FORMALIZED MATHEMATICS
Vol. 32, No. 1, pp. 289–302, 2024
DOI: 10.2478/forma-2024-0024
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Finite Fields

Christoph Schwarzweller
Institute of Informatics
University of Gdańsk
Poland

Summary. We continue the formalization of field theory in Mizar. Here we prove existence and uniqueness of finite fields by constructing the splitting field of the polynomial $X^{(p^n)} - X$ over the prime field of a field with characteristic p. We also define the Frobenius morphism and show that the automorphisms of a field with p^n elements are exactly the powers $0, \ldots, n-1$ of the Frobenius morphism, that is the automorphism group is generated by the Frobenius morphism.

MSC: 12E20 68V20

Keywords: finite field; splitting field; Galois field

MML identifier: FIELD_16, version: 8.1.14 5.88.1486

Introduction

In this paper we continue the formalization of field theory (see, e.g., [11], [12]) proving existence and uniqueness of finite fields [9, 10, 5] and also establishing the automorphisms of a finite field using the Mizar formalism [1, 2, 7, 4, 3] (compare [6] for Isabelle/HOL formalization).

In the first three sections we provide some notation and lemmas needed later. First we consider function iterations f^n where n is a natural number. We prove some standard properties, amongst others that f^n is an automorphism, if f is. Then we deal with subfields: we say that a subset S of a given field F induces a subfield of F, if S contains 0 and 1 and is closed with respect to the field operations. It is well known that in this case S with the restricted field operations itself is a field; we construct this field by defining a functor InducedSubfield(S). The third section contains a number of technical lemmas, but also the proof that a finite extension of a finite field is both again finite and simple.

In the fourth section we briefly introduce reduced rings, that is rings in which 0 is the only nilpotent element. Then we define the Frobenius morphism of a ring R, which is injective, if R is nilpotent. We also prove that the Frobenius morphism of Z/p is trivial and that a field F is perfect if and only if its Frobenius morphism is bijective. The next section is devoted to the polynomials $X^n - X$. The most important properties we prove are that a is a root of $X^n - X$ if and only if $a^n = a$ and that the derivation of $X^{(p^n)} - X$ in a field with characteristic p is -1, so that in this case $X^{(p^n)} - X$ is separable. Section 6 presents basic properties of prime fields, for example that if F is a field with p^n elements, then an element a is in the prime field of F if and only if $a^p = a$. The main result is that a finite field with p^n elements is a finite simple extension of degree n over its prime field.

Section seven is the core of the article, here we show existence and uniqueness of finite fields. If F is a field with characteristic p, then the splitting field of $X^{(p^n)} - X$ over F's prime field is a field with p^n elements: the roots of $X^{(p^n)} - X$ induce a field which – because $X^{(p^n)} - X$ is separable – contains exactly p^n elements. Because two splitting fields of $X^{(p^n)} - X$ are isomorphic, this also implies that two finite fields with the same number of elements are isomorphic. In eighth section we prove that the automorphisms of a field F with p^n elements are exactly the powers $0, \ldots, n-1$ of F's Frobenius morphism. To do so we also showed that in $F(a)$ where a is algebraic an F-fixing automorphism is uniquely determined by a, that is from $f_1(a) = f_2(a)$ already follows $f_1 = f_2$. This implies that in this case the set of automorphisms is finite. In the last section we define Galois fields over q where $q = p^n$ is a prime power. Here we assume that the finite fields contain Z/p as a subfield, so that the prime field of a finite field now is Z/p. Though this section hence is just a repetition of prior results for a special case, we think that in this form the results about finite fields are easier reusable in further developments: the results stated as theorems so far, here can be expressed using clusters.

1. Iteration of Functions

Let K, L be non empty 1-sorted structures. Let us observe that there exists a sequence which is (L^K)-valued.

Let F be an (L^K)-valued sequence and n be a natural number. One can verify that the functor $F(n)$ yields a function from K into L. Let F be a field. Let us observe that there exists a vector space over F which is trivial.

The scheme *RecExF* deals with a non empty 1-sorted structure $\mathcal{D}$ and a function $\mathcal{F}$ from $\mathcal{D}$ into $\mathcal{D}$ and a ternary predicate $\mathcal{P}$ and states that

(Sch. 1) There exists a $(\mathcal{D}^{\mathcal{D}})$-valued sequence f such that $f(0) = \mathcal{F}$ and for every natural number n, $\mathcal{P}[n, f(n), f(n+1)]$

provided

- for every natural number n and for every function g_1 from $\mathcal{D}$ into $\mathcal{D}$, there exists a function g_2 from $\mathcal{D}$ into $\mathcal{D}$ such that $\mathcal{P}[n, g_1, g_2]$.

Let L be a non empty 1-sorted structure, f be a function from L into L, and n be a natural number. The functor f^n yielding a function from L into L is defined by

(Def. 1) there exists an (L^L)-valued sequence F such that $it = F(n)$ and $F(0) = \mathrm{id}_L$ and for every natural number i, $F(i+1) = F(i) \cdot f$.

One can verify that f^1 reduces to f. Now we state the propositions:

(1) Let us consider a non empty 1-sorted structure L, and a function f from L into L. Then

(i) $f^0 = \mathrm{id}_L$, and

(ii) $f^1 = f$, and

(iii) $f^2 = f \cdot f$.

(2) Let us consider a non empty 1-sorted structure L, a function f from L into L, and a natural number n. Then $f^{n+1} = f^n \cdot f = f \cdot (f^n)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv f^{\$_1+1} = f^{\$_1} \cdot f$. For every natural number k, $\mathcal{P}[k]$. Define $\mathcal{P}[\text{natural number}] \equiv f^{\$_1} \cdot f = f \cdot (f^{\$_1})$. $f^0 \cdot f = \mathrm{id}_R \cdot f$. For every natural number k, $\mathcal{P}[k]$. □

Let L be a non empty 1-sorted structure and n be a natural number. One can check that $(\mathrm{id}_L)^n$ reduces to id_L.

Let us consider a non empty 1-sorted structure L, a function f from L into L, and natural numbers n, m. Now we state the propositions:

(3) $f^{n+m} = f^n \cdot (f^m)$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv f^{n+\$_1} = f^n \cdot (f^{\$_1})$. For every natural number k, $\mathcal{P}[k]$. □

(4) $f^{n \cdot m} = (f^n)^m$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv f^{n \cdot \$_1} = (f^n)^{\$_1}$. $f^{n \cdot 0} = \mathrm{id}_L$. For every natural number k, $\mathcal{P}[k]$. □

(5) Let us consider a non empty 1-sorted structure L, a bijective function f from L into L, and natural numbers n, m. Then $f^{n+1} = f^{m+1}$ if and only if $f^n = f^m$. The theorem is a consequence of (2).

(6) Let us consider a non empty 1-sorted structure L, a bijective function f from L into L, and natural numbers n, m, k. If $f^n = f^m$ and $k = n - m$, then $f^k = f^0$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every natural numbers n, k such that $f^n = f^{\$_1}$ and $k = n - \$_1$ holds $f^k = f^0$. For every natural number k, $\mathcal{P}[k]$. $\square$

Let F be a field. Let us observe that there exists a function from F into F which is isomorphism.

Let R be a ring and f, g be isomorphism functions from R into R. One can verify that $f \cdot g$ is isomorphism as a function from R into R.

Let f be an isomorphism function from R into R and n be a natural number. One can verify that f^n is isomorphism as a function from R into R and f^{-1} is isomorphism as a function from R into R.

2. Induced Subfields

Let F be a field and S be a subset of F. We say that S is inducing subfield if and only if

(Def. 2) 0_F, $1_F \in S$ and for every elements a, b of F such that a, $b \in S$ holds $a+b$, $a \cdot b$, $-a \in S$ and for every non zero element a of F such that $a \in S$ holds $a^{-1} \in S$.

One can verify that there exists a subset of F which is inducing subfield and every inducing subfield subset of F is non empty.

Let S be an inducing subfield subset of F. The functor InducedSubfield(S) yielding a strict, non empty double loop structure is defined by

(Def. 3) the carrier of $it = S$ and the addition of $it =$ (the addition of F) $\restriction S$ and the multiplication of $it =$ (the multiplication of F) $\restriction S$ and $0_{it} = 0_F$ and $1_{it} = 1_F$.

One can check that InducedSubfield(S) is non degenerated and InducedSubfield(S) is Abelian, add-associative, right zeroed, and right complementable and InducedSubfield(S) is commutative, associative, well unital, distributive, and almost left invertible.

Let us note that the functor InducedSubfield(S) yields a strict subfield of F. Let E be a field and F be a subfield of E. Let us note that the carrier of F is inducing subfield as a subset of E.

Let F be a field. One can verify that the carrier of F is inducing subfield as a subset of F.

3. SOME MORE PRELIMINARIES

Let R_1 be a ring, R_2 be an R_1-isomorphic ring, R_3 be an R_2-isomorphic ring, f be an isomorphism between R_1 and R_2, and g be an isomorphism between R_2 and R_3. Note that $g \cdot f$ is isomorphism as a function from R_1 into R_3.

Let F be a field, E be an extension of F, and f be an additive function from E into E. One can verify that $f \restriction$(the carrier of F) is additive as a function from F into F.

Let f be a multiplicative function from E into E. Let us observe that $f \restriction$(the carrier of F) is multiplicative as a function from F into F.

Let f be a unity-preserving function from E into E. Observe that $f \restriction$(the carrier of F) is unity-preserving as a function from F into F.

Let n, m be natural numbers. We say that m is n-power if and only if

(Def. 4) there exists a non zero natural number l such that $m = n^l$.

Let n be a natural number and l be a non zero natural number. Note that n^l is n-power and there exists a natural number which is n-power.

A power of n is an n-power natural number. Let n be a non zero natural number. Observe that every power of n is non zero.

Let n be a non trivial natural number. Let us observe that every power of n is non trivial. Now we state the propositions:

(7) Let us consider prime numbers p_1, p_2, and natural numbers n_1, n_2. Suppose ($n_1 \neq 0$ or $n_2 \neq 0$) and ${p_1}^{n_1} = {p_2}^{n_2}$. Then

  (i) $p_1 = p_2$, and

  (ii) $n_1 = n_2$.

(8) Let us consider a field F, a non zero element a of F, and a natural number n. Then $(a^{-1})^n = a^{n-1}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv (a^{-1})^{\$_1} = a^{\$_1 - 1}$. For every natural number k, $\mathcal{P}[k]$. □

(9) Let us consider a ring R, an R-homomorphic ring S, a multiplicative, unity-preserving function f from R into S, an element a of R, and a natural number n. Then $f(a^n) = f(a)^n$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv f(a^{\$_1}) = f(a)^{\$_1}$. For every natural number k, $\mathcal{P}[k]$. □

Let R be a ring and p be a polynomial over R. Note that $--p$ reduces to p.

Now we state the propositions:

(10) Let us consider a ring R, and polynomials p_1, p_2 over R. Then $p_1 * (-p_2) = -p_1 * p_2$.

(11) Let us consider an integral domain R, a domain ring extension S of R, and a non zero element p of the carrier of Polynom-Ring R. Then $\overline{\overline{\mathrm{Roots}(S, p)}} \leqslant \deg(p)$.

(12) Let us consider a field F, an extension E of F, an element a of E, and a natural number n. Then $a^n \in$ the carrier of $\mathrm{FAdj}(F, \{a\})$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv a^{\$_1} \in$ the carrier of $\mathrm{FAdj}(F, \{a\})$. For every natural number n, $\mathcal{P}[n]$. $\square$

(13) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and an F-fixing automorphism f of $\mathrm{FAdj}(F, \{a\})$. Then $f(a) \in \mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$.

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

(14) If $E_1 \approx E_2$, then every automorphism of E_1 is an automorphism of E_2.

(15) Suppose $E_1 \approx E_2$. Then the set of all f where f is an automorphism of E_1 = the set of all f where f is an automorphism of E_2. The theorem is a consequence of (14).

(16) Let us consider a field F, an extension E of F, an F-algebraic element a of E, and F-fixing automorphisms f, g of $\mathrm{FAdj}(F, \{a\})$. If $f(a) = g(a)$, then $f = g$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every polynomial p over F such that $\deg(p) = \$_1$ holds $f(\mathrm{ExtEval}(p, a)) = g(\mathrm{ExtEval}(p, a))$. For every natural number k, $\mathcal{P}[k]$. $\square$

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

(17) the set of all f where f is an F-fixing automorphism of $\mathrm{FAdj}(F, \{a\})$ is finite.

PROOF: Set M = the set of all f where f is an F-fixing automorphism of $\mathrm{FAdj}(F, \{a\})$. Set $R = \mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$. Define $\mathcal{P}$[object, object] $\equiv$ there exists an F-fixing automorphism g of $\mathrm{FAdj}(F, \{a\})$ such that $\$_1 = g$ and $\$_2 = g(a)$. Consider h being a function from M into R such that for every object o such that $o \in M$ holds $\mathcal{P}[o, h(o)]$. $\square$

(18) $\overline{\overline{\text{the set of all } f \text{ where } f \text{ is an } F\text{-fixing automorphism of } \mathrm{FAdj}(F, \{a\})}} \subseteq \overline{\overline{\mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))}}$.

PROOF: Set M = the set of all f where f is an F-fixing automorphism of $\mathrm{FAdj}(F, \{a\})$. Set $R = \mathrm{Roots}(\mathrm{FAdj}(F, \{a\}), \mathrm{MinPoly}(a, F))$. Define $\mathcal{P}$[object, object] $\equiv$ there exists an F-fixing automorphism g of $\mathrm{FAdj}(F, \{a\})$ such that $\$_1 = g$ and $\$_2 = g(a)$. Consider h being a function from M into R such that for every object o such that $o \in M$ holds $\mathcal{P}[o, h(o)]$. $\square$

(19) Let us consider a field F, an extension E of F, and a non constant element p of the carrier of Polynom-Ring F. Then $\overline{\overline{\mathrm{Roots}(E, p)}} = \deg(p)$ if and only if p splits in E and p is separable.

Let F be a finite field. One can verify that every subfield of F is finite.

Let F be a field and K be an extension of PrimeField F. Note that there exists an extension of PrimeField F which is K-extending.

Let F be a finite field. We introduce the notation order F as a synonym of $\overline{\overline{F}}$.

Note that order F is natural and order F is non trivial and every F-finite extension of F is finite and every F-finite extension of F is F-simple.

4. Reduced Rings and Frobenius Morphism

Let R be a ring. We say that R is reduced if and only if

(Def. 5) for every nilpotent element a of R, $a = 0_R$.

Let R be a non degenerated, commutative ring. One can verify that every element of R which is nilpotent is also non unital. Now we state the proposition:

(20) Let us consider a non degenerated, commutative ring R. Then R is reduced if and only if $\mathrm{nilrad}(R) = \{0_R\}$.

One can verify that every integral domain is reduced.

Let R be an integral domain. One can verify that every non zero element of R is non nilpotent.

Let R be a ring. The functor FrobeniusMorphism(R) yielding a function from R into R is defined by

(Def. 6) for every element a of R, $it(a) = a^{\mathrm{char}(R)}$.

We introduce the notation Frob(R) as a synonym of FrobeniusMorphism(R).

Let p be a prime number and R be a commutative ring with characteristic p. Let us observe that Frob(R) is additive, multiplicative, and unity-preserving.

Now we state the propositions:

(21) Let us consider a natural number n, and a ring R with characteristic n. Then $\ker \mathrm{Frob}(R) = \{a$, where a is an element of $R : a^n = 0_R\}$.

(22) Let us consider a non degenerated, commutative ring R. Then $\ker \mathrm{Frob}(R) \subseteq \mathrm{nilrad}(R)$. The theorem is a consequence of (21).

(23) Let us consider a ring R with characteristic 0. Then $\mathrm{Frob}(R) = (\text{the carrier of } R) \longmapsto 1_R$.

(24) Let us consider a prime number p. Then $\overline{\overline{\mathbb{Z}/p}} = p$.

(25) Let us consider a prime number p, and an element a of $\mathbb{Z}/p$. Then $a^p = a$. The theorem is a consequence of (24).

(26) Let us consider a prime number p. Then $\mathrm{Frob}(\mathbb{Z}/p) = \mathrm{id}_{\mathbb{Z}/p}$. The theorem is a consequence of (25).

(27) Let us consider a prime number p, a non zero natural number n, and a field F. If $\overline{\overline{F}} = p^n$, then $\mathrm{char}(F) = p$. The theorem is a consequence of (7).

(28) Let us consider a prime number p, a non zero natural number n, and a field F. Suppose $\overline{\overline{F}} = p^n$. Let us consider an element a of F. Then $a^{p^n} = a$.

Let p be a prime number and R be a reduced, commutative ring with characteristic p. One can verify that $\mathrm{Frob}(R)$ is one-to-one.

Let F be a finite field. Note that $\mathrm{Frob}(F)$ is onto. Now we state the proposition:

(29) Let us consider a prime number p, and a field F with characteristic p. Then F is perfect if and only if $\mathrm{Frob}(F)$ is an automorphism of F.

5. The Polynomial $X^n - X$

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

(Def. 7) $\mathbf{0}.R{+\cdot}[1 \longmapsto -1_R, n \longmapsto 1_R]$.

One can check that $X^n - R$ is finite-Support.

Let R be a non degenerated ring. One can verify that $X^n - R$ is non constant and monic.

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

(30) Let us consider a unital, non degenerated double loop structure R, an element a of R, and a non trivial natural number n. Then

(i) $(X^n - R)(1) = -1_R$, and

(ii) $(X^n - R)(n) = 1_R$, and

(iii) for every natural number m such that $m \neq 1$ and $m \neq n$ holds $(X^n - R)(m) = 0_R$.

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

(31) $\deg(X^n - R) = n$.

(32) $\mathrm{LC}\, X^n - R = 1_R$.

(33) Let us consider a non degenerated ring R, a non trivial natural number n, and an element a of R. Then $\mathrm{eval}(X^n - R, a) = a^n - a$.

PROOF: Set $q = X^n - R$. Consider F being a finite sequence of elements of R such that $\mathrm{eval}(q, x) = \sum F$ and $\mathrm{len}\, F = \mathrm{len}\, q$ and for every element j of $\mathbb{N}$ such that $j \in \mathrm{dom}\, F$ holds $F(j) = q(j -' 1) \cdot \mathrm{power}_R(x, j -' 1)$. Consider f_1 being a sequence of the carrier of R such that $\sum F = f_1(\mathrm{len}\, F)$ and $f_1(0) = 0_R$ and for every natural number j and for every element v of R such that $j < \mathrm{len}\, F$ 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 $\$_1 = 1$ and $f_1(\$_1) = 0_R$ or $1 < \$_1 < \mathrm{len}\, F$ and $f_1(\$_1) = -x$ or $\$_1 = \mathrm{len}\, F$ and $f_1(\$_1) = x^n - x$. For every element j of $\mathbb{N}$ such that $0 \leqslant j \leqslant \mathrm{len}\, F$ holds $\mathcal{P}[j]$. $\square$

(34) Let us consider a unital, non degenerated ring R, a non trivial natural number n, and an element a of R. Then a is a root of $X^n - R$ if and only if $a^n = a$. The theorem is a consequence of (33).

(35) Let us consider a prime number p, a non zero natural number n, and a field F with characteristic p. Suppose $\overline{\overline{F}} = p^n$. Let us consider an element a of F. Then $\mathrm{eval}(X^{p^n} - F, a) = 0_F$. The theorem is a consequence of (28) and (34).

(36) Let us consider a non degenerated ring R, a ring extension S of R, a non trivial natural number n, and an element a of S. Then $\mathrm{ExtEval}(X^n - R, a) = a^n - a$.

PROOF: Set $q = X^n - R$. Consider F being a finite sequence of elements of S such that $\mathrm{ExtEval}(q, x) = \sum F$ and $\mathrm{len}\, F = \mathrm{len}\, q$ and for every element j of $\mathbb{N}$ such that $j \in \mathrm{dom}\, F$ holds $F(j) = q(j -' 1)(\in S) \cdot \mathrm{power}_S(x, j -' 1)$. Consider f_1 being a sequence of the carrier of S such that $\sum F = f_1(\mathrm{len}\, F)$ and $f_1(0) = 0_S$ and for every natural number j and for every element v of S such that $j < \mathrm{len}\, F$ 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 $f_1(\$_1) = 0_S$ or $\$_1 = 1$ and $f_1(\$_1) = 0_S$ or $1 < \$_1 < \mathrm{len}\, F$ and $f_1(\$_1) = -x$ or $\$_1 = \mathrm{len}\, F$ and $f_1(\$_1) = x^n - x$. For every element j of $\mathbb{N}$ such that $0 \leqslant j \leqslant \mathrm{len}\, F$ holds $\mathcal{P}[j]$. $\square$

(37) Let us consider a unital, non degenerated ring R, a ring extension S of R, a non trivial natural number n, and an element a of S. Then a is a root of $X^n - R$ in S if and only if $a^n = a$. The theorem is a consequence of (36).

(38) Let us consider a prime number p, a commutative ring R with characteristic p, and a non zero natural number n. Then $\{m \cdot (1_R)$, where m is a natural number : $m < p\} \subseteq \mathrm{Roots}(X^{p^n} - R)$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \$_1 \cdot (1_R) \in \mathrm{Roots}(X^{p^n} - R)$. $0 \cdot (1_R)$ is a root of $X^{p^n} - R$. Reconsider $p_1 = p - 1$ as an element of $\mathbb{N}$. For every element k of $\mathbb{N}$ such that $0 \leqslant k \leqslant p_1$ holds $\mathcal{P}[k]$. $\square$

Let us consider a prime number p, a non zero natural number n, and a field F with characteristic p. Now we state the propositions:

(39) If $\overline{\overline{F}} = p^n$, then $\mathrm{Roots}(X^{p^n} - F) =$ the carrier of F. The theorem is a consequence of (35).

(40) $(\mathrm{Deriv}(F))(X^{p^n} - F) = -\mathbf{1}.F$.

(41) Let us consider a non trivial natural number n, a ring R, and a ring extension S of R. Then $X^n - R = X^n - S$.

Let p be a prime number, n be a non zero natural number, and F be a field with characteristic p. Note that $X^{p^n} - F$ is separable as a non constant element of the carrier of Polynom-Ring F.

Let F be a finite field. One can check that $X^{(\mathrm{order}\,F)} - F$ is separable as a non constant element of the carrier of Polynom-Ring F.

6. On Prime Fields of Finite Fields

Let us consider a finite field F. Now we state the propositions:

(42) $\overline{\overline{\mathrm{PrimeField}\,F}} = \mathrm{char}(F)$.

(43) $\mathrm{Roots}(X^{(\mathrm{char}(F))} - F) =$ the carrier of PrimeField F.

Now we state the propositions:

(44) Let us consider a prime number p, a non zero natural number n, and a field F. Suppose $\overline{\overline{F}} = p^n$. Then $\overline{\overline{\mathrm{PrimeField}\,F}} = p$. The theorem is a consequence of (27) and (24).

(45) Let us consider a finite field F, and an element a of F. Then $(\mathrm{Frob}(F))(a) = a$ if and only if $a \in \mathrm{PrimeField}\,F$.

(46) Let us consider a prime number p, a non zero natural number n, and a field F. Suppose $\overline{\overline{F}} = p^n$. Let us consider an element a of F. Then $a \in \mathrm{PrimeField}\,F$ if and only if $a^p = a$. The theorem is a consequence of (27).

(47) Let us consider a finite field F, an automorphism f of F, and an element a of F. Then $f(a) \in \mathrm{PrimeField}\,F$ if and only if $a \in \mathrm{PrimeField}\,F$. The theorem is a consequence of (46) and (9).

(48) Let us consider a prime field F, and an automorphism f of F. Then $f = \mathrm{id}_F$.

(49) Let us consider a finite field F, an automorphism f of F, and an element a of PrimeField F. Then $f(a) = a$. The theorem is a consequence of (47) and (48).

(50) Let us consider a prime number p, a non zero natural number n, a field F, and an extension E of F. Suppose $\overline{\overline{E}} = p^n$ and $F \approx \mathrm{PrimeField}\,E$. Then $\deg(E, F) = n$. The theorem is a consequence of (44) and (7).

(51) Every finite field is an (PrimeField F)-finite extension of PrimeField F.

(52) Every finite field is an (PrimeField F)-simple extension of PrimeField F.

7. Existence and Uniqueness of Finite Fields

Let p be a prime number, n be a non zero natural number, and F be a field with characteristic p. Note that $\mathrm{Roots}(X^{p^n} - F)$ is inducing subfield.

Let E be a splitting field of $X^{p^n} - (\mathrm{PrimeField}\,F)$. One can verify that $\mathrm{Roots}(E, X^{p^n} - (\mathrm{PrimeField}\,F))$ is inducing subfield.

Let us consider a prime number p, a non zero natural number n, a field F with characteristic p, and a splitting field E of $X^{p^n} - (\mathrm{PrimeField}\,F)$. Now we state the propositions:

(53) $\overline{\overline{\mathrm{Roots}(E, X^{p^n} - (\mathrm{PrimeField}\,F))}} = p^n$. The theorem is a consequence of (19).

(54) $E \approx \mathrm{InducedSubfield}(\mathrm{Roots}(E, X^{p^n} - (\mathrm{PrimeField}\,F)))$.

(55) Let us consider a prime number p, a non zero natural number n, and a field F. Suppose $\overline{\overline{F}} = p^n$.
Then F is a splitting field of $X^{p^n} - (\mathrm{PrimeField}\,F)$. The theorem is a consequence of (27) and (19).

(56) Let us consider a prime number p, a non zero natural number n, and a finite field F. Suppose $\overline{\overline{F}} = p^n$. Then $X^{p^n} - F$ is a product of linear polynomials of F and Ω_α, where α is the carrier of F. The theorem is a consequence of (7), (55), (41), and (39).

(57) Let us consider a prime number p, and a non zero natural number n. Then there exists a finite field F such that

   (i) $\mathrm{char}(F) = p$, and

   (ii) $\mathrm{order}\,F = p^n$.

The theorem is a consequence of (53).

(58) Let us consider a finite field F. Then there exists a prime number p and there exists a non zero natural number n such that $\mathrm{char}(F) = p$ and $\mathrm{order}\,F = p^n$.

(59) Let us consider finite fields F_1, F_2. If $\mathrm{order}\,F_1 = \mathrm{order}\,F_2$, then F_1 and F_2 are isomorphic.

Proof: Consider p_1 being a prime number, n_1 being a non zero natural number such that $\mathrm{char}(F_1) = p_1$ and order $F_1 = {p_1}^{n_1}$. Consider p_2 being a prime number, n_2 being a non zero natural number such that $\mathrm{char}(F_2) = p_2$ and order $F_2 = {p_2}^{n_2}$. Set $P_1 = \mathrm{PrimeField}\, F_1$. Set $P_2 = \mathrm{PrimeField}\, F_2$. $p_1 = p_2$ and $n_1 = n_2$. Consider i being a function from P_1 into P_2 such that i inherits ring isomorphism. Reconsider $E_1 = F_1$ as a splitting field of $X^{{p_1}^{n_1}} - P_1$. Set $E_2 =$ the splitting field of $(\mathrm{PolyHom}(i))(X^{{p_1}^{n_1}} - P_1)$. Consider f being a function from E_1 into E_2 such that f is i-extending and isomorphism. $(\mathrm{PolyHom}(i))(X^{{p_1}^{n_1}} - P_1) = X^{{p_2}^{n_2}} - P_2$ by [8, (7), (6)]. Reconsider $E_3 = F_2$ as a splitting field of $X^{{p_2}^{n_2}} - P_2$. Consider g being a function from E_2 into E_3 such that g is isomorphism. $\square$

(60) Every finite field is a (PrimeField F)-normal, (PrimeField F)-separable extension of PrimeField F. The theorem is a consequence of (55).

8. Automorphisms of Finite Fields

Let F be a finite field and n be a natural number. Note that $(\mathrm{Frob}(F))^n$ is isomorphism and $\mathrm{Frob}(F)$ is isomorphism. Now we state the propositions:

(61) Let us consider a prime number p, a non zero natural number n, and a field F. Suppose $\overline{\overline{F}} = p^n$. Then $(\mathrm{Frob}(F))^n = \mathrm{id}_F$. The theorem is a consequence of (27) and (28).

(62) Let us consider a prime number p, a non zero natural number n, and a field F. Suppose $\overline{\overline{F}} = p^n$. Let us consider a natural number k. If $0 < k \leqslant n - 1$, then $(\mathrm{Frob}(F))^k \neq \mathrm{id}_F$. The theorem is a consequence of (27), (34), and (7).

(63) Let us consider a prime number p, a non zero natural number n, and a field F. Suppose $\overline{\overline{F}} = p^n$. Let us consider natural numbers m, k. Suppose $0 \leqslant m \leqslant n - 1$ and $0 \leqslant k \leqslant n - 1$ and $m \neq k$. Then $(\mathrm{Frob}(F))^m \neq (\mathrm{Frob}(F))^k$. The theorem is a consequence of (27), (6), (1), and (62).

Let us consider a prime number p, a non zero natural number n, and a field F. Now we state the propositions:

(64) Suppose $\overline{\overline{F}} = p^n$.

Then $\overline{\overline{\{(\mathrm{Frob}(F))^m, \text{ where } m \text{ is a natural number} : 0 \leqslant m \leqslant n - 1\}}} = n$.

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

(65) Suppose $\overline{\overline{F}} = p^n$. Then the set of all f where f is an automorphism of $F = \{(\mathrm{Frob}(F))^m$, where m is a natural number : $0 \leqslant m \leqslant n-1\}$.

PROOF: Set $P = \mathrm{PrimeField}\, F$. Reconsider $E = F$ as an P-finite extension of P. Consider a being an element of E such that $E \approx \mathrm{FAdj}(P, \{a\})$. Set $M =$ the set of all f where f is a P-fixing automorphism of $\mathrm{FAdj}(P, \{a\})$. $\overline{\overline{\{(\mathrm{Frob}(F))^m, \text{ where } m \text{ is a natural number} : 0 \leqslant m \leqslant n-1\}}} = n$. Reconsider $K = \{(\mathrm{Frob}(F))^m$, where m is a natural number : $0 \leqslant m \leqslant n-1\}$ as a finite set. $\overline{\overline{\mathrm{Roots}(\mathrm{FAdj}(P, \{a\}), \mathrm{MinPoly}(a, P))}} \leqslant \deg(\mathrm{MinPoly}(a, P))$. $M =$ the set of all f where f is an automorphism of $\mathrm{FAdj}(P, \{a\})$ by [13, (94)], (49). $K \subseteq M$. $\square$

9. GALOIS FIELDS – AS EXTENSIONS OF Z/p

Let p be a prime number and q be a power of p.

A Galois field of q is a finite field defined by

(Def. 8) order $it = q$ and $\mathbb{Z}/p$ is a subfield of it.

A Galois field of p is a Galois field of p^1. Let q be a power of p. Observe that there exists a Galois field of q which is strict and every Galois field of q is $(\mathbb{Z}/p)$-extending and has characteristic p. Now we state the propositions:

(66) Let us consider a prime number p. Then $\mathbb{Z}/p$ is a Galois field of p. The theorem is a consequence of (24).

(67) Let us consider a prime number p, and a Galois field F of p. Then $F \approx \mathbb{Z}/p$. The theorem is a consequence of (24).

(68) Let us consider a prime number p, and a strict Galois field F of p. Then $F = \mathbb{Z}/p$.

(69) Let us consider a field F. Then F is finite if and only if there exists a prime number p and there exists a non zero natural number n and there exists a Galois field G of p^n such that F and G are isomorphic. The theorem is a consequence of (59).

(70) Let us consider a prime number p, a non zero natural number n, and a Galois field F of p^n. Then $\mathrm{PrimeField}\, F = \mathbb{Z}/p$.

(71) Let us consider a prime number p, and a non zero natural number n. Then every Galois field of p^n is a splitting field of $X^{p^n} - (\mathbb{Z}/p)$. The theorem is a consequence of (70) and (55).

(72) Let us consider a prime number p, a non zero natural number n, and Galois fields F_1, F_2 of p^n. Then F_1 and F_2 are isomorphic over $\mathbb{Z}/p$. The theorem is a consequence of (71).

(73) Let us consider a prime number p, a non zero natural number n, and a Galois field F of p^n. Then $\deg(F, \mathbb{Z}/p) = n$. The theorem is a consequence of (24) and (7).

Let p be a prime number and n be a non zero natural number. One can check that every Galois field of p^n is $(\mathbb{Z}/p)$-finite and $(\mathbb{Z}/p)$-simple.

Let F be a Galois field of p^n and m be a natural number. One can verify that $(\mathrm{Frob}(F))^m$ is $(\mathbb{Z}/p)$-fixing and every automorphism of F is $(\mathbb{Z}/p)$-fixing and every Galois field of p^n is $(\mathbb{Z}/p)$-normal and $(\mathbb{Z}/p)$-separable.

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. Equality in computer proof-assistants. In Ganzha, Maria and Maciaszek, Leszek and Paprzycki, Marcin, editor, *Proceedings of the 2015 Federated Conference on Computer Science and Information Systems*, volume 5 of *ACSIS-Annals of Computer Science and Information Systems*, pages 45–54. IEEE, 2015. doi:10.15439/2015F229.

[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] Emin Karayel. Finite fields. *Archive of Formal Proofs*, 2022. `https://isa-afp.org/entries/Finite_Fields.html`, Formal proof development.

[7] Artur Korniłowicz. Flexary connectives in Mizar. *Computer Languages, Systems & Structures*, 44:238–250, December 2015. doi:10.1016/j.cl.2015.07.002.

[8] Artur Korniłowicz and Christoph Schwarzweller. The first isomorphism theorem and other properties of rings. *Formalized Mathematics*, 22(**4**):291–301, 2014. doi:10.2478/forma-2014-0029.

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

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

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

[12] Christoph Schwarzweller. Normal extensions. *Formalized Mathematics*, 31(1):121–130, 2023. doi:10.2478/forma-2023-0011.

[13] Christoph Schwarzweller and Artur Korniłowicz. Characteristic of rings. Prime fields. *Formalized Mathematics*, 23(**4**):333–349, 2015. doi:10.1515/forma-2015-0027.

Accepted December 27, 2024