

Separable Polynomials and Separable Extensions

Christoph Schwarzweller 
 Institute of Informatics
 University of Gdańsk
 Poland

Summary. We continue the formalization of field theory in Mizar [2], [3], [4]. We introduce separability of polynomials and field extensions: a polynomial is separable, if it has no multiple roots in its splitting field; an algebraic extension E of F is separable, if the minimal polynomial of each $a \in E$ is separable. We prove among others that a polynomial $q(X)$ is separable if and only if the gcd of $q(X)$ and its (formal) derivation equals 1 – and that a irreducible polynomial $q(X)$ is separable if and only if its derivation is not 0 – and that $q(X)$ is separable if and only if the number of $q(X)$'s roots in some field extension equals the degree of $q(X)$.

A field F is called perfect if all irreducible polynomials over F are separable, and as a consequence every algebraic extension of F is separable. Every field with characteristic 0 is perfect [13]. To also consider separability in fields with prime characteristic p we define the rings $R^p = \{ a^p \mid a \in R \}$ and the polynomials $X^n - a$ for $a \in R$. Then we show that a field F with prime characteristic p is separable if and only if $F = F^p$ and that finite fields are perfect. Finally we prove that for fields $F \subseteq K \subseteq E$ where E is a separable extension of F both E is separable over K and K is separable over F .

MSC: 12F10 68V20

Keywords: separable polynomials; perfect fields; separable extensions

MML identifier: FIELD_15, version: 8.1.14 5.79.1465

INTRODUCTION

In this paper we formalize separability [7] using the Mizar formalism [2], [3], [6]. A polynomial is separable, if it has no multiple roots in its splitting field; an algebraic extension E of F is separable, if the minimal polynomial of each $a \in E$ is separable [8], [10], [5].

In the first two sections we provide some technical lemmas necessary later. They concern for example divisibility and gcds of integers, in particular we show that a prime p divides $\binom{p}{m}$ for $1 \leq m < p$. We also need a number of results on powers of polynomials among them that a polynomial $q(X)$ divides $(X - a)^n$ if and only if $q(X) = (X - a)^l$ for some $0 \leq l \leq n$ or that a is an n -fold root of $(X - a)^n$.

In the third section we define the ring $R^p = \{ a^p \mid a \in R \}$ for a given ring R with prime characteristic p . In order to do so we proved that $(a + b)^p = a^p + b^p$, also called freshman's dream.

Then we define the polynomial $q(X) = X^n - a$ necessary to describe separability in fields with characteristic $p \neq 0$. Note that the roots of $q(X)$ are the elements b with $b^p = a$, so that $q(X) = (X - b)^p$ if there exists such a b and is irreducible otherwise.

In section five we deal with multiplicity of polynomials. We show among others that a polynomial $q(X)$ has a multiple root (in a field extension where $q(X)$ splits) if and only if the gcd of $q(X)$ and its (formal) derivation is not 1. For irreducible $q(X)$ this can be sharpened to $q(X)$'s derivation being 0. We also prove that in fields with characteristic $p \neq 0$ the derivation of a polynomial $q(X)$ is 0 if and only if there exists a polynomial $r(X)$ such that $q(X) = r(X^p)$.

The next two sections are devoted to separability of polynomials. We define a polynomial $q(X)$ to be separable, if it has no multiple roots in its splitting field. Note that the splitting field of $q(X)$ is unique only up to isomorphism, so that we had to prove that the definition indeed is independent of a particular splitting field. We prove a number of characterizations of separability found in the literature, for example that $q(X)$ is separable if and only if the number of $q(X)$'s roots equals the degree of $q(X)$ in some field extension if and only if $q(X)$ is square free in every field extension in which q splits. Then we introduce perfect fields, e.g. fields in which every irreducible polynomial is separable. Fields with characteristic 0 are perfect (see [13]). Fields F with characteristic $p \neq 0$ are perfect if and only if $F = F^p$. This is shown using the polynomial $X^p - a$, which is inseparable and irreducible if there is no b with $b^p = a$. Because in finite fields the multiplicative group is cyclic in finite fields such a b always exists and so finite field are perfect.

In the last section we define separable extensions: an algebraic extension is separable if the minimal polynomial of every $a \in E$ is separable. As an easy consequence we get that for $p(X) \in F[X] \setminus F$, where F is perfect, the splitting field of $p(X)$ is both normal and separable. We also show that for fields $F \subseteq K \subseteq E$ where E is a separable extension of F both E is a separable extension of K and K is a separable extension of F .

1. PRELIMINARIES

Let R be a ring and k be a non zero natural number. One can check that $(0_R)^k$ reduces to 0_R .

Let k be a natural number. Note that $(1_R)^k$ reduces to 1_R .

Let p be a prime number. Observe that there exists a field which is finite and has characteristic p .

Let F be a finite field. Let us observe that $\text{char}(F)$ is prime.

Let R be a non degenerated ring. One can verify that every element of the carrier of Polynom-Ring R which is monic is also non zero.

Let F be a field, p be a non constant element of the carrier of Polynom-Ring F , and a be a non zero element of F . One can verify that the functor $a \cdot p$ yields a non constant element of the carrier of Polynom-Ring F . Now we state the propositions:

- (1) Let us consider a natural number n , and a non zero natural number m . Then $\frac{n}{m}$ is a natural number if and only if $m \mid n$.
- (2) Let us consider a prime number p , and natural numbers n, a, b . If $p \mid a$ and $p \nmid b$ and $n = \frac{a}{b}$, then $p \mid n$. The theorem is a consequence of (1).
- (3) Let us consider a prime number p , and a non zero natural number n . If $n < p$, then $\text{gcd}(n, p) = 1$.
- (4) Let us consider a non zero natural number n , and a prime number p . Then there exist natural numbers k, m such that
 - (i) $n = m \cdot p^k$, and
 - (ii) $p \nmid m$.

The theorem is a consequence of (1).

Let R be an integral domain, a be a non zero element of R , and n be a natural number. One can check that a^n is non zero.

Now we state the propositions:

- (5) Let us consider a ring R , an element a of R , and an even natural number n . Then $(-a)^n = a^n$.
- (6) Let us consider a ring R , an element a of R , and an odd natural number n . Then $(-a)^n = -a^n$.
- (7) Let us consider a ring R with characteristic 2, and an element a of R . Then $-a = a$.
- (8) Let us consider an add-associative, right zeroed, right complementable, Abelian, non empty double loop structure R , and an integer i . Then $i \star 0_R = 0_R$.

PROOF: Define $\mathcal{P}[\text{integer}] \equiv \$1 \star 0_R = 0_R$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [12, (64), (60), (62)]. For every integer i , $\mathcal{P}[i]$. $\square$

Let F be a finite field. Let us observe that $\text{MultGroup}(F)$ is cyclic.

Now we state the propositions:

- (9) Let us consider a field F , and an extension E of F . Then $\text{MultGroup}(F)$ is a subgroup of $\text{MultGroup}(E)$.
- (10) Let us consider a skew field R , a natural number n , an element a of R , and an element b of $\text{MultGroup}(R)$. If $a = b$, then $a^n = b^n$ by [1, (17)], [11, (8)].

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

- (11) $(a + b) \cdot p = a \cdot p + b \cdot p$.
- (12) $(a \cdot b) \cdot p = a \cdot (b \cdot p)$.
- (13) Let us consider a ring R , an element q of the carrier of $\text{Polynom-Ring } R$, a polynomial p over R , and a natural number n . If $p = q$, then $n \cdot (1_R) \cdot p = n \cdot q$ by [9, (26)].
- (14) Let us consider a ring R , an element q of the carrier of $\text{Polynom-Ring } R$, a polynomial p over R , and natural numbers n, j . If $p = n \cdot q$, then $p(j) = n \cdot q(j)$.
- (15) Let us consider a field F , an element a of F , a polynomial p over F , an extension E of F , an element b of E , and a polynomial q over E . If $a = b$ and $p = q$, then $a \cdot p = b \cdot q$.
- (16) Let us consider a field F , an irreducible element p of the carrier of $\text{Polynom-Ring } F$, and an element q of the carrier of $\text{Polynom-Ring } F$. If $q \mid p$, then q is unital or associated to p .
- (17) Let us consider a field F , an irreducible element p of the carrier of $\text{Polynom-Ring } F$, and a monic element q of the carrier of $\text{Polynom-Ring } F$. If $q \mid p$, then $q = \mathbf{1}.F$ or $q = \text{NormPoly } p$.

Let us consider a field F and a non zero element p of the carrier of $\text{Polynom-Ring } F$. Now we state the propositions:

- (18) p is reducible if and only if p is a unit of $\text{Polynom-Ring } F$ or there exists a monic element q of the carrier of $\text{Polynom-Ring } F$ such that $q \mid p$ and $1 \leq \deg(q) < \deg(p)$.
- (19) p is reducible if and only if there exists a monic element q of the carrier of $\text{Polynom-Ring } F$ such that $q \mid p$ and $1 \leq \deg(q) < \deg(p)$.

2. ON POWERS OF POLYNOMIALS

Let R be an integral domain, p be a non zero polynomial over R , and n be a natural number. Observe that p^n is non zero. Let F be a field, p be a non constant polynomial over F , and n be a non zero natural number. One can verify that p^n is non constant.

Let p be a non constant element of the carrier of Polynom-Ring F . Let us note that p^n is non constant. Let p be a constant element of the carrier of Polynom-Ring F . One can check that p^n is constant and p^n is constant. Now we state the propositions:

- (20) Let us consider an integral domain R , a polynomial p over R , and a natural number n . Then $\text{LC } p^n = (\text{LC } p)^n$.
- (21) Let us consider an integral domain R , a non zero polynomial p over R , and a natural number n . Then $\deg(p^n) = n \cdot (\deg(p))$.
- (22) Let us consider a commutative ring R , a polynomial p over R , and a non zero natural number n . Then $(p^n)(0) = p(0)^n$.
- (23) Let us consider an integral domain R , a non zero element a of R , and a natural number n . Then $\langle 0_R, a \rangle^n = a^n \cdot (\langle 0_R, 1_R \rangle^n)$.
- (24) Let us consider a field F , an element a of F , and a natural number n . Then $(a \upharpoonright F)^n = a^n \upharpoonright F$.
- (25) Let us consider a field F , a non zero element a of F , and natural numbers n, m . Then $(\text{anpoly}(a, m))^n = \text{anpoly}(a^n, n \cdot m)$.
- (26) Let us consider a field F , an element a of F , and a natural number n . Then $\deg((X - a)^n) = n$.
- (27) Let us consider a field F , an element a of F , and a non zero natural number n . Then $\text{Roots}((X - a)^n) = \{a\}$.

Let us consider a field F , an element a of F , and a natural number n . Now we state the propositions:

- (28) $\text{multiplicity}((X - a)^n, a) = n$. The theorem is a consequence of (26).
- (29) $\overline{\text{BRoots}((X - a)^n)} = n$.
- (30) Let us consider a non degenerated commutative ring R , a commutative ring extension S of R , an element a of R , an element b of S , and an element n of $\mathbb{N}$. If $a = b$, then $(X - b)^n = (X - a)^n$.
- (31) Let us consider a field F , a monic polynomial p over F , an element a of F , and a natural number n . Then $p \mid (X - a)^n$ if and only if there exists a natural number l such that $l \leq n$ and $p = (X - a)^l$. The theorem is a consequence of (27), (28), and (26).

- (32) Let us consider a non degenerated commutative ring R , elements a, b of R , and a natural number n . Then $\text{eval}((X+a)^n, b) = (a+b)^n$.
- (33) Let us consider a field F , an element a of F , and a non zero natural number n . Then $(X-a)^n$ splits in F .
 PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (X-a)^{\$1}$ splits in F . For every natural number k such that $k \geq 1$ holds $\mathcal{P}[k]$. $\square$
- (34) Let us consider a field F_1 , an F_1 -homomorphic field F_2 , a homomorphism h from F_1 to F_2 , an element a of F_1 , and a natural number n . Then $(\text{PolyHom}(h))((X-a)^n) = (X-h(a))^n$.

3. THE RINGS R^p FOR PRIMES p

Let p be a prime number. One can verify that every commutative ring with characteristic p is non degenerated. Now we state the propositions:

- (35) Let us consider a prime number p , a commutative ring R with characteristic p , and an element a of R . Then $p \cdot a = 0_R$.
- (36) Let us consider a prime number p , a commutative ring R with characteristic p , a non zero element a of R , and a non zero natural number n . If $n < p$, then $n \cdot a \neq 0_R$.

Let us consider a prime number p , a commutative ring R with characteristic p , an element a of R , and a natural number n . Now we state the propositions:

- (37) $n \cdot p \cdot a = 0_R$.
- (38) If $p \mid n$, then $n \cdot a = 0_R$. The theorem is a consequence of (37).
- (39) Let us consider a prime number p , a commutative ring R with characteristic p , a non zero element a of R , and a natural number n . Then $p \mid n$ if and only if $n \cdot a = 0_R$. The theorem is a consequence of (37) and (36).
- (40) Let us consider a prime number p , a commutative ring R with characteristic p , and elements a, b of R . Then $(a+b)^p = a^p + b^p$.

PROOF: Set $F = \langle \binom{p}{0}a^0b^p, \dots, \binom{p}{p}a^pb^0 \rangle$. Consider f_1 being a sequence of the carrier of R such that $\sum F = f_1(\text{len } F)$ and $f_1(0) = 0_R$ and for every natural number j and for every element v of R such that $j < \text{len } F$ and $v = F(j+1)$ holds $f_1(j+1) = f_1(j) + v$. Define $\mathcal{P}[\text{element of } \mathbb{N}] \equiv \$1 = 0$ and $f_1(\$1) = 0_R$ or $0 < \$1 < \text{len } F$ and $f_1(\$1) = a^p$ or $\$1 = \text{len } F$ and $f_1(\$1) = a^p + b^p$. For every element j of $\mathbb{N}$ such that $0 \leq j \leq \text{len } F$ holds $\mathcal{P}[j]$. $\square$

- (41) Let us consider a prime number p , a commutative ring R with characteristic p , elements a, b of R , and a natural number i . Then $(a+b)^{p^i} = a^{p^i} + b^{p^i}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (a + b)^{p^{\mathbb{S}_1}} = a^{p^{\mathbb{S}_1}} + b^{p^{\mathbb{S}_1}}$. For every natural number k , $\mathcal{P}[k]$. $\square$

- (42) Let us consider a prime number p , a commutative ring R with characteristic p , and an element a of R . Then $-a^p = (-a)^p$. The theorem is a consequence of (40).

Let p be a prime number and R be a commutative ring with characteristic p . The functor R^p yielding a strict double loop structure is defined by

- (Def. 1) the carrier of it = the set of all a^p where a is an element of R and the addition of it = (the addition of R) $\upharpoonright$ (the carrier of it) and the multiplication of it = (the multiplication of R) $\upharpoonright$ (the carrier of it) and $1_{it} = 1_R$ and $0_{it} = 0_R$.

Let us observe that R^p is non degenerated.

Let us consider a prime number p , a commutative ring R with characteristic p , elements a, b of R , and elements x, y of R^p . Now we state the propositions:

- (43) If $a = x$ and $b = y$, then $a + b = x + y$.

- (44) If $a = x$ and $b = y$, then $a \cdot b = x \cdot y$.

Let p be a prime number and R be a commutative ring with characteristic p . Note that R^p is Abelian, add-associative, right zeroed, and right complementable and R^p is commutative, associative, well unital, and distributive.

Let F be a field with characteristic p . One can verify that F^p is almost left invertible. Let R be a commutative ring with characteristic p . Observe that R^p has characteristic p . Let F be a field with characteristic p . One can verify that the functor F^p yields a strict subfield of F .

4. THE POLYNOMIALS $X^n - a$

Let R be a unital, non empty double loop structure, a be an element of R , and n be a non zero natural number. The functor $X^n - a$ yielding a sequence of R is defined by the term

- (Def. 2) $\mathbf{0}.R + \cdot [0 \mapsto -a, n \mapsto 1_R]$.

Let us observe that $X^n - a$ is finite-Support.

Let R be a unital, non degenerated double loop structure. One can verify that $X^n - a$ is non constant and monic.

Let R be a non degenerated ring. One can verify that the functor $X^n - a$ yields a non constant, monic element of the carrier of Polynom-Ring R . Now we state the proposition:

- (45) Let us consider a unital, non degenerated double loop structure L , an element a of L , and a non zero natural number n . Then

- (i) $(X^n - a)(0) = -a$, and
- (ii) $(X^n - a)(n) = 1_L$, and
- (iii) for every natural number m such that $m \neq 0$ and $m \neq n$ holds $(X^n - a)(m) = 0_L$.

Let us consider a unital, non degenerated double loop structure R , a non zero natural number n , and an element a of R . Now we state the propositions:

$$(46) \quad \deg(X^n - a) = n.$$

$$(47) \quad \text{LC } X^n - a = 1_R.$$

- (48) Let us consider a non degenerated ring R , a non zero natural number n , and elements a, x of R . Then $\text{eval}(X^n - a, x) = x^n - a$.

PROOF: Set $q = X^n - a$. Consider F being a finite sequence of elements of R such that $\text{eval}(q, x) = \sum F$ and $\text{len } F = \text{len } q$ and for every element j of $\mathbb{N}$ such that $j \in \text{dom } F$ holds $F(j) = q(j - '1) \cdot \text{power}_R(x, j - '1)$. $n = \deg(q)$. Consider f_1 being a sequence of the carrier of R such that $\sum F = f_1(\text{len } F)$ and $f_1(0) = 0_R$ and for every natural number j and for every element v of R such that $j < \text{len } F$ and $v = F(j + 1)$ holds $f_1(j + 1) = f_1(j) + v$. Define $\mathcal{P}[\text{element of } \mathbb{N}] \equiv \$1 = 0$ and $f_1(\$1) = 0_R$ or $0 < \$1 < \text{len } F$ and $f_1(\$1) = -a$ or $\$1 = \text{len } F$ and $f_1(\$1) = x^n - a$. For every element j of $\mathbb{N}$ such that $0 \leq j \leq \text{len } F$ holds $\mathcal{P}[j]$. $\square$

- (49) Let us consider a field F , a non zero natural number n , and elements a, b of F . Then b is a root of $X^n - a$ if and only if $b^n = a$. The theorem is a consequence of (48).
- (50) Let us consider a field F , an extension E of F , a non zero natural number n , an element a of F , and an element b of E . If $b = a$, then $X^n - a = X^n - b$. The theorem is a consequence of (43).
- (51) Let us consider a non degenerated, commutative ring R , a non trivial natural number n , and an element a of R . Then $(\text{Deriv}(R))(X^n - a) = n \cdot (X^{(n-1)} - (0_R))$. The theorem is a consequence of (43) and (14).
- (52) Let us consider a prime number p , a commutative ring R with characteristic p , and an element a of R . Then $(\text{Deriv}(R))(X^p - a) = 0.R$. The theorem is a consequence of (43) and (38).
- (53) Let us consider a prime number p , a field F with characteristic p , and elements a, b of F . If $b^p = a$, then $X^p - a = (X - b)^p$. The theorem is a consequence of (7), (43), (40), (22), and (6).
- (54) Let us consider a prime number p , a field F with characteristic p , and an element a of F . Suppose there exists no element b of F such that $b^p = a$. Then $X^p - a$ is irreducible. The theorem is a consequence of (50), (49), (53), (18), (31), (22), (5), (6), (3), (9), and (10).

5. MORE ON MULTIPLICITY OF ROOTS

Now we state the propositions:

- (55) Let us consider a field F , a non zero polynomial p over F , and an element a of F . Then $\deg(p) \geq \text{multiplicity}(p, a)$.
- (56) Let us consider a field F , a non zero polynomial p over F , an element a of F , and an element n of $\mathbb{N}$. Then $(X-a)^n \mid p$ if and only if $\text{multiplicity}(p, a) \geq n$.
- (57) Let us consider a field F , an extension E of F , a non zero element p of the carrier of Polynom-Ring F , and an element a of E . Then a is a root of p in E if and only if $\text{multiplicity}(p, a) \geq 1$. The theorem is a consequence of (56).
- (58) Let us consider a field F , a non zero polynomial p over F , an extension E of F , and a non zero polynomial q over E . Suppose $q = p$. Let us consider an E -extending extension K of F , and an element a of K . Then $\text{multiplicity}(q, a) = \text{multiplicity}(p, a)$.
- (59) Let us consider a field F , a non zero polynomial p over F , an extension E of F , and a non zero polynomial q over E . Suppose $q = p$. Let us consider an element a of E . Then $\text{multiplicity}(q, a) = \text{multiplicity}(p, a)$. The theorem is a consequence of (58).
- (60) Let us consider a field F , a non zero polynomial p over F , a non zero element c of F , and an element a of F . Then $\text{multiplicity}(c \cdot p, a) = \text{multiplicity}(p, a)$.
- (61) Let us consider a field F , an extension E of F , a non zero polynomial p over F , a non zero element c of F , and an element a of E . Then $\text{multiplicity}(c \cdot p, a) = \text{multiplicity}(p, a)$. The theorem is a consequence of (15) and (59).
- (62) Let us consider a field F , an extension E of F , non zero polynomials p, q over F , and an element a of E . Then $\text{multiplicity}(p \cdot q, a) = \text{multiplicity}(p, a) + \text{multiplicity}(q, a)$. The theorem is a consequence of (59).
- (63) Let us consider a field F , a non zero polynomial p over F , extensions E_1, E_2 of F , and a function i from E_1 into E_2 . Suppose i is F -fixing and isomorphism. Let us consider an element a of E_1 . Then $\text{multiplicity}(p, a) = \text{multiplicity}(p, i(a))$.

PROOF: Set $n = \text{multiplicity}(p, a)$. Reconsider $E_3 = E_2$ as an E_1 -homomorphic field. Reconsider $h = i$ as an additive function from E_1 into E_3 . Reconsider $X_1 = (X-a)^n$ as an element of the carrier of Polynom-Ring E_1 . Reconsider $X_2 = (X-a)^{n+1}$ as an element of the carrier of Polynom-Ring E_1 .

$(\text{PolyHom}(h))(X_1) = (X - h(a))^n$ and $(\text{PolyHom}(h))(X_2) = (X - h(a))^{n+1}$.
 $(\text{PolyHom}(h))(p) = p$. $\square$

- (64) Let us consider a field F , a non zero polynomial p over F , an extension E of F , and an element a of F . Then $\text{multiplicity}(p, {}^{\textcircled{a}}(a, E)) = \text{multiplicity}(p, a)$.
- (65) Let us consider a field F , a non zero polynomial p over F , an extension E of F , an E -extending extension K of F , and an element a of E . Then $\text{multiplicity}(p, {}^{\textcircled{a}}(a, K)) = \text{multiplicity}(p, a)$.
- (66) Let us consider a field F , a non zero polynomial p over F , a polynomial q over F , and an element a of F . Suppose $p = (X - a)^{\text{multiplicity}(p, a)} * q$. Then $\text{eval}(q, a) \neq 0_F$.
- (67) Let us consider a field F , and a non zero polynomial p over F . Then $\overline{\text{Roots}(p)} < \overline{\text{BRoots}(p)}$ if and only if there exists an element a of F such that $\text{multiplicity}(p, a) > 1$.
- (68) Let us consider a field F , a non zero polynomial p over F , and an element a of F . Then $\text{multiplicity}(\text{NormPoly } p, a) = \text{multiplicity}(p, a)$.
- (69) Let us consider a field F , and a non constant polynomial p over F . Then $\deg(p) = \overline{\text{Roots}(p)}$ if and only if p splits in F and for every element a of F , $\text{multiplicity}(p, a) \leq 1$. The theorem is a consequence of (67) and (68).
- (70) Let us consider a field F , a non zero element p of the carrier of Polynom-Ring F , and an element a of F . Suppose a is a root of p . Then
 - (i) $\text{multiplicity}(p, a) = 1$ iff $\text{eval}((\text{Deriv}(F))(p), a) \neq 0_F$, and
 - (ii) $\text{multiplicity}(p, a) > 1$ iff $\text{eval}((\text{Deriv}(F))(p), a) = 0_F$.

The theorem is a consequence of (66).

- (71) Let us consider a field F , and a non zero element p of the carrier of Polynom-Ring F . Then there exists an element a of F such that $\text{multiplicity}(p, a) > 1$ if and only if $\gcd(p, (\text{Deriv}(F))(p))$ has roots. The theorem is a consequence of (70).
- (72) Let us consider a field F , a non zero element p of the carrier of Polynom-Ring F , and an extension E of F . Suppose p splits in E . Then there exists an element a of E such that $\text{multiplicity}(p, a) > 1$ if and only if $\gcd(p, (\text{Deriv}(F))(p)) \neq \mathbf{1}.F$. The theorem is a consequence of (70).
- (73) Let us consider a field F , an irreducible element p of the carrier of Polynom-Ring F , and an extension E of F . Suppose p splits in E . Then there exists an element a of E such that $\text{multiplicity}(p, a) > 1$ if and only if $(\text{Deriv}(F))(p) = \mathbf{0}.F$. The theorem is a consequence of (17) and (72).
- (74) Let us consider a prime number p , a commutative ring R with characteristic p , and an element f of the carrier of Polynom-Ring R . Then

$(\text{Deriv}(R))(f) = \mathbf{0}.R$ if and only if for every natural number i such that $i \in \text{Support } f$ holds $p \mid i$. The theorem is a consequence of (38) and (39).

6. SEPARABLE POLYNOMIALS

Let F be a field and p be a non constant element of the carrier of Polynom-Ring F . We say that p is separable if and only if

(Def. 3) for every element a of the splitting field of p such that a is a root of p in the splitting field of p holds $\text{multiplicity}(p, a) = 1$.

We introduce the notation p is inseparable as an antonym for p is separable.

Let us observe that there exists a non constant, monic element of the carrier of Polynom-Ring F which is separable and there exists a non constant, monic element of the carrier of Polynom-Ring F which is inseparable.

Let us consider a field F and a non constant element p of the carrier of Polynom-Ring F . Now we state the propositions:

- (75) p is separable if and only if for every extension E of F such that p splits in E for every element a of E such that a is a root of p in E holds $\text{multiplicity}(p, a) = 1$. The theorem is a consequence of (63).
- (76) p is separable if and only if there exists an extension E of F such that p splits in E and for every element a of E such that a is a root of p in E holds $\text{multiplicity}(p, a) = 1$. The theorem is a consequence of (63).
- (77) p is separable if and only if for every extension E of F and for every element a of E , $\text{multiplicity}(p, a) \leq 1$. The theorem is a consequence of (58), (57), (75), and (76).
- (78) p is separable if and only if there exists an extension E of F such that p splits in E and for every element a of E , $\text{multiplicity}(p, a) \leq 1$. The theorem is a consequence of (57) and (76).
- (79) Let us consider a field F , and a separable, non constant element p of the carrier of Polynom-Ring F . Then $\deg(p) = \overline{\text{Roots}(p)}$ if and only if p splits in F . The theorem is a consequence of (75), (60), and (69).
- (80) Let us consider a field F , and a non constant element p of the carrier of Polynom-Ring F . Then p is separable if and only if $\gcd(p, (\text{Deriv}(F))(p)) = \mathbf{1}.F$. The theorem is a consequence of (77) and (72).
- (81) Let us consider a field F , and a non constant, irreducible element p of the carrier of Polynom-Ring F . Then p is separable if and only if $(\text{Deriv}(F))(p) \neq \mathbf{0}.F$. The theorem is a consequence of (77) and (73).
- (82) Let us consider a field F , and a non constant element p of the carrier of Polynom-Ring F . Then p is separable if and only if for every splitting field

E of p , there exists an element a of E and there exists a product of linear polynomials q of E and $\text{Roots}(E, p)$ such that $p = a \cdot q$. The theorem is a consequence of (75), (59), and (60).

- (83) Let us consider a field F , and a non constant, monic element p of the carrier of Polynom-Ring F . Then p is separable if and only if for every splitting field E of p , p is a product of linear polynomials of E and $\text{Roots}(E, p)$. The theorem is a consequence of (82).

Let us consider a field F and a non constant element p of the carrier of Polynom-Ring F . Now we state the propositions:

- (84) p is separable if and only if for every extension E of F such that p splits in E holds p is square-free over E . The theorem is a consequence of (60), (75), and (56).
- (85) $\overline{p}$ is separable if and only if there exists an extension E of F such that $\overline{\text{Roots}(E, p)} = \deg(p)$. The theorem is a consequence of (77), (58), (79), (69), and (78).
- (86) Let us consider a field F , a non constant element p of the carrier of Polynom-Ring F , and a non zero element a of F . Then $a \cdot p$ is separable if and only if p is separable. The theorem is a consequence of (15), (75), and (61).
- (87) Let us consider a field F , non constant elements p, q of the carrier of Polynom-Ring F , and an element r of the carrier of Polynom-Ring F . If $p = q * r$, then if p is separable, then q is separable. The theorem is a consequence of (77) and (62).
- (88) Let us consider a field F , an extension E of F , a non constant element p of the carrier of Polynom-Ring F , and a non constant element q of the carrier of Polynom-Ring E . If $p = q$, then p is separable iff q is separable. The theorem is a consequence of (80).

Let F be a field and a be an element of F . One can verify that $X - a$ is separable and irreducible. Let n be a non trivial natural number. Note that $(X - a)^n$ is inseparable and reducible. Let F be a field with characteristic 0. One can check that every irreducible element of the carrier of Polynom-Ring F is separable. Now we state the proposition:

- (89) Let us consider a prime number p , a field F with characteristic p , and an element a of F . If $a \notin F^p$, then $X^p - a$ is irreducible and inseparable. The theorem is a consequence of (54), (50), (49), (53), (28), and (77).

7. PERFECT FIELDS

Let F be a field. We say that F is perfect if and only if

(Def. 4) every irreducible element of the carrier of Polynom-Ring F is separable.

Let us note that every field with characteristic 0 is perfect. Now we state the propositions:

- (90) Let us consider a prime number p , a field F with characteristic p , and an element q of the carrier of Polynom-Ring F . Suppose for every natural number i such that $i \in \text{Support } q$ holds $p \mid i$ and there exists an element a of F such that $a^p = q(i)$. Then there exists an element r of the carrier of Polynom-Ring F such that $r^p = q$. The theorem is a consequence of (25) and (40).
- (91) Let us consider a prime number p , and a field F with characteristic p . Then F is perfect if and only if $F \approx F^p$. The theorem is a consequence of (89), (75), (57), (73), (74), and (90).
- (92) Let us consider a field F . Then F is finite if and only if there exists a non zero natural number n such that $\overline{F} = (\text{char}(F))^n$. The theorem is a consequence of (39) and (4).
- (93) Let us consider a prime number p , a finite field F with characteristic p , and an element a of F . Then there exists an element b of F such that $b^p = a$. The theorem is a consequence of (92) and (10).

Observe that every finite field is perfect and every algebraic closed field is perfect.

8. SEPARABLE EXTENSIONS

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

(Def. 5) there exists an F -algebraic element b of E such that $b = a$ and $\text{MinPoly}(b, F)$ is separable.

One can verify that there exists an element of E which is non zero and F -separable and every element of E which is F -separable is also F -algebraic. Let a be an F -separable element of E . Observe that $\text{MinPoly}(a, F)$ is separable. We say that E is F -separable if and only if

(Def. 6) E is F -algebraic and every element of E is F -separable.

We introduce the notation E is F -inseparable as an antonym for E is F -separable. Let us observe that there exists an extension of F which is F -finite and F -separable and every extension of F which is F -separable is also F -algebraic. Let E be an F -separable extension of F . Note that every element of E is F -separable. Now we state the proposition:

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

- (i) E is K -separable, and
- (ii) K is F -separable.

The theorem is a consequence of (88) and (87).

Let F be a perfect field. One can verify that every F -algebraic extension of F is F -separable and there exists an extension of F which is F -normal and F -separable. Let p be a non constant element of the carrier of Polynom-Ring F . Let us note that every splitting field of p is F -normal and F -separable.

REFERENCES

- [1] Broderick Arneson and Piotr Rudnicki. Primitive roots of unity and cyclotomic polynomials. *Formalized Mathematics*, 12(1):59–67, 2004.
- [2] 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.
- [3] 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.
- [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] Nathan Jacobson. *Basic Algebra I*. Dover Books on Mathematics, 1985.
- [6] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.
- [7] Serge Lang. *Algebra*. Springer Verlag, 2002 (Revised Third Edition).
- [8] Heinz Lüneburg. *Die grundlegenden Strukturen der Algebra (in German)*. Oldenbourg Wissenschaftsverlag, 1999.
- [9] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(3):461–470, 2001.
- [10] Knut Radbruch. *Algebra I*. Lecture Notes, University of Kaiserslautern, Germany, 1991.
- [11] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(3):559–564, 2001.
- [12] Christoph Schwarzweller and Artur Korniłowicz. Characteristic of rings. Prime fields. *Formalized Mathematics*, 23(4):333–349, 2015. doi:10.1515/forma-2015-0027.
- [13] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Simple extensions. *Formalized Mathematics*, 31(1):287–298, 2023. doi:10.2478/forma-2023-0023.

Accepted June 18, 2024
