Splitting Fields

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. In this article we further develop field theory in Mizar [1], [2]: we prove existence and uniqueness of splitting fields. We define the splitting field of a polynomial $p \in F[X]$ as the smallest field extension of F , in which p splits into linear factors. From this follows, that for a splitting field E of p we have $E = F(A)$ where A is the set of p 's roots. Splitting fields are unique, however, only up to isomorphisms; to be more precise up to F -isomorphisms i.e. isomorphisms i with $i|_F = \text{Id}_F$. We prove that two splitting fields of $p \in F[X]$ are F -isomorphic using the well-known technique [4], [3] of extending isomorphisms from $F_1 \longrightarrow F_2$ to $F_1(a) \longrightarrow F_2(b)$ for a and b being algebraic over F_1 and F_2 , respectively.

MSC: 12F05 68V20

Keywords: field extensions; polynomials splitting fields

MML identifier: FIELD_8, version: 8.1.11 5.66.1402

1. PRELIMINARIES

Now we state the propositions:

- (1) Let us consider a ring R , a polynomial p over R , and an element q of the carrier of $\text{PolyRing}(R)$. If $p = q$, then $-p = -q$.
- (2) Let us consider a ring R , a polynomial p over R , and an element a of R . Then $a \cdot p = (a \upharpoonright R) * p$.
- (3) Let us consider a ring R , and an element a of R . Then $\text{LC}(a \upharpoonright R) = a$.
- (4) Let us consider a ring R , a subring S of R , a finite sequence F of elements of R , and a finite sequence G of elements of S . If $F = G$, then $\prod F = \prod G$.

Let F be a field. Let us observe that there exists a field which is F -homomorphic, F -monomorphic, and F -isomorphic.

Let R be a ring. Observe that every R -isomorphic ring is R -homomorphic and R -monomorphic.

Let S be an R -homomorphic ring.

Observe that $\text{PolyRing}(S)$ is $(\text{PolyRing}(R))$ -homomorphic.

Let F_1 be a field and F_2 be an F_1 -isomorphic, F_1 -homomorphic field. Observe that $\text{PolyRing}(F_2)$ is $(\text{PolyRing}(F_1))$ -isomorphic.

2. MORE ON POLYNOMIALS

Now we state the propositions:

- (5) Let us consider a non degenerated ring R , a ring extension S of R , a polynomial p over R , and a polynomial q over S . If $p = q$, then $\text{LC } p = \text{LC } q$.
- (6) Let us consider a field F , an element p of the carrier of $\text{PolyRing}(F)$, an extension E of F , and an element q of the carrier of $\text{PolyRing}(E)$. Suppose $p = q$. Let us consider an E -extending extension U of F , and an element a of U . Then $\text{ExtEval}(q, a) = \text{ExtEval}(p, a)$.
- (7) Let us consider a ring R , a ring extension S of R , an element p of the carrier of $\text{PolyRing}(R)$, and an element q of the carrier of $\text{PolyRing}(S)$. Suppose $p = q$. Let us consider a ring extension T_1 of S , and a ring extension T_2 of R . If $T_1 = T_2$, then $\text{Roots}(T_2, p) = \text{Roots}(T_1, q)$.
- (8) Let us consider an integral domain R , a non empty finite sequence F of elements of $\text{PolyRing}(R)$, and a polynomial p over R . Suppose $p = \prod F$ and for every natural number i such that $i \in \text{dom } F$ there exists an element a of R such that $F(i) = \text{rpoly}(1, a)$. Then $\deg p = \text{len } F$.
 PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non empty finite sequence F of elements of $\text{PolyRing}(R)$ for every polynomial p over R such that $\text{len } F = \$_1$ and $p = \prod F$ and for every natural number i such that $i \in \text{dom } F$ there exists an element a of R such that $F(i) = \text{rpoly}(1, a)$ holds $\deg p = \text{len } F$. For every natural number k , $\mathcal{P}[k]$. $\square$
- (9) Let us consider a field F , a polynomial p over F , and a non zero element a of F . Then $a \cdot p$ splits in F if and only if p splits in F .
- (10) Let us consider a field F , a non constant, monic polynomial p over F , and a non zero polynomial q over F . Suppose $p * q$ is a product of linear polynomials of F . Then p is a product of linear polynomials of F .
 PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non constant, monic polynomial p over F for every non zero polynomial q over F such that

$\deg(p * q) = \$_1$ and $p * q$ is a product of linear polynomials of F holds p is a product of linear polynomials of F . For every natural number i such that $1 \leq i$ holds $\mathcal{P}[i]$. $\square$

- (11) Let us consider a field F , a non constant polynomial p over F , and a non zero polynomial q over F . If $p * q$ splits in F , then p splits in F . The theorem is a consequence of (10) and (9).
- (12) Let us consider a field F , and polynomials p, q over F . If p splits in F and q splits in F , then $p * q$ splits in F .
- (13) Let us consider a ring R , an R -homomorphic ring S , a homomorphism h from R to S , and an element a of R . Then $(\text{PolyHom}(h))(a \downarrow R) = h(a) \downarrow S$.
- (14) 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 , and elements p, q of the carrier of $\text{PolyRing}(F_1)$. Then $p \mid q$ if and only if $(\text{PolyHom}(h))(p) \mid (\text{PolyHom}(h))(q)$.
- (15) Let us consider a field F , an extension E of F , an F -algebraic element a of E , and an irreducible element p of the carrier of $\text{PolyRing}(F)$. Suppose $\text{ExtEval}(p, a) = 0_E$. Then $\text{MinPoly}(a, F) = \text{NormPoly } p$.
- (16) Let us consider a field F_1 , an F_1 -monomorphic, F_1 -homomorphic field F_2 , a monomorphism h of F_1 and F_2 , and an element p of the carrier of $\text{PolyRing}(F_1)$. Then $\text{NormPoly}(\text{PolyHom}(h))(p) = (\text{PolyHom}(h))(\text{NormPoly } p)$.

Let F_1 be a field, F_2 be an F_1 -isomorphic, F_1 -homomorphic field, h be an isomorphism between F_1 and F_2 , and p be a constant element of the carrier of $\text{PolyRing}(F_1)$. One can check that $(\text{PolyHom}(h))(p)$ is constant as an element of the carrier of $\text{PolyRing}(F_2)$.

Let p be a non constant element of the carrier of $\text{PolyRing}(F_1)$. Note that $(\text{PolyHom}(h))(p)$ is non constant as an element of the carrier of $\text{PolyRing}(F_2)$.

Let p be an irreducible element of the carrier of $\text{PolyRing}(F_1)$. Let us note that $(\text{PolyHom}(h))(p)$ is irreducible as an element of the carrier of $\text{PolyRing}(F_2)$.

Now we state the propositions:

- (17) Let us consider a field F_1 , a non constant element p of the carrier of $\text{PolyRing}(F_1)$, an F_1 -isomorphic field F_2 , and an isomorphism h between F_1 and F_2 . Then p splits in F_1 if and only if $(\text{PolyHom}(h))(p)$ splits in F_2 .
- (18) Let us consider a field F , an element p of the carrier of $\text{PolyRing}(F)$, an extension E of F , and an E -extending extension U of F . Then $\text{Roots}(E, p) \subseteq \text{Roots}(U, p)$.
- (19) Let us consider a field F , a non constant element p of the carrier of $\text{PolyRing}(F)$, an extension E of F , and an extension U of E . If p splits in E , then p splits in U . The theorem is a consequence of (2).

3. MORE ON PRODUCTS OF LINEAR POLYNOMIALS

Now we state the propositions:

- (20) Let us consider a field F , and a non empty finite sequence G of elements of the carrier of $\text{PolyRing}(F)$. Suppose for every natural number i such that $i \in \text{dom } G$ there exists an element a of F such that $G(i) = \text{rpoly}(1, a)$. Then G is a factorization of $\prod G$.
- (21) Let us consider a field F , and non empty finite sequences G_1, G_2 of elements of $\text{PolyRing}(F)$. Suppose for every natural number i such that $i \in \text{dom } G_1$ there exists an element a of F such that $G_1(i) = \text{rpoly}(1, a)$ and for every natural number i such that $i \in \text{dom } G_2$ there exists an element a of F such that $G_2(i) = \text{rpoly}(1, a)$ and $\prod G_1 = \prod G_2$. Let us consider an element a of F . Then there exists a natural number i such that $i \in \text{dom } G_1$ and $G_1(i) = \text{rpoly}(1, a)$ if and only if there exists a natural number i such that $i \in \text{dom } G_2$ and $G_2(i) = \text{rpoly}(1, a)$. The theorem is a consequence of (20).
- (22) Let us consider a field F , an extension E of F , and a non empty finite sequence G_1 of elements of $\text{PolyRing}(F)$. Suppose for every natural number i such that $i \in \text{dom } G_1$ there exists an element a of F such that $G_1(i) = \text{rpoly}(1, a)$.
 Let us consider a non empty finite sequence G_2 of elements of $\text{PolyRing}(E)$. Suppose for every natural number i such that $i \in \text{dom } G_2$ there exists an element a of E such that $G_2(i) = \text{rpoly}(1, a)$. Suppose $\prod G_1 = \prod G_2$.
 Let us consider an element a of E . Then there exists a natural number i such that $i \in \text{dom } G_1$ and $G_1(i) = \text{rpoly}(1, a)$ if and only if there exists a natural number i such that $i \in \text{dom } G_2$ and $G_2(i) = \text{rpoly}(1, a)$. The theorem is a consequence of (4) and (21).
- (23) Let us consider a field F , a product of linear polynomials p of F , and an element a of F . Then $\text{LC } a \cdot p = a$.
- (24) Let us consider a field F , and an extension E of F . Then every product of linear polynomials of F is a product of linear polynomials of E .
- (25) Let us consider a field F , an extension E of F , a non zero element a of F , a non zero element b of E , a product of linear polynomials p of F , and a product of linear polynomials q of E . If $a \cdot p = b \cdot q$, then $a = b$ and $p = q$. The theorem is a consequence of (5) and (2).
- (26) Let us consider a field F , an extension E of F , and a non empty finite sequence G of elements of the carrier of $\text{PolyRing}(E)$. Suppose for every natural number i such that $i \in \text{dom } G$ there exists an element a of F such that $G(i) = \text{rpoly}(1, a)$. Then $\prod G$ is a product of linear polynomials of F .

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every non empty finite sequence G of elements of $\text{PolyRing}(E)$ such that $\text{len } G = \$_1$ and for every natural number i such that $i \in \text{dom } G$ there exists an element a of F such that $G(i) = \text{rpoly}(1, a)$ holds $\prod G$ is a product of linear polynomials of F . For every natural number k , $\mathcal{P}[k]$. Consider n being a natural number such that $\text{len } G = n$. $\square$

4. EXISTENCE OF SPLITTING FIELDS

Let us consider a field F , a non constant element p of the carrier of $\text{PolyRing}(F)$, an extension U of F , and a U -extending extension E of F . Now we state the propositions:

- (27) If p splits in E , then p splits in U iff $\text{Roots}(E, p) \subseteq \text{the carrier of } U$.
- (28) If p splits in E , then p splits in U iff $\text{Roots}(E, p) \subseteq \text{Roots}(U, p)$. The theorem is a consequence of (27).
- (29) If p splits in E , then p splits in U iff $\text{Roots}(E, p) = \text{Roots}(U, p)$. The theorem is a consequence of (28) and (18).
- (30) Let us consider a field F , a non constant element p of the carrier of $\text{PolyRing}(F)$, and an extension E of F . If p splits in E , then p splits in $\text{FAdj}(F, \text{Roots}(E, p))$. The theorem is a consequence of (27).

Let F be a field and p be a non constant element of the carrier of $\text{PolyRing}(F)$.

A splitting field of p is an extension of F defined by

- (Def. 1) p splits in it and for every extension E of F such that p splits in E and E is a subfield of it holds $E \approx it$.

Let us consider a field F and a non constant element p of the carrier of $\text{PolyRing}(F)$. Now we state the propositions:

- (31) There exists an extension E of F such that E is a splitting field of p .
- (32) There exists an extension E of F such that $\text{FAdj}(F, \text{Roots}(E, p))$ is a splitting field of p . The theorem is a consequence of (30), (18), and (28).
- (33) Let us consider a field F , a non constant element p of the carrier of $\text{PolyRing}(F)$, and an extension E of F . Suppose p splits in E . Then $\text{FAdj}(F, \text{Roots}(E, p))$ is a splitting field of p . The theorem is a consequence of (30), (18), and (28).
- (34) Let us consider a field F , a non constant element p of the carrier of $\text{PolyRing}(F)$, and a splitting field E of p . Then $E \approx \text{FAdj}(F, \text{Roots}(E, p))$. The theorem is a consequence of (33).

Let F be a field and p be a non constant element of the carrier of $\text{PolyRing}(F)$. Let us observe that there exists a splitting field of p which is strict and every splitting field of p is F -finite.

5. FIXING AND EXTENDING AUTOMORPHISMS

Let R be a ring. Let us observe that there exists a function from R into R which is isomorphism.

A homomorphism of R is an additive, multiplicative, unity-preserving function from R into R .

A monomorphism of R is a monomorphic function from R into R .

An automorphism of R is an isomorphism function from R into R . Let R, S_2 be rings, S_1 be a ring extension of R , and h be a function from S_1 into S_2 . We say that h is R -fixing if and only if

(Def. 2) for every element a of R , $h(a) = a$.

Now we state the propositions:

(35) Let us consider rings R, S_2 , a ring extension S_1 of R , and a function h from S_1 into S_2 . Then h is R -fixing if and only if $h|_R = \text{id}_R$.

(36) Let us consider a field F , an extension E_1 of F , an E_1 -homomorphic extension E_2 of F , and a homomorphism h from E_1 to E_2 . Then h is F -fixing if and only if h is a linear transformation from $\text{VecSp}(E_1, F)$ to $\text{VecSp}(E_2, F)$.

(37) Let us consider a field F , an extension E of F , an E -extending extension E_1 of F , an E -extending extension E_2 of F , and a function h from E_1 into E_2 . If h is E -fixing, then h is F -fixing.

Let R be a ring, S_1, S_2 be ring extensions of R , and h be a function from S_1 into S_2 . We say that h is R -homomorphism if and only if

(Def. 3) h is R -fixing, additive, multiplicative, and unity-preserving.

We say that h is R -monomorphism if and only if

(Def. 4) h is R -fixing and monomorphic.

We say that h is R -isomorphism if and only if

(Def. 5) h is R -fixing and isomorphism.

Let S be a ring extension of R . Observe that there exists an automorphism of S which is R -fixing.

Now we state the propositions:

(38) Let us consider a ring R , a ring extension S of R , an element p of the carrier of $\text{PolyRing}(R)$, an R -fixing monomorphism h of S , and an element a of S . Then $a \in \text{Roots}(S, p)$ if and only if $h(a) \in \text{Roots}(S, p)$.

- (39) Let us consider an integral domain R , a domain ring extension S of R , a non zero element p of the carrier of $\text{PolyRing}(R)$, and an R -fixing monomorphism h of S . Then $h \upharpoonright \text{Roots}(S, p)$ is a permutation of $\text{Roots}(S, p)$. The theorem is a consequence of (38).

Let R_1, R_2, S_2 be rings, S_1 be a ring extension of R_1 , h_1 be a function from R_1 into R_2 , and h_2 be a function from S_1 into S_2 . We say that h_2 is h_1 -extending if and only if

(Def. 6) for every element a of R_1 , $h_2(a) = h_1(a)$.

Now we state the proposition:

- (40) Let us consider rings R_1, R_2, S_2 , a ring extension S_1 of R_1 , a function h_1 from R_1 into R_2 , and a function h_2 from S_1 into S_2 . Then h_2 is h_1 -extending if and only if $h_2 \upharpoonright R_1 = h_1$.

Let R be a ring and S be a ring extension of R . Let us note that every automorphism of S which is R -fixing is also (id_R) -extending and every automorphism of S which is (id_R) -extending is also R -fixing.

Now we state the proposition:

- (41) Let us consider fields F_1, F_2 , an extension E_1 of F_1 , an extension E_2 of F_2 , an E_1 -extending extension K_1 of F_1 , an E_2 -extending extension K_2 of F_2 , a function h_1 from F_1 into F_2 , a function h_2 from E_1 into E_2 , and a function h_3 from K_1 into K_2 . Suppose h_2 is h_1 -extending and h_3 is h_2 -extending. Then h_3 is h_1 -extending.

Let F be a field and E_1, E_2 be extensions of F . We say that E_1 and E_2 are isomorphic over F if and only if

(Def. 7) there exists a function i from E_1 into E_2 such that i is F -isomorphism.

Now we state the propositions:

- (42) Let us consider a field F , and an extension E of F . Then E and E are isomorphic over F .
- (43) Let us consider a field F , and extensions E_1, E_2 of F . If E_1 and E_2 are isomorphic over F , then E_2 and E_1 are isomorphic over F .

PROOF: Consider f being a function from E_1 into E_2 such that f is F -isomorphism. Reconsider $g = f^{-1}$ as a function from E_2 into E_1 . g is additive. g is multiplicative. $\square$

- (44) Let us consider a field F , and extensions E_1, E_2, E_3 of F . Suppose E_1 and E_2 are isomorphic over F and E_2 and E_3 are isomorphic over F . Then E_1 and E_3 are isomorphic over F .

PROOF: Consider f being a function from E_1 into E_2 such that f is F -isomorphism. Consider g being a function from E_2 into E_3 such that g is F -isomorphism. $\text{dom}(g \cdot f) = \text{the carrier of } E_1$. Reconsider $h = g \cdot f$ as

a function from E_1 into E_3 . h is F -fixing. $\square$

- (45) Let us consider a field F , an F -finite extension E_1 of F , and an extension E_2 of F . Suppose E_1 and E_2 are isomorphic over F . Then

- (i) E_2 is F -finite, and
- (ii) $\deg(E_1, F) = \deg(E_2, F)$.

The theorem is a consequence of (36).

6. SOME MORE PRELIMINARIES

Let R be a ring, S_1, S_2 be ring extensions of R , and h be a relation between the carrier of S_1 and the carrier of S_2 . We say that h is R -isomorphism if and only if

- (Def. 8) there exists a function g from S_1 into S_2 such that $g = h$ and g is R -isomorphism.

Now we state the propositions:

- (46) Let us consider a field F , an extension E of F , and an F -algebraic element a of E . Then

- (i) $0_{\text{FAdj}(F, \{a\})} = \text{ExtEval}(\mathbf{0}.F, a)$, and
- (ii) $1_{\text{FAdj}(F, \{a\})} = \text{ExtEval}(\mathbf{1}.F, a)$.

- (47) Let us consider a field F , an extension E of F , an F -algebraic element a of E , elements x, y of $\text{FAdj}(F, \{a\})$, and polynomials p, q over F . Suppose $x = \text{ExtEval}(p, a)$ and $y = \text{ExtEval}(q, a)$. Then

- (i) $x + y = \text{ExtEval}(p + q, a)$, and
- (ii) $x \cdot y = \text{ExtEval}(p * q, a)$.

- (48) Let us consider a field F , an extension E of F , an F -algebraic element a of E , and an element x of F . Then $x = \text{ExtEval}(x \upharpoonright F, a)$.

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

- (49) $\text{HomExtEval}(a, F)$ is a function from $\text{PolyRing}(F)$ into $\text{RAdj}(F, \{a\})$.

- (50) $\text{HomExtEval}(a, F)$ is a function from $\text{PolyRing}(F)$ into $\text{FAdj}(F, \{a\})$.
The theorem is a consequence of (49).

- (51) 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 F_1 -algebraic element a of E_1 , an F_2 -algebraic element b of E_2 , and an irreducible element p of the carrier of $\text{PolyRing}(F_1)$. Suppose $\text{ExtEval}(p, a) = 0_{E_1}$ and $\text{ExtEval}((\text{PolyHom}(h))(p), b) = 0_{E_2}$. Then

$(\text{PolyHom}(h))(\text{MinPoly}(a, F_1)) = \text{MinPoly}(b, F_2)$. The theorem is a consequence of (15) and (16).

- (52) 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 F_1 -algebraic element a of E_1 , and an F_2 -algebraic element b of E_2 . Suppose $\text{ExtEval}((\text{PolyHom}(h))(\text{MinPoly}(a, F_1)), b) = 0_{E_2}$. Then $(\text{PolyHom}(h))(\text{MinPoly}(a, F_1)) = \text{MinPoly}(b, F_2)$. The theorem is a consequence of (15) and (16).
- (53) Let us consider a field F_1 , a non constant element p_1 of the carrier of $\text{PolyRing}(F_1)$, an extension F_2 of F_1 , a non constant element p_2 of the carrier of $\text{PolyRing}(F_2)$, and a splitting field E of p_1 . Suppose $p_2 = p_1$ and E is F_2 -extending. Then E is a splitting field of p_2 .

7. UNIQUENESS OF SPLITTING FIELDS

Let F be a field, E be an extension of F , and a, b be F -algebraic elements of E . The functor $\Phi(a, b)$ yielding a relation between the carrier of $\text{FAdj}(F, \{a\})$ and the carrier of $\text{FAdj}(F, \{b\})$ is defined by the term

(Def. 9) the set of all $\langle \text{ExtEval}(p, a), \text{ExtEval}(p, b) \rangle$ where p is a polynomial over F .

Note that $\Phi(a, b)$ is quasi-total. Now we state the proposition:

- (54) Let us consider a field F , an extension E of F , and F -algebraic elements a, b of E . Then $\Phi(a, b)$ is F -isomorphism if and only if $\text{MinPoly}(a, F) = \text{MinPoly}(b, F)$. The theorem is a consequence of (46), (47), and (48).

Let F_1 be a field, F_2 be an F_1 -isomorphic, F_1 -homomorphic field, h be an isomorphism between F_1 and F_2 , E_1 be an extension of F_1 , E_2 be an extension of F_2 , a be an element of E_1 , b be an element of E_2 , and p be an irreducible element of the carrier of $\text{PolyRing}(F_1)$.

Assume $\text{ExtEval}(p, a) = 0_{E_1}$ and $\text{ExtEval}((\text{PolyHom}(h))(p), b) = 0_{E_2}$. The functor $\Psi(a, b, h, p)$ yielding a function from $\text{FAdj}(F_1, \{a\})$ into $\text{FAdj}(F_2, \{b\})$ is defined by

(Def. 10) for every element r of the carrier of $\text{PolyRing}(F_1)$, $it(\text{ExtEval}(r, a)) = \text{ExtEval}((\text{PolyHom}(h))(r), b)$.

Now we state the propositions:

- (55) 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 $\text{PolyRing}(F_1)$. Suppose $\text{ExtEval}(p, a) = 0_{E_1}$

and $\text{ExtEval}((\text{PolyHom}(h))(p), b) = 0_{E_2}$. Then $\Psi(a, b, h, p)$ is h -extending and isomorphism.

PROOF: Set $f = \Psi(a, b, h, p)$. Set $F_3 = \text{FAdj}(F_1, \{a\})$. Set $F_5 = \text{FAdj}(F_2, \{b\})$. $f(1_{F_3}) = 1_{F_5}$ by [6, (36)], [5, (14)], [7, (14)], (13). f is onto by [6, (56), (45)]. $\square$

- (56) Let us consider a field F , an extension E of F , an irreducible element p of the carrier of $\text{PolyRing}(F)$, and elements a, b of E . Suppose a is a root of p in E and b is a root of p in E . Then $\text{FAdj}(F, \{a\})$ and $\text{FAdj}(F, \{b\})$ are isomorphic. The theorem is a consequence of (55).

- (57) Let us consider a field F_1 , an F_1 -homomorphic, F_1 -isomorphic field F_2 , an isomorphism h between F_1 and F_2 , a non constant element p of the carrier of $\text{PolyRing}(F_1)$, a splitting field E_1 of p , and a splitting field E_2 of $(\text{PolyHom}(h))(p)$. Then there exists a function f from E_1 into E_2 such that f is h -extending and isomorphism.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every field F_1 for every F_1 -homomorphic, F_1 -isomorphic field F_2 for every isomorphism h between F_1 and F_2 for every non constant element p of the carrier of $\text{PolyRing}(F_1)$ for every splitting field E_1 of p for every splitting field E_2 of $(\text{PolyHom}(h))(p)$ such that $\overline{(\text{Roots}(E_1, p)) \setminus (\text{the carrier of } F_1)} = \1 there exists a function f from E_1 into E_2 such that f is h -extending and isomorphism.

For every natural number k , $\mathcal{P}[k]$. Consider n being a natural number such that $\overline{(\text{Roots}(E_1, p)) \setminus \alpha} = n$, where α is the carrier of F_1 . $\square$

- (58) Let us consider a field F , a non constant element p of the carrier of $\text{PolyRing}(F)$, and splitting fields E_1, E_2 of p . Then E_1 and E_2 are isomorphic over F .

REFERENCES

- [1] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, and Karol Pāk. 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.
- [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:https://doi.org/10.1007/11618027_4. 4th International Conference on Mathematical Knowledge Management, Bremen, Germany, MKM 2005, July 15–17, 2005, Revised Selected Papers.
- [3] Serge Lang. *Algebra*. Springer Verlag, 2002 (Revised Third Edition).
- [4] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.
- [5] Christoph Schwarzweller. Field extensions and Kronecker’s construction. *Formalized Mathematics*, 27(3):229–235, 2019. doi:10.2478/forma-2019-0022.
- [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.

- [7] 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.

Accepted June 30, 2021