FORMALIZED MATHEMATICS
Vol. 29, No. 1, Pages 39–47, 2021
DOI: 10.2478/forma-2021-0004

sciendo
https://sciendo.com/journal/forma

Algebraic Extensions

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Agnieszka Rowińska-Schwarzweller
Sopot, Poland

Summary. In this article we further develop field theory in Mizar [1], [2], [3] towards splitting fields. We deal with algebraic extensions [4], [5]: a field extension E of a field F is algebraic, if every element of E is algebraic over F. We prove amongst others that finite extensions are algebraic and that field extensions generated by a finite set of algebraic elements are finite. From this immediately follows that field extensions generated by roots of a polynomial over F are both finite and algebraic. We also define the field of algebraic elements of E over F and show that this field is an intermediate field of $E|F$.

MSC: 12F05 68V20

Keywords: algebraic extensions; finite extensions; field of algebraic numbers

MML identifier: FIELD_7, version: 8.1.11 5.65.1394

1. Preliminaries

Let L_1, L_2 be double loop structures. We say that $L_1 \approx L_2$ if and only if

(Def. 1) the double loop structure of L_1 = the double loop structure of L_2.

One can verify that the predicate is reflexive and symmetric.

Now we state the propositions:

(1) Let us consider rings R, S. Then $R \approx S$ if and only if there exists a function f from R into S such that $f = \mathrm{id}_R$ and f is isomorphism.

(2) Let us consider strict rings R, S. Then $R \approx S$ if and only if $R = S$.

Let F_1, F_2 be fields. Let us note that $F_1 \approx F_2$ if and only if the condition (Def. 2) is satisfied.

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

(Def. 2) F_1 is a subfield of F_2 and F_2 is a subfield of F_1.

Now we state the proposition:

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

Let us consider a field F and extensions E_1, E_2 of F. Now we state the propositions:

(4) If $E_1 \approx E_2$, then $\mathrm{VecSp}(E_1, F) = \mathrm{VecSp}(E_2, F)$.

(5) If $E_1 \approx E_2$, then $\deg(E_1, F) = \deg(E_2, F)$. The theorem is a consequence of (4).

Let F be a field and E be an extension of F. Note that there exists an extension of F which is E-homomorphic and there exists an extension of F which is E-monomorphic and there exists an extension of F which is E-isomorphic.

Let R be a ring and a, b be elements of R. One can check that the functor $\{a, b\}$ yields a subset of R. Let F be a field, V be a vector space over F, and a be an element of V. Note that the functor $\{a\}$ yields a subset of V. Let a, b be elements of V. Let us observe that the functor $\{a, b\}$ yields a subset of V. Let us note that every basis of V is linearly independent.

Now we state the proposition:

(6) Let us consider a field F, a vector space V over F, and a subset X of V. Then X is linearly independent if and only if for every linear combinations l_1, l_2 of X such that $\sum l_1 = \sum l_2$ holds $l_1 = l_2$.

Let F be a field and E be an extension of F. Observe that every basis of $\mathrm{VecSp}(E, F)$ is non empty and $\deg(E, F)$ is non zero.

Let E be an F-finite extension of F. Observe that every basis of $\mathrm{VecSp}(E, F)$ is finite. Let us consider a field F and an extension E of F. Now we state the propositions:

(7) $\deg(E, F) = 1$ if and only if the carrier of $E =$ the carrier of F.

(8) $\deg(E, F) = 1$ if and only if $E \approx F$. The theorem is a consequence of (7).

(9) $\deg(E, F) = 1$ if and only if $\{1_E\}$ is a basis of $\mathrm{VecSp}(E, F)$. The theorem is a consequence of (7).

Let F be a field and E be an extension of F. One can check that there exists a subset of $\mathrm{VecSp}(E, F)$ which is non empty, finite, and linearly independent.

Now we state the proposition:

(10) Let us consider a field F, an extension E of F, and subsets T_1, T_2 of E. Suppose $T_1 \subseteq T_2$. Then $\mathrm{FAdj}(F, T_1)$ is a subfield of $\mathrm{FAdj}(F, T_2)$.

Let F be a field and p be a polynomial over F. The functor $\mathrm{Coeff}(p)$ yielding a subset of F is defined by the term

(Def. 3) $\{p(i)$, where i is an element of $\mathbb{N} : p(i) \neq 0_F\}$.

Let us note that Coeff(p) is finite. Now we state the propositions:

(11) Let us consider a field F, an extension E of F, and a polynomial p over E. Suppose Coeff$(p) \subseteq$ the carrier of F. Then p is a polynomial over F.

(12) Let us consider a field F, an extension E of F, and a non zero polynomial p over E. Suppose Coeff$(p) \subseteq$ the carrier of F. Then p is a non zero polynomial over F. The theorem is a consequence of (11).

(13) Let us consider a ring R, a ring extension S of R, an element p of the carrier of PolyRing(R), and an element q of the carrier of PolyRing(S). If $p = q$, then Roots$(S, p) =$ Roots(q).

Let R be an integral domain and p be a non zero element of the carrier of PolyRing(R). Note that Roots(p) is finite. Let S be a domain ring extension of R. One can check that Roots(S, p) is finite. Let F be a field and E be an extension of F. Let us observe that there exists an extension of E which is F-extending. Let E be an F-finite extension of F. Note that there exists an F-extending extension of E which is F-finite and there exists an F-extending extension of E which is E-finite. Now we state the propositions:

(14) Let us consider a field F, an element p of the carrier of PolyRing(F), an extension E of F, an E-extending extension U of F, an element a of E, and an element b of U. If $a = b$, then ExtEval$(p, a) =$ ExtEval(p, b).

(15) Let us consider a field F, an element p of the carrier of PolyRing(F), an extension E of F, and an element q of the carrier of PolyRing(E). Suppose $q = p$. Let us consider an E-extending extension U of F, and an element a of U. Then ExtEval$(q, a) =$ ExtEval(p, a).

Let R be a ring, S be a ring extension of R, and a be an element of R. The functor ${}^@(a, S)$ yielding an element of S is defined by the term

(Def. 4) a.

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

(Def. 5) $a \in$ the carrier of R.

One can verify that there exists an element of S which is R-membered.

Let a be an element of S. Assume a is R-membered. The functor ${}^@(R, a)$ yielding an element of R is defined by the term

(Def. 6) a.

Let a be an R-membered element of S. Let us observe that ${}^@(R, a)$ reduces to a. Let F be a field and E be an extension of F. One can check that there exists an element of E which is non zero and F-algebraic.

Let a be an element of F. One can check that ${}^@(a, E)$ is F-algebraic.

Let K be an E-extending extension of F and a be an F-algebraic element of E. Note that ${}^{@}(a, K)$ is F-algebraic.

2. More on Finite Extensions

Now we state the propositions:

(16) Let us consider a field F, an extension E of F, and an E-extending extension K of F. Then every linear combination of $\mathrm{VecSp}(K, F)$ is a linear combination of $\mathrm{VecSp}(K, E)$.

(17) Let us consider a field F, an extension E of F, an E-extending extension K of F, a subset B_E of $\mathrm{VecSp}(K, E)$, and a subset B_F of $\mathrm{VecSp}(K, F)$. Suppose $B_F \subseteq B_E$. Then every linear combination of B_F is a linear combination of B_E. The theorem is a consequence of (16).

(18) Let us consider a field F, an extension E of F, an E-extending extension K of F, a finite subset B_E of $\mathrm{VecSp}(K, E)$, a finite subset B_F of $\mathrm{VecSp}(K, F)$, a linear combination l_1 of B_F, and a linear combination l_2 of B_E. If $l_1 = l_2$ and $B_F \subseteq B_E$, then $\sum l_1 = \sum l_2$.
Proof: by induction on card(the support of l_1).

Let F be a field, E be an extension of F, K be an F-extending extension of E, B_E be a subset of $\mathrm{VecSp}(E, F)$, and B_K be a subset of $\mathrm{VecSp}(K, E)$. The functor $\mathrm{Base}(B_E, B_K)$ yielding a subset of $\mathrm{VecSp}((K$ **qua** extension of $F), F)$ is defined by the term

(Def. 7) $\{a \cdot b$, where a, b are elements of $K : a \in B_E$ and $b \in B_K\}$.

Let B_E be a non empty subset of $\mathrm{VecSp}(E, F)$ and B_K be a non empty subset of $\mathrm{VecSp}(K, E)$. One can verify that $\mathrm{Base}(B_E, B_K)$ is non empty.

Now we state the propositions:

(19) Let us consider a field F, an extension E of F, an F-extending extension K of E, a linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, a linearly independent subset B_K of $\mathrm{VecSp}(K, E)$, and elements a_1, a_2, b_1, b_2 of K. Suppose $a_1, a_2 \in B_E$ and $b_1, b_2 \in B_K$. If $a_1 \cdot b_1 = a_2 \cdot b_2$, then $a_1 = a_2$ and $b_1 = b_2$.

(20) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, and a non empty, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$. Then $\overline{\overline{\mathrm{Base}(B_E, B_K)}} = \overline{\overline{B_E \times B_K}}$.
Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exist elements a, b of K such that $a \in B_E$ and $b \in B_K$ and $\$_1 = a \cdot b$ and $\$_2 = \langle a, b\rangle$. Consider f being a function from $\mathrm{Base}(B_E, B_K)$ into $B_E \times B_K$ such that for every object

x such that $x \in \mathrm{Base}(B_E, B_K)$ holds $\mathcal{P}[x, f(x)]$. $\mathrm{rng}\, f = B_E \times B_K$. f is one-to-one. □

(21) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, finite, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, and a non empty, finite, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$. Then $\overline{\overline{\mathrm{Base}(B_E, B_K)}} = \overline{\overline{B_E}} \cdot \overline{\overline{B_K}}$. The theorem is a consequence of (20).

Let F be a field, E be an extension of F, K be an F-extending extension of E, B_E be a non empty, finite, linearly independent subset of $\mathrm{VecSp}(E, F)$, and B_K be a non empty, finite, linearly independent subset of $\mathrm{VecSp}(K, E)$. Observe that $\mathrm{Base}(B_E, B_K)$ is finite.

Let B_K be a non empty, linearly independent subset of $\mathrm{VecSp}(K, E)$, l be a linear combination of $\mathrm{Base}(B_E, B_K)$, and b be an element of K. The functor $\mathrm{down}(l, b)$ yielding a linear combination of B_E is defined by

(Def. 8) for every element a of K such that $a \in B_E$ and $b \in B_K$ holds $it(a) = l(a \cdot b)$ and for every element a of E such that $a \notin B_E$ or $b \notin B_K$ holds $it(a) = 0_F$.

Let B_K be a non empty, finite, linearly independent subset of $\mathrm{VecSp}(K, E)$. The functor $\mathrm{down}\, l$ yielding a linear combination of B_K is defined by

(Def. 9) for every element b of K such that $b \in B_K$ holds $it(b) = \sum \mathrm{down}(l, b)$.

Let E be an F-finite extension of F, B_E be a basis of $\mathrm{VecSp}(E, F)$, and l_1 be a linear combination of B_K. The functor $\mathrm{lift}(l_1, B_E)$ yielding a linear combination of $\mathrm{Base}(B_E, B_K)$ is defined by

(Def. 10) for every element b of K such that $b \in B_K$ there exists a linear combination l_2 of B_E such that $\sum l_2 = l_1(b)$ and for every element a of K such that $a \in B_E$ and $a \cdot b \in \mathrm{Base}(B_E, B_K)$ holds $it(a \cdot b) = l_2(a)$.

Now we state the propositions:

(22) Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, a basis B_K of $\mathrm{VecSp}(K, E)$, and a linear combination l of $\mathrm{Base}(B_E, B_K)$. Then $\mathrm{lift}(\mathrm{down}\, l, B_E) = l$. The theorem is a consequence of (6).

(23) Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, a basis B_K of $\mathrm{VecSp}(K, E)$, and a linear combination l of B_K. Then $\mathrm{down}\,\mathrm{lift}(l, B_E) = l$.

(24) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, finite, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, a non empty, finite, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$, and linear combinations l, l_1, l_2 of $\mathrm{Base}(B_E, B_K)$. Suppo-

se $l = l_1 + l_2$. Let us consider an element b of K. Then $\mathrm{down}(l, b) = \mathrm{down}(l_1, b) + \mathrm{down}(l_2, b)$.

(25) Let us consider a field F, an extension E of F, an F-extending extension K of E, a non empty, finite, linearly independent subset B_E of $\mathrm{VecSp}(E, F)$, a non empty, finite, linearly independent subset B_K of $\mathrm{VecSp}(K, E)$, and linear combinations l, l_1, l_2 of $\mathrm{Base}(B_E, B_K)$. If $l = l_1 + l_2$, then $\mathrm{down}\, l = \mathrm{down}\, l_1 + \mathrm{down}\, l_2$. The theorem is a consequence of (24).

Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, a basis B_K of $\mathrm{VecSp}(K, E)$, and a linear combination l of $\mathrm{Base}(B_E, B_K)$. Now we state the propositions:

(26) $\sum l = \sum \mathrm{down}\, l$.

PROOF: by induction on card(the support of l).

(27) If $\sum l = 0_{\mathrm{VecSp}((K \textbf{ qua } \text{extension of } F), F)}$, then the support of $l = \emptyset$. The theorem is a consequence of (26).

Let us consider a field F, an F-finite extension E of F, an E-finite, F-extending extension K of E, a basis B_E of $\mathrm{VecSp}(E, F)$, and a basis B_K of $\mathrm{VecSp}(K, E)$. Now we state the propositions:

(28) $\mathrm{Lin}(\mathrm{Base}(B_E, B_K))$ = the vector space structure of $\mathrm{VecSp}((K$ **qua** extension of $F), F)$. The theorem is a consequence of (23) and (26).

(29) $\mathrm{Base}(B_E, B_K)$ is a basis of $\mathrm{VecSp}((K$ **qua** extension of $F), F)$. The theorem is a consequence of (27) and (28).

(30) Let us consider a field F, an F-finite extension E of F, and an E-finite, F-extending extension K of E. Then $\deg(K, F) = (\deg(K, E)) \cdot (\deg(E, F))$. The theorem is a consequence of (29) and (21).

(31) Let us consider a field F, an extension E of F, and an E-extending extension K of F. Suppose K is F-finite. Then

(i) E is F-finite, and

(ii) $\deg(E, F) \leqslant \deg(K, F)$, and

(iii) K is E-finite, and

(iv) $\deg(K, E) \leqslant \deg(K, F)$.

PROOF: Set B_F = the basis of $\mathrm{VecSp}(K, F)$. Reconsider $B_E = B_F$ as a finite subset of $\mathrm{VecSp}(K, E)$. $\mathrm{Lin}(B_E) = \mathrm{VecSp}(K, E)$. Consider I being a subset of $\mathrm{VecSp}(K, E)$ such that $I \subseteq B_E$ and I is linearly independent and $\mathrm{Lin}(I) = \mathrm{VecSp}(K, E)$. $\square$

Let F be a field and E be an F-finite extension of F. One can check that every E-finite, F-extending extension of E is F-finite.

3. Algebraic Extensions

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

(Def. 11) every element of E is F-algebraic.

One can verify that every extension of F which is F-finite is also F-algebraic.

Let E be an F-algebraic extension of F. Note that every element of E is F-algebraic. Now we state the propositions:

(32) Let us consider a field F, and an extension E of F. Then E is F-algebraic if and only if for every element a of E, $\mathrm{FAdj}(F, \{a\})$ is F-finite.

(33) 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 there exists an F-finite extension B of F such that E is B-extending and $a \in B$.

Let F be a field, E be an extension of F, and T be a subset of E. We say that T is F-algebraic if and only if

(Def. 12) for every element a of E such that $a \in T$ holds a is F-algebraic.

One can verify that there exists a subset of E which is finite and F-algebraic.

Now we state the propositions:

(34) Let us consider a field F, an extension E of F, an element b of E, a subset T of E, an extension E_1 of $\mathrm{FAdj}(F, T)$, and an element b_1 of E_1. Suppose $E_1 = E$ and $b_1 = b$. Then $\mathrm{FAdj}(F, \{b\} \cup T) = \mathrm{FAdj}(\mathrm{FAdj}(F, T), \{b_1\})$.
Proof: $\{b\} \cup T \subseteq$ the carrier of $\mathrm{FAdj}(\mathrm{FAdj}(F, T), \{b_1\})$ by [6, (35),(36)]. $\mathrm{FAdj}(F, T)$ is a subfield of $\mathrm{FAdj}(F, \{b\} \cup T)$. □

(35) Let us consider a field F, an extension E of F, an element b of E, a subset T of E, an extension E_1 of $\mathrm{FAdj}(F, \{b\})$, and a subset T_1 of E_1. Suppose $E_1 = E$ and $T_1 = T$. Then $\mathrm{FAdj}(F, \{b\} \cup T) = \mathrm{FAdj}(\mathrm{FAdj}(F, \{b\}), T_1)$.
Proof: $\{b\} \cup T \subseteq$ the carrier of $\mathrm{FAdj}(\mathrm{FAdj}(F, \{b\}), T_1)$ by [6, (35),(36)]. $\mathrm{FAdj}(F, \{b\})$ is a subfield of $\mathrm{FAdj}(F, \{b\} \cup T)$. □

Let F be a field, E be an extension of F, and T be a finite, F-algebraic subset of E. One can verify that $\mathrm{FAdj}(F, T)$ is F-finite.

Now we state the propositions:

(36) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $E \approx \mathrm{FAdj}(F, \{a\})$ if and only if $\deg \mathrm{MinPoly}(a, F) = \deg(E, F)$. The theorem is a consequence of (5), (31), (30), and (8).

(37) Let us consider a field F, and an extension E of F. Then E is F-finite if and only if there exists a finite, F-algebraic subset T of E such that $E \approx \mathrm{FAdj}(F, T)$.
Proof: by induction on $\deg(E, F)$.

Let F be a field, E be an extension of F, and p be a non zero element of the carrier of PolyRing(F). Note that Roots(E, p) is F-algebraic.

Now we state the proposition:

(38) Let us consider a field F, an extension E of F, and a non zero element p of the carrier of PolyRing(F). Then FAdj(F, Roots(E, p)) is F-algebraic.

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

(39) If K is E-algebraic and E is F-algebraic, then K is F-algebraic. The theorem is a consequence of (12), (15), and (33).

(40) If K is F-algebraic, then K is E-algebraic and E is F-algebraic. The theorem is a consequence of (15).

4. The Field of Algebraic Elements

Let F be a field, E be an extension of F, and a, b be F-algebraic elements of E. Observe that FAdj(F, $\{a, b\}$) is F-finite and 0_E is F-algebraic and 1_E is F-algebraic.

Let a, b be F-algebraic elements of E. One can verify that $a+b$ is F-algebraic and $a-b$ is F-algebraic and $a \cdot b$ is F-algebraic.

Let a be an F-algebraic element of E. Let us note that $-a$ is F-algebraic.

Let a be a non zero, F-algebraic element of E. Let us observe that a^{-1} is F-algebraic.

The functor Alg-Elem(E) yielding a subset of E is defined by the term

(Def. 13) the set of all a where a is an F-algebraic element of E.

The functor Field-Alg-Elem(E) yielding a strict double loop structure is defined by

(Def. 14) the carrier of *it* = Alg-Elem(E) and the addition of *it* = (the addition of E) $\restriction$ (the carrier of *it*) and the multiplication of *it* = (the multiplication of E) $\restriction$ (the carrier of *it*) and the one of *it* = 1_E and the zero of *it* = 0_E.

We introduce the notation F-Alg(E) as a synonym of Field-Alg-Elem(E).

Observe that F-Alg(E) is non degenerated and F-Alg(E) is Abelian, add-associative, right zeroed, and right complementable and F-Alg(E) is commutative, associative, well unital, distributive, and almost left invertible and F-Alg(E) is F-extending and F-Alg(E) is F-algebraic. Now we state the propositions:

(41) Let us consider a field F, and an extension E of F. Then F-Alg(E) is an extension of F.

(42) Let us consider a field F, and an extension E of F. Then E is an extension of F-Alg(E).

(43) Let us consider a field F, an extension E of F, and an extension K of E. Then F-Alg(K) is an extension of F-Alg(E).

(44) Let us consider a field F, and an F-algebraic extension E of F. Then F-Alg(E) $\approx E$.

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

[5] Serge Lang. *Algebra.* Springer, 3rd edition, 2005.

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

Accepted March 30, 2021