FORMALIZED MATHEMATICS
Vol. 31, No. 1, pp. 287–298, 2023
DOI: 10.2478/forma-2023-0023
e-ISSN: 1898–9934

sciendo.com/journal/forma

Simple Extensions

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Agnieszka Rowińska-Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we continue the formalization of field theory in Mizar. We introduce simple extensions: an extension E of F is simple if E is generated over F by a single element of E, that is $E = F(a)$ for some $a \in E$. First, we prove that a finite extension E of F is simple if and only if there are only finitely many intermediate fields between E and F [7]. Second, we show that finite extensions of a field F with characteristic 0 are always simple [1]. For this we had to prove, that irreducible polynomials over F have single roots only, which required extending results on divisibility and gcds of polynomials [14], [13] and formal derivation of polynomials [15].

MSC: 12F05 12F99 68V20

Keywords: field theory; intermediate field; simple extension; primitive element

MML identifier: FIELD_14, version: 8.1.14 5.76.1462

Introduction

In this paper we formalize simple extensions [6] using the Mizar formalism [3, 2, 5, 4]. An extension E of F is simple, if E is generated by a single element, that is $E = F(a)$ for some $a \in E$. It is well known that both all finite extensions of fields with characteristic 0 and finite extensions of finite fields are simple, so that most common field extensions are simple. In this paper we deal with fields of characteristic 0 only.

In the preliminary section, we provide some technical lemmas about sums of finite sequences and field extensions. We also define the set of intermediate fields between E and F needed later to characterize simple extensions.

The next two sections provide a number of basic theorems about bags and polynomials necessary to prove our main theorems, for example, that if all roots a of a polynomial of $p * q$ have multiplicity 1, then p and q have no common roots.

The fourth section deals with divisibility of polynomials [8]. We among others show that the gcd of two polynomials is the same in F and an extension E of F and that for a polynomial p_1 of the form

$$(x - a_1) \cdot (x - a_2) \cdot \cdots \cdot (x - a_n)$$

$gcd(p_1, p_2)$ with a polynomial p_2 is again of the form

$$(x - b_1) \cdot (x - b_2) \cdot \cdots \cdot (x - b_k),$$

where the b_j are exactly the common roots of p_1 and p_2. We also show that the number of monic divisors of a polynomial is bounded by $2^{\deg p}$. This is crucial in the proof that a simple extension has only a finite number of intermediate fields.

To show that finite extensions of characteric 0 are simple, it is used that an irreducible polynomial has no multiple roots. This is shown in section five using derivatives [1]: for an irreducible polynomial we have $gcd(p, p') = 1$, so p is square free.

In the last section we finally define simple extensions and primitive elements, and show the main results. A finite extension E over an infinite field F is simple if and only if there are only finitely many intermediate fields between E and F: If $E = F(a)$ is simple, then each intermediate field K is uniquely determined by the roots of a's minimal polynomial over K. Because each such polynomial is a monic divisor of p's minimal polynomial over E, there are only finitely many intermediate fields. If the number of intermediate fields is finite, then – because F is infinite – for a and b there exist x and y with $x \neq y$, and $F(a + x * b) = F(a + y * b)$. Then both a and b are in $F(a + x * b)$ [1] from which follows that $F(a, b) = F(a + x * b)$, so that E is simple by induction. Because a field with characteristic 0 is infinite, this also shows our second main result: every finite extension E over a field F with characteristic 0 is simple.

1. Preliminaries

Let n be a non zero, natural number. Note that $n - 1$ is natural. Let n be an element of $\mathbb{N}$. Note that $n -' 1$ is natural. Let R be a ring and n be a natural number. Let us note that $n \cdot (0_R)$ reduces to 0_R. Observe that every finite sequence of elements of $\mathbb{N}$ is non-negative yielding. Now we state the proposition:

(1) Let us consider a finite sequence f of elements of $\mathbb{N}$, and natural numbers i, j. If i, $j \in \operatorname{dom} f$ and $i \neq j$, then $\sum f \geqslant f(i) + f(j)$.

Let F be a field, E be an extension of F, and a, b be F-algebraic elements of E. One can verify that the functor $\{a, b\}$ yields an F-algebraic subset of E. Let K be an extension of F and E be a K-extending extension of F. Note that every F-algebraic element of E is K-algebraic. Let E be an F-finite extension of F. One can verify that every subset of E is F-algebraic.

Let K be an F-finite extension of F. Note that there exists an extension of F which is K-extending and F-finite. Let E be an extension of F and K be an extension of E. Let us observe that there exists an extension of F which is K-extending and E-extending. Now we state the propositions:

(2) Let us consider a field F, an extension E of F, and subsets T_1, T_2, T_3 of E. Suppose $\mathrm{FAdj}(F, T_1) = \mathrm{FAdj}(F, T_2)$. Then $\mathrm{FAdj}(F, T_1 \cup T_3) = \mathrm{FAdj}(F, T_2 \cup T_3)$.

(3) Let us consider a ring R, a ring extension S of R, an element a of R, an element b of S, and an element n of $\mathbb{N}$. If $a = b$, then $n \cdot a = n \cdot b$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \cdot a = \$_1 \cdot b$. For every natural number k, $\mathcal{P}[k]$. $\square$

Let F be a field and E be an extension of F.

The functor IntermediateFields(E, F) yielding a set is defined by

(Def. 1) for every object x, $x \in it$ iff there exists a strict field K such that $K = x$ and F is a subfield of K and K is a subfield of E.

One can check that IntermediateFields(E, F) is non empty and field-membered. Now we state the propositions:

(4) Let us consider a field F, an extension E of F, and a strict field K. Then $K \in$ IntermediateFields(E, F) if and only if F is a subfield of K and K is a subfield of E.

(5) Let us consider a field F, an extension E of F, and an F-extending extension K of E. Then IntermediateFields$(E, F) \subseteq$ IntermediateFields(K, F).

2. More on Bags

Let Z be a non empty set and B be a bag of Z. One can verify that the functor $\overline{\overline{B}}$ yields an element of $\mathbb{N}$. Let us consider a non empty set Z and bags B_1, B_2 of Z. Now we state the propositions:

(6) $B_1 \mid B_2$ if and only if there exists a bag B_3 of Z such that $B_2 = B_1 + B_3$.

(7) If $B_1 \mid B_2$, then $\overline{\overline{B_1}} \leqslant \overline{\overline{B_2}}$. The theorem is a consequence of (6).

(8) Let us consider a non empty set Z, a bag B of Z, and an object o. Then $B(o) \leqslant \overline{\overline{B}}$.

(9) Let us consider a non empty set Z, a bag B of Z, and objects o_1, o_2. Suppose $B(o_1) = \overline{\overline{B}}$ and $o_2 \neq o_1$. Then $B(o_2) = 0$. The theorem is a consequence of (1).

(10) Let us consider an integral domain R, and a bag B_1 of the carrier of R. Then $\overline{\overline{B_1}} = 1$ if and only if there exists an element a of R such that $B_1 = \mathrm{Bag}(\{a\})$. The theorem is a consequence of (8) and (9).

(11) Let us consider a field F, and non zero bags B_1, B_2 of the carrier of F. If $B_2 \mid B_1$ and $\overline{\overline{B_1}} = 1$, then $B_2 = B_1$. The theorem is a consequence of (10) and (7).

(12) Let us consider a non empty set Z, and bags B_1, B_2 of Z. If $B_2 \mid B_1$ and $B_1 -' B_2$ is zero, then $B_2 = B_1$.

(13) Let us consider a field F, and non empty, finite subsets S_1, S_2 of F. Then $\mathrm{Bag}(S_1) \mid \mathrm{Bag}(S_2)$ if and only if $S_1 \subseteq S_2$.

(14) Let us consider a field F, a non zero bag B of the carrier of F, and a non empty, finite subset S_1 of F. Then $B \mid \mathrm{Bag}(S_1)$ if and only if there exists a non empty, finite subset S_2 of F such that $B = \mathrm{Bag}(S_2)$ and $S_2 \subseteq S_1$. The theorem is a consequence of (13).

3. More on Polynomials

Let R be an integral domain and p, q be non constant elements of the carrier of Polynom-Ring R. Let us note that $p \cdot q$ is non constant. Now we state the propositions:

(15) Let us consider a field F, a monic polynomial p over F, and a polynomial r over F. If $p * r$ is monic, then r is monic.

(16) Let us consider an integral domain R, and a polynomial p over R. Then p is monic and constant if and only if $p = \mathbf{1}.R$.

(17) Let us consider an integral domain R, an element a of R, and a non zero natural number m. Then $(\mathrm{rpoly}(1, a))^m$ is a product of linear polynomials of R.

(18) Let us consider a field F, a polynomial p over F, an extension E of F, a polynomial q over E, and an element n of $\mathbb{N}$. If $q = p$, then $q^n = p^n$.

(19) Let us consider a field F, a polynomial p over F, and elements i, j of $\mathbb{N}$. Then $p^{i+j} = p^i * p^j$.

(20) Let us consider a field F, an element a of F, and a product of linear polynomials p of F and $\{a\}$. Then $p = \mathrm{rpoly}(1, a)$.

(21) Let us consider a field F, non zero bags B_1, B_2 of the carrier of F, a product of linear polynomials p of F and B_1, and a product of linear polynomials q of F and B_2. If $B_1 = B_2$, then $p = q$.

(22) Let us consider a field F, an extension E of F, an element p of the carrier of Polynom-Ring F, and an element q of the carrier of Polynom-Ring E. If $q = p$, then $\mathrm{Coeff}(q) = \mathrm{Coeff}(p)$.

(23) Let us consider a field F, non zero polynomials p, q over F, and an element a of F. Then $\mathrm{multiplicity}(p, a) \leqslant \mathrm{multiplicity}(p * q, a)$.

(24) Let us consider a field F, an extension E of F, polynomials p, q over F, and polynomials p_1, q_1 over E. If $p_1 = p$ and $q_1 = q$, then $p_1[q_1] = p[q]$.
PROOF: Consider f being a finite sequence of elements of the carrier of Polynom-Ring F such that $p[q] = \sum f$ and $\mathrm{len}\, f = \mathrm{len}\, p$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, f$ holds $f(n) = p(n -' 1) \cdot (q^{n -' 1})$.

Consider g being a finite sequence of elements of the carrier of Polynom-Ring E such that $p_1[q_1] = \sum g$ and $\mathrm{len}\, g = \mathrm{len}\, p_1$ and for every element n of $\mathbb{N}$ such that $n \in \mathrm{dom}\, g$ holds $g(n) = p_1(n -' 1) \cdot ({q_1}^{n -' 1})$. $f = g$ by (18), [11, (23)], [12, (2)]. □

(25) Let us consider a field F, polynomials p, q over F, an extension E of F, and an element a of E. Then $\mathrm{ExtEval}(p[q], a) = \mathrm{ExtEval}(p, \mathrm{ExtEval}(q, a))$. The theorem is a consequence of (24).

(26) Let us consider a field F, elements a, b of F, an extension E of F, and an element x of E. Then $\mathrm{ExtEval}(\langle a, b\rangle, x) = ({}^{@}(a, E)) + ({}^{@}(b, E)) \cdot x$.

(27) Let us consider a non degenerated commutative ring R, and polynomials p, q over R. Then $\mathrm{Roots}(p) \subseteq \mathrm{Roots}(p * q)$.

(28) Let us consider an integral domain R, non empty, finite subsets S_1, S_2 of R, a product of linear polynomials p of R and S_1, and a product of linear polynomials q of R and S_2. Suppose $S_1 \cap S_2 = \emptyset$. Then $p * q$ is a product of linear polynomials of R and $S_1 \cup S_2$.

(29) Let us consider a field F, and non zero polynomials p, q over F. Suppose for every element a of F such that a is a root of $p * q$ holds $\mathrm{multiplicity}(p * q, a) = 1$. Then $\mathrm{Roots}(p) \cap \mathrm{Roots}(q) = \emptyset$.

(30) Let us consider a field F, and a product of linear polynomials p of F. Then p is a product of linear polynomials of F and $\mathrm{Roots}(p)$ if and only if for every element a of F such that a is a root of p holds $\mathrm{multiplicity}(p, a) = 1$.

(31) Let us consider a field F, a non empty, finite subset S of F, a product of linear polynomials p of F and S, and a non zero polynomial q over F with roots. Suppose $p * q$ is a product of linear polynomials of F and

$S \cup \mathrm{Roots}(q)$. Then q is a product of linear polynomials of F and $\mathrm{Roots}(q)$. The theorem is a consequence of (15), (23), and (30).

(32) Let us consider a field F, a non empty, finite subset S of F, an element a of F, a product of linear polynomials p of F and $S \cup \{a\}$, and a non constant polynomial q over F. Suppose $p = \mathrm{rpoly}(1, a) * q$ and $a \notin S$. Then q is a product of linear polynomials of F and S.
PROOF: $\mathrm{rpoly}(1, a)$ is a product of linear polynomials of F and $\{a\}$. For every element b of F such that b is a root of $\mathrm{rpoly}(1, a) * q$ holds $\mathrm{multiplicity}(\mathrm{rpoly}(1, a) * q, b) = 1$. $S = \mathrm{Roots}(q)$. □

(33) Let us consider a field F, non empty, finite subsets S_1, S_2 of F, a product of linear polynomials p of F and S_1, an element a of F, and a non constant polynomial q over F. Suppose $p = \mathrm{rpoly}(1, a) * q$ and $S_2 = S_1 \setminus \{a\}$. Then q is a product of linear polynomials of F and S_2. The theorem is a consequence of (32).

4. On Divisibility and Polynomial GCDs

Let R, S be non degenerated commutative rings and p be a polynomial over R. We say that p is square-free over S if and only if

(Def. 2) there exists no non constant polynomial q_1 over S and there exists a polynomial q_2 over S such that $q_2 = p$ and ${q_1}^2 \mid q_2$.

Let R be a non degenerated commutative ring. We say that p is square-free if and only if

(Def. 3) p is square-free over R.

Let R be an integral domain. Let us note that there exists a non constant polynomial over R which is square-free and there exists a non constant polynomial over R which is non square-free. Now we state the propositions:

(34) Let us consider a non degenerated commutative ring R, and a polynomial p over R. Then p is square-free if and only if there exists no non constant polynomial q over R such that $q^2 \mid p$.

(35) Let us consider a field F, and a monic polynomial p over F. If $p \mid \mathbf{1}.F$, then $p = \mathbf{1}.F$.

(36) Let us consider a field F, and non zero polynomials p, q over F. Then $\mathrm{BRoots}(p) \mid \mathrm{BRoots}(p * q)$. The theorem is a consequence of (23).

(37) Let us consider an integral domain R, and polynomials p, q over R. If $q \mid p$, then $\mathrm{Roots}(q) \subseteq \mathrm{Roots}(p)$.

(38) Let us consider a field F, polynomials p, q over F, and a non zero polynomial r over F. If $r * q \mid r * p$, then $q \mid p$.

(39) Let us consider a field F, polynomials p, q over F, and a monic polynomial r over F. Then $\gcd(r * p, r * q) = r * (\gcd(p, q))$. The theorem is a consequence of (15), (38), and (35).

(40) Let us consider a field F, polynomials p, q over F, and elements n, k of $\mathbb{N}$. If $q^n \mid p$ and $k \leqslant n$, then $q^k \mid p$. The theorem is a consequence of (19).

(41) Let us consider a field F, an extension E of F, an element p of the carrier of Polynom-Ring F, and an element q of the carrier of Polynom-Ring E. If $q = p$, then if q is irreducible, then p is irreducible.

(42) Let us consider a GCD domain R. Then every element of R is a GCD of a and 0_R.

Let us consider an EuclideanRing R, elements a, b of R, and a GCD g of a and b. Now we state the propositions:

(43) There exist elements r, s of R such that $g = a \cdot r + b \cdot s$.

(44) $\{g\}$–ideal $= \{a, b\}$–ideal. The theorem is a consequence of (43).

(45) Let us consider a field F, an extension E of F, elements p, q of the carrier of Polynom-Ring F, and elements p_1, q_1 of the carrier of Polynom-Ring E. If $p_1 = p$ and $q_1 = q$, then $\gcd(p_1, q_1) = \gcd(p, q)$.

(46) Let us consider a field F, and an element p of the carrier of Polynom-Ring F. Then $\gcd(p, \mathbf{0}.F) = \text{NormPoly}\, p$.

(47) Let us consider a field F, an element p of the carrier of Polynom-Ring F, and a non zero element q of the carrier of Polynom-Ring F. If $q \mid p$, then $\gcd(p, q) = \text{NormPoly}\, q$.

(48) Let us consider a field F, an extension E of F, elements p, q of the carrier of Polynom-Ring F, and elements p_1, q_1 of the carrier of Polynom-Ring E. If $p_1 = p$ and $q_1 = q$, then $q_1 \mid p_1$ iff $q \mid p$. The theorem is a consequence of (45) and (47).

(49) Let us consider a field F, a non zero bag B_1 of the carrier of F, a product of linear polynomials p of F and B_1, and a non constant, monic polynomial q over F. Then $q \mid p$ if and only if there exists a non zero bag B_2 of the carrier of F such that q is a product of linear polynomials of F and B_2 and $B_2 \mid B_1$. The theorem is a consequence of (36), (12), and (21).

(50) Let us consider a field F, a non empty, finite subset S_1 of F, a product of linear polynomials p of F and S_1, and a non constant, monic polynomial q over F. Then $q \mid p$ if and only if there exists a non empty, finite subset S_2 of F such that q is a product of linear polynomials of F and S_2 and $S_2 \subseteq S_1$. The theorem is a consequence of (49), (14), and (13).

(51) Let us consider a field F, a product of linear polynomials p of F, a monic polynomial q over F, and an element a of F. Then $q \mid \text{rpoly}(1, a) * p$ if

and only if $q \mid p$ or there exists a polynomial r over F such that $r \mid p$ and $q = \text{rpoly}(1, a) * r$. The theorem is a consequence of (16), (49), and (38).

(52) Let us consider a field F, a product of linear polynomials p of F, and a polynomial q over F. Then $\text{Roots}(p) \cap \text{Roots}(q) = \emptyset$ if and only if $\gcd(p, q) = \mathbf{1}.F$.

(53) Let us consider a field F, non empty, finite subsets S_1, S_2 of F, a product of linear polynomials p_1 of F and S_1, and a polynomial p_2 over F. Suppose $S_2 = S_1 \cap \text{Roots}(p_2)$. Then $\gcd(p_1, p_2)$ is a product of linear polynomials of F and S_2.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non empty, finite subsets S_1, S_2 of F for every product of linear polynomials p_1 of F and S_1 for every polynomial p_2 over F such that $\overline{\overline{S_2}} = \$_1$ and $S_2 = S_1 \cap \text{Roots}(p_2)$ holds $\gcd(p_1, p_2)$ is a product of linear polynomials of F and S_2. $\mathcal{P}[1]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{S_2}} = n$. □

Let R be an integral domain and p be a polynomial over R. The functors: Divisors(p) and MonicDivisors(p) yielding non empty subsets of the carrier of Polynom-Ring R are defined by terms

(Def. 4) $\{q$, where q is an element of the carrier of Polynom-Ring $R : q \mid p\}$,

(Def. 5) $\{q$, where q is a monic element of the carrier of Polynom-Ring $R : q \mid p\}$,

respectively. Now we state the propositions:

(54) Let us consider a field F, and an element a of F.
Then $\text{MonicDivisors}(\text{rpoly}(1, a)) = \{\mathbf{1}.F, \text{rpoly}(1, a)\}$.

(55) Let us consider a field F, a non zero element p of the carrier of Polynom-Ring F, and a non zero element a of F.
Then $\text{MonicDivisors}(p) = \text{MonicDivisors}(a \cdot p)$.

(56) Let us consider a field F, an extension E of F, a polynomial p over F, and a polynomial q over E. If $q = p$, then $\text{MonicDivisors}(p) \subseteq \text{MonicDivisors}(q)$.

Let F be a field and p be a non zero polynomial over F. Let us note that MonicDivisors(p) is finite. Now we state the proposition:

(57) Let us consider a field F, and a non zero polynomial p over F. Then $\overline{\overline{\text{MonicDivisors}(p)}} \leqslant 2^{\deg(p)}$. The theorem is a consequence of (55), (56), and (16).

5. Formal Derivative of Polynomials and Multiplicity of Roots

Let R be a ring. We introduce the notation Deriv(R) as a synonym of Der1(R). Let R be an integral domain. Observe that Deriv(R) is derivation. Now we state the propositions:

(58) Let us consider a non degenerated commutative ring R. Then

(i) $(\mathrm{Deriv}(R))(\mathbf{1}.R) = \mathbf{0}.R$, and

(ii) $(\mathrm{Deriv}(R))(\mathbf{0}.R) = \mathbf{0}.R$.

(59) Let us consider a ring R, an element p of the carrier of Polynom-Ring R, and an element a of R. Then $(\mathrm{Deriv}(R))(a \cdot p) = a \cdot (\mathrm{Deriv}(R))(p)$.

(60) Let us consider a non degenerated commutative ring R, and a constant element p of the carrier of Polynom-Ring R. Then $(\mathrm{Deriv}(R))(p) = \mathbf{0}.R$. The theorem is a consequence of (59) and (58).

(61) Let us consider a ring R, and an element a of R. Then $(\mathrm{Deriv}(R))(\mathrm{X}- a) = \mathbf{1}.R$.

(62) Let us consider a non degenerated commutative ring R, and an element p of the carrier of Polynom-Ring R. Then $(\mathrm{Deriv}(R))(p^0) = \mathbf{0}.R$. The theorem is a consequence of (58).

(63) Let us consider an integral domain R, an element p of the carrier of Polynom-Ring R, and a non zero element n of $\mathbb{N}$. Then $(\mathrm{Deriv}(R))(p^n) = n \cdot (p^{n-1} \cdot (\mathrm{Deriv}(R))(p))$.

(64) Let us consider a non degenerated commutative ring R, and a non zero element p of the carrier of Polynom-Ring R. Then $\deg((\mathrm{Deriv}(R))(p)) < \deg(p)$.

(65) Let us consider a field F, and a non zero element p of the carrier of Polynom-Ring F. Suppose $\gcd(p, (\mathrm{Deriv}(F))(p)) = \mathbf{1}.F$. Then p is square-free.

(66) Let us consider a non degenerated commutative ring R, an element p of the carrier of Polynom-Ring R, a commutative ring extension S of R, and an element q of the carrier of Polynom-Ring S. If $q = p$, then $(\mathrm{Deriv}(S))(q) = (\mathrm{Deriv}(R))(p)$. The theorem is a consequence of (3).

Let R be a non degenerated commutative ring, S be a commutative ring extension of R, p be a non zero polynomial over R, and a be an element of S. The functor multiplicity(p, a) yielding an element of $\mathbb{N}$ is defined by

(Def. 6) there exists a non zero polynomial q over S such that $q = p$ and *it* $=$ multiplicity(q, a).

Now we state the propositions:

(67) Let us consider a field F, a non zero polynomial p over F, an element a of F, and an element n of $\mathbb{N}$. Then $n = \mathrm{multiplicity}(p, a)$ if and only if $(\mathrm{X}- a)^n \mid p$ and $(\mathrm{X}- a)^{n+1} \nmid p$.

(68) Let us consider a field F with characteristic 0, and a non zero element p of the carrier of Polynom-Ring F. Then $\deg((\mathrm{Deriv}(F))(p)) = \deg(p) - 1$. The theorem is a consequence of (60) and (64).

(69) Let us consider a field F with characteristic 0, and an element p of the carrier of Polynom-Ring F. Then $(\mathrm{Deriv}(F))(p) = \mathbf{0}.F$ if and only if p is constant. The theorem is a consequence of (68) and (60).

(70) Let us consider a field F with characteristic 0, and an irreducible element p of the carrier of Polynom-Ring F. Then $\gcd(p, (\mathrm{Deriv}(F))(p)) = \mathbf{1}.F$. The theorem is a consequence of (69) and (64).

(71) Let us consider a field F with characteristic 0, an irreducible element p of the carrier of Polynom-Ring F, an extension E of F, and an element a of E. If a is a root of p in E, then $\mathrm{multiplicity}(p, a) = 1$. The theorem is a consequence of (66), (70), (45), (65), (67), and (40).

6. Simple Extensions

Let F be a field and E be an extension of F. We say that E is F-simple if and only if

(Def. 7) there exists an element a of E such that $E \approx \mathrm{FAdj}(F, \{a\})$.

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

(Def. 8) $E \approx \mathrm{FAdj}(F, \{a\})$.

Let us note that there exists an extension of F which is F-simple and F-finite. Let E be an F-simple extension of F. One can verify that there exists an element of E which is F-primitive.

Let E be an extension of F and a be an element of E. The functor $\deg(a, F)$ yielding an integer is defined by the term

(Def. 9) $\deg(\mathrm{FAdj}(F, \{a\}), F)$.

Now we state the propositions:

(72) Let us consider a field F, an F-finite extension E of F, and an element a of E. Then $\deg(a, F) \mid \deg(E, F)$.

(73) Let us consider a field F, and an F-finite extension E of F. Then E is F-simple if and only if there exists an element a of E such that $\deg(a, F) = \deg(E, F)$.

(74) Let us consider a field F, an F-finite extension E of F, and an element a of E. Then a is F-primitive if and only if $\deg(a, F) = \deg(E, F)$.

(75) Let us consider a field F, an F-finite extension K of F, an F-finite, F-extending extension E of K, and a K-algebraic element a of E. Suppose $E \approx \mathrm{FAdj}(F, \{a\})$. Then

(i) $E \approx \mathrm{FAdj}(K, \{a\})$, and

(ii) $K \approx \mathrm{FAdj}(F, \mathrm{Coeff}(\mathrm{MinPoly}(a, K)))$.

Proof: $\mathrm{FAdj}(K, \{a\}) = \mathrm{FAdj}(F, \{a\})$ by [9, (11)]. Set $K_1 = \mathrm{FAdj}(F, \mathrm{Coeff}$ $(\mathrm{MinPoly}(a, K)))$. Reconsider $E_1 = E$ as an F-extending extension of K_1. Reconsider $a_1 = a$ as a K_1-algebraic element of E_1. $\mathrm{FAdj}(F, \{a_1\}) = \mathrm{FAdj}(K_1, \{a_1\})$. Reconsider $p = \mathrm{MinPoly}(a, K)$ as a polynomial over K_1. p is irreducible. □

(76) Let us consider an infinite field F, and an F-finite extension E of F. Then E is F-simple if and only if $\mathrm{IntermediateFields}(E, F)$ is finite. The theorem is a consequence of (5), (2), (4), (75), and (22).

(77) Let us consider a field F with characteristic 0, an extension E of F, and F-algebraic elements a, b of E. Then there exists an element x of F such that $\mathrm{FAdj}(F, \{a, b\}) = \mathrm{FAdj}(F, \{a + ({}^{@}(x, E)) \cdot b\})$.

Proof: Set $K = \mathrm{FAdj}(F, \{a, b\})$. Set $m_1 = \mathrm{MinPoly}(a, F)$. Set $m_3 = \mathrm{MinPoly}(b, F)$. Reconsider $a_3 = a$, $b_1 = b$ as an element of K. Consider Z being an extension of E such that Z is algebraic closed. Set $R_1 = \mathrm{Roots}(Z, m_1)$. Set $R_2 = (\mathrm{Roots}(Z, m_3)) \setminus \{b\}$. There exists an element x of F such that for every elements c, d of Z such that $c \in R_1$ and $d \in R_2$ holds $({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z)) \neq c + ({}^{@}(x, Z)) \cdot d$.

Consider x being an element of F such that for every elements c, d of Z such that $c \in R_1$ and $d \in R_2$ holds $({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z)) \neq c + ({}^{@}(x, Z)) \cdot d$. Set $l_1 = ({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z))$. Set $G = \mathrm{FAdj}(F, \{l_1\})$. G is a subfield of K. Reconsider $m_2 = \mathrm{MinPoly}(a, F)$, $m_4 = \mathrm{MinPoly}(b, F)$ as a polynomial over G.

Reconsider $m_2 = \mathrm{MinPoly}(a, F)$, $m_4 = \mathrm{MinPoly}(b, F)$ as a non constant polynomial over G. Set $g = \langle {}^{@}(G, l_1), -({}^{@}(x, G)) \rangle$. Set $h = m_2[g]$. Reconsider $m_5 = m_4$, $h_1 = h$ as a polynomial over Z. $\gcd(h_1, m_5) = \mathrm{X}-({}^{@}(b_1, Z))$. $b \in G$. $a \in G$. $a + ({}^{@}(x, E)) \cdot b = ({}^{@}(a_3, Z)) + ({}^{@}(x, Z)) \cdot ({}^{@}(b_1, Z))$ by [10, (12)]. □

Let F be a field with characteristic 0. One can verify that every F-finite extension of F is F-simple.

References

[1] Andreas Gathmann. *Einführung in die Algebra.* Lecture Notes, University of Kaiserslautern, Germany, 2011.

[2] Adam Grabowski and Christoph Schwarzweller. Translating mathematical vernacular into knowledge repositories. In Michael Kohlhase, editor, *Mathematical Knowledge Management*, volume 3863 of *Lecture Notes in Computer Science*, pages 49–64. Springer, 2006. doi:10.1007/11618027_4. 4th International Conference on Mathematical Knowledge Management, Bremen, Germany, MKM 2005, July 15–17, 2005, Revised Selected Papers.

[3] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Mizar in a nutshell. *Journal of Formalized Reasoning*, 3(2):153–245, 2010.

[4] 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.

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

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

[7] Serge Lang. *Algebra.* Springer Verlag, 2002 (Revised Third Edition).

[8] Heinz Lüneburg. *Gruppen, Ringe, Körper: Die grundlegenden Strukturen der Algebra.* Oldenbourg Verlag, 1999.

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

[10] Christoph Schwarzweller. Renamings and a condition-free formalization of Kronecker's construction. *Formalized Mathematics*, 28(**2**):129–135, 2020. doi:10.2478/forma-2020-0012.

[11] Christoph Schwarzweller. Ring and field adjunctions, algebraic elements and minimal polynomials. *Formalized Mathematics*, 28(**3**):251–261, 2020. doi:10.2478/forma-2020-0022.

[12] Christoph Schwarzweller. Splitting fields. *Formalized Mathematics*, 29(**3**):129–139, 2021. doi:10.2478/forma-2021-0013.

[13] Christoph Schwarzweller. On roots of polynomials and algebraically closed fields. *Formalized Mathematics*, 25(**3**):185–195, 2017. doi:10.1515/forma-2017-0018.

[14] Christoph Schwarzweller, Artur Korniłowicz, and Agnieszka Rowińska-Schwarzweller. Some algebraic properties of polynomial rings. *Formalized Mathematics*, 24(**3**):227–237, 2016. doi:10.1515/forma-2016-0019.

[15] Yasushige Watase. Derivation of commutative rings and the Leibniz formula for power of derivation. *Formalized Mathematics*, 29(**1**):1–8, 2021. doi:10.2478/forma-2021-0001.

Accepted December 18, 2023