FORMALIZED MATHEMATICS
Volume 31, 2023, Pages 121–130
DOI: 10.2478/forma-2023-0011
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Normal Extensions

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we continue the formalization of field theory in Mizar [1], [2], [4], [3]. We introduce normal extensions: an (algebraic) extension E of F is normal if every polynomial of F that has a root in E already splits in E. We proved characterizations (for finite extensions) by minimal polynomials [7], splitting fields, and fixing monomorphisms [6], [5]. This required extending results from [11] and [12], in particular that $F[T] = \{p(a_1, \dots a_n) \mid p \in F[X],\ a_i \in T\}$ and $F(T) = F[T]$ for finite algebraic $T \subseteq E$. We also provided the counterexample that $\mathcal{Q}(\sqrt[3]{2})$ is not normal over $\mathcal{Q}$ (compare [13]).

MSC: 12F05 68V20

Keywords: normal extension; fixing monomorphisms

MML identifier: FIELD_13, version: 8.1.12 5.75.1447

1. Preliminaries

Let Y be a non empty set and y_1, y_2, y_3 be elements of Y. Note that the functor $\{y_1, y_2, y_3\}$ yields a subset of Y. Let R be an integral domain and p, q be constant polynomials over R. Note that $p * q$ is constant. Let R be a ring. Note that every ring extension of R is R-homomorphic and R-monomorphic.

Let F be a field, p be a non constant element of the carrier of Polynom-Ring F, and E be a splitting field of p. Let us observe that Roots(E, p) is non empty. Let R be a ring, S be a ring extension of R, and T be a ring extension of S. One can check that there exists a homomorphism from S to T which is R-fixing and there exists a monomorphism of S and T which is R-fixing. Now we state the propositions:

(1) Let us consider a ring R, a subring S of R, a non empty finite sequence F of elements of the carrier of R, and a non empty finite sequence G of elements of the carrier of S. If $F = G$, then $\prod F = \prod G$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty finite sequence F of elements of the carrier of R for every non empty finite sequence G of elements of the carrier of S such that $\operatorname{len} F = \$_1$ and $F = G$ holds $\prod F = \prod G$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $n = \operatorname{len} F$. $\square$

(2) Let us consider a field F, and a non empty finite sequence G of elements of the carrier of Polynom-Ring F. Then $\prod G = \mathbf{0}.F$ if and only if there exists an element i of $\operatorname{dom} G$ such that $G(i) = \mathbf{0}.F$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every non empty finite sequence G of elements of the carrier of Polynom-Ring F such that $\operatorname{len} G = \$_1$ and for every element i of $\operatorname{dom} G$, $G(i) \neq \mathbf{0}.F$ holds $\prod G \neq \mathbf{0}.F$. $\mathcal{P}[1]$. For every natural number k such that $k \geqslant 1$ holds $\mathcal{P}[k]$. $\square$

(3) Let us consider a field F, and a non empty finite sequence G of elements of the carrier of Polynom-Ring F. Suppose for every element i of $\operatorname{dom} G$, $G(i) \neq \mathbf{0}.F$. Let us consider a polynomial q over F. Suppose $q = \prod G$. Let us consider an element i of $\operatorname{dom} G$, and a polynomial p over F. If $p = G(i)$, then $\deg(p) \leqslant \deg(q)$. The theorem is a consequence of (2).

(4) Let us consider a field F, an extension E of F, a non empty finite sequence G of elements of the carrier of Polynom-Ring F, and a polynomial q over F. Suppose $q = \prod G$. Let us consider an element a of E. Suppose there exists an element i of $\operatorname{dom} G$ and there exists a polynomial p over F such that $p = G(i)$ and $\operatorname{ExtEval}(p, a) = 0_E$. Then $\operatorname{ExtEval}(q, a) = 0_E$.

(5) Let us consider a field F, a non empty finite sequence G of elements of the carrier of Polynom-Ring F, and a non constant polynomial q over F. Suppose $q = \prod G$. Then q splits in F if and only if for every element i of $\operatorname{dom} G$ and for every polynomial p over F such that $p = G(i)$ holds p is constant or p splits in F.

(6) Let us consider a field F, an extension E of F, a non empty finite sequence G of elements of the carrier of Polynom-Ring F, and a non constant polynomial q over F. Suppose $q = \prod G$. Then q splits in E if and only if for every element i of $\operatorname{dom} G$ and for every polynomial p over F such that $p = G(i)$ holds p is constant or p splits in E. The theorem is a consequence of (1) and (5).

(7) Let us consider a field F, an extension E of F, a non constant polynomial p over F, and a non zero polynomial q over F. If $p * q$ splits in E, then p splits in E.

(8) Let us consider a natural number n, a field F, an extension E of F, a polynomial p of n,F, and a polynomial q of n,E. If $p = q$, then $\operatorname{Support} q = \operatorname{Support} p$.

(9) Let us consider a natural number n, a field F, an extension E of F, a polynomial p of n,F, a polynomial q of n,E, and a function x from n into E. If $p = q$, then $\operatorname{ExtEval}(p, x) = \operatorname{eval}(q, x)$.
Proof: Consider F_3 being a finite sequence of elements of the carrier of S such that $\operatorname{ExtEval}(p, x) = \sum F_3$ and $\operatorname{len} F_3 = \operatorname{len} \operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p)$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} F_3$ holds $F_3(i) = (p \cdot (\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))i)(\in S) \cdot (\operatorname{eval}((\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} p))_{/i}, x))$. Consider F_4 being a finite sequence of elements of the carrier of S such that $\operatorname{len} F_4 = \operatorname{len} \operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} q)$ and $\operatorname{eval}(q, x) = \sum F_4$ and for every element i of $\mathbb{N}$ such that $1 \leqslant i \leqslant \operatorname{len} F_4$ holds $F_{4/i} = q \cdot (\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} q))_{/i} \cdot (\operatorname{eval}((\operatorname{SgmX}(\operatorname{BagOrder} n, \operatorname{Support} q))_{/i}, x))$. For every natural number i such that $i \in \operatorname{dom} F_3$ holds $F_4(i) = F_3(i)$. $\square$

(10) Let us consider a natural number n, a field F, an extension E of F, an element a of F, and an element b of E. If $a = b$, then $a \restriction (n, F) = b \restriction (n, E)$.

(11) Let us consider a field F, an extension E_1 of F, and a field E_2. If $E_1 \approx E_2$, then E_2 is an extension of F.

(12) Let us consider fields F_1, F_2, and a product of linear polynomials p of F_1. If $F_1 \approx F_2$, then p is a product of linear polynomials of F_2.

(13) Let us consider a field F, an extension E of F, a polynomial p over F, a polynomial q over E, an element a of F, and an element b of E. If $p = q$ and $a = b$, then $a \cdot p = b \cdot q$.

(14) Let us consider fields F_1, F_2, a polynomial p over F_1, an element a of F_1, a polynomial q over F_2, and an element b of F_2. If $F_1 \approx F_2$, then if $p = q$ and $a = b$, then $a \cdot p = b \cdot q$. The theorem is a consequence of (13).

(15) Let us consider a field F, extensions E_1, E_2 of F, and a polynomial p over F. If $E_1 \approx E_2$, then if p splits in E_1, then p splits in E_2. The theorem is a consequence of (12) and (14).

(16) Let us consider a field F, extensions E_1, E_2 of F, and a non constant element p of the carrier of Polynom-Ring F. Suppose $E_1 \approx E_2$. If E_1 is a splitting field of p, then E_2 is a splitting field of p. The theorem is a consequence of (11) and (15).

(17) Let us consider a field F, and a linear element p of the carrier of Polynom-Ring F. Then F is a splitting field of p.

Let F be a field and E be an extension of F. Let us observe that there exists a subset of E which is non empty, finite, and F-algebraic. Let a be an F-algebraic element of E. Let us observe that $\{a\}$ is F-algebraic as a subset of E.

Let T_1, T_2 be F-algebraic subsets of E. One can verify that $T_1 \cup T_2$ is F-algebraic as a subset of E. Let T_1 be an F-algebraic subset of E and T_2 be a subset of E. Let us observe that $T_1 \cap T_2$ is F-algebraic as a subset of E and $T_1 \setminus T_2$ is F-algebraic as a subset of E. Let T be a non empty, F-algebraic subset of E.

Note that an element of T is an element of E. Let us note that every element of T is F-algebraic. Let E_1, E_2 be extensions of F, h be a function from E_1 into E_2, and T be a subset of E_1. Observe that the functor $h^\circ T$ yields a subset of E_2. Now we state the propositions:

(18) Let us consider a field F, an extension E of F, a subset T_1 of E, a subset T_2 of E, an extension E_1 of $\mathrm{FAdj}(F, T_2)$, and a subset T_3 of E_1. Suppose $E_1 = E$ and $T_1 = T_3$. Then $\mathrm{FAdj}(F, T_1 \cup T_2) = \mathrm{FAdj}(\mathrm{FAdj}(F, T_2), T_3)$.
PROOF: $T_1 \cup T_2 \subseteq$ the carrier of $\mathrm{FAdj}(\mathrm{FAdj}(F, T_2), T_3)$. □

(19) Let us consider a field F, an extension E of F, an E-extending extension K of F, a finite, F-algebraic subset T_1 of E, and a subset T_2 of K. If $T_1 = T_2$, then $\mathrm{FAdj}(F, T_1) = \mathrm{FAdj}(F, T_2)$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite, F-algebraic subset T_1 of E for every subset T_2 of K such that $\overline{\overline{T_1}} = \$_1$ and $T_1 = T_2$ holds $\mathrm{FAdj}(F, T_1) = \mathrm{FAdj}(F, T_2)$. $\mathcal{P}[0]$ by [14, (3)]. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{T_1}} = n$. □

(20) Let us consider fields F_1, F_2, an element p_1 of the carrier of Polynom-Ring F_1, an element p_2 of the carrier of Polynom-Ring F_2, an extension E_1 of F_1, and an extension E_2 of F_2. Suppose $E_1 = E_2$ and $p_1 = p_2$. Then $\mathrm{Roots}(E_1, p_1) = \mathrm{Roots}(E_2, p_2)$.

(21) Let us consider a field F, extensions E, K of F, an extension U_1 of E, an extension U_2 of K, a subset T_1 of U_1, and a subset T_2 of U_2. Suppose $U_1 = U_2$ and $T_1 = T_2$ and $E \approx K$. Then $\mathrm{FAdj}(E, T_1) = \mathrm{FAdj}(K, T_2)$.
PROOF: $\mathrm{FAdj}(E, T_1)$ is a subfield of $\mathrm{FAdj}(K, T_2)$. $\mathrm{FAdj}(K, T_2)$ is a subfield of $\mathrm{FAdj}(E, T_1)$ by [9, (37)], [10, (7)], [11, (35),(37)]. □

(22) Let us consider a field F, an extension E of F, an E-extending extension K of F, a subset T_1 of K, and a finite subset T_2 of K. Suppose $T_1 \subseteq T_2$ and $E \approx \mathrm{FAdj}(F, T_1)$. Then $\mathrm{FAdj}(E, T_2) = \mathrm{FAdj}(F, T_2)$. The theorem is a consequence of (21) and (18).

(23) Let us consider a field F_1, a non constant element p_1 of the carrier of Polynom-Ring F_1, an extension F_2 of F_1, a non constant element p_2 of the carrier of Polynom-Ring F_2, a splitting field E of p_2, and an F_1-algebraic subset T of F_2. Suppose $T \subseteq \mathrm{Roots}(E, p_2)$ and $F_2 \approx \mathrm{FAdj}(F_1, T)$.

If $p_1 = p_2$, then E is a splitting field of p_1. The theorem is a consequence of (19).

(24) Let us consider a field F, an extension E of F, an F-extending extension K of E, and a non constant element p of the carrier of Polynom-Ring F. If p splits in E, then $\mathrm{Roots}(K, p) = \mathrm{Roots}(E, p)$.

(25) Let us consider a field F_1, an F_1-homomorphic field F_2, a homomorphism h from F_1 to F_2, and an element a of F_1. Then $(\mathrm{PolyHom}(h))(\mathrm{X}- a) = \mathrm{X}- h(a)$.

(26) Let us consider a field F_1, an F_1-isomorphic, F_1-homomorphic field F_2, an isomorphism h between F_1 and F_2, an extension E_1 of F_1, an extension E_2 of F_2, an element a of E_1, an element b of E_2, and an irreducible element p of the carrier of Polynom-Ring F_1. Suppose $\mathrm{ExtEval}(p, a) = 0_{E_1}$ and $\mathrm{ExtEval}((\mathrm{PolyHom}(h))(p), b) = 0_{E_2}$. Then $(\Psi(a, b, h, p))(a) = b$. The theorem is a consequence of (25).

2. Preliminaries about Ring Adjunctions

Let R_1, R_2 be rings. One can check that $R_1 \approx R_2$ if and only if the condition (Def. 1) is satisfied.

(Def. 1) R_1 is a subring of R_2 and R_2 is a subring of R_1.

Now we state the propositions:

(27) Let us consider a ring R. Then $R \approx R$.

(28) Let us consider rings R_1, R_2. If $R_1 \approx R_2$, then $R_2 \approx R_1$.

(29) Let us consider rings R_1, R_2, R_3. If $R_1 \approx R_2$ and $R_2 \approx R_3$, then $R_1 \approx R_3$.

(30) Let us consider a ring R, a ring extension S of R, and subsets T_1, T_2 of S. Suppose $T_1 \subseteq T_2$. Then $\mathrm{RAdj}(R, T_1)$ is a subring of $\mathrm{RAdj}(R, T_2)$.

(31) Let us consider a ring R, a ring extension S of R, subsets T_1, T_2 of S, a ring extension S_1 of $\mathrm{RAdj}(R, T_2)$, and a subset T_3 of S_1. Suppose $S_1 = S$ and $T_1 = T_3$. Then $\mathrm{RAdj}(R, T_1 \cup T_2) = \mathrm{RAdj}(\mathrm{RAdj}(R, T_2), T_3)$.
Proof: $T_1 \cup T_2 \subseteq$ the carrier of $\mathrm{RAdj}(\mathrm{RAdj}(F, T_2), T_3)$. $\mathrm{RAdj}(F, T_2)$ is a subring of $\mathrm{RAdj}(F, T_1 \cup T_2)$. $\square$

(32) Let us consider a ring R, a ring extension S of R, and a subset T of S. Then $\mathrm{RAdj}(R, T) \approx R$ if and only if T is a subset of R.

Let n be a natural number, R, S be non degenerated commutative rings, and x be a function from n into S. The functor $\mathrm{HomExtEval}(x, R)$ yielding a function from $\mathrm{Polynom\text{-}Ring}(n, R)$ into S is defined by

(Def. 2) for every polynomial p of n,R, $it(p) = \mathrm{ExtEval}(p, x)$.

Let R be a non degenerated commutative ring and S be a commutative ring extension of R. Let us observe that $\mathrm{HomExtEval}(x, R)$ is additive, multiplicative, and unity-preserving. Now we state the proposition:

(33) Let us consider a natural number n, and a field F. Then every extension of F is $(\text{Polynom-Ring}(n, F))$-homomorphic.

Let n be a natural number and F be a field. One can check that there exists an extension of F which is $(\text{Polynom-Ring}(n, F))$-homomorphic. Now we state the proposition:

(34) Let us consider a natural number n, fields F, E, and a function x from n into E. Then $\operatorname{rng} \mathrm{HomExtEval}(x, F) =$ the set of all $\mathrm{ExtEval}(p, x)$ where p is a polynomial of n,F.

Let n be a natural number, F be a field, E be an extension of F, and x be a function from n into E. The functor $\mathrm{ImageHomExtEval}(x, F)$ yielding a strict double loop structure is defined by

(Def. 3) the carrier of $it = \operatorname{rng} \mathrm{HomExtEval}(x, F)$ and the addition of $it =$ (the addition of E) $\restriction \operatorname{rng} \mathrm{HomExtEval}(x, F)$ and the multiplication of $it =$ (the multiplication of E) $\restriction \operatorname{rng} \mathrm{HomExtEval}(x, F)$ and the one of $it = 1_E$ and the zero of $it = 0_E$.

One can check that $\mathrm{ImageHomExtEval}(x, F)$ is non degenerated and $\mathrm{ImageHomExtEval}(x, F)$ is Abelian, add-associative, right zeroed, and right complementable and $\mathrm{ImageHomExtEval}(x, F)$ is commutative, associative, well unital, and distributive. Now we state the proposition:

(35) Let us consider a natural number n, a field F, an extension E of F, and a function x from n into E. Then F is a subring of $\mathrm{ImageHomExtEval}(x, F)$. The theorem is a consequence of (10), (9), and (34).

Let F be a field, T be a finite subset of F, and x be a function from $\overline{\overline{T}}$ into F. We say that x is T-evaluating if and only if

(Def. 4) x is one-to-one and $\operatorname{rng} x = T$.

Let us note that there exists a function from $\overline{\overline{T}}$ into F which is T-evaluating and every function from $\overline{\overline{T}}$ into F which is T-evaluating is also T-valued and one-to-one. Now we state the propositions:

(36) Let us consider a field F, an extension E of F, a non empty, finite subset T of E, a bag b of $\overline{\overline{T}}$, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then $\mathrm{eval}(b, x) \in$ the carrier of $\mathrm{RAdj}(F, T)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every bag b of $\overline{\overline{T}}$ such that $\overline{\overline{\operatorname{support} b}} = \$_1$ for every T-evaluating function x from $\overline{\overline{T}}$ into E, $\mathrm{eval}(b, x) \in$ the carrier of $\mathrm{RAdj}(F, T)$. Set $n = \overline{\overline{T}}$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\operatorname{support} b}} = n$. $\square$

(37) Let us consider a field F, an extension E of F, a non empty, finite subset T of E, a polynomial p of $\overline{\overline{T}}$,F, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then $\mathrm{ExtEval}(p,x) \in$ the carrier of $\mathrm{RAdj}(F,T)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every polynomial p of $\overline{\overline{T}}$,F such that $\overline{\overline{\mathrm{Support}\,p}} = \$_1$ holds $\mathrm{ExtEval}(p,x) \in$ the carrier of $\mathrm{RAdj}(F,T)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. $\square$

Let us consider a field F, an extension E of F, a non empty, finite subset T of E, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Now we state the propositions:

(38) $\mathrm{RAdj}(F,T) = \mathrm{ImageHomExtEval}(x,F)$. The theorem is a consequence of (35).

(39) The carrier of $\mathrm{RAdj}(F,T) =$ the set of all $\mathrm{ExtEval}(p,x)$ where p is a polynomial of $\overline{\overline{T}}$,F. The theorem is a consequence of (38) and (34).

(40) Let us consider a field F, an extension E of F, and a finite subset T of E. If T is F-algebraic, then $\mathrm{FAdj}(F,T) = \mathrm{RAdj}(F,T)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every field F for every extension E of F for every finite subset T of E such that $\overline{\overline{T}} = \$_1$ holds if T is F-algebraic, then $\mathrm{FAdj}(F,T) = \mathrm{RAdj}(F,T)$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{T}} = n$. $\square$

3. On Fixing Monomorphisms

Let R be a ring and S be a ring extension of R. Note that there exists a homomorphism of S which is R-fixing and there exists a monomorphism of S which is R-fixing and there exists an automorphism of S which is R-fixing. Now we state the propositions:

(41) Let us consider a field F, an extension E of F, an extension K of E, an element p of the carrier of Polynom-Ring F, and an F-fixing homomorphism h from E to K. Then $(\mathrm{PolyHom}(h))(p) = p$.

(42) Let us consider a field F, an extension E of F, an extension K of E, an element p of the carrier of Polynom-Ring F, an element a of E, and an F-fixing homomorphism h from E to K. Then $h(\mathrm{ExtEval}(p,a)) = \mathrm{ExtEval}(p,h(a))$. The theorem is a consequence of (41).

(43) Let us consider a field F, an extension E of F, an F-fixing monomorphism h of E, and a non zero element p of the carrier of Polynom-Ring F. Then $h^{\circ}(\mathrm{Roots}(E,p)) = \mathrm{Roots}(E,p)$.

(44) Let us consider a field F, an F-algebraic extension E of F, and an F-fixing monomorphism h of E. Then the carrier of $E \subseteq \mathrm{rng}\,h$. The theorem

is a consequence of (43).

(45) Let us consider a field F, and an F-algebraic extension E of F. Then every F-fixing monomorphism of E is an automorphism of E. The theorem is a consequence of (44).

Let F be a field and E be an F-algebraic extension of F. Let us observe that every F-fixing monomorphism of E is isomorphism. Now we state the propositions:

(46) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and an F-algebraic subset T of E. Then $h^{\circ}T$ is F-algebraic. The theorem is a consequence of (42).

(47) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, a non empty, finite subset T of E, a bag b of $\overline{\overline{T}}$, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then $h(\mathrm{eval}(b, x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every bag b of $\overline{\overline{T}}$ such that $\overline{\overline{\operatorname{support} b}} = \$_1$ for every T-evaluating function x from $\overline{\overline{T}}$ into E, $h(\mathrm{eval}(b,$ $x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$. Set $n = \overline{\overline{T}}$. $\mathcal{P}[0]$. For every natural number k, $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{\overline{\operatorname{support} b}} = n$. $\square$

(48) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, a non empty, finite subset T of E, a polynomial p of $\overline{\overline{T}}$,F, and a T-evaluating function x from $\overline{\overline{T}}$ into E. Then $h(\mathrm{ExtEval}(p, x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every polynomial p of $\overline{\overline{T}}$,F such that $\overline{\overline{\operatorname{Support} p}} = \$_1$ holds $h(\mathrm{ExtEval}(p, x)) \in$ the carrier of $\mathrm{RAdj}(F, h^{\circ}T)$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\mathcal{P}[0]$ by [8, (5), (16)]. For every natural number k, $\mathcal{P}[k]$. $\square$

(49) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and a non empty, finite, F-algebraic subset T of E. Then h°(the carrier of $\mathrm{FAdj}(F, T)) \subseteq$ the carrier of $\mathrm{FAdj}(F, h^{\circ}T)$. The theorem is a consequence of (46), (40), and (48).

(50) Let us consider a field F, an extension E of F, an E-extending extension K of F, and a finite, F-algebraic subset T of K. Suppose $T \subseteq$ the carrier of E. Then $\mathrm{FAdj}(F, T)$ is a subfield of E. The theorem is a consequence of (19).

(51) Let us consider a field F, an extension E of F, an E-extending extension

K of F, an F-fixing homomorphism h from E to (K **qua** extension of E), and a finite, F-algebraic subset T of E. Suppose $h^\circ T \subseteq$ the carrier of E. Then FAdj$(F, h^\circ T)$ is a subfield of E. The theorem is a consequence of (42) and (19).

(52) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and a non empty, finite, F-algebraic subset T of E. Suppose $h^\circ T \subseteq$ the carrier of E. Then h°(the carrier of FAdj$(F, T)) \subseteq$ the carrier of E. The theorem is a consequence of (51) and (49).

(53) Let us consider a field F, an extension E of F, an F-extending extension K of E, an F-fixing monomorphism h of E and K, and a non constant element p of the carrier of Polynom-Ring F. Suppose p splits in E. Then $h^\circ(\mathrm{Roots}(E, p)) \subseteq$ the carrier of E. The theorem is a consequence of (42) and (24).

4. Normal Extensions

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

(Def. 5) E is F-algebraic and for every irreducible element p of the carrier of Polynom-Ring F such that p has a root in E holds p splits in E.

Let us observe that every extension of F which is F-normal is also F-algebraic and every extension of F which is F-quadratic is also F-normal and every algebraic closure of F is F-normal and there exists an extension of F which is F-algebraic and F-normal and FAdj$(\mathbb{F}_{\mathbb{Q}}, \{\sqrt[3]{2}\})$ is non $(\mathbb{F}_{\mathbb{Q}})$-normal. Now we state the proposition:

(54) Let us consider a field F, and an F-algebraic extension E of F. Then E is F-normal if and only if for every element a of E, MinPoly(a, F) splits in E.

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

(55) E is F-normal if and only if there exists a non constant element p of the carrier of Polynom-Ring F such that E is a splitting field of p.

(56) E is F-normal if and only if for every extension K of E, every F-fixing monomorphism of E and K is an automorphism of E.

Let F be a field and p be a non constant element of the carrier of Polynom-Ring F. One can verify that every splitting field of p is F-normal. Now we state the propositions:

(57) Let us consider a field F, an extension E of F, and an F-algebraic element a of E. Then $\mathrm{FAdj}(F, \{a\})$ is F-normal if and only if $\mathrm{MinPoly}(a, F)$ splits in $\mathrm{FAdj}(F, \{a\})$.

(58) Let us consider a field F, an extension E of F, and a non empty, finite, F-algebraic subset T of E. Then $\mathrm{FAdj}(F, T)$ is F-normal if and only if for every element a of T, $\mathrm{MinPoly}(a, F)$ splits in $\mathrm{FAdj}(F, T)$. The theorem is a consequence of (3), (6), and (4).

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

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

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

[7] 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.

[8] Christoph Schwarzweller. Artin's theorem towards the existence of algebraic closures. *Formalized Mathematics*, 30(**3**):199–207, 2022. doi:10.2478/forma-2022-0014.

[9] Christoph Schwarzweller. Existence and uniqueness of algebraic closures. *Formalized Mathematics*, 30(**4**):281–294, 2022. doi:10.2478/forma-2022-0022.

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

[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 and Sara Burgoa. Splitting fields for the rational polynomials x^2-2, x^2+x+1, x^3-1, and x^3-2. *Formalized Mathematics*, 30(**1**):23–30, 2022. doi:10.2478/forma-2022-0003.

[14] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Algebraic extensions. *Formalized Mathematics*, 29(**1**):39–48, 2021. doi:10.2478/forma-2021-0004.

Accepted June 30, 2023