Model Theory of Real Closed Fields

Victoria L. Noquez
Carnegie Mellon University

Logic and Computation Senior Thesis
Advisor: Dr. James Cummings

May 2008

Abstract

An important fact in the application of model theory to algebra is the result that quantifier elimination in a theory implies that it is model complete. In particular, quantifier elimination (and thus, model completeness) in the theory of algebraically closed fields has been used to give succinct proofs of such results as Hilbert's Nullstellensatz. This paper is an exposition of the work of Prestel [7], Marker [6] and Dickmann [4] regarding real closed fields such as the real numbers. Using methods of abstract algebra we prove that all ordered fields admit a unique real algebraic closure, and use this to show that the theory of real closed ordered fields admits quantifier elimination, and thus is model complete. From this we may conclude that the theory of real closed fields (without an ordering relation) is model complete. The result provides us with a proof of the Positivstellensatz (a modified version of Hilbert's Nullstellensatz for real closed fields) and a solution to Hilbert's 17^{th} problem.

For Lily

Introduction

The goal of this paper is to show that the theory of real closed fields is model complete and use this to prove results in algebra. I have divided it into three sections: Algebra, Logic, and Applications.

The first and most extensive section which follows Prestel's text [7] contains the algebraic preliminaries required to show the model theoretic results about real closed fields. In particular, we focus on the relationship between ordered fields and real closed fields. We will show that a field admits an ordering if and only if -1 is not the sum of squares, and then that for every ordered field F there exists a unique real closed algebraic extension field whose set of squares contains all of the non-negative elements of F.

Of central importance is the theorem by Artin and Schreier [1] which gives us the following equivalence

1. F is a real closed field.
2. F^2 determines and ordering of F by $c \geq 0 \Leftrightarrow c \in F^2$ and every polynomial of odd degree with coefficients in F has a root in F.
3. $F(\sqrt{-1})$ is algebraically closed and $F \neq F(\sqrt{-1})$.

In the Logic section we begin by noting that in a given language, if for every formula $\phi(\bar{x})$ there exists a quantifier free formula $\psi(\bar{x})$ such that a theory $T \vdash \forall \bar{v}[\phi(\bar{v}) \leftrightarrow \psi(\bar{v})]$ (in other words, T admits quantifier elimination), then that theory T is model complete. Then we provide a test (given by Marker [6]) for quantifier elimination, which tells us that a formula $\phi(\bar{x})$ has a quantifier free equivalent in a theory T if and only if for every $M, N \models T$ which have a common substructure C, $M \models \phi[\bar{a}] \Leftrightarrow N \models \phi[\bar{a}]$ for every $\bar{a} \in C$.

Then we turn our attention to the model theory of real closed fields. We will first consider the theory of real closed fields (T_{RCF}) in the language of rings, $\mathcal{L} = \langle +, \cdot, -, 0, 1 \rangle$ with no ordering relation. We axiomatize T_{RCF} in this language using the second condition in the Artin-Schreier equivalence.

However, we see that T_{RCF} as such does not admit quantifier elimination. We circumvent this problem by considering the theory of real closed ordered fields (T_{ROCF}) in the language of ordered rings, $\mathcal{L}_{OR} = \mathcal{L}_R \cup \{\leq\}$. The theory in this language does admit quantifier elimination, and thus, is model complete. Hence, since models of T_{RCF} are models of T_{ROCF}, we may conclude that T_{RCF} is model complete.

In the applications section we provide two results in algebra whose proofs use the model completeness of the theory of real closed fields. We show a solution to Hilbert's 17^{th} problem, which states that positive semi-definite rational functions over a real closed field can be expressed as the sum of squares of rational functions. We also present Dickmann's proof of the Positivstellensatz [4], a modified version of Hilbert's Nullstellensatz for real closed fields.

0.1 Algebra Background

Throughout this paper I assume some familiarity with abstract algebra. Here I include some terms and facts in algebra that I will assume the reader knows and will use without proof.

Field Theory

I will assume the reader is familiar with the basic definitions and facts in field theory, including fields, fields with characteristic zero, fields of fractions of rings, quotient rings, algebraically closed fields, and the existence of a unique (up to isomorphism) algebraic closure of any field. I will also use rings of polynomials in n variables with coefficients in a field F, denoted by $F[x_1, \ldots, x_n]$.

The following facts in Galois theory and groups are used in the lemmas leading up to and the proof of the Artin-Schreier equivalence, Theorem 21 (Section 1.3). I will use extension fields, algebraic extension fields, minimal polynomials, Galois groups and their fixed fields, Sylow-p subgroups, and the following facts:

1. The Primitive Element Theorem, which states that if K is a separable extension of F such that $[K : F]$ is finite, there exists a single element α such that $K = F(\alpha)$.

2. If g is the minimal polynomial of α over F, then $F(\alpha) \simeq \frac{F[x]}{(g)}$ where (g) is the ideal in $F[x]$ generated by g.

3. If $|G| = 2^k$ for some k, then there exists a chain of normal subgroups $1 = G_0 \lhd G_1 \lhd \ldots \lhd G_k = G$ such that the index of G_i as a subgroup of G_{i+1} is 2 for $0 \leq i \leq k - 1$.

In the section on the uniqueness of real algebraic closures (Section 1.4.2) I will use the following:

1. Symmetric polynomials in the roots of a polynomial can be expressed as polynomials in that polynomial's coefficients.

2. Given a polynomial f with roots $\beta_1, \ldots, \beta_m$, the *Vandermonde Matrix* is
$$\begin{bmatrix} 1 & \beta_1 & \ldots & \beta_1^{m-1} \\ 1 & \beta_2 & \ldots & \beta_2^{m-1} \\ \vdots & & & \vdots \\ 1 & \beta_m & \ldots & \beta_m^{m-1} \end{bmatrix}$$
and its determinant is $\prod_{1 \leq i < j \leq m} (\beta_i - \beta_j)$, which is non-zero if and only if its roots are distinct.

Rings and Ideals

In the section about the Positivstellensatz (Section 3.2) I will use polynomial rings, ideals of polynomial rings, prime ideals, and varieties as well as the following facts:

Let J be a proper ideal of $F[x_1, \ldots, x_n]$ where F is a field.

1. (Hilbert's Basissatz) There are $f_1, \ldots, f_k \in F[x_1, \ldots, x_n]$ such that $J = \langle f_1, \ldots, f_k \rangle = \{r_1 f_1 + \ldots, r_k f_k | r_i \in F[x_1, \ldots, x_n], 1 \leq i \leq k\}$. So to show $g(a_1, \ldots, a_n) = 0$ for every $g \in J$, it is sufficient to show $f_i(a_1, \ldots, a_n) = 0$ for $1 \leq i \leq k$.

2. There are finitely many prime ideals $P_1, \ldots, P_m \subset F[x_1, \ldots, x_n]$ such that $J = \bigcap_{i=1}^{m} P_i$.

3. If P is a non-empty prime ideal of $F[x_1, \ldots, x_n]$, it is maximal since $F[x_1, \ldots, x_n]$ is a principal ideal domain, so $\frac{F[x_1, \ldots, x_n]}{P}$ is a field.

1 Algebra

Before we consider the model theory of real closed fields we must first establish some algebraic facts about real closed fields.

In particular, we begin by showing that a field admits an ordering if and only if -1 cannot be expressed as the sum of square elements of the field, that is to say, it is *formally real*. We define *real closed fields* as formally real fields with no proper formally real algebraic extensions.

Then we show the main theorem of Artin and Schreier regarding real closed fields, which shows two equivalent conditions to real closed, namely

1. $F(\sqrt{-1}) \neq F$ is algebraically closed.
2. F^2 is exactly the non-negative elements of F and every polynomial of odd degree with coefficients in F has a root in F.

Finally we see that every ordered field admits a *real algebraic closure* which is unique up to isomorphism.

I assume the reader is familiar with the basic facts and definitions of field theory. There is a list of theorems and facts used included in the introduction.

Throughout this section, let F denote a field.

1.1 Orderings and Positive Cones

Definition 1. *An* ordering *of a field F is a binary relation $\leq$ which satisfies the following for $a, b, c \in F$:*

1. $a \leq a$ (reflexivity)
2. $a \leq b$, $b \leq c \Rightarrow a \leq c$ (transitivity)
3. $a \leq b$, $b \leq a \Rightarrow a = b$ (antisymmetry)
4. $a \leq b$ or $b \leq a$ (totality)
5. $a \leq b \Rightarrow a + c \leq b + c$
6. $0 \leq a$, $0 \leq b \Rightarrow 0 \leq ab$

Definition 2. *A* positive cone *is a subset $P \subset F$ which satisfies the following for $a, b \in P$:*

1. $a + b \in P$
2. $a \cdot b \in P$
3. $P \cup (-P) = F$
4. $P \cap (-P) = \{0\}$

One should note that "positive cone" is a slightly misleading term, as positive cones also contain zero. A more accurate description would be "non-negative cone".

Proposition 3. *If P is a positive cone, then the binary relation determined by $a \leq b \Leftrightarrow b - a \in P$ is an ordering on F*

Proof. Let $a, b, c \in F$ be given.

1. $0 \in P$ since $0 \in \{0\} = P \cap (-P) \subset P \Rightarrow a - a = 0 \in P \Rightarrow a \leq a$.
2. If $a \leq b$ and $b \leq c$, then $b - a, c - b \in P$. Since P is closed under addition, $b - a + c - b = c - a \in P$, so $a \leq c$.
3. If $a \leq b$ and $b \leq a$, then $a - b \in P$ and $b - a \in P$. Then, since $a - b \in P$, $-(a - b) = b - a \in -P \Rightarrow b - a \in P \cap (-P) = \{0\} \Rightarrow b - a = 0 \Rightarrow a = b$.
4. $a - b \in F = P \cup (-P) \Rightarrow a - b \in P$ or $a - b \in -P \Rightarrow a - b \in P$ or $-(a - b) = b - a \in P \Rightarrow a \leq b$ or $b \leq a$.
5. If $a \leq b$, then $b - a \in P \Rightarrow b - a + 0 \in P$ since $0 \in P$ and P is closed under addition $\Rightarrow b - a + c - c \in P \Rightarrow (b + c) - (a + c) \in P \Rightarrow a + c \leq b + c$.
6. If $0 \leq a$ and $0 \leq b$, then $a, b \in P \Rightarrow ab \in P$ since P is closed under multiplication $\Rightarrow ab - 0 \in P \Rightarrow 0 \leq ab$.

□

Proposition 4. *If $\leq$ is an ordering, $P := \{b - a | a, b \in F, a \leq b\} = \{c | c \geq 0\}$ is a positive cone.*

Proof. 1. Let $(b-a),(d-c) \in P$ be given. Then $a \leq b$ and $c \leq d$, so $a+c \leq b+c$. Since $0 \leq d-c$, we can add $b+c$ to both sides and we get $b+c \leq d-c+b+c = b+d$. Hence, by transitivity, $a+c \leq b+d$, so $b+d-(a+c) = (b-a)+(d-c) \in P$. Thus, P is closed under addition.

2. Suppose $(b-a),(d-c) \in P$. Since $d-c \in P$, $c \leq d$, so $0 \leq d-c$. Thus, since $a \leq b$, $a(d-c) \leq b(d-c)$, which means $b(d-c)-a(d-c) = (b-a)(d-c) \in P$, so P is closed under multiplication.

3. Let $x \in F$ be given. Either $x \leq 0$ or $0 \leq x$, so $x-0 = x \in P$ or $0-x = -x \in P$, so $x \in -P$. Hence, $x \in P \cup (-P)$, so $P \cup (-P) = F$.

4. Let $b-a \in P \cap (-P)$. Then $a \leq b$ and $-(b-a) = a-b \in P$, so $b \leq a$. Thus, $a = b$, so $b-a = 0$. $0 \in P \cup (-P)$ since $0 \in P$ and $-0 = 0 \in -P$, so $P \cap (-P) = \{0\}$.

□

Thus, we see that F has an ordering if and only if F contains a positive cone, so we may define orderability as follows:

Definition 5. *F is* orderable *if there exists $P \subset F$ such that P is a positive cone.*

Since a positive cone P determines a particular ordering of a field F, we may refer to P as the ordering of F (as opposed to the binary relation which P determines). We let $\langle F, P \rangle$ denote a field F with positive cone P.

Though a positive cone determines a particular ordering of F, F may contain multiple positive cones which determine different orderings. In other words, an orderable field is not necessarily uniquely orderable.

Now we consider a slightly weaker condition on subsets of F than being a positive cone.

Definition 6. *A* pre-positive cone *of a field F is $P \subset F$ satisfying the following for $a, b \in P$:*

1. $a+b \in P$
2. $ab \in P$
3. $-1 \notin P$

4. $a^2 \in P$

Claim 7. *Every positive cone is a pre-positive cone.*

Proof. Let P be a positive cone and let $x \in F$ be given. We know that P is closed under addition and multiplication. Then, we know that $1^2 = 1 \in P$, which means that $-1 \in -P$, so $-1 \notin P$ since $P \cap (-P) = \{0\}$. Since $x \in F = P \cup (-P)$, either $x \in P$ or $x \in -P$. If $x \in P$, then since P is closed under multiplication, $xx = x^2 \in P$. If $x \in -P$, then $-x \in P$, so $(-x)(-x) = x^2 \in P$. Thus, for any $x \in F$, $x^2 \in P$. □

We will use the following lemma in our proof of Proposition 9.

Lemma 8. *If P is a pre-positive cone of a field F, then $Px \cap (1+P) = \{cx | c \in P\} \cap \{1+d | d \in P\} = \emptyset$ or $-Px \cap (1+P) = \{-cx | c \in P\} \cap \{1+d | d \in P\} = \emptyset$ for every $x \in F$.*

Proof. Let $x \in F$ be given and suppose $Px \cap (1+P)$ and $-Px \cap (1+P)$ are both non-empty. Then we may choose $c_1, d_1, c_2, d_2 \in P$ such that $xc_1 = 1+d_1$ and $-xc_2 = 1 + d_2$. Multiplying the two equations gives us $-c_1c_2x^2 = 1 + d_1 + d_2 + d_1d_2 \Leftrightarrow -1 = c_1c_2x^2 + d_1 + d_2 + d_1d_2$. Since P is a pre-positive cone, it contains all squares in F and is closed under multiplication and addition, so $c_1c_2x^2 + d_1 + d_2 + d_1d_2 = -1 \in P$, which is a contradiction, since $-1 \notin P$. □

Proposition 9. *For every pre-positive cone P_0 of F, there is a positive cone P of F such that $P_0 \subset P$.*

Proof. By Zorn's lemma, the set of pre-positive cones extending P_0 has some maximal element under inclusion. Let P be such a pre-positive cone. We will show that P is a positive cone.

1. P is closed under addition since it is a pre-positive cone.

2. Similarly, P is closed under multiplication because it is a pre-positive cone.

3. Let $x \in F$ be given. First suppose $Px \cap (1+P) = \emptyset$. Let $P' = P - Px$. Since $0^2 = 0 \in P$, for any $p \in P$, $p + 0 \cdot x = p \in P'$, so $P \subset P'$. Then, we claim that P' is a pre-positive cone: Let $(p_1 - q_1x), (p_2 - q_2x) \in P'$ be given, where $p_1, q_1, p_2, q_2 \in P$.

(a) Since P is a pre-positive cone it is closed under addition, so $(p_1 + p_2), (q_1 + q_2) \in P$, which means that $(p_1 - q_1x) + (p_2 - q_2x) = (p_1 + p_2) - (q_1 + q_2)x \in P - Px = P'$. Thus, P' is closed under addition.

(b) Since P is a pre-positive cone, $x^2 \in P$ for every $x \in F$, so $p_1p_2 + q_1q_2x^2 \in P$, and thus, $(p_1 - q_1x)(p_2 - q_2x) = (p_1p_2 + q_1q_2x^2) - (q_1 + q_2)x \in P - Px = P'$. Thus, P' is closed under multiplication.

(c) Suppose $-1 \in P'$. Then for some $p, q \in P$, $-1 = p - qx \Rightarrow p + 1 = qx \Rightarrow p + 1 \in Px$, but $p + 1 \in (1 + P)$, so $Px \cap (1 + P) \neq \emptyset$. $\Rightarrow\Leftarrow$. Thus, $-1 \notin P$.

(d) Since P is a pre-positive cone, $F^2 \subset P$, and since $P \subset P'$, $F^2 \subset P'$.

Thus, since P' is a pre-positive cone, by the maximality of P, $P = P'$. Then, since $0^2 = 0 \in P$ and $1^2 = 1 \in P$, $0 - 1 \cdot x = -x \in P'$, so $-x \in P$.

Then, if we assume $-Px \cap (1 + P) = \emptyset$, by the same argument we can show that $x \in P$. Hence, by Lemma 8, for every $x \in F$, either $x \in P$ or $-x \in P$, so $P \cup (-P) = F$.

4. Let $a \in F$ be given such that $a \neq 0$. Suppose $a \in P \cap (-P)$. Then, since $a \in -P$, $-a \in P$, so $a, -a \in P$. Since F is a field of characteristic 0 and $a \neq 0$, $\frac{1}{a} \in F$. $F = P \cup (-P)$, so either $\frac{1}{a} \in P$ or $\frac{1}{a} \in -P$. If $\frac{1}{a} \in P$, since P is a pre-positive cone it is closed under multiplication, so $-a(\frac{1}{a}) = -1 \in P$. If $\frac{1}{a} \in -P$, then $-\frac{1}{a} \in P$, so $a(-\frac{1}{a}) = -1 \in P$. In both cases, we arrive at a contradiction. Furthermore, we know that $0 \in P \cap (-P)$ since $0^2 = 0 \in P$, and $-0 = 0 \in (-P)$. Thus, $P \cap (-P) = \{0\}$.

Hence, P is a positive cone. □

So we have a slightly weaker condition than the existence of a positive cone, that of a pre-positive cone, which guarantees orderability.

We will use the following facts about sums of squares in a field in our discussion of formally real fields.

Definition 10. $S_F := \{\sum_{i=1}^{n} a_i^2 | n \in \mathbb{N}, a_i \in F\}$.

Claim 11. *S_F is contained in every pre-positive cone.*

Proof. Let P be a pre-positive cone and $\sum_{i=1}^{n} a_i^2 \in S_F$ be given. Then, we know that for each $1 \leq i \leq n$, $a_i^2 \in F^2 \subset P$, and since P is closed under addition, their sum is in P. □

Claim 12. *S_F is closed under addition and the non-zero elements of S_F are a multiplicative subgroup of $F \setminus \{0\}$.*

Proof. The sum of two sums of squares is clearly a sum of squares, so S_F is closed under addition.

Let $S'_F := S_F \setminus \{0\}$. First of all, $1^2 = 1 \in S'_F$. If $\sum_{i=1}^{n} a_i^2, \sum_{j=1}^{m} b_j^2 \in S'_F$, then their product $(\sum_{i=1}^{n} a_i^2)(\sum_{j=1}^{m} b_j^2) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i^2 b_j^2 = \sum_{i=1}^{n}\sum_{j=1}^{m} (a_i b_j)^2 \in S'_F$. Then, for $\sum_{i=1}^{n} a_i^2$ in S'_F, $\frac{1}{\sum_{i=1}^{n} a_i^2} = \frac{\sum_{i=1}^{n} a_i^2}{(\sum_{i=1}^{n} a_i^2)^2} = \sum_{i=1}^{n} (\frac{a_i}{\sum_{i=1}^{n} a_i^2})^2 \in S'_F$. Hence, S'_F is a multiplicative subgroup of F. □

1.2 Formally Real Fields

We will use formally real fields to define real closed fields in the next section.

Definition 13. *A field is* formally real *if -1 is not the sum of squares.*

Proposition 14. *The following are equivalent:*

(a) F is formally real
(b) F is orderable
(c) $\sum_{i=1}^{n} a_i^2 = 0 \Rightarrow a_i = 0$ for all $1 \leq i \leq n$
(d) $F \neq S_F$

Proof. (a)⇒(c) Let F be formally real and suppose we can choose $a_1, \ldots, a_n$ such that $a_i \neq 0$ (without loss of generality) for every $1 \leq i \leq n$ but $\sum_{i=1}^{n} a_i^2 = 0$. Then $\sum_{i=1}^{n-1} a_i^2 + a_n^2 = 0$, so $\sum_{i=1}^{n-1} a_i^2 = -a_n^2 = (-1)a_n^2$. Then, $-1 = \frac{\sum_{i=1}^{n-1} a_i^2}{a_n^2} = \sum_{i=1}^{n-1} (\frac{a_i}{a_n})^2 \in S_F \Rightarrow\Leftarrow$.
(c) ⇒ (a) If $-1 \in S_F$, then $1^2+(-1) \in S_F$, and $1^2+(-1) = 0$, but $1^2, -1 \neq 0$.
(b) ⇒ (d) Since F is orderable we can choose a positive cone $P \subset F$. Since P is a positive cone, P is also a pre-positive cone, so $S_F \subset P$. Since $1 \in S_F \subset P$, $-1 \in -P$. Then, since $P \cap (-P) = \{0\}$, $-1 \notin P$, which means that $-1 \notin S_F$. Thus, $S_F \neq F$.
(d) ⇒ (a) If $-1 \in S_F$, then for any $a \in F$, $a = \frac{4a}{4} = \frac{a^2+2a+1-(a^2-2a+1)}{4} = (\frac{a+1}{2})^2 + (-1)(\frac{a-1}{2})^2$ which is a sum of squares, so $S_F = F$.
(a) ⇒ (b) If $-1 \notin S_F$, then S_F is a pre-positive cone since S_F is closed under addition and multiplication (by Claim 12), and for every $a \in F$, $a^2 \in S_F$. Thus, we can extend S_F to a positive cone, which orders F.

□

The equivalence of most interest in the following sections is (a)⇔(b).

1.3 Real Closed Fields

Now we are ready to define real closed fields.

Definition 15. *A field F is* real closed *if F is formally real, but has no formally real proper algebraic extension field.*

In a sense, we may think of real closed fields as maximal formally real fields.

We will see two equivalent conditions for a field to be real closed in Theorem 21, but in order to complete its proof we must first show the following lemmas:
Let $\langle F, P \rangle$ be a field with an ordering.

Lemma 16. *(Springer) Let F_1 be an algebraic extension field of F of odd degree and let $a_1, \ldots, a_n \in F$, $a_i \neq 0$ for $1 \leq i \leq n$ be given. If $\sum_{i=1}^{n} a_i x_i^2 = 0$ has a non-trivial solution in F_1, it also has one in F.*

Proof. Since F_1 is a finite degree extension of F, by the primitive element theorem we may choose some α such that $F_1 = F(\alpha)$. Let g be the minimal polynomial of α over F, and let $m \neq 0$ be such that $\deg g = 2m + 1$.

Suppose $\sum_{i=1}^{n} a_i x_i^2 = 0$ has a non-trivial solution in F_1. Then, since $F_1 \simeq \frac{F[x]}{(g)}$ (where (g) is the ideal generated by g in $F[x]$), we can choose $f_1, \ldots, f_n \in F[x]$ with $\deg f_i \leq 2m$ such that $\sum_{i=1}^{n} a_i (f_i(x))^2 = h(x)g(x)$ for some $h \in F[x]$ (note that if the f_i have some common divisor $d \in F[x]$, we may consider $\frac{h}{d} \in F[x]$, so we may assume without loss of generality that they have no common divisors). The degree of $\sum_{i=1}^{n} a_i (f_i(x))^2$ is even and at most $2(2m)$, so since $\deg g$ is odd, the degree of h must be odd and less than or equal to $2(2m) - (2m + 1) = 2m - 1$.

Thus, $h = h_1 h_2$ for some $h_1, h_2 \in F[x]$ where h_1 is irreducible and of odd degree. Adjoin a root β of h_1 to F to obtain $F_2 := F(\beta)$. Then $f_1, \ldots, f_n$ is a non-trivial solution in $\frac{F[x]}{(h_1)}$. Since h_1 is irreducible, it is the minimal polynomial of β over F, so $F_2 \simeq \frac{F[x]}{(h_1)}$, which means there is a non-trivial solution in F_2.

Since $[F_2 : F]$ is odd and strictly less than $[F_1 : F]$, we may continue this process until we have a field F' in which $\sum_{i=1}^{n} a_i x^2$ has a non-trivial solution and $[F' : F] = 1$, so $F' = F$. Hence, there is a non-trivial solution in F. □

The following consequence of Springer's Lemma is presented as Theorem 1.26 by Prestel [7].

Theorem 17. *If P is a positive cone of a field F and $a \in P$, P can be extended to a positive cone P' of F' in the following cases:*

1. $F' = F(\sqrt{a})$

2. $[F' : F]$ *is odd*

Proof. 1. Let $a \in P$ be given and suppose $F' := F(\sqrt{a})$ is not orderable. Then by Proposition 14 we may choose $a_1, \ldots, a_m \in F'$ such that for each $1 \leq i \leq m$, $a_i \neq 0$, and $\sum_{i=1}^{m} a_i^2 = 0$. Then, for each a_i, there are $b_i, c_i \in F$ not both equal to 0 such that $a_i = b_i + c_i\sqrt{a}$, and $a_i^2 = b_i^2 + ac_i^2 + (2b_ic_i)\sqrt{a}$ which gives us

$$\sum_{i=1}^{m} b_i^2 + ac_i^2 + (\sum_{i=1}^{m} 2b_ic_i)\sqrt{a}$$

So we must have both $\sum_{i=1}^{m} b_i^2 + ac_i^2 = 0$ and $\sum_{i=1}^{m} 2b_ic_i = 0$.

Then, since P is closed under addition and multiplication, $S_F \subset P$, and $a \in P$, $ac_i^2 \in P$ and $b_i^2 \in S_F \subset P$ for every $1 \leq i \leq m$. Thus, we have a sum of non-zero elements of P equal to 0. $\Rightarrow\Leftarrow$.

2. Suppose we cannot choose an ordering of F'. Then by Proposition 14 we can choose $a_1, \ldots, a_n \in F'$ such that $a_i \neq 0$ for $1 \leq i \leq n$, but $\sum_{i=1}^{n} a_i^2 = 0$. Then $\sum_{i=1}^{n} x_i^2 = 0$ has a non trivial solution in F', and since $[F' : F]$ is odd, by Lemma 16, there is a non-trivial solution in F. $\Rightarrow\Leftarrow$ □

This theorem will be useful in our discussion of real closed fields, as it provides us with conditions under which we may extend the ordering of a field, and thus, conditions under which a field is not real closed. Alternatively, we will use this to show that roots of odd polynomials and square roots of positive elements of a real closed field F are contained in F.

The following facts about maximal orderings will also be useful in our proof of Theorem 21 and in showing the existence of real algebraic closures of ordered fields.

Definition 18. *A field $\langle F, P\rangle$ is* maximally ordered *if there is no proper algebraic extension field which admits an ordering P' which extends P.*

Theorem 19. *If $\langle F, P\rangle$ is maximally ordered, then every $a \in P$ is a square.*

Proof. Let $\langle F, P\rangle$ be a maximally ordered field and let $a \in P$. By Theorem 17 P extends to an ordering of $F(\sqrt{a})$. By the maximality of P, we must have $F(\sqrt{a}) = F$, so $\sqrt{a} \in F$. Thus, every element of P is a square. □

Corollary 20. *If $\langle F, P\rangle$ is a maximally ordered field, then F^2 is the unique ordering of F.*

Proof. Since every element of P is a square, $P \subset S_F$. Since P is a positive cone, $S_F \subset P$, so $P = S_F$. Suppose P' is an ordering of F, and suppose $P' \neq P$. Then, since $P = S_F \subset P'$, we may choose $a' \in P' \setminus P$, and since $a' \notin S_F$, $a' \neq 0$. Then, $a' \notin S_F$ and S_F is a positive cone, so $-a' \in S_F \subset P'$ $\Rightarrow\Leftarrow$

□

From here on, let i denote $\sqrt{-1}$ and note that for a real closed field F, every element of $F(\sqrt{-1})$ is uniquely of the form $a + bi$ for $a, b \in F$.

Now we have Artin and Schreier's Theorem which gives us two equivalent conditions for a field F to be real closed.

Theorem 21. *(Artin-Schreier) For a field F, the following are equivalent*

1. *F is real closed.*
2. *F^2 is a positive cone of F and every polynomial of odd degree has a root in F.*
3. *$F(\sqrt{-1})$ is algebraically closed and $F \neq F(\sqrt{-1})$.*

Proof. 1 $\Rightarrow$ 2: Suppose F is real closed. Then F is formally real, so it has some ordering P. Suppose H is a proper algebraic extension of F with an ordering extending P. Since H is ordered, it is formally real, but since F is real closed, $H = F$. Hence, $\langle F, P\rangle$ is maximally ordered. By Corollary 20, F^2 is the unique ordering of F, so F^2 is a positive cone.

Let g be a polynomial of odd degree. Then we can choose $h \in F[x]$ such that h is an irreducible factor of g with odd degree. Consider α such that $h(\alpha) = 0$. Then h is the minimal polynomial of α over $F(\alpha)$, so since h is odd, $[F(\alpha) : F]$ is odd. Thus, by Theorem 17, we can extend P to an ordering P' in $F(\alpha)$. But again, since F is real closed, we must have $F(\alpha) = F$. Hence, every odd degree polynomial has a root in F.

2 $\Rightarrow$ *3*: Suppose F^2 is a positive cone of F and every polynomial of odd degree has a root in F. Since $-1 \notin F^2$, $\sqrt{-1} \notin F$, so $F \neq F(\sqrt{-1})$. Let F' be an algebraic extension of $F(\sqrt{-1})$, and let $\mathcal{G}$ be the Galois group of F' over F. Let G be a Sylow-2 subgroup of $\mathcal{G}$ and E be the fixed field of G. Then $[E : F]$ is odd, but since every odd degree polynomial has a root in F, $F = E$. Now consider G_1, the Galois group of F' over $F(\sqrt{-1})$. The order of G_1 must a power of 2 since $[F' : F] = [F' : E][E : F]$, so we may choose a subgroup H of G_1 with index 2. Then, the fixed field F_2 of H is an extension of $F(\sqrt{-1})$ of degree 2, so (since F has characteristic 0) for some $b \in F(\sqrt{-1})$, $F_2 = F(\sqrt{-1})(\sqrt{b})$.

Let $a \in F$ be given. Then, since F^2 is a positive cone of F, $F = F^2 \cup (-F^2)$, so either $a \in F^2$ or $a \in -F^2$. If $a \in F^2$, $\sqrt{a} \in F \subset F(\sqrt{-1})$. If $a \in -F^2$, then $-a \in F^2$, so $\sqrt{-a} \in F$. Thus, $\sqrt{a} = \sqrt{-1 \cdot (-a)} = \sqrt{-1}\sqrt{-a} \in F(\sqrt{-1})$. So every $a \in F$ is in $S_{F(\sqrt{-1})}$.

Then, let $a+bi \in F(\sqrt{-1})$ be given where $a, b \in F$. For $c := \sqrt{\frac{1}{2}(\sqrt{a^2+b^2}+a)}$ and $d := \sqrt{\frac{1}{2}(\sqrt{a^2+b^2}-a)}$, $c, d \in F(\sqrt{-1})$, since $\sqrt{a^2+b^2} \in F$ because $a^2+b^2 \in S_F \subset P = F^2$, and $\frac{1}{2}(\sqrt{a^2+b^2}+a)$ and $\frac{1}{2}(\sqrt{a^2+b^2}-a)$ are both in F. Then,

$2cd = 2\sqrt{\frac{1}{2}(\sqrt{a^2+b^2}+a)}\sqrt{\frac{1}{2}(\sqrt{a^2+b^2}-a)} = 2\sqrt{(\frac{1}{2})^2(a^2+b^2-a^2)} = 2\sqrt{(\frac{1}{2})^2 b^2} = \frac{2b}{2} = b$

and

$c^2 - d^2 = \frac{1}{2}((\sqrt{a^2+b^2}+a) - (\sqrt{a^2+b^2}-a)) = \frac{1}{2}(2a) = a$

Then note that $(c+di)^2 = c^2 - d^2 + 2cdi = a + bi$. Thus, every element of $F(\sqrt{-1})$ is a square.

Hence, there are no proper extensions of $F(\sqrt{-1})$ of degree 2, so $F(\sqrt{-1})$ is algebraically closed.

3 $\Rightarrow$ *1*: Suppose $F(\sqrt{-1})$ is algebraically closed and $F \neq F(\sqrt{-1})$. Let $P_0 = F^2$. We will show that P_0 is a pre-positive cone of F. Clearly the second and fourth conditions of Definition 6 are satisfied by F^2. Since $F \neq F(\sqrt{-1})$, $-1 \notin F^2 = P_0$.

Let $a^2, b^2 \in F^2$ be given. As noted above, every element of $F(\sqrt{-1})$ is a square, so we can choose some $c, d \in F$ such that $a + bi = (c+di)^2 = (c^2 - d^2) + (2cd)i$, so $a = (c^2 - d^2)$ and $b = 2cd$. Then, $a^2 + b^2 = (c^2-d^2)^2 + 4c^2d^2 = c^4 - 2c^2d^2 + d^4 + 4c^2d^2 = c^4 + 2c^2d^2 + d^4 = (c^2+d^2)^2 \in F^2 = P_0$. Hence, P_0

is closed under addition. Thus, P_0 is a pre-positive cone.

By Proposition 9 we may choose a positive cone $P \subset F$ such that $P_0 \subset P$. This means that F is orderable, and thus, is formally real.

Let E be a formally real algebraic extension of F. Then take α such that $E = F(\alpha)$ and let g be the minimal polynomial of α over F. Then, since F is a subfield of $F(\sqrt{-1})$ and $F(\sqrt{-1})$ is algebraically closed, every root of g, and thus, $\alpha \in F(\sqrt{-1})$. Hence, E is a subfield of $F(\sqrt{-1})$. Then, $2 = [F(\sqrt{-1}) : F] = [F(\sqrt{-1}) : E][E : F]$, so if E is a proper extension, then we must have $[F(\sqrt{-1}) : E] = 1$. However, we have seen that $F(\sqrt{-1})$ is not orderable, so if E is formally real, we must have $E = F$. Thus, there are no proper formally real extensions of F, so F is real closed.

□

We will use the second condition in our axiomatization of the theory of real closed fields in the language of fields in the next section, and the third condition in our proof of the existence and uniqueness of real algebraic closures.

We need one more lemma about polynomials in real closed fields before we discuss real algebraic closures.

Lemma 22. *If F is real closed, then for every $f \in F[x]$, f splits into irreducible factors of the type $(x - a)$ or $(x - a)^2 + b^2$ for some $a, b \in F$, $b \neq 0$.*

Proof. Since F is real closed, by Theorem 21, $F(\sqrt{-1})$ is algebraically closed, so f splits into irreducible factors of degree 1 or 2, which means they are of the type $(x - a)$ or $(x^2 + dx + c)$ for some $a, c, d \in F$.

Consider $g := x^2 + dx + c$. Define $a := -\frac{1}{2}d$, then $g = x^2 - 2ax + c = (x - a)^2 + (c - a^2)$. Since F is real closed, by Theorem 21, F^2 is a positive cone, so $c - a^2 = 0$, $c - a^2 \in F^2 \setminus \{0\}$ or $c - a^2 \in -F^2 \setminus \{0\}$.

If $c - a^2 = 0$, then $g = (x - a)^2 = (x - a)(x - a)$, so g reduces into factors of the first type.

If $c - a^2 \in -F^2 \setminus \{0\}$, let $b^2 = -(c - a^2) = a^2 - c$. Then $(x - (a + b))(x - (a - b)) = x^2 - 2ax + a^2 - b^2 = x^2 - 2ax + a^2 - (a^2 - c) = x^2 + dx + c = g$. Hence, g splits into factors of the first type.

If $c - a^2 \in F^2$, let $b^2 = c - a^2$. Then let $\gamma = a + bi$ and $\overline{\gamma} = a - bi$. Note that $\gamma, \overline{\gamma} \notin F$ since $F \neq F(\sqrt{-1})$. Then $(x-\gamma)(x-\overline{\gamma}) = x^2-2ax+a^2-b^2i^2 = x^2-2ax+a^2+b^2 = x^2-2ax+a^2+c-a^2 = x^2+dx+c = g$. Hence, the roots

of g are γ and $\overline{\gamma}$ (since g is of degree 2 it cannot have more than two roots) neither of which are in F, and thus, g is irreducible, and $g = (x-a)^2 + b^2$. □

So, since every polynomial with coefficients from a real closed field F splits into factors of the type $(x-a)$ or $(x-a)^2 + b^2$, $b \neq 0$, its roots are either in F or come in pairs of the form $a+bi$ and $a-bi$ for $a, b \in F$, $b \neq 0$.

Also, since every element of $F(\sqrt{-1})$ is of the form $a+bi$, we may define conjugation for $\gamma \in F(i)$ (as in the complex numbers). If $\gamma = a+bi$ for some $a, b \in F$, then $\overline{\gamma} = a-bi$ is the conjugate of γ.

1.4 Real Algebraic Closures

The existence and uniqueness of real algebraic closures of ordered fields is essential to showing that the theory of real closed ordered fields admits quantifier elimination in the language of ordered rings.

Definition 23. *R is a* real algebraic closure *of an ordered field $\langle F, P\rangle$ if*

1. *R is real closed*
2. *R is algebraic over F*
3. *$P \subset R^2$*

1.4.1 Existence of Real Algebraic Closures

Theorem 24. *Every ordered field admits a real algebraic closure.*

Proof. Let K be some fixed algebraic closure of F and consider the set of pairs $\langle F', P'\rangle$ such that $F \subset F' \subset K$ and P' extends P. By Zorn's lemma, we can choose a maximal (under inclusion) extension field, F' with an ordering P' such that $P \subset P'$. We will show that F' is a real algebraic closure of F.

1. First note that F' is maximally ordered, since any algebraic extension of F' extending P' is also an algebraic extension of F extending P. So, by Corollary 20, $P' = (F')^2$ is the unique ordering of F'.

   Then, let E be a formally real extension of F' and Q be an ordering of E. Then, $P' = (F')^2 \subset E^2 \subset Q$ since Q is a positive cone, and thus, a pre-positive cone by Claim 7. So Q extends P', and thus, P. Hence,

by the maximality of $\langle F', P' \rangle$, $F' = E$, and by the uniqueness of P', $Q = P'$.

Hence, F' has no proper formally real algebraic extensions, and thus, is real closed.

2. F' is algebraic over F by selection.

3. $P' = (F')^2$ and since P' extends P, $P \subset (F')^2$.

Thus, F' is a real algebraic closure of F.

□

1.4.2 Uniqueness of Real Algebraic Closures

Artin and Schreier's proof of the uniqueness of real algebraic closure [1] uses Sturm's Theorem, which is a symbolic procedure to determine the number of real roots of a polynomial. Knebusch [5] gave a new proof using a particular quadratic form over F and the fact that the signature of two equivalent quadratic forms is equal. Becker and Spitzlay [2] showed the connection with this an Sturm's theorem. Here we will present the proof given by Prestel [7], which follows the proof by Becker and Spitzlay.

First we must recall some facts and definitions about quadratic forms. One should note that many of these rely on the fact that we were working in a field with characteristic 0. For a more detailed explanation of quadratic forms, see Chapter 2 in Prestel's book [7].

Definition 25. *A* quadratic form *over a field F is a polynomial of degree two of the form*

$$\rho(x_1, \ldots, x_n) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$$

where $a_{ij} = a_{ji}$.

We call n the dimension. We may think of the quadratic form as an $n \times n$ symmetric matrix with entries a_{ij}. Then we have

$$\rho(x_1, \ldots, x_n) = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \begin{bmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Definition 26. *Two quadratic forms* (a_{ij}) *and* (b_{ij}) *are* equivalent *if there is a* $n \times n$ *invertible matrix* M *such that* $(a_{ij}) = M^T(b_{ij})M$ *(where* M^T *is the transpose of* M*).*

Thus, for any change of variables by some invertible matrix M such that $x = My$ yields an equivalent quadratic form, since $x^T\rho x = (My)^T\rho My = y^T(M^T\rho M)y$.

Lemma 27. *If* $\rho(x_1, \ldots, x_n)$ *is an* n*-dimensional quadratic form with some* $c \neq 0$ *and* $v_1, \ldots, v_n \in F$ *such that* $\rho(v_1, \ldots, v_n) = c$*, then for some* $a_2, \ldots, a_n \in F$*,* ρ *is equivalent to*

$$\begin{bmatrix} c & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{bmatrix}$$

This is analogous to the fact in linear algebra that any real-valued symmetric matrix (such as a quadratic form over the reals) can be diagonalized by a real orthogonal matrix. More explicitly, for every symmetric real matrix A there is an orthogonal real matrix Q such that $D = Q^TAQ$ where D is a diagonal real matrix.

For ease of notation, from now on we will use $\langle a_1, \ldots, a_n\rangle$ to denote the matrix

$$\begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix}$$

Definition 28. *If* ρ *is an* n*-dimensional quadratic form over a field* F *with an ordering* P*, and* $\rho \simeq \langle a_1, \ldots, a_n\rangle$ *for some* $a_i \in F$*,* $1 \leq i \leq n$*, then the* signature *of* ρ *with respect to* p *is*

$sgn_P\rho :=$ *number of* $a_i \in P \setminus \{0\}$ *- number of* $a_i \in (-P) \setminus \{0\}$

Theorem 29. *If* $\langle a_1, \ldots, a_n\rangle \simeq \langle b_1, \ldots, b_n\rangle$*, then their signatures are equal.*

Again, the proof of this is analogous to the proof of the same fact for real valued matrices (see the second chapter of Prestel's book [7]).

Now we can define the quadratic form which we will use in our proof of uniqueness of real algebraic closures.

Let $\langle F, P\rangle$ be an ordered field and $f \in F[x]$ an irreducible non-constant polynomial. Let K be an algebraic closure of F and let $\alpha_1, \ldots, \alpha_n \in K$ be the roots of f. Define

$$\sigma_i := \sum_{r=1}^{n} \alpha_r^i \quad (i \in \mathbb{N})$$

These are symmetric polynomials in the roots of f, and thus can be expressed as rational functions of the coefficients of f. Since $f \in F[x]$, its coefficients are in F, and thus, $\sigma_i \in F$ for every $i \in \mathbb{N}$.

Define

$$\rho_f(x_1, \ldots, x_n) = \sum_{1 \le r,s \le n} \sigma_{r+s-2} x_r x_s$$

Since each $\sigma_{r+s-2} \in F$, and $\sigma_{r+s-2} = \sigma_{s+r-2}$, this is a quadratic form over F.

Theorem 30. *For every real algebraic closure R of $\langle F, P\rangle$ in K,*

$$sgn_P \rho_f = \text{number of } \alpha_i \in R$$

Proof. Let R be a real algebraic closure of $\langle F, P\rangle$ in K. By Lemma 22 we may choose some $\beta_1, \ldots, \beta_m$ and $a_1, b_1, a_2, b_2, \ldots, a_l, b_l$ in F, $b_i \neq 0$ for $1 \le i \le l$ (where $m+2l = n$), such that $f = (x-\beta_1)\ldots(x-\beta_m)((x-a_1)^2+b_1^2)\ldots((x-a_l)^2+b_l^2)$. Thus, the roots of f in R are $\beta_1, \ldots, \beta_m$ and the roots of f in $K \setminus R$ are $a_1 + b_1 i, a_1 - b_1 i, \ldots, a_l + b_l i, a_l - b_l i$ (these are not in R since $R \neq R(i)$). Let $\gamma_j = a_j + b_j i$ and $\overline{\gamma_j} = a_j - b_j i$. Thus, we have

$$\begin{aligned}
\rho_f(x_1, \ldots, x_n) &= \sum_{1 \le r,s \le n} \sigma_{r+s-2} x_r x_s \\
&= \sum_{1 \le r,s,t \le n} \alpha_t^{r-1+s-1} x_r x_s \\
&= \sum_{t=1}^{n} \Big(\sum_{1 \le r,s \le n} \alpha_t^{r-1+s-1} x_r x_s \Big) \\
&= \sum_{t=1}^{n} \Big(\Big(\sum_{1 \le r \le n} \alpha_t^{r-1} x_r \Big) \Big(\sum_{1 \le s \le n} \alpha_t^{s-1} x_s \Big) \Big) \\
&= \sum_{t=1}^{n} \Big(\sum_{r=1}^{n} \alpha_t^{r-1} x_r \Big)^2 \\
&= \sum_{t=1}^{m} \Big(\sum_{r=1}^{n} \beta_t^{r-1} x_r \Big)^2 + \sum_{s=1}^{l} \Big(\Big(\sum_{r=1}^{n} \gamma_s^{r-1} x_r \Big)^2 + \Big(\sum_{r=1}^{n} (\overline{\gamma_s})^{r-1} x_r \Big)^2 \Big)
\end{aligned}$$

$$= \sum_{t=1}^{m}(\sum_{r=1}^{n}\beta_t^{r-1}x_r)^2 + \sum_{s=1}^{l}2[(\sum_{r=1}^{n}(\frac{\gamma_s^{r-1}+\overline{\gamma_s^{r-1}}}{2})x_r)^2 + (\sum_{r=1}^{n}(\frac{\gamma_s^{r-1}-\overline{\gamma_s^{r-1}}}{2})x_r)^2]$$

$$= \sum_{t=1}^{m}y_t^2 + \sum_{s=1}^{l}2(y_{m+2s-1}^2 - y_{m+2s}^2) =: \rho_f'$$

using the substitution

$$y_t = \sum_{r=1}^{n}\beta_t^{r-1}x_r \text{ for } 1 \le t \le m,$$

$$y_{m+2s-1} = \sum_{r=1}^{n}(\frac{\gamma_s^{r-1}+\overline{\gamma_s^{r-1}}}{2})x_r, \text{ and}$$

$$y_{m+2s} = \sum_{r=1}^{n}(\frac{\gamma_s^{r-1}-\overline{\gamma_s^{r-1}}}{2i})x_r \text{ for } 1 \le s \le l.$$

Note that ρ_f' can be represented by the matrix $N := \langle 1, \ldots, 1, 2, \ldots, 2, -2, \ldots, -2\rangle$ with m entries with 1, l entries with 2 and l entries with -2.

Then, let the matrix M be such that for $1 \le k \le m$, $M_{j,k} = \beta_k^{j-1}$, and for $1 \le s \le l$, $M_{j,m+2s-1} = \frac{\gamma_s^{j-1}+\overline{\gamma_s^{j-1}}}{2}$ and $M_{j,m+2s} = \frac{\gamma_s^{j-1}-\overline{\gamma_s^{j-1}}}{2i}$. We see that

$$\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = M \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Let K denote the $n \times n$ matrix with diagonal entries of 1 for the first m rows and for $1 \le s \le l$, $K_{m+2s-1,2s-1} = K_{m+2s,2s-1} = 1$, $K_{m+2s-1,2s} = i$, and $K_{m+2s,2s} = -i$ with 0 everywhere else. In other words, K is the matrix

$$\begin{bmatrix}
1 & & & & & & & \\
& \ddots & & & & & 0 & \\
& & 1 & & & & & \\
& & & 1 & i & & & \\
& & & 1 & -i & & & \\
& & & & & \ddots & & \\
& 0 & & & & & 1 & i \\
& & & & & & 1 & -i
\end{bmatrix}$$

$detK = (-2i)^l$, which is never 0. Then, we see that KM is the Vandermonde matrix of f whose determinant is non-zero since the roots of f are distinct. Thus, $det(KM) \neq 0$ so $det(K)det(M) \neq 0$ which means $det(M) \neq 0$.

Thus, M is invertible.

$x^T(\sigma_{r+s-2})x = y^T N y = (Mx)^T N(Mx) = x^T(M^T NM)x$ so $(\sigma_{r+s-2}) = M^T NM$. Thus, they are equivalent.

Hence, since the ordering of R extends P, the signature of ρ'_f, and thus, of ρ_f with respect to P is $m + l - l = m$.

□

Lemma 31. *Let R_1, R_2 be real algebraic closures of the ordered field $\langle F, P\rangle$ and $\langle F, P\rangle \subset \langle F_1, P_1\rangle \subset \langle R_1, R_1^2\rangle$ such that $[F_1 : F]$ is finite. Then there is an embedding of $\langle F_1, P_1\rangle$ into $\langle R_2, R_2^2\rangle$ which is the identity on F.*

Proof. Without loss of generality let R_1, R_2 be contained in some algebraic closure K of F. Then, since $[F_1 : F]$ is finite we may chose some $\alpha \in R_1$ such that $F(\alpha) = F_1$. Let $f \in F[x]$ be the minimal polynomial of α. By Theorem 30, since R_1 contains at least one root of f, $sgn_P \rho_f \neq 0$. Then, since R_2 is also a real algebraic closure of F, f must also have a root β in R_2 since $sgn_P \rho_f \neq 0$. Thus, there is an embedding which is the identity on F of F_1 into R_2 (in which α is mapped to β).

Let $\sigma_1, \ldots, \sigma_n$ be all such embeddings of F_1 into R_2, and suppose they all do not preserve order. Then we can choose $a_1, \ldots, a_n \in P_1$ such that $\sigma_i(a_i) \notin R_2^2$. Consider $F_2 := F_1(\sqrt{a_1}, \ldots, \sqrt{a_n}) \subset R_1$ since $a_i \in P_1$ for $1 \leq i \leq n$. Since $[F_2 : F] = [F_2 : F_1][F_1 : F]$ is finite, by the same argument as above, there is an embedding σ which is the identity on F of F_2 into R_2.

Then note that $\sigma \restriction_{F_1} = \sigma_i$ for some $1 \leq i \leq n$. But $\sigma_i(a_i) = \sigma(a_i) = \sigma(\sqrt{a_i})^2 \in R_2^2$, which is a contradiction.

Thus, for some $1 \leq i \leq n$, σ_i embeds $\langle F_1, P_1\rangle$ into $\langle R_2, R_2^2\rangle$.

□

Corollary 32. *Suppose σ is an order-isomorphism from $\langle F_1, P_1\rangle$ to $\langle F_2, P_2\rangle$ and R_1, R_2 are real algebraic closures of $\langle F_1, P_1\rangle$ and $\langle F_2, P_2\rangle$ respectively. If there is some $\langle F_1, P_1\rangle \subset \langle F'_1, P'_1\rangle \subset \langle R_1, R_1^2\rangle$ such that $[F'_1 : F_1]$ is finite, then there is an extension of σ to an embedding from $\langle F'_1, P'_1\rangle$ into $\langle R_2, R_2^2\rangle$.*

Theorem 33. *(Artin-Schreier) Any ordered field $\langle F, P\rangle$ has a unique (up to isomorphism) real algebraic closure.*

Proof. We have already shown that a real algebraic closure exists in Theorem 24. Let R_1, R_2 be two real algebraic closures of $\langle F, P\rangle$.

Now consider the set of quintuples $\langle F_1, P_1, F_2, P_2, \sigma\rangle$ where $F \subset F_i \subset R_i$ and $P \subset P_i \subset R_i^2$ for $i = 1, 2$ and σ is an order isomorphism from F_1 to F_2.

Then we may establish a partial ordering $\leq_P$ define by $\langle F_1, P_1, F_2, P_2, \sigma\rangle \leq_P \langle F_1', P_1', F_2', P_2', \sigma'\rangle$ if $F_i \subset F_i'$, $P_i \subset P_i'$ for $i = 1, 2$ and $\sigma' \restriction_{F_1} = \sigma$.

Then by Zorn's lemma we may choose a maximal element with respect to this ordering, $\langle F_1, P_1, F_2, P_2, \sigma\rangle$. Suppose $F_1 \neq R_1$. Then we may choose $\alpha \in R_1 \setminus F_1$, so $F_1(\alpha) \subset R$ is a finite extension of F. Let $P_1' := F_1' \cap R_1^2$. Note that this is in fact a positive cone and since R_1^2 extends P_1, $P_1 \subset F_1' \cap R_1^2$.

From Lemma 31 we may choose σ' which extends σ and is an embedding of F_1' into R_2. Thus, if we let F_2' be the range of σ' (which is a superfield of F_2 since σ' restricted to F_1 is σ, whose range is F_2) and let P_2' denote its corresponding ordering ($\sigma'(a) \leq \sigma'(b)$ in $F_2' \Leftrightarrow a \leq b$ in F_1'), we have $\langle F_1', P_1', F_2', P_2', \sigma'\rangle \geq_P \langle F_1, P_1, F_2, P_2, \sigma\rangle$, which contradicts its maximality.

Hence, F_1 must be equal to R_1.

Using the same argument on $\langle F_2, P_2, F_1, P_1, \sigma^{-1}\rangle$ we see that $F_2 = R_2$.

Thus, we have an order isomorphism from R_1 to R_2.

□

2 Logic

Now that we have established the necessary algebraic preliminaries, we may turn our attention to the model theoretic aspects of real closed fields. We will use the fact that *quantifier elimination* in a theory implies that it is *model complete*.

Our goal here is to show that the theory of real closed fields (T_{RCF}) is model complete. However, without a symbol for ordering, there is no quantifier free formula equivalent to $\exists z(z^2+x=y)$, which defines the ordering for a real closed field. So instead we show quantifier elimination in the theory of real closed ordered fields (T_{ROCF}) in the language of ordered rings.

Then, since models of T_{RCF} are models of T_{RCOF} and there is a formula in $\mathcal{L}_R$ equivalent to the ordering symbol, we may conclude that T_{RCF} is model complete.

2.1 Model Theory Background

I will be begin with a few key definitions and facts in model theory. For further background, see Chang and Keisler's book [3].

We will begin by considering a stronger notion than submodel, that is, *elementary submodel*.

Definition 34. *If M, N are structures in some language $\mathcal{L}$, M is an* elementary submodel *of N, denoted by $M \prec N$, if $M \subset N$ and for every $\phi(\bar{x})$ in the language $\mathcal{L}$ and every $\bar{a} \in M$,*
$M \models \phi[\bar{a}]$ if and only if $N \models \phi[\bar{a}]$.

Equivalently, if M, N are models in some language $\mathcal{L}$, M is an elementary submodel of N if for every $\phi(\overline{x}, \overline{y})$ in the language, if there is $\overline{a} \in |M|$ and $\overline{b} \in |N|$ such that $N \models \phi[\overline{a}, \overline{b}]$, then there is $\overline{b'} \in |M|$ such that $M \models \phi[\overline{a}, \overline{b'}]$.

This shows us that if $M \prec N$ and N contains a witness of some formula, one must also exist in M. Thus, any existentially quantified formula which is modeled by N is also necessarily modeled by M.

Definition 35. *A theory T is* model complete *if for every $M, N \models T$,*
$M \subset N \Rightarrow M \prec N$.

A stronger condition than model completeness is quantifier elimination.

Definition 36. *A theory T admits* quantifier elimination *if for any formula $\phi(v_1, \ldots, v_m)$ in the language of T, there is a quantifier free formula $\psi(v_1, \ldots, v_m)$ in the language such that $T \models \forall \bar{v}[\phi(\bar{v}) \leftrightarrow \psi(\bar{v})]$.*

If a theory admits quantifier elimination, it is necessarily model complete, since quantifier free formulas are preserved under substructure and extension.

The following, presented by Marker as Theorem 1.4 [6], gives us a test for quantifier elimination (and thus, model completeness).

Theorem 37. *Let $\mathcal{L}$ be a language containing at least one constant symbol. Let T be an $\mathcal{L}$-theory and let $\phi(x_1, \ldots, x_m)$ be an $\mathcal{L}$-formula (with free variables $x_1, \ldots, x_m$, m may be 0).*
The following are equivalent:

1. *There is a quantifier free $\mathcal{L}$-formula $\psi(x_1, \ldots, x_m)$ such that*
   $T \vdash \forall \bar{x}(\phi(\bar{x}) \leftrightarrow \psi(\bar{x}))$
2. *If M and N are $\mathcal{L}$-structures such that $M, N \models T$, and C is an $\mathcal{L}$-structure such that $C \subset M$ and $C \subset N$, then $M \models \phi(\bar{a})$ if and only if $N \models \phi(\bar{a})$ for all $\bar{a} \in |C|$.*

Proof.
[*1*$\Rightarrow$ *2*]:
Let $\bar{a} \in |C|$ be given.
$M \models \phi(\bar{a})$
$\Leftrightarrow M \models \psi(\bar{a})$ since $M \models \forall \bar{v}(\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$
$\Leftrightarrow C \models \psi(\bar{a})$ since $C \subset M$ and $\psi(\bar{x})$ is quantifier free
$\Leftrightarrow N \models \psi(\bar{a})$ since $C \subset N$ and $\psi(\bar{x})$ is quantifier free
$\Leftrightarrow N \models \phi(\bar{a})$ since $N \models \forall \bar{v}(\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$

[*2* $\Rightarrow$ *1*]: (by contradiction)
Suppose $\phi(\bar{x})$ is not consistent with T. Then $T \models \neg\phi(\bar{x})$, so if c is a constant in the langauge, $T \models \forall \bar{v}[\phi(\bar{v}) \leftrightarrow c \neq c]$, and hence we have an equivalent quantifier free formula to ϕ. Similarly, if $\neg\phi(\bar{x})$ is not consistent with T, $T \models \phi(\bar{x})$, so $T \models \forall v[\phi(\bar{v}) \leftrightarrow c = c]$. Thus, we may assume that $\phi(\bar{x})$ and $\neg\phi(\bar{x})$ are each consistent with T.
Define $\Gamma(\bar{x}) := \{\psi(\bar{x}) | \psi(\bar{x})$ is quantifier free and $T \vdash \forall \bar{x}(\phi(\bar{x}) \rightarrow \psi(\bar{x}))\}$, the set of quantifier free consequences of $\phi(\bar{x})$.
We will begin by proving a lemma.

Lemma 38. $T \cup \Gamma(\bar{d}) \vdash \phi(\bar{d})$

Proof. (by contradiction)

Suppose not. Then $T \cup \Gamma(\bar{d}) \cup \{\neg\phi(\bar{d})\}$ is consistent, so there exists an $\mathcal{L}$-structure M such that $M \models T \cup \Gamma(\bar{d}) \cup \{\neg\phi(\bar{d})\}$.

Let C be the substructure of M generated by $\bar{d}$. This is the smallest $\mathcal{L}$-structure with $\bar{d}$ in the universe which is closed under the functions and contains the constants of the language. So C is exactly the terms of the language with parameters in $\bar{d}$.

Note that since $C \subset M$, $M \models \Gamma(\bar{d})$, and every formula in $\Gamma(\bar{d})$ is quantifier free, $C \models \Gamma(\bar{d})$.

Let $Diag(C)$ be the set of atomic or negated atomic formulas with parameters in C which are true in C in a language $\mathcal{L}_d$ with constants for each element of $\bar{d}$.

Let $\Sigma = T \cup Diag(C) \cup \{\phi(\bar{d})\}$.

Claim 39. Σ *is consistent.*

> Suppose Σ is not consistent. Since $T \cup Diag(C)$ is consistent, $T \cup Diag(C) \models \neg\phi(\bar{d})$. By compactness, we may choose $\psi_1(\bar{d}), \ldots, \psi_n(\bar{d}) \in Diag(C)$ such that
>
> $$T \models \forall\bar{v}(\bigwedge_{i=1}^{n} \psi_i(\bar{v}) \rightarrow \neg\phi(\bar{v}))$$
>
> which is equivalent to
>
> $$T \models \forall\bar{v}(\phi(\bar{v}) \rightarrow \bigvee_{i=1}^{n} \neg\psi_i(\bar{v}))$$
>
> For each $1 \leq i \leq n$, $\psi_i(\bar{v})$ is atomic or negated atomic, which means that $\psi_i(\bar{v})$ is quantifier free, so $\bigvee_{i=1}^{n} \neg\psi_i(\bar{v}) \in \Gamma$. Thus, $C \models \bigvee_{i=1}^{n} \neg\psi_i(\bar{d})$, which means that for at least one $1 \leq i \leq n$, $C \models \neg\psi_i(\bar{d})$, but $\psi_i(\bar{d}) \in Diag(C)$, so $C \models \psi_i(\bar{d})$. $\Rightarrow\Leftarrow$

Since Σ is consistent, there exists an $\mathcal{L}$-structure N such that $N \models \Sigma$. Since $\phi(\bar{d}) \in \Sigma$, $N \models \phi(\bar{d})$. Since $Diag(C) \subset \Sigma$, every quantifier free formula with parameters from C which is true in C is true in N, so (without loss of generality) $C \subset N$.

By *2.*, since $M \models \neg\phi(\bar{d})$, $\bar{d} \in |C|$ and $C \subset M$, $C \subset N$, we must have $N \models \neg\phi(\bar{d})$. $\Rightarrow\Leftarrow$

□

Since $T \cup \Gamma(\bar{d}) \vdash \phi(\bar{d})$, by compactness there are $\psi_1, \ldots, \psi_n \in \Gamma$ such that $T \vdash \forall\bar{v}(\bigwedge_{i=1}^{n} \psi_i(\bar{v}) \rightarrow \phi(\bar{v}))$.

Thus, $T \models \forall\bar{v}(\bigwedge_{i=1}^{n} \psi_i(\bar{v}) \leftrightarrow \phi(\bar{v}))$ and $\bigwedge_{i=1}^{n} \psi_i(\bar{v})$ is quantifier free.

□

2.2 Model Theory of Real Closed Fields

The language of rings (and fields), $\mathcal{L}_R := \langle +, \cdot, -, 0, 1\rangle$ consists of no relations, two binary operators, $+, \cdot$, one unary operator, $-$, and two constants $0, 1$.

The theory of real closed fields in this language consists of the following axioms:

1. $\forall x \forall y \forall z[x \cdot (y + z) = x \cdot y + x \cdot z]$
2. $\forall x \forall y \forall z[x + (y + z) = (x + y) + z]$
3. $\forall x \forall y \forall z[x \cdot (y \cdot z) = (x \cdot y) \cdot z]$
4. $\forall x \forall y[x + y = y + x]$
5. $\forall x \forall y[x \cdot y = y \cdot x]$
6. $\forall x[x + 0 = x \wedge x + (-x) = 0]$
7. $\forall x[x \cdot 1 = x]$
8. $\forall x[x \neq 0 \rightarrow \exists y(x \cdot y = 1)]$

9. $\forall x \exists y[y \cdot y = x \vee y \cdot y = -x]$

10. $q_n \equiv \forall a_0 \ldots \forall a_n \exists x[a_n \neq 0 \wedge a_0 + \ldots + a_n x^n = 0]$ for odd $n \in \mathbb{N}$

The first eight axioms are true of all fields. 9 and 10 are the conditions in the second part of Theorem 21 in the language of fields.

As it turns out, the theory of real closed fields in this language does not admit quantifier elimination. We will use the following ordering in our proof of this.

If F is an ordered field, the following defines an ordering on $F(x)$ (the field of fractions of $F[x]$):

- For $f, g \in F[x]$ if $f = g$ then $f \leq g$. For $f \neq g \in F[x]$ such that $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ and $g(x) = x^m + b_{m-1}x^{m-1} + \ldots + b_0$, if $n > m$, then $f \geq g$. Otherwise, let $k := \max\{l | a_l \neq b_l\}$. If $a_k > b_k$, then $f \geq g$ and if $a_k < b_k$, then $g \geq f$ (note that since they are not equal, such a k exists).

- Then, for $\frac{p}{q}, \frac{r}{s} \in F(x)$ where $p, q, r, s \in F[x]$, $q, s \neq 0$, $\frac{p}{q} \leq \frac{r}{s}$ if and only if $ps \leq qr$.

With simple calculations one may easily verify that $\leq$ defined as such does indeed satisfy the conditions of Definition 1.

Theorem 40. *The theory of real closed fields does not admit quantifier elimination.*

Proof. Let $\phi(x, y)$ be a formula in $\mathcal{L}_R$ which is true when $x \leq y$, in particular, in real closed fields, this is equivalent to $\exists z[x + z^2 = y]$ since the non-negative elements are exactly the squares.

Let $F := \mathbb{Q}$ and x, y be two transcendental numbers over F such that $x, y \notin F$, $x \notin F(y)$ and $y \notin F(x)$.

Now consider $F(x)$ with the ordering described above, call it $\leq_1$. Thus, we may view this as an ordered field. Then consider $(F(x))(y)$ with the ordering as above. These are rational functions of y with coefficients from $F(x)$. Then, $x, y \in (F(x))(y)$, and as polynomials of y, x has degree 0 and y has degree 1, so $x \leq_1 y$ and $x \neq y$.

Then, by applying the same ordering to $(F(y))(x)$, call it $\leq_2$, $y \leq_2 x$ and $x \neq y$.

Let R_1 be the real algebraic closure of $\langle F(x, y), \leq_1 \rangle$ and R_2 be the real algebraic closure of $\langle F(x, y), \leq_2 \rangle$ (which uniquely exist since these are ordered

fields). $R_1, R_2 \models T_{RCF}$ and have a common substructure, $F(x, y)$. But $x, y \in F(x, y)$ and $R_1 \models \phi(x, y) \wedge x \neq y$ while $R_2 \models \phi(y, x)$, which means $R_2 \models \phi(y, x) \vee x = y$, so $R_2 \models \neg(\phi(x, y) \wedge x \neq y)$. Thus, the negation of the second condition in Theorem 37 holds, so there is no quantifier free formula $\psi(x, y)$ in $\mathcal{L}$ for which $T_{RCF} \vdash \forall a, b[\phi(a, b) \leftrightarrow \psi(a, b)]$.

Hence, T_{RCF} does not admit quantifier elimination.

□

Instead, we will consider the theory of real closed ordered fields, T_{ROCF}, in the language of ordered rings, $\mathcal{L}_{OR} = \mathcal{L}_R \cup \{\leq\}$, which does admit quantifier elimination.

Here we present a variation of Marker's proof [6]. We will use $a < b$ as shorthand for $a \leq b \wedge a \neq b$.

Theorem 41. *The theory of real closed ordered fields admits quantifier elimination.*

Proof. Let F_1, F_2 be models of T_{ROCF} and let $(K, \leq)$ be a common substructure of F_1 and F_2. Let K' denote the field of fractions of K. This is an ordered field, and thus, there is a real algebraic closure R of K'. By Theorem 33, R is unique, so we must have $R \subset F_1$ and $R \subset F_2$.

Let $\phi(v, \bar{w})$ be a quantifier free formula in $\mathcal{L}_{OR}$, $\bar{a} \in K$ and $b \in F_1$ and suppose $F_1 \models \phi[b, \bar{a}]$ (so $F_1 \models \exists v \phi(v, \bar{a})$). We want to show that $F_2 \models \exists v \phi(v, \bar{a})$. It will suffice to show that $R \models \exists v \phi(v, \bar{a})$.

Since ϕ is quantifier free, there are polynomials $f_1, \ldots, f_n, g_1, \ldots, g_m \in K[x]$ such that $\phi(v, \bar{a})$ is equivalent to

$$\bigwedge_{i=1}^{n} f_i(v) = 0 \wedge \bigwedge_{i=1}^{m} g_i(v) > 0$$

Then, if f_i is not zero, since $F_1 \models \phi[b, \bar{a}]$, $f_i(b) = 0$, which means that b is algebraic over K, and thus, contained in $R \subset F_2$. Hence, we only need to consider $\phi(v, \bar{a})$ of the form

$$\bigwedge_{i=1}^{m} g_i(v) > 0$$

Since R is real closed, by Lemma 22 we can factor each g_i into a product of factors of the form $(x - a)$ and $(x - a)^2 + b^2$ where $a, b \in R$, $b \neq 0$. Note

that since R^2 is the positive cone of R, $(x-a)^2+b^2 \geq 0$ for all a, b, x, so if $(x-c_{1_i}), \ldots, (x-c_{p_i})$ for some $c_{1_i}, \ldots, c_{p_i} \in R$ are the linear terms of g_i, then in order for $g_i(x) > 0$, an even number of them must be strictly negative and the rest strictly positive. Without loss of generality, suppose $c_{j_i} \leq c_{k_i}$ for $1 \leq j < k \leq p_i$. Then, if p_i is even, their product is positive when $c_{p_i} < x$ or $c_{(p_i-2)_i} < x < c_{(p_i-1)_i}$,..., or $x < c_{1_i}$, or if p_i is odd, when $c_{p_i} < x$, or $c_{(p_i-2)_i} < x < c_{(p_i-1)_i}$,..., or $c_{1_i} < x < c_{2_i}$. Thus, $g_i(x) > 0$ if and only if $\bigvee_{j=1}^{\frac{p_i-1}{2}} [c_{(2j-1)_i} < x \wedge x < c_{(2j)_i}] \vee c_{p_i} < x$ when p_i is odd or $x < c_{1_i} \vee \bigvee_{j=1}^{\frac{p_i-2}{2}} [c_{(2j)_i} < x \wedge x < c_{(2j+1)_i}] \vee c_{p_i} < x$ when p_i is even. Let $\psi_i(x)$ denote this formula for g_i where $1 \leq i \leq m$. Then, in the language $\mathcal{L}_{OR} \cup \{c_{j_i} | 1 \leq i \leq m, 1 \leq j \leq p_i\}$ this is equivalent to the formula

$$\bigwedge_{k=1}^{m} \psi_k(x)$$

Alternatively, we may think of this now as a formula with $m \cdot p_m + 1$ parameters, $\theta(x, c_{1_1}, \ldots, c_{p_m})$ in the language $\mathcal{L}_{OR}$.

Now let $C = \max\{c_{p_i} | 1 \leq i \leq m\} + 1$. Note that $C \in R$, and thus in F_2, and for each $1 \leq i \leq m$, $C > c_{p_i}$ so $\psi_i(C)$ holds. Thus, $R \models \theta(C, c_{1_1}, \ldots, c_{p_m})$, so $R \models \phi[C, \bar{a}]$. Hence, since $R \subset F_2$, and $R \models \exists v \phi(v, \bar{a})$, $F_2 \models \exists v \phi(v, \bar{a})$.

Thus, condition 2 in Theorem 37 is satisfied, so there is a quantifier free formula in $\mathcal{L}_{OR}$, $\phi'(\bar{v})$, such that $T_{ROCF} \vdash \forall \bar{v}[(\exists x \phi(x, \bar{v}) \leftrightarrow \phi'(\bar{v})]$.

Given any formula in the language we may inductively elimination quantifiers to obtain a formula of the form $\exists v \phi(v, \bar{a})$ where $\phi(x, \bar{a})$ is quantifier free. Thus, we see that T_{ROCF} admits quantifier elimination.

□

Corollary 42. *T_{ROCF} is model complete.*

Now, consider $F, K \models T_{RCF}$ such that $F \subset K$. We may view these as $\mathcal{L}_{OR}$ structures since $\mathcal{L}_R \subset \mathcal{L}_{OR}$ and F is still a substructure of K. So by the model completeness of T_{ROCF}, $F \prec K$ in $\mathcal{L}_{OR}$, and since we may replace any instance of $a \leq b$ in an $\mathcal{L}_{OR}$-formula with $\exists z(a + z^2 = b)$ to obtain a $\mathcal{L}_R$-formula, $F \prec K$ in $\mathcal{L}_R$. Hence, T_{RCF} is model complete.

3 Applications

Here we have two applications of the model completeness result for the theory of real closed fields. In each of these we construct an extension field which is real closed and show the claim is true there, then use the model completeness to conclude that the claim is true in the given field.

3.1 Hilbert's 17^{th} Problem

The first application of the model completeness result will be in Robinson's version of Artin's solution to Hilbert's 17^{th} problem, as presented by Marker [6].

The problem is regarding positive semi-definite rational functions, which are defined as follows:

Definition 43. *Let $f(x_1, \ldots, x_n)$ be a rational function over a real closed field R. f is* positive semi-definite *if $f(\bar{a}) \geq 0$ for all $\bar{a} \in R$.*

Theorem 44. *If f is a positive semi-definite rational function over a real closed field R, then f is a sum of squares of rational functions over R.*

Proof. Let $f(x_1, \ldots, x_n)$ be a positive semi-definite rational function which is not a sum of squares of rational functions. Then, we know that for any positive cone P of $R(\bar{x})$, the sums of squares of $R(\bar{x})$ is contained in P. Let K be the real algebraic closure of $\langle R(\bar{x}), P\rangle$. Then since K is real closed, its non-negative elements are exactly the squares, so since $f(\bar{x})$ is not the sum of squares, $K \models \exists \bar{v} f(\bar{v}) < 0$. By model completeness, $R \models \exists \bar{v} f(\bar{v}) < 0$, but this contradicts the fact that f is positive semi-definite.

Hence, if f is a positive semi-definite rational function it can be expressed as as a sum of squares of rational functions.

□

3.2 Positivstellensatz

The following is a modified version of Hilbert's Nullstellensatz for real closed fields. We will present the proof given by Dickmann [4]

We will begin with a few definitions and lemmas. Let R denote a real closed field.

Definition 45. *If J is an ideal in $R[x_1, \ldots, x_n]$, $V(J) := \{\bar{a} \in R | \forall f \in J, f(\bar{a}) = 0\}$ is the* variety *generated by J.*

Definition 46. *If V is a set of points in R^n, $I(V) := \{f \in R[x_1, \ldots, x_n] | \forall v \in V, f(\bar{v}) = 0\}$ is the* ideal generated by V.

Definition 47. *If J is an ideal in $R[x_1, \ldots, x_n]$ J is* real over R *if for every $\sum_{i=1}^{m} p_i f_i^2 \in J$ with $f_i \in R[x_1, \ldots, x_n]$ and $p_i \in R^2 \setminus \{0\}$, then $f_1, \ldots, f_n \in J$.*

Lemma 48. *If J is a proper ideal of $R[x_1, \ldots, x_n]$, then J is real over R if and only if J is radical and is the intersection of finitely many prime ideals which are real over R.*

Lemma 49. *For $S \subset F^n$, $I(S) \subset R[x_1, \ldots, x_n]$ is real over R.*

Theorem 50. *Let R be a real closed field and let J be an ideal in $R[x_1, \ldots, x_n]$. $J = I(V(J))$ if and only if J is real over R.*

Proof. First note that if $J = R[x_1, \ldots, x_n]$, $I(V(J)) = I(\emptyset) = R[x_1, \ldots, x_n] = J$ and J is real over R. Also, if $J = \emptyset$, $I(V(J)) = I(F^n) = \emptyset = J$ and J is real over R.

Assume now that J is a proper ideal of $R[x_1, \ldots, x_n]$.

$\Rightarrow$: Clearly $J \subset I(V(J))$, so we only need to prove the reverse inclusion, $I(V(J)) \subset J$. Let $g_1, \ldots, g_m \in R[x_1, \ldots, x_n]$ be given such that $\langle g_1, \ldots, g_m \rangle = J$. So, if $f \in J$ then

$$R \models \forall \bar{v} [\bigwedge_{j=1}^{m} g_j(\bar{v}) = 0 \rightarrow f(\bar{v}) = 0]$$

Let $f \in I(V(J))$ be given. We need to show that $f \in J$.

By Lemma 48 we can find prime ideals $P_1, \ldots, P_l$ which are real over R such that $J = \bigcap_{j=1}^{l} P_j$. Then, $f \in J$ if and only if $f \in P_j$ for each $1 \leq j \leq l$, which by model completeness is true when

$$R[x_1, \ldots, x_n]/P_j \models f(x_1/P_j, \ldots, x_n/P_j) = 0$$

Since for every P_j, $R[x_1, \ldots, x_n]/P_j$ is a field (since P_j is prime, and thus, maximal since F is a field) and has an ordering extending that of R, there

is a real algebraic closure, call it L_j, of each of these. In particular, $R \subset L_j$ for each $1 \leq j \leq m$.

Then, since $g_1, \ldots, g_m \in J$,

$$L_j \models \bigwedge_{k=1}^{m} g_k(x_1/P_j, \ldots, x_n/P_j) = 0$$

Since $R \subset L_j$, $L_j \models \forall \bar{v}[\bigwedge_{j=1}^{m} g_j(\bar{v}) = 0 \rightarrow f(\bar{v}) = 0]$, so if we let $\bar{v} = \langle x_1/P_j, \ldots, x_n/P_j \rangle$ we can conclude

$$L_j \models f(x_1/P_j, \ldots, x_n/P_j) = 0$$

Thus, $f \in P_j$. Hence, since this is true for each $1 \leq j \leq l$, f is in their intersection, so $f \in J$.

$\Leftarrow$: Let $S = V(J)$ and apply Lemma 49.

□

References

[1] Emil Artin and Otto Schreier, *Algebraische Konstruktion reeller Körper*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 85–99.

[2] Eberhard Becker and Karl-Josef Spitzlay, *Zum Satz von Artin-Schreier über die Eindeutigkeit des reellen Abschlusses eines angeordneten Körpers*, Comment. Math. Helv. **50** (1975), 81–87. MR MR0366882 (51 #3128)

[3] C. C. Chang and H. J. Keisler, *Model theory*, third ed., Studies in Logic and the Foundations of Mathematics, vol. 73, North-Holland Publishing Co., Amsterdam, 1990. MR MR1059055 (91c:03026)

[4] M. A. Dickmann, *Applications of model theory to real algebraic geometry. A survey*, Methods in mathematical logic (Caracas, 1983), Lecture Notes in Math., vol. 1130, Springer, Berlin, 1985, pp. 76–150. MR MR799038 (87e:14025)

[5] Manfred Knebusch, *On the uniqueness of real closures and the existence of real places*, Comment. Math. Helv. **47** (1972), 260–269. MR MR0316430 (47 #4977)

[6] David Marker, Margit Messmer, and Anand Pillay, *Model theory of fields*, second ed., Lecture Notes in Logic, vol. 5, Association for Symbolic Logic, La Jolla, CA, 2006. MR MR2215060 (2006k:03063)

[7] Alexander Prestel, *Lectures on formally real fields*, Lecture Notes in Mathematics, vol. 1093, Springer-Verlag, Berlin, 1984. MR MR769847 (86h:12013)