FUNDAMENTA
MATHEMATICAE
159 (1999)

# Ordered fields and the ultrafilter theorem

by

**R. Berr** (Dortmund), **F. Delon** (Paris)
and **J. Schmid** (Dortmund)

**Abstract.** We prove that on the basis of ZF the ultrafilter theorem and the theorem of Artin–Schreier are equivalent. The latter says that every formally real field admits a total order.

**Introduction.** In 1900 at the international congress of mathematicians in Paris Hilbert raised his famous 23 problems. Among these was the following (the 17th):

Let $f \in \mathbb{R}[X_1, \ldots, X_n]$ be a polynomial which is positive semidefinite, i.e., $f(x) \geq 0$ for all $x \in \mathbb{R}^n$. Is $f$ a sum of squares of rational functions?

Hilbert already knew that $f$ is not necessarily a sum of squares of polynomials unless $n = 1$. In 1927 Artin solved Hilbert's 17th problem affirmatively (cf. [1]). The methods he used were developed in the joint paper [2] with Schreier and are nowadays known as Artin–Schreier theory. The crucial notion of Artin–Schreier theory is that of a formally real field. A field $K$ is called *formally real* if $-1$ is not a sum of squares in $K$. The first basic theorem proved by Artin and Schreier stated that each formally real field $K$ admits an ordering, i.e. a subset $P \subset K$ such that $P + P \subset P$, $P \cdot P \subset P$, $P \cap -P = \{0\}$ and $P \cup -P = K$.

The proof runs as follows. Let $T = \sum K^2$ be the set of all sums of squares of $K$. Then $T + T \subset T$, $T \cdot T \subset T$, $K^2 \subset T$ and by the assumption $-1 \notin T$, i.e. $T$ is a preordering. An application of Zorn's Lemma yields a preordering maximal for set-theoretic inclusion. Now an elementary computation shows that this maximal preordering is an ordering.

In 1954 Tarski [6] mentioned that the axiom of choice (in the form of Zorn's Lemma) is not necessary. The ultrafilter theorem suffices to prove the theorem of Artin–Schreier. A proof can be found in [3] (Theorem 2.2 and Example 2.3.3). As mentioned by Tarski the problem whether the

1991 *Mathematics Subject Classification*: Primary 03E24; Secondary 12J15.

theorem of Artin–Schreier is equivalent to the ultrafilter theorem remains open.

Recently, questions of similar type appeared in computer algebra. Lombardi–Roy [4] and Sander [5] proved independently that the existence and uniqueness of the real closure of an ordered field can be proven within ZF.

In this paper we close the gap mentioned above and show that the theorem of Artin–Schreier, the ultrafilter theorem and certain other theorems from real algebra are mutually equivalent on the basis of ZF.

**1. Preliminaries.** It is the aim of this section to prove a couple of preliminary results which will be needed for the proof that every filter is contained in an ultrafilter provided every formally real field admits an ordering. Since these results are of quite technical nature we briefly sketch their meaning for the proof.

Let $S$ be a non-empty set and let $\mathcal{F}$ be a filter on $S$. It is our goal to show that $\mathcal{F}$ is contained in an ultrafilter. To this end we consider $A = \mathbb{Q}[X_I \mid I \subset S]$ and construct in a first step a ring homomorphism $\varphi : A \to (K, T)$ into a preordered field $(K, T)$ such that

$$\mathcal{F} = \{I \subset S \mid \varphi(X_I) \in T\}.$$

In the next step we embed $K$ into a formally real field $L$ with $T = K \cap \sum L^2$ and show that for any ordering $P \subset L$,

$$\mathcal{U} = \{I \subset S \mid \varphi(X_I) \in P\}$$

is an ultrafilter containing $\mathcal{F}$. For the construction of $K$ one has to consider ideals in certain polynomial rings over $A$ which are generated by elements of the form $aX^2 + bY^2 + c$ with $a, b, c \in A$. In Lemmas 1.1–1.4 we will be concerned with these ideals. The remaining statements are related to the construction of the preordering $T \subset K$ and the extension field $L \supset K$.

Throughout this section we are working inside ZF and all fields are assumed to have characteristic zero. Given a ring $R$ we let $R^\times$ denote the group of units of $R$.

LEMMA 1.1. *Let $R$ be an integral domain with $K$ as its field of quotients. Let $a, b, c \in R \setminus \{0\}$ and assume that $a \in R^\times$. Let $\mathfrak{p}, \mathfrak{q}$ be the ideals generated by $aX^2 + bY^2 + c$ in $R[X, Y]$ and $K[X, Y]$ respectively. Then*

(1) $\mathfrak{p}$, $\mathfrak{q}$ *are prime ideals*,
(2) $\mathfrak{q} \cap R[X, Y] = \mathfrak{p}$.

P r o o f. We first prove (2). Let $f \in \mathfrak{q} \cap R[X, Y]$. Then $f(X, Y) = g(X, Y) \cdot (aX^2 + bY^2 + c)$ for some $g \in K[X, Y]$. Let

$$f(X, Y) = \sum_{i=0}^{n+2} f_i(Y) X^i \quad \text{and} \quad g(X, Y) = \sum_{i=0}^{n} g_i(Y) X^i$$

for certain $f_i \in R[Y]$ and $g_i \in K[Y]$. Comparing the coefficients we get $ag_n = f_{n+2} \in R[Y]$ and $ag_{n-1} = f_{n+1} \in R[Y]$. Hence $g_n, g_{n-1} \in R[Y]$ because $a$ is a unit in $R$.

For $1 \le i \le n-1$ we obtain again by comparing the coefficients

$$ag_{i-1}(Y) + (bY^2 + c) \cdot g_{i+1}(Y) = f_{i+1}(Y) \in R[Y].$$

Now an easy induction yields $g_n, g_{n-1}, \dots, g_1, g_0 \in R[Y]$ and hence $g \in R[X, Y]$. Therefore $f \in \mathfrak{p}$. The other inclusion is trivial.

An easy computation shows that $aX^2 + bY^2 + c$ is irreducible in $K[X, Y]$. Thus $\mathfrak{q}$ is a prime ideal of $K[X, Y]$ and from (2) we conclude that $\mathfrak{p}$ is a prime ideal of $R[X, Y]$. This proves (1). ∎

LEMMA 1.2. *Let $R$ be an integral domain. Let $I \neq \emptyset$ and $a_i, b_i, c_i \in R^\times$ $(i \in I)$. Let $\mathfrak{p}$ be the ideal of $R[\{X_i, Y_i \mid i \in I\}]$ which is generated by the polynomials $a_iX_i^2 + b_iY_i^2 + c_i$ $(i \in I)$. Then $\mathfrak{p}$ is a prime ideal.*

P r o o f. In a first step we assume that $I$ is finite. We prove the assertion by induction on the number $n$ of elements of $I$. We may assume that $I = \{1, \dots, n\}$. The case $n = 1$ follows from Lemma 1.1(1). Let

$$\begin{aligned}\mathfrak{q} &= (a_1X_1^2 + b_1Y_1^2 + c_1, \dots, a_{n-1}X_{n-1}^2 + b_{n-1}Y_{n-1}^2 + c_{n-1}) \\ &\subset R[X_1, Y_1, \dots, X_{n-1}, Y_{n-1}].\end{aligned}$$

By the induction hypothesis $\mathfrak{q}$ is a prime ideal. Thus the residue class ring

$$A = R[X_1, Y_1, \dots, X_{n-1}, Y_{n-1}]/\mathfrak{q}$$

is a domain. An easy argument yields

$$R[X_1, Y_1, \dots, X_n, Y_n]/\mathfrak{p} \cong A[X_n, Y_n]/(a_nX_n^2 + b_nY_n^2 + c_n).$$

Now Lemma 1.1(1) shows that the right hand side is a domain. Thus $\mathfrak{p}$ is a prime ideal.

In the second step we assume that $I$ is arbitrary. Let $f, g \in R[\{X_i, Y_i \mid i \in I\}]$ and assume that $fg \in \mathfrak{p}$. Thus there are a finite set $J \subset I$ and polynomials $h_i \in R[\{X_i, Y_i \mid i \in I\}]$ such that

$$fg = \sum_{i \in J} h_i \cdot (a_iX_i^2 + b_iY_i^2 + c_i).$$

In the polynomials $f, g, h_i$ $(i \in J)$ only finitely many indeterminates occur. Enlarging $J$ if necessary we may assume that $f, g, h_i \in R[\{X_i, Y_i \mid i \in J\}]$. Then $fg \in \mathfrak{q}$ where $\mathfrak{q}$ is the ideal of $R[\{X_i, Y_i \mid i \in J\}]$ generated by the polynomials $a_iX_i^2 + b_iY_i^2 + c_i$ $(i \in J)$. By the first step $\mathfrak{q}$ is a prime ideal. Thus $f \in \mathfrak{q} \subset \mathfrak{p}$ or $g \in \mathfrak{q} \subset \mathfrak{p}$. ∎

LEMMA 1.3. *Let $K$ be a field and let $T$ be a preordering of $K$. Let $I \neq \emptyset$ and $a_i, b_i, c_i \in K^\times$ $(i \in I)$. Assume that for each $i \in I$ either $c_i a_i^{-1}$ or $c_i b_i^{-1}$ is in $T$. Let*

$$\mathfrak{p} = (a_i X_i^2 + b_i Y_i^2 - c_i \mid i \in I) \subset K[\{X_i, Y_i \mid i \in I\}]$$

*and let $L$ be the field of quotients of the ring $K[\{X_i, Y_i \mid i \in I\}]/\mathfrak{p}$. Then there is a preordering $T'$ of $L$ which extends $T$, i.e., $T' \cap K = T$.*

Proof. We prove the lemma in three steps. In the first step we assume that $I$ contains only one element. We omit all indices. Since the situation is symmetric in $X$ and $Y$ we may assume $ca^{-1} \in T$. First note that

$$L \cong K(Y)[X]/(X^2 + ba^{-1}Y^2 - ca^{-1}).$$

We denote by $x \in L$ the image of $X$ under the canonical projection $K(Y)[X] \to L$. Now let $T' \subset L$ be the semiring generated by $T$ and the squares of $L$. We claim $T = T' \cap K$. Obviously, $T \subset T' \cap K$. So let $t \in T' \cap K$. Then there are $n \in \mathbb{N}$, $t_i \in T$ and $g, g_i, h_i \in K[Y]$, $i = 1, \ldots, n$, with $g \neq 0$ and

$$tg^2 = \sum_{i=1}^{n} (h_i + xg_i)^2 \cdot t_i = \sum_{i=1}^{n} (h_i^2 + x^2 g_i^2) \cdot t_i + 2x \cdot \sum_{i=1}^{n} g_i h_i t_i.$$

But $x^2 = ca^{-1} - ba^{-1}Y^2 \in K(Y)$ implies $\sum g_i h_i t_i = 0$. Therefore

$$tg^2 = \sum_{i=1}^{n} h_i^2 t_i + (ca^{-1} - ba^{-1}Y^2) \cdot \sum_{i=1}^{n} g_i^2 t_i.$$

Now assume $g(0) = 0$. Since $ca^{-1} \in T$ we see $h_i(0) = 0 = g_i(0)$ for all $i$. Hence we may assume that $g(0) \neq 0$. But then $ca^{-1} \in T$ implies $tg(0)^2 \in T$, hence $t \in T$. Therefore $T'$ extends $T$.

In the second step we assume that $I$ is finite and proceed by induction on the number $n$ of its elements. We may assume that $I = \{1, \ldots, n\}$. The case $n = 1$ is exactly the first step. Let

$$\begin{aligned}\mathfrak{q} &= (a_1 X_1^2 + b_1 Y_1^2 + c_1, \ldots, a_{n-1} X_{n-1}^2 + b_{n-1} Y_{n-1}^2 + c_{n-1}) \\ &\subset K[X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}].\end{aligned}$$

By Lemma 1.2, $\mathfrak{q}$ is a prime ideal. So $A = K[X_1, Y_1, \ldots, X_{n-1}, Y_{n-1}]/\mathfrak{q}$ is a domain. Let $F$ be its field of quotients. By the induction hypothesis $T$ extends to a preordering $T'$ of $F$. From the first step we see that $T'$ extends to a preordering $T''$ of $E = \mathrm{Quot}(F[X_n, Y_n]/(a_n X_n^2 + b_n Y_n^2 + c_n))$. An easy argument yields

$$K[X_1, Y_1, \ldots, X_n, Y_n]/\mathfrak{p} \cong A[X_n, Y_n]/(a_n X_n^2 + b_n Y_n^2 + c_n).$$

By Lemma 1.1(2) the right hand side embeds into $E$. Thus there is also an embedding $L \to E$. Now one can easily see that $T''$ induces the desired preordering on $L$.

In the final step we assume that $I$ is arbitrary. Let $T'$ be the semiring generated by $T$ and the squares of $L$. It suffices to show that $T' \cap K = T$. The inclusion $T \subset T' \cap K$ is clear. So let $a \in T' \cap K$. Then there are $f_0 \in K[\{X_i, Y_i \mid i \in I\}] \setminus \mathfrak{p}, f_1, \ldots, f_n \in \sum K[\{X_i, Y_i \mid i \in I\}]^2$ and $t_1, \ldots, t_n \in T$ such that

$$af_0^2 \equiv \sum_{i=1}^{n} f_i \cdot t_i \bmod \mathfrak{p}.$$

Thus there is a finite set $J \subset I$ and polynomials $g_i \in K[\{X_i, Y_i \mid i \in I\}]$ $(i \in J)$ such that

$$af_0^2 - \sum_{i=1}^{n} f_i \cdot t_i = \sum_{i \in J} g_i \cdot (a_i X_i^2 + b_i Y_i^2 + c_i).$$

In the polynomials $f_0, \ldots, f_n, g_i$ $(i \in J)$ only finitely many indeterminates occur. After enlarging $J$ if necessary we may assume that $f_0, \ldots, f_n, g_i \in K[\{X_i, Y_i \mid i \in J\}]$.

By Lemma 1.2 the ideal $\mathfrak{q}$ of $K[\{X_i, Y_i \mid i \in J\}]$ generated by $a_i X_i^2 + b_i Y_i^2 - c_i$ $(i \in J)$ is prime. Let $F$ be the field of fractions of $K[\{X_i, Y_i \mid i \in J\}]/\mathfrak{q}$. By the second step $T$ extends to a preordering $T''$ of $F$. The above equation then yields $a \in T''$. Since $a \in K$ we obtain $a \in T'' \cap K = T$.

This proves the lemma. ∎

Now we fix some notations. Let $S$ be an arbitrary non-empty set. We denote by $A_S$ the ring of polynomials in the power set of $S$ over the field $\mathbb{Q}$ of rational numbers. If we look at $I \subset S$ as an indeterminate we write $X_I$. So $A_S = \mathbb{Q}[\{X_I \mid I \subset S\}]$. We denote by $\mathfrak{p}_S$ the ideal of $A_S$ generated by all elements of the form $X_I + X_{I^c}$ $(I \subset S)$. Let $B_S = A_S/\mathfrak{p}_S$. We denote by $x_I$ the residue class of the indeterminate $X_I$.

LEMMA 1.4. *Let $S$ be a non-empty set. Then $\mathfrak{p}_S$ is a prime ideal of $A_S$ and $X_I \notin \mathfrak{p}_S$ for all $I \subset S$.*

Proof. Let $f, g \in A_S$ and assume that $fg \in \mathfrak{p}_S$. Then there are distinct subsets $I_1, \ldots, I_n \subset S$ with $I_j \neq I_k^c$ for $j \neq k$ and polynomials $h_i \in A_S$ $(1 \leq i \leq n)$ such that $fg = \sum_{i=1}^{n} h_i \cdot (X_{I_i} + X_{I_i^c})$. In the polynomials $f, g, h_1, \ldots, h_n$ only finitely many indeterminates occur. After enlarging the list $I_1, \ldots, I_n$ we may assume $f, g, h_1, \ldots, h_n \in \mathbb{Q}[X_{I_1}, X_{I_1^c}, \ldots, X_{I_n}, X_{I_n^c}]$. Thus $fg \in \mathfrak{q} = (X_{I_1} + X_{I_1^c}, \ldots, X_{I_n} + X_{I_n^c}) \subset \mathbb{Q}[X_{I_1}, X_{I_1^c}, \ldots, X_{I_n}, X_{I_n^c}]$. Since

$$\mathbb{Q}[X_{I_1}, X_{I_1^c}, \ldots, X_{I_n}, X_{I_n^c}]/\mathfrak{q} \cong \mathbb{Q}[X_{I_1}, \ldots, X_{I_n}]$$

we find that $\mathfrak{q}$ is a prime ideal. Hence $f \in \mathfrak{q} \subset \mathfrak{p}_S$ or $g \in \mathfrak{q} \subset \mathfrak{p}_S$. Finally, a straightforward argument shows $X_I \notin \mathfrak{p}_S$ for all $I \subset S$. ∎

Since $\mathfrak{p}_S$ is a prime ideal, $B_S$ is a domain. Its field of quotients will be denoted by $K_S$. Now let $\mathcal{F}$ be a filter on $S$. As mentioned at the beginning of this section we will construct a preordering $T_\mathcal{F} \subset K_S$ with $x_I \in T_\mathcal{F}$ if and only if $I \in \mathcal{F}$. To this end we need the following simple fact.

LEMMA 1.5. *Let $S$ be a non-empty set and let $\mathcal{F}$ be a filter on $S$. Let $A_1, \ldots, A_n$ be subsets of $S$. Then there is a filter $\mathcal{G}$ on $S$ such that*

(1) $\mathcal{F} \subset \mathcal{G}$,
(2) *for each $i$ either $A_i \in \mathcal{G}$ or $S \setminus A_i \in \mathcal{G}$.*

Proof. Without loss of generality we may assume $n = 1$. Let $A \subset S$. Only the case $A \notin \mathcal{F}$ has to be considered. But then $I \not\subset A$ for all $I \in \mathcal{F}$. Hence $\mathcal{G}_1 = \mathcal{F} \cup \{I \cap A^c \mid I \in \mathcal{F}\}$ is a filter basis which yields the desired filter $\mathcal{G}$. ∎

If $\mathcal{F}$ is a filter on $S$ we let $T_\mathcal{F}$ denote the semiring generated by the squares of $K_S$ and the elements $x_I$ $(I \in \mathcal{F})$.

LEMMA 1.6. *Let $\mathcal{F}$ be a filter on the set $S$. Then*

(1) *$T_\mathcal{F}$ is a preordering of $K_S$,*
(2) *for all $I \subset S$: $I \in \mathcal{F} \Leftrightarrow x_I \in T_\mathcal{F}$.*

Proof. (1) By definition $T_\mathcal{F}$ is additively and multiplicatively closed and contains all the squares of $K_S$. It remains to show that $-1 \notin T_\mathcal{F}$. Assume the contrary. Then there are $n \in \mathbb{N}$, $a_0, \ldots, a_n \in \sum K_S^2$ and $t_1, \ldots, t_n$ such that

$$-1 = a_0 + \sum_{i=1}^{n} a_i \cdot t_i$$

and each $t_i$ is a finite product of certain $x_I$ $(I \in \mathcal{F})$. After multiplication with a common denominator we obtain

$$-b^2 = b_0 + \sum_{i=1}^{n} b_i \cdot t_i$$

for certain $b_0, \ldots, b_n \in \sum B_S^2$, $b \in B_S \setminus \{0\}$. The elements $b, b_0, \ldots, b_n$ are the residue classes of polynomials $f \in A_S \setminus \mathfrak{p}_S$, $f_0, \ldots, f_n \in \sum A_S^2$ and $t_1, \ldots, t_n$ are residue classes of certain $P_1, \ldots, P_n \in \mathbb{Q}[\{X_I \mid I \subset S\}]$ where each $P_i$ is a product of certain $X_I$ with $I \in \mathcal{F}$. Thus

$$f^2 + f_0 + \sum_{i=1}^{n} f_i \cdot P_i \in \mathfrak{p}_S.$$

In these polynomials only finitely many indeterminates occur. So there are $J_1, \ldots, J_m \subset S$ such that $J_1, \ldots, J_m, J_1^c, \ldots, J_m^c$ are pairwise distinct, $P_1, \ldots, P_n \in \mathbb{Q}[X_{J_1}, \ldots, X_{J_n}]$ and $f, f_0, \ldots, f_n \in \mathbb{Q}[X_{J_1}, \ldots, X_{J_m}, X_{J_1^c}, \ldots$ $\ldots, X_{J_m^c}]$. Now we apply the substitution homomorphism $\Phi : A_S \to$

$\mathbb{Q}[X_{J_1},\dots,X_{J_m}]$ given by $X_{J_i} \mapsto X_{J_i}$, $X_{J_i^c} \mapsto -X_{J_i}$ $(1 \le i \le m)$, $X_J \mapsto 0$ $(J \notin \{J_1,\dots,J_m,J_1^c,\dots,J_m^c\})$ and obtain

$$\Phi(f)^2 + \Phi(f_0) + \sum_{i=1}^{n} \Phi(f_i)\cdot P_i = 0$$

or

$$\Phi(f)^2 = -\Phi(f_0) - \sum_{i=1}^{n} \Phi(f_i)\cdot P_i.$$

This is a polynomial equation in the indeterminates $X_{J_1},\dots,X_{J_m}$ over $\mathbb{Q}$. Since $f_0,\dots,f_n$ are sums of squares so are $\Phi(f_0),\dots,\Phi(f_n)$. Thus $\Phi(f)(x)^2 \le 0$ for all $x \in H = \{(x_1,\dots,x_m) \in \mathbb{Q}^m \mid x_1,\dots,x_m \ge 0\}$ and therefore $\Phi(f)(x) = 0$ for $x \in H$. Thus $f(X_{J_1},\dots,X_{J_m},-X_{J_1},\dots,-X_{J_m}) = \Phi(f) = 0$. This yields the contradiction $f \in (X_{J_1} + X_{J_1^c},\dots,X_{J_m} + X_{J_m^c}) \subset \mathfrak{p}_S$ and (1) is proved.

(2) If $I \in \mathcal{F}$ then $x_I \in T_{\mathcal{F}}$ by the definition. So let $x_I \in T_{\mathcal{F}}$. Since $x_I \ne 0$ we get $-x_I = x_{I^c} \notin T_{\mathcal{F}}$ because $T_{\mathcal{F}}$ is a preordering. Thus $I^c \notin \mathcal{F}$. Now assume that also $I \notin \mathcal{F}$. By the proof of Lemma 1.5 we know that there is a filter $\mathcal{G} \supset \mathcal{F}$ on $S$ with $I^c \in \mathcal{G}$. Then $x_I \in T_{\mathcal{F}} \subset T_{\mathcal{G}}$ and by (1) we know that $T_{\mathcal{G}}$ is a preordering. But $I^c \in \mathcal{G}$ implies $x_{I^c} = -x_I \in T_{\mathcal{G}}$, which gives the desired contradiction. ∎

LEMMA 1.7. *Let $S$ be a non-empty set and $\mathcal{F}$ a filter on $S$. Then there is an extension field $L \supset K_S$ such that*

(1) $x_I \in \sum L^2$ $(I \in \mathcal{F})$,
(2) *each preordering $T \supset T_{\mathcal{F}}$ extends to $L$.*

Proof. Let $A = K_S[\{Y_I, Z_I \mid I \in \mathcal{F}\}]$ and let $\mathfrak{p}$ be the ideal of $A$ which is generated by the polynomials $Y_I^2 + Z_I^2 - x_I$ $(I \in \mathcal{F})$. By Lemma 1.2, $\mathfrak{p}$ is a prime ideal. Let $L$ be the field of quotients of $A/\mathfrak{p}$. Then (1) is clear and (2) follows from Lemma 1.3. ∎

**2. The main theorem.** Before we state the main theorem we recall some definitions and facts from real algebra.

By a ring we always mean a commutative ring with a unit element $1 \ne 0$. A subset $T \subset R$ is called a (*quadratic*) *preordering* if

$$T + T \subset T, \quad T \cdot T \subset T, \quad R^2 \subset T \quad \text{and} \quad -1 \notin T.$$

A preordering $T$ is called *total* if $T \cup -T = R$. Finally, an *ordering* $P \subset R$ is a total preordering for which $P \cap -P$ is a prime ideal. In the case of a field this last condition reduces to $P \cap -P = \{0\}$. Therefore the orderings of a field are exactly the total preorderings.

A ring $R$ is called *real* or *formally real* if

$$\sum_{i=1}^{n} a_i^2 = 0 \quad \Rightarrow \quad a_1 = \ldots = a_n = 0.$$

$R$ is called *semi-real* if $-1 \notin \sum R^2$. Note that a semi-real field is also formally real; however, for rings this is not true.

THEOREM. *On the basis of ZF the following statements are equivalent*:

(1) *Each filter on a non-empty set is contained in an ultrafilter.*
(2) *Each formally real field admits an ordering.*
(3) *Each preordering of a field is contained in an ordering.*
(4) *Each semi-real ring admits an ordering.*
(5) *Each preordering of a ring is contained in a total preordering.*
(6) *Each preordering of a ring is contained in an ordering.*

P r o o f. We prove the following implications:

$$\begin{array}{ccccccccc} (6) & \Rightarrow & (3) & & & & & & \\ \Downarrow & & \Downarrow & & & & & & \\ (4) & \Rightarrow & (2) & \Rightarrow & (1) & \Rightarrow & (5) & \Rightarrow & (6) \end{array}$$

The implications in the left square are obvious.

(2)⇒(1). Let $\mathcal{F}$ be a filter on a non-empty set $S$. By Lemma 1.7 there is an extension field $L \supset K_S$ such that $x_I \in \sum L^2$ $(I \in \mathcal{F})$ and each preordering $T \supset T_{\mathcal{F}}$ of $K_S$ extends to $L$. Given a total order $P \subset L$, in general

$$\mathcal{U} = \{I \subset S \mid x_I \in P\}$$

is not a filter. For example, if $I, J \in \mathcal{U}$ it may happen that $I \cap J \notin \mathcal{U}$. This problem leads to the following construction. Let

$$A = L[\{Y_{IJ}, Z_{IJ} \mid (I,J) \in S \times S\}],$$
$$\mathfrak{p} = (x_I Y_{IJ}^2 + x_J Z_{IJ}^2 - x_{I\cap J} \mid (I,J) \in S \times S) \subset A.$$

By Lemma 1.2, $\mathfrak{p}$ is a prime ideal of $A$. We let $F$ denote the quotient field of $A/\mathfrak{p}$.

We assume that $F$ is not formally real. Then $-1 \in \sum F^2$. In this representation of $-1$ as a sum of squares in $F$ only finitely many indeterminates occur. Hence there are $I_1, \ldots, I_n, J_1, \ldots, J_n \subset S$ such that $E = \mathrm{Quot}(B/\mathfrak{q})$ is not formally real where

$$B = L[Y_{I_1J_1}, Z_{I_1J_1}, \ldots, Y_{I_nJ_n}, Z_{I_nJ_n}],$$
$$\mathfrak{q} = (x_{I_i} Y_{I_iJ_i}^2 + x_{J_i} Z_{I_iJ_i}^2 - x_{I_i\cap J_i} \mid i \in \{1, \ldots, n\}) \subset B.$$

By Lemma 1.5 there is a filter $\mathcal{G} \supset \mathcal{F}$ on $S$ such that for each

$$I \in \{I_1, \dots, I_n, J_1, \dots, J_n, I_1 \cap J_1, \dots, I_n \cap J_n\}$$

either $I \in \mathcal{G}$ or $I^c \in \mathcal{G}$. Since $T_{\mathcal{F}} \subset T_{\mathcal{G}}$ the preordering $T_{\mathcal{G}}$ extends to a preordering $T$ of $L$.

Let $i \in \{1, \dots, n\}$ and let $I = I_i$ and $J = J_i$. We show that $x_{I\cap J} \cdot x_I^{-1} \in T$ or $x_{I\cap J} \cdot x_J^{-1} \in T$. If $I \cap J \in \mathcal{G}$ then also $I \in \mathcal{G}$. Thus $x_{I\cap J}, x_I \in T_{\mathcal{G}}$ and therefore $x_{I\cap J} \cdot x_I^{-1} \in T_{\mathcal{G}} \subset T$. If $I \cap J \notin \mathcal{G}$ then without loss of generality $I \notin \mathcal{G}$. Then $(I \cap J)^c, I^c \in \mathcal{G}$ by the choice of $\mathcal{G}$. Hence $-x_{I\cap J} = x_{(I\cap J)^c} \in T_{\mathcal{G}}$ and $-x_I = x_{I^c} \in \mathcal{G}$ and therefore $x_{I\cap J} \cdot x_I^{-1} \in T_{\mathcal{G}} \subset T$.

By Lemma 1.3, $T$ extends to a preordering $T'$ of $E$. Hence $E$ is formally real and we got a contradiction.

Thus $F$ is formally real. By (2) it admits an ordering $P$. Let

$$\mathcal{U} = \{I \subset S \mid x_I \in P\}.$$

We show that $\mathcal{U}$ is an ultrafilter that contains $\mathcal{F}$.

If $I \in \mathcal{F}$ then $x_I \in \sum L^2 \subset \sum F^2 \subset P$. Hence $I \in \mathcal{U}$ and so $\mathcal{F} \subset \mathcal{U}$. Since $S \in \mathcal{F}$ we get $S \in \mathcal{U}$. Hence $x_S \in P$ and therefore $-x_S = x_\emptyset \notin P$. Thus $\emptyset \notin \mathcal{U}$.

Let $I, J \in \mathcal{U}$. Then $x_I, x_J \in P$ and thus $x_{I\cap J} = x_I y_{IJ}^2 + x_J z_{IJ}^2 \in P$ where $y_{IJ}$ and $z_{IJ}$ are the residue classes of $Y_{IJ}$ and $Z_{IJ}$ respectively. So $I \cap J \in \mathcal{U}$. Let $I \subset S$ and assume that $I \notin \mathcal{U}$. Then $x_I \notin P$ and hence $x_{I^c} = -x_I \in P$. Therefore $I^c \in \mathcal{U}$.

Finally, we have to show that $I \in \mathcal{U}$ and $I \subset J$ implies that also $J \in \mathcal{U}$. Assume that $J \notin \mathcal{U}$. As we have seen above this yields $J^c \in \mathcal{U}$ and hence we get the contradiction $I \cap J^c = \emptyset \in \mathcal{U}$.

(1)⇒(5). Let $T$ be a preordering of the ring $R$. Let $X$ be the set of all preorderings $Q$ of $R$ which contain $T$. For a finite non-empty subset $A \subset R$ we let

$$D_A = \{Q \in X \mid -1 \in Q + aQ \text{ for each } a \in A \setminus Q\}.$$

Finally, let

$$\mathcal{D} = \{D_A \mid \emptyset \neq A \subset R \text{ finite}\}.$$

We first claim that $\mathcal{D}$ has the finite intersection property.

Let $A_1, \dots, A_n \subset R$ be finite non-empty subsets of $R$. Define $A = \bigcup_{i=1}^n A_i$. Then it is easy to see that $D_A \subset \bigcap_{i=1}^n D_{A_i}$. Hence it suffices to show that $D_A \neq \emptyset$. Let $\Sigma = \{A \cap Q | \ Q \in X\}$. Since $A$ is finite $\Sigma$ has a maximal element $V$ with respect to set-theoretic inclusion. $V$ is of the form $V = A \cap Q$ for some preordering $Q \in X$. We claim that $Q \in D_A$.

Let $a \in A \setminus Q$ and define $Q' = Q + aQ$. Then $a \in Q'$ and hence $V$ is a proper subset of $A \cap Q'$. Thus $Q' \notin X$ by the maximality of $V$. Therefore $-1 \in Q' = Q + aQ$.

Since $\mathcal{D}$ has the finite intersection property it is contained in some filter $\mathcal{F}$. By (1), $\mathcal{F}$ is contained in some ultrafilter $\mathcal{U}$. For $Z \in \mathcal{U}$ let $P_Z = \bigcap_{Q \in Z} Q$. Obviously $P_Z \in X$ $(Z \in \mathcal{U})$. Now define

$$P = \bigcup_{Z \in \mathcal{U}} P_Z.$$

We claim that $P$ is a total preordering which contains $T$.

The inclusion $T \subset P$ is clear. Since $P_Y, P_Z \subset P_{Y \cap Z}$ the system $(P_Z)_{Z \in \mathcal{U}}$ is inductively directed. Hence $P$ is a preordering. It remains to show that $P$ is total. Let $a \in R$ and let $Z = \{Q \in X \mid a \in Q\}$. If $Z \in \mathcal{U}$ then $a \in \bigcap_{Q \in Z} Q = P_Z \subset P$. If $Z \notin \mathcal{U}$ then $Z^{\mathrm{c}} \in \mathcal{U}$ because $\mathcal{U}$ is an ultrafilter. Let $A = \{a, -a\}$. Then $Y = Z^{\mathrm{c}} \cap D_A \in \mathcal{U}$. For $Q \in Y$ we get $a \in A \setminus Q$ and thus $-1 \in Q + aQ$ as $Q \in D_A$. Therefore $-1 \notin Q - aQ$. Now $Q \in D_A$ implies $-a \notin A \setminus Q$ and hence $-a \in Q$. Therefore $-a \in \bigcap_{Q \in Y} Q = P_Y \subset P$.

(5)⇒(6). Let $T$ be a preordering of the ring $R$. By (5) there is a total preordering $Q$ which contains $T$. Let

$$\mathfrak{p} = \{a \in R \mid 1 + xa \in Q \text{ for all } x \in R\}.$$

We first show that $\mathfrak{p}$ is a proper prime ideal of $R$. Let $a, b \in \mathfrak{p}$ and let $x \in R$. Then $1 + 2xa, 1 + 2xb \in Q$ and hence $2 + 2x(a + b) \in Q$. Since $Q$ is total, $1 + x(a + b) \in Q$. Thus $a + b \in \mathfrak{p}$. The inclusion $R\mathfrak{p} \subset \mathfrak{p}$ is obvious by the definition. Since $1 - 2 \cdot 1 = -1 \notin Q$ we obtain $1 \notin \mathfrak{p}$ and therefore $\mathfrak{p}$ is a proper ideal of $R$.

In order to show that $\mathfrak{p}$ is a prime ideal let $a, b \in R \setminus \mathfrak{p}$. Then there are $x, y \in R$ with $xa - 1, yb - 1 \in Q$. Hence $xyab - 1 \in Q$. Now assume $ab \in \mathfrak{p}$. Then $1 - 2xyab \in Q$, which implies the contradiction $-1 = 1 - 2xyab + 2(xyab - 1) \in Q$. So $ab \notin \mathfrak{p}$.

Now we show that $\mathfrak{p}$ is convex with respect to $Q$, i.e.,

$$a + b \in \mathfrak{p},\ a, b \in Q \Rightarrow a, b \in \mathfrak{p}.$$

It is sufficient to show $a \in \mathfrak{p}$. Let $x \in R$. If $x \in Q$ then $1 + xa \in Q$. So assume $-x \in Q$. Then $1 + xa = 1 + x(a + b) + (-x)b \in Q$. Hence $a \in \mathfrak{p}$.

Now let $P = \mathfrak{p} + Q$. We claim that $P$ is an ordering of $R$ which contains $T$. Since $\mathfrak{p}$ and $Q$ are additively closed, so is $P$. Since $\mathfrak{p}$ is an ideal, $P$ is also multiplicatively closed. Obviously $T \subset Q \subset P$ and therefore $P \cup -P = R$ because $Q \cup -Q = R$. It remains to show that $P \cap -P$ is a prime ideal of $R$. We actually show $P \cap -P = \mathfrak{p}$.

Obviously $\mathfrak{p} \subset P \cap -P$. Let $x \in P \cap -P$. Then there are $a, b \in \mathfrak{p}$ and $p, q \in Q$ such that $x = a + p$ and $-x = b + q$. Thus $p + q = -(a + b) \in \mathfrak{p}$. As $\mathfrak{p}$ is convex with respect to $Q$ we get $p, q \in \mathfrak{p}$ and hence $x = a + p \in \mathfrak{p}$.

This proves the theorem. ∎

**References**

[1] E. Artin, *Über die Zerlegung definiter Funktionen in Quadrate*, Abh. Math. Sem. Univ. Hamburg 5 (1927), 100–115.
[2] E. Artin und O. Schreier, *Algebraische Konstruktion reeller Körper*, ibid., 85–99.
[3] T. Jech, *The Axiom of Choice*, North-Holland, 1973.
[4] H. Lombardi and M.-F. Roy, *Constructive elementary theory of ordered fields*, in: Effective Methods in Algebraic Geometry, Progr. Math. 94, Birkhäuser, 1991, 249–262.
[5] T. Sander, *Existence and uniqueness of the real closure of an ordered field without Zorn's Lemma*, J. Pure Appl. Algebra 73 (1991), 165–180.
[6] A. Tarski, *Prime ideal theorems for set algebras and ordering principles*, *preliminary report*, Bull. Amer. Math. Soc. 60 (1954), 391.

Fachbereich Mathematik
Universität Dortmund
D-44221 Dortmund, Germany
E-mail: berr@math.uni-dortmund.de
schmid@math.uni-dortmund.de

CNRS–UFR de Mathématiques
Université Paris 7
2 Place Jussieu, Case 7012
F-75251 Paris Cedex 05, France
E-mail: delon@logique.jussieu.fr

*Received 3 March 1998;*
*in revised form 5 May 1998*