

MÉMOIRES DE LA S. M. F.

ALEXANDER PRESTEL

Model theory of fields : an application to positive semidefinite polynomials

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

http://www.numdam.org/item?id=MSMF_1984_2_16__53_0

© Mémoires de la S. M. F., 1984, tous droits réservés.

L'accès aux archives de la revue « Mémoires de la S. M. F. » (<http://smf.emath.fr/Publications/Memoires/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

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 $f \in \mathbb{R}[X_1, \dots, X_n]$ can be written as a finite sum of $2m$ -th powers of rational functions in X_1, \dots, X_n over \mathbb{R} ?

INTRODUCTION

From Artin's solution of Hilbert's 17-th Problem, it is clear that polynomials $f \in \mathbb{R}[X_1, \dots, X_n]$ which can be written as a sum of squares of rational functions in $\bar{X} = (X_1, \dots, X_n)$ over \mathbb{R} are exactly the positive semidefinite ones, i.e. those satisfying $f(\bar{a}) \geq 0$ for all $\bar{a} = (a_1, \dots, a_n) \in \mathbb{R}^n$. 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 ΣR^S the set of finite sums of s -th powers of elements from R , the question then is: When does $f \in \Sigma \mathbb{R}(\bar{X})^{2m}$ hold? For odd exponents the answer is trivial, since $\mathbb{R}(\bar{X}) = \Sigma \mathbb{R}(\bar{X})^{2m+1}$ by a result of Joly (see [J], Théorème (2.8)).

0037-9484/84 03 53 13/\$ 3.30/ © Gauthier-Villars

We will give the following answer for homogeneous^{*)} polynomials f :

THEOREM 1 Let $f \in \mathbb{R}[X_1, \dots, X_n]$ be homogeneous and positive semi-definite. Then $f \in \Sigma \mathbb{R}(\bar{X})^{2m}$ if and only if $2m \mid \deg f$ and $2m \mid \text{ord } f(p_1, \dots, p_n)$ for all polynomials $p_1, \dots, p_n \in \mathbb{R}[t]$ 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 $f \in K_0[X_1, \dots, X_n]$ 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 \mathbb{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 \mathbb{R} and for $n = 2$, by the Compactness Theorem one could conclude that for each $d \in \mathbb{N}$, there were some formula $\varphi(a_0, \dots, a_d)$, in the language of rings, such that for all real closed fields \mathbb{R} we could get (after dehomogenizing)

$$\mathbb{R} \models \varphi(a_0, \dots, a_d) \text{ iff } a_0 + \dots + a_d X^d \in \Sigma \mathbb{R}(X)^{2m}.$$

Equivalently, one could find bounds N and s , depending only on d and m such that, for all $a_0, \dots, a_d \in \mathbb{R}$, $f = a_0 + \dots + a_d X^d \in \Sigma \mathbb{R}(X)^{2m}$

^{*)} This is no restriction of the generality.

implies

$$f = \sum_{i=1}^N \frac{g_i(X)^{2m}}{h_i(X)^{2m}} \quad \text{and} \quad \deg g_i, \deg h_i \leq s.$$

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 $n \geq 0$,

$X^{2m} + nX^2 + 1 = h^{(n)}(X)^{-2m} \sum_{i=1}^{N(n)} g_i^{(n)}(X)^{2m}$. 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 ' $f \in \Sigma R(\bar{X})^{2m}$ ' is not elementary in the coefficients of f . This should be seen in contrast to the case $m = 1$. In this case, $f \in \Sigma R(\bar{X})^2$ can be expressed by the formula

$$\forall a_1, \dots, a_n \exists b \quad f(a_1, \dots, a_n) = b^2,$$

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 $a \in K$:

$$a \in \Sigma K^{2m} \quad \text{iff} \quad \begin{cases} a \in \Sigma K^2 \text{ and } 2m \mid v(a) \text{ for all} \\ \text{valuations } v \text{ of } K \text{ with formally} \\ \text{real residue field } \bar{K}_v. \end{cases}$$

A. PRESTEL

A valuation here and in what follows may have an arbitrary ordered abelian group Γ as group of values. By $2m|v(a)$ we then mean that there is some $b \in K$ satisfying $2m v(b) = v(b^{2m}) = v(a)$. 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 $2m$ if

$$(i) \quad S + S \subset S, S \cdot S \subset S, K^{2m} \subset S, -1 \notin S.$$

In case $m = 1$, we obtain the usual notion of preordering (cf. [7]).

A preordering S of level $2m$ 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,

$$a \leq_P b \quad \text{iff} \quad b - a \in P$$

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

$$(iii) \quad S = \bigcup_{S \subset P} P$$

where P ranges over complete preorderings of level $2m$. From [1], Section 2, we further obtain that for every complete preordering P of level $2m$,

$$(iv) \quad A_P = \{x \in K \mid -n \leq_P x \leq_P n \text{ for some } n \in \mathbb{N}\} \text{ defines a valuation ring on } K \text{ such that } '1 + M_P \subset P \text{ and } \overline{P \cap A_P} \text{ is an ordering (of level 2) of the residue field } \bar{K}_P.$$

MODEL THEORY OF FIELDS

Here M_p denotes the maximal ideal of A_p and \bar{a} the residue of a , i.e. $\bar{a} = a + M_p$.

LEMMA 1 Let P_0 be an archimedean ordering of the subfield K_0 of K . Then $a \in K$ belongs to $\Sigma P_0 \cdot K^{2m}$ if and only if $a \in \Sigma P_0 \cdot K^2$ and $2m \mid v(a)$ for every valuation v , real over P_0 .

Let v have valuation ring A and residue field \bar{K} . We call v real over P_0 , if $\overline{P_0 \cap A}$ is an ordering of \bar{K}_0 which extends to some ordering of \bar{K} . Since P_0 is archimedean, it follows that v must be trivial on K_0 , i.e. $v(K_0) = \{0\}$ or, equivalently, $K_0 \subset A$. Moreover, it follows that the set $\Sigma P_0 \cdot K^{2m}$ of sums of $2m$ -th powers with coefficients from P_0 , actually is a preordering of level $2m$ on K .

Proof: First assume that $a \in \Sigma P_0 \cdot K^{2m}$. Then clearly $a \in \Sigma P_0 \cdot K^2$. But also $2m \mid v(a)$ is easily seen for valuations v , real over P_0 . Indeed, for such a valuation we have

$$(v) \quad v\left(\sum_i p_i x_i^2\right) = \min\{v(p_i x_i^2)\}.$$

In fact, if $v(p_1 x_1^2)$ is of minimal value, then $\sum_i (p_i x_i^2)^{-1} (p_i x_i^2)$ 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 $a = \sum p_i a_i^{2m}$ clearly imply $2m \mid v(a)$.

Next assume the conditions on the RHS of the lemma. If $a \notin \Sigma P_0 \cdot K^{2m}$, 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 $K_0 \subset A_p$ since P_0 is archimedean. Thus v_p is trivial on K_0 . Moreover, $\overline{P \cap A_p}$ is an ordering of the residue field which clearly extends $\overline{P_0 \cap A_p}$.

A. PRESTEL

Hence we know that $2m \mid v_p(a)$. Let $b \in K$ be such that $v(ab^{-2m}) = 0$. Then ab^{-2m} is a unit. Since $ab^{-2m} \in \Sigma P_O \cdot K^2$, the residue class $\overline{ab^{-2m}}$ belongs to the ordering $\overline{P \cap A_P}$ of \bar{K} . Therefore we can find $p \in P$ such that

$$ab^{-2m} p^{-1} \in 1 + M_P.$$

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_O is an archimedean ordering of K_O and $K = K_O(X_1, \dots, X_n)$, the field of rational functions in $\bar{X} = (X_1, \dots, X_n)$ over K_O . By R_O we denote the real (algebraic) closure of K_O with respect to P_O . Moreover, $R_O((t))$ denotes the field of formal Laurent series

$$\rho = \sum_{i=r}^{\infty} a_i t^i \quad \text{with } a_i \in R_O, r \in \mathbb{Z}.$$

The canonical valuation on $R_O((t))$ is denoted by ord . We have

$$\text{ord}\left(\sum_{i=r}^{\infty} a_i t^i\right) = r \quad \text{if } a_r \neq 0.$$

If almost all coefficients a_i vanish, ρ is called a finite Laurent series.

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

- (1) $f \in \Sigma P_O \cdot K_O(\bar{X})^{2m}$,
- (2) f is positive semidefinite over R_O and $2m \mid \text{ord } f(\rho_1, \dots, \rho_n)$ for all $\rho_1, \dots, \rho_n \in R_O((t))$,
- (3) the same as in (2) except that ρ_1, \dots, ρ_n are finite Laurent series.

MODEL THEORY OF FIELDS

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

Next observe that the substitutions $x_i \rightarrow \rho_i$ 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 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 $2m \mid v(f)$. From the construction of v , this implies $2m \mid \text{ord } f(\rho_1, \dots, \rho_n)$.

Since (2) \Rightarrow (3) is trivial, it remains to prove (3) \Rightarrow (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 $f \in \Sigma P_0 \cdot K_0(\bar{X})^2$. Thus in view of Lemma 1, it remains to prove $2m \mid v(f)$ 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 $2m \nmid v(f)$.

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 $2m \nmid v'(f)$, but having additional properties^{*)} like

- (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_0 of K_0 with respect to P_0 ; i.e. a valuation \bar{w} of \bar{K}_v , trivial on K_0 , with residue field contained in R_0 . The valuation \bar{w} of \bar{K}_v , can be lifted through v' to some refinement w of v' . Then, the value group $\bar{w}(\bar{K}_v)$ 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_0 , with residue field contained in R_0 and still satisfying $2m \nmid w(f)$. Applying once more the above mentioned result of [6], we finally obtain a valuation w' , trivial on K_0 , such that $2m \nmid w'(f)$ and

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

Thus, in particular \bar{K}_w , is contained in R_0 .

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 $R_0((t))$ such that ord induces w' on K . Hence X_1, \dots, X_n are identified with some Laurent series $\rho_1, \dots, \rho_n \in R_0((t))$ and thus $2m \nmid \text{ord } f(\rho_1, \dots, \rho_n)$.

Finally, we observe that in the topology induced by the valuation ord on $R_0((t))$,

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

By the continuity of f and the fact that the set $\{\rho \in R_0((t)) \mid 2m \nmid \text{ord } \rho\}$ is open, we may assume that ρ_1, \dots, ρ_n are finite Laurent series satisfying $2m \nmid f(\rho_1, \dots, \rho_n)$. This contradiction to the assumptions of (3) proves (1).

q.e.d.

MODEL THEORY OF FIELDS

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 $\rho_n = t, \dots, \rho_n = t$ and choosing $a \in \mathbb{R}$, such that $f(at, t, \dots, t) \neq 0$, 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 $2m \mid \text{ord}(p_1, \dots, p_n)$ for all $p_i \in \mathbb{R}[t]$ such that $\text{ord } p_i = 0$ for at least one p_i . Let ρ_1, \dots, ρ_n be finite Laurent series in t . If $r = \min_i \{\text{ord } \rho_i\}$, clearly all $p_i = \rho_i t^{-r}$ are polynomials, one having $\text{ord} = 0$. Thus it follows from the condition in Theorem 1 that $2m \mid \text{ord} f(p_1, \dots, p_n)$. From

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

and $2m \mid d$ we therefore conclude $2m \mid \text{ord} f(\rho_1, \dots, \rho_n)$ 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 $f(X_1, \dots, X_n)$ be a polynomial of degree d over a formally real field K_0 . Then $f \in \Sigma K_0(X_1, \dots, X_n)^{2m}$ if and only if

$$x_0^d \cdot f\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \Sigma K_0(x_0, x_1, \dots, x_n)^{2m}.$$

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 $f \in \mathbb{Q}[X_1, \dots, X_n]$. 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 $\Sigma P_0 \cdot K_0(X)^{2m}$ if and only if f is positive semidefinite over R_0 , $2m \mid \deg f$ 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

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

By this assumption, it is possible to express the phrase

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

by a formula φ 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 ω be such a non-standard natural number. Since φ 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

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

Note that v^* has a formally real residue field; in fact, $\overline{\mathbb{R}}_{v^*} = \mathbb{R}$. 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

$$v(a_n X^n + \dots + a_0) = \min_i \{ (v^*(a_i), i) \} ,$$

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

$$2m \mid v(X^{2m} + \omega X^2 + 1) = (v^*(\omega), 2) .$$

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

- [1] BECKER, E.: Summen n -ter Potenzen in Körpern. J.reine angew. Math. 307/308 (1979), 8-30
- [2] BECKER, E.: The real holomorphy ring and sums of $2n$ -th powers. Lecture Notes in Math. 959 (Springer, 1982), 139-181
- [3] BOURBAKI, N.: Elements of mathematics, commutative algebra. Paris 1972
- [4] ENDLER, O.: Valuation theory. Berlin-Heidelberg-New York 1972

MODEL THEORY OF FIELDS

- [5] JOLY, R.J.: Sommes de puissance d-ièmes dans un anneau commutatif. Acta arithmetica 17 (1970), 37-114
- [6] KUHLMANN, F.V. - PRESTEL, A.: On places of algebraic function fields. (To appear)
- [7] PRESTEL, A.: Lectures on formally real fields. Monografías de matematica 22, IMPA, Rio de Janeiro 1975

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