FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 333–349, 2015
DOI: 10.1515/forma-2015-0027

DE GRUYTER OPEN
degruyter.com/view/j/forma

Characteristic of Rings. Prime Fields

Christoph Schwarzweller
Institute of Computer Science
University of Gdańsk
Poland

Artur Korniłowicz
Institute of Informatics
University of Białystok
Poland

Summary. The notion of the characteristic of rings and its basic properties are formalized [14], [39], [20]. Classification of prime fields in terms of isomorphisms with appropriate fields ($\mathbb{Q}$ or $\mathbb{Z}/p$) are presented. To facilitate reasonings within the field of rational numbers, values of numerators and denominators of basic operations over rationals are computed.

MSC: 13A35 12E05 03B35

Keywords: commutative algebra; characteristic of rings; prime field

MML identifier: RING_3, version: 8.1.04 5.34.1256

The notation and terminology used in this paper have been introduced in the following articles: [25], [27], [6], [31], [2], [21], [32], [12], [11], [7], [8], [13], [28], [35], [37], [1], [34], [19], [29], [26], [33], [22], [3], [4], [9], [30], [15], [5], [40], [23], [16], [36], [38], [17], [18], [24], and [10].

1. Preliminaries

Now we state the propositions:

(1) Let us consider a function f, a set A, and objects a, b. If $a, b \in A$, then $(f \restriction A)(a,b) = f(a,b)$.

(2) $+_{\mathbb{C}} \restriction \mathbb{R} = +_{\mathbb{R}}$.
Proof: Set $c = +_{\mathbb{C}} \restriction \mathbb{R}$. For every object z such that $z \in \operatorname{dom} c$ holds $c(z) = +_{\mathbb{R}}(z)$ by [7, (49)]. □

(3) $\cdot_{\mathbb{C}} \restriction \mathbb{R} = \cdot_{\mathbb{R}}$.
Proof: Set $d = \cdot_{\mathbb{C}} \restriction \mathbb{R}$. For every object z such that $z \in \operatorname{dom} d$ holds $d(z) = \cdot_{\mathbb{R}}(z)$ by [7, (49)]. □

(4) $+_{\mathbb{Q}} \restriction \mathbb{Z} = +_{\mathbb{Z}}$.
PROOF: Set $c = +_{\mathbb{Q}} \restriction \mathbb{Z}$. For every object z such that $z \in \operatorname{dom} c$ holds $c(z) = (+_{\mathbb{Z}})(z)$ by [7, (49)]. $\square$

(5) $\cdot_{\mathbb{Q}} \restriction \mathbb{Z} = \cdot_{\mathbb{Z}}$.
PROOF: Set $d = \cdot_{\mathbb{Q}} \restriction \mathbb{Z}$. For every object z such that $z \in \operatorname{dom} d$ holds $d(z) = \cdot_{\mathbb{Z}}(z)$ by [7, (49)]. $\square$

2. Properties of Fractions

From now on p, q denote rational numbers, g, m, m_1, m_2, n, n_1, n_2 denote natural numbers, and i, j denote integers.

Now we state the propositions:

(6) If $n \mid i$, then $i \operatorname{div} n = \frac{i}{n}$.

(7) $i \operatorname{div}(\gcd(i, n)) = \frac{i}{\gcd(i,n)}$. The theorem is a consequence of (6).

(8) $n \operatorname{div}(\gcd(n, i)) = \frac{n}{\gcd(n,i)}$. The theorem is a consequence of (6).

(9) If $g \mid i$ and $g \mid m$, then $\frac{i}{m} = \frac{i \operatorname{div} g}{m \operatorname{div} g}$.

(10) $\frac{i}{m} = \frac{i \operatorname{div}(\gcd(i,m))}{m \operatorname{div}(\gcd(i,m))}$. The theorem is a consequence of (9).

(11) If $0 < m$ and $m \cdot i \mid m$, then $i = 1$ or $i = -1$.

(12) If $0 < m$ and $m \cdot n \mid m$, then $n = 1$.

(13) If $m \mid i$, then $i \operatorname{div} m \mid i$. The theorem is a consequence of (6).

Let us assume that $m \neq 0$. Now we state the propositions:

(14) $\gcd(i \operatorname{div}(\gcd(i, m)), m \operatorname{div}(\gcd(i, m))) = 1$. The theorem is a consequence of (6) and (11).

(15) (i) $\operatorname{den}(\frac{i}{m}) = m \operatorname{div}(\gcd(i, m))$, and
(ii) $\operatorname{num}(\frac{i}{m}) = i \operatorname{div}(\gcd(i, m))$.
The theorem is a consequence of (10) and (14).

(16) (i) $\operatorname{den}(\frac{i}{m}) = \frac{m}{\gcd(i,m)}$, and
(ii) $\operatorname{num}(\frac{i}{m}) = \frac{i}{\gcd(i,m)}$.
The theorem is a consequence of (15), (8), and (7).

(17) (i) $\operatorname{den}(-(\frac{i}{m})) = m \operatorname{div}(\gcd(-i, m))$, and
(ii) $\operatorname{num}(-(\frac{i}{m})) = -i \operatorname{div}(\gcd(-i, m))$.
The theorem is a consequence of (15).

(18) (i) $\operatorname{den}(-(\frac{i}{m})) = \frac{m}{\gcd(-i,m)}$, and
(ii) $\operatorname{num}(-(\frac{i}{m})) = \frac{-i}{\gcd(-i,m)}$.
The theorem is a consequence of (17), (8), and (7).

(19) (i) $\mathrm{den}(\frac{m}{i})^{-1} = m \,\mathrm{div}(\gcd(m, i))$, and

(ii) $\mathrm{num}(\frac{m}{i})^{-1} = i \,\mathrm{div}(\gcd(m, i))$.

The theorem is a consequence of (15).

(20) (i) $\mathrm{den}(\frac{m}{i})^{-1} = \frac{m}{\gcd(m,i)}$, and

(ii) $\mathrm{num}(\frac{m}{i})^{-1} = \frac{i}{\gcd(m,i)}$.

The theorem is a consequence of (19), (8), and (7).

Let us assume that $m \neq 0$ and $n \neq 0$. Now we state the propositions:

(21) (i) $\mathrm{den}((\frac{i}{m}) + (\frac{j}{n})) = m \cdot n \,\mathrm{div}(\gcd(i \cdot n + j \cdot m, m \cdot n))$, and

(ii) $\mathrm{num}((\frac{i}{m}) + (\frac{j}{n})) = i \cdot n + j \cdot m \,\mathrm{div}(\gcd(i \cdot n + j \cdot m, m \cdot n))$.

The theorem is a consequence of (15).

(22) (i) $\mathrm{den}((\frac{i}{m}) + (\frac{j}{n})) = \frac{m \cdot n}{\gcd(i \cdot n + j \cdot m, m \cdot n)}$, and

(ii) $\mathrm{num}((\frac{i}{m}) + (\frac{j}{n})) = \frac{i \cdot n + j \cdot m}{\gcd(i \cdot n + j \cdot m, m \cdot n)}$.

The theorem is a consequence of (21), (8), and (7).

(23) (i) $\mathrm{den}((\frac{i}{m}) - (\frac{j}{n})) = m \cdot n \,\mathrm{div}(\gcd(i \cdot n - j \cdot m, m \cdot n))$, and

(ii) $\mathrm{num}((\frac{i}{m}) - (\frac{j}{n})) = i \cdot n - j \cdot m \,\mathrm{div}(\gcd(i \cdot n - j \cdot m, m \cdot n))$.

The theorem is a consequence of (15).

(24) (i) $\mathrm{den}((\frac{i}{m}) - (\frac{j}{n})) = \frac{m \cdot n}{\gcd(i \cdot n - j \cdot m, m \cdot n)}$, and

(ii) $\mathrm{num}((\frac{i}{m}) - (\frac{j}{n})) = \frac{i \cdot n - j \cdot m}{\gcd(i \cdot n - j \cdot m, m \cdot n)}$.

The theorem is a consequence of (23), (8), and (7).

(25) (i) $\mathrm{den}((\frac{i}{m}) \cdot (\frac{j}{n})) = m \cdot n \,\mathrm{div}(\gcd(i \cdot j, m \cdot n))$, and

(ii) $\mathrm{num}((\frac{i}{m}) \cdot (\frac{j}{n})) = i \cdot j \,\mathrm{div}(\gcd(i \cdot j, m \cdot n))$.

The theorem is a consequence of (15).

(26) (i) $\mathrm{den}((\frac{i}{m}) \cdot (\frac{j}{n})) = \frac{m \cdot n}{\gcd(i \cdot j, m \cdot n)}$, and

(ii) $\mathrm{num}((\frac{i}{m}) \cdot (\frac{j}{n})) = \frac{i \cdot j}{\gcd(i \cdot j, m \cdot n)}$.

The theorem is a consequence of (25), (8), and (7).

(27) (i) $\mathrm{den}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = m \cdot n \,\mathrm{div}(\gcd(i \cdot j, m \cdot n))$, and

(ii) $\mathrm{num}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = i \cdot j \,\mathrm{div}(\gcd(i \cdot j, m \cdot n))$.

The theorem is a consequence of (15).

(28) (i) $\mathrm{den}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = \frac{m \cdot n}{\gcd(i \cdot j, m \cdot n)}$, and

(ii) $\mathrm{num}(\frac{(\frac{i}{m})}{(\frac{n}{j})}) = \frac{i \cdot j}{\gcd(i \cdot j, m \cdot n)}$.

The theorem is a consequence of (27), (8), and (7).

Now we state the propositions:

(29) $\operatorname{den} p = \operatorname{den} p \operatorname{div}(\gcd(\operatorname{num} p, \operatorname{den} p))$. The theorem is a consequence of (15).

(30) $\operatorname{num} p = \operatorname{num} p \operatorname{div}(\gcd(\operatorname{num} p, \operatorname{den} p))$. The theorem is a consequence of (15).

Let us assume that $m = \operatorname{den} p$ and $i = \operatorname{num} p$. Now we state the propositions:

(31) (i) $\operatorname{den}(-p) = m \operatorname{div}(\gcd(-i, m))$, and

(ii) $\operatorname{num}(-p) = -i \operatorname{div}(\gcd(-i, m))$.

The theorem is a consequence of (17).

(32) (i) $\operatorname{den}(-p) = \frac{m}{\gcd(-i,m)}$, and

(ii) $\operatorname{num}(-p) = \frac{-i}{\gcd(-i,m)}$.

The theorem is a consequence of (31), (8), and (7).

Let us assume that $m = \operatorname{den} p$ and $n = \operatorname{num} p$ and $n \neq 0$. Now we state the propositions:

(33) (i) $\operatorname{den} p^{-1} = n \operatorname{div}(\gcd(n, m))$, and

(ii) $\operatorname{num} p^{-1} = m \operatorname{div}(\gcd(n, m))$.

The theorem is a consequence of (19).

(34) (i) $\operatorname{den} p^{-1} = \frac{n}{\gcd(n,m)}$, and

(ii) $\operatorname{num} p^{-1} = \frac{m}{\gcd(n,m)}$.

The theorem is a consequence of (33), (8), and (7).

Let us assume that $m = \operatorname{den} p$ and $n = \operatorname{den} q$ and $i = \operatorname{num} p$ and $j = \operatorname{num} q$. Now we state the propositions:

(35) (i) $\operatorname{den}(p + q) = m \cdot n \operatorname{div}(\gcd(i \cdot n + j \cdot m, m \cdot n))$, and

(ii) $\operatorname{num}(p + q) = i \cdot n + j \cdot m \operatorname{div}(\gcd(i \cdot n + j \cdot m, m \cdot n))$.

The theorem is a consequence of (21).

(36) (i) $\operatorname{den}(p + q) = \frac{m \cdot n}{\gcd(i \cdot n + j \cdot m, m \cdot n)}$, and

(ii) $\operatorname{num}(p + q) = \frac{i \cdot n + j \cdot m}{\gcd(i \cdot n + j \cdot m, m \cdot n)}$.

The theorem is a consequence of (35), (8), and (7).

(37) (i) $\operatorname{den}(p - q) = m \cdot n \operatorname{div}(\gcd(i \cdot n - j \cdot m, m \cdot n))$, and

(ii) $\operatorname{num}(p - q) = i \cdot n - j \cdot m \operatorname{div}(\gcd(i \cdot n - j \cdot m, m \cdot n))$.

The theorem is a consequence of (23).

(38) (i) $\operatorname{den}(p - q) = \frac{m \cdot n}{\gcd(i \cdot n - j \cdot m, m \cdot n)}$, and

(ii) $\operatorname{num}(p - q) = \frac{i \cdot n - j \cdot m}{\gcd(i \cdot n - j \cdot m, m \cdot n)}$.

The theorem is a consequence of (37), (8), and (7).

(39) (i) $\operatorname{den}(p \cdot q) = m \cdot n \operatorname{div}(\gcd(i \cdot j, m \cdot n))$, and

(ii) $\mathrm{num}(p \cdot q) = i \cdot j \,\mathrm{div}(\gcd(i \cdot j, m \cdot n))$.

The theorem is a consequence of (25).

(40) (i) $\mathrm{den}(p \cdot q) = \frac{m \cdot n}{\gcd(i \cdot j, m \cdot n)}$, and

(ii) $\mathrm{num}(p \cdot q) = \frac{i \cdot j}{\gcd(i \cdot j, m \cdot n)}$.

The theorem is a consequence of (39), (8), and (7).

Let us assume that $m_1 = \mathrm{den}\, p$ and $m_2 = \mathrm{den}\, q$ and $n_1 = \mathrm{num}\, p$ and $n_2 = \mathrm{num}\, q$ and $n_2 \neq 0$. Now we state the propositions:

(41) (i) $\mathrm{den}(\frac{p}{q}) = m_1 \cdot n_2 \,\mathrm{div}(\gcd(n_1 \cdot m_2, m_1 \cdot n_2))$, and

(ii) $\mathrm{num}(\frac{p}{q}) = n_1 \cdot m_2 \,\mathrm{div}(\gcd(n_1 \cdot m_2, m_1 \cdot n_2))$.

The theorem is a consequence of (27).

(42) (i) $\mathrm{den}(\frac{p}{q}) = \frac{m_1 \cdot n_2}{\gcd(n_1 \cdot m_2, m_1 \cdot n_2)}$, and

(ii) $\mathrm{num}(\frac{p}{q}) = \frac{n_1 \cdot m_2}{\gcd(n_1 \cdot m_2, m_1 \cdot n_2)}$.

The theorem is a consequence of (41), (8), and (7).

3. Preliminaries about Rings and Fields

In the sequel R denotes a ring and F denotes a field.

Let us note that there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is positive and there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is negative.

Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x + y$ with $a + b$. We identify $x \cdot y$ with $a \cdot b$. Let a be an element of $\mathbb{F}_{\mathbb{Q}}$ and x be a rational number. We identify $-x$ with $-a$. Let a be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. We identify x^{-1} with a^{-1}. Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x - y$ with $a - b$. Let a be an element of $\mathbb{F}_{\mathbb{Q}}$ and b be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. We identify $\frac{x}{y}$ with $\frac{a}{b}$. Let F be a field. Let us observe that $(1_F)^{-1}$ reduces to 1_F.

Let R, S be rings. We say that R includes an isomorphic copy of S if and only if

(Def. 1) there exists a strict subring T of R such that T and S are isomorphic.

We introduce the notation R includes S as a synonym of R includes an isomorphic copy of S.

Let us observe that the predicate R and S are isomorphic is reflexive.

Now we state the propositions:

(43) Let us consider a field E. Then every subfield of E is a subring of E.

(44) Let us consider rings R, S, T. If R and S are isomorphic and S and T are isomorphic, then R and T are isomorphic.

(45) Let us consider a field F, and a subring R of F. Then R is a subfield of F if and only if R is a field.

(46) Let us consider a field E, and a strict subfield F of E. Then E includes F.

(47) $\mathbb{Z}^{\mathrm{R}}$ is a subring of $\mathbb{F}_{\mathbb{Q}}$.

(48) $\mathbb{R}_{\mathrm{F}}$ is a subfield of $\mathbb{C}_{\mathrm{F}}$.

Let R be an integral domain. Observe that there exists an integral domain which is R-homomorphic and there exists a commutative ring which is R-homomorphic and there exists a ring which is R-homomorphic.

Let R be a field. Let us note that there exists an integral domain which is R-homomorphic.

Let F be a field, R be an F-homomorphic ring, and f be a homomorphism from F to R. Note that $\mathrm{Im}\, f$ is almost left invertible.

Let F be an integral domain, E be an F-homomorphic integral domain, and f be a homomorphism from F to E. Note that $\mathrm{Im}\, f$ is non degenerated.

Let us consider a ring R, an R-homomorphic ring E, a subring K of R, a function f from R into E, and a function g from K into E. Now we state the propositions:

(49) If $g = f \restriction$(the carrier of K) and f is additive, then g is additive. The theorem is a consequence of (1).

(50) If $g = f \restriction$(the carrier of K) and f is multiplicative, then g is multiplicative. The theorem is a consequence of (1).

(51) If $g = f \restriction$(the carrier of K) and f is unity-preserving, then g is unity-preserving.

Now we state the propositions:

(52) Let us consider a ring R, an R-homomorphic ring E, and a subring K of R. Then E is K-homomorphic. The theorem is a consequence of (49), (50), and (51).

(53) Let us consider a ring R, an R-homomorphic ring E, a subring K of R, a K-homomorphic ring E_1, and a homomorphism f from R to E. If $E = E_1$, then $f \restriction K$ is a homomorphism from K to E_1. The theorem is a consequence of (49), (50), and (51).

Let us consider a field F, an F-homomorphic field E, a subfield K of F, a function f from F into E, and a function g from K into E. Now we state the propositions:

(54) If $g = f \restriction$(the carrier of K) and f is additive, then g is additive. The theorem is a consequence of (1).

(55) If $g = f\restriction$(the carrier of K) and f is multiplicative, then g is multiplicative. The theorem is a consequence of (1).

(56) If $g = f\restriction$(the carrier of K) and f is unity-preserving, then g is unity-preserving.

Now we state the propositions:

(57) Let us consider a field F, an F-homomorphic field E, and a subfield K of F. Then E is K-homomorphic. The theorem is a consequence of (54), (55), and (56).

(58) Let us consider a field F, an F-homomorphic field E, a subfield K of F, a K-homomorphic field E_1, and a homomorphism f from F to E. If $E = E_1$, then $f\restriction K$ is a homomorphism from K to E_1. The theorem is a consequence of (54), (55), and (56).

Let n be a natural number. We introduce the notation $\mathbb{Z}/n$ as a synonym of $\mathbb{Z}_n^{\mathrm{R}}$.

One can verify that $\mathbb{Z}/n$ is finite.

Let n be a non trivial natural number. One can check that $\mathbb{Z}/n$ is non degenerated.

Let n be a positive natural number. Note that $\mathbb{Z}/n$ is Abelian, add-associative, right zeroed, and right complementable and $\mathbb{Z}/n$ is associative, well unital, distributive, and commutative.

Let p be a prime number. Observe that $\mathbb{Z}/p$ is almost left invertible.

4. Embedding the Integers in Rings

Let R be an add-associative, right zeroed, right complementable, non empty double loop structure, a be an element of R, and i be an integer. The functor $i \star a$ yielding an element of R is defined by

(Def. 2) there exists a natural number n such that $i = n$ and $it = n \cdot a$ or $i = -n$ and $it = -n \cdot a$.

Let us consider an add-associative, right zeroed, right complementable, non empty double loop structure R and an element a of R. Now we state the propositions:

(59) $0 \star a = 0_R$.

(60) $1 \star a = a$.

(61) $(-1) \star a = -a$.

Now we state the propositions:

(62) Let us consider an add-associative, right zeroed, right complementable, Abelian, non empty double loop structure R, an element a of R, and integers i, j. Then $(i+j) \star a = i \star a + j \star a$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer k such that $k = \$_1$ holds $(i+k) \star a = i \star a + k \star a$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [36, (8)]. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(63) Let us consider an add-associative, right zeroed, right complementable, Abelian, non empty double loop structure R, an element a of R, and an integer i. Then $(-i) \star a = -i \star a$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer k such that $k = \$_1$ holds $(-k) \star a = -k \star a$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [36, (33), (30)]. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

Let us consider an add-associative, right zeroed, right complementable, Abelian, non empty double loop structure R, an element a of R, and integers i, j. Now we state the propositions:

(64) $(i-j) \star a = i \star a - j \star a$. The theorem is a consequence of (62) and (63).

(65) $i \cdot j \star a = i \star (j \star a)$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer k such that $k = \$_1$ holds $k \cdot j \star a = k \star (j \star a)$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(66) $i \star (j \star a) = j \star (i \star a)$. The theorem is a consequence of (65).

Now we state the propositions:

(67) Let us consider an add-associative, right zeroed, right complementable, Abelian, left unital, distributive, non empty double loop structure R, and integers i, j. Then $i \cdot j \star 1_R = (i \star 1_R) \cdot (j \star 1_R)$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer k such that $k = \$_1$ holds $k \cdot j \star 1_R = (k \star 1_R) \cdot (j \star 1_R)$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by (64), [18, (9)], (60), (62). For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(68) Let us consider a ring R, an R-homomorphic ring S, a homomorphism f from R to S, an element a of R, and an integer i. Then $f(i \star a) = i \star f(a)$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer j such that $j = \$_1$ holds $f(j \star a) = j \star f(a)$. For every integer i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i-1]$ and $\mathcal{P}[i+1]$ by (62), (60), [36, (8)], (61). For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

5. Mono- and Isomorphisms of Rings

Let R, S be rings. We say that S is R-monomorphic if and only if

(Def. 3) there exists a function f from R into S such that f is monomorphic.

Let R be a ring. Note that there exists a ring which is R-monomorphic.

Let R be a commutative ring. One can check that there exists a commutative ring which is R-monomorphic and there exists a ring which is R-monomorphic.

Let R be an integral domain. One can verify that there exists an integral domain which is R-monomorphic and there exists a commutative ring which is R-monomorphic and there exists a ring which is R-monomorphic.

Let R be a field. Let us observe that there exists a field which is R-monomorphic and there exists an integral domain which is R-monomorphic and there exists a commutative ring which is R-monomorphic and there exists a ring which is R-monomorphic.

Let R be a ring and S be an R-monomorphic ring. Let us note that there exists a function from R into S which is additive, multiplicative, unity-preserving, and monomorphic.

A monomorphism of R and S is an additive, multiplicative, unity-preserving, monomorphic function from R into S. One can check that every S-monomorphic ring is R-monomorphic and every R-monomorphic ring is R-homomorphic.

Let S be an R-monomorphic ring and f be a monomorphism of R and S. Let us note that $(f^{-1})^{-1}$ reduces to f.

Now we state the propositions:

(69) Let us consider a ring R, an R-homomorphic ring S, an S-homomorphic ring T, a homomorphism f from R to S, and a homomorphism g from S to T. Then $\ker f \subseteq \ker g \cdot f$.

(70) Let us consider a ring R, an R-homomorphic ring S, an S-monomorphic ring T, a homomorphism f from R to S, and a monomorphism g of S and T. Then $\ker f = \ker g \cdot f$. The theorem is a consequence of (69).

(71) Let us consider a ring R, and a subring S of R. Then R is S-monomorphic.

(72) Let us consider rings R, S. Then S is an R-monomorphic ring if and only if S includes R. The theorem is a consequence of (44).

Let R, S be rings. We say that S is R-isomorphic if and only if

(Def. 4) there exists a function f from R into S such that f is isomorphism.

Let R be a ring. Let us note that there exists a ring which is R-isomorphic.

Let R be a commutative ring. Note that there exists a commutative ring which is R-isomorphic and there exists a ring which is R-isomorphic.

Let R be an integral domain. One can check that there exists an integral domain which is R-isomorphic and there exists a commutative ring which is

R-isomorphic and there exists a ring which is R-isomorphic.

Let R be a field. One can verify that there exists a field which is R-isomorphic and there exists an integral domain which is R-isomorphic and there exists a commutative ring which is R-isomorphic and there exists a ring which is R-isomorphic.

Let R be a ring and S be an R-isomorphic ring. Observe that there exists a function from R into S which is additive, multiplicative, unity-preserving, and isomorphism.

An isomorphism between R and S is an additive, multiplicative, unity-preserving, isomorphism function from R into S. Let f be an isomorphism between R and S. Let us note that the functor f^{-1} yields a function from S into R. One can check that there exists a function from S into R which is additive, multiplicative, unity-preserving, and isomorphism.

An isomorphism between S and R is an additive, multiplicative, unity-preserving, isomorphism function from S into R. One can check that every S-isomorphic ring is R-isomorphic and every R-isomorphic ring is R-monomorphic.

Now we state the propositions:

(73) Let us consider a ring R, an R-isomorphic ring S, and an isomorphism f between R and S. Then f^{-1} is an isomorphism between S and R.

(74) Let us consider a ring R, and an R-isomorphic ring S. Then R is S-isomorphic. The theorem is a consequence of (73).

Let R be a commutative ring. Let us note that every R-isomorphic ring is commutative. Let R be an integral domain. One can check that every R-isomorphic ring is non degenerated and integral domain-like.

Let F be a field. One can verify that every F-isomorphic ring is almost left invertible.

(75) Let us consider fields E, F. Then E includes F if and only if there exists a strict subfield K of E such that K and F are isomorphic.

6. Characteristic of Rings

Let R be a ring. The functor $\mathrm{char}(R)$ yielding a natural number is defined by

(Def. 5) $it \star 1_R = 0_R$ and $it \neq 0$ and for every positive natural number m such that $m < it$ holds $m \star 1_R \neq 0_R$ or $it = 0$ and for every positive natural number m, $m \star 1_R \neq 0_R$.

Let n be a natural number. We say that R has characteristic n if and only if

(Def. 6) $\mathrm{char}(R) = n$.

Now we state the propositions:

(76) $\mathrm{char}(\mathbb{Z}^{\mathrm{R}}) = 0$.

(77) Let us consider a positive natural number n. Then $\mathrm{char}(\mathbb{Z}/n) = n$. The theorem is a consequence of (60) and (59).

Observe that $\mathbb{Z}^{\mathrm{R}}$ has characteristic 0.

Let n be a positive natural number. Note that $\mathbb{Z}/n$ has characteristic n.

Let n be a natural number. One can check that there exists a commutative ring which has characteristic n.

Let n be a positive natural number and R be a ring with characteristic n. Let us note that $\mathrm{char}(R)$ is positive.

Let R be a ring. The functor $\mathrm{charSet}\, R$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 7) $\{n$, where n is a positive natural number : $n \star 1_R = 0_R\}$.

Let n be a positive natural number and R be a ring with characteristic n. Note that $\mathrm{charSet}\, R$ is non empty.

Now we state the propositions:

(78) Let us consider a ring R. Then $\mathrm{char}(R) = 0$ if and only if $\mathrm{charSet}\, R = \emptyset$.

(79) Let us consider a positive natural number n, and a ring R with characteristic n. Then $\mathrm{char}(R) = \min \mathrm{charSet}\, R$.

(80) Let us consider a ring R. Then $\mathrm{char}(R) = \min^* \mathrm{charSet}\, R$. The theorem is a consequence of (78) and (79).

(81) Let us consider a prime number p, a ring R with characteristic p, and a positive natural number n. Then n is an element of $\mathrm{charSet}\, R$ if and only if $p \mid n$. The theorem is a consequence of (67), (62), and (79).

Let R be a ring. The functor $\mathrm{canHom}\mathbb{Z}(R)$ yielding a function from $\mathbb{Z}^{\mathrm{R}}$ into R is defined by

(Def. 8) for every element x of $\mathbb{Z}^{\mathrm{R}}$, $it(x) = x \star 1_R$.

Observe that $\mathrm{canHom}\mathbb{Z}(R)$ is additive, multiplicative, and unity-preserving and every ring is $(\mathbb{Z}^{\mathrm{R}})$-homomorphic.

Now we state the propositions:

(82) Let us consider a ring R, and a non negative element n of $\mathbb{Z}^{\mathrm{R}}$. Then $\mathrm{char}(R) = n$ if and only if $\ker \mathrm{canHom}\mathbb{Z}(R) = \{n\}$–ideal. The theorem is a consequence of (64), (63), and (80).

(83) Let us consider a ring R. Then $\mathrm{char}(R) = 0$ if and only if $\mathrm{canHom}\mathbb{Z}(R)$ is monomorphic. The theorem is a consequence of (82).

Let R be a ring with characteristic 0. Observe that $\mathrm{canHom}\mathbb{Z}(R)$ is monomorphic and there exists a function from $\mathbb{Z}^{\mathrm{R}}$ into R which is additive, multiplicative, unity-preserving, and monomorphic.

Now we state the propositions:

(84) Let us consider a ring R, and a homomorphism f from $\mathbb{Z}^{\mathrm{R}}$ to R. Then $f = \mathrm{canHom}\mathbb{Z}(R)$.
PROOF: Define $\mathcal{P}[\text{integer}] \equiv$ for every integer j such that $j = \$_1$ holds $f(j) = j \star 1_R$. For every integer u such that $\mathcal{P}[u]$ holds $\mathcal{P}[u-1]$ and $\mathcal{P}[u+1]$ by [16, (8)], (60), (64), (62). For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. □

(85) Let us consider a homomorphism f from $\mathbb{Z}^{\mathrm{R}}$ to $\mathbb{Z}^{\mathrm{R}}$. Then $f = \mathrm{id}_{\mathbb{Z}^{\mathrm{R}}}$. The theorem is a consequence of (84).

(86) Let us consider an integral domain R. Then

(i) $\mathrm{char}(R) = 0$, or

(ii) $\mathrm{char}(R)$ is prime.

The theorem is a consequence of (60) and (67).

(87) Let us consider a ring R, and an R-homomorphic ring S. Then $\mathrm{char}(S) \mid \mathrm{char}(R)$. The theorem is a consequence of (84), (69), and (82).

(88) Let us consider a ring R, and an R-monomorphic ring S. Then $\mathrm{char}(S) = \mathrm{char}(R)$. The theorem is a consequence of (84), (70), and (82).

(89) Let us consider a ring R, and a subring S of R. Then $\mathrm{char}(S) = \mathrm{char}(R)$. The theorem is a consequence of (71) and (88).

Let n be a natural number and R be a ring with characteristic n. One can verify that every ring which is R-monomorphic has also characteristic n and every subring of R has characteristic n and $\mathbb{C}_{\mathrm{F}}$ has characteristic 0 and $\mathbb{R}_{\mathrm{F}}$ has characteristic 0 and $\mathbb{F}_{\mathbb{Q}}$ has characteristic 0 and there exists a field which has characteristic 0.

Let p be a prime number. Let us note that there exists a field which has characteristic p. Let R be an integral domain with characteristic p. One can verify that $\mathrm{char}(R)$ is prime.

Let F be a field with characteristic 0. Note that every subfield of F has characteristic 0. Let p be a prime number and F be a field with characteristic p. Note that every subfield of F has characteristic p.

7. Prime Fields

Let F be a field. The functor carrier $\cap F$ yielding a subset of F is defined by the term

(Def. 9) $\{x$, where x is an element of F : for every subfield K of F, $x \in K\}$.

The functor PrimeField F yielding a strict double loop structure is defined by

(Def. 10) the carrier of it = carrier $\cap F$ and the addition of it = (the addition of F) $\restriction$ carrier $\cap F$ and the multiplication of it = (the multiplication of F) $\restriction$ carrier $\cap F$ and the one of $it = 1_F$ and the zero of $it = 0_F$.

One can verify that PrimeField F is non degenerated and PrimeField F is Abelian, add-associative, right zeroed, and right complementable and PrimeField F is commutative and PrimeField F is associative, well unital, distributive, and almost left invertible.

Let us note that the functor PrimeField F yields a strict subfield of F. Now we state the propositions:

(90) Let us consider a field F, and a strict subfield E of PrimeField F. Then $E =$ PrimeField F.

(91) Let us consider a field F, and a subfield E of F. Then PrimeField F is a subfield of E.

Let us consider fields F, K. Now we state the propositions:

(92) $K =$ PrimeField F if and only if K is a strict subfield of F and for every strict subfield E of K, $E = K$. The theorem is a consequence of (91) and (90).

(93) $K =$ PrimeField F if and only if K is a strict subfield of F and for every subfield E of F, K is a subfield of E. The theorem is a consequence of (91).

Now we state the propositions:

(94) Let us consider a field E, and a subfield F of E. Then PrimeField F = PrimeField E. The theorem is a consequence of (93) and (92).

(95) Let us consider a field F. Then PrimeField PrimeField F = PrimeField F.

Let F be a field. Let us observe that PrimeField F is prime.

Now we state the propositions:

(96) Let us consider a field F. Then F is prime if and only if $F =$ PrimeField F.

(97) Let us consider a field F with characteristic 0, and non zero integers i, j. Suppose $j \mid i$. Then $(i \operatorname{div} j) \star 1_F = (i \star 1_F) \cdot (j \star 1_F)^{-1}$.

PROOF: Consider k being an integer such that $i = j \cdot k$. $j \star 1_F \neq 0_F$ by [34, (3)], (63), [36, (17)]. $i \star 1_F \neq 0_F$ by [34, (3)], (63), [36, (17)]. $\square$

Let x be an element of $\mathbb{F}_{\mathbb{Q}}$. Note that the functor den x yields a positive element of $\mathbb{Z}^{\mathrm{R}}$. One can check that the functor num x yields an element of $\mathbb{Z}^{\mathrm{R}}$. Let F be a field. The functor canHom$\mathbb{Q}(F)$ yielding a function from $\mathbb{F}_{\mathbb{Q}}$ into F is defined by

(Def. 11) for every element x of $\mathbb{F}_{\mathbb{Q}}$, $it(x) = \frac{(\operatorname{canHom}\mathbb{Z}(F))(\operatorname{num} x)}{(\operatorname{canHom}\mathbb{Z}(F))(\operatorname{den} x)}$.

Observe that canHom$\mathbb{Q}(F)$ is unity-preserving.

Let F be a field with characteristic 0. One can check that canHom$\mathbb{Q}(F)$ is additive and multiplicative and every field with characteristic 0 is $(\mathbb{F}_{\mathbb{Q}})$-monomorphic.

Now we state the proposition:

(98) Let us consider a field F. Then canHom$\mathbb{Z}(F) =$ canHom$\mathbb{Q}(F)\restriction\mathbb{Z}$.

Let us observe that there exists a field which is $(\mathbb{F}_{\mathbb{Q}})$-homomorphic and has characteristic 0.

Now we state the proposition:

(99) Let us consider an $(\mathbb{F}_{\mathbb{Q}})$-homomorphic field F with characteristic 0, and a homomorphism f from $\mathbb{F}_{\mathbb{Q}}$ to F. Then $f =$ canHom$\mathbb{Q}(F)$.
PROOF: Set $g =$ canHom$\mathbb{Q}(F)$. Define $\mathcal{P}[\text{integer}] \equiv$ for every element j of $\mathbb{F}_{\mathbb{Q}}$ such that $j = \$_1$ holds $f(j) = g(j)$. For every integer i, $\mathcal{P}[i]$ from [34, Sch. 4]. For every integer i and for every element j of $\mathbb{F}_{\mathbb{Q}}$ such that $j = i$ holds $f(j) = (\text{canHom}\mathbb{Z}(F))(i)$ by (98), [7, (49)]. □

One can verify that $\mathbb{F}_{\mathbb{Q}}$ is $(\mathbb{F}_{\mathbb{Q}})$-homomorphic.

Let F be a field with characteristic 0. One can verify that PrimeField F is $(\mathbb{F}_{\mathbb{Q}})$-homomorphic.

Now we state the proposition:

(100) Let us consider a homomorphism f from $\mathbb{F}_{\mathbb{Q}}$ to $\mathbb{F}_{\mathbb{Q}}$. Then $f = \mathrm{id}_{\mathbb{F}_{\mathbb{Q}}}$. The theorem is a consequence of (99).

Let F be a field, S be an F-homomorphic field, and f be a homomorphism from F to S. One can verify that the functor Im f yields a strict subfield of S. Let F be a field with characteristic 0. Let us note that canHom$\mathbb{Q}$(PrimeField F) is onto.

Now we state the propositions:

(101) Let us consider a field F with characteristic 0. Then $\mathbb{F}_{\mathbb{Q}}$ and PrimeField F are isomorphic.

(102) PrimeField $\mathbb{F}_{\mathbb{Q}} = \mathbb{F}_{\mathbb{Q}}$.

(103) Let us consider a field F with characteristic 0. Then F includes $\mathbb{F}_{\mathbb{Q}}$.

(104) Let us consider a field F with characteristic 0, and a field E. If F includes E, then E includes $\mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (72) and (88).

(105) Let us consider a prime number p, a ring R with characteristic p, and an integer i. Then $i \star 1_R = (i \bmod p) \star 1_R$. The theorem is a consequence of (67) and (62).

Let p be a prime number and F be a field. The functor canHom$\mathbb{Z}/p(F)$ yielding a function from $\mathbb{Z}/p$ into F is defined by the term

(Def. 12) canHom$\mathbb{Z}(F)\restriction$(the carrier of $\mathbb{Z}/p$).

Note that canHom$\mathbb{Z}/p(F)$ is unity-preserving.

Let F be a field with characteristic p. One can verify that $\mathrm{canHom}\mathbb{Z}/p(F)$ is additive and multiplicative and every field with characteristic p is $(\mathbb{Z}/p)$-monomorphic and there exists a field which is $(\mathbb{Z}/p)$-homomorphic and has characteristic p and $\mathbb{Z}/p$ is $(\mathbb{Z}/p)$-homomorphic.

Now we state the propositions:

(106) Let us consider a prime number p, a $(\mathbb{Z}/p)$-homomorphic field F with characteristic p, and a homomorphism f from $\mathbb{Z}/p$ to F. Then $f = \mathrm{canHom}\mathbb{Z}/p(F)$.

Proof: Set $g = \mathrm{canHom}\mathbb{Z}/p(F)$. Reconsider $p_1 = p - 1$ as an element of $\mathbb{N}$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every element j of $\mathbb{Z}/p$ such that $j = \$_1$ holds $f(j) = g(j)$. For every element k of $\mathbb{N}$ such that $0 \leqslant k < p_1$ holds if $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by [3, (13), (44)], [29, (14), (7)]. For every element k of $\mathbb{N}$ such that $0 \leqslant k \leqslant p_1$ holds $\mathcal{P}[k]$ from [34, Sch. 7]. □

(107) Let us consider a prime number p, and a homomorphism f from $\mathbb{Z}/p$ to $\mathbb{Z}/p$. Then $f = \mathrm{id}_{\mathbb{Z}/p}$. The theorem is a consequence of (106).

Let p be a prime number and F be a field with characteristic p. Observe that $\mathrm{PrimeField}\, F$ is $(\mathbb{Z}/p)$-homomorphic and $\mathrm{canHom}\mathbb{Z}/p(\mathrm{PrimeField}\, F)$ is onto.

Now we state the propositions:

(108) Let us consider a prime number p, and a field F with characteristic p. Then $\mathbb{Z}/p$ and $\mathrm{PrimeField}\, F$ are isomorphic.

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

(110) Let us consider a prime number p. Then $\mathrm{PrimeField}\, \mathbb{Z}/p = \mathbb{Z}/p$.

(111) Let us consider a prime number p, and a field F with characteristic p. Then F includes $\mathbb{Z}/p$.

(112) Let us consider a prime number p, a field F with characteristic p, and a field E. If F includes E, then E includes $\mathbb{Z}/p$. The theorem is a consequence of (72) and (88).

Let p be a prime number. One can check that $\mathbb{Z}/p$ is prime.

Now we state the propositions:

(113) Let us consider a field F. Then $\mathrm{char}(F) = 0$ if and only if $\mathrm{PrimeField}\, F$ and $\mathbb{F}_{\mathbb{Q}}$ are isomorphic. The theorem is a consequence of (101), (43), and (89).

(114) Let us consider a prime number p, and a field F. Then $\mathrm{char}(F) = p$ if and only if $\mathrm{PrimeField}\, F$ and $\mathbb{Z}/p$ are isomorphic. The theorem is a consequence of (108), (43), and (89).

(115) Let us consider a strict field F. Then F is prime if and only if F and $\mathbb{F}_{\mathbb{Q}}$ are isomorphic or there exists a prime number p such that F and $\mathbb{Z}/p$

are isomorphic. The theorem is a consequence of (86), (101), (108), (44), (57), and (58).

References

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[5] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.

[6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[12] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Set of points on elliptic curve in projective coordinates. *Formalized Mathematics*, 19(**3**):131–138, 2011. doi:10.2478/v10037-011-0021-6.

[13] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Gaussian integers. *Formalized Mathematics*, 21(**2**):115–125, 2013. doi:10.2478/forma-2013-0013.

[14] Nathan Jacobson. *Basic Algebra I.* 2nd edition. Dover Publications Inc., 2009.

[15] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

[16] 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.

[17] Jarosław Kotowicz. Quotient vector spaces and functionals. *Formalized Mathematics*, 11 (**1**):59–68, 2003.

[18] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[19] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[20] Heinz Lüneburg. *Die grundlegenden Strukturen der Algebra (in German).* Oldenbourg Wisenschaftsverlag, 1999.

[21] Anna Justyna Milewska. The field of complex numbers. *Formalized Mathematics*, 9(**2**): 265–269, 2001.

[22] Michał Muzalewski. Opposite rings, modules and their morphisms. *Formalized Mathematics*, 3(**1**):57–65, 1992.

[23] Michał Muzalewski. Category of rings. *Formalized Mathematics*, 2(**5**):643–648, 1991.

[24] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[25] Michał Muzalewski and Wojciech Skaba. From loops to Abelian multiplicative groups with zero. *Formalized Mathematics*, 1(**5**):833–840, 1990.

[26] Karol Pąk. Linear map of matrices. *Formalized Mathematics*, 16(**3**):269–275, 2008. doi:10.2478/v10037-008-0032-0.

[27] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[28] Christoph Schwarzweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Formalized Mathematics*, 6(**3**): 381–388, 1997.

[29] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[30] Christoph Schwarzweller. The field of quotients over an integral domain. *Formalized Mathematics*, 7(**1**):69–79, 1998.

[31] Yasunari Shidama, Hikofumi Suzuki, and Noboru Endou. Banach algebra of bounded functionals. *Formalized Mathematics*, 16(**2**):115–122, 2008. doi:10.2478/v10037-008-0017-z.

[32] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.

[33] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[34] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[35] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[36] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[37] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

[38] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[39] B.L. van der Waerden. *Algebra I*. 4th edition. Springer, 2003.

[40] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received August 14, 2015