GRADUATE SEMINAR REPORT

ON

HILBERT'S 17th PROBLEM

By

Astatke Gizaw

Mathematics Department

Addis Ababa University



Advisor

Dr. H. Wolter

June 1986

Addis Ababa

CONTENTS

	Page
Acknowledgements	i
Introduction	ii
Assumptions and Notations	iii
Part A	
I. Ordering and Positive Cone of a Field	1
II. Maximally Ordered and Real Closed Fields	3
III. Artin-Schreier Theorem	4
Part B	
IV. Formally Real Fields	8
V. Totally Positive Elements of a Field	10
VI. Artin's Theorem and Hilbert's 17^{th} Problem	12
References	14

ACKNOWLEDGEMENTS

I wish to thank Dr. H. Wolter my instructor and advisor for his constant and useful advice in preparing both parts of this seminar report. I would also like to thank W/O Azeb Belay for typing the manuscript carefully.

INTRODUCTION

This is a report of two seminars which I presented on 28, Feb. 1986 and 16 June 1986 to the department of Mathematics.

The report consists of two parts - Part A and B. In Part A a theorem due to Artin and Schreier characterizing real closed fields is proved. Artin and Schreier developed the theory of formally real fields in an attempt to solve Hilbert's 17^{th} problem which was forwarded by D. Hilbert to the Paris Congress of Mathematicians in 1900.

In 1927 Artin proved a stronger result than that demanded by Hilbert. In Part B a solution to Hilbert's problem is given via a theorem due to Artin.

Assumptions and Notations

The Fundamental Theorem of Galois Theory and Sylow's Theorem are assumed in this report and the following notations are adopted throughout.

N	The set of natural numbers.
Q	The field of rational numbers
R	The field of real numbers
F	Any field
F^2	The set of squares of elements in F
$S(F)$	Finite sums of squares of elements in F.
$[E:F]$	The degree of extension of the field E over the field F
$F(x_1,\ldots x_n)$	The field of rational expressions in n indeterminates over F
$F[x_1,\ldots,x_n]$	The ring of polynomials in n indeterminates over F
$\rightarrow$	Implies
$\rightarrow\leftarrow$	Contradiction

I - Ordering and Positive Cone of a Field

Definition: An ordering of a field F, $\leq$, is a binary relation satisfying the following: For all a,b and c in F,

i. $a \leq a$

ii. $a \leq b, b \leq c, \longrightarrow a \leq c$

iii. $a \leq b, b \leq a, \longrightarrow a = b$

iv. $a \leq b$ or $b \leq a$

v. $a \leq b \longrightarrow a+c \leq b+c$

vi. $0 \leq a, 0 \leq b \longrightarrow 0 \leq ab$

The set $P = \{a \in F : 0 \leq a\}$ is called the positive cone of F with respect to the ordering $\leq$.

Definition: Any subset P of a field F satisfying the following is called a positive cone of F.

i. $P+P \subset P$

ii. $P.P \subset P$

iii. $P \cap -P = \{0\}$

iv. $P \cup -P = F$

Corollary: The relation $a \leq b \longleftrightarrow (b-a) \in P$ defines an ordering on F with P as its positive cone.

Proof: (i) Let $a \in F$. Then $a-a = 0 \in P \longrightarrow a \leq a$ The conditions (ii) - (vi) in the definition of an ordering are similarly verified.

Definition: A field F admitting at least one ordering is called formally real.

Theorem 1: Let F be formally real and P a positive cone of F. Then

(i) $F^2 \subseteq S(F) \subseteq P$ and (ii) $-1 \notin S(F)$

Proof: i) $a \in F^2 \longrightarrow a = b^2$ for some $b \in F$

$\longrightarrow a \in S(F)$

$\longrightarrow F^2 \subseteq S(F)$

$b \in S(F) \longrightarrow b = \sum_{i=1}^{n} a_i^2$, $a_i \in F$, $n \in \mathbb{N}$.

$a_i \in F \longrightarrow a_i \in P$ or $-a_i \in P$

$\longrightarrow a_i^2 = (-a_i)^2 \in P$

$\longrightarrow \sum_{i=1}^{n} a_i^2 \in P \longrightarrow b \in P \longrightarrow S(F) \subseteq P$

Thus $F^2 \subseteq S(F) \subseteq P$

ii) Assume $-1 \in S(F)$. By ii) $-1 \in P$. But then

$(-1)^2 = 1 \in P$. We have $1 \in P$ and $-1 \in P$. $\longrightarrow \longleftarrow$

Thus $-1 \notin S(F)$

Lemma 2: Let P_1 and P_2 be positive cones of F such that $P_1 \subseteq P_2$. Then

$P_1 = P_2$.

Proof: If $a = 0$ in F, $a \in P_1$ and $a \in P_2$.

Let $a \neq 0$ and $a \in P_2 \setminus P_1$. Then $a \in P_2$ and $-a \in P_1$.

$\longrightarrow a \in P_2$ and $-a \in P_2$ since $P_1 \subseteq P_2$

$\longrightarrow a \in P_2$ and $a \in -P_2 \longrightarrow \longleftarrow$ to $P_2 \cap -P_2 = \{0\}$

$\therefore \quad P_1 = P_2$

Theorem 3: If S(F) is a positive cone of F, then F has a unique ordering

Proof: Let P be a positive cone of an arbitrary ordering of F.

By Theorem 1, $S(F) \subseteq P$

By Lemma 2, $S(F) = P$

F has a unique ordering.

Lemma 4: A positive cone P of F can be extended to a positive cone P_1 of F_1 in the following cases:

a. $F_1 = F(\sqrt{a})$ and $aP \subseteq P$ for some $a \in F$.

b. $[F_1 : F]$ is odd

Proof: See Alexander Prestel (no date). Lectures on Formally Real Fields. pp. 18-19.

II - Maximally Ordered and Real Closed Fields

Definition: A field F together with an ordering $\leq$ is called maximally ordered if there is no proper algebraic extension field F_1 of F which admits an ordering $\leq_1$ extending $\leq$.

Proposition 5: Every positive element of a maximally ordered field F is a square and hence F has a unique ordering.

Proof: Let P be a positive cone of F and $a \in P \setminus \{0\}$. $F(\sqrt{a})$ is an algebraic extension of F and $aP \subseteq P$. By Thm. 4(a) P extends to a positive cone of $F(\sqrt{a})$. Since F is maximally ordered we must have $F = F(\sqrt{a})$. $\longrightarrow \sqrt{a} \in F \longrightarrow (\sqrt{a})^2 = a \in F^2 \longrightarrow$ a is a square. The uniqueness follows by Thm. 3 if we show that $S(F) = P$.

By Thm. 1 $F^2 \subseteq S(F) \subseteq P$

Since $P \subseteq F^2$ we have $S(F) = P$

$\longrightarrow$ S(F) is a positive cone and hence by Thm. 3 F has a unique ordering.

Definition: A field F is said to be real closed if F is formally real, but has no formally real proper algebraic extension.

Theorem 6: F is real closed iff F is maximally ordered.

Proof: Let F be real closed. Then F is formally real and has no formally real proper algebraic extension.

—> F has no proper algebraic extension extending the ordering in F.

—> F is maximally ordered.

Conversely, assume F is not real closed.

Suppose F_1 is a proper algebraic extension of F with a positive cone P_1.

Let P be the unique positive cone in F

$a \in P \longrightarrow a \in F^2 \longrightarrow a \in F_1^2 \longrightarrow a \in P_1$

$\longrightarrow P \subseteq P_1$

—> The ordering in F_1 is an extension of that of F

—> F is not maximally ordered. Contradiction!

Thus F must be real closed.

III - Artin-Schreier Theorem

Theorem 7 (Artin-Schreier). The following are equivalent for any field F.

a. F is real closed.

b. F^2 is a positive cone of F and every polynomial of odd degree with coefficients in F has a root in F.

c. $F(\sqrt{-1})$ is algebraically closed and $F \neq F(\sqrt{-1})$

Proof: a —> b: Let F be real closed and P a positive cone of F.

F is real closed —> F is maximally ordered by Thm. 6.

By prop. 5 $P \subseteq F^2$ and by Thm. 1 $F^2 \subseteq P$

—> $F^2 = P$. i.e., F^2 is a positive cone of F.

Suppose that f is a polynomial of odd degree over F. Let a be a root of f and assume that $a \notin F$. Then F(a) is a proper algebraic extension of F and [F(a):F] is odd. Then by lemma 4 F(a) extends the ordering in F.

—> F is not maximally ordered

—> F is not real closed. Contradiction!

Hence every polynomial of odd degree over F has a root in F.

b—> c: The following two claims show that $F(\sqrt{-1})$ is algebraically closed.

Claim 1: Every algebraic element over $F(\sqrt{-1})$ is algebraic over F

Proof: Let α be algebraic over $F(\sqrt{-1})$ of degree n. Then $[F(\sqrt{-1})(\alpha): F(\sqrt{-1})] = n$

—> $[F(\sqrt{-1})(\alpha):F] = [F(\sqrt{-1})(\alpha):F(\sqrt{-1})][F(\sqrt{-1}):F] = 2n$

—> α is algebraic over F.

Claim 2: Every algebraic element over F is in $F(\sqrt{-1})$

Proof: Let f(x) be an irreducible polynomial over F and let E be the splitting field of $f(x).(x^2+1)$ so that E contains $F(\sqrt{-1})$. [E:F] is finite since we adjoin to F a finite number of elements to get E. Since F is oredered, char F = 0 and so F is separable. Thus E is a splitting field of a set of separable polynomials. Then by Characterization Theorem of Galois extensions E is a finite Galois extension of F. Now let G be the Galois group of E over F and let $|G| = 2^m.u$, u odd.

By Syllow's 1st Theorem there is a subgroup G_1 of G such that $[G:G_1] = u$.

By Galois Theory there is an intermediate field L such that $[L:F] = [G:G_1] = u$

We must have u = 1 since F has no proper algebraic extension of odd degree.

Then $|G| = 2^m$. Let G_2 be the subgroup corresponding to $F(\sqrt{-1})$. Then

$[G:G_2] = [F(\sqrt{-1}):F] = 2$

$\longrightarrow |G_2| = 2^{m-1}$. If $\underline{m=1}$, we have $[E:F] = 2$ and $\underline{E = F(\sqrt{-1})}$ since $F(\sqrt{-1}) \subseteq E$.

If $\underline{m>1}$, by Syllow's Theorem, there is a subgroup G_3 of G_2 such that

$[G_2:G_3] = 2$

Again by Galois Theory there is an intermediate field K corresponding to G_3 such that

$[K:F(\sqrt{-1})] = [G_2:G_3] = 2$

$\longrightarrow F(\sqrt{-1})$ has a quadratic extension

Claim: $F(\sqrt{-1})$ has no quadratic extension

w.t.S Every element of $F(\sqrt{-1})$ is a square.

Let $z \in F(\sqrt{-1})$. Then $z = a+b\sqrt{-1}$; $\underline{a,b \in F = F^2 \cup -F^2}$

Let $x = \sqrt{\tfrac{1}{2}(a+\sqrt{a^2+b^2})}$, $y = \sqrt{\tfrac{1}{2}(-a+\sqrt{a^2+b^2})}$

This choice is possible since $\pm a + \sqrt{a^2+b^2} \in F^2$

Otherwise $a+\sqrt{a^2+b^2} < 0 \longrightarrow \sqrt{a^2+b^2} < -a$

$\longrightarrow a^2 + b^2 < a^2 \longrightarrow b^2 < 0$ contradiction!

But then we have $x^2 - y^2 = a$ and $2xy = b$ and $(x+y\sqrt{-1})^2 = a+b\sqrt{-1}$

$\longrightarrow z$ is a square. This shows that $F(\sqrt{-1})$ has no quadratic extension.

Therefore we must have m = 1 and so $E = F(\sqrt{-1})$

$\longrightarrow$ Every algebraic element over F is in $F(\sqrt{-1})$

By claim 1 and claim 2, we have $\underline{F(\sqrt{-1})}$ is $\underline{\text{algebraically closed}}$.

Finally F^2 is a positive cone of F implies $-1 \notin F^2$ and $\sqrt{-1} \notin F$. But $\sqrt{-1} \in F(\sqrt{-1})$ and thus $F \neq F(\sqrt{-1})$

c $\longrightarrow$ a: Since $[F(\sqrt{-1}):F] = 2$ there is no algebraic extension between F and $F(\sqrt{-1})$. Since $F(\sqrt{-1})$ is algebraically closed, it is the only proper algebraic extension of F (upto isomorphism)

Thus it is sufficient to show that F is formally real while $F(\sqrt{-1})$ is not.

Claim: F^2 is a positive cone of F

i. Let $a,b \in F$

$F(\sqrt{-1})$ is algebraically closed $\longrightarrow (a+b\sqrt{-1}) = (c+d\sqrt{-1})^2$ for some $c,d \in F$

$\longrightarrow$ $a = c^2 - d^2$ and $b = 2cd$

$\longrightarrow$ $a^2 + b^2 = (c^2 - d^2)^2 + 4c^2d^2 = (c^2+d^2)^2 \in F^2$

$\longrightarrow$ $F^2 + F^2 \subseteq F^2$

ii. $a^2b^2 = (ab)^2 \in F^2 \longrightarrow F^2 \cdot F^2 \subseteq F^2$

iii. $x \in F^2 \cap -F^2 \longrightarrow x = a^2 = -b^2 \longrightarrow -1 = \left(\frac{a}{b}\right)^2$ if $b \neq 0$

$\longrightarrow \sqrt{-1} \in F$ which is impossible. Then $b=a=0$ and hence $F^2 \cap -F^2 = \{0\}$

iv. $a \in F \setminus (F^2 \cup -F^2) \longrightarrow \pm a \notin F^2 \longrightarrow \sqrt{\pm a} \notin F$

$\longrightarrow \sqrt{\pm a} \in F(\sqrt{-1}) \longrightarrow \sqrt{\pm a} = c+d\sqrt{-1}$; $c,d \in F$

$\longrightarrow \pm a = c^2 - 2cd\sqrt{-1} - d^2 \longrightarrow \sqrt{-1} \in F$ contradiction!

Hence $F = F^2 \cup -F^2$

(i) - (iv) $\longrightarrow F^2$ is a psoitive cone of F

claim: $F(\sqrt{-1})$ is not formally real.

$-1 = (\sqrt{-1})^2 \longrightarrow -1 \in S(F(\sqrt{-1}))$

$\longrightarrow F(\sqrt{-1})$ is not formally real by Thm. 1.

IV - Formally Real Fields

In the first part of this report, we have seen that $P + P \subset P$ where P is a positive cone of a formally real field F. If $\sum_{i=1}^{n} a_i^2 = 0$, $a_i \in F$ we must have $a_i = 0$ $i = 1,\ldots,n$. Otherwise $\sum_{i=1}^{n} a_i^2 = 0 \longrightarrow \sum_{i=1}^{n} \left(\frac{a_i}{a_n}\right)^2 = -1$ contradicting the fact that $P + P \subset P$. Thus the following is an equivalent definition of a formally real field.

Definition: F is formally real if the only relations of the form $\sum_{i=1}^{n} a_i^2 = 0$ in F are those for which every $a_i = 0$

Lemma 8: F is formally real iff $-1 \notin S(F)$

Proof: F is not formally real iff $\exists\, a_i \neq 0$ in F and $n \in N$ such that

$$\sum_{i=1}^{n} a_i^2 = 0$$

$$\longleftrightarrow \sum_{i=1}^{n} \left(\frac{a_i}{a_n}\right)^2 = 0$$

$$\longleftrightarrow \sum_{i=1}^{n-1} \left(\frac{a_i}{a_n}\right)^2 + 1 = 0$$

$$\longleftrightarrow \sum_{i=1}^{n-1} \left(\frac{a_i}{a_n}\right)^2 = -1$$

The Lemma follows by contraposition.

Corollary 10: The transcendental extension $F(x)$ of a formally real field F is formally real.

Proof: Suppose $F(x)$ is not formally real. Then

$$\exists\, f_i \neq 0 \text{ in } F(x) \text{ such that } \sum_{i=1}^{n} f_i^2 = 0$$

$$\longrightarrow \sum_{i=1}^{n} \left(\frac{h_i(x)}{g_i(x)}\right)^2 = 0 \;,\; h_i,\, g_i \neq 0 \text{ in } F[x].$$

$$\longrightarrow \prod_{i\neq 1}^{n} [g_i h_1(x)]^2 + \ldots + \prod_{i\neq n} [g_i h_n(x)]^2 = 0 \qquad (*)$$

Since the ring of polynomials $F[x]$ is closed under addition and multiplication, and $F[x]$ is an integral domain, the expression on the left side of $(*)$ is a nonzero polynomial with coefficients in F. But then $(*)$ implies that x is algebraic over F. Contradiction!

Remark: It easily follows by induction that $F(x_1,\ldots,x_n)$ is formally real whenever F is formally real and $x_1,\ldots,x_n$ are transcendental over F. One also notes that corollary 10 is not true for algebraic extensions. We know that $\sqrt{-1}$ is algebraic ove R, R is formally real, but $R(\sqrt{-1})$ is not formallyrreal.

V - Totally Positive Elements of a Field

Definition: $a \in F$ is said to be totally positive if $a > 0$ in every ordering of F.

Theorem 11: Let $a \in F$, $a \neq 0$ and char $F \neq 2$. Then a is totally positive iff $a \in S(F)$

Proof: Assume $a \notin S(F)$.

Let $\overline{F}$ be an algebraic closure of F and let H be the collection of subfields E of $\overline{F}$ containing F in which a is not a sum of squares. By Lemma 9, H is a collection of formally real fields. Since $F \in H$ $H \neq \emptyset$, and H can be partially ordered by set inclusion. Now every chain (ordered subcollection of H) has an upper bound in H and thus H has a maximal element M by Zorn's Lemma.

Claim 1: M is formally real

Since $M \in H$, $a \notin S(M)$. Then $S(M) \neq M$ and so M is formally real by Lemma 9(III)

Claim 2: -a is a square in M.

Suppose $\sqrt{-a} \notin M$. Then we have $F \subseteq M \subseteq M(\sqrt{-a}) \subseteq \overline{F}$ as $\overline{F}$ is algebraically closed. Since M is maximal in H, $M(\sqrt{-a}) \notin H$.

Thus $a \in S(M(\sqrt{-a}))$

$\longrightarrow$ $a = \Sigma (a_i + b_i\sqrt{-a})^2$, $a_i, b_i \in M$ not all zero.

$\longrightarrow$ $a = \Sigma a_i^2 - a \Sigma b_i^2 + 2\sqrt{-a}\,(\Sigma a_i b_i)$

$\longrightarrow$ $\Sigma a_i b_i = 0$ since $\sqrt{-a} \notin M$.

$\longrightarrow$ $a(1+\Sigma b_i^2) = \Sigma a_i^2$

$\longrightarrow$ $a = (\Sigma a_i^2)(1+\Sigma b_i^2)^{-1}$ since $\Sigma b_i^2 \neq -1$

$\longrightarrow$ $a \in S(M)$ by Lemma 9(i) and (iii).

Contradiction!

Thus $-a = b^2$ for some $b \in M$

$\longrightarrow$ $-a > 0$ in every ordering of M, ($F^2 \subseteq S(F) \subseteq P$)

$\longrightarrow$ $a < 0$ in every ordering of M.

Now the induced ordering in F by M gives an ordering of F in which $a < 0$

$\longrightarrow$ a is not totally positive. Contradiction!

Conversely, $a \neq 0$ and $a \in S(F)$

$\longrightarrow$ $a \neq 0$ and $a \in P$ for any positive cone P of F

$\longrightarrow$ $a > 0$ in every ordering of F

$\longrightarrow$ a is totally positive.

Corollary 12: If F is not formally real, then every element of F is totally positive given char $F \neq 2$.

Proof: F is not formally real $\longrightarrow$ $S(F) = F$ by Lemma 9(iii)

$\longrightarrow$ $a \in S(F)$ for all $a \in F$

$\longrightarrow$ a is totally positive.

VI - Artin's Theorem and Hilbert's 17th Problem

Lemma 13: Let F be a subfield of R and suppose that $F(x_1,\ldots,x_n)$ extends the ordering in F. Then if $f \in F(x_1,\ldots,x_n)$ there exists $(a_1,\ldots,a_n) \in Q^n$ such that $f(a_1,\ldots,a_n)$ and f have the same sign in F and $F(x_1,\ldots,x_n)$ respectively.

Proof: The proof is done by induction on the number n of the x_i. If $n = 0$, $F(x_1,\ldots,x_n) = F$ and $f \in F$ is a constant and the conclusion follows trivially. For a complete proof see Nathan Jacobson (1964). Lectures in Abstract Algebra. Vol. II, 1st edition. D. Van Nostrand Comp. Inc., p. 290.

Theorem 14 (Artin's Theorem): Let F be a uniquely orderd subfield of R and let $f \in F(x_1,\ldots,x_n)$ such that $f(a_1,\ldots,a_n) \geq 0$ for all rational n-tuples $(a_i)_{i=1}^n$ for which f is defined. Then f is a sum of squares in $F(x_1,\ldots,x_n)$.

Proof: Suppose f is not a sum of squares. Then f is not totally positive by Theorem 11.

—> There is an ordering of $F(x_i)$ in which $f < 0$. Since the ordering in F is unique, this ordering in $F(x_i)$ is an extension of the ordering in F. By Lemma 13 there is a rational n-tuple $(a_i)_{i=1}^n$ such that $f(a_i)_{i=1}^n < 0$. Contradiction!

Hilbert's 17th Problem: Let f be a rational function of n variables with rational coefficients such that f is rationally definite in the sense that $f(a_1,\ldots a_n) \geq 0$ for all real n-tuples for which f is defined. Then is f necessarily a sum of squares of rational functions with rational coefficients?

Solution: Since Q is uniquely ordered and $f(a_1,\ldots,a_n) \geq 0$ for every rational n-tuple, the conditions in Artins Theorem are satisfied. Thus f is a sum of squares of rational functions with rational coefficients.

REFERENCES

1. Alexander Prestel - Lectures on Formally real Fields.
2. N.Jacobson - Lectures in Abstract Algebra.
3. R. Kochendorffer - Inroduction to Algebra.
4. S. Lang - Algebra.