# Model Theory of Real Closed Fields
# Louise Hay Logic Seminar, UIC

Victoria Noquez

September 20, 2012

## Abstract

We will discuss the algebra of ordered fields, and use this to show that the theory of real closed fields admits quantifier elimination, and thus, is model complete in the language of ordered rings.

From this, we prove that the theory of real closed fields is o-minimal, and give proofs of Hilbert's 17th problem and the Real Nullstellensatz.

## 1 Overview of Real Algebra

We begin by discussing the algebra of ordered fields.

**Definition 1.** A field $F$ is *orderable* if there is a linear order $<$ such that $x < y \Leftrightarrow x+z < y+z$ and $x < y \wedge z > 0 \Rightarrow zx < yz$ for all $x, y, z \in F$.

**Definition 2.** A field is *formally real* if $-1 \notin \Sigma F^2$. $\Sigma F^2 = \{a_1^2 + \ldots + a_n^2 | n \in \mathbb{N}, a_i \in F$ for $1 \leq i \leq n\}$, the sums of squares in $F$.

**Theorem 1.** *$F$ is formally real if and only if $F$ is orderable.*

**Lemma 2.** *A field $F$ is formally real if and only if for all $m \in \mathbb{N}$ and $a_1, \ldots, a_m \in F$, $\sum_{i=1}^{m} a_i^2 = 0 \Rightarrow a_i = 0 \; \forall 1 \leq i \leq m$.*

*Proof.* $\Leftarrow$: If $m = 1$, then $a_1^2 = 0 \Rightarrow a_1 = 0$. Otherwise, suppose there is $i$ such that $a_i^2 \neq 0$. Then $\sum_{1 \leq j \leq m, j \neq i} (\frac{a_j}{a_i})^2 = -1$. $\Rightarrow\Leftarrow$

$\Rightarrow$: Suppose $\sum_{i=1}^{m} a_i^2 = -1$ for some $a_1 \ldots a_m \in F$. Then $\sum_{i=1}^{m} a_i^2 + 1 = 0 \Rightarrow 1 = 0$. $\Rightarrow\Leftarrow$

So $F$ is formally real.

□

**Lemma 3.** *If $F$ is formally real and $a \in F$ with $-a \notin \Sigma F^2$, then there is an ordering $<$ of $F$ in which $a > 0$.*

*Proof.* Note that if $x \in \sum F^2$, then $x \geq 0$ in any ordering of $F$.

Also note that if $-a$ is not a sum of squares, $a \neq 0$.

If $\sqrt{a} \in F$, then $a \in F^2 \subset \sum F^2$, so in any ordering, $a > 0$.

We will show that $F(\sqrt{a})$ is formally real. Then, since in this field $a$ is a square, any ordering will be such that $a > 0$, so we get the desired ordering of $F$ by restricting this ordering to $F$.

Suppose $-1 = \sum(b_i + c_i\sqrt{a})^2$, that is, $-1$ is a sum of squares in $F(\sqrt{a})$. Then $0 = \sum b_i^2 + 1 + \sum c_i^2 a + \sqrt{a}\sum 2b_i c_i$. So since $1, \sqrt{a}$ are a basis of $F(\sqrt{a})$, we must have $\sum b_i^2 + 1 + \sum c_i^2 a = 0$ and $\sum 2b_i c_i = 0$. In particular, $-a = \frac{\sum b_i^2 + 1}{\sum c_i^2} = \frac{\sum b_i^2 \sum c_i^2}{(\sum c_i^2)^2} + \frac{\sum c_i^2}{(\sum c_i^2)^2}$ which is the sum of squares $\Rightarrow\Leftarrow$.

Thus, $F(\sqrt{a})$ is formally real, as required.

□

**Definition 3.** A formally real field is *real closed* if it has no proper formally real algebraic extensions.

**Proposition 4.** *For a formally real field $F$, TFAE*

*(1) $F$ is real closed.*

*(2) $F(i)$ is algebraically closed, where $i = \sqrt{-1}$.*

*(3) For all $a \in F$, one of $\pm a$ is a square and every polynomial of odd degree has a root.*

The third condition is nice because it can be expressed by first order sentences, so we'll use it when we axiomatize RCF (the theory of real closed fields). An ordered field $(F, <)$ is real closed if and only if for all $p(x) \in F[x]$, $a < b$, $p(a) < 0 < p(b) \Rightarrow \exists c$ such that $a < c < b \wedge p(c) = 0$.

**Definition 4.** If $F$ is formally real, $R \supset F$ is a *real closure* if $R$ is a real closed algebraic extension of $F$.

In general, we can extend orderings in different ways. Considered $\mathbb{Q}(x) \subset \mathbb{Q}(\sqrt{x}) \subset R_1$ and $\mathbb{Q}(x) \subset \mathbb{Q}(\sqrt{-x}) \subset R_2$ where $R_1, R_2$ are the respective real algebraic closures. In $R_1$, $x = (\sqrt{x})^2 > 0$ and in $R_2$, $-x = (\sqrt{-x})^2 > 0$, and $\forall a \in F \exists z \in F(z^2 = a \vee z^2 = -a)$.

**Theorem 5.** *If $(F, <)$ is an ordered field*

*(1) There is a real closure, $R$, with $(F, <) \subset (R, <)$.*

*(2) Any two such real closures are isomorphic.*

# 2 Quantifier Elimination in $RCF$

**Definition 5.** A theory $T$ admits *quantifier elimination* if for every formula $\phi$ there is a quantifier free formula $\psi$ such that $T \vDash \phi \leftrightarrow \psi$.

Let $\mathcal{L}$ denote the language of rings, $\{+, \cdot, 0, 1, -\}$. As it turns out, $RCF$ does not admit quantifier elimination in $\mathcal{L}$. Suppose it did, and let $\phi(x, y)$ be a quantifier free formula equivalent to $\exists z(z \neq 0 \wedge y - x = z^2)$. That is, $\phi(x, y) \leftrightarrow x < y$.

Consider $R \vDash RCF$, and $x, y$ algebraically independent over $R$. We will see below in Lemma **??** that $R(x, y)$ is formally real. Since $x - y$ and $y - x$ are not sums of squares (or else we would have a non-zero polynomial in $x, y$ which is equal to 0, contradicting that $x$ and $y$ are algebraically independent), we can order $R(x, y)$ in two ways, $<_1$ and $<_2$ such that $x <_1 y$ and $y <_2 x$. Then, if we consider $K_1 \supset (R(x, y), <_1)$ and $K_2 \supset (R(x, y), <_2)$ the real algebraic closures extending these orderings, we get $K_1 \vDash \forall a, b \phi(a, b) \leftrightarrow a <_1 b$ and $K_2 \vDash \forall a, b \phi(a, b) \leftrightarrow a <_2 b$. In particular, $K_1 \vDash \phi(x, y)$ and $K_2 \vDash \phi(y, x)$, so $K_2 \vDash \neg\phi(x, y)$.

Now consider $K_1, K_2$ as $\mathcal{L}$ structures. So, since $\phi$ is in $\mathcal{L}$, we still have $K_1 \vDash \phi(x, y)$ and $K_2 \vDash \neg\phi(x, y)$. But since $R(x, y) \subset K_1, K_2$, $\phi$ is quantifier free, and $x, y \in R(x, y)$, we get $R(x, y) \vDash \phi(x, y)$ and $R(x, y) \vDash \neg\phi(x, y)$. $\Rightarrow\Leftarrow$.

To avoid this, we expand the language to $\mathcal{L}_{or} = \mathcal{L} \cup \{<\}$, the language of ordered rings. Since the relation $<$ is definable in real closed fields (via $\exists z \neq 0(y - x = z^2)$), by adding $<$ to the language, we still have the same definable sets.

We will use the following test for quantifier elimination.

**Theorem 6.** *Let $T$ be an $\mathcal{L}$-theory. Suppose that for all quantifier free formulas $\phi(\overline{v}, w)$, if $\mathcal{M}, \mathcal{N} \vDash T$, $\mathcal{A}$ is a common substructure of $\mathcal{M}$ and $\mathcal{N}$, $\overline{a} \in A$, and there is $b \in M$ such that $\mathcal{M} \vDash \phi(\overline{a}, b)$, then there is $c \in N$ such that $\mathcal{N} \vDash \phi(\overline{a}, c)$. Then, $T$ has quantifier elimination.*

**Theorem 7.** *$RCF$ admits quantifier elimination in $\mathcal{L}_{or}$.*

*Proof.* Begin with $K, L \vDash RCF$ and $A \subset K, L$ a common substructure. Then $A$ is an ordered integral domain. Extend the ordering of $A$ to its fraction field $F_0 \subset K \cap L$, and let $F$ be the real algebraic closure of $F_0$. By the uniqueness of $F$ (Theorem 5), we may wlog assume $F \subset K \cap L$. So it will suffice to show that if $\phi(v, \overline{w})$ is a quantifier free formula, $\overline{a} \in F$, $b \in K$, $K \vDash \phi(b, \overline{a})$, then there is $b' \in F$, and thus, $K$, such that $F \vDash \phi(b', \overline{a})$ (so $K \vDash \phi(b', \overline{a})$).

Note that for a polynomial $p(x) \in F[x]$, $p(x) \neq 0 \leftrightarrow (p(x) > 0 \vee -p(x) > 0)$ and $p(x) \not> 0 \leftrightarrow (p(x) = 0 \vee -p(x) > 0)$, so we may replace negative atomic formulas with positive ones.

So there are polynomials $p_1, \ldots, p_m, q_1, \ldots, q_m \in F[x]$ such that $\phi(v, \overline{a})$ is equivalent to a finite disjunction of formulas of the form $\bigwedge_{i=1}^{m} p_i(v) = 0 \wedge q_i(v) > 0$. It will be enough to consider one such disjunct.

If one of the $p_i$'s is not identically 0, then $b$ is algebraic over $F$. Since $F$ has no real proper algebraic extensions, we can't have $b \in K \setminus F$, so we must have $b \in F$, as required. If not, then the disjunct is of the form $\bigwedge_{i=1}^{n} q_i(v) > 0$. Each polynomial $q_i(x)$ has only finitely many zeros, and thus, can only change signs finitely many times. So we can choose $c_i < b < d_i$ such that $q_i$ does not have any 0's on $(c_i, d_i)$. Let $c = max(c_1, \ldots, c_n)$ and $d = \min(d_1, \ldots, d_n)$. Then $c < d$, and $\bigwedge_{i=1}^{n} q_i(x) > 0$ whenever $c < x < d$. Thus, there must be $b' \in F$ such that $F \vDash \phi(b', \overline{a})$.

□

**Corollary 8** (Model Completeness)**.** *If $R_1, R_2 \vDash RCF$ and $R_1 \subset R_2$, then $R_1 \prec R_2$.*

**Definition 6.** For $R \vDash RCF$, $X \subset R^n$ is *semialgebraic* if it is a finite boolean combination of sets of the form $\{\overline{x} \in R^n | f(\overline{x}) = 0\}$ and $\{\overline{x} \in R^n | g(\overline{x}) > 0\}$, $f, g \in R[\overline{x}]$.

The semialgebraic sets are exactly those defined by quantifier free formulas, so by quantifier elimination, these are exactly the definable sets.

**Theorem 9.** *$RCF$ is an o-minimal theory.*

*Proof.* Let $R \vDash RCF$ and $X \subset R$ be definable. Let $\phi(x)$ define $X$. $\phi(x)$ is equivalent to a formula of the form $\phi(x) = \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} p_{ij}(x) = 0 \wedge q_{ij}(x) > 0$. (As before, the negation of $=$ and $<$ can be expressed with $=$ and $<$, so it is enough to consider formulas of this form).

To see that RCF is o-minimal, it will be enough to show that each of these disjuncts is a finite union of points and intervals.

But this is clear, since $p_{ij}$ and $q_{ij}$ have only finitely many zeros, so we can express the set of $x$ on which $q_{ij}$ is positive with finitely many intervals, and there are only finitely places where $p_{ij}(x) = 0$. And an intersection of finitely many finite unions of points and intervals is itself also a finite union of points and intervals.

□

# 3 Consequences of Model Completeness in $RCF$

## 3.1 Hilbert's 17th problem

For this, we will consider a real closed field $R$ and its field of rational functions, $R(\overline{x})$. The problem was originally stated for $\mathbb{R}$, but the result holds for any real closed field.

**Lemma 10.** *$R(\overline{x})$ is formally real.*

*Proof.* Suppose $0 = \sum_{i=1}^{n} (\frac{f_i(\overline{x})}{g_i(\overline{x})})^2$ where $f_i, g_i \in R[\overline{x}]$, $g_i \neq 0$. So if we let $G_i(\overline{x}) = \prod_{1 \leq j \leq n, i \neq j} g_i(\overline{x})$, then $0 = \sum_{i=1}^{n} (G_i(\overline{x}) f_i(\overline{x}))^2$, contradicting that $\overline{x}$ is transcendental over $R$. Thus, we must have $f_i = 0$ for each $1 \leq i \leq n$.

Hence, by Lemma 2, $R(\overline{x})$ is formally real. □

**Theorem 11** (Hilbert's 17$^{\text{th}}$ Problem)**.** *For $R \vDash RCF$, let $f \in R(x_1, \ldots, x_n)$ be such that $\forall \overline{x} f(\overline{x}) \geq 0$. Then there are $g_1(x), \ldots, g_m(x) \in R(\overline{x})$ such that $f = \sum_{i=1}^{m} g_i^2$.*

*Proof.* Suppose not. By Lemma 3, since $f$ is not a sum of squares, there is an ordering of $R(\overline{x})$ in which $f(\overline{x}) < 0$. Let $K$ be the real algebraic closure of $R(\overline{x})$. So since $R \subset R(\overline{x}) \subset K$, by model completeness, since $R, K \vDash RCF$, $R \prec K$. $K \vDash \exists \overline{x} f(\overline{x}) < 0$ (namely, $\overline{x} \in K$ itself). So $R \vDash \exists \overline{x} f(\overline{x}) < 0$ ⇒⇐. □

## 3.2 Real Nullstellensatz

**Theorem 12** (Real Nullstellensatz)**.** *Let $F$ be a real closed field and let $J \subset F[X_1, \ldots, X_n]$ be an ideal. We say that $J$ is* real *if for any $p_1, \ldots, p_m \in F[X_1, \ldots, X_n]$ such that $\sum p_i^2 \in J$, then $p_i \in J$ for $1 \leq i \leq m$. $I(V(J)) = J$ if and only if $J$ is real.*

*Proof.* $\Rightarrow$: If $V(J) = \emptyset$, then $J = I(V(J)) = F[X_1, \ldots, X_n]$, so $J$ is real. Otherwise, let $x \in V(J)$.

Suppose for some $p_1, \ldots, p_m$, $\sum_{i=1}^{m} p_i^2 \in J$. Then $\sum_{i=1}^{m} (p_i(x))^2 = 0$ since $x \in V(J)$, so by Lemma 2, $p_i(x) = 0$ for all $1 \leq i \leq m$ since $F \vDash RCF$. Thus, $p_i \in I(V(J)) = J$.

$\Leftarrow$: We will need a few lemmas for the other direction.

**Lemma 13.** *If $P$ is a real prime ideal of $F[X_1, \ldots, X_n]$, then if $K$ is the field of fractions of $F[X_1, \ldots, X_n]/P$, $K$ is formally real.*

*Proof.* Let $\sum_{i=1}^{m} (\frac{a_i + P}{b_i + P})^2 = P$ where $a_i, b_i \in F[X_1, \ldots, X_n]$, $b_i \notin P$, (so, a sum of squares in $K$ which is equal to 0). Let $c_i = \prod_{1 \leq j \leq m, j \neq i} b_j + P$. Then $\sum_{i=1}^{m} (c_i a_i + P)^2 = P$. So $\sum_{i=1}^{m} (c_i a_i)^2 \in P$, and thus $c_i a_i \in P$ since $P$ is real. We know that $c_i \notin P$, or else we would get some $b_j \in P$ since $P$ is prime. So we must have $a_i \in P$. Thus, $a_i + P = P$, so $\frac{a_i + P}{b_i + P} = P$, that is, 0 in $K$.

Hence, by Lemma 2, $K$ is formally real.

□

**Lemma 14.** *If $J = \bigcap_{i=1}^{m} P_i$ where the $P_i$'s are prime and $J$ is real, then each $P_i$ is real.*

*Proof.* Let $P_1, \ldots, P_m$ be such that $J = \bigcap_{i=1}^{m} P_i$, and no $P_i \subset P_j$ for $i \neq j$. If $m = 1$, then $P_1 = J$ is real. If not, consider $P_i$ and let $c_j \in P_j \setminus P_i$ for all $j \neq i$, $c = \prod_{1 \leq j \leq m, i \neq j} c_j$. Let $\sum_{k=1}^{q} a_k^2 \in P_i$. Then $c^2 \sum_{k=1}^{q} a_k^2 = \sum_{k=1}^{q} (ca_k)^2$. Since, $\sum_{k=1}^{q} a_k^2 \in P_i$, this is in $P_i$, and since $c^2 \in P_j$ for all $j \neq i$, it is in $P_j$. Thus, $\sum_{k=1}^{q} (ca_k)^2 \in \bigcap_{i=1}^{m} P_i = J$. So since $J$ is real, $ca_k \in J$, and thus, $ca_k \in P_i$ for each $1 \leq k \leq q$. So since $P_i$ is prime, $c \in P_i$ or $a_k \in P_i$. But if $c \in P_i$ then $c_j \in P_i$ for some $j \neq i$. Thus, we must have $a_k \in P_i$ for all $1 \leq k \leq q$. Hence, each $P_i$ is real. □

Since $J$ is real, it is radical: let $f \in \sqrt{J}$, and $n$ be such that $f^n \in J$. Let $m$ be such that $m + n = 2^k$ for some $k$. then $f^m f^n \in J$, so $f^{2^k} \in J$. Thus, since $J$ is real, $f \in J$.

So by the primary decomposition theorem, $J = \bigcap_{i=1}^{m} P_i$ for some prime ideals $P_1, \ldots, P_m \in F[X_1, \ldots, X_n]$. And by Lemma 14, each of these are real ideals.

Clearly, $J \subset I(V(J))$, so let $f \in I(V(J))$. To show that $f \in J$, we will show that $f \in P_i$ for each $i$. Since $F$ is a field, $F[X_1, \ldots, X_n]$ is Noetherian, so $P_i = \langle g_1, \ldots, g_k \rangle$. For any $\overline{v}$ , if $g_1(\overline{v}) = \ldots = g_k(\overline{v}) = 0$, then $\overline{v} \in V(J)$. So for such a $\overline{v}$, since $f \in I(V(J))$, $f(\overline{v}) = 0$. Thus, $F \vDash \forall \overline{v}(\bigwedge g_i(\overline{v}) = 0 \rightarrow f(\overline{v}) = 0)$. Let $K$ be the field of fractions of $F[X_1, \ldots, X_n]/P$. $K$ is formally real by Lemma 13, so let $L$ be its real closure. $F \subset L$, so by model completeness, $F \preceq L$, so $L \vDash \forall \overline{v}(\bigwedge g_i(\overline{v}) = 0 \rightarrow f(\overline{v}) = 0)$. $L \vDash \bigwedge g_i(X_1/P_i, \ldots, X_n/P_i) = 0$ since $g_1, \ldots, g_k \in P_i$, so $L \vDash f(X_1/P_i, \ldots, X_n/P_i) = 0$. Thus, $f \in P_i$.

□