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>

Société Mathématique de France
2° série, mémoire n° 16, 1984, p.53-65

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/

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 $2m \mid \operatorname{ord} f(p_1,\dots,p_n)$ 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 $\operatorname{ord} h(t)$ 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 $f \in K_o[X_1,\dots,X_n]$ where K_o is some other formally real field. The main theorem of this note refers to a fixed archimedean ordering on K_o . 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 $\varphi(a_o,\dots,a_d)$, in the language of rings, such that for all real closed fields R we could get (after dehomogenizing)

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

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

*) 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 <u>For all</u> $m \geq 2$ <u>and all</u> $n \geq 0$,

$X^{2m} + nX^2 + 1 = h^{(n)}(X)^{-2m} \sum_{i=1}^{N(n)} g_i^{(n)}(X)^{2m}$. <u>Moreover, if</u> n <u>tends to infinity, so does</u> $N(n)$ <u>or</u> $\deg h^{(n)}$.

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

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

saying that f is positive semidefinite.

1. <u>On Theorem 1</u>

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 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 <u>preordering</u> of level $2m$ if

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

In case $m = 1$, we obtain the usual notion of preordering (cf. [7]). A preordering S of level $2m$ is called <u>complete</u> if

(ii) $a^2 \in S$ 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,

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

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) $$S = \bigcap_{S \subset P} P$$

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) $A_P = \{x \in K \mid -n \le_P x \le_P n$ 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 $\bar{K}_P$.