ALEXANDER PRESTEL

Model theory of fields : an application to positive semidefinite polynomials

_Mémoires de la S. M. F._ 2e série, tome 16 (1984), p. 53-65

<http://www.numdam.org/item?id=MSMF_1984_2_16__53_0>
MODEL THEORY OF FIELDS:
AN APPLICATION TO POSITIVE SEMIDEFINITE POLYNOMIALS

Alexander Prestel

Abstract: Using some model theoretic arguments, we will settle the following problem raised by E. Becker: Which polynomials \( f \in \mathbb{R}[X_1, \ldots, X_n] \) can be written as a finite sum of \( 2m \)-th powers of rational functions in \( X_1, \ldots, X_n \) over \( \mathbb{R} \)?

INTRODUCTION

From Artin's solution of Hilbert's 17-th Problem, it is clear that polynomials \( f \in \mathbb{R}[X_1, \ldots, X_n] \) which can be written as a sum of squares of rational functions in \( \bar{X} = (X_1, \ldots, X_n) \) over \( \mathbb{R} \) are exactly the positive semidefinite ones, i.e. those satisfying \( f(\bar{a}) \geq 0 \) for all \( \bar{a} = (a_1, \ldots, a_n) \in \mathbb{R}^n \). In view of this result, the question naturally arises under what conditions such an \( f \) can be even written as a sum of \( 2m \)-th powers of rational functions in \( \bar{X} \) over \( \mathbb{R} \).

Denoting for a ring \( R \), by \( \sum R^s \) the set of finite sums of \( s \)-th powers of elements from \( R \), the question then is: When does \( f \in \sum \mathbb{R}(\bar{X})^{2m} \) hold? For odd exponents the answer is trivial, since \( \mathbb{R}(\bar{X}) = \sum \mathbb{R}(\bar{X})^{2m+1} \) by a result of Joly (see [J], Théorème (2.8)).
We will give the following answer for homogeneous polynomials $f$:

**THEOREM 1** Let $f \in \mathbb{R}[X_1, \ldots, X_n]$ be homogeneous and positive semi-definite. Then $f \in \Sigma \mathbb{R}(\bar{x})^{2m}$ if and only if $2m \mid \deg f$ and $2m \mid \text{ord} f(p_1, \ldots, p_n)$ for all polynomials $p_1, \ldots, p_n \in \mathbb{R}[t]$ with at least one $p_i$ having a non-vanishing absolute term.

Here $\text{ord} h(t)$ is the order of $h(t)$ at the place $t = 0$, i.e. the maximal $r$ such that $t^r$ divides $h(t)$. The proof of this theorem ultimately makes use of the Ax-Kochen-Ershov Theorem on the model completeness of certain classes of henselian fields.

Clearly, one is tempted to ask the corresponding question for polynomials $f \in K_0[X_1, \ldots, X_n]$ where $K_0$ is some other formally real field. The main theorem of this note refers to a fixed archimedean ordering on $K_0$. Thus, in particular, if $R$ is some archimedean real closed field, we will have the same situation as in Theorem 1. All attempts to generalize this result to non-archimedean real closed fields failed, and, as it finally turned out, must fail.

In case Theorem 1 would hold for all real closed fields $R$ and for $n = 2$, by the Compactness Theorem one could conclude that for each $d \in \mathbb{N}$, there were some formula $\varphi(a_o, \ldots, a_d)$, in the language of rings, such that for all real closed fields $R$ we could get (after dehomogenizing)

$$R \not\models \varphi(a_o, \ldots, a_d) \iff a_o + \ldots + a_dx^d \in \Sigma \mathbb{R}(X)^{2m}.$$  

Equivalently, one could find bounds $N$ and $s$, depending only on $d$ and $m$ such that, for all $a_o, \ldots, a_d \in R$, $f = a_o + \ldots + a_dx^d \in \Sigma \mathbb{R}(X)^{2m}$

*) This is no restriction of the generality.
This, however, turns out to be wrong in general. Using a simple non-standard argument (i.e. an application of the Compactness Theorem), we will prove

**THEOREM 2** For all $m \geq 2$ and all $n \geq 0$,
\[
x^{2m} + nx^2 + 1 = h^{(n)}(x)-2m \prod_{i=1}^{N(n)} g_i^{(n)}(x)^{2m}.
\]
Moreover, if $n$ tends to infinity, so does $N(n)$ or $\deg h^{(n)}$.

By this theorem and the remarks above, Theorem 1 cannot hold for arbitrary real closed fields $R$. In fact, Theorem 2 shows that, for $m \geq 2$, the property 'f $\in \Sigma R$' is not elementary in the coefficients of $f$. This should be seen in contrast to the case $m = 1$. In this case, $f \in \Sigma R^2$ can be expressed by the formula
\[
\forall a_1, \ldots, a_n \exists b \ f(a_1, \ldots, a_n) = b^2,
\]
saying that $f$ is positive semidefinite.

1. On Theorem 1

In [1] Becker developed a general theory of sums of $2m$-th powers in formally real fields. From this theory ([1], Satz 2.14) one obtains the following characterization: Let $K$ be formally real. Then for any $a \in K$:

\[
a \in \Sigma K^2 \iff \left\{ \begin{array}{l}
a \in \Sigma K^{2m} \text{ and } 2m\mid v(a) \text{ for all valuations } v \text{ of } K \\
\text{with formally real residue field } \bar{K}_v.\end{array} \right.
\]
A. PRESTEL

A valuation here and in what follows may have an arbitrary ordered abelian group \( \Gamma \) as group of values. By \( 2^m | v(a) \) we then mean that there is some \( b \in K \) satisfying \( 2^m v(b) = v(b^{2^m}) = v(a) \). Concerning the theory of valuations we refer the reader to [3] and [4].

The first lemma will be a slight generalization of the above equivalence. For its proof we need some notations and results from [1].

A subset \( S \) of \( K \) is called a **preordering** of level \( 2^m \) if

\[(i) \quad S + S \subseteq S, \quad S \cdot S \subseteq S, \quad K^{2^m} \subseteq S, \quad -1 \notin S.\]

In case \( m = 1 \), we obtain the usual notion of preordering (cf. [7]). A preordering \( S \) of level \( 2^m \) is called **complete** if

\[(ii) \quad a^2 \in S \text{ implies } a \in S \cup -S.\]

In what follows, complete preorderings will always be denoted by \( P \). If \( m = 1 \), completeness of \( P \) just means \( P \cup -P = K \). Thus in this case, \( P \) is an ordering in the usual sense. In general,

\[a \preceq_P b \iff b - a \in P\]

defines a partial ordering on \( K \), which for level 2 is linear. By [1], Section 1, for any preordering \( S \) of level \( 2^m \) we have

\[(iii) \quad S = \bigcup_{S \in P} P\]

where \( P \) ranges over complete preorderings of level \( 2^m \).

From [1], Section 2, we further obtain that for every complete preordering \( P \) of level \( 2m \),

\[(iv) \quad A_p = \{ x \in K | -n \preceq_P x \preceq_P n \text{ for some } n \in \mathbb{N} \} \]

defines a valuation ring on \( K \) such that \( 1 + M_p \subset P \) and \( \overline{P \cap A_p} \)

is an ordering (of level 2) of the residue field \( \overline{K_p} \).
Here $M_p$ denotes the maximal ideal of $A_p$ and $\tilde{a}$ the residue of $a$, i.e. $\tilde{a} = a + M_p$.

**Lemma 1** Let $P_o$ be an archimedean ordering of the subfield $K_o$ of $K$. Then $a \in K$ belongs to $\Sigma P_o \cdot K^{2m}$ if and only if $a \in \Sigma P_o \cdot K^2$ and $2m|v(a)$ for every valuation $v$, real over $P_o$.

Let $v$ have valuation ring $A$ and residue field $\bar{K}$. We call $v$ real over $P_o$, if $P_o \cap A$ is an ordering of $\bar{K}$ which extends to some ordering of $\bar{K}$. Since $P_o$ is archimedean, it follows that $v$ must be trivial on $K_o$, i.e. $v(K_o) = \{0\}$ or, equivalently, $K_o \subseteq A$. Moreover, it follows that the set $\Sigma P_o \cdot K^{2m}$ of sums of $2m$-th powers with coefficients from $P_o$, actually is a preordering of level $2m$ on $K$.

**Proof:** First assume that $a \in \Sigma P_o \cdot K^{2m}$. Then clearly $a \in \Sigma P_o \cdot K^2$. But also $2m|v(a)$ is easily seen for valuations $v$, real over $P_o$. Indeed, for such a valuation we have

\[(v) \quad v(\Sigma p_i x_i^2) = \min\{v(p_i x_i^2)\}.
\]

In fact, if $v(p_i x_i^2)$ is of minimal value, then $\Sigma (p_i x_i^2)^{-1} (p_i x_i^2)$ belongs to $A_v$ and yields a non-vanishing residue class in $\bar{K}_v$ by the assumption on $v$. Thus its value is $0$. This proves $(v)$. Now $(v)$ and $a = \Sigma p_i a_i^{2m}$ clearly imply $2m|v(a)$.

Next assume the conditions on the RHS of the lemma. If $a \notin \Sigma P_o \cdot K^{2m}$, then by (iii) there is a complete preordering $P$ such that $a \notin P$. By (iv), $P$ defines the valuation ring $A_P$. Let $v_P$ denote a valuation corresponding to $A_P$. Note that $K_o \subseteq A_P$ since $P_o$ is archimedean. Thus $v_P$ is trivial on $K_o$. Moreover, $P_o \cap A_P$ is an ordering of the residue field which clearly extends $P_o \cap A_P$.
Hence we know that $2m|v_p(a)$. Let $b \in K$ be such that $v(ab^{-2m}) = 0$. Then $ab^{-2m}$ is a unit. Since $ab^{-2m} \in \Sigma P_0 \cdot K^2$, the residue class \[ab^{-2m}\] belongs to the ordering $\frac{P \cap A_p}{K}$ of $\bar{K}$. Therefore we can find $p \in P$ such that \[ab^{-2m} \cdot p^{-1} \in 1 + M_p.\]

Since $1 + M_p \subset P$, this implies $a \in P$, a contradiction.

q.e.d.

We will now apply Lemma 1 to the situation where $P_0$ is an archimedean ordering of $K_0$ and $K = K_0(X_1, \ldots, X_n)$, the field of rational functions in $\bar{X} = (X_1, \ldots, X_n)$ over $K_0$. By $R_0$ we denote the real (algebraic) closure of $K_0$ with respect to $P_0$. Moreover, $R_0((t))$ denotes the field of formal Laurent series \[\rho = \sum_{i=r}^{\infty} a_i t^i \quad \text{with} \quad a_i \in R_0, \ r \in \mathbb{Z}.\]

The canonical valuation on $R_0((t))$ is denoted by ord. We have \[\text{ord}(\sum_{i=r}^{\infty} a_i t^i) = r \quad \text{if} \quad a_r \neq 0.\]

If almost all coefficients $a_i$ vanish, $\rho$ is called a finite Laurent series.

**MAIN THEOREM** With the above notations, the following are equivalent for all $f \in K_0[\bar{X}]:$

1. $f \in \Sigma P_0 \cdot K_0(\bar{X})^{2m},$
2. $f$ is positive semidefinite over $R_0$ and $2m|\text{ord } f(\rho_1, \ldots, \rho_n)$ for all $\rho_1, \ldots, \rho_n \in R_0((t)),$
3. the same as in (2) except that $\rho_1, \ldots, \rho_n$ are finite Laurent series.
MODEL THEORY OF FIELDS

Proof: (1)⇒(2): Clearly, \( f \) is positive semidefinite over \( R_0 \).

Next observe that the substitutions \( x_i \to \rho_i \) define a homomorphism
from \( K_0[\bar{x}] \) to \( R_0((t)) \) which can be easily extended to some place
from \( K_0(\bar{x}) \) to \( R_0((t)) \). Lifting the valuation \( \text{ord} \) from \( R_0((t)) \) through
this place, we obtain a valuation \( v \) on \( K = K_0(\bar{x}) \) with residue
field contained in \( R_0 \). Thus \( v \) is real over \( P_0 \). By Lemma 1 we
therefore have \( 2m|v(f) \). From the construction of \( v \), this implies
\( 2m|\text{ord } f(\rho_1,\ldots,\rho_n) \).

Since \((2)⇒(3)\) is trivial, it remains to prove \((3)⇒(1)\), which is
the main point of this theorem. From the positive semidefiniteness of
\( f \) over \( R_0 \) it follows by well-known arguments that \( f \in \Sigma P_0 \cdot K_0(\bar{x}) \).
Thus in view of Lemma 1, it remains to prove \( 2m|v(f) \) for every
valuation \( v \) of \( K \), real over \( P_0 \). As explained after Lemma 1, \( v \)
is trivial on \( K_0 \). Thus \( v \) is a place of the function field \( K/K_0 \)
in the usual sense. (We may consider \( K_0 \) as a subfield of \( \bar{K}_v \).
Let us assume \( 2m \not\mid v(f) \).

By the result of [6] we know that we may replace the valuation
\( v \) by some other valuation \( v' \), trivial on \( K_0 \), still satisfying
\( 2m \not\mid v'(f) \), but having additional properties

(a) value group of \( v' \) is \( \mathbb{Z} \),
(b) residue field of \( v' \) is a subfield of \( \bar{K}_v \) finitely generated over
\( K_0 \).

Since \( v \) is real over \( P_0 \), the residue field \( \bar{K}_v \) admits an ordering
extending that of \( K_0 \). Hence the well-known theory of function fields

*) The proof of this 'density' theorem for places on function fields
makes essential use of the Ax-Kochen-Ershov Theorem mentioned in
the introduction.
A. PRESTEL

over real closed fields yields a place from the residue field $\bar{K}_{v'}$ of $v'$ to the real closure $R_O$ of $K_O$ with respect to $P_O$; i.e., a valuation $\tilde{w}$ of $\bar{K}_{v'}$, trivial on $K_O$, with residue field contained in $R_O$. The valuation $\tilde{w}$ of $\bar{K}_{v'}$ can be lifted through $v'$ to some refinement $w$ of $v'$. Then, the value group $\tilde{w}(\bar{K}_{v'})$ is an isolated subgroup of the value group $w(K)$, the quotient being isomorphic to $v'(K)$. Thus $w$ is a valuation of $K$, trivial on $K_O$, with residue field contained in $R_O$ and still satisfying $2m+w(f)$. Applying once more the above mentioned result of [6], we finally obtain a valuation $w'$, trivial on $K_O$, such that $2m+w'(f)$ and

(a) value group of $w'$ is $\mathbb{Z}$,
(b) residue field of $w'$ is a subfield of $R_{w'}$, finitely generated over $K_O$.

Thus, in particular $\bar{K}_{w'}$ is contained in $R_O$.

We now pass from $K$ to the completion $\hat{K}_w$ of $K$ with respect to the valuation $w'$. From the above properties of $w'$ we conclude that $\hat{K}_w$, and hence also $K$ may be identified with some subfield of $R_O((t))$ such that ord induces $w'$ on $K$. Hence $X_1,\ldots,X_n$ are identified with some Laurent series $\rho_1,\ldots,\rho_n \in R_O((t))$ and thus $2m+\text{ord } f(\rho_1,\ldots,\rho_n)$.

Finally, we observe that in the topology induced by the valuation ord on $R_O((t))$,

$$\sum_{i=r}^{s} a_i t^i = \lim_{s \to \infty} \sum_{i=r}^{s} a_i t^i .$$

By the continuity of $f$ and the fact that the set $\{ \rho \in R_O((t)) | 2m+\text{ord } \rho \}$ is open, we may assume that $\rho_1,\ldots,\rho_n$ are finite Laurent series satisfying $2m+\text{ord } f(\rho_1,\ldots,\rho_n)$. This contradiction to the assumptions of (3) proves (1). q.e.d.
Proof of Theorem 1: Assume first $f \in \Sigma \mathbb{R}(\bar{x})^{2m}$. We may assume that $f$ actually is a polynomial in $X_1$. Applying now condition (3) of the Main Theorem to $\rho_1 = at$ and $\rho_n = t, \ldots, \rho_n = t$ and choosing $a \in \mathbb{R}$, such that $f(at, t, \ldots, t) \neq 0$, we conclude that $2m \mid \deg f$.

Since every polynomial in $t$ in particular is a finite Laurent series, (3) yields the necessity of the condition in Theorem 1.

Conversely, let $2m \mid \deg f = d$ and $2m \mid \ord(p_1, \ldots, p_n)$ for all $p_i \in \mathbb{R}[t]$ such that $\ord p_i = 0$ for at least one $p_i$. Let $\rho_1, \ldots, \rho_n$ be finite Laurent series in $t$. If $r = \min\{\ord \rho_i\}$, clearly all $p_i = \rho_i t^{-r}$ are polynomials, one having $\ord = 0$.

Thus it follows from the condition in Theorem 1 that $2m \mid \ord f(p_1, \ldots, p_n)$.

From

$$f(p_1, \ldots, p_n) = f(\rho_1 t^{-r}, \ldots, \rho_n t^{-r}) = t^{-dr} f(\rho_1, \ldots, \rho_n)$$

and $2m \mid d$ we therefore conclude $2m \mid \ord f(\rho_1, \ldots, \rho_n)$ as asserted in (3) of the Main Theorem. Now the equivalence of (3) and (1) yields the result $f \in \Sigma \mathbb{R}(\bar{x})^{2m}$.

q.e.d.

It should be observed that there is no restriction in considering homogeneous polynomials only. One easily checks the following

Remark: Let $f(X_1, \ldots, X_n)$ be a polynomial of degree $d$ over a formally real field $K_0$. Then $f \in \Sigma K_0(X_1, \ldots, X_n)^{2m}$ if and only if

$$X_o^d \cdot f \left( \frac{X_1}{X_o}, \ldots, \frac{X_n}{X_o} \right) \in \Sigma K_0(X_0, X_1, \ldots, X_n)^{2m}.$$  

The following corollary is an immediate consequence of the equivalence of the Main Theorem, observing that a polynomial $f \in \mathbb{Q}[\bar{x}]$ is positive semidefinite over $\mathbb{R}$ if it is so over $\mathbb{Q}$. With a little
A. PRESTEL

more effort, this corollary can already be deduced from Lemma 1.

COROLLARY Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$. Then $f \in \Sigma \mathbb{R}(\bar{x})^{2m}$ if and only if $f \in \Sigma \mathbb{Q}(\bar{x})^{2m}$.

2. On Theorem 2

Let us now consider the case $n = 1$, i.e. $K = K_0(X)$. As before we assume that $P_0$ is an archimedean ordering of $K_0$. The valuations $v$ of $K$, real over $P_0$, are trivial on $K_0$. The totality of these valuations is well-known. Such a valuation is either the 'degree'-valuation of $K_0(X)$ or corresponds one-to-one to a pair consisting of an irreducible polynomial $p \in K_0[X]$ and a zero of $p$ in $R_0$, the real (algebraic) closure of $K_0$ with respect to $P_0$. Thus the following lemma is already a consequence of Lemma 1.

LEMMA 2 With the notations from above, a polynomial $f \in K_0[X]$ belongs to $\Sigma P_0K_0(X)^{2m}$ if and only if $f$ is positive semidefinite over $R_0$, $2m|\deg f$ and, in the factorization of $f$, $2m$ divides the exponent of every prime polynomial $p$ having a zero in $R_0$.

Specializing $K_0$ to $\mathbb{R}$ and $P_0$ to the unique ordering of $\mathbb{R}$, we proceed to the

Proof of Theorem 2: Note first of all that the polynomial $x^{2m} + nx^2 + 1$ is positive definite, has no real zero and its degree is divisible by $2m$. Hence by Lemma 2 we can find a natural number $N(n)$ and polynomials $g_i^{(n)}$, $h^{(n)} \in \mathbb{R}[X]$ ($1 \leq i \leq N(n)$) such that

$$x^{2m} + nx^2 + 1 = \sum_{i=1}^{N(n)} \frac{g_i^{(n)}(x)^{2m}}{h^{(n)}(x)^{2m}}$$
MODEL THEORY OF FIELDS

Assume that there are bounds $N$ and $d$, independent of $n$, such that for all $n$

$$N(n) \leq N \quad \text{and} \quad \deg h^{(n)} \leq d.$$

Then we also have

$$\deg g^{(n)}_i \leq d + 1 \quad \text{for all} \quad i \leq N(n).$$

By this assumption, it is possible to express the phrase

$$(\forall n \in \mathbb{N})(\exists g_1, \ldots, g_N, h)(x^{2m} + nx^2 + 1)h^{2m} = \sum_{i=1}^{N} g_i^{2m}$$

by a formula $\varphi$ in the first order language of fields, involving some unary predicate for $\mathbb{N}$. Thus

$$(\mathbb{R}, \mathbb{N}) \models \varphi.$$  

Let $(\mathbb{R}^*, \mathbb{N}^*)$ be a proper elementary extension of $(\mathbb{R}, \mathbb{N})$. Then, as it is well-known $\mathbb{N}^*$ contains elements which are bigger than every $n \in \mathbb{N}$. Let $\omega$ be such a non-standard natural number. Since $\varphi$ also holds in $(\mathbb{R}^*, \mathbb{N}^*)$, we conclude that

$$(*) \quad x^{2m} + \omega x^2 + 1 \in \Sigma \mathbb{R}^*(X)^{2m}.$$  

This will lead us to a contradiction.

Let $v^*$ be a valuation on $\mathbb{R}^*$ which corresponds to the valuation ring

$$A = \{x \in \mathbb{R}^*| -n \leq x \leq n \quad \text{for some} \quad n \in \mathbb{N}\}.$$  

Note that $v^*$ has a formally real residue field; in fact, $\mathbb{R}_{v^*} = \mathbb{R}$. Moreover, $v^*(\omega) < 0$ if we write the valuation additively. Now by [3], Ch.VI, §10, Proposition 1, $v^*$ can be extended to a valuation $v$ of $\mathbb{R}^*(X)$ by setting
A. PRESTEL

\[ v(a_nx^n + \ldots + a_0) = \min \{ (v^*(a_i), i) \} \]

where the value group is \( v^*(\mathbb{R}^*) \times \mathbb{Z} \), ordered lexicographically such that the first component dominates. This extension has the same residue field as \( v^* \), hence is a valuation of \( \mathbb{R}^*(X) \) to which the condition of Lemma 1 applies. From (*) we therefore conclude

\[ 2m | v(X^{2m} + \omega X^2 + 1) = (v^*(\omega), 2) . \]

This is a contradiction, since \( 2m \) does not divide \( 2 \), except for \( m = 1 \).

q.e.d.

Using a result of Becker ([2], Theorem 2.9), we can find a bound \( N \) in Theorem 2 depending only on \( m \). (In fact, if \( m = 2 \), we may take \( N = 36 \).) Then the assertion of Theorem 2 may be modified, saying that for this fixed \( N \), \( \deg h^{(n)} \) tends to infinity, if \( n \) does.

REFERENCES


MODEL THEORY OF FIELDS


Alexander Prestel
Fakultät für Mathematik
Universität, Postfach 5560
7750 Konstanz
West-Germany