TARSKI'S PRINCIPLE AND THE ELIMINATION OF QUANTIFIERS

RICHARD G. SWAN

Abstract. This is an expository article on Tarski's principle and the elimination of quantifiers for real closed and algebraically closed fields.

1. Introduction

Tarski's Principle [12] is usually discussed in the context of formal languages and model theory. The aim of the present article is to present this result using only ordinary notions of algebra. Hopefully this will make this important result accessible to a wider class of readers. We follow the method of Kreisel and Krivine [6] fairly closely. This has the advantages of being very elementary and also constructive. I have also included some standard applications in section 4 and have added a final section proving the classical properties of real closed fields which are used here. Further results on real closed fields can be found in the original paper of Artin and Schreier [1] and excellent surveys of later results are given in Lam's papers [8], [9].

2. Elementary predicates

Let F be a field, possibly ordered. We consider a special class of relations between elements of F known as elementary predicates. We begin with relations of the form $f(x_1, \dots, x_n) = 0$ and, in the case of an ordered field, also $f(x_1, \dots, x_n) > 0$, where f is a polynomial with integral coefficients. In applying these relations to elements $a_1, \dots, a_n$ of our field we interpret the constant term c of f as $c1$ where 1 is the unit element of F. These relations will be referred to as atomic predicates.

Remark 2.1. The use of integral coefficients does not prevent us from looking at polynomials with coefficients in F. It only forces us to specify these explicitly i.e. $ax^2 + bx + c = 0$ must be written as $f(a, b, c, x) = 0$ where $f(x_1, x_2, x_3, x) = x_1x^2 + x_2x + x_1$.

Although I will not use any deep results from logic, I will use some of the elementary notation of symbolic logic since I think this will make clear what sort of assertions are being considered. We can combine the predicates by using the usual logical connectives: disjunction: $P \vee Q$ (for "P or Q"), conjunction: $P \wedge Q$ (for "P and Q"), and negation: $\neg P$ (for "not P"). We enclose the parts in brackets when necessary to avoid ambiguity. Other logical connectives can be expressed in terms of these: $P \supset Q$ (P implies Q) as $\neg P \vee Q$ and $P \equiv Q$ (P is equivalent to Q) as $(P \supset Q) \wedge (Q \supset P)$.

The class of elementary predicates is defined as the smallest class containing the atomic predicates and closed under $\neg$, $\vee$, $\wedge$ and the quantifiers: $(\forall x)P(x, y_1, \dots, y_n)$ ("$P(x, y_1, \dots, y_n)$ holds for all x") and $(\exists x)P(x, y_1, \dots, y_n)$ ("$P(x, y_1, \dots, y_n)$ holds for some x"). The class of quantifier–free elementary predicates is defined as the smallest class containing the atomic predicates which is closed under $\neg$, $\vee$, $\wedge$, no quantifiers being used.

Remark 2.2. In using the quantifiers $\forall$ and $\exists$, it is best to use a new variable not occurring elsewhere as the quantified variable. In this way we avoid confusing constructions like $(\exists x)[x = 0 \wedge (\forall x)\neg(x^2 + 1 = 0)]$. Rules for parsing such things may be found in the references.

Terminology 2.3.

(1) An elementary predicate in the theory of fields will mean one involving only atomic predicates of the form $f = 0$. If it is intended to be applied to algebraically closed fields, we refer to it as an elementary predicate in the theory of algebraically closed fields.
(2) An elementary predicate in the theory of ordered fields will mean one which may involve atomic predicates of the form $f > 0$ as well as those of the form $f = 0$. If it is intended to be applied to real closed fields, we refer to it as an elementary predicate in the theory of real closed fields.
(3) An elementary predicate involving no free (i.e. unquantified) variables will be called an elementary statement.

Example 2.4. We give a few examples of elementary predicates and statements. The fact that F has characteristic p with p non–zero can be expressed by $p = 0$ using the convention that the constant term of a polynomial is to be interpreted as $p \cdot 1$ in F. It can also be expressed by $(\forall x)[px = 0]$. The fact that F has characteristic 0, however, must be expressed by an infinite number of statements $\neg[p = 0]$ for all primes p. The algebraic closure of the field can be expressed by an infinite sequence of statements $(\forall a_1) \ldots (\forall a_n)(\exists x)[x^n + a_1 x^{n-1} + \ldots a_n = 0]$.

3. Elimination of Quantifiers

Definition 3.1. Two elementary predicates $P(x_1, \ldots, x_n)$ and $Q(x_1, \ldots, x_n)$ are said to be equivalent in the theory of algebraically closed fields if for any algebraically closed field F and elements $a_1, \ldots, a_n \in F$, $P(a_1, \ldots, a_n)$ is true if and only if $Q(a_1, \ldots, a_n)$ is true. Similarly P and Q are equivalent in the theory of real–closed fields if for any real–closed field F and elements $a_1, \ldots, a_n \in F$, $P(a_1, \ldots, a_n)$ is true if and only if $Q(a_1, \ldots, a_n)$ is true. Recall that in the real closed case we allow atomic predicates of the form $f > 0$ as well as $f = 0$.

It is important to specify the type of field being considered in applying this definition. For example, the fact that $x \geq 0$ in a real closed field could be expressed by $(\exists y)[x = y^2]$ but this in not true in the ordered field $\mathbb{Q}$.

As above we say that an elementary predicate is quantifier–free if it is constructed from atomic predicates without using any quantifiers $\forall$ or $\exists$. The main object of this exposition is to prove the following theorem.

Theorem 3.2 (Tarski)**.**

(1) *Any elementary predicate in the theory of algebraically closed fields is equivalent to a quantifier–free one.*
(2) *Any elementary predicate in the theory of real–closed fields is equivalent to a quantifier–free one.*

Corollary 3.3. *Let $F \subseteq E$ be algebraically closed fields and let $P(x_1, \ldots, x_n)$ be an elementary predicate in the theory of algebraically closed fields. If $a_1, \ldots, a_n$ are elements of F then $P(a_1, \ldots, a_n)$ is true in F if and only if it is true in E. The same holds for the real–closed case.*

Once the quantifiers have been eliminated this follows immediately from the fact that it is true for the atomic predicates occurring in P. In the real–closed case note that $a > 0$ in E if and only if it is true in F since $a = b^2$ in F implies the same relation in E while $a = b^2$ in E implies $a \neq -c^2$ in F.

Corollary 3.4 (Elementary Lefschetz Principle)**.** *Let S be an elementary statement in the theory of algebraically closed fields. If S is true for one algebraically closed field F then S is true in all algebraically closed fields having the same characteristic as F.*

Proof. This follows from the previous corollary for algebraically closed fields containing or contained in F. The general case now follows since any algebraically closed field contains the algebraic closure of the prime field. □

Corollary 3.5 (Tarski Principle)**.** *Let S be an elementary statement in the theory of real–closed fields. If S is true for one real–closed field F then S is true in all real–closed fields.*

Proof. This follows as in the case of algebraically closed fields once we know that the real–closure of $\mathbb{Q}$ is unique. A proof of this is given in the next section. □

4. Applications

In this section we will give some standard applications to illustrate the usefulness of Tarski's theorem. We begin with the Hilbert Nullstellensatz.

Theorem 4.1. *Let k be any field and let $A = k[x_1, \ldots, x_n]/I$ be a finitely generated k–algebra. If $A \neq 0$ there is a k–algebra homomorphism $A \to \bar{k}$ of A to the algebraic closure $\bar{k}$ of k.*

Proof. Let $\mathfrak{m} \supseteq I$ be a maximal ideal containing I. Let $I = (h_1, \ldots, h_m)$ and let K be an algebraically closed field containing $A/\mathfrak{m}$. Let $a_1, \ldots, a_N$ be the coefficients of the h_i and let $P(a_1, \ldots, a_N)$ be the predicate $(\exists x_1) \ldots (\exists x_n)[h_1(x) = 0 \wedge \cdots \wedge h_m(x) = 0]$. Since this holds in K it also holds in $\bar{k} \subseteq K$ and the theorem follows. □

Corollary 4.2 (Hilbert's Nullstellensatz)**.** *With the notation of the theorem we have*

(1) *For each maximal ideal $\mathfrak{m}$ of A, $A/\mathfrak{m}$ is a finite algebraic extension of k.*
(2) *Let $V(I) = \{(z_1, \ldots, z_n) \in \bar{k}^n | h(z) = 0$ for all $h \in I\}$. Then the set of $f \in A$ which vanish on $V(I)$ is the radical $\sqrt{I}$.*
(3) *If P is a prime ideal of A then $P = \bigcap_{\mathfrak{m} \supseteq P} \mathfrak{m}$.*

Proof.

(1) The field $A/\mathfrak{m}$ maps to $\bar{k}$ and so is algebraic over k and is finitely generated as a k algebra.
(2) If g vanishes on $V(I)$ then there is no k–algebra homomorphism of A_g to $\bar{k}$ so the image of g in A must be nilpotent i.e. some g^m lies in I.

(3) Let $B = A/P$. If g does not lie in P, $B_g \neq 0$ so there is a k–algebra homomorphism $B_g \to \bar{k}$. The kernel of $A \to B \to \bar{k}$ is a maximal ideal of A containing P but not containing g.

□

In the rest of this sections I will write $\mathbb{R}$ for any real closed field, the real numbers being, of course, the most interesting example. We begin with Artin's solution of Hilbert's 17th problem [2].

Theorem 4.3 (Artin [2])**.** *Let $f(x_1, \dots, x_n)$ be a polynomial in $\mathbb{R}[x_1, \dots, x_n]$ such that $f(a_1, \dots, a_n) \geq 0$ for all $a_1, \dots, a_n$ in $\mathbb{R}$. Then f is a sum of squares in the quotient field $\mathbb{R}(x_1, \dots, x_n)$.*

Examples show that f need not by a sum of squares in the polynomial ring $\mathbb{R}[x_1, \dots, x_n]$ itself.

Proof. The following short proof is due to Gondard and Ribenboim [5]. Lemma 10.1 shows that if f is not a sum of squares in $F = \mathbb{R}(x_1, \dots, x_n)$ then $E = F(\sqrt{-f})$ is real. Let K be a real closure of E. Since $-f$ is a square in K we have $f < 0$. Let $c_1, \dots, c_N$ be the coefficients of f and consider $(\exists X_1)\dots(\exists X_n)[f(X_1, \dots, X_n) < 0]$ as a predicate $P(c_1, \dots, c_N)$ in these coefficients. It is satisfied in K (by the values $X_i = x_i$). Therefore it is satisfied in $\mathbb{R}$ by Corollary 3.3 so there are elements $a_1, \dots, a_n$ in $\mathbb{R}$ which satisfy $f(a_1, \dots, a_n) < 0$ contradicting the hypothesis. □

Next we prove Lang's Homomorphism Theorem [7].

Theorem 4.4 (Lang [7])**.** *Let $A = \mathbb{R}[x_1, \dots, x_n]/I$ be an $\mathbb{R}$–algebra of finite type which is a domain with a real quotient field. Then there is an $\mathbb{R}$–algebra homomorphism $A \to \mathbb{R}$.*

Proof. Let $I = (h_1, \dots, h_m)$ and let ξ_i be the image of x_i in A. Then the predicate $(\exists X_1)\dots(\exists X_n)[h_1(X) = 0 \wedge \dots \wedge h_m(X) = 0]$ in the coefficients of the h_i, is satisfied in the quotient field F of A (by $X_i = \xi_i$) and therefore in a real closure K of F. By Corollary 3.3, it is satisfied in $\mathbb{R}$ also so there are elements r_i in $\mathbb{R}$ such that all $h_i(r) = 0$. The required homomorphism is obtained by sending x_i to r_i. □

Corollary 4.5 ([9, Cor. 5.5(B)])**.** *Let $A = \mathbb{R}[x_1, \dots, x_n]/I$ be an $\mathbb{R}$–algebra of finite type. Then there is an $\mathbb{R}$–homomorphism $A \to \mathbb{R}$ if and only if there is no relation $1 + \sum a_i^2 = 0$ in A*

Proof. The "only if" part is obvious.For the converse let $S = \{1 + \sum a_i^2\}$. This is multiplicative and does not contain 0. Let P be an ideal maximal with respect to $P \cap S = \emptyset$. Then P is prime. Replacing A by A/P we can assume that A is a domain and that S meets all non–zero ideals so that A_S is a field. We claim that this field is real. Suppose $1 + \sum(f_i/s)^2 = 0$ with $s \in S$ and $f_i \in A$. Then $s^2 + \sum(f_i)^2 = 0$ in A but the sum on the left hand side lies in S. Lang's theorem now applies to give the required homomorphism. □

Remark 4.6. For a domain, the condition that there is no relation $1 + \sum a_i^2 = 0$ is weaker than requiring the quotient field to be real. For example let $A = \mathbb{R}[x_1, \dots, x_n]/(\sum x_i^2)$.

Let $A = \mathbb{R}[x_1, \ldots, x_n]/I$ be as above. Let $V(I)$ be the set of $(a_1, \ldots, a_n) \in \mathbb{R}^n$ for which $f(a_1, \ldots, a_n) = 0$ for all $f \in I$. The following is a well known theorem of Dubois and Risler [3], [10], [4].

Corollary 4.7 (Reellnullstellensatz)**.** *$f \in \mathbb{R}[x_1, \ldots, x_n]$ vanishes on $V(I)$ if and only if there are elements g_i of $\mathbb{R}[x_1, \ldots, x_n]$ and $r > 0$ with $f^{2r} + \sum g_i^2 \in I$.*

Proof. The "if" part is obvious. For the converse let $A = \mathbb{R}[x_1, \ldots, x_n]/I$ and note that there is no $\mathbb{R}$–algebra homomorphism $A_f \to \mathbb{R}$ so there is a relation $1 + \sum (g_i/f^s)^2 = 0$ in A_f which implies a relation $f^{2t}(f^{2s} + \sum g_i^2) = 0$ in A. □

With the same notation, suppose that I is the ideal of all polynomials vanishing on $V(I)$ so that A is a ring of functions on $V(I)$. Let S be the set of all elements of A which have no zeros on $V(I)$. and define the "real coordinate ring" of A to be A_S. This can be described algebraically in terms of A as follows.

Corollary 4.8. *With this notation we have $A_S = A_\Sigma$ where Σ is the set of all $1 + \sum f_i^2$ in A.*

Proof. Clearly Σ is contained in S. We have to show that if $s \in S$ there is a $\sigma \in \Sigma$ which is divisible by s. Since s is never zero on $V(I)$ there is no $\mathbb{R}$–algebra homomorphism $A/(s) \to \mathbb{R}$. By corollary 4.5 we have some $1 + \sum f_i^2 \in (s)$ so $\sigma = 1 + \sum f_i^2$ will do. □

In [11] I gave a generalization of this result to the case of semi–algebraic sets.

Using these methods we can also show that the real closure of an ordered field is unique if it preserves the ordering. It is well known that a filtered limit of non–empty compact spaces is compact and non–empty. I will give a simple proof of the non–emptyness for the case of finite sets.

Lemma 4.9. *Let $\{X_\alpha | \alpha \in D\}$ be an inverse system of non–empty finite sets where D is a directed set.. Then $\lim X_\alpha$ is non–empty.*

Proof. Since the intersection of a chain of non–empty finite sets is non–empty, Zorn's lemma applies to show that $\{X_\alpha\}$ has a sub inverse system $\{Y_\alpha\}$ minimal with respect to consisting of non–empty sets. Fix an α. If each y in Y_α is not in the image of some $Y_{\beta(y)}$, choose $\gamma > \beta(y)$ for all y. Then the image of $Y_\gamma \to Y_\alpha$ would be empty so Y_γ would be empty. This shows that there is some y in Y_α which lies in the image of all Y_β with $\beta \geq \alpha$. Let Z_β be the inverse image of y in Y_β for $\beta \geq \alpha$ and let $Z_\beta = Y_\beta$ for all other β. Then $\{Z_\beta\}$ is a sub inverse system of non–empty sets so the minimality of $\{Y_\beta\}$ shows that $Z_\beta = Y_\beta$ for all β. Therefore each Y_α has exactly one element so $\lim Y_\alpha$ is a single element which lies in $\lim X_\alpha$. □

Lemma 4.10. *Let E and K be fields containing a field F. Assume that E is algebraic over F. If for each subfield E' of E finite over F there is an F–embedding of E' in K, then there is an F–embedding of E in K*

Proof. Write $\mathrm{Hom}_F(E, K)$ for the set of F–algebra homomorphisms $E \to K$. The fields E' form a directed set and for each of them $\mathrm{Hom}_F(E', K)$ is finite and non–empty by hypothesis. By Lemma 4.9 we see that $\mathrm{Hom}_F(E, K) = \lim \mathrm{Hom}_F(E', K)$ is non–empty. □

Theorem 4.11. *Let E be a real closure of F (with E algebraic over F). Let K be a real closed field containing F which induces the same ordering on F as E does. Then there is an F–embedding of E in K.*

Proof. Let E' be a subfield of E finite over F. Write $E' = F[x]/(f(x))$ and consider $(\exists x)[f(x) = 0]$ as a predicate in the coefficients $a_1, \dots, a_n$ of f. By Theorem 3.2, this is equivalent to a quantifier free predicate $P(a_1, \dots, a_n)$. This holds in E and therefore in F since it involves only elements of F. Since K induces the same order on F, $P(a_1, \dots, a_n)$ also holds in K so there is a ξ in K satisfying $f(\xi) = 0$ and we embed E' in K by sending x to ξ. It now follows by Lemma 4.10 that E embeds in K. $\square$

Remark 4.12. The fact that $P(a_1, \dots, a_n)$ holds in F does not imply that f has a root in F since the equivalence of $P(a_1, \dots, a_n)$ with $(\exists x)[f(x) = 0]$ only holds for real closed fields.

It is well known that any ordered field has a real closure which induces the given ordering on it. I have included the usual proof in section 10. The next corollary shows that this is unique up to isomorphism.

Corollary 4.13. *If E and K are real closures of F which induce the same ordering on F then there is an F–isomorphism $E \approx K$.*

Proof. Embed E in K by the theorem. Then K is real and algebraic over E. Since E is real closed this implies $E = K$. $\square$

Corollary 4.14. *Let F be a subfield of the real closed field K. Let E be the algebraic closure of F in K. Then E is real closed.*

Proof. If $a > 0$ in E then $\sqrt{a}$ is in K and therefore in E. It follows that all positive elements of E are squares in E so E has a unique order. Let L be a real closure of E. By the theorem we can embed L in K. Since L is algebraic over E and E is algebraically closed in K we have $L = E$. $\square$

In contrast to Theorem 4.1 if k is a subfield of $\mathbb{R}$, and $A = k[x_1, \dots, x_n]/I$ satisfies the conditions of Lang's Theorem 4.4 it may still happen that there is no k–algebra homomorphism $A \to \mathbb{R}$. For example, let $k = \mathbb{Q}(\sqrt{2})$ and let $A = k[x]/(x^2 - \sqrt{2}) = \mathbb{Q}(\sqrt[4]{2})$. This maps to $\mathbb{R}$ but if we embed k in $\mathbb{R}$ be sending $\sqrt{2}$ to $-\sqrt{2}$, there is no extension to A. One has to assume that the order induced on k by $\mathbb{R}$ and by a real closure of the quotient field of A agree. The precise result is as follows.

Theorem 4.15 ([8, §6.2])**.** *Let $A = k[x_1, \dots, x_n]/I$ be a k–algebra of finite type which is a domain with quotient field F. Suppose F is ordered and let K be a real closure of k which induces the same order on k as F does. Then there is a k–algebra homomorphism $A \to K$.*

Proof. The proof is essentially the same as Theorem 4.11. Let E be a real closure of F inducing the given ordering on F. Let

$$(\exists X_1) \dots (\exists X_n)[h_1(X) = 0 \wedge \dots \wedge h_m(X) = 0]$$

be the predicate considered in the proof of Theorem 4.4. By Theorem 3.2, this, when applied to real closed fields, is equivalent to a quantifier free predicate $P(a_1, \dots, a_N)$ in the coefficients $a_0, \dots, a_N$ of $h_1, \dots, h_m$. This holds in E and therefore in F since it involves only elements of F. Since K induces the same order on F, $P(a_1, \ldots, a_n)$ also holds in K so there are elements ξ_j in K satisfying $h_i(\xi_1, \ldots, \xi_n) = 0$ giving the required homomorphism. □

5. Preliminary Reduction

In order to prove Theorem 3.2 it will obviously suffice to eliminate one quantifier at a time. Since $(\forall x)P(x)$ is equivalent to $\neg(\exists x)\neg P(x)$, it is enough to consider the case of one existential quantifier $(\exists x)P(x, y_1, \ldots, y_n)$ where P is quantifier–free. We will normally omit mentioning the other variables y_i. This P is constructed from atomic predicates of the form $f = 0$ and $g > 0$ (or $g \neq 0$ in the algebraically closed case) where f and g are polynomials in $x, y_1, \ldots, y_n$. We regard them as polynomials in x with coefficients in $\mathbb{Z}[y_1, \ldots, y_n]$.

Lemma 5.1. *Let P be a quantifier–free predicate constructed from atomic predicates $A_1, \ldots, A_n$. Then P is equivalent to a disjunction $P_1 \vee P_2 \vee \cdots \vee P_m$ where each P_i has the form $B_{i1} \wedge B_{i2} \wedge \cdots \wedge B_{ir_i}$ with each B_{ij} of the form A_k or $\neg A_k$.*

Proof. Since $P \supset Q$ is equivalent to $\neg P \vee Q$ and $P \equiv Q$ is equivalent to $[P \supset Q] \wedge [Q \supset P]$, we can build up P using only $\neg$, $\vee$ and $\wedge$. By induction on the length it is sufficient to show that if P and Q have the required form then so do $P \vee Q$, $P \wedge Q$, and $\neg P$. This is trivial for $P \vee Q$. If $P = P_1 \vee P_2 \vee \cdots \vee P_m$ and $Q = Q_1 \vee Q_2 \vee \cdots \vee Q_n$, then $P \wedge Q$ is equivalent to the disjunction $\bigvee_{i,j} P_i \wedge Q_j$, and $\neg P$ is equivalent to $\bigwedge_i \neg P_i$. Now $\neg P_i$ is equivalent to $\neg B_{i1} \vee \neg B_{i2} \vee \cdots \vee \neg B_{ir_i}$. This has the required form and therefore so does $\bigwedge_i \neg P_i$ by the case $P \wedge Q$. □

Corollary 5.2. *A quantifier–free predicate in the theory of fields is equivalent to the disjunction of predicates of the form $f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 \neq 0 \wedge \cdots \wedge g_q \neq 0$. A quantifier–free predicate in the theory of ordered fields is equivalent to the disjunction of predicates of the form $f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0$.*

Proof. The first statement is immediate. For the second note that $\neg[f = 0]$ i.e. $f \neq 0$ is equivalent to $[f > 0] \vee [-f > 0]$ and that $\neg[f > 0]$ is equivalent to $[f = 0] \vee [-f > 0]$. Since $[C \vee D] \wedge E$ is equivalent to $[C \wedge E] \vee [D \wedge E]$ the result follows easily. □

Corollary 5.3. *It will suffice to prove the elimination of quantifiers for predicates of the form $(\exists x)[f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0]$ in the real–closed case and $(\exists x)[f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 \neq 0 \wedge \cdots \wedge g_q \neq 0]$ in the algebraically closed case.*

This follows from the fact that $(\exists x)[P_1 \vee P_2 \vee \cdots \vee P_m]$ is equivalent to $[(\exists x)P_1] \vee [(\exists x)P_2] \vee \cdots \vee [(\exists x)P_n]$

6. Pseudomonic Form

The proof of the theorem is complicated by the fact that the polynomials involved need not be monic. In fact, the coefficients will, in general, be polynomials in the other variables.

Definition 6.1. I will say that a quantifier–free predicate $P(x)$ is in pseudomonic form (relative to the variable x) if it has the form $c \neq 0 \wedge Q(x)$ where c is a polynomial not involving x and divisible by the leading coefficients (with respect to x) of all polynomials occurring in $Q(x)$

Lemma 6.2. *A quantifier–free predicate in the theory of fields is equivalent to the disjunction of quantifier–free predicates in pseudo–monic form.*

Proof. Let $h_1(x), \dots, h_r(x)$ be all the polynomials occurring in the given predicate $P(x)$. Let c_i be the leading coefficient of h_i. Then $P(x)$ is equivalent to the disjuction $[c_1 = 0 \wedge P(x)] \vee [c_1 \neq 0 \wedge P(x)]$. In $[c_1 = 0 \wedge P(x)]$ we can erase the leading term of h_1 and use induction on the number of terms (in x) in $P(x)$ to put $[c_1 = 0 \wedge P(x)]$ in the required form. The expression $[c_1 \neq 0 \wedge P(x)]$ is equivalent to the disjunction $[c_1 c_2 \neq 0 \wedge P(x)] \vee [c_1 \neq 0 \wedge c_2 = 0 \wedge P(x)]$. The expression with $c_2 = 0$ is treated by induction as before and we repeat the process on the other expression using c_3, etc. □

Remark 6.3. Note that this reduction does not increase the degrees of the polynomials involved.

Corollary 6.4. *A quantifier–free predicate in the theory of fields is equivalent to the disjunction of pseudo–monic predicates of the form* $c \neq 0 \wedge f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 \neq 0 \wedge \cdots \wedge g_q \neq 0$ *where c is divisible by the leading coefficients of the* f_i *and the* g_j*. A quantifier–free predicate in the theory of ordered fields is equivalent to the disjunction of predicates of the form* $c \neq 0 \wedge f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0$ *where c is divisible by the leading coefficients of the* f_i *and the* g_j*.*

7. Euclidean Algorithm

In proving the theorems we will take the following as our induction hypothesis.

Induction Hypothesis(n). *Let* $P(x)$ *be a quantifier–free predicate and let* f *be a polynomial of degree at most* n *in* x*. Let* c *be a polynomial in the variables other than* x *which is divisible by the leading coefficient of* f*. Then* $(\exists x)[c \neq 0 \wedge f = 0 \wedge P(x)]$ *is equivalent to a quantifier–free predicate.*

We first show that the polynomials in $P(x)$ can be assumed to have degrees less than n

Lemma 7.1. *Let* f *be a polynomial of degree* d *over a commutative ring with leading coefficient* a*. Let* g *be a polynomial of degree* m *over the same ring where* $m \geq d$*. Then we can write* $a^{m-d+1} g = fq + r$ *where* $\deg r < d$

Proof. Let b be the leading coefficient of g and let $g_1 = ag - bx^{m-d} f$. Then $\deg g_1 < m$. If $m = d$ we are done and otherwise the result follows by induction on m □

Lemma 7.2. *A predicate of the form* $(\exists x)[a \neq 0 \wedge f = 0 \wedge P(x)]$ *where* a *is divisible by the leading coefficient of* f *is equivalent to a predicate* $(\exists x)[a \neq 0 \wedge f = 0 \wedge Q(x)]$ *where all polynomials in* $Q(x)$ *have degree less than that of* f*.*

Proof. If $g(x)$ occurs in $P(x)$ we can replace $g(x)$ by $a^N g(x)$ since the value of $Q(x)$ is only relevant when $a \neq 0$. We choose N even so as not to affect the sign of $g(x)$ in the ordered case. By Lemma 7.1 we can write $a^N g(x) = f(x)q(x) + r(x)$ (for sufficiently large N) where $\deg r < \deg f$. We can then replace $a^N g(x)$ by $r(x)$ since the value of $Q(x)$ is only relevant in case $f = 0$. □

The proof will now proceed as follows. The induction hypothesis is clearly true for $n = 0$ since f will then be a constant and therefore $c \neq 0 \wedge f = 0$ is always false. We state the following steps for the real–closed case. The same results hold in the algebraically closed case if we replace all conditions $g > 0$ by $g \neq 0$.

Lemma 7.3. *If the induction hypothesis holds for n then the induction hypothesis holds for $n + 1$ provided that any predicate*

$$(\exists x)[c \neq 0 \wedge f = 0 \wedge g_1 > 0, \dots g_q > 0]$$

with $\deg f = n+1$, $\deg g_i \leq n$ *for all i, and c divisible by the leading coefficients of f and all g_i, is equivalent to a quantifier–free predicate*

Proof. We must show that a predicate $(\exists x)[a \neq 0 \wedge f = 0 \wedge P(x)]$ with $\deg f = n+1$ and a divisible by the leading coefficient of f is equivalent to a quantifier–free predicate. By Lemma 7.2 we can assume that all polynomials in $P(x)$ have degree at most n. After reducing $P(x)$ to a disjunction of pseudomonic expressions of the form $c \neq 0 \wedge f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0$, our predicate reduces to a disjunction of predicates of the form

$$ac \neq 0 \wedge f = 0 \wedge f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0$$

where ac is divisible by the leading coefficients of f, the f_i, and the g_j, and the f_i and g_j have degrees at most n. If $p \neq 0$ the induction hypothesis applies using f_1. Therefore only the case $p = 0$ remains to be proved. □

Lemma 7.4. *If the induction hypothesis holds for all n and if any predicate of the form*

$$(\exists x)[c \neq 0 \wedge g_1 > 0, \dots g_q > 0]$$

with c divisible by the leading coefficients of all g_i, is equivalent to a quantifier–free predicate, then any predicate $(\exists x)P(x)$ with $P(x)$ quantifier–free is equivalent to a quantifier–free predicate.

Proof. We reduce $P(x)$ to a disjunction of pseudomonic expressions of the form

$$c \neq 0 \wedge f_1 = 0 \wedge \cdots \wedge f_p = 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0$$

where c is divisible by the leading coefficients of the f_i and the g_j. If $p \neq 0$ the induction hypothesis applies using f_1. Therefore only the case $p = 0$ remains to be proved. □

In verifying the hypotheses of these two lemmas I will always make sure that the sought for quantifier–free predicate has the form $c \neq 0 \wedge Q$. Then, in checking the equivalence by assigning values in a real closed field to the variables other than x, we can assume that $c \neq 0$ for the assigned values, the case $c = 0$ being trivial. As always, c will denote a polynomial in the variables other than x.

8. The algebraically closed case

We first consider the case of algebraically closed fields. In order to prove Theorem 3.2 in this case it will suffice, by the remarks in the last section to prove the following two lemmas.

Lemma 8.1. *In the theory of algebraically closed fields a predicate of the form* $(\exists x)[c \neq 0 \wedge g_1 \neq 0 \wedge \cdots \wedge g_q \neq 0]$ *where* c *is divisible by the leading coefficients of the* g_i*, is equivalent to the quantifier–free predicate* $c \neq 0$*.*

Proof. The predicate is equivalent to $(\exists x)[c \neq 0 \wedge g(x) \neq 0]$ where $g = g_1 \cdots g_q$. Suppose that we have assigned values (in an algebraically closed field) to the variables other than x. If $c \neq 0$ then the leading coefficient of g is non–zero. Since the field is infinite, any x not a root of g will satisfy $g(x) \neq 0$. □

Lemma 8.2. *In the theory of algebraically closed fields a predicate of the form* $(\exists x)[c \neq 0 \wedge f = 0 \wedge g_1 \neq 0 \wedge \cdots \wedge g_q \neq 0]$ *where* c *is divisible by the leading coefficients of* f *and the* g_i *is equivalent a quantifier–free predicate.*

Proof. As in the previous proof the predicate is equivalent to $(\exists x)[c \neq 0 \wedge f = 0 \wedge g \neq 0]$. Suppose that we have assigned values to all the variables except x in such a way that $c \neq 0$. There will be an element x with $f(x) = 0$ and $g(x) \neq 0$ unless every root of f is also a root of g. As observed in [6], this will happen if and only if f divides g^d where $\deg f = d$. . Let m be the degree of g and write $c^{m-d+1}g^d = fq + r$ where $\deg r < \deg f$. After assigning values to all variables but x in such a way that $c \neq 0$, r is still the remainder in dividing $c^{m-d+1}g^d$ by f and f divides g^d if and only if it divides $c^{m-d+1}g^d$ which happens if and only if r is identically zero. Therefore, if we write $r(x) = a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_0$, our predicate is equivalent to $c \neq 0 \wedge [a_{d-1} \neq 0 \vee a_{d-2} \neq 0 \vee \cdots \vee a_0 \neq 0]$. □

9. The real–closed case

The following theorem lists the (well–known) results on real closed fields which we will need. These results are all proved in the original paper [1]. I have also included proofs in section 10 for completeness.

Theorem 9.1. *A real closed field* F *has the following properties.*

1. *F has a unique ordering. The positive elements are the non–zero squares.*
2. *Let $f(X) \in F[X]$ be a polynomial over F. Suppose that $f(a) < 0$ and $f(b) > 0$ where $a < b$. Then there is an element $c \in F$ with $a < c < b$ and $f(c) = 0$.*
3. *Let $f(X) \in F[X]$ be a polynomial over F. Let $a < b$ and assume that $f'(x) > 0$ for all x in (a, b) where $f'(x)$ is the derivative of f with respect to x. Then $f(a) < f(b)$.*

Before giving the proof of Tarski's theorem we consider a few special cases which will be useful.

Lemma 9.2. *Suppose the induction hypothesis holds for* n*. Let* $\deg g \leq n$ *and let* c *be a polynomial in the other variables divisible by the leading coefficient of* g*. Let* y *and* z *be variables not occurring in* g*. Then the following assertions are equivalent to quantifier–free predicates in* y*,* z*, and the remaining variables.*

1. *$c \neq 0$, $y < z$, and g is never zero in the open interval (y, z).*

(2) *$c \neq 0$ and g is never zero in the open interval (y, ∞).*
(3) *$c \neq 0$ and g is never zero in the open interval $(-\infty, z)$.*
(4) *$c \neq 0$ and g is never zero.*

Proof. The predicate (1)is equivalent to $c \neq 0 \wedge y < z \wedge \neg(\exists x)[y < x < z \wedge g(x) = 0]$. Since this will be false if $c = 0$, it does not affect the truth of the assertion if we insert $c \neq 0$ in the last bracket getting $c \neq 0 \wedge y < z \wedge \neg(\exists x)[y < x < z \wedge c \neq 0 \wedge g(x) = 0]$. The induction hypothesis can now be applied to eliminate the quantifier. A similar argument applies to the other predicates. We omit $y < z$ and replace $y < x < z$ by $y < x$, $x < z$ for (2) and (3) and omit it for (4). □

Lemma 9.3. *Let $f = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ be a polynomial over a real closed field with $a_0 \neq 0$. If $|x| > |a_0|^{-1} \sum_0^n |a_i|$ then $f(x) = a_0 x^n \theta$ where $\theta > 0$.*

Proof. We have $\theta = 1 + a_0^{-1} a_1 x + \ldots a_0^{-1} a_n x^n$. Since $|x| \geq 1$, $|x|^{-k} \leq |x|^{-1}$ for $k \geq 1$ so $\theta \geq 1 - \sum_1^n |a_0|^{-1} |x|^{-1} > 0$ □

As usual we use $x >> 0$ to mean x is sufficiently large and $x << 0$ to mean $-x$ is sufficiently large.

Corollary 9.4. *Let c be a polynomial in the variables other than x and let $f(x)$ be a polynomial whose leading coefficient divides c. Then the assertions*
(1) *$c \neq 0$ and $f(x) > 0$ for $x >> 0$*
(2) *$c \neq 0$ and $f(x) < 0$ for $x << 0$*

are equivalent to quantifier–free predicates in the coefficients of f

In fact (1) is equivalent to $c \neq 0 \wedge a_0 > 0$ while (2) is equivalent to $c \neq 0 \wedge (-1)^n a_0 < 0$.

We now turn to the proof of Tarski's theorem. As shown above, to prove Theorem 3.2 it will suffice to prove the following two lemmas.

Lemma 9.5. *Suppose the induction hypothesis holds for n. Then a predicate*

$$(\exists x)[c \neq 0 \wedge g_1 > 0, \ldots g_q > 0]$$

with $\deg g_i \leq n$ for all i, and c divisible by the leading coefficients of all g_i, is equivalent to a quantifier–free predicate.

Lemma 9.6. *Suppose the induction hypothesis holds for n. Then a predicate*

$$(\exists x)[c \neq 0 \wedge f = 0 \wedge g_1 > 0, \ldots g_q > 0]$$

with $\deg f = n + 1$, $\deg g_i \leq n$ for all i, and c divisible by the leading coefficients of f and all g_i, is equivalent to a quantifier–free predicate.

In each case we give an explicit construction of an equivalent predicate to which the induction hypothesis for n applies. Since these are rather lengthy I will write them out in the usual mathematical terminology avoiding long strings of $\vee$'s and $\wedge$'s.

In the next two lemmas, the condition $c \neq 0$ is never used but it seemed simpler to include it than to explain later where this condition should go in the applications to Lemmas 9.5 and 9.6.

Lemma 9.7. *The predicate*

$$(\exists x)[c \neq 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0]$$

with c divisible by the leading coefficients all g_i, is equivalent to the disjunction of the following predicates where i, j, and k run from 1 to q.

A(i,j): *$c \neq 0$ and there exist y and z such that*
 (1) $y < z$
 (2) $g_i(y) = 0$
 (3) $g_j(z) = 0$
 (4) *For $k = 1, \dots, q$, g_k is never 0 on (y, z)*
 (5) *For $k = 1, \dots, q$, $g_k(\frac{y+z}{2}) > 0$*

B(i): *$c \neq 0$ and there exists y such that*
 (2) $g_i(y) = 0$
 (4) *For $k = 1, \dots, q$, g_k is never 0 on (y, ∞)*
 (5) *For $k = 1, \dots, q$, $g_k(y+1) > 0$*

C(j): *$c \neq 0$ and there exists z such that*
 (3) $g_j(z) = 0$
 (4) *For $k = 1, \dots, q$, g_k is never 0 on $(-\infty, z)$*
 (5) *For $k = 1, \dots, q$, $g_k(z-1) > 0$*

D: *$c \neq 0$ and*
 (4) *For $k = 1, \dots, q$, g_k is never 0*
 (5) *For $k = 1, \dots, q$, $g_k(0) > 0$*

Proof. Suppose all variables except x have been assigned values in a real closed field F in such a way that $c \neq 0$. If one of the itemized predicates holds, condition (5) gives the required value of x for which all g_k are positive. Conversely, assume that such an x exists. Let $a_1, \dots, a_N$ be all roots of all g_k in F arranged in increasing order. Write $a_0 = -\infty$ and $a_{N+1} = \infty$. This gives a partition of F into non–overlapping intervals $(a_0, a_1], [a_1, a_2], \dots, [a_N, a_{N+1})$. The value of x is not one of the a_μ since all g_k are positive at x. Suppose the value of x lies in the interval $(a_\mu, a_{\mu+1})$. We consider the case that $\mu \neq 0$ and $\mu + 1 \neq N + 1$. The argument in the remaining cases is similar. Let a_μ be a root of g_i and let $a_{\mu+1}$ be a root of g_j. Set $y = a_\mu$ and $z = a_{\mu+1}$. Then conditions (1), (2), and (3) clearly hold, (4) is clear since the a_μ are all zeros of all g_k, and (5) holds because all g_k are positive at x and the g_k cannot change sign in the interval (y, z) otherwise Theorem 9.1(2) would imply that some g_k has a zero in (y, z). □

Proof of Lemma 9.5. Assume the induction hypothesis for n and suppose $\deg g_k \leq n$ for all k. Then the numbered conditions are all equivalent to quantifier–free predicates in y and z. For (4) we use Lemma 9.2 and the induction hypothesis. After replacing this by a quantifier–free predicate we can rewrite A(i,j) as $(\exists y)[c \neq 0 \wedge g_i(y) = 0 \wedge (\exists z)[c \neq 0 \wedge g_j(z) = 0 \wedge Q(y, z)]]$ where $Q(y, z)$ is a quantifier–free predicate equivalent to the remaining conditions of A(i,j). Since $\deg g_i \leq n$ and $\deg g_j \leq n$, the induction hypothesis applies to eliminate the quantifier $(\exists z)$ and the again to eliminate the quantifier $(\exists y)$ A similar argument applies to the remaining cases. For B(i) we get $(\exists y)[c \neq 0 \wedge g_i(y) = 0 \wedge Q(y)]$ and similarly for C(j) we get $(\exists z)[c \neq 0 \wedge g_j(z) = 0 \wedge Q(z)]$. For D we get a quantifier–free predicate once (4) has been replaced by a quantifier–free condition. □

We now turn to the proof of Lemma 9.6. Following [6], the trick here is to add another condition involving the derivative f' of f, replacing

$$(\exists x)[c \neq 0 \wedge f = 0 \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0]$$

by the disjunction of 3 predicates

$$(\exists x)[c \neq 0 \wedge f = 0 \wedge R_\nu(x) \wedge g_1 > 0 \wedge \cdots \wedge g_q > 0]$$

where $R_1(x)$ is $f'(x) > 0$, $R_2(x)$ is $f'(x) = 0$, and $R_3(x)$ is $f'(x) < 0$. The case involving R_2 is immediate by the induction hypothesis since $\deg f' = n$ and the leading coefficient divides c since n is a unit in our field. The case involving R_3 reduces to that involving R_1 by replacing f by $-f$. To do the case involving R_1 we define $g_0 = f'$ and use the following lemma.

Lemma 9.8. *Let $g_0 = f'$, the derivative of f with respect to x, and let c be divisible by the leading coefficients of f and all g_i. Then the predicate*

$$(\exists x)[c \neq 0 \wedge f = 0 \wedge g_0 > 0 \wedge \cdots \wedge g_q > 0]$$

is equivalent to the disjunction of the following predicates where i, j, and k run from 0 to q.

A(i,j): *$c \neq 0$ and there exist y and z such that*
- (1) $y < z$
- (2) $g_i(y) = 0$.
- (3) $g_j(z) = 0$.
- (4) *For $k = 0, \ldots, q$, g_k is never 0 on (y, z).*
- (5) *For $k = 0, \ldots, q$, $g_k(\frac{y+z}{2}) > 0$.*
- (6) *$f(y) < 0$ and $f(z) > 0$.*

B(i): *$c \neq 0$ and there exists y such that*
- (2) $g_i(y) = 0$.
- (4) *For $k = 0, \ldots, q$, g_k is never 0 on (y, ∞).*
- (5) *For $k = 0, \ldots, q$, $g_k(y + 1) > 0$.*
- (6) *$f(y) < 0$ and $f(v) > 0$ for $v >> 0$.*

C(j): *$c \neq 0$ and there exists z such that*
- (3) $g_j(z) = 0$.
- (4) *For $k = 0, \ldots, q$, g_k is never 0 on $(-\infty, z)$.*
- (5) *For $k = 0, \ldots, q$, $g_k(z - 1) > 0$.*
- (6) *$f(u) < 0$ for $u << 0$ and $f(z) > 0$.*

D: *$c \neq 0$ and*
- (4) *For $k = 0, \ldots, q$, g_k is never 0.*
- (5) *For $k = 0, \ldots, q$, $g_k(0) > 0$.*
- (6) *$f(u) < 0$ for $u << 0$ and $f(v) > 0$ for $v >> 0$.*

Proof. Suppose all variables except x have been assigned values in a real closed field F in such a way that $c \neq 0$. If one of the itemized predicates holds, then by (4) and Theorem 9.1(2), each g_i is of constant sign on the interval (y, z) (or (y, ∞), $(-\infty, z)$, $(-\infty, \infty)$ in cases B, C, or D). Therefore by (5) we have $g_i > 0$ on (y, z) for all i. By condition (6), f changes sign on this interval so by Theorem 9.1(2), f has a zero in the interval and all g_k are positive there. Conversely, suppose that x exists. Partition F into intervals as in the proof of Lemma 9.5 (using also the roots of g_0). As in that proof we let x lie in the interval $(y, z) = (a_\mu, a_{\mu+1})$ and observe that conditions (1) to (5) hold as before. Since $g_0 = f' > 0$ on our interval and

$y < x < z$, Theorem 9.1(3) implies that $f(y) < 0$ and $f(z) > 0$ showing that (6) holds. □

Proof of Lemma 9.6. As in the proof of Lemma 9.5 we assume the induction hypothesis for n and suppose $\deg f \leq n+1$ and $\deg g_k \leq n$ for all k including 0. Then the numbered conditions are all equivalent to quantifier–free predicates in y and z. For (4) we use Lemma 9.2 and the induction hypothesis as before while for (6) we use Corollary 9.4 which does not require the induction hypothesis. The rest of the proof is exactly the same as that of Lemma 9.5 □

This completes the proof of Tarski's theorem.

10. Real closed fields

For completeness the present section gives proofs for the classical results on real closed fields used above following [1]. Recall that a field F is called real or formally real if $\sum a_i^2 = 0$ in F implies that all $a_i = 0$. This implies that the field has characteristic 0. The field F is called real closed if it is real and no proper algebraic extension of F is real. Any real field F has a real closure, an algebraic extension of F which is real closed. Just take a maximal real extension of F in the algebraic closure of F. The standard example of a real closed field is, of course, $\mathbb{R}$ the field of real numbers.

Lemma 10.1. *Let F be a real field and let $a \in F$ be non–zero. Then $F(\sqrt{a})$ is real if and only if $-a$ is not a sum of squares in F.*

Proof. If $F(\sqrt{a})$ is real and $-a = \sum c_i^2$ then $b^2 + \sum c_i^2 = 0$ where $b = \sqrt{a}$ so $b = 0$. Conversely if $F(\sqrt{a})$ is not real we can write $\sum (x_i + y_i\sqrt{a})^2 = 0$ where not all $y_i = 0$. This implies $\sum x_i^2 + a\sum y_i^2 = 0$ so $-a = (\sum x_i^2)(\sum y_i^2)/(\sum y_i^2)^2$ which is a sum of squares. □

If F is real closed, $F(\sqrt{a})$ will be real if and only if a is a square in F, otherwise $F(\sqrt{a})$ would be a proper algebraic extension of F which is real.

Corollary 10.2. *Let F be a real closed field and let $a \in F$ be non–zero. Then a is a square in F if and only if $-a$ is not a sum of squares in F.*

Theorem 10.3. *If F is real closed it has a unique ordering and the positive elements are the non–zero squares.*

Proof. An ordering of a field F can be specified by giving $P = \{x | x \geq 0\}$ satisfying the conditions: $P \cap -P = \{0\}$, $P \cup -P = F$, $P + P \subseteq P$, and $PP \subseteq P$. Clearly P contains all sums of squares. But a sum of squares $\sum a_i^2$ is already a square otherwise Corollary 10.2 would show that $-\sum a_i^2 = \sum b_j^2$ which implies that all a_i and b_j are zero. Tha same reasoning shows that one of a and $-a$ must be a square and that if both are squares then $a = 0$. Therefore the set of squares satisfies the conditions above so the field is ordered. Any P contains the squares and can be no larger without violating $P \cap -P = \{0\}$ so the ordering is unique. □

The following result is often referred to as the Weierstrass Nullstellensatz.

Theorem 10.4. *Let F be a real closed field and let $f(x)$ be a polynomial over F. Let $a, b \in F$ with $a < b$. If $f(a) < 0$ and $f(b) > 0$ then $f(c) = 0$ for some c satisfying $a < c < b$.*

Proof. It will suffice to show that f has a root c in F. It is then easy to see that f has a root between a and b. If $c < a$ write $f(x) = (x - c)g(x)$. Then $g(a) < 0$ and $g(b) > 0$ so by induction on the degree we can assume that g has a root between a and b. A similar argument applies if $c > b$.

To prove that f has a root in F we adapt the argument of [1, Satz 2]. We use induction on the degree n of f. Write f as a product of irreducible polynomials. One of these must change sign in going from a to b. Therefore we can assume f is irreducible. If f has no root in F then $E = F[X]/(f(X))$ is a proper algebraic extension of F and so is not real. Therefore, if α is the image of X in E we can write $\sum_i(\sum_{j=0}^{n-1} a_{ij}\alpha^j)^2 = 0$ in E where not all $a_{ij} = 0$. Let $g_i(X) = \sum_{j=0}^{n-1} a_{ij}X^j$. Then we have an equation $\sum_i g_i(X)^2 = f(X)h(X)$ with not all $g_i = 0$. Choose such an equation with $\deg h$ least. Note $\deg h \leq n-2$ since $\deg g_i < n$ and $\deg f = n$. Now $f(a)h(a) \geq 0$ and $f(b)h(b) \geq 0$ so either $h(a) = 0$ or $h(b) = 0$ or h changes sign in going from a to b. By the induction hypothesis, h has a root r in F. Therefore $\sum_i g_i(r)^2 = 0$ so all $g_i(r) = 0$. It follows that we can write $g_i(X) = (X - r)k_i(X)$ in $F[X]$ getting $(X - r)^2 \sum_i k_i(X)^2 = f(X)h(X)$. Since f has no root in F, this implies that $(X - r)^2$ divides h so $h(X) = (X - r)^2 h_1(X)$ and we get an equation $\sum_i k_i(X)^2 = f(X)h_1(X)$ contradicting the choice of h as having the least possible degree. □

Theorem 10.5 (Rolle's Theorem)**.** *Let F be a real closed field and let $f(x)$ be a polynomial over F. Let $a, b \in F$ with $a < b$. If $f(a) = 0$ and $f(b) = 0$ then $f'(c) = 0$ for some c satisfying $a < c < b$.*

Proof. We follow the proof in [13, §114] .We can assume that f has no zero between a and b. Write $f(X) = (X - a)^p(X - b)^q g(X)$ where g is not zero at a or b. Therefore g is not zero on the closed interval $[a, b]$ and so is of constant sign on that interval by the previous theorem. Now $f'(X) = (X - a)^{p-1}(X - b)^{q-1}h(X)$ where $h(X) = p(X - b)g(X) + q(X - a)g(X) + (X - a)(X - b)g'(X)$. We have $h(a) = p(a - b)g(a)$ and $h(b) = q(b - a)g(b)$ so $h(a)$ and $h(b)$ have opposite signs. Therefore h has a root c with $a < c < b$ by the previous theorem. □

Corollary 10.6 (The mean value theorem)**.** *Let F be a real closed field and let $f(x)$ be a polynomial over F. Let $a, b \in F$ with $a < b$. Then $f(b) - f(a) = (b - a)f'(c)$ for some c satisfying $a < c < b$.*

This follows by the familiar proof of elementary calculus.

Corollary 10.7. *Let F be a real closed field and let $f(x)$ be a polynomial over F. Let $a, b \in F$ with $a < b$. If $f'(c) > 0$ for all c satisfying $a < c < b$ then $f(b) > f(a)$.*

The following is not needed in the proof of Tarski's theorem but is included since it was mentioned in section 4.

Theorem 10.8. *Let F be an ordered field. Then F has a real closure whose ordering agrees with that of F.*

This real closure is unique as was shown in section 4. To prove the theorem it will suffice to extend F to a real field E such the each positive element of F is a square in E. Then any real closure of E will do.

Lemma 10.9. *Let F be an ordered field. Let E be the field obtained from F by adjoining the square roots of all positive elements of F. Then E is real.*

Proof. It is sufficient to show that finitely generated subfields of E are real. Let $K = F(\sqrt{a_1}, \dots, \sqrt{a_n})$ where the a_i are positive elements of F. We can assume no $\sqrt{a_i}$ is superfluous so $|K : F| = 2^n$. A base for K as a vector space over F is given by the elements $e_I = \sqrt{a_I}$ where $I \subseteq \{1, \dots, n\}$ and $a_I = \prod_{i\in I} a_i$. Write $I \oplus J$ for the set of i lying in exactly one of I and J. Then $e_I e_J = a_{I\cap J} e_{I\oplus J}$. Suppose that $\sum_\alpha (\sum_I c_I^{(\alpha)} e_I)^2 = 0$ where the $c_I^{(\alpha)}$ lie in F. The coefficient of $e_\emptyset$ in this sum is $\sum_{I,\alpha} (c_I^{(\alpha)})^2 a_I = 0$. Since all term of this sum are positive, all $c_I^{(\alpha)} = 0$ as required. □

References

1. E. Artin and O. Schreier, Algebraische Konstruktion reelle Körper, Abh. Math. Sem. Univ. Hamburg 5(1927), 85–99.
2. E. Artin, Über die Zerlegung definiter Funktionen in Quadrate, Abh. Math. Sem. Univ. Hamburg 5(1927), 100–115.
3. D. Dubois, A Nullstellensatz for ordered fields, Arkiv för Mat. 8(1969), 111–114.
4. D. Dubois and E. Efroymson, Algebraic theory of real varieties, in Studies and Essays presented to Yu–Why Chen on his 60th birthday, Math. Res. Center, Nat. Taiwan Univ, Taipei, 1970, pp.107–135.
5. D. Gondard and P. Ribenboim, Fonctions définie positives sur les variétés réelles, Bull. Sci. Math. 98(1974), 39–47.
6. G. Kreisel and J–L. Krivine, Elements of Mathematical Logic. Model Theory, North Holland Publ. Co., Amsterdam 1967.
7. S. Lang, The theory of real places, Ann. Math. 57(1953), 378–391.
8. The theory of ordered fields, pp. 1–152 in Ring Theory and Algebra III (ed. B. McDonald), Proc. of Algebra Conf. at Univ. of Oklahoma, M. Dekker 1980.
9. An introduction to real algebra, Rocky Mountain J. Math. 14(1984),767–814.
10. J–J. Risler, Une charactérization des idéaux des variétés algébriques réelles, C. R. Acad. Paris 271(1970), 1171–1173.
11. R. G. Swan, Topological examples of projective modules, Trans. Amer. Math. Soc. 230 (1977), 201–234.
12. A. Tarski, A decision method for elementary algebra and geometry, Rand Corporation Publication 1948.
13. H. Weber, Lehrbuch der Algebra, vol. I, Chelsea, New York.

Department of Mathematics, The University of Chicago, Chicago, IL 60637
E-mail address: swan@math.uchicago.edu