FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 341–352, 2023
DOI: 10.2478/forma-2023-0027
e-ISSN: 1898–9934

sciendo.com/journal/forma

Extensions of Orderings

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we extend the algebraic theory of ordered fields [6], [8] in Mizar. We introduce extensions of orderings: if E is a field extension of F, then an ordering P of F extends to E, if there exists an ordering O of E containing P. We first prove some necessary and sufficient conditions for P being extendable to E, in particular that P extends to E if and only if the set $QS\ E := \{\sum a * b^2 \mid a \in P,\ b \in E\}$ is a preordering of E – or equivalently if and only if $-1 \notin QS\ E$. Then we show for non-square $a \in F$ that P extends to $F(\sqrt{a})$ if and only if P and finally that every ordering P of F extends to E if the degree of E over F is odd.

MSC: 12J15 12F99 68V20

Keywords: ordered fields; quadratic extensions; extensions of odd degree

MML identifier: REALALG3, version: 8.1.14 5.76.1462

Introduction

In this article we extend the algebraic theory of ordered fields [5] using the Mizar formalism [1, 4, 2]. We define extensions of orderings: if E is a field extension of F and P an ordering of F, then P extends to E, if there is an ordering of E containing P.

In the preliminary section, we provide a number of technical lemmas. Among others we define the sets P^+ and P^- of positive and negative elements, respectively, and show that the existence of a partition $\{P^+, \{0\}, P\}$ is equivalent to our definition of orderings, e.g. that $P^+ \cup \{0\}$ is a positive cone [5].

The next section is devoted to polynomials [9]. Here we prove some theorems necessary for our main results, for example, that every polynomial of odd degree has an irreducible factor of odd degree. We also show the – rather technical – fact that evaluating a sum of polynomials is the same as summing up evaluations of the addends, that is for $a \in E$ we have

$$(\sum_{i=1}^{n} p_i)(a) \;=\; \sum_{i=1}^{n} p_i(a).$$

The third section presents more properties of the fields $F(a)$ for an element a such that $a^2 \in F$, but $a \notin F$. In this case the degree of the extension is 2, so that the representation of elements of $F(a)$ by $x + \cdot a \cdot y$ with $x, y \in F$ is unique [7]. This follows from $\{1, a\}$ being a basis of $F(a)$'s corresponding vector space [3].

Then in Section 4 we define extensions (cf. [13, 10]) of orderings and introduce the set of P-quadratic sums of E

$$QS(E) \;:=\; \{\sum a \cdot b^2 \mid a \in P,\ b \in E\}.$$

We show that P extends to E if and only if $QS(E)$ is an ordering of P, which is the case if and only if $1 \notin QS(E)$. This allows to prove our main theorems [8]: Firstly, that for a non-square element $a \in F$ an ordering P of F extends to $F(a)$ if and only if $\sqrt{a} \in P$; because if

$$-1 \;=\; \sum a_i \cdot (x_i + \cdot a \cdot y_i)^2 \in QS(E),$$

then because $-1 = 1 + a * 0$ would follow

$$-1 \;=\; \sum a_i \cdot {x_i}^2 + \cdot a_i \cdot y_i^2 \cdot a^2,$$

and hence $-1 \in P$, because $a_i, a^2 \in F$.

Secondly, that every ordering P of F extends to a field extension E of odd degree. The proof is by induction and uses the fact that E is a simple extension of F, e.g. $E = F(a)$. Then, because $\{1, a, \ldots, a^{n-1}\}$ is a basis of E, from $-1 = \sum a_i \cdot (x_i + a \cdot y_i)^2$ would follow the existence of an irreducible polynomial h with odd degree $< n$, so that by induction hypothesis P extends to $F(b)$, where h is the minimal polynomial of b. Then, however, the equation can again be pushed down to F giving $-1 \in P$.

1. Preliminaries

The scheme *3SeqDEx* deals with a non empty set $\mathcal{D}$ and a natural number $\mathcal{A}$ and a binary predicate $\mathcal{P}$ and a binary predicate $\mathcal{Q}$ and a binary predicate $\mathcal{R}$ and states that

(Sch. 1) There exist finite sequences p, q, r of elements of $\mathcal{D}$ such that $\operatorname{dom} p = \operatorname{Seg} \mathcal{A}$ and $\operatorname{dom} q = \operatorname{Seg} \mathcal{A}$ and $\operatorname{dom} r = \operatorname{Seg} \mathcal{A}$ and for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ holds $\mathcal{P}[k, p(k)]$ and for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ holds $\mathcal{Q}[k, q(k)]$ and for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ holds $\mathcal{R}[k, r(k)]$

provided

- for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ there exists an element x of $\mathcal{D}$ such that $\mathcal{P}[k, x]$ and
- for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ there exists an element x of $\mathcal{D}$ such that $\mathcal{Q}[k, x]$ and
- for every natural number k such that $k \in \operatorname{Seg} \mathcal{A}$ there exists an element x of $\mathcal{D}$ such that $\mathcal{R}[k, x]$.

Now we state the proposition:

(1) Let us consider an add-associative, right zeroed, right complementable, non empty additive loop structure L. Then $-\{0_L\} = \{0_L\}$.

Let R be a ring. The functor $2.(R)$ yielding an element of R is defined by the term

(Def. 1) $1_R + 1_R$.

Let us note that there exists a field which has characteristic 2. Let R be a ring with characteristic 2. One can verify that $2.(R)$ is zero.

Let R be a non degenerated ring without characteristic 2. One can verify that $2.(R)$ is non zero and $2.(\mathbb{F}_{\mathbb{Q}})$ is non square and $2.(\mathbb{R}_{\mathrm{F}})$ is a square and there exists a field which is preordered and polynomial-disjoint and every non degenerated ring which is preordered and has also not characteristic 2. Now we state the proposition:

(2) Let us consider a field F, an extension E of F, and a finite sequence f of elements of E. Suppose for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) \in F$. Then

(i) f is a finite sequence of elements of F, and

(ii) $\sum f \in F$.

Let F be a field, a be sum of squares element of F, and b be sum of squares, non zero element of F. Observe that $a \cdot (b^{-1})$ is a sum of squares. Let f be a quadratic, non empty finite sequence of elements of F. Let us note that $\sum f$ is a sum of squares. Let R be a zero structure. Let us observe that there exists a finite sequence of elements of R which is trivial and $\varepsilon_{(\text{the carrier of } R)}$ is trivial and every finite sequence of elements of R which is empty is also trivial.

Let f, g be trivial finite sequences of elements of R. Observe that $f \frown g$ is trivial. Let R be a non degenerated ring, f be a non trivial finite sequence of elements of R, and g be a finite sequence of elements of R. Observe that $f \frown g$ is non trivial and $g \frown f$ is non trivial. Let R be a ring and f be a trivial finite sequence of elements of R. One can check that $\sum f$ is zero. Let E be a field, F be a subfield of E, and a be an element of F. The functor ${}^{@}(a, E)$ yielding an element of E is defined by the term

(Def. 2) a.

Let a be an element of E. We say that a is F-membered if and only if

(Def. 3) $a \in$ the carrier of F.

Let us observe that there exists an element of E which is F-membered. Let a be an element of E. Assume a is F-membered. The functor ${}^{@}(F, a)$ yielding an element of F is defined by the term

(Def. 4) a.

Let a be an F-membered element of E. Observe that ${}^{@}(F, a)$ reduces to a. Let R be a non degenerated ring. One can check that 1_R is non zero and -1_R is non zero. Let R be a preordered, non degenerated ring, P be a preordering of R, and a, b be P-positive elements of R. Let us observe that $a + b$ is P-positive.

Let R be a preordered integral domain. Let us note that $a \cdot b$ is P-positive. Let R be a ring and S be a subset of R. The functors: S^+ and S^- yielding subsets of R are defined by terms

(Def. 5) $S \setminus \{0_R\}$,

(Def. 6) $(-S) \setminus \{0_R\}$,

respectively. Let R be a preordered, non degenerated ring and P be a preordering of R. Let us note that P^+ is non empty and P^- is non empty and $P^+ \cap P^-$ is empty and P^+ is closed under addition. Let R be a preordered integral domain. Note that P^+ is closed under multiplication. Now we state the propositions:

(3) Let us consider a preordered, non degenerated ring R, and a preordering P of R. Then

(i) $P + P^+ \subseteq P^+$, and

(ii) $P^+ + P \subseteq P^+$.

(4) Let us consider a preordered integral domain R, and a preordering P of R. Then

(i) $(P^-) \cdot (P^-) \subseteq P^+$, and

(ii) $(P^+) \cdot (P^-) \subseteq P^-$, and

(iii) $(P^-) \cdot (P^+) \subseteq P^-$.

(5) Let us consider a non degenerated integral domain R, and a subset S of R. Suppose S is a positive cone. Then

(i) $\{S^+, \{0_R\}, S^-\}$ is a partition of the carrier of R, and

(ii) S^+ is closed under addition and closed under multiplication.

(6) Let us consider a non degenerated ring R, and a subset S of R. Suppose $\{S, \{0_R\}, -S\}$ is a partition of the carrier of R and S is closed under addition and closed under multiplication. Then $S \cup \{0_R\}$ is a positive cone. The theorem is a consequence of (1).

(7) Let us consider an ordered field F, an extension E of F, an ordering P of F, and a finite sequence f of elements of E. Suppose for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) \in P$. Then $\sum f \in P$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence f of elements of E such that $\operatorname{len} f = \$_1$ and for every natural number i such that $i \in \operatorname{dom} f$ holds $f(i) \in P$ holds $\sum f \in P$. $\mathcal{P}[0]$ by [11, (2)], [12, (25)]. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\operatorname{len} f = n$. $\square$

(8) Let us consider an ordered field F, an ordering P of F, and a field E. Suppose $E \approx F$. Then

(i) E is ordered, and

(ii) there exists a subset Q of E such that $Q = P$ and Q is a positive cone.

Let F be an ordered field. Let us observe that there exists an extension of F which is ordered.

2. Some Properties of Polynomials

Let F be a field, g be a non empty finite sequence of elements of the carrier of Polynom-Ring F, and i be an element of $\operatorname{dom} g$. Let us observe that the functor $g(i)$ yields an element of the carrier of Polynom-Ring F. Let us consider a field F and polynomials p, q over F. Now we state the propositions:

(9) If $\operatorname{LC} p + \operatorname{LC} q \neq 0_F$, then $\deg((p+q)) = \max(\deg(p), \deg(q))$.

(10) (i) if $\deg(p) > \deg(q)$, then $\operatorname{LC}(p+q) = \operatorname{LC} p$, and

(ii) if $\deg(p) < \deg(q)$, then $\operatorname{LC}(p+q) = \operatorname{LC} q$, and

(iii) if $\deg(p) = \deg(q)$ and $\operatorname{LC} p + \operatorname{LC} q \neq 0_F$, then $\operatorname{LC}(p+q) = \operatorname{LC} p + \operatorname{LC} q$.

The theorem is a consequence of (9).

Now we state the propositions:

(11) Let us consider a field F, and an element p of the carrier of Polynom-Ring F. Then $\deg(\mathrm{NormPoly}\, p) = \deg(p)$.

(12) Let us consider a field F, and a non constant element p of the carrier of Polynom-Ring F. Then there exists a non constant, monic element q of the carrier of Polynom-Ring F such that

(i) $q \mid p$, and

(ii) q is irreducible.

Proof: Define $\mathcal{Q}$[natural number] $\equiv$ for every non constant element p of the carrier of Polynom-Ring F such that $\deg(p) = \$_1$ there exists a non constant, monic element q of the carrier of Polynom-Ring F such that $q \mid p$ and q is irreducible. For every natural number k, $\mathcal{Q}[k]$. $\square$

(13) Let us consider a field F, and an element p of the carrier of Polynom-Ring F. Suppose $\deg(p)$ is odd. Then there exists a non constant, monic element q of the carrier of Polynom-Ring F such that

(i) $q \mid p$, and

(ii) q is irreducible, and

(iii) $\deg(q)$ is odd.

The theorem is a consequence of (11) and (12).

(14) Let us consider a field F, a finite sequence f of elements of the carrier of Polynom-Ring F, and a non zero polynomial p over F. Suppose $p = \sum f$. Let us consider a finite sequence g of elements of F, and a natural number n. Suppose for every element i of $\mathrm{dom}\, f$ for every polynomial q over F such that $q = f(i)$ holds $\deg(q) \leqslant n$. Then $\deg(p) \leqslant n$.

(15) Let us consider an ordered field F, an ordering P of F, a finite sequence f of elements of the carrier of Polynom-Ring F, and a non zero polynomial p over F. Suppose $p = \sum f$ and for every element i of $\mathrm{dom}\, f$ and for every polynomial q over F such that $q = f(i)$ holds $\deg(q)$ is even and $\mathrm{LC}\, q \in P$. Then $\deg(p)$ is even.

(16) Let us consider a field F, an extension E of F, a polynomial p over F, an element a of F, and elements x, b of E. If $b = a$, then $\mathrm{ExtEval}(a \cdot p, x) = b \cdot (\mathrm{ExtEval}(p, x))$.

(17) Let us consider a field F, an extension E of F, a finite sequence f of elements of the carrier of Polynom-Ring F, and a polynomial p over F. Suppose $p = \sum f$. Let us consider an element a of E, and a finite sequence g of elements of E. Suppose $\mathrm{len}\, g = \mathrm{len}\, f$ and for every element i of $\mathrm{dom}\, f$ and for every polynomial q over F such that $q = f(i)$ holds $g(i) = \mathrm{ExtEval}(q, a)$. Then $\mathrm{ExtEval}(p, a) = \sum g$.

3. More on the Fields $F(a)$

Now we state the propositions:

(18) Let us consider a field F, an extension E of F, an element a of E, and an element b of F. If $b = a^{\mathbf{2}}$, then $\mathrm{ExtEval}(\mathrm{X}^2\text{-}\, b, a) = 0_E$.

(19) Let us consider a field F, an extension E of F, and an element a of E. If $a^{\mathbf{2}} \in F$, then a is F-algebraic. The theorem is a consequence of (18).

(20) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $a \notin F$ if and only if for every non zero polynomial p over F such that $\mathrm{ExtEval}(p, a) = 0_E$ holds $\deg(p) \geqslant 2$.

(21) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Suppose $a \notin F$. Let us consider an element b of F. If $b = a^{\mathbf{2}}$, then $\mathrm{MinPoly}(a, F) = \mathrm{X}^2\text{-}\, b$. The theorem is a consequence of (18) and (20).

(22) Let us consider a field F, an extension E of F, and an element a of E. Suppose $a \notin F$ and $a^{\mathbf{2}} \in F$. Then

(i) $\{1_E, a\}$ is a basis of $\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)$, and

(ii) $\deg(\mathrm{FAdj}(F, \{a\}), F) = 2$.

Proof: Reconsider $a_1 = a$ as an F-algebraic element of E. Reconsider $b = a^{\mathbf{2}}$ as an element of F. $\deg(\mathrm{MinPoly}(a_1, F)) = \deg(\mathrm{X}^2\text{-}\, b)$. $\mathrm{Base}(a_1) = \{1_E, a\}$. $\square$

(23) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and an element b of E. Then $b \in$ the carrier of $\mathrm{FAdj}(F, \{a\})$ if and only if there exists a polynomial p over F such that $\deg(p) < \deg(\mathrm{MinPoly}(a, F))$ and $b = \mathrm{ExtEval}(p, a)$.

(24) Let us consider a field F, an extension E of F, and an element a of E. Suppose $a^{\mathbf{2}} \in F$. Let us consider an element b of $\mathrm{FAdj}(F, \{a\})$. Then there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that

(i) $c_1, c_2 \in F$, and

(ii) $b = c_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot c_2$.

The theorem is a consequence of (22).

(25) Let us consider a field F, an extension E of F, and an element a of E. Suppose $a \notin F$ and $a^{\mathbf{2}} \in F$. Let us consider elements c_1, c_2, d_1, d_2 of $\mathrm{FAdj}(F, \{a\})$. Suppose $c_1, c_2, d_1, d_2 \in F$ and $c_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot c_2 = d_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot d_2$. Then

(i) $c_1 = d_1$, and

(ii) $c_2 = d_2$.

PROOF: Set $K = \mathrm{FAdj}(F, \{a\})$. Set $V = \mathrm{VecSp}(K, F)$. Set $j = {}^{@}(K, a)$. Reconsider $1_V = 1_K$, $j_1 = j$ as an element of V. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ $\$_1 = 1_K$ and $\$_2 = c_1 - d_1$ or $\$_1 = j$ and $\$_2 = c_2 - d_2$ or $\$_1 \neq 1_K$ and $\$_1 \neq j$ and $\$_2 = 0_F$. For every object x such that $x \in$ the carrier of V there exists an object y such that $y \in$ the carrier of F and $\mathcal{P}[x, y]$.

Consider l being a function from the carrier of V into the carrier of F such that for every object x such that $x \in$ the carrier of V holds $\mathcal{P}[x, l(x)]$. For every element v of V such that $v \notin \{1_V, j_1\}$ holds $l(v) = 0_F$. $\{1_V, j_1\}$ is linearly independent. $\square$

Let us consider a field F, an extension E of F, an element a of E, an element b of F, and a quadratic, non empty finite sequence f of elements of $\mathrm{FAdj}(F, \{a\})$. Now we state the propositions:

(26) Suppose $a \notin F$ and $a^{\mathbf{2}} = b$. Then there exist quadratic, non empty finite sequences g_1, g_2 of elements of F and there exists a non empty finite sequence g_3 of elements of F such that $\sum f = ({}^{@}(\sum g_1 + b \cdot (\sum g_2), \mathrm{FAdj}(F, \{a\}))) + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot ({}^{@}(\sum g_3, \mathrm{FAdj}(F, \{a\})))$.

(27) Suppose $a \notin F$ and $a^{\mathbf{2}} = b$ and $\sum f \in F$. Then there exist quadratic, non empty finite sequences g_1, g_2 of elements of F such that $\sum f = \sum g_1 + b \cdot (\sum g_2)$. The theorem is a consequence of (26) and (25).

4. Extensions of Orderings

Let F be an ordered field, E be a field, and P be an ordering of F. We say that P extends to E if and only if

(Def. 7) there exists a subset O of E such that $P \subseteq O$ and O is a positive cone.

Let E be an ordered extension of F and O be an ordering of E. We say that O extends P if and only if

(Def. 8) $O \cap (\text{the carrier of } F) = P$.

Let us consider an ordered field F, an ordered extension E of F, an ordering P of F, and an ordering O of E. Now we state the propositions:

(28) O extends P if and only if for every element a of F, $a \in P$ iff $a \in O$.

(29) O extends P if and only if $P \subseteq O$.

Let R be an ordered ring, P be an ordering of R, and a be an element of R. The functor $\mathrm{signum}(P, a)$ yielding an integer is defined by the term

(Def. 9) $$\begin{cases} 1, & \textbf{if } a \in P \setminus \{0_R\}, \\ 0, & \textbf{if } a = 0_R, \\ -1, & \textbf{otherwise}. \end{cases}$$

The functor signum(P) yielding a function from the carrier of R into $\mathbb{Z}$ is defined by

(Def. 10) for every element a of R, $it(a) = \mathrm{signum}(P, a)$.

Now we state the propositions:

(30) Let us consider an ordered integral domain R, an ordering P of R, and an element a of R. Then $a = \mathrm{signum}(P, a) \star |a|_P$.

(31) Let us consider an ordered field F, an ordered extension E of F, an ordering P of F, and an ordering O of E. Then O extends P if and only if $\mathrm{signum}(O){\restriction}(\text{the carrier of } F) = \mathrm{signum}(P)$. The theorem is a consequence of (29).

Let F be an ordered field, E be an extension of F, P be an ordering of F, and f be a finite sequence of elements of E. We say that f is P-quadratic if and only if

(Def. 11) for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, f$ there exists a non zero element a of E and there exists an element b of E such that $a \in P$ and $f(i) = a \cdot b^{\mathbf{2}}$.

Observe that there exists a finite sequence of elements of E which is P-quadratic and non empty. Let f, g be P-quadratic finite sequences of elements of E. One can check that $f \frown g$ is P-quadratic as a finite sequence of elements of E. Now we state the proposition:

(32) Let us consider an ordered field F, an extension E of F, an ordering P of F, a P-quadratic finite sequence f of elements of E, and finite sequences g_1, g_2 of elements of E. Suppose $f = g_1 \frown g_2$. Then

(i) g_1 is P-quadratic, and

(ii) g_2 is P-quadratic.

Let F be an ordered field, E be an extension of F, and P be an ordering of F. The functor P-quadraticSums(E) yielding a non empty subset of E is defined by the term

(Def. 12) the set of all $\sum f$ where f is a P-quadratic finite sequence of elements of E.

We introduce the notation $\mathrm{QS}(E, P)$ as a synonym of P-quadraticSums(E). Let us observe that $\mathrm{QS}(E, P)$ is closed under addition and closed under multiplication and has all sums of squares. Now we state the propositions:

(33) Let us consider an ordered field F, an ordering P of F, an extension E of F, and a non zero element a of E. Then $a \in \mathrm{QS}(E, P)$ if and only if there exists a P-quadratic, non empty finite sequence f of elements of E such that $\sum f = a$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\, f$ holds $f(i) \neq 0_E$. The theorem is a consequence of (32).

(34) Let us consider an ordered field F, an extension E of F, and an ordering P of F. Then $P \subseteq \mathrm{QS}(E, P)$.

(35) Let us consider an ordered field F, an ordered extension E of F, an ordering P of F, and an ordering O of E. If O extends P, then $\mathrm{QS}(E, P) \subseteq O$.
PROOF: $P \subseteq O$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every P-quadratic finite sequence f of elements of E such that $\operatorname{len} f = \$_1$ holds $\sum f \in O$. For every natural number k, $\mathcal{P}[k]$. $\square$

Let us consider an ordered field F, an extension E of F, and an ordering P of F. Now we state the propositions:

(36) $\mathrm{QS}(E, P)$ is a prepositive cone if and only if $-1_E \notin \mathrm{QS}(E, P)$.

(37) P extends to E if and only if $\mathrm{QS}(E, P)$ is a prepositive cone. The theorem is a consequence of (29), (35), (36), and (34).

(38) P extends to E if and only if for every P-quadratic, non empty finite sequence f of elements of E such that $\sum f = 0_E$ holds f is trivial. The theorem is a consequence of (29), (36), and (37).

(39) Let us consider an ordered field F, an extension E of F, an ordering P of F, and an element a of E. Suppose $a^{\mathbf{2}} \in F$. Let us consider a P-quadratic, non empty finite sequence f of elements of $\mathrm{FAdj}(F, \{a\})$. Then there exist non empty finite sequences g_1, g_2 of elements of $\mathrm{FAdj}(F, \{a\})$ such that

   (i) $\sum f = \sum g_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot (2 \star \sum g_2)$, and

   (ii) for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} g_1$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$ and there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_1(i) = b \cdot ({c_1}^{\mathbf{2}} + {c_2}^{\mathbf{2}} \cdot ({}^{@}(\mathrm{FAdj}(F, \{a\}), a))^{\mathbf{2}})$, and

   (iii) for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} g_2$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$ and there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_2(i) = b \cdot c_1 \cdot c_2$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every P-quadratic, non empty finite sequence f of elements of $\mathrm{FAdj}(F, \{a\})$ such that $\operatorname{len} f = \$_1$ there exist non empty finite sequences g_1, g_2 of elements of $\mathrm{FAdj}(F, \{a\})$ such that $\sum f = \sum g_1 + ({}^{@}(\mathrm{FAdj}(F, \{a\}), a)) \cdot (2 \star \sum g_2)$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} g_1$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$.

There exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_1(i) = b \cdot ({c_1}^{\mathbf{2}} + {c_2}^{\mathbf{2}} \cdot ({}^{@}(\mathrm{FAdj}(F, \{a\}), a))^{\mathbf{2}})$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} g_2$ there exists a non zero element b of $\mathrm{FAdj}(F, \{a\})$ and there exist elements c_1, c_2 of $\mathrm{FAdj}(F, \{a\})$ such that $b \in P$ and c_1, $c_2 \in F$ and $g_2(i) = b \cdot c_1 \cdot c_2$. For every non zero natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $n = \operatorname{len} f$. $\square$

(40) Let us consider an ordered field F, an extension E of F, and an element a of E. Suppose $a^{\mathbf{2}} \in F$. Let us consider an ordering P of F. Then P extends to $\mathrm{FAdj}(F, \{a\})$ if and only if $a^{\mathbf{2}} \in P$. The theorem is a consequence of (29), (8), (39), (2), (25), (7), (36), and (37).

(41) Let us consider an ordered, polynomial-disjoint field F, an ordering P of F, and a non square element a of F. Then P extends to $\mathrm{FAdj}(F, \{\sqrt{a}\})$ if and only if $a \in P$. The theorem is a consequence of (40).

(42) $\mathrm{Positives}(\mathbb{F}_{\mathbb{Q}})$ extends to $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{2.(\mathbb{F}_{\mathbb{Q}})}\})$. The theorem is a consequence of (41).

(43) $\mathrm{Positives}(\mathbb{F}_{\mathbb{Q}})$ does not extend to $\mathrm{FAdj}(\mathbb{F}_{\mathbb{Q}}, \{\sqrt{-1_{\mathbb{F}_{\mathbb{Q}}}}\})$.

(44) Let us consider an ordered field F, an ordering P of F, an extension E of F, an element a of F, and elements b, c of E. Suppose $b^{\mathbf{2}} = a$ and $c^{\mathbf{2}} = -a$. Then

   (i) P extends to $\mathrm{FAdj}(F, \{b\})$, or

   (ii) P extends to $\mathrm{FAdj}(F, \{c\})$.

   The theorem is a consequence of (40).

(45) Let us consider an ordered, polynomial-disjoint field F, an ordering P of F, and non square elements a, b of F. Suppose $b = -a$. Then

   (i) P extends to $\mathrm{FAdj}(F, \{\sqrt{a}\})$, or

   (ii) P extends to $\mathrm{FAdj}(F, \{\sqrt{b}\})$.

   The theorem is a consequence of (41).

Let us consider a formally real field F, an extension E of F, an element a of F, and an element b of E. Now we state the propositions:

(46) If $b^{\mathbf{2}} = a$ and $a \in \mathrm{QS}(F)$, then $\mathrm{FAdj}(F, \{b\})$ is formally real. The theorem is a consequence of (40).

(47) If $b^{\mathbf{2}} = a$ and $\mathrm{FAdj}(F, \{b\})$ is not formally real, then $-a \in \mathrm{QS}(F)$. The theorem is a consequence of (8) and (27).

Let us consider an ordered, polynomial-disjoint field F and a non square element a of F. Now we state the propositions:

(48) If $a \in \mathrm{QS}(F)$, then $\mathrm{FAdj}(F, \{\sqrt{a}\})$ is formally real. The theorem is a consequence of (46).

(49) If $\mathrm{FAdj}(F, \{\sqrt{a}\})$ is not formally real, then $-a \in \mathrm{QS}(F)$. The theorem is a consequence of (47).

(50) Let us consider an ordered field F, an ordering P of F, and an extension E of F. If $\deg(E, F)$ is an odd natural number, then P extends to E.
PROOF: Define $\mathcal{Q}$[natural number] $\equiv$ for every extension E of F such that $\deg(E, F) = 2 \cdot \$_1 + 1$ holds P extends to E. For every natural number k, $\mathcal{Q}[k]$. Reconsider $n = \deg(E1, F)$ as an odd natural number. Consider k being an integer such that $n = 2 \cdot k + 1$. $\square$

(51) Let us consider an ordered field F, an ordering P of F, an irreducible element p of the carrier of Polynom-Ring F, an extension E of F, and an element a of E. Suppose $\deg(p)$ is odd and a is a root of p in E. Then P extends to $\mathrm{FAdj}(F, \{a\})$. The theorem is a consequence of (11) and (50).

References

[1] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

[2] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. Equality in computer proof-assistants. In Ganzha, Maria and Maciaszek, Leszek and Paprzycki, Marcin, editor, *Proceedings of the 2015 Federated Conference on Computer Science and Information Systems*, volume 5 of *ACSIS-Annals of Computer Science and Information Systems*, pages 45–54. IEEE, 2015. doi:10.15439/2015F229.

[3] Adam Grabowski, Artur Korniłowicz, and Christoph Schwarzweller. On algebraic hierarchies in mathematical repository of Mizar. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*, volume 8 of *Annals of Computer Science and Information Systems*, pages 363–371, 2016. doi:10.15439/2016F520.

[4] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[5] Serge Lang. *Algebra*. PWN, Warszawa, 1984.

[6] Alexander Prestel. *Lectures on Formally Real Fields*. Springer-Verlag, 1984.

[7] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

[8] Knut Radbruch. *Geordnete Körper*. Lecture Notes, University of Kaiserslautern, Germany, 1991.

[9] Piotr Rudnicki, Christoph Schwarzweller, and Andrzej Trybulec. Commutative algebra in the Mizar system. *Journal of Symbolic Computation*, 32(1/2):143–169, 2001. doi:10.1006/jsco.2001.0456.

[10] Christoph Schwarzweller. Normal extensions. *Formalized Mathematics*, 31(1):121–130, 2023. doi:10.2478/forma-2023-0011.

[11] Christoph Schwarzweller. Field extensions and Kronecker's construction. *Formalized Mathematics*, 27(**3**):229–235, 2019. doi:10.2478/forma-2019-0022.

[12] Christoph Schwarzweller. Ordered rings and fields. *Formalized Mathematics*, 25(**1**):63–72, 2017. doi:10.1515/forma-2017-0006.

[13] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Quadratic extensions. *Formalized Mathematics*, 29(**4**):229–240, 2021. doi:10.2478/forma-2021-0021.

Accepted December 18, 2023