_1}) < (S_2, P_{S_2})$ if S_2

is an extension field of S_1 and P_{S_2} is an order on S_2 which extends P_{S_1}. By Zorn's Lemma, there exist maximal elements. Let $(\hat{F}, \hat{P})$ be maximal in $\mathcal{P}$.

Let $f(x) = \prod_{i=1}^{n} (x - \xi_i) \prod_{i=1}^{s} f_i(x)$ be the factorization of f over $\hat{F}$, where each f_i is irreducible over $\hat{F}$ and deg $f_i \geq 2$. Since f_i has no zero in $\hat{F}$, $f_i(a)f_i(b) > 0$ for all i. Thus $f(a)f(b) < 0$ implies $(a - \xi_j)(b - \xi_j) < 0$ for some j; i.e. ξ_j is between a and b.

<u>Corollary 1.13</u>. Under the same hypothesis as Theorem 1.12, $F[x]/(f(x))$ has an order extending P for which there is a ξ in $F[x]/(f(x))$ such that $a < \xi < b$ and $f(\xi) = 0$.

<u>Proof</u>: Let $\hat{F}$ be the same as in the second part of the proof of Theorem 1.12. Let $\xi \in \hat{F}$ with $a < \xi < b$ and $f(\xi) = 0$.

Consider ω: $F[x] \longrightarrow \hat{F}$ by $\omega(x) = \xi$.

Then $\omega(F[x]) = F[\xi] \cong F[x]/(f(x))$. Note that $F[\xi] \subset \hat{F}$, $\hat{F}$ ordered, $\hat{P}$ its order. Using the restriction of order $\hat{F}$ to $F[\xi]$, we have $K = F[x]/(f(x))$ ordered and ξ is a root of f(x) in K with $a < \xi < b$.

<u>Corollary 1.14</u>. If (F, P) is an ordered field and F' is an extension field of F with $[F' : F] = n$, where n is odd, then F' has an order P' extending P.

<u>Proof</u>: If f(x) is the field polynomial, then $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ with $a_i \in F$, $n = [\, F' : F]$. Let $t > \max \{1, nb\}$

where $b = \max\{|a_i|\}$. Then $f(t) = t^n + \sum_{i=0}^{n-1} a_i t^i \geqslant t^n + \sum_{i=0}^{n-1} -|a_i|\cdot t^i \geqslant t^n - (nb)t^{n-1} > 0$, and $f(-t) = (-t)^n + \sum_{i=0}^{n-1} a_i(-t)^i \leqslant -t^n + \sum_{i=0}^{n-1} |a_i| t^i \leqslant -t^n + (nb)t^{n-1} < 0$. By Theorem 1.12, F' has an order P' extending P.

Corollary 1.15. If (F, P) is ordered, $p \in P$, then $F(\sqrt{p})$ can be ordered to extend P.

Proof: We can assume that $\sqrt{p} \notin P$; i.e., $x^2 - p = f(x)$ is irreducible. Note that $f(0) < 0$ and $f(t) > 0$ for $t^2 > p$.

Definition 1.16. (F, P) is order closed if and only if there is no ordered field (F', P') with $1 < [F' : F] < \infty$ such that P' extends P.

Definition 1.17. F is real closed if and only if F has an order but no proper algebraic extension is orderable.

Theorem 1.18. F is real closed if and only if (F, P) is order closed for some order P. If F is real closed, then F has a unique order. Thus if (F, P) is order closed, then P is the only order on F.

Proof: Let F be real closed; then $\Sigma(F, Q^+) = D$ is the intersection of all orders of F by the proof of Corollary 1.11. Suppose $a, -a \notin D$, then there is an order P with $a \in P$, and since $a \notin D$, $x^2 - a$ is irreducible over F. Hence, by Corollary 1.15, P can be extended to an order on $F(\sqrt{a})$. This contradicts F being real closed. Thus D is the unique order on F and (F, D) is order closed.

Conversely, let F be order closed, D as above. We show that D = P. If $p \in P \setminus D$, then by Corollary 1.15, P can be extended to $F(\sqrt{p})$ and $F(\sqrt{p})$ is a proper extension of F, yielding a contradiction. Thus there is no order on an extension field which extends P, so F is real closed.

<u>Note 7</u>. If F is real closed, then

(1) F[x] has no irreducible polynomial of odd degree, by Corollary 1.14.

(2) If $a \in D$, then $a = b^2$ for some $b \in F$, by Corollary 1.15.

<u>Corollary 1.19</u>. If F is real closed, then any element of F is either a square or the negative of a square.

<u>Proof</u>: This is clear from Note 7 since $a \in F$ implies $a = 0$, $a \in D$ or $-a \in D$.

<u>Corollary 1.20</u>. Let F be real closed. Any automorphism of such a field is an order isomorphism.

<u>Proof</u>: If s is an automorphism of F, then s maps the set of non-zero squares into itself, since $s(a^2) = s(a)s(a) = (s(a))^2$. Hence s is an order isomorphism.

<u>Theorem 1.21</u>. If F is a real closed field, then $\sqrt{-1} \notin F$ and $F(\sqrt{-1})$ is algebraically closed.

Proof: Since F is formally real, $\sqrt{-1} \not\in F$. That $F(\sqrt{-1})$ is algebraically closed will follow if we can show every non-constant polynomial with coefficients in F has a root in $F(\sqrt{-1})$.

Since we know $F \subset F(\sqrt{-1})$, let $a \longrightarrow \bar{a}$ be the automorphism of $F(\sqrt{-1})$ over F such that $\bar{i} = -i$ for $i = \sqrt{-1}$. If $f(x) \varepsilon F(\sqrt{-1})[x]$, then $f(x)\bar{f}(x) \varepsilon F[x]$, and if this has a root in $F(\sqrt{-1})$, then f(x) will have a root in $F(\sqrt{-1})$.

From Corollary 1.14, we know that if F is real closed, F[x] has no irreducible polynomial of odd degree. We show next that every element of $F(\sqrt{-1})$ has a square root in this field.

First, if $a \varepsilon F$, and $a > 0$, then $a = b^2$, $b \varepsilon F$, by Corollary 1.15. If $a \varepsilon F$, $a < 0$, $-a > 0$, $-a = b^2$ and $a = (\sqrt{-1})^2 b^2$.

If $t = a + bi$, $i = \sqrt{-1}$, $a, b \varepsilon F$, and $b \neq 0$, set $a + bi = (c + di)^2$, $c, d \varepsilon F$. This is equivalent to :

$$a = c^2 - d^2, \quad b = 2cd \;\ldots\ldots\ldots\ldots(1)$$

Since $b \neq 0$, we may (by multiplying by a suitable element of F) assume that $b = 2$. So $1 = cd$, $d = c^{-1}$, and $a = c^2 - d^2$ becomes $a = c^2 - c^{-2}$. If we let $c^2 = k$, then we get $a = k - k^{-1}$ or $k^2 - ak -1 = 0$. This has a solution $(a + \sqrt{a^2 + 4})/2$ in F since $a^2 + 4 > 0$, and $a + \sqrt{a^2 + 4} > 0$. So there exists c in F with $c^2 = (a + \sqrt{a^2 + 4})/2$. Then $c^4 = (2a^2 + 4 + 2a\sqrt{a^2 + 4})/4$, $c^4 - c^2 a = 1$ and $c^2 - c^{-2} = a$. Hence c, and $d = c^{-1}$ satisfy (1) with $b = 2$. We therefore proved that every element of $F(\sqrt{-1})$ has a square root in this field. Consequently there exists no extension field Δ of $F(\sqrt{-1})$ such that $[\Delta : F(\sqrt{-1})] = 2$.

Let $f(x)$ be any polynomial of positive degree with coefficients in F. Let E be a splitting field over F of $(x^2 + 1)f(x)$. Then $E \supset F(\sqrt{-1})$. Since F, a real closed field, is of characteristic zero, E is Galois over F with group G of order $2^n m$ where m is odd. By Sylow's theorem, G has a subgroup H of order 2^n. Let Δ be the subfield over F of H-invariants; i.e., $\Delta = \{x \varepsilon F \mid \sigma(x) = x \text{ for all } x \varepsilon H\}$. Then $[E : \Delta] = 2^n$ and $[\Delta : F] = m$. Since F has no proper odd dimensional extension field we must have $\Delta = F$ and $m = 1$. Hence $[E : F] = 2^n$, and $[E : F(\sqrt{-1})] = 2^{n-1}$. If $n = 1$, we are done. Suppose not; by Sylow's theorem, G has a subgroup H' of order 2^{n-2}. Let Δ' be the subfield over F of H'-invariants. Then $[E : \Delta'] = 2^{n-2}$ and $[\Delta' : F(\sqrt{-1})] = 2$. As we have shown earlier in this proof, this is impossible. Therefore $n-1 = 0$, or $n = 1$, $[E : F] = 2$, and $E = F(\sqrt{-1})$. Hence $F(\sqrt{-1})$ is a splitting field of $(x^2 + 1)f(x)$, and $f(x)$ has a root in $F(\sqrt{-1})$. Thus we have proved that $F(\sqrt{-1})$ is algebraically closed.

The above result is the generalization to real closed fields of the Fundamental Theorem of Algebra.

Theorem 1.22. If F is a field such that $\sqrt{-1} \notin F$ and

$F(\sqrt{-1})$ is algebraically closed, then F is real closed.

<u>Proof</u>: Let $f(x)$ be an irreducible polynomial in $F[x]$ and let ξ be a root of $f(x)$ contained in $F(\sqrt{-1})$. Then $[F(\xi) : F] = \deg f(x)$, and $[F(\xi) : F] \leqslant [F(\sqrt{-1}) : F] = 2$. Hence $\deg f(x) = 1$ or 2.

Now let $a, b \neq 0 \in F$ and $g(x) = (x^2 - a)^2 + b^2$
$= (x^2 - a - bi)(x^2 - a + bi)$
$= (x - \sqrt{a + bi})(x + \sqrt{a + bi})(x - \sqrt{a - bi})(x + \sqrt{a - bi})$,
where $i = \sqrt{-1}$. Since any irreducible polynomial in $F[x]$ has degree 1 or 2, $g(x)$ is a product of two irreducible quadratic polynomials. The one divisible by $x - \sqrt{a + bi}$ can not be

$$(x - \sqrt{a + bi})(x + \sqrt{a + bi}) = x^2 - (a + bi);$$

for this would imply $a + bi \in F$. Hence we have either $(x - \sqrt{a + bi})(x - \sqrt{a - bi})$ or $(x - \sqrt{a + bi})(x + \sqrt{a - bi})$. Either possibility implies that $\sqrt{a^2 + b^2} = t \in F$, $a^2 + b^2 = t^2 \in F$, i.e., the sum of two squares of elements in F is a square in F. Since -1 is not a square, -1 is not a sum of squares in F. Therefore F is formally real. If P is a proper algebraic extension of F, then P is isomorphic to $F(\sqrt{-1})$. Then P is not formally real so F is real closed.

<u>Theorem 1.23</u>. (Darboux property - DuBois - Bourbaki) If (F, P) is an order closed field, $f(x)$ a polynomial over F with $f(a)f(b) < 0$, then there exists $c \in F$ such that

$a < c < b$ with $f(c) = 0$.

Proof: By Theorem 1.12, there is such a c in an extension $(\hat{F}, \hat{P})$ where $\hat{P}$ extends P. Since F is real closed, $(\hat{F}, \hat{P}) = (F, P)$. •

Theorem 1.24. Let (F, P) be an ordered field and let $\bar{F}$ be an algebraic closure of F. Then $\bar{F}$ contains a real closed field Δ containing F.

Proof: Let $\mathcal{P} = \{S \mid S$ is an ordered subfield of $\bar{F}$ and $S \supset F\}$. $\mathcal{P}$ is not empty since $F \in \mathcal{P}$. Moreover it is inductively ordered by $\subseteq$. By Zorn's Lemma, it has a maximal element Δ. If Δ is not real closed, it has a proper algebraic extension Δ' which is an ordered field. Since $\bar{F}$ is algebraically closed, so we may assume that $\Delta' \subset \bar{F}$. This contradicts the maximality of Δ in F. Hence Δ is real closed.

SECTION II

STURM'S THEOREM

In this section we shall derive a classical result, Sturm's theorem, which permits us to determine the exact number of distinct roots in a real closed field of a polynomial equation f(x) = 0.

Definition 2.1. Given a function f, the function f' defined by

$$f' = \left\{(x, y) \mid y = \lim_{h \to 0} \frac{f(x + h) - f(x)}{h}\right\}$$

is called the derived function of f. For x in the domain of f', the number f'(x) is called the derivative of f at x, and

$$f'(x) = \lim_{h \to 0} \frac{f(x + h) - f(x)}{h} \quad .$$

The familiar rules (f + g)' = f' + g' and (fg)' = f'g + fg' can easily be shown to hold. Taylor's formula also holds.

Lemma 2.2. Let f(x) be a polynomial contained in F[x]. Let a be a root of f(x). Then a is a multiple root of f(x) if and only if f'(a) = 0.

Proof: We have f(x) = (x - a)g(x), so that f'(x) = g(x) + g'(x)(x - a). If a is a multiple root of

$f(x)$, $g(a) = 0$ and $f'(a) = 0$.

Conversely, if $f'(a) = 0$, then $g(a) = 0$, and a is a multiple root of $f(x)$.

Lemma 2.3. Let F be a real closed field. If $a \varepsilon F$ is a root of $f(x) \varepsilon F[x]$, then there exists an $h \varepsilon F$, $h > 0$, such that $f(x)f'(x) < 0$ for all x in $(a - h, a)$, and $f(x)f'(x) > 0$ for all x in $(a, a + h)$.

Proof: Substituting $(a - h)$ in $f(x)$ and $f'(x)$ and expanding, we get

$$f(a - h) = f(a) - f'(a)h + \frac{f^{(2)}(a)}{2!} h^2 - \dots + \frac{f^{(n)}(a)}{n!} (-h)^n$$

$$f'(a - h) = f'(a) - f^{(2)}(a)h + \dots + \frac{f^{(n)}(a)}{(n-1)!} (-h)^{n-1}$$

In case a is a simple root, then the signs of these expansions, which depend on those of their first nonzero terms, are unlike for positive small h. When the sign of h is changed, the signs of the expressions become the same.

If a is a r-multiple root of $f(x) \varepsilon F[x]$, then $f(a)$, $f'(a), \dots, f^{(r-1)}(a)$ all vanish. The first terms which do not vanish in the series expansion for $f(a - h)$ and $f'(a - h)$ are respectively,

$$\frac{f^{(r)}(a)}{r!} (-h)^r, \quad \frac{f^{(r)}(a)}{(r-1)!} (-h)^{r-1} .$$

Clearly they have different signs; but when the sign of h is changed, they will have the same signs.

If we extend the reasoning above to every consecutive pair of the series, $f(x)$, $f^{(1)}(x)$, . . . , $f^{(r-1)}(x)$, we will have the following proposition

Proposition 2.4. If a is an r-multiple root of $f(x) \varepsilon F[x]$, then signs in the series, $f(b)$, $f^{(1)}(b)$, . . . , $f^{(r-1)}(b)$ alternate for $b \varepsilon (a - h, a)$.

Lemma 2.5. Let F be a field of characteristic 0, $f(x)$ a polynomial contained in $F[x]$. If $d(x)$ is the highest common factor of $f(x)$ and $f'(x)$, then $g(x) = f(x)d(x)^{-1}$ has simple roots which are the distinct roots of $f(x)$.

Let F be a real closed field and let $f(x)$ be a polynomial with coefficients in F. We call a sequence of polynomials

$$f_0(x) = f(x),\ f_1(x),\ .\ .\ .\ ,\ f_s(x)$$

a Sturm sequence of polynomials for $f(x)$ for the interval $[a, b]$ (i.e. $a \leqslant x \leqslant b$) if $f_i(x) \varepsilon F[x]$ for $i = 1, . . . , s$, and

(1) $f_s(x)$ has no root in $[a, b]$,

(2) $f_0(a) \neq 0$, $f_0(b) \neq 0$,

(3) if $c \varepsilon [a, b]$ is a root of $f_i(x)$, $0 < i < s$, then $f_{i-1}(x)f_{i+1}(x) < 0$, and

(4) if $f(c) = 0$, where $c \varepsilon (a, b)$, then there exist

intervals $[c_1, c)$ and $(c, c_2]$ such that $f_0(x)f_1(x) < 0$ for x in the first of these and $f_0(x)f_1(x) > 0$ for x in the second. (I.e. $f_0(x)f_1(x)$ is an increasing function of x at $x = c$.)

If $r = \{r_0, r_1, \ldots, r_m\}$ is a finite sequence of non-zero elements of F, then we define the <u>number of variations in sign</u> of r to be the number of i, $0 \leqslant i \leqslant m - 1$, such that $r_ir_{i+1} < 0$. If $r = \{r_0, r_1, \ldots, r_m\}$ is an arbitary sequence of elements of F, then we define the number of variations in sign of r to be the number of variations in sign of the abbreviated sequence r' obtained by dropping the 0's in r. For example,

$$\{1, 0, 0, 0, 5, -3, 0, 6, 9, -3\}$$

has three variations in sign. We will denote the number of variations in sign of the sequence $\{f_0(t), f_1(t), \ldots, f_s(t)\}$ by $V(t)$.

<u>Theorem 2.6</u>. Let f(x) be a polynomial with coefficients in a real closed field F and let $f_0(x) = f(x), f_1(x), \ldots, f_s(x)$ be a Sturm sequence for f(x) in the interval $[a, b]$. Then the number of distinct roots of f(x) in (a, b) is $V(a) - V(b)$.

<u>Proof</u>: The interval $[a, b]$ is decomposed into subintervals by the roots of the polynomials $f_j(x)$ of the given Sturm sequence. Thus we have a sequence $a = a_0 < a_1$

$< \ldots < a_m = b$ such that none of the $f_j(x)$ has a root in (a_i, a_{i+1}). Choose $a_i' \varepsilon (a_{i-1}, a_i)$, $1 \leqslant i \leqslant m$ and let $V(a_i)$ be the number of variations in sign of the sequence $\{f_j(a_i'), j = 0, 1, \ldots, s\}$. Evidently, $V(a) - V(b) = (V(a) - V(a_1')) + \sum_{i=1}^{m-1}(V(a_i') - V(a_{i+1}')) + (V(a_m') - V(b))$.

The computation is divided into four parts.

(I) If $f_j(a) \neq 0$ for all j, such that $0 < j < s$, then $f_k(a)f_k(a_1') > 0$ for $k = 0, 1, \ldots, s$. Hence $V(a) = V(a_1')$.

(II) If $f_j(a) = 0$ for some j, $0 < j < s$. Then by (3) $f_{j-1}(a)f_{j+1}(a) < 0$. Since $f_{j-1}(x)$ and $f_{j+1}(x)$ have no roots in (a, a_1), $f_{j-1}(a)f_{j-1}(a_1') > 0$, and $f_{j+1}(a)f_{j+1}(a_1') > 0$. Hence $f_{j-1}(a_1')f_{j+1}(a_1') < 0$. It follows that $f_{j-1}(a)$, $f(a)$ $(= 0)$, $f_{j+1}(a)$ and $f_{j-1}(a_1')$, $f_j(a_1')$, $f_{j+1}(a_1')$ contribute the same number of variations of sign to $V(a)$ and $V(a_1)$ respectively. Taking into account all the j, we see that $V(a) - V(a_1') = 0$. Similar argument shows that $V(a_m') - V(b) = 0$.

(III) If $f_j(a_i) = 0$ for $1 < j < s$, $1 \leqslant i \leqslant m - 1$, the argument used above shows that $f_{j-1}(a_i')$, $f_j(a_i')$, $f_{j+1}(a_i')$ and $f_{j-1}(a_{i+1}')$, $f_j(a_{i+1}')$, $f_{j+1}(a_{i+1}')$ have the same number of variations of sign.

(IV) If $f(a_i) = 0$ for $1 \leqslant i \leqslant m - 1$, then by (4)

$f(a_i')f_1(a_i') < 0$ and $f(a_{i+1}')f_1(a_{i+1}') > 0$. This implies $f(a_i'), f_1(a_i')$ has one variation and $f(a_{i+1}'), f_1(a_{i+1}')$ has none. Hence we see that $V(a_i') - V(a_{i+1}') = 1$ if $f(a_i) = 0$.

Hence $V(a) - V(b) = V(a) - V(a_1') + \sum_{i=1}^{m-1}(V(a_i') - V(a_{i+1}')) + V(a_m') - V(b)$ is the number of a_i such that $f(a_i) = 0$.

Let $f(x)$ be an arbitary polynomial such that $f(a) \neq 0$, $f(b) \neq 0$. We define <u>the standard sequence</u> for $f(x)$ by

$$f_0(x) = f(x),\ f_1(x) = f'(x) \text{ (formal derivative of } f(x))$$
$$f_0(x) = q_1(x)f_1(x) - f_2(x),\ \deg f_2 < \deg f_1$$
$$f_1(x) = q_2(x)f_2(x) - f_3(x),\ \deg f_3 < \deg f_2$$
$$\vdots$$
$$f_{i-1}(x) = q_i(x)f_i(x) - f_{i+1}(x),\ \deg f_{i+1} < \deg f_i$$
$$f_{s-1}(x) = q_s(x)f_s(x)$$

Thus the $f_i(x)$ are obtained by modifying the Euclid algorithm for finding the highest common factor of $f(x)$ and $f'(x)$ in such a way that the last polynomial obtained at each stage is the negative of the remainder in the division process. Clearly, $f_s(x)$ is the highest common factor of $f(x)$ and $f'(x)$ and this is a divisor of all the $f_i(x)$. Now set $g_i(x) = f_i(x)f_s(x)^{-1}$, and consider the sequence

$$g_0(x),\ g_1(x),\ .\ .\ .\ ,\ g_s(x)$$

Proposition 2.7. The sequence constructed above is a Sturm sequence for $g_0(x)$ in any interval $[a, b]$ such that $f(a) \neq 0$, $f(b) \neq 0$.

Proof: (i) Since $g_s(x) = 1$, $g_s(x)$ has no roots in $[a, b]$.

(ii) $g_0(x) = f_0(x)f_s(x)^{-1}$, so $g_0(a) \neq 0$, $g_0(b) \neq 0$ since $f_0(a) \neq 0$, $f_0(b) \neq 0$.

(iii) Note that $f_{j-1}(x) = q_j(x)f_j(x) - f_{j+1}(x)$. Dividing both sides by $f_s(x)$, we get $g_{j-1}(x) = q_j(x)g_j(x) - g_{j+1}(x)$, $0 < j < s$. If $g_i(c) = 0$, $c \in [a, b]$, we get $g_{i-1}(c) = -g_{i+1}(c)$. Now $g_{i-1}(c) = 0$, implies $g_{i+1}(c) = 0$. Replacing i with i + 1 and continuing we eventually get $g_s(c) = 0$. This contradicts that $g_s(c) = 1$. Therefore, $g_{i-1}(c)g_{i+1}(c) < 0$.

(iv) Suppose $c \in (a, b)$ and $g_0(c) = 0$, then $f_0(x) = (x - c)^e h(x)$, where $e > 0$ and $h(c) \neq 0$; then $f'(x) = e(x - c)^{e-1}h(x) + (x - c)^e h'(x)$. Also, $f_s(x) = (x - c)^{e-1}k(x)$, where $k(x) \neq 0$. So $h(x) = k(x)l(x)$, $l(c) \neq 0$, $h'(x) = k(x)m(x)$. Hence $g_0(x) = (x - c)l(x)$, where $l(c) \neq 0$, and $g_1(x) = el(x) + (x - c)m(x)$, $g_1(c) = el(c) \neq 0$.

Now choose an interval $[c_1, c_2]$ containing c in its interior such that $l(x) \neq 0$ and $g_1(x) \neq 0$ in $[c_1, c_2]$. Then $g_1(x)$ and $l(x)$ are either both positive or both negative. $g_0(x)g_1(x) = (x - c)l(x)g_1(x) < 0$ for $x \in [c_1, c)$, and $g_0(x)g_1(x) = (x - c)l(x)g_1(x) > 0$ for $x \varepsilon (c, c_2]$. Hence (4) holds.

Note: If $f(x)$ has no multiple roots, then the sequence $\{f_i(x)\}$ is a Sturm sequence for $f(x) = f_0(x)$. Otherwise, $g_0(x)$ has the same number of distinct roots as f_0. Hence we can use the sequence $\{g_i(x)\}$ to determine the number of distinct roots of $f(x)$ in (a, b). This is the content of Sturm's Theorem.

Theorem 2.8. (STURM'S THEOREM) Let $f(x)$ be any polynomial with coefficients in a real closed field F. And let $f_0(x) = f(x)$, $f_1(x) = f'(x)$, $f_2(x)$, . . . , $f_s(x)$ be the standard sequence for $f(x)$. Assume $[a, b]$ is an interval such that $f(a) \neq 0$, $f(b) \neq 0$. Then the number of distinct roots of $f(x)$ in (a, b) is $V(a) - V(b)$.

Proof: Let $g_i(x) = f_i(x)f_s(x)^{-1}$ as above. Then apart from the multiplicities, the polynomials $f(x)$ and $g_0(x)$ have the same roots in (a, b) by Lemma 2.5. Since the sequence $\{g_i(x)\}$ is a Sturm sequence for $g_0(x)$, the number of these roots is $V(a_g) - V(b_g)$ where $V(c_g)$ is the number of variations in sign in $\{g_i(c)\}$. Since $f_i(c) = g_i(c)f_s(c)$, and $f_s(a) \neq 0$, $f_s(b) \neq 0$, it is clear that $V(a_g) = V(a)$, and $V(b_g) = V(b)$. Hence the number of distinct roots of $f(x)$ in (a, b) is $V(a) - V(b)$.

Theorem 2.9. (ROLLE'S THEOREM) Let F be a real closed field. If $f(x) \varepsilon F[x]$ has roots $a, b \varepsilon F$, with $a < b$, then there exists a $c \varepsilon F$, with $a < c < b$, such that $f'(c) = 0$.

Proof: We can assume f has no roots in (a, b). Now by Lemma 2.3, there exist h_1, h_2 positive with

$f(x)f'(x) > 0$ for $x \varepsilon (a, a + h_1)$

$f(x)f'(x) < 0$ for $x \varepsilon (b - h_2, b)$.

Choose x_1, x_2 with $a < x_1 < x_2 < b$ and $x_1 < a + h_1$, $b - h_2 < x_2$, then $f(x_1)f'(x_1)f(x_2)f'(x_2) < 0$. But $f(x_1)f(x_2) > 0$, since otherwise f has a root in (x_1, x_2) by Theorem 1.23. Thus $f'(x_1)f'(x_2) < 0$ and f' has a root in (x_1, x_2) by Theorem 1.23.

Lemma 2.10. Let F be a real closed field. Suppose $a, b \varepsilon F$, and $f(x) \varepsilon F[x]$. If $f(a) = f(b) = 0$, and $f(x) \neq 0$ for all x in (a, b), then $f'(x)$ has an odd number of roots in (a, b).

Proof: Since f(x) has no roots in (a, b), either $f(x) > 0$ for all x in (a, b) or $f(x) < 0$ for x in (a, b). Say $f(x) > 0$ for all x in (a, b). Suppose $f'(x)$ has an even number of roots in (a, b), say $a_1, a_2, \ldots, a_{2r}$, where $a < a_1 < a_2 < \ldots < a_{2r} < b$ and r any non-negative integer. $r = 0$ will contradict Rolle's Theorem, so consider the case $r > 0$.

Since $f(a) = f(b) = 0$, we know that $f(x)f'(x) > 0$ for all x in (a, a_1), and $f(x)f'(x) < 0$ for all x in (a_{2r}, b). Since there is no root for $f'(x)$ in (a_i, a_{i+1}), for $i = 1, 2, \ldots, 2r-1$, hence $f'(x) < 0$ for all x in (a_{2i-1}, a_{2i}) for $i = 1, 2, \ldots, r$, $f'(x) > 0$ for all x in (a_{2i}, a_{2i+1}) for $i = 1, 2, \ldots, r-1$, and $f'(x) > 0$ for all x in (a_{2r}, b). This would imply that $f(x)f'(x) > 0$ for all x in (a_{2r}, b).

A similar argument in case $f(x) < 0$ for all x in (a, b) leads the conclusion that $f(x)f'(x) < 0$ for all x in (a, a_1), a contradiction.

Hence $f'(x)$ has an odd number of roots in (a, b).

Theorem 2.11. (MEAN-VALUE THEOREM) If $a < b$ in a real closed field F, then there exists a c, with $a < c < b$, such that $f(b) - f(a) = (b - a)f'(c)$.

Proof: Since $b > a$, $b - a \neq 0$, $(f(b) - f(a))/(b - a)$ is defined. Let $(f(b) - f(a))/(b - a) = t$. Then $f(b) - f(a) = t(b - a)$, or $f(b) = t(b - a) + f(a)$. Let $g(x) = -f(b) + f(x) + (b - x)t$, then $g'(x) = f'(x) - t$. But $g(a) = 0$, and $g(b) = 0$. Hence, by Rolle's Theorem, there exists a $c \varepsilon (a, b)$ such that $g'(c) = 0$. Since $g'(c) = f'(c) - t$, $f'(c) = t$. Hence $f(b) - f(a) = (b - a)f'(c)$.

Lemma 2.12. Let $f(x)$ be a polynomial in $F[x]$, where F is a formally real field. Let $f'(x)$ be its formal derivative. If $f'(x)$ has no roots in (a, b), and $M = \max \{f(a), f(b)\}$, $m = \min \{f(a), f(b)\}$, then $M \geq f(x)$ for all x in $[a, b]$, $m \leq f(x)$ for all x in $[a, b]$.

Proof: Let $g(x) = f(x) - M$. Note that $g'(x) = f'(x)$. Since $g'(x)$ has no roots in (a, b), $m \neq M$; $g(x)$ has no roots in (a, b) either, for otherwise, by Rolle's Theorem, we will get a contradiction. Since either $g(a) < 0$ or $g(b) < 0$, we see that $g(t) < 0$ for all t in (a, b). Hence $g(x) = f(x) - M \leq 0$ for all x in $[a, b]$, i.e., $f(x) \leq M$ for all x in $[a, b]$.

A similar argument shows $f(x) \geq m$ for all x in $[a, b]$.

Proposition 2.13. Let $S = \{x \varepsilon [a, b] \mid f'(x) = 0\} \cup \{a, b\}$. Let $M = \max \{f(x) \mid x \varepsilon S\}$, $m = \min \{f(x) \mid x \varepsilon S\}$. Then $M \geq f(t)$ for all t in $[a, b]$, $m \leq f(t)$ for all t in $[a, b]$.

Proof: S is finite. Let $S = \{x_0, x_1, . . . , x_n\}$ with $x_i < x_j$ if $i < j$. The proposition follows from applying Lemma 2.12 to the intervals $[x_i, x_{i+1}]$, $i = 0, 1, . . . , n-1$.

Corollary 2.14. $f(x)$ has a maximum and minimum on any closed interval $[a, b]$.

Proof: This follows immediately from Proposition 2.13.

Theorem 2.15. (BUDAN'S THEOREM) Let F be a real closed field. Let $f(x) \in F[x]$ have degree n and assume elements a, b satisfy $a < b$ and are not roots of $f(x)$. For $r \in F$, let $V(r)$ denote the number of variations in sign in the sequence $\{f(r), f'(r), \ldots, f^{(n)}(r)\}$. Then $V(a) - V(b)$ exceeds the number of roots of $f(x)$ in F in (a, b), each counted with its multiplicity, by a non-negative even integer.

Proof: (i) If $f(x)$ has a single root t in (a, b), one change of sign is lost, for $f(x)$ and $f'(x)$ have unlike signs for all x in $(t - h, t)$, and like signs for all x in $(t, t + h)$, where $h > 0$, by Lemma 2.3.

(ii) If $f(x)$ has an r-multiple root t in (a, b), r changes of sign are lost, for, by Proposition 2.4, $f(x)$, $f'(x), \ldots, f^{(r-1)}, f^{(r)}$ have alternating signs immediately before, and immediately after the passage have all the same sign as $f^{(r)}$.

(iii) If $f^{(m)}(t) = 0$ for $t \in (a, b)$, but $f^{(m-1)}(t) \neq 0$, $f^{(m+1)}(t) \neq 0$, then $f^{(m-1)}(t)$ and $f^{(m+1)}(t)$ are either of like sign or unlike sign. Suppose they are of like sign, either " + 0 + " or " - 0 - ". By Proposition 2.4, immediately before the root $(x < t)$ we have + - +, or - + -, and immediately after we have + + +, or - - -. So two variations of sign are lost. Suppose they are of unlike sign; then no change of sign is lost, for immediately before the passage, the signs of $f^{(m-1)}(x)$, $f^{(m)}(x)$, $f^{(m+1)}(x)$ must be either + + - or - - + and after the passage these become + - -, and - + +. Therefore, on the whole, we conclude that either no variation can be gained, or two variations may be lost.

(iv) Suppose $f^{(m)}(x) = 0$ has an r-fold root $t \varepsilon (a, b)$ and $f^{(m-1)}(t) \neq 0$; i.e., $f^{(m-1)}(t) \neq 0$, $f^{(m)}(t) = f^{(m+1)}(t) = \ldots = f^{(m+r-1)}(t) = 0$.

Let's look at the series of functions

$f^{(m-1)}(x)$, $f^{(m)}(x)$, . . . , $f^{(m+r-1)}(x)$, $f^{(m+r)}(x)$.

There are two cases to consider:

(1) $f^{(m-1)}(a)$ and $f^{(m+r)}(a)$ have like signs. If r is even, r changes of sign are lost. If r is odd, r+1 changes of sign are lost. Because signs alternate to the left of t and are the same to the right of t.

(2) $f^{(m-1)}(a)$ and $f^{(m+r)}(a)$ have unlike signs. If r is even, r changes of sign are lost. If r is odd, r-1 changes of sign are lost.

Since $f(x)$, $f'(x)$, . . . , $f^{(n)}(x)$ have only finite number of roots, by induction, the theorem is proved.

Corollary 2.16. (DESCARTES' RULE) Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_ix^{n-i}$, $a_0 \neq 0$, $a_j \varepsilon F$, for $j = 1, 2, \ldots, i$. Let S denote the number of variations in sign in the sequence $\{a_0, \ldots, a_i\}$. Then S exceeds the number of positive roots of f(x), counting multiplicities, by a non-negative even integer.

Proof: When zero is substituted for x in $f^{(i)}(x)$, $f^{(i-1)}(x)$, . . . , $f^{(1)}(x)$, $f(x)$, the signs are the same as the signs of the coefficients a_0, a_1, . . . , a_i. For sufficiently large x, the signs are the same as a_0. By Budan's Theorem, the number of positive roots can not exceed the number of variations lost during the passage from 0 to $+\infty$, that is the number of changes of sign in the series $\{a_0, a_1, \ldots, a_i\}$.

We observe that $f(r) = f(-(-r))$, and r is a negative solution of $f(x) = 0$ if and only if $-r$ is a positive solution of $f(-x) = 0$; thus, we can study the negative solutions of $f(x) = 0$ by examination of the positive solutions of $f(-x) = 0$.

Proposition 2.17. Let F be an ordered field. $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ is a polynomial with coefficients in F. Let $M = \max\{1, \sum_{i=1}^{n} |a_i|\}$. Then every root of f(x) in F is contained in the interval $[-M, M]$.

Proof: If $f(x) = 0$, then $x^n = -\sum_{i=1}^{n} a_i x^{n-i}$. $0 \neq |x|^n = |-\sum_{i=1}^{n} a_i x^{n-i}| \leqslant \sum_{i=1}^{n} |a_i||x|^{n-i}$, $1 \leqslant \sum_{i=1}^{n} (|a_i|/|x|^i)$. Suppose $|x| > M \geqslant 1$, then $|x|^i > M$ for all i, so $|a_i|/|x|^i < |a_i|/M$; $1 \leqslant \sum_{i=1}^{n} (|a_i|/|x|^i) < \sum_{i=1}^{n} (|a_i|/M)$ $= (\sum_{i=1}^{n} |a_i|)/M$, so $M < \sum_{i=1}^{n} |a_i|$, a contradiction. Hence $-M \leqslant x \leqslant M$.

If we set $\mu = 1 + |a_1| + . . . + |a_n|$, then the roots of $f(x)$ in F are in $(-\mu, \mu)$. If $f_0(x) = f(x), f_1(x), . . . , f_s(x)$ is the standard sequence for $f(x)$, then the number of roots of $f(x)$ in F is $V(-\mu) - V(\mu)$ where $V(r)$ is the number of variations in sign in $\{f_0(r), f_1(r), . . . , f_s(r)\}$. This gives a constructive way of determining the number of roots of $f(x)$ in F.

SECTION III

REAL CLOSURE OF AN ORDERED FIELD

Any ordered field can be imbedded in a real closed field. We shall now show that, if F is an ordered field, then there exists a real closed algebraic extension field Δ of F whose (unique) ordering is an extension of that of F. Moreover, we shall see that Δ is essentially unique.

Definition 3.1. Let F be an ordered field. Then an extension field Δ of F is called a real closure of F if:

(1) Δ is real closed,

(2) Δ is algebraic over F,

(3) the ordering of Δ is an extension of that of F.

Similarily,

Definition 3.2. Let (F, P) be an ordered field. Then (Δ, P') is an order closure of (F, P) if and only if (Δ, P') $\supset$ (F, P), (Δ, P') is order closed and Δ is algebraic over F.

Theorem 3.3. Let F be an ordered field, ν a real closed extension field whose order is an extension of that of F. Then ν contains a real closure of F.

Proof: Let T be an algebraic closure of F in ν. Let $\bar{F}$ be the algebraic closure of F in $\nu[\sqrt{-1}]$. Note that $\bar{F}$ is algebraically closed since $\nu[\sqrt{-1}]$ is.

Let $p(x) \in T[x] \subset \nu[x]$ be irreducible over $T[x]$, and suppose $\xi \in \bar{F}$ is a root of $p(x)$. We want to show $\sqrt{-1} \in T[\xi]$, so that no proper algebraic extension of T can be ordered.

Note that $\xi \notin \nu$. So $\xi = a + b\sqrt{-1}$ for some $a, b \in \nu$, and $b \neq 0$. $\bar{\xi} = a - b\sqrt{-1}$, $p(\bar{\xi}) = 0$, so $\bar{\xi} \in \bar{F}$, and $\sqrt{-1} \in \bar{F}$.

Thus $2a = \xi + \bar{\xi} \in \bar{F} \cap \nu$, so $a \in T$,

$2b = \sqrt{-1}(\bar{\xi} - \xi) \in \bar{F} \cap \nu$, so $b \in T$.

Hence $\sqrt{-1} = (\xi - a)/b \in T[\xi]$. T is a real closure of F.

Theorem 3.4. Every ordered field has an order closure.

Proof: Let (F, P) be an order field and let $\bar{F}$ be the algebraic closure of F. Let $\mathcal{P} = \{(K, P_K) \mid K \subset \bar{F}, (K, P_K)$ is an order extension of $(F, P)\}$. Define $(K, P_K) < (T, P_T)$ if (T, P_T) is an order extension of (K, P_K). $\mathcal{P}$ is not empty since it contains (F, P). Moreover, $\mathcal{P}$ is inductively ordered, so by Zorn's Lemma, $\mathcal{P}$ contains a maximal element (Δ, P'). If (Δ, P') is not an order closure, it has a proper algebraic extension Δ' which is an ordered field. Since $\bar{F}$ is algebraically closed, we may assume that $\Delta' \subset \bar{F}$. This contradicts the maximality of Δ in $\bar{F}$. Thus Δ is an order closure, hence a real closure.

Lemma 3.5. Let F_1, and F_2 be ordered fields with real closures Δ_1 and Δ_2, respectively. And let $a \longrightarrow \bar{a}$

be an order isomorphism of F_1 onto F_2. If $f(x) \varepsilon F_1[x]$, then $f(x)$ and its image $\bar{f}(x)$ under $a \longrightarrow \bar{a}$ have the same number of roots in Δ_1 and Δ_2, respectively.

Proof: We have seen that there exists a $\mu > 0$, $\mu \varepsilon F$, such that every root of $f(x)$ in Δ_1 is contained in $(-\mu, \mu)$. Moreover, by Sturm's Theorem, the number of roots of $f(x)$ in the interval $(-\mu, \mu)$, hence the total number of roots of $f(x)$ in Δ_1, is given by $V(-\mu) - V(\mu)$, where $V(r)$ is the number of variations in sign of the standard sequence of f at r. Since the standard sequence of f is contained in $F_1[x]$, all of this carries over to $\bar{f}(x)$ in Δ_2. Hence the number of roots of $\bar{f}(x)$ in Δ_2 is the same as the number of roots of $f(x)$ in Δ_1.

Lemma 3.6. Let F_1, F_2, Δ_1, Δ_2, be as in Lemma 3.5. Let $S \subset \Delta_1$, S finite; then there exists a subfield T_1 of Δ_1 containing F_1 and S and an isomorphism σ of T_1 into Δ_2 which extends $a \longrightarrow \bar{a}$ and $\sigma(x) < \sigma(y)$ in Δ_2 whenever $x, y \varepsilon S$ and $x < y$.

Proof: Let $S = \{a_1, a_2, \ldots, a_n\}$ be a finite subset of Δ_1, and $a_1 < a_2 < a_3 < \ldots < a_n$. Let $f(x)$ be a polynomial in $F_1[x]$ which has a_i, $1 \leqslant i \leqslant n$, $b_j = \sqrt{a_{j+1} - a_j}$, $1 \leqslant j \leqslant n-1$, among its roots. We note that $b_j \varepsilon \Delta_1$ since Δ_1 is real closed and $a_{j+1} - a_j > 0$. Let T_1 be the finite dimensional extension of F_1 generated by the roots of $f(x)$

in Δ_1. Then $T_1 = F_1(\xi_1)$ and, if $g(x)$ is the minimum polynomial of ξ_1 over F_1, $\bar{g}(x)$ has a root ξ_2 in Δ_2. We have an isomorphism σ of T_1 onto $F_2(\xi_2)$ such that $\sigma(a) = \bar{a}$, $a \varepsilon F_1$, and $\sigma(\xi_1) = \xi_2$. Then $\sigma(a_{j+1}) - \sigma(a_j) = \sigma(a_{j+1} - a_j) = (\sigma(b_j))^2 > 0$. Hence $\sigma(a_1) < \sigma(a_2) < . . . < \sigma(a_n)$ in Δ_2 as required.

Theorem 3.7. Let F_1, F_2, Δ_1, Δ_2 be as above. Then any order isomorphism of F_1 onto F_2 has a unique extension to an isomorphism Δ_1 onto Δ_2. The extension is an order isomorphism.

Proof: Let $\xi \varepsilon \Delta_1$, and let $p(x)$ be the minimum polynomial of ξ over F_1. Let $a_1 < a_2 < . . . < a_m$ be the roots of $p(x)$ in Δ_1, and suppose $a_k = \xi$. Then $\bar{p}(x)$ has exactly m roots, $a_1' < a_2' < . . . < a_m'$ in Δ_2 and we now set $\eta(\xi) = a_k'$.

η is well-defined and $\eta(a) = \bar{a}$ for all a in F_1.

Let $x, y \varepsilon \Delta_1$.

Let p_1 be the minimum polynomial of x.

Let p_2 be the minimum polynomial of y.

Let p_3 be the minimum polynomial of xy.

Let p_4 be the minimum polynomial of x + y.

Consider the set $S = \{\xi \mid p_i(\xi) = 0$ for some i, $1 \leq i \leq 4\}$. We have seen there exists a subfield T_1 of Δ_1 with $S \subset T_1$, and σ: $T_1 \longrightarrow \Delta_2$, an isomorphism preserving order on S.

As before, let $p(x)$ be the minimum polynomial of ξ over F_1 and let $a_1 < a_2 < \ldots < a_m$ be the roots of $p(x)$ contained in Δ_1. Then $a_i \varepsilon S$ and $\sigma(a_1) < \sigma(a_2) < \ldots < \sigma(a_m)$. We have $\bar{p}(\sigma(a_i)) = 0$ and it follows from the definition of η that $\eta(\xi) = \sigma(\xi)$. Since σ is an isomorphism, this implies $\eta(x + y) = \eta(x) + \eta(y)$ and $\eta(xy) = \eta(x)\eta(y)$. Hence η is an isomorphism of Δ_1 onto Δ_2 extending the given isomorphism of F_1 onto F_2.

Now if η' is an isomorphism of Δ_1 onto Δ_2, then η' preserves order (i.e., η' maps squares into squares). Suppose η' extends the mapping $a \longrightarrow \bar{a}$. Let $\xi \varepsilon \Delta_1$, and let $a_1 < a_2 < \ldots < a_m$ be the roots in Δ_1 of the minimum polynomial $p(x)$ of ξ over F_1. Then $\eta'(a_1) < \ldots < \eta'(a_m)$ are the roots in Δ_2 of $\bar{p}(x)$. It follows that $\eta'(\xi) = \eta(\xi)$. Hence the extension is unique.

Remark: If Δ_1 and Δ_2 are two real closures of a given ordered field F, then the identity mapping on F can be extended to an order isomorphism of Δ_1 onto Δ_2. In this sense real closures are equivalent and we may therefore speak of the real closure of F.

Proposition 3.8. The field $Q(\sqrt{2})$ where Q is the field of rational numbers has exactly two distinct orders.

Proof: Consider $Q[x]/(x^2 - 2) = Q(\xi)$ where $\xi^2 = 2$. It has two distinct natural isomorphisms from $Q(\xi)$

into the real closure $\bar{Q}$ of rationals. One is given by $f_1(\xi) = \sqrt{2}$ and $f_1(a) = a$ for all a in Q; the other one is given by $f_2(\xi) = -\sqrt{2}$ and $f_2(a) = a$ for all $a \in Q$.

Let P be the set of positive elements of $\bar{Q}$. We claim $f_1^{-1}(P)$ and $f_2^{-1}(P)$ are two distinct orderings for $Q(\xi)$.

Subproof: (1) If $0 \neq x \in Q(\xi)$, either $f_i(x) \in P$, $x \in f_i^{-1}(P)$; or $-f_i(x) \in P$, $-x \in f_i^{-1}(P)$, $i = 1, 2$.

(2) $f_i^{-1}(P)$ is closed under addition and multiplication for $i = 1, 2$. Whenever $x \in f_i^{-1}(P)$, then $f_i(x) \in P$ and whenever $y \in f_i^{-1}(P)$, then $f_i(y) \in P$. It follows that whenever $f_i(x + y) \in P$, then $x + y \in f_i^{-1}(P)$, and whenever $f_i(xy) \in P$, then $xy \in f_i^{-1}(P)$.

(3) They are distinct because $\xi \in f_1^{-1}(P) \setminus f_2^{-1}(P)$.

So we have established two distinct orderings for Q. (i.e., $a + b\xi \in f_1^{-1}(P)$ if and only if $a + b\sqrt{2} > 0$; and $a + b\xi \in f_2^{-1}(P)$ if and only if $a - b\sqrt{2} > 0$).

Let P' be an order of $Q(\xi)$. Let S be a real closure of $(Q(\xi), P')$; Let P'^* be the order of S. Note that $S \cong \bar{Q}$ by a map $f\colon S \longrightarrow \bar{Q}$, and $f^{-1}(P) = P'^*$.

$f|_{Q(\xi)}\colon Q \longrightarrow \bar{Q}$. Since there are only two such maps, $f|_{Q(\xi)} = f_i$ for $i = 1, 2$. Also, $P' = P'^* \cap Q(\xi)$ $= f^{-1}(P) \cap Q(\xi) = f|_{Q(\xi)}{}^{-1}(P) = f_i^{-1}(P)$; i.e., $P' = f_i^{-1}(P)$ for $i = 1, 2$.

Therefore the only orderings are $f_i^{-1}(P)$, $i = 1, 2$.

Proposition 3.9. Let Q be the field of rational numbers and let $F = Q(\xi)$ where ξ is transcendental. Then F has uncountably many distinct orderings.

Proof: Let R be the real numbers. We know there are an uncountable number of transcendental elements $t \in R$.

Let $S = \{t \in R \mid t \text{ transcendental}\}$. For $t \in S$, let ρ_t be the isomorphism $Q(\xi) \longrightarrow R$, which maps ξ to t and a to a for all $a \in Q$.

Let P be the order on R, then $\rho_t^{-1}(P) = P_t$ is an order on $Q(\xi)$ by using the same argument as Proposition 3.8.

We claim $P_t = P_{t'}$ if and only if $t = t'$. If not, we may assume $t' < t$. So there exists a rational number a such that $t' < a < t$ which implies $\rho_{t'}(\xi) < a < \rho_t(\xi)$. So $\xi = \rho_{t'}^{-1}\rho_{t'}(\xi) < \rho_{t'}^{-1}(a) = a$ and $\xi = \rho_t^{-1}\rho_t(\xi) > \rho_t^{-1}(a) = a$, i.e., $\xi <_{\rho_{t'}} a$ and $\xi >_{\rho_t} a$.

Hence there are uncountably many orderings on $Q(\xi)$, if ξ is transcendental.

SECTION IV

FUNDAMENTAL THEOREM OF ALGEBRA

Definition 4.1. An ordered field F is said to be Archimedean[1] (or Archimedean ordered) if there exists a positive integer n such that $n > a$ for every $a \in F$.

Example: Q, the field of rational numbers, and R, the field of real numbers, are Archimedean ordered.

Note: If the ordering of a field is not Archimedean, there exist "infinitely large" elements, larger than any rational number, and "infinitely small" elements which are smaller than any positive rational number but larger than zero.

Example: Consider $Q(t)$, where Q is the set of rationals and t is an indeterminate. Define an order on $Q(t)$ by: $f(t)$ is positive if the leading coefficient of f is positive, $f(t)$ is negative if the leading coefficient of f is negative, $f(t)/q(t)$ is positive if the leading coefficient of fq is positive, and $f(t)/q(t)$ is negative if the leading coefficient of fq is negative, where $f(t)$, $q(t) \in Q[t]$, and $q(t) \neq 0$.

[1] The "Archimedean axiom" in geometry runs as follows: Starting from a given point P ("zero point") a given line segment PQ ("unity segment") can always be laid off in the direction PR a number of times so that the last end point lies beyond any given point R.

This ordered field is not Archimedean since if $f(t) = t$ in $Q(t)$, there does not exist an integer such that $n > f(t)$, i.e., t is infinitely large. Since $n < t$ for all integers $n > 0$, $1/n > 1/t$ for all integers $n > 0$. $1/t$ is called as "infinitesimal".

Remark: An ordered field need not be dense (order sense) in a finite ordered extension, as we can see in the example which follows.

Example: Let $f(x) = (x^2 - t)^2 - t^3 \varepsilon F[x]$, where $F = Q(t)$ is ordered with t a positive infinitesimal.

First we define $f(a) = (a^2 - t)^2 - t^3$ and observe $f(a) = f(-a)$. Let $x >> y$ mean for all positive integers n, $x > ny$. Note that $t >> t^2 >> t^3$ since t is infinitesimal and $a >> t$ if a is positive in Q.

If $a = p(t)$ with rational coefficients and constant term zero, we can write $a^2 - t = (-t) + t^2(q(t))$ for some $q(t)$. Now $(a^2 - t)^2 = t^2 - 2t^3q(t) + t^4(q(t))^2$, so that

$$f(a) = (a^2 - t)^2 - t^3 = t^2 - 2t^3q(t) + t^4(q(t))^2 - t^3$$
$$= t^2 - t^3(h(t)) > 0 \text{ for all } a \varepsilon F.$$

$f(x)$ has four roots in any order closure of F. Two are positive, $\sqrt{t(1+\sqrt{t})}$ and $\sqrt{t(1-\sqrt{t})}$, and two are negative, $-\sqrt{t(1-\sqrt{t})}$, and $-\sqrt{t(1+\sqrt{t})}$. Call them x_1, x_2, x_3, and x_4 respectively. Note that $x_1 > x_2 > x_3 > x_4$, and $f(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)$. Let $x_1 > a > x_2$, then $f(a) = (a - x_1)(a - x_2)(a - x_3)(a - x_4) < 0$, so $a \not\varepsilon F$.

The above example is also a counterexample to the converse of Theorem 1.12.

Theorem 4.2. Let T be an ordered field, and T' a subfield of T with the induced ordering. Then T is Archimedean if:

(1) T' is Archimedean

(2) $[T : T'] < \infty$.

Proof: Take any $a \in T \setminus T'$, $a > 0$. Since $[T : T'] < \infty$, let $f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i}$ be the minimal polynomial of a in $T'[x]$. Since a is a root of $f(x)$ in T, $0 < a \leq M$ where $M = \max (1, \sum_{i=1}^{n} |a_i|)$, and $M > 0$ in T', by Proposition 2.17. But T' is Archimedean, so there exists an integer n such that $n > M$ and $n > M \geq a > 0$. Hence $n > a$ and the theorem is proved.

Corollary 4.3. The order closure of an Archimedean ordered field is Archimedean.

Proof: Let T be an Archimedean ordered field, and $\bar{T}$ its order closure. Take any $t \in \bar{T}$, then $T(t)$ with the induced ordering is an ordered field. And $[T(t) : T] < \infty$, so $T(t)$ is Archimedean, and there exists an integer n such that $n > t$. This is true for all $t \in \bar{T}$, so $\bar{T}$ is Archimedean.

If S is a set of real numbers, we say that b is an upper bound for S if for each $x \in S$ we have $x \leq b$. We sometimes express this by writing $S \leq b$. A number c is called a least upper bound for S if it is an upper bound for S and if $c \leq b$ for each upper bound b of S. Clearly the least upper bound of a set S is unique if it exists. We shall denote the least upper bound of S by sup S.

We will take as known the fact that the field of real numbers satisfies the

Completeness Axiom: Every nonempty set S of real numbers which has an upper bound has a least upper bound.

We can define lower bounds and greatest lower bounds in a similar fashion. We denote the greatest lower bound of a set S by inf S.

Definition 4.4. A set A of rational numbers is said to be a cut if (1) A contains at least one rational, but not every rational;

(2) if $p \in A$ and $q < p$ (q rational), then $q \in A$;

(3) A contains no largest rational.

If A and B are any two sets of rational numbers such that: (1) every rational number is either in A or in B;

(2) no rational number is in A and in B;

(3) neither A nor B is empty;

(4) if $a \in A$, and $b \in B$, then $a < b$

hold. Then we say A and B define a Dedekind cut.

Lemma 4.5. Let R be the field of reals. R is

Archimedean. Let $a \varepsilon R$ and $a > 0$. If $S_a = \{t \varepsilon Q \subset R \mid t < a\}$ and S_a' is the complement of S_a in Q, then $\sup S_a = \inf S_a'$.

Proof: S_a is bounded above, since R is Archimedean. And S_a' is bounded below. Since S_a contains every $s < r$ for every $r \varepsilon S_a$. S_a and its complement S_a' in the set of positive rationals define a Dedekind cut. $\sup S_a = t \lesssim s = \inf S_a'$. Suppose $t < s$, then there exist $m \varepsilon Q$ and $t < m < s$. Then either $a < m$ or $m < a$, this can not be either if $t < s$. So $t = s$.

Theorem 4.6. If (F, P) is an Archimedean ordered field, then there exists a unique order isomorphism from F into R.

Proof: We first define f: $P \longrightarrow R$ via

$f(a) = \sup S_a$ ($= \inf S_a'$ by Lemma 4.5).

f is well defined. We will show that f is a homomorphism, i.e., $f(a + b) = f(a) + f(b)$; $f(ab) = f(a)f(b)$

Let a, b be any positive elements of F and let $m_1/n_1 \varepsilon S_a$, $m_2/n_2 \varepsilon S_b$, where m_i, $n_i \varepsilon P$. Then

$m_1/n_1 \leqslant a$; $m_1 \leqslant n_1 a$ $m_1 n_2 \leqslant n_1 n_2 a$ since $n_2 \varepsilon P$.

$m_2/n_2 \leqslant b$; $m_2 \leqslant n_2 b$ $n_1 m_2 \leqslant n_1 n_2 b$ since $n_1 \varepsilon P$.

$m_1 n_2 + n_1 m_2 \leqslant n_1 n_2 (a + b)$ $\therefore m_1/n_1 + m_2/n_2 \varepsilon S_{a+b}$.

But $f(a + b) = \sup S_{a+b}$, so $m_1/n_1 + m_2/n_2 \varepsilon \sup S_{a+b}$.

$m_1/n_1 \leqslant \sup S_{a+b} - m_2/n_2$ is true for all $m_1/n_1 \varepsilon S_a$,

$\therefore \sup S_a \leqslant \sup S_{a+b} - m_2/n_2$.

$m_2/n_2 \in \sup S_{a+b} - \sup S_a$ is true for all $m_2/n_2 \in S_b$, $\sup S_b \leqslant \sup S_{a+b} - \sup S_a$. Hence $\sup S_a + \sup S_b \leqslant \sup S_{a+b}$, i.e., $f(a) + f(b) \leqslant f(a+b)$.

On the other hand, a repetition of the argument just given shows, that $f(a) + f(b) \geqslant f(a + b)$ since $f(a + b) = \inf S_{a+b}'$. So $f(a) + f(b) = f(a + b)$.

By a similar argument we can show that $f(a)f(b) = f(ab)$.

We now extend the mapping f to all of F by defining

$f(0) = 0$ and $f(-a) = -f(a)$ if $a \in P$.

f is a homomorphism. If $a \in P$, $-b \in P$, then $f(a + b) = f(a - (-b)) = f(a) - f(-b) = f(a) + f(b)$ and $f(ab) = -f(-ab) = -f(a)f(-b) = f(a)f(b)$.

If $-a \in P$, $-b \in P$; $f(ab) = f(-a)f(-b) = f(a)f(b)$.

The other cases are similar.

We note that $f(1) \neq 0$, so f is not the zero map. R is a field, so f is an isomorphism. Since positive elements are mapped into positive elements by f, f is an order isomorphism of F into R. Also we observed that f maps any rational number m to m. We claim that f is unique. Suppose not; there exists an order isomorphism g from F into R such that $f(a) \neq g(a)$ for some a in R. Then either $f(a) < g(a)$, or $f(a) > g(a)$. If $f(a) < g(a)$, then there exists a rational t such that $f(a) < t < g(a)$. Then $a < f^{-1}(t) = t$ and $a > g^{-1}(t) = t$, a contradiction.

<u>Corollary 4.7</u>. R, the field of real numbers, is

order closed.

Proof: Let $\bar{R}$ be the order closure of R. Since R is Archimedean ordered, $\bar{R}$ is also Archimedean ordered by Corollary 4.3. Hence there exists a unique order isomorphism f from $\bar{R}$ into R. $f|_R$ is an order isomorphism. But there is only one; and clearly the identity map on R is an order isomorphism, so $f|_R = I_R$. Hence $f = I_R$.

Therefore we can identify R as an order closed field. $\sqrt{-1} \notin R$ and $R(\sqrt{-1})$ is algebraically closed by Theorem 1.21. This is known as

FUNDAMENTAL THEOREM OF ALGEBRA: Every algebraic equation $f(x) = 0$ with coefficients in the field of complex numbers has a root in this field.

REFERENCES

[1] W. Burnside, Theory of Equations, Hodges, Figgis, & Co., Dublin, 1892.

[2] D. Dubois, A Note on David Harrison's Theory of Preprimes, University of New Mexico, 1966.

[3] D. Dubois, Second Note on David Harrison's Theory of Preprimes, University of New Mexico, 1966.

[4] D. Dubois, Infinite Primes in Commutative Fields, I, University of New Mexico, 1966.

[5] N. Jacobson, Lectures in Abstract Algebra, Vol. III, Van Nostrand, New York, 1964.

[6] H. Royden, Real Analysis, Macmillan, New York, 1966.

[7] B. van der Waerden, Modern Algebra, Ungar, New York, 1948.

[8] O. Zariski and P. Samuel, Commutative Algebra, Vol. II, Van Nostrand, New York, 1960.