ANNALES
DE LA FACULTÉ
DES SCIENCES
DE
TOULOUSE
Mathématiques

STUART A. STEINBERG

An ℓ-algebra approach to Artin's solution of Hilbert's Seventeenth Problem

Tome XIX, nº S1 (2010), p. 215-220.

<http://afst.cedram.org/item?id=AFST_2010_6_19_S1_215_0>

Annales de la Faculté des Sciences de Toulouse Vol. XIX, n° Spécial, 2010
pp. 215–220

An ℓ-algebra approach to Artin's solution of Hilbert's Seventeenth Problem

Stuart A. Steinberg[(1)]

Dedicated to Melvin Henriksen

Abstract. — Using lattice-ordered algebras it is shown that a totally ordered field which has a unique total order and is dense in its real closure has the property that each of its positive semidefinite rational functions is a sum of squares.

Résumé. — En utilisant les algèbres réticulées, on montre qu'un corps totalement ordonné qui a un unique ordre total et qui est dense dans sa clôture réelle a la propriété que chacune des ses fonctions rationnelles positives semi-définies est une somme de carrés.

Hilbert's seventeenth problem asks if a rational function with rational coefficients which is positive semidefinite over the field of real numbers is a sum of squares of rational functions with rational coefficients. Artin [1] (or [10]) showed that this is indeed the case and, in fact, proved the stronger theorem that any subfield of the reals which has a unique total order also has this property. In [8, p. 641] (also see [7, p. 295]), Jacobson presented this result for totally ordered fields that were not necessarily archimedean, and McKenna gave the converse of this theorem in [11]. In this note I will give a proof, using some aspects of the theory of lattice-ordered rings given in Henriksen and Isbell [6], of Jacobson's version of Artin's theorem. I believe this proof of Artin's solution to Hilbert's problem was known to Weinberg in 1968. One aspect of this approach is that it avoids any use of model theory.

(1) The University of Toledo, Toledo, Ohio, U.S.A.
stuart.steinberg@utoledo.edu

Let K be a totally ordered field. A rational function $r(x_1, \cdots, x_n) \in K(x_1, \cdots, x_n)$ is *positive semidefinite* on K, abbreviated P.S.D., if $r(a_1, \cdots, a_n) \geqslant 0$ for all $a_1, \cdots, a_n$ in K for which $r(a_1, \cdots, a_n)$ is defined. The positive cone of the partially ordered group G will be denoted by G^+, and $S(R)$ denotes the set of sums of squares in the commutative ring R. If F is an extension field of the totally ordered field K it is well-known that $K^+S(F) = \{\Sigma_i a_i f_i^2 : a_i \in K^+, f_i \in F\}$ is the intersection of those total orders of F which contain K^+. The subfield K of the totally ordered field F is *dense* in F if for all a, b in F with $a < b$ there exists some $c \in K$ with $a < c < b$. According to McKenna the totally ordered field K has *Hilbert's property* if, for every n, each rational function in $K(x_1, \cdots, x_n)$ that is P.S.D. on K is a sum of squares in $K(x_1, \cdots, x_n)$. The theorem to be proved, as stated in [8, p. 641], is

THEOREM 0.1. — (Artin [1]). *Let F be the real closure of the totally ordered field K. If K has a unique total order and is dense in F, then K has Hilbert's property.*

The cardinality of the set X will be denoted by $|X|$. If A and B are subsets of the partially ordered set X, then $A < B$ (respectively, $A \leqslant B$) means $a < b \,(a \leqslant b)$ for every $a \in A$ and $b \in B$. For an ordinal number α, X is called an *η_α-set* (respectively, an *almost η_α-set*) if whenever A and B are subsets of X with $A < B \,(A \leqslant B)$ and $|A \cup B| < \aleph_\alpha$, then $A < c < B \,(A \leqslant c \leqslant B)$ for some $c \in X$; in these definitions either A or B could be empty. The cardinal number $\aleph_\alpha$ is regular if $|\bigcup_{i \in I} A_i| < \aleph_\alpha$ provided $|I| < \aleph_\alpha$ and $|A_i| < \aleph_\alpha$ for every $i \in I$. We start with a well-known embedding theorem.

THEOREM 0.2. — *Suppose $\alpha \geqslant 1$ and $\aleph_\alpha$ is a regular cardinal. Let K be a totally ordered subfield of the totally ordered field L and let F be a real closed η_α-field. If $\sigma : K \longrightarrow F$ is an embedding of totally ordered fields with $|K| < \aleph_\alpha$ and $|L| \leqslant \aleph_\alpha$, then σ can be extended to an embedding of totally ordered fields $\tau : L \longrightarrow F$.*

Proof. — A proof for the case $K = \mathbb{Q}$ is contained in the proof of Theorem 2.1 of [3]. A slight modification of the proof of Theorem 4.4.3 in [13, p. 95] proves this stronger result. □

Our construction of a totally ordered η_1-field will use the following fact about lattices.

LEMMA 0.3. — ([14, p. II-62] ; also, see [4, p. 176]). *Let $f : L \longrightarrow M$ be a lattice homomorphism of the lattice L onto the lattice M. If S is a countable* *subset of M then there exists a subset T of L such that $f : T \longrightarrow S$ is an order isomorphism.*

Proof. — We assume that S is infinite; the case that S is finite is done similarly. Suppose $S = \{f(x_1), f(x_2), \cdots\}$. Let $t_1 = x_1$. Suppose $t_1, \cdots, t_{n-1}$ have been chosen so that $f : \{t_1, \cdots, t_{n-1}\} \longrightarrow \{f(x_1), \cdots, f(x_{n-1})\}$ is an order isomorphism with $f(t_i) = f(x_i)$. Let $X = \{t_i : f(t_i) < f(x_n)\}$, $Y = \{t_j : f(x_n) < f(t_j)\}$, $x = \bigvee_i t_i$, $y = \bigwedge_j t_j$ and $t_n = (x \vee x_n) \wedge y)$. If X or Y is empty just delete x or y from the definition of t_n; we will assume neither X nor Y is empty since the other cases follow in a similar way. Now, $X < Y$ since $f(t_i) < f(t_j)$ and hence $t_i < t_j$ for $t_i \in X$ and $t_j \in Y$. Thus $x \leqslant y$,

$$f(x) = \bigvee_i f(t_i) \leqslant f(x_n) \leqslant \bigwedge_j f(t_j) = f(y),$$

and

$$f(t_n) = (f(x) \vee f(x_n)) \wedge f(y) = f(x_n) \wedge f(y) = f(x_n).$$

Now, $t_i < t_n$ iff $f(t_i) < f(t_n)(i = 1, \cdots, n-1)$. For, $t_i < t_n$ gives $f(x_i) = f(t_i) \leqslant f(t_n) = f(x_n)$ and hence $f(t_i) < f(t_n)$; and $f(t_i) < f(t_n) = f(x_n)$ gives $t_i \leqslant x \leqslant y$, $t_i \leqslant (x \vee x_n) \wedge y = t_n$, and hence $t_i < t_n$. Similarly, $t_n < t_j$ iff $f(t_n) < f(t_j)$ for $j = 1, \cdots, n-1$. ☐

Theorem 0.4. — ([15]; also [14, p. II-63]). *Let $\{M_n : n \in \mathbb{N}\}$ be a sequence of nonzero ℓ-groups. Then $\overline{M} = \Pi_n M_n / \oplus_n M_n$ and all of its homomorphic images are almost η_1-groups.*

Proof. — The homomorphisms in "homomorphic images" are, of course, morphisms between ℓ-groups. We will only consider $\overline{M}$ since the same proof works for M/C where C is a normal convex ℓ-subgroup of $\Pi_n M_n$ which contains $\oplus_n M_n$. Suppose $\overline{A} < \overline{B}$ are countable subsets of $\overline{M}$. We assume $\overline{A}$ and $\overline{B}$ are infinite. From Lemma 0.3 we can find subsets $A = \{a_n : n \in \mathbb{N}\} < \{b_n : n \in \mathbb{N}\} = B$ of $\Pi_n M_n$ such that $\overline{A} = \{\overline{a}_n : n \in \mathbb{N}\}$, $\overline{B} = \{\overline{b}_n : n \in \mathbb{N}\}$ and $A \cup B \longrightarrow \overline{A} \cup \overline{B}$ is an order isomorphism. For each $n \in \mathbb{N}$ take $g_n \in M_n$ with

$$\{a_1(n), \cdots, a_n(n)\} \leqslant g_n \leqslant \{b_1(n), \cdots, b_n(n)\},$$

and let $g \in \Pi_n M_n$ be defined by $g(n) = g_n$. Then $\overline{A} \leqslant \overline{g} \leqslant \overline{B}$. To see that $\overline{A} \leqslant \overline{g}$ fix $k \in \mathbb{N}$. If $n \in \mathbb{N}$ and $a_k(n) \nleqslant g_n$, then $k > n$; that is, $n \in \{1, \cdots, k-1\}$. So if $h_k \in \Pi_n M_n$ is defined by

$$h_k(n) = \begin{cases} -g_n + a_k(n) & \text{if } a_k(n) \nleqslant g_n \\ 0 & \text{if } a_k(n) \leqslant g_n \end{cases}$$

then $h_k \in \oplus_n M_n$ and $a_k \leqslant g + h_k$; hence $\overline{a}_k \leqslant \overline{g}$. Similarly, $\overline{g} \leqslant \overline{B}$. ☐

The following well-known result follows quickly from Theorem 0.4.

Corollary 0.5. — *Suppose K is a real closed field and $\mathcal{F}$ is an ultrafilter on $\mathbb{N}$ which contains all complements of finite subsets of $\mathbb{N}$. Then the ultraproduct $K^{\mathbb{N}}/\mathcal{F}$ is a real closed η_1-field.*

Proof. — For $f \in K^{\mathbb{N}}$ let $Z(f) = \{n \in \mathbb{N} : f(n) = 0\}$. Recall that $K^{\mathbb{N}}/\mathcal{F} = K^{\mathbb{N}}/I(\mathcal{F})$ where $I(\mathcal{F}) = \{f \in K^{\mathbb{N}} : Z(f) \in \mathcal{F}\}$ is a maximal ideal of $K^{\mathbb{N}}$ which is an ℓ-ideal (all of the ideals of $K^{\mathbb{N}}$ are ℓ-ideals). Using the standard characterization of a real closed field as a totally ordered field in which each positive element is a square and each polynomial of odd degree has a root it is clear that $K^{\mathbb{N}}/\mathcal{F}$ is real closed. Since $I(\mathcal{F})$ contains $\oplus_n K$, $K^{\mathbb{N}}/\mathcal{F}$ is a totally ordered almost η_1-field. But a totally ordered almost η_α-division ring D is an η_α-division ring. For suppose, for example, that $A \leqslant c \leqslant B$ with $|A \cup B| < \aleph_\alpha$, $c \in A$, and B has no least element. Then $0 < B - c$ has no least element, $(B-c)^{-1} < u^{-1}$ for some $u \in D$ since $(B-c)^{-1}$ has no largest element, $u < B - c$, and $A < c + u < B$. □

An ℓ-ring R which is an algebra over the partially ordered ring C is called an ℓ-algebra if $C^+R^+ \subseteq R^+$. Let $\mathcal{S}$ be a set of words in the free ℓ-algebra on a countably infinite free generating set. The variety of ℓ-algebras determined by $\mathcal{S}$ is the class $\mathcal{V}(\mathcal{S})$ consisting of all those ℓ-algebras R which satisfy each word in $\mathcal{S}$: $g(a_1, \cdots, a_n) = 0$ for all $a_1, \cdots, a_n \in R$ and all $g(x_1, \cdots, x_n) \in \mathcal{S}$. According to Birkhoff's theorem [2, p. 169] a class of ℓ-algebras $\mathcal{V}$ is a variety if and only if each ℓ-subalgebra and each homomorphic image of an ℓ-algebra in $\mathcal{V}$ also belongs to $\mathcal{V}$, and the direct product of any set of ℓ-algebras from $\mathcal{V}$ is in $\mathcal{V}$. If K is an ℓ-algebra, then $\mathcal{V}_C(K)$ denotes the variety of ℓ-algebras generated by K. The ℓ-algebra R belongs to $\mathcal{V}_C(K)$ if and only if it satisfies each ℓ-algebra identity that K satisfies. A small extension of a result from [6] is crucial to this proof.

Theorem 0.6 ([6, 3.8]). — *Let C be a common totally ordered subring of the totally ordered fields K and L. If K is real closed then $L \in \mathcal{V}_C(K)$.*

Proof. — Suppose $g(x_1, \cdots, x_n)$ is a word in the free (commutative) C-f-algebra that K satisfies. Let $\alpha_1, \cdots, \alpha_m$ be all the elements of C which occur in $g(x_1, \cdots, x_n)$ and let $a_1, \cdots, a_n \in L$. If $\mathcal{F}$ is an ultrafilter on $\mathbb{N}$ which contains the complement of each finite subset of $\mathbb{N}$, then by Corollary 0.5 and Theorem 0.2 the embedding

$$\mathbb{Q}(\alpha_1, \cdots, \alpha_m) \longrightarrow K \longrightarrow K^{\mathbb{N}}/\mathcal{F}$$

can be extended to an embedding $\psi : \mathbb{Q}(\alpha_1, \cdots, \alpha_m, a_1, \cdots, a_n) \longrightarrow K^{\mathbb{N}}/\mathcal{F}$. Since ψ fixes each α_i we have $\psi(g(a_1, \cdots, a_n)) = g(\psi(a_1), \cdots, \psi(a_n)) = 0$. □

We will now give the proof of Theorem 0.1.

Suppose $r(x_1, \cdots, x_n) = f(x_1, \cdots, x_n)g(x_1, \cdots, x_n)^{-1} \in K(x_1, \cdots, x_n)$ is P.S.D. on K and let $h(x_1, \cdots, x_n) = f(x_1, \cdots, x_n)g(x_1, \cdots, x_n)$. Then $h(\alpha_1, \cdots, \alpha_n) \geqslant 0$ for all $\alpha_1, \cdots, \alpha_n \in F$ and hence $h(x_1, \cdots, x_n)^- = 0$ is an identity for the K-ℓ-algebra F. Let P be a total order of $K(x_1, \cdots, x_n)$ which extends K^+ and let E be the real closure of $(K(x_1, \cdots, x_n), P)$. Then $\mathcal{V}_K(F) = \mathcal{V}_K(E)$ by Theorem 0.6 and hence $h(x_1, \cdots, x_n)^- = 0$ is also an identity for the K-ℓ-algebra E. So $h(x_1, \cdots, x_n) \in P$ and hence $r(x_1, \cdots, x_n) \in K^+S(K(x_1, \cdots, x_n)) = S(K(x_1, \cdots, x_n))$ since $K^+ = S(K)$. □

The proof I have given of Theorem 0.1 also proves the following additional versions of Artin's theorem. The first version is given in [5] and [7, p. 295] and the second version which, along with the reference [5], was kindly pointed out to me by Delzell, comes from Lang [9, p. 387]. Of course, for the second version one needs to use the well-known fact that for a field E whose characteristic is not 2, $S(E)$ is the intersection of all of the total orders of E [7, p. 288].

Let K be a subfield of the real closed field F with the total order it inherits from F. If $r(x_1, \cdots, x_n) \in K(x_1, \cdots, x_n)$ is P.S.D. on F, then $r(x_1, \cdots, x_n) \in K^+S(K(x_1, \cdots, x_n))$.

Let $r(x_1, \cdots, x_n) \in K(x_1, \cdots, x_n)$ where K is a field whose characteristic is not 2. If $r(x_1, \cdots, x_n)$ is P.S.D. on each algebraic extension L of K, for any total order of L, then $r(x_1, \cdots, x_n)$ is a sum of squares in $K(x_1, \cdots, x_n)$.

Bibliography

[1] Artin (E.). — Über die Zerlegung definiter Funktionen in Quadrate, Hamb. Abh., 5, p. 100-115 (1927).

[2] Cohn (P. M.). — Universal algebra, Revised edition, Reidel, Dordrecht (1981).

[3] Erdos (P.), Gillman (L.) and Henriksen (M.). — An isomorphism theorem for real-closed fields, Ann. of Math., 61, p. 542-554 (1955).

[4] Gillman (L.) and Jerison (M.). — Rings of continuous functions, Van Nostrand, Princeton (1960).

[5] Henkin (L.). — Sums of squares, in Summaries of Talks, Summer Institute of Symbolic Logic in 1957 at Cornell University, Institute for Defense Analyses, Princeton, p. 284-291 (1960).

[6] Henricksen (M.) and Isbell (J. R.). — Lattice-ordered rings and function rings, Pacific J. Math., 12, p. 533-565 (1962).

[7] Jacobson (N.). — Lectures in abstract algebra, Volume III – Theory of fields and Galois Theory, Van Nostrand, Princeton (1964).

[8] Jacobson (N.). — Basic algebra II, Freeman, San Francisco (1980).

[9] Lang (S.). — The theory of real places, Ann. Math. 57, p. 378-391 (1953).

[10] Lang (S.) and Tate (J. T.). — The collected papers of Emil Artin, Addison-Wesley, Reading (1965).

[11] McKenna (K.). — New facts about Hilbert's seventeenth problem, Lecture Notes in Mathematics 498, Model theory and algebra, A memorial tribute to Abraham Robinson, p. 220-230 (1975).

[12] Pfister (A.). — Hilbert's seventeenth problem and related problems on definite forms, Mathematical developments arising from Hilbert problems, Proceedings of symposia in pure mathematics 28, part 2, Amer. Math. Soc., Providence, p. 483-489 (1976).

[13] Prestel (A.) and Delzell (C. N.). — Positive polynomials, Springer, Berlin (2001).

[14] Weinberg (E. C.). — Lectures on ordered groups and rings, University of Illinois, Urbana (1968).

[15] Weinberg (E. C.). — University of Illinois seminar (1971).