FORMALIZED MATHEMATICS
Vol. 28, No. 3, Pages 251–261, 2020
DOI: 10.2478/forma-2020-0022

sciendo
https://www.sciendo.com/

Ring and Field Adjunctions, Algebraic Elements and Minimal Polynomials

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In [6], [7] we presented a formalization of Kronecker's construction of a field extension of a field F in which a given polynomial $p \in F[X] \backslash F$ has a root [4], [5], [3]. As a consequence for every field F and every polynomial there exists a field extension E of F in which p splits into linear factors. It is well-known that one gets the smallest such field extension – the splitting field of p – by adjoining the roots of p to F.

In this article we start the Mizar formalization [1], [2] towards splitting fields: we define ring and field adjunctions, algebraic elements and minimal polynomials and prove a number of facts necessary to develop the theory of splitting fields, in particular that for an algebraic element a over F a basis of the vector space $F(a)$ over F is given by $a^0, \ldots, a^{n-1}$, where n is the degree of the minimal polynomial of a over F.

MSC: 12F05 68V20

Keywords: ring and field adjunctions; algebraic elements and minimal polynomials

MML identifier: FIELD_6, version: 8.1.10 5.64.1388

1. Preliminaries

Now we state the proposition:

(1) Let us consider a ring R. Then R is degenerated if and only if the carrier of $R = \{0_R\}$.

ISSN 1426–2630(Print), 1898-9934(Online)

Let F be a field. Note that $\{0_F\}$–ideal is maximal.

Let R be a non degenerated, non almost left invertible commutative ring. Let us note that $\{0_R\}$–ideal is non maximal.

Let R be a ring. We say that R has a subfield if and only if

(Def. 1) there exists a field F such that F is a subring of R.

Observe that there exists a ring which has a subfield.

Let R be a ring which has a subfield.

A subfield of R is a field defined by

(Def. 2) *it* is a subring of R.

Now we state the proposition:

(2) Let us consider a non degenerated ring R, and a non zero polynomial p over R. Then $p(\deg p) = \mathrm{LC}\, p$.

Let R be a non degenerated ring and p be a non zero polynomial over R. One can verify that $\mathrm{LM}(p)$ is non zero.

Let us consider a ring R and a polynomial p over R. Now we state the propositions:

(3) $\deg \mathrm{LM}(p) = \deg p$.

(4) $\mathrm{LC}\, \mathrm{LM}(p) = \mathrm{LC}\, p$.

(5) Let us consider a non degenerated ring R, and a non zero polynomial p over R. Then $\deg(p - \mathrm{LM}(p)) < \deg p$. The theorem is a consequence of (2), (3), and (4).

(6) Let us consider a ring R, a polynomial p over R, and a natural number i. Then $(\langle 0_R, 1_R\rangle * p)(i+1) = p(i)$.

(7) Let us consider a ring R, and a polynomial p over R. Then $(\langle 0_R, 1_R\rangle * p)(0) = 0_R$.

(8) Let us consider an integral domain R, and a non zero polynomial p over R. Then $\deg(\langle 0_R, 1_R\rangle * p) = \deg p + 1$.

(9) Let us consider a commutative ring R, a polynomial p over R, and an element a of R. Then $\mathrm{eval}(\langle 0_R, 1_R\rangle * p, a) = a \cdot (\mathrm{eval}(p, a))$. The theorem is a consequence of (1).

(10) Let us consider a ring R, a ring extension S of R, an element p of the carrier of $\mathrm{PolyRing}(R)$, an element a of R, and an element b of S. If $b = a$, then $\mathrm{ExtEval}(p, b) = \mathrm{eval}(p, a)$.

(11) Let us consider a field F, an element p of the carrier of $\mathrm{PolyRing}(F)$, an extension E of F, an E-extending extension K of F, an element a of E, and an element b of K. If $a = b$, then $\mathrm{ExtEval}(p, a) = \mathrm{ExtEval}(p, b)$.

Let L be a non empty zero structure, a, b be elements of L, f be a (the carrier of L)-valued function, and x, y be objects. Observe that $f {+\cdot} [x \longmapsto a, y \longmapsto b]$ is (the carrier of L)-valued.

Let f be a finite-Support sequence of L. One can verify that $f+\cdot[x \longmapsto a, y \longmapsto b]$ is finite-Support as a sequence of L.

2. On Subrings and Subfields

Now we state the propositions:

(12) Let us consider strict rings R_1, R_2. Suppose R_1 is a subring of R_2 and R_2 is a subring of R_1. Then $R_1 = R_2$.

(13) Let us consider a ring S, and subrings R_1, R_2 of S. Then R_1 is a subring of R_2 if and only if the carrier of $R_1 \subseteq$ the carrier of R_2.

(14) Let us consider a ring S, and strict subrings R_1, R_2 of S. Then $R_1 = R_2$ if and only if the carrier of R_1 = the carrier of R_2. The theorem is a consequence of (13) and (12).

Let us consider a ring S, a subring R of S, elements x, y of S, and elements x_1, y_1 of R. Now we state the propositions:

(15) If $x = x_1$ and $y = y_1$, then $x + y = x_1 + y_1$.

(16) If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

(17) Let us consider a ring S, a subring R of S, an element x of S, and an element x_1 of R. If $x = x_1$, then $-x = -x_1$. The theorem is a consequence of (15).

(18) Let us consider a field E, a subfield F of E, a non zero element x of E, and an element x_1 of F. If $x = x_1$, then $x^{-1} = {x_1}^{-1}$. The theorem is a consequence of (16).

(19) Let us consider a ring S, a subring R of S, an element x of S, an element x_1 of R, and an element n of $\mathbb{N}$. If $x = x_1$, then $x^n = {x_1}^n$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every element x of S for every element x_1 of R such that $x = x_1$ holds $x^{\$_1} = {x_1}^{\$_1}$. For every natural number k, $\mathcal{P}[k]$. $\square$

(20) Let us consider a ring S, a subring R of S, elements x_1, x_2 of S, and elements y_1, y_2 of R. Suppose $x_1 = y_1$ and $x_2 = y_2$. Then $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle$.

(21) Let us consider a commutative ring R, a commutative ring extension S of R, elements x_1, x_2 of S, elements y_1, y_2 of R, and an element n of $\mathbb{N}$. Suppose $x_1 = y_1$ and $x_2 = y_2$. Then $\langle x_1, x_2 \rangle^n = \langle y_1, y_2 \rangle^n$.

(22) Let us consider an integral domain R, a domain ring extension S of R, a non zero element n of $\mathbb{N}$, and an element a of S.

Then $\mathrm{ExtEval}(\langle 0_R, 1_R \rangle^n, a) = a^n$. The theorem is a consequence of (21).

(23) Let us consider a ring R, a ring extension S of R, an element a of R, and an element b of S. If $a = b$, then $a \restriction R = b \restriction S$.

(24) Let us consider a field F, an extension E of F, an element p of the carrier of PolyRing(F), and an element q of the carrier of PolyRing(E). If $p = q$, then NormPoly p = NormPoly q. The theorem is a consequence of (18) and (16).

(25) Let us consider a field F, an extension E of F, an element p of the carrier of PolyRing(F), and an element a of E. Then ExtEval$(p, a) = 0_E$ if and only if ExtEval(NormPoly $p, a) = 0_E$. The theorem is a consequence of (24).

(26) Let us consider a ring R, a ring extension S of R, an element a of S, and a polynomial p over R. Then ExtEval$(-p, a) = -$ExtEval(p, a). The theorem is a consequence of (17).

(27) Let us consider a ring R, a ring extension S of R, an element a of S, and polynomials p, q over R. Then ExtEval$(p - q, a) =$ ExtEval$(p, a) -$ ExtEval(q, a). The theorem is a consequence of (26).

(28) Let us consider a ring R, a ring extension S of R, an element a of S, and a constant polynomial p over R. Then ExtEval$(p, a) =$ LC p.

(29) Let us consider a non degenerated ring R, a ring extension S of R, elements a, b of S, and a non zero polynomial p over R. Suppose $b =$ LC p. Then ExtEval(Leading-Monomial $p, a) = b \cdot (a^{\deg p})$.

3. Ring and Field Adjunctions

Let R be a ring, S be a ring extension of R, and T be a subset of S. The functor $/\backslash(\mathrm{R}, T)$ yielding a non empty subset of S is defined by the term

(Def. 3) $\{x$, where x is an element of S : for every subring U of S such that R is a subring of U and T is a subset of U holds $x \in U\}$.

The functor RingAdjunction(R, T) yielding a strict double loop structure is defined by

(Def. 4) the carrier of *it* $= /\backslash(\mathrm{R}, T)$ and the addition of *it* $=$ (the addition of S) $\restriction /\backslash(\mathrm{R}, T)$ and the multiplication of *it* $=$ (the multiplication of S) $\restriction /\backslash(\mathrm{R}, T)$ and the one of *it* $= 1_S$ and the zero of *it* $= 0_S$.

We introduce the notation RAdj(R, T) as a synonym of RingAdjunction(R, T).

One can check that RAdj(R, T) is non empty.

Let R be a non degenerated ring. Let us observe that RAdj(R, T) is non degenerated.

Let R be a ring. Observe that RAdj(R, T) is Abelian, add-associative, right zeroed, and right complementable.

Let R be a commutative ring and S be a commutative ring extension of R. One can check that RAdj(R, T) is commutative.

Let R be a ring and S be a ring extension of R. Let us observe that RAdj(R, T) is associative, well unital, and distributive.

Now we state the propositions:

(30) Let us consider a ring R, and a ring extension S of R. Then every subset T of S is a subset of RAdj(R, T).

(31) Let us consider a ring R, a ring extension S of R, and a subset T of S. Then R is a subring of RAdj(R, T).

(32) Let us consider a ring R, a ring extension S of R, a subset T of S, and a subring U of S. Suppose R is a subring of U and T is a subset of U. Then RAdj(R, T) is a subring of U.

(33) Let us consider a strict ring R, a ring extension S of R, and a subset T of S. Then RAdj$(R, T) = R$ if and only if T is a subset of R. The theorem is a consequence of (30).

Let R be a ring, S be a ring extension of R, and T be a subset of S. Let us note that the functor RAdj(R, T) yields a strict subring of S. One can check that RAdj(R, T) is R-extending.

Let F be a field, R be a ring extension of F, and T be a subset of R. Let us note that RAdj(F, T) has a subfield.

Now we state the proposition:

(34) Let us consider a field F, a ring extension R of F, and a subset T of R. Then F is a subfield of RAdj(F, T). The theorem is a consequence of (31).

Let F be a field, E be an extension of F, and T be a subset of E. The functor $/\backslash(\mathrm{F}, T)$ yielding a non empty subset of E is defined by the term

(Def. 5) $\{x$, where x is an element of E : for every subfield U of E such that F is a subfield of U and T is a subset of U holds $x \in U\}$.

The functor FieldAdjunction(F, T) yielding a strict double loop structure is defined by

(Def. 6) the carrier of $it = /\backslash(\mathrm{F}, T)$ and the addition of $it =$ (the addition of $E) \restriction /\backslash(\mathrm{F}, T)$ and the multiplication of $it =$ (the multiplication of $E) \restriction /\backslash(\mathrm{F}, T)$ and the one of $it = 1_E$ and the zero of $it = 0_E$.

We introduce the notation FAdj(F, T) as a synonym of FieldAdjunction(F, T). One can check that FAdj(F, T) is non degenerated and FAdj(F, T) is Abelian, add-associative, right zeroed, and right complementable and FieldAdjunction$(F,$

T) is commutative, associative, well unital, distributive, and almost left invertible.

Now we state the propositions:

(35) Let us consider a field F, and an extension E of F. Then every subset T of E is a subset of $\mathrm{FAdj}(F, T)$.

(36) Let us consider a field F, an extension E of F, and a subset T of E. Then F is a subfield of $\mathrm{FAdj}(F, T)$.

(37) Let us consider a field F, an extension E of F, a subset T of E, and a subfield U of E. Suppose F is a subfield of U and T is a subset of U. Then $\mathrm{FAdj}(F, T)$ is a subfield of U.

(38) Let us consider a strict field F, an extension E of F, and a subset T of E. Then $\mathrm{FAdj}(F, T) = F$ if and only if T is a subset of F. The theorem is a consequence of (35).

Let F be a field, E be an extension of F, and T be a subset of E. Let us observe that the functor $\mathrm{FAdj}(F, T)$ yields a strict subfield of E. Let us note that $\mathrm{FAdj}(F, T)$ is F-extending.

Let us consider a field F, an extension E of F, and a subset T of E. Now we state the propositions:

(39) $\mathrm{RAdj}(F, T)$ is a subring of $\mathrm{FAdj}(F, T)$.

(40) $\mathrm{RAdj}(F, T) = \mathrm{FAdj}(F, T)$ if and only if $\mathrm{RAdj}(F, T)$ is a field. The theorem is a consequence of (31), (30), (37), (39), and (12).

4. Algebraic Elements

Let R be a non degenerated commutative ring, S be a commutative ring extension of R, and a be an element of S. Observe that $\mathrm{HomExtEval}(a, R)$ is additive, multiplicative, and unity-preserving and every commutative ring extension of R is $(\mathrm{PolyRing}(R))$-homomorphic.

Let F be a field. Let us note that there exists an extension of F which is $(\mathrm{PolyRing}(F))$-homomorphic.

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

(Def. 7) $\ker \mathrm{HomExtEval}(a, F) \neq \{0_{\mathrm{PolyRing}(F)}\}$.

We introduce the notation a is F-transcendental as an antonym for a is F-algebraic. Now we state the proposition:

(41) Let us consider a ring R, a ring extension S of R, and an element a of S. Then $\mathrm{AnnPoly}(a, R) = \ker \mathrm{HomExtEval}(a, R)$.

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

(42) a is F-algebraic if and only if a is integral over F. The theorem is a consequence of (25).

(43) a is F-algebraic if and only if there exists a non zero polynomial p over F such that $\mathrm{ExtEval}(p, a) = 0_E$. The theorem is a consequence of (42).

Let F be a field and E be an extension of F. Note that there exists an element of E which is F-algebraic.

Let us consider a field F, a $(\mathrm{PolyRing}(F))$-homomorphic extension E of F, and an element a of E. Now we state the propositions:

(44) $\mathrm{RAdj}(F, \{a\}) = \mathrm{Im}\, \mathrm{HomExtEval}(a, F)$. The theorem is a consequence of (20), (32), and (14).

(45) The carrier of $\mathrm{RAdj}(F, \{a\})$ = the set of all $\mathrm{ExtEval}(p, a)$ where p is a polynomial over F. The theorem is a consequence of (44).

5. On Linear Combinations and Polynomials

Now we state the propositions:

(46) Let us consider a field F, a vector space V over F, a subspace W of V, and a linear combination l_1 of W. Then there exists a linear combination l_2 of V such that

(i) the support of l_2 = the support of l_1, and

(ii) for every element v of V such that $v \in$ the support of l_2 holds $l_2(v) = l_1(v)$.

PROOF: Consider f being a function such that $l_1 = f$ and $\mathrm{dom}\, f$ = the carrier of W and $\mathrm{rng}\, f \subseteq$ the carrier of F. Define $\mathcal{P}$[element of V, element of F] $\equiv$ $\$_1 \in$ the support of l_1 and $\$_2 = f(\$_1)$ or $\$_1 \notin$ the support of l_1 and $\$_2 = 0_F$. For every element x of the carrier of V, there exists an element y of the carrier of F such that $\mathcal{P}[x, y]$. Consider g being a function from V into F such that for every element x of V, $\mathcal{P}[x, g(x)]$. □

(47) Let us consider a field F, an extension E of F, an element a of E, an element n of $\mathbb{N}$, and a linear combination l of $\mathrm{VecSp}(E, F)$. Then there exists a polynomial p over F such that

(i) $\deg p \leqslant n$, and

(ii) for every element i of $\mathbb{N}$ such that $i \leqslant n$ holds $p(i) = l(a^i)$.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a natural number i such that $i \leqslant n$ and $\$_1 = i$ and $\$_2 = l(a^i)$ or there exists a natural number i such that $i > n$ and $\$_1 = i$ and $\$_2 = 0_F$. For every element x of $\mathbb{N}$, there exists an element y of the carrier of F such that $\mathcal{P}[x, y]$. Consider p being a function from $\mathbb{N}$ into the carrier of F such that for every element x of $\mathbb{N}$, $\mathcal{P}[x, p(x)]$. For every natural number i such that $i \leqslant n$ holds $p(i) = l(a^i)$. For every natural number i such that $i \geqslant n + 1$ holds $p(i) = 0_F$. □

(48) Let us consider a field F, an extension E of F, an element a of E, an element n of $\mathbb{N}$, a linear combination l of VecSp(E, F), and a non zero polynomial p over F. Suppose $l(a^{\deg p}) = \mathrm{LC}\, p$ and the support of $l = \{a^{\deg p}\}$. Then $\sum l = \mathrm{ExtEval}(\mathrm{LM}(p), a)$. The theorem is a consequence of (35) and (29).

(49) Let us consider a field F, an extension E of F, an element a of E, an element n of $\mathbb{N}$, and a subset M of VecSp(E, F). Suppose $M = \{a^i$, where i is an element of $\mathbb{N} : i \leqslant n\}$ and for every elements i, j of $\mathbb{N}$ such that $i < j \leqslant n$ holds $a^i \neq a^j$. Let us consider a linear combination l of M, and a polynomial p over F. Suppose $\deg p \leqslant n$ and for every element i of $\mathbb{N}$ such that $i \leqslant n$ holds $p(i) = l(a^i)$. Then $\mathrm{ExtEval}(p, a) = \sum l$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv$ for every linear combination l of M such that $\overline{\overline{\text{the support of } l}} = \$_1$ for every polynomial p over F such that $\deg p \leqslant n$ and for every element i of $\mathbb{N}$ such that $i \leqslant n$ holds $p(i) = l(a^i)$ holds $\sum l = \mathrm{ExtEval}(p, a)$. $\mathcal{P}[0]$ by [8, (13)]. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\alpha}} = n$, where α is the support of l. □

6. Minimal Polynomials

Let F be a field, E be an extension of F, and a be an F-algebraic element of E. We introduce the notation MinPoly(a, F) as a synonym of the minimal polynomial of a over F.

Note that MinPoly(a, F) is monic and irreducible.

Let us consider a field F, an extension E of F, an F-algebraic element a of E, and an element p of the carrier of PolyRing(F). Now we state the propositions:

(50) $p = \mathrm{MinPoly}(a, F)$ if and only if p is monic and irreducible and ker Hom-ExtEval$(a, F) = \{p\}$–ideal. The theorem is a consequence of (42) and (41).

(51) $p = \mathrm{MinPoly}(a, F)$ if and only if p is monic and $\mathrm{ExtEval}(p, a) = 0_E$ and for every non zero polynomial q over F such that $\mathrm{ExtEval}(q, a) = 0_E$ holds $\deg p \leqslant \deg q$. The theorem is a consequence of (42) and (50).

(52) $p = \mathrm{MinPoly}(a, F)$ if and only if p is monic and irreducible and ExtEval$(p,$

$a) = 0_E$. The theorem is a consequence of (42) and (50).

(53) $\mathrm{ExtEval}(p, a) = 0_E$ if and only if $\mathrm{MinPoly}(a, F) \mid p$. The theorem is a consequence of (50) and (51).

(54) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $\mathrm{MinPoly}(a, F) = \mathrm{rpoly}(1, a)$ if and only if $a \in$ the carrier of F. The theorem is a consequence of (10), (52), and (17).

(55) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and elements i, j of $\mathbb{N}$. If $i < j < \deg \mathrm{MinPoly}(a, F)$, then $a^i \neq a^j$. The theorem is a consequence of (7), (6), (17), (52), and (53).

(56) Let us consider a field F, a ($\mathrm{PolyRing}(F)$)-homomorphic extension E of F, and an element a of E. Then a is F-algebraic if and only if $\mathrm{FAdj}(F, \{a\}) = \mathrm{RAdj}(F, \{a\})$. The theorem is a consequence of (50), (44), and (40).

(57) Let us consider a field F, a ($\mathrm{PolyRing}(F)$)-homomorphic extension E of F, and a non zero element a of E. Then a is F-algebraic if and only if $a^{-1} \in \mathrm{RAdj}(F, \{a\})$. The theorem is a consequence of (56), (35), (18), (45), (17), (28), and (43).

(58) Let us consider a field F, an extension E of F, and an element a of E. Then a is F-transcendental if and only if $\mathrm{RAdj}(F, \{a\})$ and $\mathrm{PolyRing}(F)$ are isomorphic. The theorem is a consequence of (44) and (56).

(59) Let us consider a field F, a ($\mathrm{PolyRing}(F)$)-homomorphic extension E of F, and an F-algebraic element a of E.
Then $\mathrm{PolyRing}(F)/\{\mathrm{MinPoly}(a, F)\}$–ideal and $\mathrm{FAdj}(F, \{a\})$ are isomorphic. The theorem is a consequence of (50), (44), and (56).

7. A Basis of the Vector Space $\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)$

Let F be a field, E be an extension of F, and a be an F-algebraic element of E. The functor $\mathrm{Base}(a)$ yielding a non empty subset of $\mathrm{VecSp}(\mathrm{FAdj}(F, \{a\}), F)$ is defined by the term

(Def. 8) $\{a^n$, where n is an element of $\mathbb{N} : n < \deg \mathrm{MinPoly}(a, F)\}$.

One can verify that $\mathrm{Base}(a)$ is finite. Now we state the propositions:

(60) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and a polynomial p over F. Then $\mathrm{ExtEval}(p, a) \in \mathrm{Lin}(\mathrm{Base}(a))$. The theorem is a consequence of (51).

(61) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and a linear combination l of $\mathrm{Base}(a)$. Then there exists a polynomial p over F such that

(i) $\deg p < \deg \mathrm{MinPoly}(a, F)$, and

(ii) for every element i of $\mathbb{N}$ such that $i < \deg \mathrm{MinPoly}(a, F)$ holds $p(i) = l(a^i)$.

The theorem is a consequence of (46) and (47).

(62) Let us consider a field F, an extension E of F, an F-algebraic element a of E, a linear combination l of Base(a), and a non zero polynomial p over F. Suppose $l(a^{\deg p}) = \mathrm{LC}\, p$ and the support of $l = \{a^{\deg p}\}$. Then $\sum l = \mathrm{ExtEval}(\mathrm{LM}(p), a)$. The theorem is a consequence of (35), (36), (19), and (29).

(63) Let us consider a field F, an extension E of F, an F-algebraic element a of E, a linear combination l of Base(a), and a polynomial p over F. Suppose $\deg p < \deg \mathrm{MinPoly}(a, F)$ and for every element i of $\mathbb{N}$ such that $i < \deg \mathrm{MinPoly}(a, F)$ holds $p(i) = l(a^i)$. Then $\sum l = \mathrm{ExtEval}(p, a)$.

PROOF: Define $\mathcal{P}[\underline{\text{natural number}}] \equiv$ for every linear combination l of Base(a) such that $\overline{\overline{\text{the support of } l}} = \$_1$ for every polynomial p over F such that $\deg p < \deg \mathrm{MinPoly}(a, F)$ and for every element i of $\mathbb{N}$ such that $i < \deg \mathrm{MinPoly}(a, F)$ holds $p(i) = l(a^i)$ holds $\sum l = \mathrm{ExtEval}(p, a)$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\alpha}} = n$, where α is the support of l. $\square$

(64) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and a linear combination l of Base(a). Suppose $\sum l = 0_F$. Then $l = \mathbf{0}_{\mathrm{LC}_{\mathrm{VecSp}(\mathrm{FAdj}(F,\{a\}),F)}}$. The theorem is a consequence of (61), (63), and (53).

(65) Let us consider a field F, a (PolyRing(F))-homomorphic extension E of F, and an F-algebraic element a of E. Then Base(a) is a basis of VecSp(FAdj($F, \{a\}$), F). The theorem is a consequence of (64), (56), (45), and (60).

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

(66) $\overline{\overline{\mathrm{Base}(a)}} = \deg \mathrm{MinPoly}(a, F)$.

PROOF: Set $m = \deg \mathrm{MinPoly}(a, F)$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element x of $\mathrm{Seg}\, m$ and there exists an element y of $\mathbb{N}$ such that $\$_1 = x$ and $y = x - 1$ and $\$_2 = a^y$. Consider f being a function such that $\mathrm{dom}\, f = \mathrm{Seg}\, m$ and for every object x such that $x \in \mathrm{Seg}\, m$ holds $\mathcal{P}[x, f(x)]$. $\square$

(67) $\deg(\mathrm{FAdj}(F, \{a\}), F) = \deg \mathrm{MinPoly}(a, F)$. The theorem is a consequence of (66) and (65).

Let F be a field, E be an extension of F, and a be an F-algebraic element of E. Let us note that FAdj($F, \{a\}$) is F-finite.

Now we state the proposition:

(68) Let us consider a field F, an extension E of F, and an element a of E. Then a is F-algebraic if and only if $\mathrm{FAdj}(F, \{a\})$ is F-finite. The theorem is a consequence of (27), (22), (43), (35), (19), (47), (11), and (49).

References

[1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pąk. The role of the Mizar Mathematical Library for interactive proof development in Mizar. *Journal of Automated Reasoning*, 61(1):9–32, 2018. doi:10.1007/s10817-017-9440-6.

[3] Nathan Jacobson. *Basic Algebra I*. Dover Books on Mathematics, 1985.

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

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

[6] 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.

[7] Christoph Schwarzweller. Representation matters: An unexpected property of polynomial rings and its consequences for formalizing abstract field theory. In M. Ganzha, L. Maciaszek, and M. Paprzycki, editors, *Proceedings of the 2018 Federated Conference on Computer Science and Information Systems*, volume 15 of *Annals of Computer Science and Information Systems*, pages 67–72. IEEE, 2018. doi:10.15439/2018F88.

[8] Yasushige Watase. Algebraic numbers. *Formalized Mathematics*, 24(**4**):291–299, 2016. doi:10.1515/forma-2016-0025.

Accepted September 25, 2020