Model Theoretic Approach to Nullstellensatz

Derya Çıray

May 2011

Contents

Introduction

At the turn of the 19th to 20th century David Hilbert presented a list of 23 problems that he considered to be the most important problems left from the old century to be solved in the new one. The 17th problem, in simple form, is as follows:

Suppose $f \in R[X_1, \ldots, X_n]$ is a real polynomial and $f(x) \geq 0$ for all $x \in \mathbb{R}^n$. Does there exist a representation of f in the form

$$f = \sum_i r_i^2$$

for finitely many r_i from the field $\mathbb{R}(X_1, \ldots, X_n)$ of rational functions in $X_1, \ldots, X_n$?

In 1926, E.Artin presentNed a solution to the problem. Artin proved a theorem answering the question in positive for all real closed fields. This solution gave rise to develop methods focusing on "reality" and "positivity". In a way we can say that Artin's solution is the beginning of real algebra.

The German term "nullstellensatz" means "theorem of zeros". Both Real Nullstellensatz and Hilbert's Nullstellensatz relate algebraic sets (simply the zeros of sets of polynomials) to ideals. We may consider Real Nullstellensatz as the analogue of Hilbert's Nullstellensatz for real closed fields.

Krivine, in 1964, proved the Real Nullstellensatz but Krivine's paper remained unknown until 1970's. All his results got rediscovered later in 1969 by Dubois and Risler. They reproved the Real Nullstellensatz for $A = R[X]$(polynomial ring over a real closed field). Later using different methods Stengle[1974] and Prestel[1975] also proved Real Nullstellensatz.

The main part of this work is to present a model theoretic proof of the Real Nullstellensatz as an analogue of the model theoretic proof of Hilbert Nullstellensatz.

First chapter contains the theory of real closed fields. First we give definitions of ordered and real fields. Defining a real field to be a field in which -1 cannot

be expressed as a sum of squares, we obtain the result that a real field has at least one ordering. We also give an alternative definition of real fields as follows. A field is real if and only if $\sum_{i=1}^{n} a_i^2 = 0$ implies $a_i = 0$ with $a_i \in R$ for $i = 1, \ldots, n$. After that, we define real closed field as a real field, maximal with respect to the property of reality in an algebraic closure and show that real closed fields have a unique order. Finally we arrive at the following result; every real field embeds into a real closed field, i.e. has a real closure, moreover this real closure is unique up to isomorphism. To prove this result, we use Sturm's Theorem that counts the roots of a polynomial over a real field and the important result that real closed fields have intermediate value property. All the theory developed in chapter 1 is due to Artin-Schreier. We followed [SL] and [PG] for Chapter 1. The results we achieve in Chapter 1 are used in Chapter 3 for proving some properties of real ideals and in the proof of Real Nullstellensatz.

In Chapter 2, we give model theoretic facts which are necessary to give a model theoretic proof of nullstellensatz. As the model theoretic part of the proof of nullstellensatz uses the fact that ACF and RCOF are model complete, after giving basic facts and some theorems about quantifier elimination. We showed, in Chapter 2, that ACF and RCF admit quantifier elimination and from that we conclude that ACF and RCF are model complete.

Last chapter finally consists of a model theoretic proof of Hilbert's Nullstellensatz and Real Nullstellensatz using the same methods as to emphasize the analogy. In the beginning, we give some definitions from algebraic geometry; affine variety and ideal of a variety in order to understand the statements of both Hilbert's and Real Nullstellensatz. Before giving the proof of Hilbert's Nullstellensatz We visited some algebraic facts from field theory. Also before the proof of Real Nullstellensatz we define the notion of real ideal and study some of its properties. Since the real closure of a real field and algebraic closure of a field has analogous properties, we use the same method for both of the proofs. Real ideals for a real field took the place of radical ideals.

The historical comments in the preface are mostly due to Prestel and Delzell [PD].

Chapter 1

Real Fields

Ordered Fields

Definition 1. A field F is called ordered field if it has a order relation $\leq$ such that

(i) $x \leq y$ implies $x + z \leq y + z$ for $z \in F$,

(ii) If $z \geq 0$ and $x \leq y$ then $xz \leq yz$

Proposition 1.1. *In any ordered field, if $x \leq y$ and $z \leq w$ then;*

(a) $x + z \leq z + w$

(b) $xz \leq wy$ *if* $0 \leq x, z$

Proof. (a) We have $x + z \leq y + z$ and $y + z \leq y + w$ by (i). Hence, $x + z \leq y + w$.

(b) Since $0 \leq x, z\ 0 \leq x \leq y$ and $0 \leq z \leq w$. By (ii), we have $xz \leq yz$ and $zy \leq wy$. Hence, $xz \leq wy$.

□

Definition 2. Let F be a field. A subset P of F with thr following properties is called an ordering F.

(i) P is closed under addition and multiplication,

(ii) $F = P \cup -P \cup \{0\}$ is a disjoint union, where $-P = \{-x : x \in P\}$

Proposition 1.2. *A field is ordered if and only if it has an ordering.*

Proof. ($\Longleftarrow$) Let F be a field and let P an ordering of F. Define the relation, $x < y$ if $y - x \in P$ and $x \leq y$ to mean $x < y$ or $x = y$.

Clearly, $\leq$ is an order relation; reflexivity is clear from the definition. If $x \leq y$ and $y \leq x$ this means $x < y$ and $y < x$ or $x = y$.

$x < y$ means $y - x \in P$.

$y < x$ means $x - y \in P$ hence $y - x \in -P$.

Since P and $-P$ are disjoint sets, $x \leq y$ and $y \leq x$ implies $x = y$.

Now, assume $x \leq y$ and $y \leq x$. Trivially, we may say $x \leq z$, if we have any of the equalities $x = y$ or $y = z$. So, assume $x < y$ or $y < z$. $x < y$ means $y - x \in P$ and $y < z$ means $z - y \in P$. Using the fact that P is closed under addition $y - x + z - y = z - x$ is an element of P. Hence $x < z$.

We also need to check (i) and (ii) in the definition of ordered fields, as to check that the ordering is compatible with the field operations. Again the equalities can be ignored.

(i) $x < y$ means $y - x \in P$, so $y + z - (z + x) \in P$ which means $x + y < y + z$.

(ii) If $z > 0$ then $z - 0 = z \in P$. Given $x < y$, that is $y - x \in P$, the fact that P is closed under multiplication implies that $z(y - x) = zy - zx$ is in P. Hence $zx < zy$.

($\Longrightarrow$) Let F be an ordered field. Consider the set $P = \{x \in F : x > 0\}$. Clearly, P is closed under addition and multiplication and F is disjoint union of P and $-P = \{x \in F : x < 0\}$ and $\{0\}$. □

Note that, Proposition 1.2 is reformulation of the definition of ordered fields. The ordering P of an ordered field F, is called the set of positive elements of F and the set $-P$ is called the set of negative elements. We also use the expression "F is ordered by P "for an ordered field F and it's ordering P.

Now, we will continue with some properties of ordered fields.

Proposition 1.3. *An ordered field has characteristic* 0.

Proof. Let F be an ordered by P.

If $1 \in -P$ then $-1 \in P$. So, $-1 \cdot -1 = 1 \in P$ since P is closed under multiplication. This gives a contradiction since P and $-P$ are disjoint.

Also, $1 \neq 0$, hence $1 \in P$. P is closed under addition so, $1 + \ldots + 1 \in P$. Since $0 \notin P$ and $1 + 1 + \ldots + 1 \neq 0$, F has characteristic zero. □

Proposition 1.4. *Let F be an ordered field $x^2 \geq 0$ for all $x \in F$.*

Proof. Let F be a field ordered by P. Let x be any element of F. x is an element of one of the sets P, $-P$ or $\{0\}$. The proof is trivial if $x = 0$ or $x \in P$. Assuming $x \in -P$ we have $-x \in P$, but P is closed under multiplication so, $(-x)(-x) = x^2 \in P$. □

Corollary 1.5. *A sum of squares is positive or* 0 *in ordered fields.*

Proof. Immediate consequence of Proposition 1.4 and the fact that P is closed under addition. □

Proposition 1.6. *Let F be field ordered by P. P is closed under taking inverses.*

Proof. Let P be the ordering of F. Assume $x \in P$ but $x^{-1} \notin P$. Then $x^{-1} \in -P$, so $-x^{-1} \in P$. Since P is closed under multiplication $x \cdot -x^{-1} = -1 \in P$, a contradiction. □

Proposition 1.7. *Let F be ordered by P, $x_1, \ldots, x_n \in F$. If $x_1^2 + x_2^2 + \ldots + x_n^2 = 0$ then $x_i = 0$ for all $i = 1, 2, \ldots, n$*

Proof. Since $x^2 \geq 0$ for all x, $0 \leq x_i^2 \leq x_1^2 + \ldots + x_n^2 = 0$ for all $i = 1, \ldots, n$. So, $x_i^2 = 0$ and hence $x_i = 0$ for all $i = 1, \ldots, n$. □

Proposition 1.8. *A field F can be ordered if -1 cannot be expressed as a sum of squares of the elements of F.*

Proof. Let P be a set of nonzero finite sums of squares of the elements of F. It is clear from the definition of P that P is closed under addition.

As $\left(\sum_i a_i^2\right) \cdot \left(\sum_j b_j^2\right) = \sum_{i,j} (a_i b_j)^2$, P is closed under multiplication. Since for $a \neq 0$ we have $a^{-1} = a \cdot (a^{-1})^2$, P is closed under taking inverses. So by Zorn's

Lemma there is a maximal subset M of F that contains P such that it is maximal with respect to closedness under addition, multiplication and taking inverses.

It follows that $M \cap -M = \emptyset$; otherwise for some $a, b \in M$ we would have $a = -b$ and so $-1 = a \cdot b^{-1} \in M$.

Assume that $a \neq 0, a \notin -M$. If $x, y \in M$ then $x + ay \neq 0$. If $x, y \in M \cup \{0\}$ then $x + ay = 0$ implies $x = y = 0$.

Define the set $T = \{x + ay : x, y \in M \cup \{0\}\} \setminus \{0\}$

So we have, $P \subseteq M \subseteq T$. One can easily check that M is closed under multiolication and taking inverses. Hence $M = T$ by maximality of M. Thus $a \in M$.

Hence F is disjoint union of $M, -M, \{0\}$. □

Real Closed Fields

In this part we will give definitions of real and real closed fields. We will prove that every ordered field has a real closure and the ordering of a real closed field is unique.

Definition 3. A field F is said to be a real field if -1 is not a sum of squares in F.

Using Corollary 1.5 and Proposition 1.8 we can give the definition of a real field as "A field is real if and only if it is orderable ". Important examples of real fields are $\mathbb{R}$ and $\mathbb{Q}$ which have unique ordering but we have to be careful because in general, a real field has more than one ordering. For example, the field of rational functions, $\mathbb{Q}(X)$ has $2^{\aleph_0}$ orderings [DM1 pg.93].

The following proposition allows us to give an alternative definition for Real fields.

Proposition 1.9. *R is a real field if and only if $\sum_{i=1}^{n} a_i^2 = 0$ implies $a_i = 0$ for $a_i \in R, i = 1, \ldots, n$.*

Proof. ($\Longrightarrow$) Follows from Proposition 1.8 and Proposition 1.7.
($\Longleftarrow$) Let $-1 = \sum_{i=1}^{n} (a_i)^2, a_i \in R, i = 1, \ldots, n$ then $0 = -1 + 1 = \sum_{i=1}^{n} (a_i)^2 + 1^2$ and by assumption we have $0 = 1$, a contradiction. □

Proposition 1.10. *Let F be a real field, $\alpha \notin F$ and $K = F(\alpha)$ be a simple extension of F. If α^2 is a sum of squares in F then K is real.*

Proof. Assume that K is not real, then we may write

$$-1 = \sum_{i=1}^{n} (a_i + \alpha b_i)^2$$

where a_i and b_i are in F.

$$-1 + 0\alpha = \sum_{i=1}^{n} a_i^2 + \sum_{i=1}^{n} 2\alpha a_i b_i + \sum_{i=1}^{n} \alpha^2 b_i^2$$

hence

$$-1 = \sum_{i=1}^{n} a_i^2 + \sum_{i=1}^{n} \alpha^2 b_i^2$$

and this contradicts with the definition of real field.

Hence $K = F(\alpha)$ is a real field. □

Corollary 1.11. *If K is real, $a \in K$ then $K(\sqrt{a})$ or $K(\sqrt{-a})$ is real.*

Proof. Follows from Proposition 1.10 because for any ordering P of K either $a \in P$ or $-a \in P$. □

Proposition 1.12. *Let F be a real field. Let f be an irreducible polynomial of odd degree n in $F[X]$. If α is a root of f then $F(\alpha)$ is real.*

Proof. We proceed by induction on n. If n = 1, this is clear. Let $f(X)$ be an irreducable polynomial of $F[X]$ with degree $n>1$ and has a root α. Assume$F(\alpha)$ is not a real field, then -1 is expressed as a sum of squares in $F(\alpha)$. Elements of $F(\alpha)$ can be expressed as $g(\alpha)$ where $g \in F[X]$ and degree of g is less then degree of f. Now, we may write;

$-1 = \sum_{i=1}^{m} (g_i(\alpha))^2$ for some $g_i \in F[X]$ for $i = 1, 2, \ldots, m$. Then there exists a polynomial h in $F[X]$ such that

$$-1 = \sum_{i=1}^{m} (g_i(x))^2 + h(x)f(x) \qquad (\star)$$

the degree of $\sum_{i=1}^{n}(g_i(x))^2$ is even and it is not equal to zero. Because in that case $g_i(\alpha)$ will be in F and -1 will be expressed as a sum of squares of elements of F which is impossible since F is real.

As mentioned, $deg(g_i) \leq n-1$ for all $i = 1, 2, \ldots, m$, then $deg(\sum_{i=1}^{n}(g_i(x))^2) \leq 2n-2$. Now we can conclude that $h(x)$ has odd degree and $deg(h(x)) \leq 2n-2-n = n-2$.

Let β be a root of h. Then $(\star)$ implies $-1 = \sum_{i=1}^{n}(g_i(\beta))^2$. Since, $deg(h) < deg(g)$ by induction hypothesis $F(\beta)$ is real, a contradiction. □

Definition 4. A field R is real closed if it is real and any proper algebraic extension of R is not real

We can give the field of real numbers as an example since it is real and the only proper algebraic extension of $\mathbb{R}$ is $\mathbb{C}$; the field of complex numbers is not a real field.

Proposition 1.13. *Let R be a real closed field ordered by P. Any element of P is a square in R.*

Proof. Let a be an element of P which is not a square. Then the polynomial $x^2 - a$ is irreducible in $R[X]$. Let $\alpha \notin R$ be a root of this polynomial, so $\alpha^2 = a$. The algebraic extension $R(\alpha)$ of R is real by Proposition 1.10. $R(\alpha) \neq R$ since $\alpha \notin R$. Hence, we get a contradiction; R is real closed so any algebraic extension of R which is real must be equal to R. □

Corollary 1.14. *If R is a real closed field then for any $a \in R$, either a or $-a$ is a square.*

Proof. Immediate consequence of Proposition 1.13 and the fact that for any ordering P of R, a or $-a$ is in P. □

Corollary 1.15. *A real closed field has a unique ordering.*

Proof. Any real closed field is real, so orderable. By Corollary 1.13, any ordering of a real closed field is the set of all nonzero squares and hence is uniquely determined. □

Proposition 1.16. *Let R be a real closed field. Every polynomial of odd degree in $R[X]$ has a root in R.*

Proof. Let $f(x) \in R[X]$ be an irreducible polynomial and has an odd degree. Let α be a root of f. $R(\alpha)$ is real by Proposition 1.12, but since R is real closed $R(\alpha) = R$, hence $\alpha \in R$. □

Theorem 1.17. *Let K be a field and $f(x) \in K[x]$ an irreducible polynomial if K has characteristic 0, then f is separable. ([PG], 7.2.5)*

Proof. Let $\alpha \in \overline{K}$ be a root of f. Then α is algebraic over K and irreducible polynomial of α over K is f. If α is a multiple root of f then $f'(\alpha) = 0$, f divides f' and $f' = 0$ since $\deg f' < \deg f$. This cannot happen if K has characteristic 0. □

Theorem 1.18. *[PG, 7.2.10] (Primitive Element) Every finite seperable extension is simple.*

Theorem 1.19. *If R is real closed field, then $\overline{R} = R(\sqrt{-1})$.*

Proof. $\sqrt{-1}$ is the root of the polynomial $x^2 + 1$. $\sqrt{-1} \notin R$ otherwise -1 is expressed as a square. $R(\sqrt{-1})$ is an algebraic extension of R. Since R is real closed $R(\sqrt{-1})$ is not real.

Let $\alpha = c + d\sqrt{-1}$ be an element of $R(\sqrt{-1})$, so $c, d \in R$. We have

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

where $a^2 = \frac{c+\sqrt{c^2+d^2}}{2}$ and $b^2 = \frac{-c+\sqrt{c^2+d^2}}{2}$. Clearly, $a, b \in R$. So every element in $R(\sqrt{-1})$ has a square root in $R(\sqrt{-1})$. R has characteristic zero so by Theorem 1.17 every finite extension of $R(\sqrt{-1})$ is contained in an extension K which is finite and Galois over R. Let G be the Galois group over R and H be a 2-Sylow subgroup of

G. Let F be its fixed field. Counting degrees and orders we find that the degree of F over R is odd. By Theorem 1.18 there exists an element in F such that $F = R(\alpha)$. Then α is the root of an irreducible polynomial in $R[X]$ of odd degree. So the degree is 1 by Proposition 1.16. Hence $G = H$ is a 2-group. So K is Galois over $R(\sqrt{-1})$. Let G_1 be its Galois group. Since G_1 is a 2-group, if G_1 is not the trivial group, then G_1 has a subgroup G_2 of index 2. Let F' be the fixed field of G_2. Then F' is of degree 2 because every element has a square root. Thus G_1 is the trivial group and $K = R(\sqrt{-1})$. [SL] □

Corollary 1.20. *A field R is real closed if and only if $R(\sqrt{-1})$ is algebraically closed and $\sqrt{-1} \notin R$.*

Proof. ($\Longrightarrow$) Proved as Theorem 1.19.

($\Longleftarrow$) Let P be the set of nonzero squares of R. Let a^2 and b^2 be squares in R. $a + b\sqrt{-1} = c + d\sqrt{-1}$ for some $c, d \in R$ because $R(\sqrt{-1})$ is algebraically closed.

We have $a + b\sqrt{-1} = c^2 - d^2 + 2cd\sqrt{-1}$. Using linear independency of 1 and $\sqrt{-1}$ we get $a^2 = c^2 - d^2$ and $b = 2cd$. Then $a^2 + b^2 = c^4 - 2c^2d^2 + d^4 + 4c^2d^2 = (c^2 + d^2)^2$. So sum of squares is also a square in R. Hence P is closed under addition. It is clear that it is also closed under multiplication. Let $a \in R \setminus P$ be a nonzero element then the root of $x^2 - a$ is algebraic over R. Let α be the root of that polynomial, since $R(\sqrt{-1})$ is the algebraic closure of R, $\alpha = c + d\sqrt{-1}$ for some $c, d \in R$. $\alpha^2 = c^2 - d^2 + 2cd\sqrt{-1}$. Again using linear independency of 1 and $\sqrt{-1}$. We have, $a = \alpha^2 = -d^2$. So $-a$ is a square in R and is an element of P. So disjoint union of P, $-P$ and $\{0\}$ gives R. Hence R is ordered by P.

Any orderable field is real, hence R is real. Clearly, R may have no other algebraic extension then $R(\sqrt{-1})$ since it is algebraically closed. In the proof of Theorem 1.19 we proved that $R(\sqrt{-1})$ is not real. Hence R is real closed. □

Corollary 1.21. *Let R be a real field. R is real closed if and only if*

1. *Every polynomial of odd degree in $R[X]$ has a root in R.*
2. *For any nonzero $a \in R$ either a or $-a$ is a square in R.*

Proof. ($\Longrightarrow$) Proved as Proposition 1.13 and 1.16.

($\Longleftarrow$) Proved in the proof of 1.20 □

By a real closure of ordered field F, we mean an algebraic extension of F which is real closed.

Theorem 1.22. *Every ordered field F has a real closure that has an ordering including the given ordering of F.*

Proof. An ordered field F is not algebraically closed because by Proposition 1.4 the polynomial $x^2 + 1$ is irreducible over F. Consider the ordered set $\mathscr{S} = \{F_0 = F, F_1, F_2, \ldots\}$ such that F_{i+1} is a real extension of F_i for any natural number i. This set is nonempty since F is real. It is ordered by inclusion and union of any chain from $\mathscr{S}$ is again an element of $\mathscr{S}$ Thus, $\mathscr{S}$ is an inductive set and by Zorn's Lemma it has a maximal element, say R. R is a real field contained in $\overline{F}$. R has no algebraic extension which is real since it is maximal. Hence R is real closed.

Let a be a positive element of F. By Prob 1.13 a is a square in R. Hence a is positive in R. Hence the ordering of F is induced by the unique ordering of R. □

Now, we are going to prove that, the real closure of an ordered field is unique up to isomorphism. We will use *Sturm's Theorem* that provides an algorithm for counting the number of roots of a polynomial on a given interval.

First, we have a theorem which will be useful in proving *Sturm's Theorem*. The following theorem says that real closed fields satisfy the intermediate value theorem.

Theorem 1.23. *Let R be a real closed field and $f(x) \in R[X]$. Let $a, b \in R$ be such that $f(a) < 0$ and $f(b) > 0$, then there exists $c \in R$ between a and b such that $f(c) = 0$*

Proof. $R(\sqrt{-1})$ is algebraically closed by Theorem 1.19. So f has irreducible factors of degree 1 or 2.

Any even factor can be expressed as a sum of squares; let $x^2 + cx + d$ be irreducible $c, d \in R$; $x^2 + cx + d = (x - \frac{c}{2})^2 + (d - \frac{c^2}{4})$. Since, $x^2 + cx + d$ is irreducible we have $4d > c^2$.

So even factors, are always positive when they are evaluated at any element of R. This means that f changes sign if a factor with degree one changes sign. Let c be the root of this factor then $a - c < 0$ and $b - c > 0$, so $a < c$ and $b > c$. Clearly, c is an element of R. As a result there exists $c \in R$ between a and b such that $f(c) = 0$. □

Lemma 1.24. *Let K be a subfield of an ordered field F. Let $\alpha \in F$ be algebraic over K. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial in $K[X]$ such that α is a root of $f(x)$. Then $|\alpha| \leq 1 + |a_{n-1}| + \cdots + |a_n|$*

Proof. There is nothing to prove if $|\alpha| \leq 1$. So assume $|\alpha| > 1$.

$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0$, so

$|\alpha^n| = |a_{n-1}\alpha^{n-1} + \ldots + a_0| \Rightarrow |\alpha^n| \leq |a_{n-1}||\alpha^{n-1}| + \ldots + |a_0| \Rightarrow$

$|\alpha^{n-1}| > 1$ since $|\alpha| > 1$. So we get;

$$\frac{|\alpha^n|}{|\alpha^{n-1}|} \leq \frac{|a_{n-1}||\alpha^{n-1}| + \ldots + |a_0|}{|\alpha^{n-1}|}$$

thus,

$|\alpha| \leq |a_{n-1}| + |a_{n-2}| + \ldots + |a_0|$. □

Definition 5. Let R be a real closed field, $f(x) \in R[X]$ which does not have multiple roots in R, $[u, v] \subset R$. A sequence of polynomials $f_i(x) \in R[X]$, $i = 0, 1, \ldots, m$ satisfying the following properties is called a Sturm sequence of f over [u,v].

ST1. $f_0 = f, f_1 = f'$

ST2. f_m is nonzero constant

ST3. There is no point $x \in [u, v]$ such that $f_j(x) = f_{j+1}(x) = 0$ for any $0 \leq j \leq m-1$

ST4. If $x \in [u, v]$ and $f_j(x) = 0$ for some $j = 1, \ldots, m-1$ then $f_{j-1}(x)$ and $f_{j+1}(x)$ have opposite signs.

ST5. $f_j(u) \neq 0$ and $f_j(v) \neq 0$ for $j = 0, 1, \ldots, m$

In an ordered field, the number of sign changes of a sequence $x_0, x_1, \ldots, x_k$ of nonzero elements is the number of indices $0 < i$ such that $x_i x_{i-1} < 0$. Let $f_0, \ldots, f_m$ be a Sturm sequence of f over $[u, v]$. Let $x \in [u, v]$ such that x is not a root of any polynomial f_i for $i = 0, 1, \ldots, m$. $V_S(x)$ denotes the number of sign changes in the sequence $f_o(x), \ldots, f_m(x)$.

Theorem 1.25. *(Sturm's Theorem) Let R be a real closed field and S be a Sturm sequence of $f(x) \in R[X]$ over $[u, v]$. The number of roots of f in $[u, v]$ is equal to $V_S(u) - V_S(v)$.*

Proof. Let $S = \{f_0, f_1, \ldots, f_k\}$ be the Sturm sequence of f over $[u, v]$.

Let $u < r_1 < \ldots < r_m < v$ where $r_1, \ldots, r_m$ are all roots of the polynomials in the Strum sequence. Let $a, b \in R$ such that $u \leq a < b \leq v$.

First, we will show that if there are no roots between a and b, then $V_S(a) = V_S(b)$. Assume not. Without loss of generality we may assume that $V_S(a) < V_S(b)$. Then there exist $f_i, f_{i+1} \in S$ such that $f_i(b), f_{i+1}(b)$ have different signs where $f_i(a), f_{i+1}(a)$ does not. Then $f_i(a), f_i(b)$ or $f_{i+1}(a), f_{i+1}(b)$ have different signs. Hence by Theorem 1.23 f_i or f_{i+1} has a root between a and b.

Secondly, we will show that $V_S(a) = V_S(b)$ if there is one root of any polynomial $f_1, \ldots, f_k$ between a and b. So we will conclude that roots of $f_1, \ldots, f_k$ does not effect $V_S(a)$ and $V_S(b)$. Let r_j be a root of f_i for $i = 1, \ldots, k$. By ST4, $f_{i-1}(r_j)$ and $f_{i+1}(r_j)$ has different signs. Since there is only one root between a and b, by Theorem 1.23 $f_{i+1}(a), f_{i+1}(r_j), f_{i+1}(b)$ have the same sign and $f_{i-1}(a), f_{i-1}(r_j), f_{i-1}(b)$ have the same sign. Then $f_{i-1}(a)$ and $f_{i+1}(a)$ have different signs and $f_{i-1}(b)$ and $f_{i+1}(b)$ have different signs. As a result, the number of sign changes in the sequences $f_{i-1}(a), f_i(a), f_{i+1}(a)$ and $f_{i-1}(b), f_i(b), f_{i+1}(b)$ are equal to 2. Hence $V_S(a) = V_S(b)$.

Finally, we will show that if there is one root of the polynomial f between a and b, then $V_S(a) = V_S(b) + 1$. Let $a < r_j < b$ with $f(r_j) = 0$ and there is no other root in (a, b). Since r_j is a root of f, $f(x) = (x - r_j)g(x)$ for some $g(x) \in R[X]$, r_j is not a root of $g(x)$ because f does not have multiple roots. Any root of $g(x)$ is a root of $f(x)$ so $g(x)$ has no other root in (a, b). By Theorem 1.23 $g(a), g(r_j), g(b)$ have the same sign. The polynomial $f'(x) = g(x) + (x - r_j)g'(x)$ does not have a root in (a, b) since $g(x)$ does not have a root. Also, r_j is a root of f'. Similarly, $f'(a), f'(r_j), f'(b)$ have the same sign.

Now, $a < r_j < b$ implies $a - r_j < 0$ and $b - r_j > 0$. Evaluating $f(x) = (x - r_j)g(x)$ at a and b we get $f(a)$ and $g(a)$ have different signs and $f(b)$ and $g(b)$ have same sign.As we know that $g(a)$ and $g(b)$ have the same sign, we can say that $f(a)$ and $f(b)$ have different signs.

Recall, $f'(a)$ and $f'(b)$ have the same sign. Then, $f(a)f'(a) < 0 < f(b)f'(b)$. So, the sequence $f_0(a), f'(a)$ has a sign change, but $f(b), f'(b)$ does not. Hence $V_S(a) = V_S(b) + 1$.

Now, assume $u < r_1 < \ldots < r_t < v$ be the roots of f where $t \leq m$. We showed that for any two elements x, y in the interval (r_j, r_{j+1}) for some $j = 0, 1 \ldots, t$ with $r_0 = u$ and $r_{t+1} = v$ we have $V_S(x) = V_S(y)$. Take arbitrary elements x_j's in the intervals (r_j, r_{j+1}). Then,

$V_S(u) = V_S(x_0) = V_S(x_1) + 1 = V_S(x_2) + 2 = \ldots = V_S(x_t) + t = V_S(v) + t.$

Hence, $V_S(u) - V_S(v) = t$. □

Corollary 1.26. *Let K be an ordered field and f be an irreducible polynomial in $K[X]$ which has degree ≥ 1. Let R_1 and R_2 be two real closures of K inducing the given ordering on K. The number of roots of f in R_1 and R_2 are the same.*

Proof. Let R_1 and R_2 be two real closures of K. So, f is a polynomial in $R_1[X]$ and $R_2[X]$ and we may conclude that f has no multiple roots using Theorem 1.23 since ordered fields have characteristic 0 by Lemma 1.17.

By Lemma 1.24, any root α of f in R_1 or in R_2 is bounded. Let $\alpha_1, \ldots, \alpha_m$ be all the roots of f in R_1 , and $|\alpha_i| < c_i$ for $i = 1, \ldots, m$ where $c_i \in R_1$.

Let $c_j = max\{c_1, \ldots, c_m\}$. This maximality is preserved both in R_1 and R_2, because both R_1 and R_2 induce the given ordering of K. So, $[-c_j, c_j]$ contains all roots; $\alpha_1, \ldots, \alpha_m$.

Hence by Sturm's Theorem , number of roots of f in both R_1 and R_2 is $V_S(-c_j) - V_S(c_j)$. □

Corollary 1.27. *A real field has a unique real closure up to isomorphism*

Proof. Let K be a real field and R_1, R_2 be it's two real closures. Let f be an irreducible polynomial over K. Let $\alpha_1 < \alpha_2 < \ldots < \alpha_n$ and $\beta_1 < \beta_2 < \ldots < \beta_m$ be the distinct roots of f in R_1 and R_2 respectively. By Corollary 1.26 we have $n = m$.

There is an isomorphism between $K(\alpha_1)$ and $K(\beta_2)$ which takes α_1 to β_2. So, $K(\alpha_1)$ embeds into R_2. Similarly, there is an embedding $\varphi : K(\alpha_1, \ldots, \alpha_n) \to R_2$ where $\varphi(\alpha_i) = \beta_i$ for $i = 1, 2, \ldots, n$.

Let a be a positive element in $K(\alpha_1, \ldots, \alpha_n)$ then $\sqrt{a}$ is in R_1.

$K(\alpha_1, \ldots, \alpha_n, \sqrt{a})$ is real since $a \in K(\alpha_1, \ldots, \alpha_n)$ by Proposition 1.10. We have an embedding $\psi : K(\alpha_1, \ldots, \alpha_n, \sqrt{a}) \to R_2$ which extens φ.

$\varphi(a) = \psi(a) - \psi(\sqrt{a} \cdot \sqrt{a}) = \psi(\sqrt{a})\psi(\sqrt{a})$

Hence $\psi(a)$ is a square, so positive. As a result, ψ is order preserving.

We have seen that there are subextensions of R_1 over K which are real and embeds in R_2, moreover preserves the ordering. By Zorn's Lemma, there is a maximal real field and because of its maximality it is real closed. So it is R_1. Hence there is an embedding of R_1 into R_2 preserving the order. Hence R_1 and R_2 are isomorphic. □

Chapter 2

Some Facts From Model Theory

We do not give all basic definitions of Model theory. For the further definitions and background see Chang and Keisler[CK].

Proposition 2.1. *[DM1, 1.1.8] Let $\mathcal{M}$ be a substructure of $\mathcal{N}$, $\bar{a} \in \mathcal{M}$ and $\phi(\bar{a})$ is a quantifier-free formula. Then,*

$$\mathcal{M} \models \phi(\bar{a}) \text{ if and only if } \mathcal{N} \models \phi(\bar{a})$$

Proof. First, we will show that if $t(\bar{v})$ is a term and $\bar{b} \in M$ then $t^{\mathcal{M}}(\bar{b}) = t^{\mathcal{N}}(\bar{b})$ using induction on terms.

If t is a constant symbol c, then $c^{\mathcal{M}} = c^{\mathcal{N}}$

If t is a variable v_i, then $t^{\mathcal{M}}(\bar{b}) = b_i = t^{\mathcal{N}}(\bar{b})$

If t is equal to $f(t_1, \ldots, t_n)$ where f is an n-ary function symbol, $t_1, \ldots, t_n$ are terms and $t_i^{\mathcal{M}}(\bar{b} = t_i^{\mathcal{N}}(\bar{b})$ for $i = 1, \ldots, n$. Since, $\mathcal{M} \subseteq \mathcal{N}$, $f^{\mathcal{M}} = f^{\mathcal{N}}$. Thus,

$$\begin{aligned} t^{\mathcal{M}}(\bar{b}) &= f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(\bar{b}), \ldots, t_n^{\mathcal{N}}(\bar{b})) \\ &= f^{\mathcal{N}}(\bar{b}) \end{aligned}$$

Now, we prove the proposition by inducton on formulas.

If ϕ is $t_1 = t_2$ then

$$\begin{aligned} M \models \phi(\bar{a}) &\iff t_1^{\mathcal{M}}(\bar{a}) = t_2^{\mathcal{M}}(\bar{a}) \\ &\iff t_1^{\mathcal{N}}(\bar{a}) = t_2^{\mathcal{N}}(\bar{a}) \\ &\iff \mathcal{N} \models \phi(\bar{a}) \end{aligned}$$

If ϕ is $R(t_1, \ldots, t_n)$ where R is a n-ary relation symbol, then

$$\begin{aligned} \mathcal{M} \models \phi(\bar{a}) &\iff (t_1^{\mathcal{M}}(\bar{a}), \ldots, t_n^{\mathcal{M}}(\bar{a})) \in R^{\mathcal{M}} \\ &\iff (t_1^{\mathcal{M}}(\bar{a}), \ldots, t_n^{\mathcal{M}}(\bar{a})) \in R^{\mathcal{N}} \\ &\iff (t_1^{\mathcal{N}}(\bar{a}), \ldots, t_n^{\mathcal{N}}(\bar{a})) \in R^{\mathcal{N}} \\ &\iff \mathcal{N} \models \phi(\bar{a}) \end{aligned}$$

Thus, the proposition is true for atomic formulas.

Suppose that the proposition is true for φ and that ϕ is $\neg\varphi$, then

$$\begin{aligned} \mathcal{M} \models \phi(\bar{a}) &\iff \mathcal{M} \not\models \varphi(\bar{a}) \\ &\iff \mathcal{N} \not\models \varphi(\bar{a}) \\ &\iff \mathcal{N} \models \phi(\bar{a}) \end{aligned}$$

Suppose that the proposition is true for ψ_0 and ψ_1 and that ϕ is $\psi_0 \wedge \psi_1$, then

$$\begin{aligned} \mathcal{M} \models \psi(\bar{a}) &\iff \mathcal{M} \models \psi_0(\bar{a}) \text{ and } \mathcal{M} \models \psi_1(\bar{a}) \\ &\iff \mathcal{N} \models \psi_0(\bar{a}) \text{ and } \mathcal{N} \models \psi_1(\bar{a}) \\ &\iff \mathcal{N} \models \phi(\bar{a}) \end{aligned}$$

The set of quantifier-free formulas is the smallest set of formulas containing the atomic formulas and closed under negation and conjunction. The proposition is true for all quantifier-free formulas. □

Definition 6. A theory $\mathcal{T}$ is said to have quantifier elimination if for every formula ϕ there exists a quantifier-free formula ψ such that $\mathcal{T} \models \phi \leftrightarrow \psi$.

Definition 7. Let $\mathcal{M}$ and $\mathcal{N}$ be two $\mathcal{L}$-structures. We say that $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$ and denote it by $\mathcal{M} \prec \mathcal{N}$, if $\mathcal{M} \subseteq \mathcal{N}$ and for any $\mathcal{L}$-formula $\varphi(\bar{v})$

and for any $\bar{a} \in \mathcal{M}$,

$$\mathcal{M} \models \varphi(\bar{v}) \Longleftrightarrow \mathcal{N} \models \varphi(\bar{a})$$

Definition 8. An $\mathcal{L}$-theory $\mathcal{T}$ is model complete if $\mathcal{M} \prec \mathcal{N}$ for any models $\mathcal{M}$ and $\mathcal{N}$ of $\mathcal{T}$ where $\mathcal{M} \subseteq \mathcal{N}$

Theorem 2.2. *If $\mathcal{T}$ has quantifier elimination then $\mathcal{T}$ is model complete.*

Proof. Assume $\mathcal{M}, \mathcal{N} \models \mathcal{T}$ and $\mathcal{M} \subseteq \mathcal{N}$. We show, $\mathcal{M}$ is elementary submodel.

Let $\phi(\bar{v})$ be a formula, since $\mathcal{T}$ has quantifier elimination, there exists a quantifier free formula $\psi(\bar{v})$ such that both

$$\mathcal{M} \models \forall \bar{v}\, (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$$

and

$$\mathcal{N} \models \forall \bar{v}\, (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$$

Also, quantifier-free formulas are preserved under extensions. These facts imply that; for $\bar{a} \in \mathcal{M}$,

$$\begin{aligned} \mathcal{M} \models \phi(\bar{a}) &\Longleftrightarrow \mathcal{M} \models \psi(\bar{a}) \\ &\Longleftrightarrow \mathcal{N} \models \psi(\bar{a}) \\ &\Longleftrightarrow \mathcal{N} \models \phi(\bar{a}). \end{aligned}$$

Hence $\mathcal{M}$ is an elementary submodel of $\mathcal{N}$.

Hence $\mathcal{T}$ is model complete. □

Theorem 2.3. *([DM1, Theorem 3.1.4]) For an $\mathcal{L}$-theory $\mathcal{T}$ the following are equivalent*

(i) $\mathcal{T}$ admits quantifier-elimination;

(ii) For any models $\mathcal{M}$ and $\mathcal{N}$ of $\mathcal{T}$ and their common substructure $\mathcal{A}$, for any quantifier-free $\mathcal{L}$-formula $\varphi(\bar{u}, v)$ and $\bar{a} \in \mathcal{A}$, if $\mathcal{M} \models \exists v\, \varphi(\bar{a}, v)$ then $\mathcal{N} \models \exists v\, \varphi(\bar{a}, v)$

Proof. $(i) \implies (ii)$: Suppose that $\mathcal{T} \models \forall \bar{u}(\phi(\bar{u}, v) \leftrightarrow \psi(\bar{u}, v))$ where ψ is quantifier-free. Let the structures $\mathcal{M}$ and $\mathcal{N}$ be models of $\mathcal{T}$ and $\mathcal{A}$ is a common substructure. Let $\bar{a} \in \mathcal{A}$. In Proposition 2.1, we saw that quantifier-free formulas are preserved under substructure and extension. Thus,

$$\begin{aligned} \mathcal{M} \models \phi(\bar{a}, v) &\iff \mathcal{M} \models \psi(\bar{a}, v) \\ &\iff \mathcal{A} \models \psi(\bar{a}, v) \\ &\iff \mathcal{N} \models \psi(\bar{a}, v) \\ &\iff \mathcal{N} \models \psi(\bar{a}, v) \end{aligned}$$

$(ii) \implies (i)$: We may assume that both $\mathcal{T} \cup \{\phi(\bar{v})\}$ and $\mathcal{T} \cup \{\neg\phi(\bar{v})\}$ are satisfiable because if, $\mathcal{T} \models \forall \bar{v}\phi(\bar{v})$ then $\mathcal{T} \models \forall \bar{v}(\phi(\bar{v}) \leftrightarrow c = c)$ and if $\mathcal{T} \models \forall \bar{v}\neg\phi(\bar{v})$ then $\mathcal{T} \models \forall \bar{v}(\phi(\bar{v}) \leftrightarrow c \neq c)$. If there are no constant symbols in the langtuage then there are no quantifier-free sentences. But then for each sentence we can find a quantifier free formula $\psi(v_1)$ such that $\mathcal{T} \models \phi \Leftrightarrow \psi(v_1)$.

Let $\Gamma(\bar{v}) = \{\psi(\bar{v}) : \psi \text{ is a quantifier-free and } \mathcal{T} \models \forall \bar{v}(\phi(\bar{v}) \to \psi(\bar{v}))\}$

Let $d_1, \ldots, d_m$ be new constant symbols. We will show that $\mathcal{T} \cup \Gamma(\bar{d}) \models \phi(\bar{d})$. Then by compactness, there are $\psi_1, \ldots, \psi_n \in \Gamma$ such that

$$\mathcal{T} \models \forall \bar{v} \left(\bigwedge_{i=1}^{n} \psi_i(\bar{v}) \to \phi(\bar{v}) \right)$$

Thus,

$$\mathcal{T} \models \forall \bar{v} \left(\bigwedge_{i=1}^{n} \psi_i(\bar{v}) \leftrightarrow \phi(\bar{v}) \right)$$

and $\bigwedge_{i=1}^{n} \psi_i(\bar{v})$ is quantifier-free. So it is enough to prove that $\mathcal{T} \cup \Gamma(\bar{d}) \models \phi(\bar{d})$. Suppose not. Let $\mathcal{M} \models \mathcal{T} \cup \Gamma(\bar{d}) \cup \{\neg\phi(\bar{d})\}$.

Let $\mathcal{A}$ be the structure of $\mathcal{M}$ generated by $\bar{d}$.

Let $\sum = \mathcal{T} \cup \text{Diag}(\mathcal{A}) \cup \phi(\bar{d})$. If $\sum$ is unsatisfiable then there are quantifier-free formulas $\psi_1(\bar{d}), \ldots, \psi_n(\bar{d}) \in \text{Diag}(\mathcal{A})$ such that

$$\mathcal{T} \models \forall \bar{v} \left(\bigwedge_{i=1}^{n} \psi_i(\bar{v}) \to \neg\phi(\bar{v}) \right)$$

but then

$$\mathcal{T} \models \forall \bar{v} \left(\phi(\bar{v}) \rightarrow \bigvee_{i=1}^{n} \neg \psi_i(\bar{v}) \right)$$

so, $\bigvee_{i=1}^{n} \neg \psi_i(\bar{v}) \in \mathcal{T}$ and $\mathcal{A} \models \bigvee_{i=1}^{n} \neg \psi_i(\bar{d})$, a contradiction. Thus $\sum$ is satisfiable.

Let $\mathcal{N} \models \sum$. We have $\mathcal{N} \models \phi(\bar{d})$ [DM1Lemma2.3.3]. But $\mathcal{M} \models \neg\phi(\bar{d})$, using our assumption (ii), we have $\mathcal{N} \neg\phi(\bar{d})$, a contradiction. □

Definition 9. A model $\mathcal{M}$ of a theory $\mathcal{T}$ is called *algebraically prime* over its substructure $\mathcal{A}$ is any embedding of $\mathcal{A}$ into a model $\mathcal{N}$ of $\mathcal{T}$ extends to an embedding of $\mathcal{M}$ into $\mathcal{N}$.

Definition 10. A theory $\mathcal{T}$ is said to *has algebraically prime models* if for any substructure $\mathcal{A}$ of a model of $\mathcal{T}$ there is a model of $\mathcal{T}$ which is algebaically prime over $\mathcal{A}$.

Definition 11. A substructure $\mathcal{M}$ of a structure $\mathcal{N}$ is called *simply closed in* $\mathcal{N}$ (in symbols $\mathcal{M} \prec_s \mathcal{N}$) if for every quantifier-free formula $\psi(\bar{u}, v)$ and $\bar{a} \in \mathcal{M}$, if $\mathcal{N} \models \exists v\, \psi(\bar{a}, v)$ then $\mathcal{M} \models \exists v\, \psi(\bar{a}, v)$

Theorem 2.4. *Let $\mathcal{T}$ be an $\mathcal{L}$-theory such that $\mathcal{T}$ has algebraically prime models and $\mathcal{M} \prec_s \mathcal{N}$ whenever $\mathcal{M} \subseteq \mathcal{N}$ are models of $\mathcal{T}$. Then $\mathcal{T}$ has quantifier-elimination.*

Proof. We will check the condition (*ii*) of Theorem 2.3. Let $\tilde{\mathcal{A}}$ be a model of $\mathcal{T}$ algebraically prime over $\mathcal{A}$. Then we may assume that $\tilde{\mathcal{A}}$ is a common substructure of $\mathcal{M}$ and $\mathcal{N}$. Moreover, $\tilde{\mathcal{A}}$ is simply closed in $\mathcal{M}$ and $\mathcal{N}$. So, $\mathcal{M} \models \exists v\, \phi(\bar{a}, v)$ implies $\tilde{\mathcal{A}} \models \exists v\, \phi(\bar{a}, v)$ and hence $\mathcal{N} \models \exists v\, \phi(\bar{a}, v)$. □

Model Theory of ACF

Our aim now is to show that theory of algebraically closed fields (ACF) has quantifier elimination and hence is model complete. We will show that it admits quantifier elimination for our purpose.

The theory of algebraically closed fields is formulated in the language of rings $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$.

The axioms for algebraically closed fields are given by;

- The axioms for additive commutative rings;
  - $\forall x \forall y \forall z \, (x - y = z \leftrightarrow x = y + z)$
  - $\forall x \, (x \cdot 0 = 0)$
  - $\forall x \forall y \forall z \, (x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  - $\forall x \, (x \cdot 1 = x \wedge 1 \cdot x = x)$
  - $\forall x \forall y \forall z \, (x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
  - $\forall x \forall y \forall z \, ((x + y) \cdot z = (x \cdot z) + (y \cdot z))$
  - $\forall x (x + 0 = 0 + x = x)$
- The axioms of fields;
  - $\forall x \forall y \, (x \cdot y = y \cdot x)$
  - $\forall x \, (x \neq 0 \rightarrow \exists y (x \cdot y = 1))$
- Finally, the axioms for algebraically closedness;
  - $\forall a_0, \ldots, \forall a_{n-1} \exists x \left(x^n + \sum_{i=0}^{n-1} a_i x^i = 0 \right)$ for $n = 1, 2, \ldots$

We denote the axioms of algebraically closed fields ACF for short.

Lemma 2.5. *ACF has algebraically prime models.*

Proof. Let $\mathcal{D}$ be a substructure of an algebraically closed field then $\mathcal{D}$ is an integral domain. The algebraic closure $\bar{F}$ of the field of fractions F of $\mathcal{D}$ is a model of ACF which is algebraically prime over $\mathcal{D}$. Indeed, any embedding of $\mathcal{D}$ into an algebraically closed field K extends to an embedding of F into K, and any embedding of F into K extends to an embedding of $\bar{F}$ into K. □

Theorem 2.6. *ACF has quantifier elimination.*

Proof. We will use Theorem 2.4 One of the assumptions of Theorem 2.4 is satisfied by the previous lemma. It remains to show that whenever F and K algebraically closed fields with $F \subseteq K$, F is simply closed in K.

Let $\phi(\bar{x}, y)$ be any quantifier free formula and $\bar{a} \in F$.

Let $b \in K$ such that $\mathcal{K} \models \phi(\bar{a}, b)$. We want to show that there is $b' \in F$ such that $\mathcal{F} \models \phi(\bar{a}, b')$

We may assume that $\phi(\bar{v}, x)$ is a conjunction of atomic and negated atomic formulas. Indeed, we may assume that $\phi(\bar{v}, x)$ is in disjunctive normal form, that is $\phi(\bar{v}, x)$ is.

$$\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \theta_{ij}(\bar{v}, x)$$

for some atomic or negated atomic formulas θ_{ij}

Since $\mathcal{K} \models \phi(\bar{a}, b)$,

$$F \models \bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} \theta_{ij}(\bar{a}, b)$$

So,

$$F \models \bigwedge_{j=1}^{m} \theta_{ij}(\bar{a}, b)$$

for some i.

In the language of rings, atomic formulas are of the form $p(\bar{v}) = 0$ where $p \in \mathbb{Z}[x_1, \ldots, x_n]$. If $p(\bar{v}, x) \in \mathbb{Z}[\bar{Y}, X]$ we can view $p(\bar{a}, x)$ as a polynomial in $F[X]$.

Thus, $\phi(\bar{a}, v)$ is equivalent to

$$\bigwedge_{i=1}^{n} p_i(v) = 0 \wedge \bigwedge_{i=1}^{m} q_i(v) \neq 0$$

for some polynomials $p_1, \ldots, p_n, q_1, \ldots, q_m \in F[X]$.

If one of the polynomials p_i is nonzero,assume, then b is algebraic over F and since F is algebraically closed b is in F. So assume $n = 0$.

And so,

$$\mathcal{K} \models \bigwedge_{i=1}^{m} q_i(b) \neq 0$$

Now $q_i(x) = 0$ has finitely many solutions for each $i = 1, \ldots, m$ and consequently there exists finitely many elements that satisfy $\bigvee_{i=1}^{m} q_i(x) = 0$. Since F is algebraically closed field, it is infinite. There are remaining elements on F, say b', that

does not satisfy $\bigwedge_{i=1}^{m} q_i(v) = 0$. Hence

$$F \models \bigvee_{i=1}^{m} q_i(b') \neq 0$$

in other words,

$$F \models \phi(\bar{a}, b')$$

This completes the proof. □

Corollary 2.7. *ACF is model complete*

Proof. Immediate consequence of the previous theorem and Theorem 2.2 □

Model Theory of Real Closed Fields

Proposition 2.8. *The class of real closed fields is axiomatizable*

Proof. The axioms for the class of real closed fields are the following axioms together with the field axioms in $\mathcal{L}_r$;

- For each $n \geq 1$, $\forall x_1 \ldots \forall x_n \, (x_1^2 + \ldots + x_n^2 + 1 \neq 0)$
- $\forall x \exists y \, (y^2 = x \vee y^2 + x = 0)$
- For each $n \geq 0$, $\forall x_0 \ldots \forall x_{2n} \exists y \, (y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$

□

We will denote the theory of real closed fields in language of rings as RCF.

Proposition 2.9. *RCF does not admit quantifier elimination.*

Proof. The formula $\exists y \, (x = y^2)$ is not equivalent to any quantifier free formula $\varphi(x)$ relative to the theory of real closed fields. Suppose not. We know that $\mathbb{R} \models \exists y \, (\sqrt{2} = y^2)$ we have $\mathbb{R} \models \varphi(\sqrt{2})$ and so $\mathbb{Q}(\sqrt{2}) \models \varphi(\sqrt{2})$. Since there is an automorphism of $\mathbb{Q}(\sqrt{2})$ taking $\sqrt{2}$ to $-\sqrt{2}$, we have $\mathbb{Q}(\sqrt{2}) \models \varphi(-\sqrt{2})$. Then $\mathbb{R} \models \varphi(-\sqrt{2})$ and so $\mathbb{R} \models \exists y \, (-\sqrt{2} = y^2)$, whch is not true. □

Proposition 2.10. *The class of real closed ordered fields is axiomatizable.*

Proof. The axioms of real closed ordered fields are the axioms of RCF plus the axioms of ordered fields. □

The class of ordered fields is axiomatized by the axioms of the fields together with the axioms for linear order;

- $\forall x \neg(x < x)$
- $\forall x \forall y \forall z ((x < y \wedge y < z) \rightarrow x < z)$
- $\forall x \forall y (x < y \vee x = y \vee y < x)$

and the axioms

- $\forall x \forall y \forall z (x < y \rightarrow x + z < y + z)$
- $\forall x \forall y \forall z ((x < y \wedge z > 0) \rightarrow x \cdot z < y \cdot z)$
- $0 < 1$

We denote the axioms of real closed ordered fields, $RCOF$ for short.

Now we will prove $RCOF$ admits quantifier elimination. We will use the same theorem in the case of ACF. So we need the following lemma.

Lemma 2.11. *RCOF has algebraically prime models.*

Proof. Let $\mathcal{D}$ be a substructure of a real closed field ordered field. Then $\mathcal{D}$ is an ordered integral domain. The ordering of $\mathcal{D}$ uniquely extends to the field of fractions F of $\mathcal{D}$. Then the real closure $\tilde{F}$ of the ordered field F is algebraically prime over $\mathcal{D}$. Indeed, let $\mathcal{K}$ be a real closed ordered field containing $\mathcal{D}$. Then F embeds to $\mathcal{K}$ over $\mathcal{D}$, so we may assume $F \subseteq K$. Then $\tilde{F}$ embeds to K over F, and so over $\mathcal{D}$. □

Lemma 2.12. *Let $\phi(v, \bar{w})$ be a quantifier-free formula in the language of ordered rings, F is a field and $\bar{a} \in F$. Then*

$$F \models \phi(v, \bar{a}) \leftrightarrow \bigvee_{k=1}^{p} \left(\bigwedge_{i=1}^{n} p_{k,i}(v) = 0 \ \wedge \ \bigwedge_{j=1}^{m} q_{k,j}(v) > 0 \right)$$

where $p_1, \ldots, p_n, q_1, \ldots, q_m \in F[X]$

Proof. Atomic formulas in $\mathcal{L}_{or}$ are of the forms

$$p(\bar{v}) = 0,$$
$$p(\bar{v}) > 0,$$
$$p(\bar{v}) < 0$$

and negated atomic formulas are of the forms

$$p(\bar{v}) \neq 0,$$
$$p(\bar{v}) \not< 0,$$
$$p(\bar{v}) \not> 0$$

where $p \in \mathbb{Z}[\bar{x}]$

Since,

$$\begin{aligned} p(\bar{v}) < 0 &\leftrightarrow -p(\bar{v}) > 0 \\ p(\bar{v}) \neq 0 &\leftrightarrow p(\bar{v}) > 0 \vee -p(\bar{v}) > 0 \\ p(\bar{v}) \not< 0 &\leftrightarrow p(\bar{v}) = 0 \vee p(\bar{v}) > 0 \\ p(\bar{v}) \not> 0 &\leftrightarrow p(\bar{v}) = 0 \vee -p(\bar{v}) > 0 \end{aligned}$$

any atomic formula can be expressed as $p(\bar{v}) > 0 \vee q(\bar{v}) = 0$.

So,

$$F \models \phi(\bar{v}) \leftrightarrow \bigvee_{k=1}^{p} \left(\bigwedge_{i=1}^{n} p_{k,i}(\bar{v}) > 0 \ \wedge \ \bigwedge_{j=1}^{m} q_{k,j}(\bar{v}) = 0 \right)$$

Now, if $p(v, \bar{w}) \in \mathbb{Z}[X, \bar{Y}]$ for $\bar{a} \in F^n$ we can view $p(x, \bar{a})$ as a polynomial in $F[X]$.

Hence,

$$F \models \phi(v, \bar{a}) \leftrightarrow \bigvee_{k=1}^{p} \left(\bigwedge_{i=1}^{n} p_{k,i}(\bar{v}) > 0 \ \wedge \ \bigwedge_{j=1}^{m} q_{k,j}(\bar{v}) = 0 \right)$$

for $p_{k,i}, q_{k,j} \in F[\bar{X}], k = 1, \ldots, p$, $l = 1, \ldots, n$ and $j = 1, \ldots, m$. □

Theorem 2.13. *RCOF has quantifier elimination.*

Proof. In order to use Theorem 2.4, we already proved in Lemma 2.11 that *RCOF* has algebraically prime models. It remains to show that for any $\mathcal{F}, \mathcal{K} \models RCF$ with $\mathcal{F} \subseteq \mathcal{K}, \mathcal{F}$ is simply closed in $\mathcal{K}$.

Let $\phi(\bar{v}, m)$ be any quantifier-free formula and $\bar{a} \in \mathcal{F}$. Let $b \in \mathcal{K}$ such that $\mathcal{K} \models \phi(\bar{a}, b)$. We will show that there is $b' \in \mathcal{F}$ such that $\mathcal{F} \models \phi(\bar{a}, b')$

By Lemma 2.12 and $\mathcal{K} \models \phi(\bar{a}, b)$, we may write;

$$\mathcal{K} \models \bigvee_{k=1}^{p} \left(\bigwedge_{i=1}^{n} p_{k,i}(b) > 0 \ \wedge \ \bigwedge_{j=1}^{m} q_{k,j}(b) = 0 \right)$$

so,

$$\mathcal{K} \models \left(\bigwedge_{i=1}^{n} p_{k,i}(b) > 0 \ \wedge \ \bigwedge_{j=1}^{m} q_{k,j}(b) = 0 \right)$$

for some k.

If some of $q_{k,j}(x)$ is nonzero then this means b is a root of a polynomial in $F[X]$. Hence b is algebraic over F and since F is real closed, b is in F. So, we choose b' to be b. Thus, we may assume that

$$\phi(v, \bar{a}) \leftrightarrow \bigwedge_{j=1}^{m} q_j(\bar{v}) > 0$$

Denote by $\mathscr{S}$ the set of roots in F of the polynomials $q_1, \ldots, q_m$; then $\mathscr{S}$ is finite. First suppose, that $a < b$ for all $a \in F$. Since $\mathscr{S}$ is finite, there is $c \in F$ such that $(c, b) \cap \mathscr{S} = \emptyset$. Then for any $b' \in F$ with $c < b'$, we have $b' < b$ and $q_i(b') > 0$ for all i. Otherwise by intermadiate value property for K, there is $e \in K$ with $q_i(e) = 0$, $b' < e < b$. Since $q_i \in F[X]$, e is algebraic over F and so is $e \in F$. Then $e \in (c, b) \cap \mathscr{S}$, a contradiction.

The case, when $b < a$ for all $a \in F$ is similar. Now, suppose $a_1 < b < a_2$ for some $a_1, a_2 \in F$. As $\mathscr{S}$ is finite, there are $c, d \in F$ with $c < b < d$ such that $(c, d) \cap \mathscr{S} = \emptyset$. As above, for any $b' \in F$ with $c < b' < d$ we have $q_i(b') > 0$ for all i.

So we can find $c_i, d_i \in F$ such that $c_i < b < d_i$ and $q_i(x) > 0$ for all $x \in (c_i, d_i)$.

Choose $c = max\{c_i : i = 1, \ldots, m\}$ and $d = min\{d_i : i = 1, \ldots, m\}$. Now, $\bigwedge_{j=1}^{m} q_i(x) > 0$ for $c < x < d$.

Hence, we can find $b' \in (c, d)$ such that $\mathcal{F} \models \phi(b, \bar{a})$.

Hence, the theory $RCOF$ admits elimination of quantifiers in $\mathcal{L}_{or}$.

□

Corollary 2.14. *RCF is model complete.*

Proof. Let F and K be real closed fields and $F \subseteq K$. There is an ordering $<$ of K

such that $(K, <)$ is a model of $RCOF$. Restricting $<$ on F, we get a substructure $(F, <)$ of $(K, <)$ which is a model of $RCOF$ as well. Since $RCOF$ admits quantifier-elimination and so is model complete, we have $(F, <) \preceq (K, <)$ and in particular $F \preceq K$. □

Chapter 3

Hilbert's Nullstellensatz and Real Nullstellensatz

An algebraic variety is the set of solutions of a system of polynomial equations. Algebraic varieties are the fundamental object of algebraic geometry to study.

Definition 12. Let K be a field, S be a set of polynomials in $K[\bar{X}]$. Define

$$V(S) = \{\bar{a} \in K^n : f(\bar{a}) = 0 \text{ for all } f \in S\}$$

$V(S)$ is called the affine algebraic variety defined by S.

Definition 13. Let V be a subset of K^n where K is a field. Define

$$I(V) = \{f \in K[\bar{X}] : f(\bar{x}) = 0 \text{ for all } \bar{x} \in V\}$$

Clearly, $I(V)$ is an ideal of $K[\bar{X}]$.

As it is seen from the definitions there exists a relation between varieties which are geometric objects and ideals which are algebraic objects. The correspondence between algebraic and geometric objects are obtained by the functions I and V where V maps ideals to affine varieties and I maps affine varieties to ideals.

A natural question is whether this correspondence is one-to-one. On this point Hilbert Nullstellensatz states that there is a one-to-one correspondence between affine varieties and radical ideals when the ground field is algebraically closed. And finally for the real case it is stated by Real Nullstellensatz that the bijective

correspondence occurs between varieties and real ideals when the ground field is real closed.

In this part I will give a model theoretic proof of *Real Nullstellensatz* as an analogue of the model theoretic proof of *Hilbert's Nullstellensatz*.

Theorem 3.1. *(Hilbert Basis Theorem) [SL (4.1)] If K is field, then the polynomial ring $K[X_1, \ldots, X_n]$ is a Noetherian ring. In particular, every ideal of $K[X_1, \ldots, X_n]$ is finitely generated.*

Lemma 3.2. *Let R be a unital ring which is not trivial. Let I be a proper ideal of R. Then there exists a maximal ideal R containing I.*

Proof. Let S be the set of all proper ideals of R containing I. S is the nonempty since I is in S. For any chain T of S, let J be the union of ideals in T. J is also an ideal containing I. Assuming $1 \in J$ implies that one of the ideals of T contains 1 which is not possible. So J is a proper ideal.

By Zorn's Lemma, S has a maximal element. □

Lemma 3.3. *Let R be a ring and P be a prime ideal of R, then R/P is a domain.*

Proof. Let $\bar{f}, \bar{g} \in R/P$ such that $\bar{f}.\bar{g} = \bar{0}$, then $\bar{fg} = 0$ which means $f.g$ is an element of P. Since P is prime either f or g is in P. Hence either $\bar{f}$ or $\bar{g}$ is $\bar{0}$. □

Definition 14. Let R be a commutative ring and I be a deal of R. Define radical of the ideal I;

$$Rad(I) = \{\, r \in R : r^n \in I \text{ for some positive integer n}\}$$

An ideal I of R is called radical ideal if it's radical is equal to itself.

Lemma 3.4. *(Primary Decomposition) If $I \subset K[\bar{x}]$ is a radical ideal, then there are prime ideals $P_1, \ldots, P_m$ containing I such that $I = P_1 \cap \ldots \cap P_m$. [SL, 10.3.3]*

Theorem 3.5. *(Hilbert's Nullstellensatz) Let K be an algebraically closed field, I be an ideal in $K[\bar{X}]$. Then $I = I(V(I))$ if and only if I is a radical ideal.*

Proof. ($\Longrightarrow$) Let $m \in \mathbb{N}$, $f \in K[\bar{X}]$ and $f^m \in I = I(V(I))$. So for all $\bar{\alpha} \in V(I)$, $f^m(\bar{\alpha}) = 0$. Since K has no non-zero nilpotent elements, $f(\bar{\alpha}) = 0$ and this implies that $f \in I(V(I))$. Hence $f \in I$.

($\Longleftarrow$) Assume I is a radical ideal in $K[\bar{X}]$. The inclusion $I \subseteq I(V(I))$ is true for any ideal; let $f \in I$, for any $\bar{\alpha} \in V(I)$, $f(\bar{\alpha}) = 0$, hence $f \in I(V(I))$. For $I(V(I)) \subseteq I$ we will use some model theory.

First, by Hilbert Basis Theorem, $K[\bar{X}]$ is a Noetherian ring and ideals of it are finitely generated. Let $\{g_1, \ldots, g_r\}$ be a set of generators of I.

$$\begin{aligned} V(I) &= \{\bar{x} \in K^n : f(\bar{x}) = 0, \text{ for all } f \in I\} \\ &= \{\bar{x} \in K^n : g_i(\bar{x}) = 0 \text{ for all } i = 1, \ldots, r\} \end{aligned}$$

$$\begin{aligned} I(V(I)) &= \{g \in K[\bar{X}] : g(\bar{x}) = 0 \text{ for all } \bar{x} \in V(I)\} \\ &= \{g \in K[\bar{X}] : g(\bar{x}) = 0 \text{ for all } \bar{x} \in K^n \text{ such that } g_i(\bar{x}) = 0 \text{ for } i = 1, \ldots, r\} \end{aligned}$$

Thus, $g \in I(V(I))$ if and only if

$$K \models \forall \bar{x} \left(\bigwedge_{i=1}^{r} g_i(\bar{x}) = 0 \rightarrow g(\bar{x}) = 0 \right) \qquad (\star)$$

By using Lemma 3.4 there are $P_1, \ldots, P_k$ prime ideals such that $\bigcap_{i=1}^{k} P_i = I$

Let us fix $j \in \{1, \ldots, k\}$. It is enough to show that $g \in P_j$.

Lemma 3.3 states that $K[\bar{X}]/P_j$ is a domain. So we can take the algebraic closure of the field of fractions of $K[\bar{X}]/P_j$ and call it L_j. The composition

$$K \subset K[\bar{X}] \rightarrow K[\bar{X}]/P_j \subset L_j$$

is an embedding, so we can consider it as an inclusion: $K \subseteq L_j$. By model completeness of ACF and ($\star$) we conclude:

$$L_j \models \forall \bar{x} \left(\bigwedge_{i=1}^{r} g_i(\bar{x}) = 0 \rightarrow g(\bar{x}) = 0 \right) \qquad (\star\star)$$

We also have

$$L_j \models \bigwedge_{i=1}^{r} g_i(x_1/P_j, \ldots, x_n/P_j) = 0 \qquad (\star\star\star)$$

since $g_1, \ldots, g_r \in P_j$. Using $(\star\star)$ and $(\star\star\star)$, we get;

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

So, $K[\bar{x}]/P_j \models g(x_1/P_j, \ldots, x_n/P_j) = 0$

And, this means that $g \in P_j$. Hence $g \in I$. □

Definition 15. Let A be a commutative ring. An ideal I of A is said to be *real* if, for every sequence $a_1, \ldots, a_p$ of elements of A, $a_1^2 + a_2^2 + \ldots, a_p^2 \in I$ implies $a_i \in I$ for all $i = 1, \ldots, p$.

Lemma 3.6. *Let A be a commutative ring. Every real ideal of A is a radical ideal.*

Proof. Let I be a real ideal. Let $b \in A$ and $n \in \mathbb{N}$ such that $b^n \in I$. I want to show that $b \in I$. If n is even then $b^{n/2} \in I$. If n is odd then $b^n \cdot b \in I$ and $b^{\frac{n+1}{2}} \in I$. Continuing this way we have $b \in I$. □

Lemma 3.7. *Let A be a commutative Noetherian ring. Let I be a real ideal of A. If $I = \bigcap_{i=1}^{n} P_i$ where P_i's are prime ideals containing I then P_i's are real.*

Proof. We show that P_1 is real. Suppose $a_1^2 + \cdots + a_k^2 \in P_1$. Now choose $b_i's$ from each $P_i \setminus P_1$ for $i = 2, \cdots, n$ and put $b = b_2 \cdot b_3 \cdot \ldots b_n$. As P_1 is prime, $b \notin P_1$.

Clearly, $b \in \bigcap_{i=2}^{n} P_i$. Consider the sum $(a_1b)^2 + (a_2b)^2 + \cdots + (a_kb)^2 \in \bigcap_{i=2}^{n} P_i$. This sum is equal to $(a_1^2 + \cdots + a_k^2)b^2 \in P_1$. So, $(a_1b)^2 + (a_2b)^2 + \cdots + (a_kb)^2 \in \bigcap_{i=1}^{n} P_i = I$. Since I is real $a_ib \in I \subseteq P_1$, for all i. As P_1 is prime and $b \notin P_1$, we have $a_i \in P_1$ for all i □

Lemma 3.8. *Let A be a commutative ring and I be a real prime ideal of A. Then the field of fractions of A/I is real.*

Proof. I will use the fact that, R is a real field if and only if for $\alpha_1, \ldots, \alpha_n \in R$ the sum $\sum_{i=1}^{n} \alpha_i^2 = 0$ implies $\alpha_i = 0$

Let F be the field of fractions of A/I. For $a \in A$, let $\bar{a}$ denote $a + I \in A/I$. We take $\alpha_1, \ldots, \alpha_n \in F$ such that $\sum_{i=1}^{n} \alpha_i^2 = 0$. There are $a_1, b_1, \ldots, a_n, b_n \in R$ such that $\alpha_i = \frac{\bar{a}_i}{\bar{b}_i}$ for each $i = 1, \ldots, n$. Hence we have; $\sum_{i=1}^{n} \frac{\bar{a}_i 2}{\bar{b}_i{}^2} = 0$.

Here note that, $\bar{b}_i$'s can not be $\bar{0}$. So b_i's are not in I.

For each $i = 1, \ldots, n$, define B_i as $\frac{1}{b_i} \prod_{j \neq i} b_j$,

$$\sum_{i=1}^{n} \bar{a}_i{}^2 \bar{B}_i{}^2 = 0 \Longrightarrow \overline{\sum_{i=1}^{n} a_i^2 B_i^2} = 0$$

$\Longrightarrow \sum_{i=1}^{n} a_i^2 B_i^2 \in I$. So $a_i B_i \in I$ for $i = 1, \ldots, n$, since I is real.

I is a prime ideal so $a_i \in I$ or $B_i \in I$, but assuming $B_i \in I$ contradicts the fact that b_i's are not in I, hence $a_i \in I$.

Then, $\bar{a}_i = 0 \Longrightarrow \bar{a}_i/\bar{b}_i = 0$. Hence F is real. □

Corollary 3.9. *Let R be a real closed ordered field and I be a real and prime ideal of $R[\bar{x}]$. Then the field of fractions of $R[\bar{x}]/I$ is an ordered field whose ordering induce the ordering on R.*

Proof. Since R is real closed, it has a unique ordering and it may be considered as a subfield of feld of fractons of $R[\bar{x}]/I$. So it is enough to show that the field of fractions of $R[\bar{x}]/I$ is real. And this follows from Lemma 3.8, since $R[\bar{x}]$ is a commutative Noetherian ring and I is real and prime. □

Theorem 3.10. *(Dubois-Reisler) Let R be a real closed field and let I be an ideal in $R[\bar{X}]$, then $I = I(V(I))$ if and only if I is real.*

Proof. ($\Longleftarrow$):

$I \subseteq I(V(I))$:

Let $f \in I$. For any $\bar{x} \in V(I)$, $f(\bar{x}) = 0$. Hence $f \in I(V(I))$.

$I(V(I)) \subseteq I$

Since the ring of polynomials of finitely many variables over a field is a Noetherian

ring and ideals of Noetherian rings are finitely generated, there is $\{g_1, \ldots, g_r\}$ a finite set of generators of I.

$$\begin{aligned} V(I) &= \{\bar{x} \in R^n : f(\bar{x}) = 0 \text{ for all } f \in I\} \\ &= \{\bar{x} \in R^n : g_i(\bar{x}) = 0 \text{ for all } i = 1, \ldots, r\} \end{aligned}$$

and

$$\begin{aligned} I(V(I)) &= \{g \in R[\bar{X}] : g(\bar{x}) = 0 \text{ for all } \bar{x} \in V(I)\} \\ &= \{g \in R[\bar{X}] : g(\bar{x}) = 0 \text{ for all } \bar{x} \in R^n \text{ such that } g_i(\bar{x}) = 0 \text{ for } i = 1, \ldots, r\} \end{aligned}$$

So, if $g \in I(V(I))$, then

$$R \models \forall \bar{x}[\bigwedge_{i=1}^{r} g_i(\bar{x}) = 0 \to g(\bar{x}) = 0] \qquad (\star)$$

$R[\bar{X}]$ is Noetherian. So using Lemma 3.6 and Lemma 3.4, we may conclude that there are $P_1, \ldots, P_k$ prime ideals containing I such that $\bigcap_{i=1}^{k} P_i = I$.

We want to show that $g \in I$, so it is enough to show that $g \in P_j$ for a fixed j.

Let us look at the ring $R[\bar{X}]/P_j$. P_j is a real ideal by 3.7. So, by 3.8, the field of fractions of $R[\bar{X}]/P_j$ is a real field. Let us call the real closure of this field L_j. Again we can assume that R is a subfield fo L_j. By 3.9, the ordering on L_j extends the ordering of R. The theory of real closed fields is model complete so from $(\star)$ we conclude;

$$L_j \models \forall \bar{x}\,[\bigwedge_{i=1}^{r} g_i(\bar{x}) = 0 \to g(\bar{x}) = 0] \qquad (\star\star)$$

For any $g \in R[\bar{X}]$, $g \in P_j$ is equivalent to the condition that;

$$R[\bar{X}]/P_j \models g(x_1/P_j \ \ldots, x_n/P_j) = 0$$

Since we know that $g_1, \ldots, g_r \in P_j$, we get

$$L_j \models \bigwedge_{i=1}^{r} g_i(x_1/P_j, \ldots, x_n/P_j) = 0 \qquad (\star\star\star)$$

Finally take $\bar{x}$ to be $(x_1/P_j, \ldots, x_n/P_j)$ in $(\star\star)$, by $(\star\star)$ and $(\star\star\star)$ we have

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

Hence $g \in P_j$, and $g \in I$.

($\Longrightarrow$) Let $\sum_{i=1}^{m} a_i^2 \in I$ for $a_1, \ldots, a_m \in R[\bar{X}]$. By our assumption $\sum_{i=1}^{m} a_i^2 \in I(V(I))$. So, $\sum_{i=1}^{m} a_i^2(\bar{x}) = 0$ for all $\bar{x} \in V(I)$.

Since R is real and $a_i(\bar{x}) \in R$, $a_i(\bar{x}) = 0$ for all $i = 1, \ldots, m$ and for all $\bar{x} \in V(I)$. So, we can conclude that $a_i \in I$.

□

Bibliography

[BCR] *JACEK BOCHNAK, MICHEL COSTE, MARIE-FRANÇOISE ROY*, Real Algebraic Geometry, Springer, A series of Modern Surveys in Mathematics, 1998

[BP] *BRUNO POIZAT*, A course in Model Theory - An Introduction to Contemporary Mathematical Logic, Springer, Universitext, 2000

[CK] *C. C. CHANG, H. JEROME KEISLER*, Model Theory, Studies on Logic and the Foundations of Mathematic, Elsevier Science Publishers,1990. 1998

[D] *M.A. DICKMANN*, Application of Model Theory to Real Algebraic Geometry

[DM1] *DAVID MARKER*, Model Theory - An Introduction, Springer, Graduate Texts in Mathematics, 2002.

[DM2] *DAVID MARKER*, Model Theory of Fields, Association For Symbolic Logic, 2006

[GC] *GREG CHAPLIN*, Model Theoretic Algebra - Selected Topics, Springer, Lecture Notes in Mathematics, 1976.

[PD] *ALEXANDER PRESTEL, CHARLES N.DELZELL*, Positive Polynomials - From Hilbert's 17th Problem to Real Algebra, Springer, Monographs in Mathematics, 2001

[PG] *PIERRE GRILLET*, Algebra, A Wiley-Interscience Publication, 1999

[SL] *SERGE LANG*, Algebra, Springer, Graduate Texts in Mathematics