Hilbert seventeenth problem:Sums of squares

Tian Zi'ang

February 25, 2024

Contents

1 Artin-Schreier theory of real algebra

What's the meaning of 'real'?Yes,it's about real numbers.R denotes the field of real numbers.In analysis,R is a completion of the field of rational numbers.We have a relation $<$ in R which gives the completeness axiom that a subset of R which has an upper bound has a least upper bound.We will care about the polynomial functions over R,hence we will introduce a new concept:real closed field.

1.1 ordered field

Definition 1.1.1. *For a field F,a positive cone is a subset $P \subset F$ such that for any $a, b \in P$*

$$a + b \in P$$

$$a \times b \in P$$

$$0 \in P$$

And if $c \in F$ then either $c \in P$,c=0,or $-c \in P$.

Now,if we get P for a positive cone,we can define $a > b$ meaning that $a - b \in P$ and $a - b \neq 0$. Then,if $a > b$,we have $a + c > b + c$ for any $c \in F$,and $ap > bp$ for any $p > 0$.

Definition 1.1.2. *An ordered field (F,P) is a field F and a positive cone P.*

Any ordered field (F,P),$a \in F$ and $a \neq 0$,then we have $a^2 > 0$.So if we pick $a_1, a_2, ...a_r \neq 0$,we have $\sum a_i^2 \neq 0.1+1+1+...+1 = 1^2+1^2+1^2+...1^2 \neq 0$,hence any ordered field must be characteristic 0.

Example 1.1.3. *The field of complex numbers C,there exists $1^2 + \sqrt{-1}^2 = 0$,hence C is not orderable. The field of real numbers R,from the completeness axiom,is orderable.*

Definition 1.1.4. *A pre-positive cone of a field F is a subset $P \subset F$ such that for arbitrary $a, b \in P$:*

$$a + b \in P$$

$$a \times b \in P$$

$$-1 \notin P$$

And $x^2 \in P$ for all $x \in F$.

Corollary 1.1.4.1. *Any positive cone is pre-positive cone.*

Proof. The first and second is from the definition of positive cone.$1 = 1^2 > 0$,then$-1 < 0.a^2 > 0$. □

Theorem 1.1.1. *Any pre-positive cone P_0 of a field F,we have a positive cone P such that $P_0 \subset P$.*

Lemma 1.1.2. *If P is a pre-positive cone of F,then for any $x \in F$,$Px \cap (1 + P) = \{cx|c \in P\} \cap \{1 + d|d \in P\} = \emptyset$,or$-Px \cap (1 + P) = \{-cx|c \in P\} \cap \{1 + d|d \in P\} = \emptyset$.*

Proof of lemma. We use contradiction to proof.Suppose the two intersection are both not empty,there exists $c_1, c_2, d_1, d_2 \in P$,such that

$$c_1 x = 1 + d_1$$

$$-c_2 x = 1 + d_2$$

Hence,we have:$-c_1 c_2 x^2 = 1 + d_1 + d_2 + d_1 d_2$.
That is $-1 = c_1 c_2 x^2 + d_1 + d_2 + d_1 d_2$
The righthandside of the equation is in P(by the definition of pre-positive cone),but $-1 \notin P$,contradiction. □

Proof of theorem. We denote $\mathfrak{A}$ to be the set of pre-positive cones $P_0 \subset P' \subset F$.And $\mathfrak{A} \neq \emptyset$ because $P_0 \in \mathfrak{A}$.The union of a chain in $\mathfrak{A}$ is a pre-positive cone.By Zorn's Lemma,there exists a maximal member P.From Lemma 1.1.2,for $x \in F$,if $Px \cap (1+P) = \{cx|c \in P\} \cap \{1+d|d \in P\} = \emptyset$,we consider $P_1 = P - Px = \{a - bx|a, b \in P\}$,then $-1 \notin P_1$.

$$(a_1 - b_1x) + (a_2 - b_2x) = (a_1 + a_2) - (b_1 + b_2)x$$

$$(a_1 - b_1x)(a_2 - b_2x) = (a_1a_2 + b_1b_2x^2) - (a_1b_2 + a_2b_1)x$$

$$x^2 \in P_1 \Longleftarrow 0 \in P$$

Hence P_1 is also a pre-positive cone,$P \subset P_1$.For P is the maximal,P=P_1.Then,$-x \in P$.On the other hand,$-Px \cap (1+P) = \{-cx|c \in P\} \cap \{1+d|d \in P\} = \emptyset$ implies $x \in P$.P is a positive cone. □

This theorem is very useful in the next subsection.

1.2 formally real field

All above,we give a field an good ordering by positive cone.And we see that $\sum a_i^2 > 0$ when $a_1, a_2, ...a_r \neq 0$,in an ordered field.Then, -1 is never a sum of squares.In 1926, Artin-Schreier gave the theory of formally real field,which is the essential part of Hilbert seventeenth problem.

Definition 1.2.1. *A formally real field is a field F in which -1 is not a sum of squares.*

Theorem 1.2.1. *A field F is an ordered field (by a positive cone P) if and only if is formally real.*

Proof of Theorem 1.2.1. In an ordered field F,$\sum a_i^2 > 0 > -1$,hence F is formally real field.In a formally real field F,We consider $\mathfrak{A}$ to be the set of

sums of squares in F(like$\sum a_i^2$).By the definition of formally real field,$-1 \notin \mathfrak{A}$.

$$(\sum a_i^2)(\sum b_i^2) = \sum (a_i b_j)^2$$

And $\mathfrak{A}$ is closed under addition.We see that $\mathfrak{A}$ is a pre-positive cone of F.By theorem 1.1.1,there exists $\mathfrak{A} \subset A_0$,A_0 is a positive cone of F,F is ordered field. □

1.3 real closed field

The concept of real closed fields made a great impact in real algebraic geometry,model theory,theory of hypereal numbers.Alfred Tarski proved (c.1931) that the first-order theory of real closed fields is complete, and decidable.Also,the model theorists use this to research the generalized continuum hypothesis.In particular,the main result is the Hilbert's seventeenth problem.

Definition 1.3.1. *A field R is called real closed field if R is formally real field and no proper algebraic extension of R is formally real.(Artin-Schreier version)*

In fact,there are so many different definitions of real closed field.All of them is from different opinions,
like model theory:Any sentence in the first-order language of fields is true in F if and only if it is true in the reals(real numbers).
algebraic geometry:There is a total order on R making it an ordered field such that, in this ordering, every positive element of R has a square root in R and any polynomial of odd degree with coefficients in R has at least one root in R. These equivalence will be in the paper later.

Theorem 1.3.1 (Artin-Schreier)**.** *The following are equivalent.*
(1)A field R is real closed
(2)R is ordered ,every positive element of R has a square root in R ,every polynomial of odd degree in one indeterminate with coefficient in R has a root

in R.

(3)R($\sqrt{-1}$) is algebraic closed and R$\neq$ R($\sqrt{-1}$).

Lemma 1.3.2. *If F is formally real field.F(r) is formally real field if either r=$\sqrt{a}$ where $a > 0$ in F or r is algebraic over F with minimum polynomial of odd degree.*

Proof. (1) r=$\sqrt{a}$,$a > 0$.We use the contradiction.Suppose F(r) is not formally real,then $-1 = \sum_1^n (a_i + rb_i)^2$,where $a_i, b_i \in F$.

$$-1 = (\sum_1^n a_i^2 + a\sum_1^n b_i^2) + r(2\sum_1^n a_i b_i)$$

For $a > 0$,$\sum_1^n a_i^2 + a\sum_1^n b_i^2 \neq -1$.This is impossible,contradiction.
(2)we pick the minimum polynomial f(x) of r.deg f(x)=m,m is odd.We use induction on m.We also use contradiction to prove.Suppose F(r) not formally real.$-1 = \sum_1^n g_i(r)^2$,where g_i is polynomial of r with degree $< r$.Hence we have $\sum_1^n g_i(x)^2 = -1 + f(x)g(x)$,$g(x) \in F[x]$.

$$deg(-1 + f(x)g(x)) = deg(\sum_1^n g_i(x)^2) < 2m$$

.Hence $deg(g(x)) < m$.By induction,g(x) has an irreducible factor h(x) of degree odd.Pick s to be a root of h(x),F(s) formally real field.Since g(s)=0,We get $\sum_1^n g_i(s)^2 = -1$.contradiction. □

Proof of Theorem1.3.1. (1) $\Longrightarrow$ (2) If R is real closed field.From the lemma 1.3.2,R(r) is formally real,where $r = \sqrt{a}, a > 0$ in R.But There is no proper algebraic extension of R satisfying that it's formally real.Hence $\sqrt{a} \in R$.Any

polynomial of odd degree g(x),there exists an irreducible h(x) with degree odd.Pick s to be a root of h(x).R(s) is formally real,hence $s \in R$.

(2) $\Longrightarrow$ (3)(fundamental theorem of algebra)

We put i=$\sqrt{-1}$.There is an automorphism $r = a+bi \to \bar{r} = a-bi$.C=$R(\sqrt{-1})$.If $f(x) \in C[x]$,then $f(x)\bar{f(x)} \in R[x]$.We only need to prove :Any monic polynomial g(x) with coefficient in R has a root in C.This is proved if deg(g(x)) is odd.

$$(x+yi)^2 = r = a+bi, x, y, a, b \in R$$

By multiplying some element of R,we may assume b=1.Hence $y = x^{-1}$.

$$x^2 - x^{-2} = a, z = x^2, z^2 - az - 1 = 0$$

Now,there exists $x^2 = \frac{1}{2}(a + \sqrt{a^2+4}) > 0$.Hence any element of C ,its square root in C.Let E be a splitting field of f(x)(x^2+1).Since R is characteristic 0,E is Galois over R.G=Gal(E/R),$|G| = 2^e m$,m is odd.By Sylow's theorem,there exists a subgroup H,$|H| = 2^e$.There exists a corresponding field D,[E:D]=2^e,[D:R]=m.m is odd,only m=1.Hence D=R.If $e > 1$,from Galois theory,there exists subfield F [F:C]=2,but any element in C has a square root,contradiction.Hence e=1,E=C.C contains a root of f(x),C is algebraically closed.

(3) $\Longrightarrow$ (1)C=R($\sqrt{-1}$).$R \subsetneq C$.C is algebraically closed,any algebraic extension of R is a subfield of C/R.Hence proper algebraic extension is C,$i^2 = -1$,not formally real. □

Theorem 1.3.3 (intermediate value theorem for polynomials)**.** *Let R be a real closed field,$f(x) \in R[x]$.Suppose a,b are elements in R,$f(a)f(b) < 0$,then there exists a 'c' between a,b such that f(c)=0.*

Proof. We may assume f(x) is monic.Then $f(x) = (x-r_1)...(x-r_m)g_1(x)...g_n(x)$.

Where

$$g_i(x) = x^2 + a_i x + b_i, c_i^2 < 4d_i$$

This result is directly from the fundamental theorem of algebra,which has been proved in Theorem 1.3.1.

$$g_i(x) = (x + \frac{1}{2}c_i)^2 + \frac{1}{4}(4d_i - c_i^2) > 0$$

If any i,$r_i > a, b$,or $r_i < a, b \implies f(a)f(b) > 0$ contradiction.
Hence there exists r_i between a and b.$c = r_i$. □

In 1836,J.S.F.Sturm gave the classical theorem.Here I followed Jacobson's expression in *Basic Algebra*,Vol 1,pp.312.

Definition 1.3.2. *A Strum sequence of f(x) in* $[a, b]$ *is* $f_0(x) = f(x), f_1(x), ...f_m(x)$,*such that*
(1)f_m *has no root in [a,b]*
(2)$f_0(a)f_0(b) \neq 0$
(3)If $c \in [a, b]$ *is a root of* $f_j(x)$,$0 < j < s$,*then* $f_{j-1}(c)f_{j+1}(c) < 0$
(4)If $f(c) = 0$ *for* c*∈[a,b],there exists* $c_1 < c < c_2$,*such that* $f_0(u)f_1(u) < 0, u \in (c_1, c)$,*and* $f_0(u)f_1(u) > 0, u \in (c, c_2)$.

Theorem 1.3.4 (Sturm)**.** *Let R be a real closed field.Let* $f_0(x) = f(x), f_1(x), ...f_m(x)$ *be a Strum sequence for f(x) in [a,b].Then the number of distinct roots of f(x) in (a,b) is* $V_a - V_b$.*In general,*V_c *denotes the number of variations in sign of the sequence* $\{f_0(c), ..., f_m(c)\}$

Proof of Sturm's theroem. Pick a sequence $a = a_0 < a_1 < ... < a_n = b$,such that none of $f_j(x)$ has a root in (a_i, a_{i+1}).
Let $c \in (a_0, a_1)$ so no f_j has a root in (a_0, c).By Theorem 1.3.3,$f_j(a_0)f_j(c) \geqslant 0$ for $0 \leq j \leq m$.If$f_j(a_0) \neq 0$,we have $V_{a_0} = V_c$.If $f_j(a_0) = 0$,by (3) of the

definition1.3.2,$f_{j-1}(a_0)f_{j+1}(a_0) < 0$.Thus $f_{j-1}(a_0), 0, f_{k+1}(a_0)$ and $f_{k-1}(c), f_k(c), f_{k+1}(c)$ have same variation of sign.Hence $V_{a_0} = V_c$.

Similarly,if $d \in (a_{i-1}, a_i)$,then $V_d = V_{a_i}$.Now, suppose $f(a_i) = 0$.By (4) of definition 1.3.2,$f_0(c)f_1(c) < 0$ and $f_0(d)f_1(d) > 0$.Hence $V_c - V_d = 1$ if $f_(a_j) = 0$.Hence $V_a - V_b$ is the number of roots of f(x). □

Corollary 1.3.2.1. *Let $f_0(x) = f(x)$, $f_1(x) = f^{'}(x)$(formal derivative of f(x)). We modify the Euclid algorithm for finding g.c.d of f(x) and $f^{'}(x)$,and at each stage is the negative of remainder.This is a Sturm sequence,we call it standard sequence for f(x).*

1.4 real algebraic closure

Also,Artin and Schreier gave a great result here,they used Sturm's theorem to prove the existence and uniqueness of real algebraic closure.

Definition 1.4.1. *R is a real algebraic closure of an ordered field (F,P) if:*
(1)R is real closed
(2)R is algebraic over F
(3)$P \subset R^2$

Theorem 1.4.1. *Any ordered field has a real closure.*

Existence of real closure. Let F denote the ordered field,K denote the algebraic closure of F. Consider the set of pairs $(F^{'}, P^{'})$,$F \subset F^{'} \subset K$ and $P \subset P^{'}$,where $(F^{'}, P^{'})$ is ordered field. By Zorn's lemma,there exists a maximal element (R,P_0).We claim R is real closed.Otherwise,there exists $R^{'}$ is a proper algebraic extension of R,but R is the maximal one($R^{'}$ is formally real and algebraic extension of F), contradiction.Hence R is real closed and algebraic over F.Let E be the subfield of $\bar{F}$,obtained by adjoining to F the square roots of all positive element of F.E is formally real,otherwise $\sum a_i^2 = -1$,a_i

in the subfield,using Lemma 1.3.2,E is formally real .$E \subset R$,$P \subset E^2 \subset R^2$ .Hence there exists R is real closure of F. □

Lemma 1.4.2. *Let $R_i, i = 1, 2$,be a real closed field,F_i a subfield of R_i,$a \to \bar{a}$ an order isomorphism of F_1 onto F_2,where the order of F_i is inherited from R_i.$f(x) \in F_1[x]$,and f(x) is monic.f(x) in R_1 and $\bar{f}(x)$ in R_2 have the same number of the root.*

Proof of the lemma. f(x)=x^n+a_1x^{n-1}...+a_n.Let M=1+|a_1|+...+|a_n| Then,by Sturm's theorem,first number is $V_{-M} - V_M$,second number is $V_{-\bar{M}} - V_{\bar{M}}$.Since the order isomorphism,both number of the roots is same. □

Theorem 1.4.3 (Artin-Schreier)**.** *Any ordered field has a unique (up to isomorphism) real closure.*

Lemma 1.4.4. *Any ordered fields F_1 and F_2 with real closure R_1 and R_2 respectively.Then any order isomorphism of F_1 to F_2 can be extended uniquely to an isomorphism of R_1 to R_2,which preserves order.*

Proof of lemma 1.4.4. We let the order isomorphism be $\theta : a \to \bar{a}$ from F_1 to F_2.We define a map f from R_1 to R_2:Any $r \in R_1$,there exists a minimum polynomial $g(x) \in F_1[x]$,let $r_1 < r_2 < ... < r_k = r < ... < r_n$ be the distinct roots of $g(x)$.By lemma 1.4.2,the polynomial $\bar{g}(x)$ has n roots,f(r) is the k th root of $\bar{g}(x)$.f is bijective and an extension of $a \to \bar{a}$.Now we want to prove:f is an isomorphism.For any finite set $S \subset R_1$,there exists a subfield E_1 of R_1/F_1 and a monomorphism η of E_1/F_1 onto R_2/F_2 that extends θ and preserves the order of the elements of S.($S = \{s_1 < s_2 < ... < s_n\}$,then $\eta s_1 < \eta s_2 < ... < \eta s_n$).$T = S \cup \left\{\sqrt{s_{i+1} - s_i} | i = 1, 2, ...n-1\right\}$.Let $E_1 = F_1(T)$,E_1 is finite dimensional over F_1,so $E_1 = F_1(\omega)$,let $g(x)$ be the minimum polynomial of

ω.By lemma 1.4.2,$\bar{g}(x)$ has a root $\bar{\omega}$,hence we have $\eta(\omega) = \bar{\omega}$.

$$\eta(s_{i+1}) - \eta(s_i) = \eta(s_{i+1} - s_i) = \eta(\sqrt{s_{i+1} - s_i})^2 = (\eta\sqrt{s_{i+1} - s_i})^2 > 0$$

.Now,for any x,y in E_1,$S = \{x, y, x + y, xy\}$.

$$f(x + y) = \eta(x + y) = \eta(x) + \eta(y) = f(x) + f(y)$$

$$f(xy) = \eta(xy) = \eta(x)\eta(y) = f(x)f(y)$$

.Hence f is an isomorphism. □

Theorem 1.4.3. By lemma 1.4.4,let $F_1 = F_2 = F$,R_1, R_2 be two different real closure,the identity map can be extended to two real closure.Hence they are same real closure. □

1.5 characterization of real closed fields

We have proved the fundamental theorem of algebra in real closed field. Now,we will prove a stronger one.

Theorem 1.5.1. *Let C be a algebraically closed field,R a proper subfield of finite codimension in C:$[C : R] < \infty$.Then R is real closed and $C = R(\sqrt{-1})$.*

We need some lemma to prove this.

Lemma 1.5.2. *Let F be a field of characteristic p,a an element of F that is not pth power.Then for any $e \geq 1$,the polynomial $x^{p^e} - a$ is irreducible in $F[x]$.*

Proof. If E is a splitting field of $x^{p^e} - a$,then we have the factorization $x^{p^e} - a = (x - r)^{p^e}$ in E[x].Hence if $g(x)$ is a monic factor of $x^{p^e} - a$ in F[x],$r^k \in F$ and $r^{p^e} = a \in F$.Let $p^f = (p^e, k)$,we have: $p^f = mp^e + nk$.Then $r^{p^f} =$

$(r^{p^e})^m(r^k)^n \in F$

If b=r^{p^f},then $b^{p^{e-f}} = a$,hence a is a pth power in F,contradiction. □

Lemma 1.5.3. *If F be a field of characteristic p and $a \in F$ is not of the form $u^p - u$,$u \in F$,then $x^p - x - a$ is irreducible in F[x].*

Proof. If r is a root of $x^p - x - a$ in E[x],E is a splitting field,then r+1,...,r+(p-1) are also roots of $x^p - x - a$.Hence we have :

$$x^p - x - a = \prod_{i=0}^{p-1}(x - r - i)$$

If g(x)=$x^k - bx^{k-1} + ...$ is a factor of $x^p - x - a$,then $kr + l1 = b$ where l is an integer.Hence $r \in F$.Since $r^p - r = a$,contradiction. □

Lemma 1.5.4. *Let F and a be same as lemma 1.5.3.Let E be a splitting field for $x^p - x - a$.Then there exists an extension field K/E such that $[K : E] = p$.*

Proof. We have $E = F(r)$ where $r^p = r + a$.We claim that the element $ar^{p-1} \in E$ is not of the form $u^p - u$,$u \in E$.Let:

$$u = u_0 + u_1 r + ... + u_{p-1} r^{p-1}$$

And $u^p - u = ar^{p-1}$ and $r^p = r + a$ give that:

$$u_0^p + u_1^p(r + a) + u_2^p(r + a)^2 + ... + u_{p-1}^p(r + a)^{p-1}$$

$$-u_0 - u_1 r - ... - u_{p-1} r^{p-1} = ar^{p-1}$$

Since $(1, r, ..., r^{p-1})$ is a base,we have $u_{p-1}^p - u_{p-1} = a$,contradiction. By lemma 1.5.3,$x^p - x - ar^{p-1}$ is irreducible in E[x].Hence [K:E]=p. □

Proof of theorem 1.5.1. Let $C^{'} = R(\sqrt{-1}) \subset C$.C is algebraic closure of $C^{'}$.Any algebraic extension of $C^{'}$ is isomorphic to a subfield of $C/C^{'}$.

By lemma 1.5.2,there exists an algebraic extension of $C^{'}$ that is p^e-dimensional for any e.

Then C is separable algebraic over $C^{'}$,C is finite dimensional over $C^{'}$,it's Galois.

Let G=Gal$(C/C^{'})$.

Now we suppose $C \neq C^{'}$,then $|G| \neq 1$.Let p be a prime divisor of $|G|$.Then G has a cyclic subgroup H of order p.E is the correspondence subfield.If char is p,then C=E(r),where r has minimum polynomial:$x^p - x - a$.By lemma 1.5.4,there exists a p-dimension extension of C but C is algebraic closed.

Hence the char is not p.C contains p distinct root of unity.Now we consider:

$$x^{p^2} - a$$

which factor is $\prod_{i=1}^{p^2}(x - u^i s)$where u is a primitive p^2-root of unity.And $s^{p^2} = a$.If any $u^i s \in E$ and $((u^i s)^p)^p = a$.contradiction.

Let P be the prime field of C and consider the subfield P(v) of C where v is a primitive p^2-root of unity.If P=Q,,we know that cyclotomic field of p^rth roots of unity has dimensionality $\phi(p^r)$ over Q.

By [12] p.291,there exusts K is cyclic:K=Gal(P(w)/P),where w is a primitive p^{r+1}st root of unity.By Galois's correspondence,P(w) contains only one subgroup of order p.Hence $p = 2$ and char is 0.

Let h(x) be the minimum polynomial of w over E.Since $v \notin E$,$w \notin E$ and C=E(w).Hence deg(h(x))=p.Moreover,h(x) is a divisor of $x^{p^{r+1}} - 1 = \prod_{1}^{p-1}(x - w^i)$,so the coefficient of h(x) are contained in the subfield $D = E \cap P(w)$.$[P(w) : D] = p$.

By [11],we get $\sqrt{-1} \notin E$,[C:E]=2.Hence we complete the proof. □

2 Model theory of real closed field

Tarski first showed completeness and decidability for the fields of real and complex numbers. His proof gave an explicit algorithm for eliminating quantifiers.Robinson showed that quantifier-elimination results could be proved by finding the right embedding theorems. These ideas were further extended by Blum.Robinson also introduced the notion of model completeness and saw how it could be used to answer Hilbert's 17th-problem. The main result of this section is:the model of real ordered closed field is complete.And the Tarski-Seidenburg Principle is important.We assume the first order logic in our proof.

2.1 model theory background :Quantifier elimination

We will begin with some definitions in model theory.The main target of this subsection is to introduce a little model theory.Hence if you want to know more about model theory,you can see David Marker's book Model theory:An introduction.

Definition 2.1.1. *Let T be a set of sentences in L(language) and let A be an L structure. We say that A is a model of T, and write $A \models T$, if every sentence in T is true in A.We say a theory is satisfiable if it has a model.*

Definition 2.1.2. *If M,N are L-structures,M is an elementary submodel of N,denote $M \prec N$,if $M \subset N$ and any formula $\phi(\bar{x})$ and $\bar{a} \in M$,$M \models \phi(\bar{a}) \leftrightarrow N \models \phi(\bar{a})$.*

Definition 2.1.3. *A theory T is model complete if for every $M, N \models T$,$M \subset N \implies M \prec N$.*

Theorem 2.1.1 (Tarski-Vaught test)**.** *Let B be an L-structure and suppose $A \subset B$. Then A is the underlying set of an elementary substructure of B if and only if for every formula $\psi(x_1, ..., x_m, y)$ in L and every sequence $a_1, ..., a_m$ in A, if $B \models \exists y \psi[a_1, ..., a_m]$, then there exists $b \in A$ such that $B \models \psi[a_1, ..., a_m, b]$*

Definition 2.1.4. *A theory T admits Quantifier elimination if for any formula $\phi(x_1, x_2, ...x_n)$ in the language of T,there exists a quantifier free formula $\psi(x_1, x_2, ...x_n)$,such that $T \models \forall \bar{v}[\phi(\bar{v}) \leftrightarrow \psi(\bar{v})]$.*

Theorem 2.1.2. *Let L be a language containing at least one constant symbol. Let T be an L-theory and let $\phi(x_1, ..., x_m)$ be an L-formula (with free variables $x_1, ..., x_m$, m may be 0).The following are equivalent:*
1. There is a quantifier free L-formula $\psi(x_1, ..., x_m)$ such that $T \vdash \forall \bar{x}(\phi(\bar{x}) \leftrightarrow \psi(\bar{x}))$
2. If M and N are L-structures such that $M, N \models T$, and C is an L structure such that $C \subset M$ and $C \subset N$, then $M \models \phi(\bar{a})$ if and only if $N \models \phi(\bar{a})$ for all $\bar{a} \in C$.

Proof. (1) $\Longrightarrow$ (2):

$$M \models \phi(\bar{a}) \iff M \models \psi(\bar{a}) \iff C \models \psi(\bar{a})$$

Since $C \subset M$ and $\psi(\bar{x})$ is quantifier free.
Similarly,$N \models \phi(\bar{a}) \iff C \models \psi(\bar{a})$,hence $M \models \phi(\bar{a}) \iff N \models \phi(\bar{a})$.
(2) $\Longrightarrow$ (1):we use contradiction.Suppose $\phi(\bar{x})$ is not consistent.Then we have:

$$T \models \forall \bar{x}(\phi(\bar{x}) \leftrightarrow c \neq c)$$

We may assume $\phi(\bar{x})$ is consistent.

Now we define $\gamma(x) = \{\psi(\bar{x})|\psi(\bar{x})$ is quantifier free and $T \vdash \forall\bar{x}(\phi(\bar{x}) \rightarrow \psi(\bar{x}))\}$

Lemma 2.1.3. $T \cup \gamma(\bar{d}) \vdash \phi(\bar{d})$

Proof of lemma. Suppose $T \cup \gamma(\bar{d}) \cup \{\neg\phi(\bar{d})\}$ is satisfiable.There exists a model $M \models T \cup \gamma(\bar{d}) \cup \{\neg\phi(\bar{d})\}$.We pick C to be a substructure of M generated by $\bar{d}$.Since $\gamma(\bar{d})$ is quantifier free,$C \models \gamma(\bar{d})$. Let Diag(C) denote the set of atomic formulas with parameters in C,which are true in C .Let $\sigma = T \cup Diag(C) \cup \{\phi(\bar{d})\}$.
Here we claim σ is satisfiable.If not,$T \cup Diag(C) \models \neg\phi(\bar{d})$.By compactness of model,we can choose $\psi_1(\bar{d}), ...\psi_m(\bar{d}) \in Diag(C)$,$T \models \forall\bar{d}[\wedge_1^n\psi_i(\bar{d}) \rightarrow \phi(\bar{d})]$.

$$\iff T \models \forall\bar{d}[\neg\phi(\bar{d}) \rightarrow \vee_1^m\neg\psi_i(\bar{d})]$$

where $\vee_1^m\neg\psi_i(\bar{d})$ is quantifier free formula,hence $\in \gamma$.Since $C \models \gamma$,$C \models \vee_1^m\neg\psi_i(\bar{d})$,there exists i such that $C \models \neg\psi_i(\bar{d})$,contradiction.Now σ is satisfiable.There exists a model $N \models \sigma$.Hence we have $N \models \phi(\bar{d})$.By (2),

$$M \models \neg\phi(\bar{d}), C \subset M, C \subset N, \bar{d} \in C \implies N \models \neg\phi(\bar{d})$$

.Contradiction. □

Since $T \cup \gamma(\bar{d}) \vdash \phi(\bar{d})$,by compactness ,there exists $\psi_1, ...\psi_m \in \gamma$ where $T \vdash \forall\bar{v}(\wedge_1^m\psi_i(\bar{v}) \rightarrow \phi(\bar{v}))$.Hence we find that $\wedge_1^m\psi_i(\bar{v})$. □

This theorem gives a method to test whether a model is a quantifier elimination.

2.2 real closed field model

First,we will find the language and axioms in real closed field.
Language:$L_R = \{+, \times, -, 0, 1\}$,where $+$ and $\times$ are binary operators,$-$ is the unary operator,0 and 1 are constant.(We may be not to write $\times$)
Axiom:

$$\forall x \forall y \forall z[x(y+z) = xy + xz]$$

$$\forall x \forall y \forall z[x + (y+z) = (x+y) + z]$$

$$\forall x \forall y \forall z[(xy)z = x(yz)]$$

$$\forall x \forall y[x + y = y + x]$$

$$\forall x \forall y[xy = yx]$$

$$\forall x[x + 0 = 0 \wedge x + (-x) = 0]$$

$$\forall x[x \times 1 = x]$$

$$\forall x[(x = 0) \vee (\exists y[xy = 1])]$$

$$\forall x \exists y[y^2 = x \vee y^2 = -x]$$

$$\forall a_0 \forall a_1 ... \forall a_n \exists x[a_n = 0 \wedge a_0 + a_1 x + ... + a_n x^n = 0] \quad for \quad odd \quad n \in N$$

We can find that the first eight axioms are field axioms.The night and ten axioms are theorem 1.3.1 (2).We can define the order $x \leq y$ by $\exists z[x+z^2 = y]$.

Theorem 2.2.1. *The theory of real closed field with language L_R does not admit the quantifier elimination.*

Proof. Let $\phi(x, y)$ be a formula in L_R which is true when $x \leq y$. Let F=Q and x,y be two transcendental numbers over F such that $x, y \notin F$, $x \notin F(y)$ and $y \notin F(x)$.

We consider an order in F(x):

1.for polynomial of rational coefficients is just the lexicographic ordering

2. For rational expression $\frac{p}{q} \leq \frac{r}{s} \iff ps \leq rq$

Now consider F(x) with the lexicographic ordering, call it $\leq_1$.we may say this as an ordered field.Then consider (F(x))(y) with the ordering as above. These are rational functions of y with coefficients from F(x).

Then, x, y $\in$(F(x))(y), and as polynomials of y, x has degree 0 and y has degree 1, so x$\leq_1$y and x$\neq$ y. Then, by applying the same ordering to (F(y))(x), call it $\leq_2$, y $\leq_2$ x and x$\neq$y.

Let R_1 be the real algebraic closure of [F(x,y), $\leq_1$] and R_2 be the real algebraic closure of [F(x,y), $\leq_2$](which uniquely exist since we have proved in subsection 1.4).

$R_1, R_2 \models T_R$ and have a common substructure, F(x,y). But x, y$\in$F(x,y) and $R_1 \models \phi(x,y) \wedge (x \neq y)$ while $R_2 \models \phi(y,x)$, which means $R_2 \models \phi(y,x) \vee (x = y)$, so $R_2 \models \neg(\phi(x,y) \wedge x \neq y)$.

Thus, the negation of (2) in Theorem 2.1.2 holds, so there is no quantifier free formula $\psi(x,y)$ in L for which $T_R \vdash \forall a \forall b[\phi(a,b) \leftrightarrow \psi(a,b)]$. Hence, T_R does not admit quantifier elimination. □

Theorem 2.2.1 tells us that the theory of real closed field is not so good.Hence we consider the new language:$L_{OR} = L_R \cup \{\leq\}$,we give this theory a new name:real ordered closed field theory,denoted by T_{ROCF}.

Theorem 2.2.2. *The theory T_{ROCF} admits the quantifier elimination.*

Proof of theorem. Let F_1, F_2 be models of T_{ROCF},(K,$\leq$) be the common substructure of F_1, F_2.Let $K^{'}$ denote the fraction of K.It's easy to see that $K^{'}$ is an ordered field.Hence we can find a real closure of $K^{'}$:R.And $R \subset F_1$,$R \subset F_2$. Let $\phi(v, \bar{w})$ be a quantifier free formula in L_{OR}, $\bar{a} \in K$ and $b \in F_1$ and suppose $F_1 \models \phi(b, \bar{a})$ (so $F_1 \models \exists v \phi(v, \bar{a})$). We want to show that $F_2 \models \exists v \phi(v, \bar{a})$. It will suffice to show that R$\models\exists$vϕ(v, $\bar{a}$).

Since ϕ is quantifier free,there are $f_1, f_2, ...f_n, g_1, g_2, ...g_m \in K(x)$,such that:

$$\phi(v, \bar{a}) \leftrightarrow \wedge_1^n [f_i(v) = 0] \wedge \wedge_1^m [g_i(v) > 0]$$

If f_i is not zero,since $F_1 \models \phi(b, \bar{a})$,$f_i(b) = 0$ implies that b is algebraic over K.Then $b \in R$.

Otherwise,$\phi(v, \bar{a}) \leftrightarrow \wedge_1^m [g_i(v) > 0]$.By the fundamental theorem of algebra for real closed field,g_i is a product of $(x - a)$ and $((x - a)^2 + b^2)$.And the latter is always positive when b is not 0.

Hence we can find some terms $(x - c_{1_i}), ...(x - c_{p_i}).c_{1_i} < ... < c_{p_i}$. Now we can use L_{OR} to describe that $g_i(x) > 0$.In fact,$g_i(x) > 0 \iff \vee_1^{\frac{p_i-1}{2}} [c_{(2j-1)_i} < x \wedge x > c_{(2j)_i}] \vee c_{p_i} > x$ when p_i is odd,$x < c_{1_i} \vee \vee_1^{\frac{p_i-2}{2}} [c_{(2j)_i} < x \wedge x < c_{(2j+1)_i}] \vee c_{p_i} < x$ when p_i is even.We denote this formula as $\theta(x, c_{1_1}, ...c_{p_m})$.

Let $C = max\{p_i | 1 \leq i \leq m\}+1$,$C \in R$.We can see that $R \models \theta(C, c_{1_1}, ...c_{p_m})$.$R \models \exists v \phi(v, \bar{a})$.By theorem 2.1.2(2),we have T_{ROCF} admits quantifier elimination.

□

Corollary 2.2.0.1. *The theory of real closed field with L_R is completeness.*

This is because consider $F, K \models T_{RCF}$,$F \subset K$.By completeness of T_{ROCF},$F \prec K$ in L_{OR}.We can replace $x < y$ as $\exists z[x + z^2 = y]$.Hence $F \prec K$ in L_R.

2.3 Seidenberg's decision method for an algebraic curve

Due to A.Seidenberg,we get a method to deciding whether a given equation $f(x, y) = 0$,$f(x, y) \in R[x, y]$,has a solution in $R^{(2)}$.The main idea is here:we want to find the real point nearest the origin.

Seidenberg's decision method is also very useful in partial differential equations.

Lemma 2.3.1. *Let $f(x,y) \in R[x,y]$,x,y are indeterminates,R is a real closed field.Then if f(x,y)=0 has a solution in R,it has a solution (a,b) nearest the origin.*

Proof of lemma. We consider the polynomials $f(x,y)$ and $x^2+y^2-t^2$ where t is an indeterminate.We consider the resultant with respect to y:g(t,x).We let S be the set of $c \in R$,such that g(c,x) has a solution in [-c,c].

If $c \in S$,(a,b) is a point of intersection of the circle and f(x,y)=0.Then by the definition of resultant,f(a,y) and $y^2+a^2-c^2$ has a common factor:y-b.Hence $g(c,a)=0$

Conversely,if $g(c,x)$ has a root a in R.Then $y^2+a^2-c^2$ and f(a,y) has a same solution.$b=\sqrt{c^2-a^2}$.Then (a,b) or (a,-b) is an intersection of circle and $x^2+y^2=c^2$.

Let $S^{'}$ be the subset of S of c such that $g(c,-c) \neq 0$.$S^{'}$ is a union of finite system of polynomials $p(c)=0$ and $q(c)>0$.Since the complement set of $S^{'}$ with respect to S is either finite or all $c \geq 0$.Hence $S^{'}$ is a collection of finite closed intervals.

Let $d \notin S^{'}$,$g(d,x)$ has no solution in [-d,d].Let $g(x)=g_0(x)+g_1(x)(t-d)+...+g_m(x)(t-d)^m$.Then there exists $b>0, B>0$,such that $|g_0(u)| \geq b$,$|g_i(u)| \leq B$ when u in [-d,d].

If $|c-d| \leq \frac{1}{2}$,$|c-d| < \frac{b}{4B}$,

$$|g(c,u)| \geq |g_o(u)| - |g_1(u)(c-d)+...+g_m(u)(c-d)^m| \geq b-2B|c-d| \geq \frac{b}{2}$$

Hence any d is in the complement. □

Definition 2.3.1. *A point (a,b) on C:$f(x,y)=0$ is a single point if* $((\frac{\partial f}{\partial x})_{(a,b)}, (\frac{\partial f}{\partial y})_{(a,b)}) \neq (0,0)$

Lemma 2.3.2. *Let p be a point of intersection of a circle and a curve*

C:f(x,y)=0.Assume that p is a single point of C and tangent at p to C contains points interior to the circle.Then C itself has points interior to the circle.

Proof of lemma. We may assume that p is the origin and the tangent is x-axis.Thus,$f(0,0) = 0$ and $(\frac{\partial f}{\partial x})_{(0,0)} = 0$.We may assume that $(\frac{\partial f}{\partial y})_{(0,0)} = 1$.Let (a,b) be the center of the circle.

$$f(x,y) = f(0,0)+(\frac{\partial f}{\partial x})_{(0,0)}x+(\frac{\partial f}{\partial y})_{(0,0)}y+\frac{1}{2}[(\frac{\partial^2 f}{\partial x^2})_{(0,0)}x^2+2(\frac{\partial^2 f}{\partial x\partial y})_{(0,0)}xy+(\frac{\partial^2 f}{\partial y^2})_{(0,0)}y^2]+...$$

Hence we may assume f(x,y)=$y(1 + h(x,y)) + g(x)$,where $h(0,0) = 0$ and $x^2|g(x)$.
We pick $\delta > 0$,such that $|h(x,y)| \leq \frac{1}{2}$ when $|x| \leq \delta, |y| \leq \delta$.Now $\delta(1+h(x,\delta))$ is between $\frac{1}{2}\delta$ and $\frac{3}{2}\delta$,$-\delta(1 + h(x,-\delta))$ is between $-\frac{1}{2}\delta$ and $-\frac{3}{2}\delta$.
Since $g(0) = 0$,there exists $0 < \delta^{'} < \delta$,such that $f(x,\delta) > 0$ and f(x,δ)<0 when $|x| \leq \delta^{'}$.Hence there exists y_0 such that for any $|x_0| < \delta^{'}$,f(x_0, y_0)=0,$|y_0| \leq \delta$.

$$y_0 = -g(x_0)(1 + h(x_0,y_0))^{-1}$$

$$(a - x_0)^2 + (b - y_0)^2 = (a - x_0)^2 + (b + \frac{g(x_0)}{1 + h(x_0,y_0)})^2 = a^2 + b^2 - 2ax_0$$

$$+x_0^2 + \frac{2bg(x_0)}{1 + h(x_0,y_0)} + \frac{g(x_0)^2}{(1 + h(x_0,y_0))^2}$$

Since $x^2|g(x)$,we pick x_0 sufficiently small.Hence (x_0, y_0) inside the circle. □

Now,we will obtain the Seidenberg's decision method for $f(x,y) = 0$.
First we find the greatest common divisor of the coefficients of f(x,y) with respect to y:d(x).Let $f(x,y) = f_1(x,y)d(x)$.Hence we may assume that f(x,y) is primitive with respect to y.
Let h(t,x) be the resultant of f(x,y) and $(\frac{\partial f}{\partial x})y - (x - t)(\frac{\partial f}{\partial y})$.If $h(t,x) \equiv$

0,f(x,y) and $(\frac{\partial f}{\partial x})y-(x-c)(\frac{\partial f}{\partial y})$ has same divisor for any c.Then $(\frac{\partial f}{\partial y})=(c_1-c_2)^{-1}[g(c_1,x,y)-g(c_2,x,y)]$ for any c_1,c_2.Hence we will see that $(\frac{\partial f}{\partial y})$ and f(x,y) have same divisor.contradiction,hence h(t,x)≠0.

We choose a c and let h(x)=h(c,x)≠0.And g(x,y)=g(c,x,y)Let k(y) be the resultant of f(x,y) and g(x,y) with respect to x.Similarly,k(y) is not 0.

If f(x,y) has a solution,then by lemma 2.3.1,there exists a solution (a,b),such that f(a,b)=g(a,b)=0.Hence now f(a,y) and g(a,y) has a common divisor (y-b).Then h(a)=0.

Conversely,if h(x) has a solution.We define $C=R(\sqrt{-1})$,which is algebraic closed.Let V be the intersection of f(x,y)=0 and g(x,y)=0.If (a,b)∈V,then h(a)=k(b)=0.h and k are finite degree so V is finite.

Let l(x) be the coefficient of highest power of y in f(x,y).If l(a)≠0,$a \in R$,h(a)=0 implies that there exists a b such that (a,b)∈V.If $b \in R$,(a,b) is a solution.

If b∉R,then (a,b) and (a,$\bar{b}$) are two points in C with same x-axis coefficient.

Now we want to find suitable coordinates such that $l(a) \neq 0$ and no two points with same x-axis coefficient.

Let $m \in R$ and $m \neq 0$.Let $x^{'}=m^{-1}x-y, y^{'}=y$;hence f(x,y)=$f(m(x^{'}+y^{'}),y^{'})$.Let $f_n(x,y)$ be the homogeneous part of degree n in f(x,y).$f_n(x,1)\neq 0 \implies \exists m f_n(m,1)\neq 0$.

Now we will find "no two points with same x-axis coefficient".We take d(x) as the g.c.d of h(x) and $h^{'}(x).h_1(x)$ is the quotient of h(x) by dividing d(x).Let $r_1,...,r_n$ be the sequence of root of $h_1(x)$.Similarly,$s_1,...s_m$ is the sequence of root in $k_1(x)$.

Lemma 2.3.3. *There exists a polynomial p(x) such that whose roots are*

$$(r_i-r_{i'})(s_j-s_{j'})^{-1}$$

which satisfying that "no two points with same x-axis coefficient"

Proof.

$$\prod_{i\neq i',j\neq j'}[(y_i-y_{i'})x-(x_i-x_{i'})]$$

$$\prod_{i\neq i'}[t-(x_i-x_{i'})]=t^m-m_1(p_1,...p_n)t^{m-1}+...$$

Let $p_1=\sum x_i$,$p_2=\sum_{i<j}x_ix_j$,...,$p_n=x_1...x_n$. Then $\prod_{i\neq i',j\neq j'}[(y_i-y_{i'})x-(x_i-x_{i'})]=\prod_{i\neq i'}[(y_i-y_{i'})^mx^m-m_1(p_1,...p_n)+...]=z_0x^{m^2}-z_1x^{m^2-1}+z_2x^{m^2-2}-...$,where $z_i\in Z[p_1,...p_n,q_1,...q_r]$ where $q_1=\sum y_i, q_2=\sum_{i<j}y_iy_j$. Let p_i and q_i be the correspondence coefficients of $h_1(x)$ and $k_1(x)$. Now that $m^{-1}r_i-s_j\neq m^{-1}r_{i'}-s_{j'}$ □

Hence f(x,y)=0 has a solution if and only if h(x) relative to new coordinates has a solution.h(x)=0 is easy because the Sturm's theorem.

2.4 Tarski-Seidenberg Principle

In fact,quantifier elimination for real closed field has a geometric interpretation.Now,we tell a little real algebraic geometry.

Tarski-Seidenberg Principle is used in real algebraic geometry as a transfer tool.

Tarski's original account is very interesting.He defined his metamathematical principle.Any element sentence of "elementary algebra" which is true in a real closed is true for any real closed field.He use "atomic formula" as an expression.

Tarski-Seidenberg Principle is important in partial differential equation and mathematical logic.

Definition 2.4.1. *An ordered field F,we say X is semi-algebraic if $X\subseteq F^n$ and it is a Boolean combination of sets of the form $\{x|p(x)>0\}$, where $p(X)\in F[X_1,...,X_n]$.*

By quantifier elimination, the semi-algebraic sets are exactly the definable sets.

Definition 2.4.2. *We say that $X \subset M^n$ is definable if and only if there is an L-formula $\psi(v_1, ..., v_n, w_1, ..., w_m)$and $b \in M^m$ such that $X = \{a \in M^n : M \models \psi(a, b)\}$.*

We define a function :sign in R.
sign(a)=0 if a=0
sign(a)=-1 if $a < 0$
sign(a)=1 if $a > 0$

Theorem 2.4.1 (Tarski-Seidenberg principle)**.** *Let $f_i(X, Y) = h_{i,m}(Y)X^{m_i} + ... + h_{i,0}(Y)$ for i = 1, ... , s be a sequence of polynomials in n + 1 variables with coefficients in Z, where $Y = (Y_1, ..., Y_n)$. Let f be a function from $\{1, ..., s\}$ to $\{-1, 0, 1\}$. Then there exists a boolean combination B(Y) (i.e. a finite composition of disjunctions, conjunctions and negations) of polynomial equations and inequalities in the variables Y with coefficients in Z such that for every real closed field Rand for every $y \in R^n$, the system*

$$sign(f_1(X, y)) = \epsilon(1)$$

$$sign(f_2(X.y)) = \epsilon(2)$$

.

$$sign(f_s(X, y)) = \epsilon(s)$$

has a solution x in R if and only if B(y) holds true in R.

The proof of this theorem is so hard.But the main idea is that:we will use Seidenberg's decision method to deciding a n-indeterminate polynomial using n-1 indeterminate polynomial,then we use induction to prove.

Proof of Tarski-Seidenberg principle. If $\epsilon(i) = 1$,it's equivalent to $\exists z[f_i(X,y)z^2 - 1 = 0]$.Similarly for $\epsilon(i) = -1$.Hence we get a terms of equations $F_i(X,y,z_i)$.There exists a solution if and only if $\sum_1^s [F_i(X,y,z_i)]^2 = 0$ which we denote as $H(z_1,...z_p;X,y) = 0$.

We will use induction for m($X = (x_1,...,x_n)$) to prove:we use the Seidenberg's decision method.We regard $(x_1,..x_{n-2})$ as parameter,then use the method.There exists H_j with variable $(x_1,...x_{n-1})$ where H_j has a solution if and only if H has a solution. Also, H_j has parameter y.

When $n = 1$, just by decision method,there exists $B(Y)$. □

Theorem 2.4.2. *The semi-algebraic set is closed under projection.*

Proof.

Lemma 2.4.3. *Every semi-algebraic subset of R^n can be written as a finite union of semi-algebraic sets of the form: $\{x \in R^n | f_1(x) = ... = f_t(x) = 0, g_1(x) > 0, ..., g_m(x) > 0\}$, where $f_1...,f_t,g_1,...,g_m$ are in $R[x_1,...,x_n]$.*

We only need to prove $\pi : R^n \to R^{n-1}$.

By lemma 2.4.3, it is enough to prove the theorem for a semi-algebraic set of the form: $\{(y,X) \in R^n \times R | f_i(y,X) = 0, i = 1,...,l, g_j(y,X) > 0, j = 1,...,m\}$. By the Tarski-Seidenberg principle , there exists a boolean combination of polynomial equations and inequalities B(Y) in the variables Y with coefficients in R such that, for every Y in R^n, the system $\{f_1(y,X) = ... = f_l(y,X) = 0, g_1(y,X) > 0, ...g_m(y,X) > 0\}$ has a solution x in R if and only if B(y) is satisfied. Since the set of y in R^n , satisfying B(y), is semi-algebraic, the theorem is proved. □

3 Hilbert's seventeenth problem and Positivstellensatz

Tarski first showed completeness and decidability for the fields of real and complex numbers. His proof gave an explicit algorithm for eliminating quantifiers. Robinson showed that quantifier-elimination results could be proved by finding the right embedding theorems. These ideas were further extended by Blum. Robinson also introduced the notion of model completeness and saw how it could be used to prove Hilbert's Nullstellensatz and answer Hilbert's 17th-problem.

3.1 A.Robinson's proof of 17th problem

A.Robinson's proof is the easiest proof of 17th problem.He use the model completeness of real closed field.(In fact,Hilbert's 17th problem is for real numbers field.But Artin-Schreier use their theory to prove the 17th problem.)Using model theory make it more easier than Artin's proof.

Definition 3.1.1. *An rational function f over a real closed field R,is called positive semi-definite if $f(\bar{a}) \geq 0$for all $\bar{a} \in R$.*

Theorem 3.1.1. *If f is a positive semi-definite rational function over a real closed field R, then f is a sum of squares of rational functions over R.*

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

semi-definite.

Hence any positive semi-definite rational function is the sum of squares. □

Corollary 3.1.1.1 (K.McKenna). *If F is an ordered field,such that any positive semi-definite function is a sum of squares,then F is uniquely ordered and is dense in its real closure.*

3.2 Positivstellensatz

The real Nullstellensatz was originally proved by Krivine. His model theoretic proof was not noticed by real algebraic geometry, and the result was proved again later by Dubois and Risler. Model-completeness and quantifier elimination have many applications in real algebraic geometry.
Here we may use some definition in algebraic geometry.

Definition 3.2.1. *Let J is an ideal in* $R[x_1, ..., x_n]$, *V (J)* $:= \{\bar{a} \in R | \forall f \in J, f(\bar{a}) = 0\}$ *is the variety generated by J.*

Definition 3.2.2. *If V is a set of points in* R^n , *I(V)* $:= \{f \in R[x_1, ..., x_n] | \forall v \in V, f(\bar{v}) = 0\}$ *is the ideal generated by V.*

Definition 3.2.3. *If J is an ideal in* $R[x_1, ..., x_n]$*.J is real over R if for every* $\sum_{1}^{m} p_i f_i^2 \in J$ *with* $f_i \in R[x_1, ..., x_n]$ *and* $p_i \in R^2 \backslash 0$, *then* $f_1, ..., f_n \in J$.

Lemma 3.2.1. *If J is a proper ideal of* $R[x_1, ..., x_n]$, *then J is real over R if and only if J is radical and is the intersection of finitely many prime ideals which are real over R.*

Theorem 3.2.2 (Positivstellensatz). *Let R be a real closed field and let J be an ideal in* $R[x_1, ..., x_n]$. *J = I(V (J)) if and only if J is real over R.*

Proof of Dickman. $\Longrightarrow$:We only need to prove that I(V(J))$\subset J$.
We pick $g_1, ..., g_m \in R[x_1, ..., x_n]$ such that $< g_1, ..., g_m >= J$ by Hilbert's

basis theorem.

Any $f \in I(V(J))$,we want to prove that $f \in J$.

By the lemma,we have $J = \cap_1^k P_i$,where P_i are prime ideal. Hence we only need to prove that $f \in P_i$.We consider R_i to be the real closure of $R[x_1, ...x_n]\backslash P_i$.

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

$$\Longrightarrow R_i \models \wedge g_k(x_1/P_j, ..., x_n/P_j) = 0$$

$$\Longrightarrow R_i \models f(x_1/P_j, ..., x_n/P_j) = 0$$

Hence $f \in p_j$.

$\Longleftarrow$ J=I(V(J)),let S=V(J).We only need to prove that I(S) is real. Suppose I(S) is not real,there exists $f_1, ..., f_s$ all not in J,such that $\sum p_j f_j^2 \in J$.

I(S) is vanishing at S,hence $\sum p_j f_j(x)^2 = 0$,but $p_j > 0$ and $f_j(x) \neq 0$.Contradiction.

□

4 Pfister theory of quadratic forms

The main theorem of this section is that if R is a real closed field,any element of $R(x_1, ..., x_n)$ that is sum of squares is a sum of 2^n squares.The algebraic theory of quadratic forms, starting with the work of Witt in the 1930s through its rebirth in 1960s with the work of Pfister, shifts the emphasis from a particular quadratic form to the set of all such (non degenerate) forms over a fixed ground field, associating to this set an algebraic object, the Witt ring. We will begin with some notations for quadratic forms.

Notation 4.1. *We denote the quadratic form as Q.*

And $B(x, y) = Q(x + y) - Q(x) - Q(y).Q(x, y) = \frac{1}{2}B(x, y)$

We may assume characteristic is not 2.

We consider the tensor product of quadratic forms:

$$(Q_1 \otimes Q_2)(v_1 \otimes v_2) = Q_1(v_1)Q_2(v_2)$$

Where $Q_1 \otimes Q_2$ is defined on $V_1 \otimes V_2$. And we define:

$$(Q_1 \otimes Q_2)(u_i \otimes v_j, u_k \otimes v_l) = Q_1(u_i, u_k)Q_2(v_j, v_l)$$

.

If u=$\sum a_i u_i$ and v=$b_j v_j$,

$$(Q_1 \otimes Q_2)(u \otimes v) = (Q_1 \otimes Q_2)(u \otimes v, u \otimes v)$$

$$= (Q_1 \otimes Q_2)(\sum a_i b_j u_i \otimes v_j, \sum a_k b_l u_k v_l)$$

$$= \sum a_i a_k b_j b_l Q_1(u_i, u_k)Q_2(v_j, v_l)$$

$$= (\sum a_i a_k Q_1(u_i, u_k))(\sum b_j b_l (Q_2(v_j, v_l)))$$

$$= Q_1(u)Q_2(v)$$

Hence $Q_1 \otimes Q_2$ is well-defined.

Also,we define $Q_1 \oplus Q_2$ in $V_1 \oplus V_2$.

$$Q_1 \oplus Q_2(u, v) = Q_1(u) + Q_2(v)$$

If we pick an orthogonal basis for V,$(u_1, ..., u_n)$,such that $Q(u_i) = b_i$

We will write that:

$$Q \sim diag\{b_1, ..., b_n\}$$

4.2 A.Hurwitz's Problem

This problem is also called by "1,2,4,8" problem.A.Hurwitz gave this problem in 1898,which made an great impact in Pfister theory.
From commutativity of multiplication (for numbers), a product of two squares is a square:

$$x^2y^2 = (xy)^2$$

A more interesting identity is the following one, which expresses a sum of two squares times a sum of two squares as another sum of two squares:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

There is also an identity like this for a sum of four squares:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

$$= (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2$$

$$+(x_1y_3 + x_3y_1 - x_2y_4 + x_4y_2)^2 + (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2.$$

This was discovered by Euler in the 18th century, forgotten, and then rediscovered in the 19th century by Hamilton in his work on quaternions. Shortly after Hamilton's rediscovery of Cayley discovered a similar 8-square identity.

Theorem 4.2.1 (Hurwitz's problem)**.**

$$(\sum_1^n x_i^2)(\sum_1^n y_i^2) = \sum_1^n z_i^2$$

where z_i are bilinear with $(x_1, ..., x_n)$ and $(y_1, ..., y_n)$.
We want to find all of n such that there exists the identities.

Definition 4.2.1. *We can define a quadratic form for this problem :*

$$Q(x) = \sum_{1}^{n} x_i^2$$

. And if there exists the identities,we can define:

$$x \times y = z$$

where z is the form can be in the identity.
Hence now the equation became that

$$Q(x)Q(y) = Q(xy)$$

For some $Q(v) \neq 0$,we define

$$u = v^2 Q(v)^{-1}$$

Now we have Q(u)=1 and

$$Q(ux) = Q(x) = Q(xu)$$

We define a new product:

$$x * y = (u_R^{-1}x)(u_L^{-1}y)$$

Then u^2 is the unit of product.

Definition 4.2.2. *An composition algebra is a pair of consisting of a non-associative algebra A with a unit 1 and a non-degenerated quadratic form Q such that $Q(xy) = Q(x)Q(y)$*

Now we will determine all the composition algebras.

$$Q(x+z)Q(y) = Q((x+z)y) = Q(xy+zy)$$

$$\implies Q(y)(Q(x)+Q(y)+B(x,z)) = Q(xy)+B(xy,zy)+Q(zy)$$

Which is from the notation 4.1

$$\implies B(x,z)Q(y) = B(xy,zy)$$

Similarly:

$$Q(x)B(y,w) = B(xy,zy)$$

If we let $y = y+w$ in $B(x,z)Q(y) = B(xy,zy)$,we will get:

$$B(x,z)B(y,w) = B(xy,zw)+B(zy,wx)$$

Definition 4.2.3. *We define a map j:*$x \to \dfrac{B(x,1)}{Q(1)}1 - x = B(x,1)1 - x$
$\bar{x} = j(x)$,$T(x) = B(x,1)$
We have $Q(x) = Q(\bar{x})$,$\bar{\bar{x}} = x$

Lemma 4.2.2. *We want to have the following property:*

$$\bar{x}x = Q(x)1 = x\bar{x}$$

$$\bar{x}(xy) = (\bar{x}x)y$$

$$(y\bar{x})x = y(x\bar{x})$$

$$x\bar{y} = \bar{y}\bar{x}$$

Proof of lemma. First,we have $Q(x)B(1,y) = B(x,xy)$.And:

$$B(x,\bar{y}z) = B(x,B(y,1)z - yz) = B(y,1)B(x,z) - B(x,yz)$$

$$= B(yx, z) + B(yz, x) - B(x, yz) = B(yx, z)$$

Then $B(x, xy) = B(\bar{x}x, y)$,hence $B(Q(x)1 - \bar{x}x, y) = 0$ for any y.Hence $\bar{x}x = Q(x)1$.(B is non-degenerated)

$$B(\bar{x}(xy), z) = B((B(x, 1)1 - x)(xy), z) = B(x, 1)B(xy, z) - B(x(xy), z)$$

$$= B(x(xy), z)+B(xy, xz)-B(x(xy), z) = B(xy, xz) = Q(x)B(y, z) = B(Q(x)y, z)$$

Hence we have $\bar{x}(xy) = Q(x)y = (\bar{x}x)y$.

$$B(x\bar{y}, z) = B(1, (xy)z)$$

$$B(\bar{y}\bar{x}, z) = B((B(y, 1)1 - y)(B(x, 1)1 - x), z)$$

$$= B(B(x, 1)B(y, 1)1 - B(y, 1)x - B(x, 1)y + yx, z)$$

$$= B(x, 1)B(y, 1)B(z, 1) - B(y, 1)B(z, x) - B(x, 1)B(y, z) + B(yx, z)$$

$$= B(xy, 1)B(z, 1) + B(x, y)B(z, 1) - B(yz, x) - B(xy, z) - B(xz, y)$$

$$= B((xy)z, 1)+B(xy, z)+B(xz, y)+B(yz, x)-B(yz, x)-B(xy, z)-B(xz, y)$$

$$= B((xy)z, 1)$$

Hence we have $x\bar{y} = \bar{y}\bar{x}$ □

Now,we have an involution j in A.By the lemma 4.2.2's second and third equality,we have $[x, \bar{x}, y] = 0 = [y, x, \bar{x}]$ where "[, ,]" is the associator.And $x = T(x)1 - \bar{x}$:

$$[x, x, y] = 0 = [y, x, x]$$

Definition 4.2.4. *An alternative algebra is an algebra which satisfies the equality:*$[x, x, y] = 0 = [y, x, x]$.

Now, any composition algebra is an alternative algebra.What is converse?There is an important equality due to Moufang:

$$(ux)(yu) = u(xy)u$$

Proof of Moufang's identity. First,by the linearization of "[]",we have $[x, y, z]+[z, x, y] = 0$.Hence we have $[x, y, x] = 0$.

$$x^2y = x(xy), (xy)x = x(yx), yx^2 = (yx)x$$

Here:

$$(u^2x)y + 2(ux)(yu) + x(yu^2) = u((ux)y) + ((ux)y)u + u(x(yu)) + (x(yu))u$$

$$= u[(ux)y + x(yu)] + [(ux)y + x(yu)]u = u[u(xy) + (xy)u] + [u(xy) + (xy)u]u$$

$$= u^2(xy) + 2u(xy)u + (xy)u^2$$

Where $[u^2, x, y] = [x, y, u^2]$,hence (ux)(yu)=u(xy)u is true if char not 2. □

If A is an alternative algebra with an involution j,$\bar{x}x = Q(x)1$.Then we have :

$$\bar{x}y + \bar{y}x = (x \bar{+} y)(x + y) - \bar{x}x - \bar{y}y = B(x, y)1$$

If we pick $y = 1$,we have $x + \bar{x} = T(x)1$,hence T(x)=B(x,1). Now :

$$Q(xy)1 = (x\bar{y})(xy) = (\bar{y}\bar{x})(xy) = [(T(y)1 - y)\bar{x}](xy)$$

$$= (T(y)\bar{x} - y\bar{x})(xy) = T(y)\bar{x}(xy) - (\bar{y}x)(xy)$$

$$= Q(x)T(y)y - y(\bar{x}x)y \quad (Moufang)$$

$$= Q(x)[T(y)1 - y]y = Q(x)(\bar{y}y) = Q(x)Q(y)1$$

Hence any alternative algebra is a composition algebra.

Definition 4.2.5. *Any alternative algebra A,let D be A^2,we define a binary product in D:*

$$(u,v)(x,y) = (ux + c\bar{y}v, yu + v\bar{x})$$

And an involution:j:$(x,y) \to (\bar{x,y}) = (\bar{x}, -y)$.

$$(\bar{x,y})(x,y) = ((Q(x) - cQ(y))1, 0)$$

Hence the quadratic form on D is $(x,y) \to Q(x) - cQ(y)$. *Any the bilinear form is* $((u,v),(x,y)) \to B(u,x) - cB(v,y)$. *Then we call that D is a c-double of A.*

Lemma 4.2.3. *(1)The c-double D is commutative and associative if and only if A is commutative and associative and j=1*
(2)D is associative if and only if A is commutative and associative
(3)D is alternative if and only if A is associative

Proof of lemma. Let $X = (x,y)$,$U = (u,v)$ and $Z = (z,t)$.

$$[U,X] = ([u,x] + c(\bar{y}v = \bar{v}y), y(u - \bar{u}) + v(\bar{x} - x))$$

$$[U,X,Z] = ([u,x,z] + c\bar{t}(yu) - u(\bar{t}y) + \bar{t}(v\bar{x}) - (\bar{x}\bar{t})v + (\bar{y}v)z - (z\bar{y}v)$$

$$, t(ux) - (tx)u + (yu)\bar{z} - (y\bar{z})u + (v\bar{x})\bar{z} - v(\bar{z}\bar{x}) + ct(\bar{y}v) - v(y\bar{t}))$$

(1):if A is commutative and associative with j=1,then $[U,X] = 0$ and $[U,X,Z] = 0$,D is commutative and associative.
If D is commutative and associative,then A is an subalgebra of D.In [U,X],we let u=x=0 and v=1,we get $\bar{y} = y$.

(2) If A is associative and commutative then $[U, X, Z] = 0$,hence D is associative.

If D is associative and let v=z=0,and t=1,we get yu=uy.

A is a subalgebra of D so A is associative and commutative.

(3)D is alternative then:

$$[\bar{X}, X, Z] = (c[\bar{x}, \bar{t}, y], -[y, \bar{z}, \bar{x}])$$

Hence A is associative.

If A is associative we have $[\bar{X}, X, Z] = 0$

Since $X + \bar{X} = T(X)1$,it is equivalent to $[X, X, Z] = 0$,D is alternative. □

What is converse again?if we get an algebra A,how can we find a C such that A is a double of C?

Lemma 4.2.4. *Let (A,Q) is a composition algebra,C is a proper subalgebra containing 1 and $\bar{C} \subset C$ such that C is a non-degenerate subspace of A relative to B.Then C can be imbedded in a subalgebra D of A satisfying that D is isomorphic to a double of C.*

Proof of lemma. Since C is non-degenerate ,we have $A = C \otimes C^{\perp}$.

We find $t \in C^{\perp}$ such that $Q(t) = -c \neq 0$.Since $1 \in C$,T(t)=B(1,t)=0.

Hence $\bar{t} = -t$ and $t^2 = -\bar{t}t = -Q(t)1 = c1$.

If B(x,t)=0 and $x \in C$.we have $\bar{x}t + \bar{t}x = 0$,and

$$tx = \bar{x}t, \quad x \in C$$

If $x, y \in C$ then B(x,yt)=B($\bar{y}x, t$)=0 ($\bar{y}x \in C$)

Hence Ct=$\{yt | y \in C\} \subseteq C^{\perp}$

Let D=$C \oplus Ct$.

$$(u + vt)(x + yt) = ux + (yu + v\bar{x})t + (vt)(yt)$$

Now we want to find (vt)(yt) is what?

$$(vt)(yt) = (t\bar{v})(yt)(by \quad B(v,t) = 0) = t(\bar{v}y)t(by \quad Moufang's \quad identity)$$

$$= (\bar{y}v)t^2 = c\bar{y}x$$

Hence we have :

$$(u + vt)(x + yt) = (ux + c\bar{y}v) + (yu + v\bar{x})t$$

D is a subalgebra.

D is a c-double of C where c is Q(t). □

Theorem 4.2.5 (Hurwitz)**.** *The list of composition algebra over F (char not 2):(1)F1(2)quadratic algebra(3)quaternion algebra(4)octonion algebras.*

Hutwitz. (1)A=F1,is a composition algebra.

Otherwise $F1 \subsetneq A$,A contains quadratic algebra by lemma 4.2.4.

(2)A is quadratic algebra by lemma 4.2.3 A is commutative and associative

Otherwise A contains quadratic algebra.By lemma 4.2.4,quaternion algebra is in A

(3)A is quaternion algebra,by lemma 4.2.3,A is associative.

Otherwise A contains quaternion algebra.By lemma 4.2.4,octonion algebra is in A.

(4)A is octonion algebra,by lemma 4.2.3,A is alternative.

Otherwise there exists an subalgebra B,where B is not alternative,hence the algebra is not alternative,so not a composition algebra. □

In fact,we proved that there are only four composition algebra over a field F.
Now,we want to know the Q of them.
The first case is trivial:Q(x)=x^2.
The second case is commutative and associative,Q(x)=$x_0^2 - cx_1^2$
The third case is associative.If we consider the field F is real numbers,the algebra is Hamilton's numbers,$x = x_0 + x_1 i + x_2 j + x_3 k$,hence Q(x)=$x_0^2 + x_1^2 + x_2^2 + x_3^2$
The fourth case is also the difficult one.This algebra is called Cayley-Graves algebra O.

4.3 Pfister forms

In a real closed field R,any positive semi-definite rational function of n variables over R is a sum of 2^n squares.
This is the main result of Pfister theory.
In 1893,Hilbert showed that any positive semi-definite rational function in two variables is expressible as a sum of four squares.
In 1966 in an unpublished paper,J.Ax showed that any positive semi-definite function in three variables is a sum of eight squares and he conjectured that for n variables,it will be 2^n squares.
In 1967,by A.Pfister gave a proof with ingenious method.
The proof of this theorem is based as some results on quadratic forms,like Hurwitz's problem.In fact ,they are all interesting.

Definition 4.3.1. *A quadratic form Q is said to be strongly multiplicative if Q is equivalent to cQ for any $c \neq 0$ representation.*

Lemma 4.3.1. *$diagb_1, b_2 \sim diagc_1, c_2$ if and only if c_1 is represented by $b_1 x_1^2 + b_2 x_2^2$ and $b_1 b_2$ and $c_1 c_2$ differ by a square factor.*

Proof of Lemma. $\Longrightarrow$:c_1 is represented by $b_1x_1^2 + b_2x_2^2 = Q$,pick y such that Q(y)=c_1.

The discriminant of Q is b_1b_2 hence b_1b_2 and c_1c_2 differ by a square factor.

$\Longleftarrow$:Q(y)=c_1,Then diagb_1, b_2~diagc_1, c where $c_1c = k^2b_1b_2$.

Hence $c_2 = n^2c$ for some n,$diag\{b_1, b_2\} \sim diag\{c_1, c_2\}$. □

Lemma 4.3.2. *Let Q be a strongly multiplicative quadratic form,$a \in F^*$.Let $Q_a \sim diag1, a$.Then $Q_a \otimes Q$ is strongly multiplicative.*

Proof of lemma. First,we see that $Q_a \otimes Q$ is equivalent to $Q \oplus aQ$.

We map $u \otimes v \to (u, v)$,we will get $Q \oplus aQ$.

Let k be an element represented by Q,which is not zero.So $k = b + ac$ where b,c are represented by Q.

(1)c=0,since $Q \sim bQ$ by definition of strongly multiplicative.

$$Q \oplus aQ \sim bQ \oplus abQ = b(Q \oplus aQ) = k(Q \oplus aQ)$$

where k=b.

(2)b=0,since $cQ \sim Q$,

$$k(Q \oplus aQ) = kQ \oplus kaQ = acQ \oplus a^2cq \sim aQ \oplus Q$$

where k=ac,$k(Q \oplus aQ) \sim Q \oplus aQ$

(3)$bc \neq 0$.Then:

$$Q \oplus aQ \sim bQ \oplus acQ \sim diag\{b, ac\} \otimes Q$$

By lemma 4.3.2,we get $diag\{b, ac\} \sim diag\{k, kabc\}$.

Hence we have:

$$diag\{b, ac\} \otimes Q \sim diag\{k, kabc\} \otimes Q \sim kdiag\{1, abc\} \otimes Q$$

$$\sim kQ \oplus kabcQ \sim kQ \oplus kaQ = k(Q \otimes aQ)$$

Hence $Q \oplus aQ$ is strongly multiplicative. □

Then,by lemma 4.3.3,we get:

$$diag\{1, a_1\} \otimes diag\{1, a_2\} \otimes ... \otimes diag\{1, a_n\}$$

is strongly multiplicative quadratic form.
Hence in particular:

$$\sum_{1}^{2^n} x_i^2 \sim diag\{1, 1\} \otimes diag\{1, 1\} \otimes ... \otimes diag\{1, 1\}$$

is strongly multiplicative quadratic form.

Definition 4.3.2 (Pfister)**.** *We call the quadratic form:*

$$\sum_{1}^{2^n} x_i^2$$

Pfister forms of dimension 2^n

Theorem 4.3.3.

$$diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\} = diag\{1\} \oplus D$$

Let Q *be a quadratic form such that* $Q \sim D$*.And* $b_1 \neq 0$ *is represented by* Q*.*

There exists $b_2, ...b_n \in F^*$ *such that*

$$diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\} \sim diag\{1, b_1\} \otimes ... \otimes diag\{1, b_n\}$$

Proof. We use induction on n.

If $n = 1$,diag$\{1, a_1\} \sim diag\{1, b_1\}$.

We assume this for n and:

$$diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\} \otimes diag\{1, a\} = diag\{1\} \oplus D^{'}$$

We may assume $b_1^{'}$ is represented by $Q^{'}$ where $Q^{'} \sim D^{'}$.

Then $b_1^{'} = b_1 + ab$ where b is represented by $x^2 \oplus Q \sim diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\}$.

(1) b=0.Then:

$$diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\} \otimes diag\{1, a\}$$

$$\sim diag\{1, b_1\} \otimes ... \otimes diag\{1, b_n\} \otimes diag\{1, a\}$$

(2)$b_1 = 0$.Then $b_1^{'} = ab$,and:

$$diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\} \otimes diag\{1, a\}$$

$$\sim (diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\}) \oplus a(diag\{1, a_1 \otimes ... \otimes diag\{1, a_n\})$$

$$\sim (diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\}) \oplus ab(diag\{1, a_1 \otimes ... \otimes diag\{1, a_n\}) \quad (lemma 4.3.3))$$

$$\sim diag\{1, b_1^{'}\} \otimes diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\}$$

(3)$bb_1 \neq 0$.Then by the hypothesis:

$$diag\{1, a_1\} \otimes ... \otimes diag\{1, a_n\} \otimes diag\{1, ab\}$$

$$\sim diag\{1, b_1\} \otimes diag\{1, b_2\} \otimes ... \otimes diag\{1, b_n\} \otimes diag\{1, ab\}$$

And we have:

$$diag\{1, ab\} \otimes diag\{1, b_1\} \sim diag\{1, ab, b_1, abb_1\}$$

$$\sim diag\{1, abb_1\} \oplus diag\{b_1, ab\}$$

$$\sim diag\{1, abb_1\} \oplus diag\{b_1^{'}, b_1 abb_1^{'}\} \quad (lemma 4.3.1)$$

$$\sim diag\{1, b_1^{'}\} \otimes diag\{1, b_1 ab\}$$

□

Theorem 4.3.4. *Suppose that every Pfister form of dimension 2^n represents every non-zero sum of two squares in F.Then every Pfister form of dimension 2^n represents every non-zero sum of k squares in F for arbitrary k.*

Proof of theorem. We use induction on k.k=1 is clear and k=2 is the condition.

We may assume this for k: We want to prove that:Q is a Pfister form of dimension 2^n and a is a sum of k squares.

c=1+a,we need c is represented by Q.

$$Q = x^2 \oplus Q^{'}$$

Then:

$$diag\{1, -c\} \otimes Q \sim Q \oplus (-cQ) \sim x^2 \oplus Q^{'} \oplus (-cQ)$$

By theorem 4.3.3,we have:

$$diag\{1,-c\}\otimes Q \sim diag\{1,-1-x^2\}\otimes Q^{''}$$

where $Q^{''}$ is Pfister form of dimension 2^n. Hence:

$$Q\oplus(-cQ) \sim diag\{1,-1-x^2\}\otimes Q^{''}$$

Then $Q\oplus(-cQ)$ represents 0 non-trivially. □

4.4 Tsen-Lang's proof of Pfister theory

Some results of this will be in the proof of Hilbert 17th problem.In fact,these proof is based on Artin's theory .
We will begin with some definitions:

Definition 4.4.1. *A field F is called a C_i-field if for any positive integer d,and homogeneous polynomial f in F with degree d in more than d^i indeterminates has a non-trivial zero in $F^{(d^i)}$*

Here is the maim theorem of their proof:

Theorem 4.4.1. *If F is algebraically closed and $x's$ are indeterminates: F($x_1,...x_n$) is a C_n-field.*

The proof of this theorem is inductive. We will use some results in algebra without proof:

Lemma 4.4.2. *Let F be an algebraically closed,$f_1,...f_r$ polynomials without constant term of n indeterminate.If $n>r$,then $f_1(x_1,...,x_n)=0,...,f_r(x_1,...,x_n)=0$ has a non-trivial solution in $F^{(n)}$.*

Definition 4.4.2. *A polynomial with coefficients in F is called normic of order i(¿0) for F if it is homogeneous of degree $d > 1$ in d^i indeterminate and has only trivial zero.*

The next lemma gave an inductive proof:

Lemma 4.4.3. *If there exists a normic polynomial of order i for F,then there exists a normic polynomial of order i+1 for F(t).*

Proof of lemma. Let $F(x_1, ..., x_n)$ be a normic polynomial of order i.We claim:

$$F(x_1, ..., x_{d^i}) + F(x_{d^i+1}, ..., x_{2d^i})t + ... + F(x_{(d-1)d^i+1}, ..., x_{d^{i+1}})t^{d-1}$$

is a normic polynomial.

If this polynomial is equal to zero with $x_i \neq 0$ for some i.The root is $(a_1, ..., a_{d^{i+1}})$.

We may assume that k is the minimal k such that a_k is not divisible by t.

We suppose that $jd^i \leq k \leq (j+1)d^i$.

Then we have:

$$N(a_{jd^i+1}, ..., a_{(j+1)d^i}) \equiv 0(mod \quad t)$$

Hence the constant term:b_i of a_i:

$$N(b_{jd^i+1}, ..., b_{(j+1)d^i}) = 0$$

But N$(x_1, ..., x_{d^i})$ has no non-trivial root.

Contradiction. □

Lemma 4.4.4 (Artin)**.** *Let F be a C_i-field for which there exists a normic polynomial of order i.*

Let $f_1, ..., f_r$ be homogeneous polynomials of degree d in indeterminate $x_1, ..., x_n$ in F.If $n > rd^i$,then f's have a common non-trivial zero.

This lemma is an extension of lemma 4.4.2.Also,it's based on this.

Proof of lemma. Let N be a normic polynomial of order i.Degree of N is e. $e^i = rs + t$ where $0 \leq t < r$. We let:

$$M = N(f_1(x_1, ..., x_n), ..., f_r(x_1, ..., x_n)$$

$$, f_1(x_{n+1}, ..., x_{2n}), ..., f_r(x_{n+1}, ..., x_{2n}), ..., 0..., 0)$$

Where deg(M)=ed.

We want:$ns > (ed)^i > d^i rs$.

And we can choose different e:

For F is C_i-field,M has a non-trivial zero.Hence f_i have the common non-trivial zero in F. □

Lemma 4.4.5. *Let F be a C_i-field,such that there exists a normic polynomial of the order for F.Then F(t) is a C_{i+1}-field.*

Proof of lemma. For any polynomial f$(x_1, ..., x_n)$,where f is homogeneous of order d.And $n > d^{i+1}$.

We want to show that f has non-trivial roots.

For $x_j \in F(t)$,we may assume that:

$$x_j = x_{j0} + ... + x_{js}t^s, \quad 1 \leq j \leq n$$

Hence we have:

$$f = f_0 + f_1 t + ... + f_{sd+r}t^{sd+r}$$

We want to use lemma 4.4.4 to prove this lemma:we want to find a common non-trivial root of $f_0, ..., f_{sd+r}$.

Since $n > d^(i+1)$,then n(s+1)$> sd(d^i) + (r+1)d^i \quad (r < d)$. Hence there

exists a non-trivial root of f. □

Corollary 4.4.2.1. *Let i=0,then any algebraically closed field F,F(x) is a C_i-field.*

Now we prove the theorem 4.4.1 for any n.

By lemma 4.4.3, there exists a normic polynomial of order i for $F(x_1, ..., x_i)$. Then we use induction for n and by lemma 4.4.5,we get $F(x_1, ..., x_n)$ is a C_n-field.

Theorem 4.4.6. *Let R be a real closed field and let Q be a Pfister form on a 2^n-dimensional vector space over $R(x_1, ..., x_n)$.Then Q represents every non-zero sum of two squares in $R(x_1, ..., x_n)$*

Proof of theorem. We have $b = b_1^2 + b_2^2 \neq 0$,then b is represented by Q.

If $b_1 b_2 = 0$,Q represents 1 hence represents a square.

We may assume that $b_1 b_2 \neq 0$.

Let C=$R(\sqrt{-1})$,i=$\sqrt{-1}$.Then $C(x_1, ..., x_n)$ over $R(x_1, ..., x_n)$ is an extension.Let $q = b_1 + b_2 i$,(1,q) is a base for C over R.And :

$$q^2 - 2b_1 q + b = 0$$

There exists $\bar{x} = \bar{x_1} + q\bar{x_2}$,such that Q($\bar{x}$)=q. Then we have:

$$Q(\bar{x_1}) + 2qQ(\bar{x_1}, \bar{x_2}) + q^2 Q(u_2) = q$$

Since (1,q) is a base.We have $Q(\bar{x_1}) = bQ(\bar{x_2})$.b is represented by Q. □

Corollary 4.4.2.2. *Let R be a real closed field.Then any positive semi-definite rational function of n variables over R is a sum of 2^n squares.*

Proof. From Hilbert's 17th problem,we have any positive semi-definite rational function is a sum of squares.

By theorem 4.4.6,we have Pfister form Q represents any non-zero sum of two squares.

We can see that this conclusion is just the hypothesis of Theorem 4.3.4.

Now by theorem 4.3.4,we have:

The sum of squares in R$(x_1, ..., x_n)$ is a sum of 2^n squares. □

Hence we have proved the main result of this section.
More exactly,we can take a number $n \leq k(n) \leq 2^n$ such that a sum of squares is a sum of k(n) squares.

5 History around Hilbert's 17th problem

We proved all the theorem in section 1,2,3,4.Now,I will tell you the history of Hilbert 17th Problem.
The starting point of Hilbert's 17th problem:in 1885,The 21 year old Minkowski expressed his opinion that there exist real polynomials which are non-negative on the whole R^n and cannot be written as finite sums of squares of real polynomials.
But David.Hilbert didn't agree with.In 1888 Hilbert proved in a now famous paper the existence of a real polynomial in two variables of degree six which is non-negative on R^2 but not a sum of squares of real polynomials.His proof is based on algebraic curves.
The first explicit example of this kind was given by T. Motzkin in 1967. It is the polynomial:

$$M(x, y) = x^4y^2 + x^2y^4 + 1 - 3x^2y^2.$$

If $M = \sum f_j^2$,since M(0,y)=M(x,0)=0,we have:

$$f_j = a_j + b_jxy + c_jx^2y + d_jxy^2$$

Hence we have:

$$-3 = \sum b_j^2$$

contradiction.
Hilbert also showed that each non-negative polynomial in two variables of degree four is a finite sum of squares of polynomials.
But here polynomials are not rational polynomials.
In 1893, Hilbert proved by an ingenious and difficult reasoning that each non-negative polynomial $p \in R[x, y]$ on R^2 is a finite sum of squares of rational functions from R(x, y).
Here:

$$M(x,y) = \frac{x^4y^2(x^2+y^2-2)^2 + x^2y^4(x^2+y^2-2)^2 + x^2y^2(x^2+y^2-2)^2 + (x^2-y^2)^2}{(x^2+y^2)^2}$$

Motivated by his previous work Hilbert posed his famous 17th problem at the International Congress of Mathematicians in Paris (1900):
Hilbert's 17th problem:
Suppose that $f \in R(x_1, ..., x_n)$ is positive semi-definite rational polynomial.Is f a finite sum of squares of rational functions?
In 1927,E.Artin used Artin-Schreier's real closed field theory:the section 1 of the paper,to prove the problem.
I didn't give the proof of Artin.Artin's proof is non-constructive.It is based on Polya's theory about homogeneous polynomial.
The proof of Hilbert's 17th problem is based on model theory.In 1955,A.Robinson gave the proof using quantifier elimination.It's much easier.
There is also a quantitative version of Hilbert's 17th problem which asks how many squares are needed.In fact,this is the section 4 in the paper:Pfister's theory.
For a ring K, the pythagoras number p(K) is the smallest natural number m such that each finite sum of squares of elements of K is a sum of m squares.
Pfister's theory showed that:

$$p(R(x_1, ..., x_n) \leq 2^n$$

His proof is used Pfister's form.
What is the $p(R(x_1, ..., x_n))$ exactly?
In fact,for $n \geq 3$ is still unknown.For n=2,by the theory of elliptic curves over algebraic function fields,we can show that polynomial $M(x, y)$ is not a sum of 3 squares.
Artin's theorem(Hilbert's 17th problem) triggered many further developments. The most important one in the context of optimization is to look for polynomials which are nonnegative on sets defined by polynomial inequalities rather than the whole R^n.
In real algebraic geometry,we define this set:semi-algebraic set in section 2.
The preorder:

$$T_F := \{ \sum_{\epsilon_i \in \{0,1\}} f_1^{\epsilon_1} ... f_k^{\epsilon_k} \sigma_\epsilon | \sigma_\epsilon \in \sum_n^2 \}$$

In fact,the T_F are positive semi-definite on closed semi-algebraic set.
In 1991,there exists a result of Positivstellensatz.

References

[1] M. Atiyah and I. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading, MA, 1996.

[2] Emil Artin and Otto Schreier, Algebraische Konstruktion reeller K¨orper, Abh. Math. Sem. Univ. Hamburg 5 (1927), 85–99.

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

[4] J.S.W. Cassels, W.J. Ellison and A. Pfister, On sums of squares and on elliptic curves over function fields, J. Number Theory 3(1971), 125–49

[5] H. Bochnak, M. Coste, M.-F. Roy. Real algebraic geometry. Springer, 1998

[6] G. Stengle. A Nullstellensatz and a Positivstellensatz in semialgebraic geometry.Math. Ann., 207 (1974), 87–97.

[7] G.Kreisel,J.L.Krivine,Elements of Mathematical logic.

[8] A. Pfister, Quadratic Forms and Applications in Algebraic Geometry and Topology, London Math. Soc. Lect. Notes 217, Cambridge, 1995.

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

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

[11] Jakobson,N.Lectures in Abstract Algebra, vol.III,Van Nostrand Inc., (1964).

[12] Jakobson,N.Basic Algebra, 2 vols. W.I. Freeman (1974)

[13] McKenna,K.New facts about Hilbert's seventeenth problem, in Model Theory and Algebra, A Memorial Tribute to A. Robinson, Lect.Notes Math 498(1975), pp.220-230.

[14] Robinson,A.On ordered fields and definite functions. Math. Ann. 130(1955) ,pp. 257-271.

[15] Tarski,A.A decision method for elementary algebra and geometry 2nd. revised ed., Berkeley, Los Angeles (1951).