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

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], [1], [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 
   \((f \upharpoonright A)(a, b) = f(a, b)\).

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

3. \( \cdot_{\mathbb{C}} \upharpoonright \mathbb{R} = \cdot_{\mathbb{R}} \).
   Proof: Set \( d = \cdot_{\mathbb{C}} \upharpoonright \mathbb{R} \). For every object \( z \) such that \( z \in \text{dom} \ d \) holds 
   \( d(z) = \cdot_{\mathbb{R}}(z) \) by [7] (49). □
(4) \( +\mathbb{Q} \upharpoonright \mathbb{Z} = +\mathbb{Z} \).

Proof: Set \( c = +\mathbb{Q} \upharpoonright \mathbb{Z} \). For every object \( z \) such that \( z \in \text{dom} \ c \) holds \( c(z) = (+\mathbb{Z})(z) \) by \([7, (49)]\). \( \square \)

(5) \( \cdot \mathbb{Q} \upharpoonright \mathbb{Z} = \cdot \mathbb{Z} \).

Proof: Set \( d = \cdot \mathbb{Q} \upharpoonright \mathbb{Z} \). For every object \( z \) such that \( z \in \text{dom} \ d \) 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 \( i \div n = \frac{i}{n} \).

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

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

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

(10) \( \frac{i}{m} = \frac{i \div (\gcd(i, m))}{m \div (\gcd(i, m))} \). 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 \( i \div m \mid i \). The theorem is a consequence of (6).

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

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

(15) (i) \( \text{den}(\frac{i}{m}) = m \div (\gcd(i, m)) \), and

(ii) \( \text{num}(\frac{i}{m}) = i \div (\gcd(i, m)) \).

The theorem is a consequence of (10) and (14).

(16) (i) \( \text{den}(\frac{i}{m}) = \frac{m}{\gcd(i, m)} \), and

(ii) \( \text{num}(\frac{i}{m}) = \frac{i}{\gcd(i, m)} \).

The theorem is a consequence of (15), (8), and (7).

(17) (i) \( \text{den}(-\frac{i}{m}) = m \div (\gcd(-i, m)) \), and

(ii) \( \text{num}(-\frac{i}{m}) = -i \div (\gcd(-i, m)) \).

The theorem is a consequence of (15).

(18) (i) \( \text{den}(-\frac{i}{m}) = \frac{m}{\gcd(-i, m)} \), and

(ii) \( \text{num}(-\frac{i}{m}) = \frac{-i}{\gcd(-i, m)} \).

The theorem is a consequence of (17), (8), and (7).
(19) (i) \( \text{den}(\frac{m}{i})^{-1} = m \div \gcd(m,i) \), and
(ii) \( \text{num}(\frac{m}{i})^{-1} = i \div \gcd(m,i) \).
The theorem is a consequence of (15).

(20) (i) \( \text{den}(\frac{m}{i})^{-1} = \frac{m}{\gcd(m,i)} \), and
(ii) \( \text{num}(\frac{m}{i})^{-1} = \frac{i}{\gcd(m,i)} \).
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) \( \text{den}((\frac{i}{m}) + (\frac{j}{n})) = m \cdot n \div \gcd(i \cdot n + j \cdot m, m \cdot n) \), and
(ii) \( \text{num}((\frac{i}{m}) + (\frac{j}{n})) = i \cdot n + j \cdot m \div \gcd(i \cdot n + j \cdot m, m \cdot n) \).
The theorem is a consequence of (15).

(22) (i) \( \text{den}((\frac{i}{m}) + (\frac{j}{n})) = \frac{m \cdot n}{\gcd(i \cdot n + j \cdot m, m \cdot n)} \), and
(ii) \( \text{num}((\frac{i}{m}) + (\frac{j}{n})) = \frac{i \cdot n + j \cdot m}{\gcd(i \cdot n + j \cdot m, m \cdot n)} \).
The theorem is a consequence of (21), (8), and (7).

(23) (i) \( \text{den}((\frac{i}{m}) - (\frac{j}{n})) = m \cdot n \div \gcd(i \cdot n - j \cdot m, m \cdot n) \), and
(ii) \( \text{num}((\frac{i}{m}) - (\frac{j}{n})) = i \cdot n - j \cdot m \div \gcd(i \cdot n - j \cdot m, m \cdot n) \).
The theorem is a consequence of (15).

(24) (i) \( \text{den}((\frac{i}{m}) - (\frac{j}{n})) = \frac{m \cdot n}{\gcd(i \cdot n - j \cdot m, m \cdot n)} \), and
(ii) \( \text{num}((\frac{i}{m}) - (\frac{j}{n})) = \frac{i \cdot n - j \cdot m}{\gcd(i \cdot n - j \cdot m, m \cdot n)} \).
The theorem is a consequence of (23), (8), and (7).

(25) (i) \( \text{den}((\frac{i}{m}) \cdot (\frac{j}{n})) = m \cdot n \div \gcd(i \cdot j, m \cdot n) \), and
(ii) \( \text{num}((\frac{i}{m}) \cdot (\frac{j}{n})) = i \cdot j \div \gcd(i \cdot j, m \cdot n) \).
The theorem is a consequence of (15).

(26) (i) \( \text{den}((\frac{i}{m}) \cdot (\frac{j}{n})) = \frac{m \cdot n}{\gcd(i \cdot j, m \cdot n)} \), and
(ii) \( \text{num}((\frac{i}{m}) \cdot (\frac{j}{n})) = \frac{i \cdot j}{\gcd(i \cdot j, m \cdot n)} \).
The theorem is a consequence of (25), (8), and (7).

(27) (i) \( \text{den}(\frac{m}{j}) = m \cdot n \div \gcd(i \cdot j, m \cdot n) \), and
(ii) \( \text{num}(\frac{m}{j}) = i \cdot j \div \gcd(i \cdot j, m \cdot n) \).
The theorem is a consequence of (15).

(28) (i) \( \text{den}(\frac{m}{j}) = \frac{m \cdot n}{\gcd(i \cdot j, m \cdot n)} \), and
(ii) \( \text{num}(\frac{m}{j}) = \frac{i \cdot j}{\gcd(i \cdot j, m \cdot n)} \).
The theorem is a consequence of (27), (8), and (7).

Now we state the propositions:
(29) \( \text{den } p = \text{den } p \div \gcd(\text{num } p, \text{den } p) \). The theorem is a consequence of (15).

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

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

(31) \( \text{(i) } \text{den } (-p) = m \div \gcd(-i, m) \), and
    \( \text{(ii) } \text{num } (-p) = -i \div \gcd(-i, m) \).
    The theorem is a consequence of (17).

(32) \( \text{(i) } \text{den } (-p) = \frac{m}{\gcd(-i, m)} \), and
    \( \text{(ii) } \text{num } (-p) = \frac{-i}{\gcd(-i, m)} \).
    The theorem is a consequence of (31), (8), and (7).

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

(33) \( \text{(i) } \text{den } p^{-1} = n \div \gcd(n, m) \), and
    \( \text{(ii) } \text{num } p^{-1} = m \div \gcd(n, m) \).
    The theorem is a consequence of (19).

(34) \( \text{(i) } \text{den } p^{-1} = \frac{n}{\gcd(n, m)} \), and
    \( \text{(ii) } \text{num } p^{-1} = \frac{m}{\gcd(n, m)} \).
    The theorem is a consequence of (33), (8), and (7).

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

(35) \( \text{(i) } \text{den } (p + q) = m \cdot n \div \gcd(i \cdot n + j \cdot m, m \cdot n) \), and
    \( \text{(ii) } \text{num } (p + q) = i \cdot n + j \cdot m \div \gcd(i \cdot n + j \cdot m, m \cdot n) \).
    The theorem is a consequence of (21).

(36) \( \text{(i) } \text{den } (p + q) = \frac{m \cdot n}{\gcd(i \cdot n + j \cdot m, m \cdot n)} \), and
    \( \text{(ii) } \text{num } (p + q) = \frac{i \cdot n + j \cdot m}{\gcd(i \cdot n + j \cdot m, m \cdot n)} \).
    The theorem is a consequence of (35), (8), and (7).

(37) \( \text{(i) } \text{den } (p - q) = m \cdot n \div \gcd(i \cdot n - j \cdot m, m \cdot n) \), and
    \( \text{(ii) } \text{num } (p - q) = i \cdot n - j \cdot m \div \gcd(i \cdot n - j \cdot m, m \cdot n) \).
    The theorem is a consequence of (23).

(38) \( \text{(i) } \text{den } (p - q) = \frac{m \cdot n}{\gcd(i \cdot n - j \cdot m, m \cdot n)} \), and
    \( \text{(ii) } \text{num } (p - q) = \frac{i \cdot n - j \cdot m}{\gcd(i \cdot n - j \cdot m, m \cdot n)} \).
    The theorem is a consequence of (37), (8), and (7).

(39) \( \text{(i) } \text{den } (p \cdot q) = m \cdot n \div \gcd(i \cdot j, m \cdot n) \), and
(ii) \(\text{num}(p \cdot q) = i \cdot j \div \gcd(i \cdot j, m \cdot n)\).

The theorem is a consequence of (25).

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

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

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

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

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

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

The theorem is a consequence of (27).

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

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

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 \(\mathbb{Z}^R\) which is positive and there exists an element of \(\mathbb{Z}^R\) which is negative.

Let \(a, b\) be elements of \(\mathbb{F}_Q\) 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 \(\mathbb{F}_Q\) and \(x\) be a rational number. We identify \(-x\) with \(-a\). Let \(a\) be a non zero element of \(\mathbb{F}_Q\). We identify \(x^{-1}\) with \(a^{-1}\). Let \(a, b\) be elements of \(\mathbb{F}_Q\) and \(x, y\) be rational numbers. We identify \(x - y\) with \(a - b\). Let \(a\) be an element of \(\mathbb{F}_Q\) and \(b\) be a non zero element of \(\mathbb{F}_Q\). We identify \(y\) with \(b\). 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) $\mathbb{Z}^R$ is a subring of $\mathbb{F}_Q$.

(48) $\mathbb{R}_F$ is a subfield of $\mathbb{C}_F$.

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 $\text{Im } f$ 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 $\text{Im } f$ 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 $g = f |(\text{the carrier of } K)$ and $f$ is additive, then $g$ is additive. The theorem is a consequence of (1).

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

(51) If $g = f |(\text{the carrier of } K)$ 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 $f |K$ 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 $g = f |(\text{the carrier of } K)$ and $f$ is additive, then $g$ is additive. The theorem is a consequence of (1).
If \( g = f \mid (\text{the carrier of } K) \) and \( f \) is multiplicative, then \( g \) is multiplicative. The theorem is a consequence of (1).

If \( g = f \mid (\text{the carrier of } K) \) and \( f \) is unity-preserving, then \( g \) is unity-preserving.

Now we state the propositions:

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).

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 \( f \mid K \) 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 \( \mathbb{Z}_n^R \).

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:

\begin{align*}
(59) \quad 0 \star a &= 0_R, \\
(60) \quad 1 \star a &= a, \\
(61) \quad (-1) \star a &= -a.
\end{align*}

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 $\mathcal{P}[u + 1]$ by \[36\] (64), \[18\] (9), (60), (62). 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 char($R$) yielding a natural number is defined by

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

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

(Def. 6) $\text{char}(R) = n$. 
Now we state the propositions:

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

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

Observe that \( \mathbb{Z}^R \) 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 \( \text{char}(R) \) is positive.

Let \( R \) be a ring. The functor charSet \( R \) yielding a subset of \( \mathbb{N} \) is defined by

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

Let \( n \) be a positive natural number and \( R \) be a ring with characteristic \( n. \)

Note that charSet \( R \) is non empty.

Now we state the propositions:

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

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

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

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

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

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

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

Now we state the propositions:

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

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

Let \( R \) be a ring with characteristic 0. Observe that canHom\( \mathbb{Z}(R) \) is monomorphic and there exists a function from \( \mathbb{Z}^R \) 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 $\mathbb{Z}^R$ to $R$. Then $f = \text{canHom}_\mathbb{Z}(R)$.

**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]. \(\square\)

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

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

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

(ii) $\text{char}(R)$ 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 $\text{char}(S) \mid \text{char}(R)$. The theorem is a consequence of (84), (69), and (82).

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

(89) Let us consider a ring $R$, and a subring $S$ of $R$. Then $\text{char}(S) = \text{char}(R)$.

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 $\mathbb{C}_F$ has characteristic 0 and $\mathbb{R}_F$ has characteristic 0 and $\mathbb{F}_Q$ 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 $\text{char}(R)$ 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

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

The functor PrimeField $F$ yielding a strict double loop structure is defined by
(Def. 10) the carrier of \( it = \text{carrier} \cap F \) and the addition of \( it = (\text{the addition of } F) \upharpoonright \text{carrier} \cap F \) and the multiplication of \( it = (\text{the multiplication of } F) \upharpoonright \text{carrier} \cap F \) and the one of \( it = 1_F \) and the zero of \( it = 0_F \).

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

Let us note that the functor \( \text{PrimeField } F \) yields a strict subfield of \( F \). Now we state the propositions:

(90) Let us consider a field \( F \), and a strict subfield \( E \) of \( \text{PrimeField } F \). Then \( E = \text{PrimeField } F \).

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

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

(92) \( K = \text{PrimeField } F \) 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) \( K = \text{PrimeField } F \) 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 \( \text{PrimeField } F = \text{PrimeField } E \). The theorem is a consequence of (93) and (92).

(95) Let us consider a field \( F \). Then \( \text{PrimeField } \) \( \text{PrimeField } F = \text{PrimeField } F \).

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

Now we state the propositions:

(96) Let us consider a field \( F \). Then \( F \) is prime if and only if \( F = \text{PrimeField } F \).

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

**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 \([34 \ (3)], \ (63), \ [36 \ (17)]\). \( \Box \)

Let \( x \) be an element of \( \mathbb{F}_Q \). Note that the functor \( \text{den } x \) yields a positive element of \( \mathbb{Z}^R \). One can check that the functor \( \text{num } x \) yields an element of \( \mathbb{Z}^R \).

Let \( F \) be a field. The functor \( \text{canHom}_Q(F) \) yielding a function from \( \mathbb{F}_Q \) into \( F \) is defined by

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

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

Now we state the proposition:

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

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

Now we state the proposition:

(99) Let us consider an $(\mathbb{F}_q)$-homomorphic field $F$ with characteristic 0, and a homomorphism $f$ from $\mathbb{F}_q$ to $F$. Then $f = \text{canHom}_{\mathbb{Q}}(F)$.

**Proof:** Set $g = \text{canHom}_{\mathbb{Q}}(F)$. Define $P[\text{integer}] \equiv$ for every element $j$ of $\mathbb{F}_q$ such that $j = 1$ holds $f(j) = g(j)$. For every integer $i$, $P[i]$ from [34 Sch. 4]. For every integer $i$ and for every element $j$ of $\mathbb{F}_q$ such that $j = i$ holds $f(j) = (\text{canHom}_{\mathbb{Z}}(F))(i)$ by (98), [7 (49)]. □

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

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

Now we state the proposition:

(100) Let us consider a homomorphism $f$ from $\mathbb{F}_q$ to $\mathbb{F}_q$. Then $f = \text{id}_{\mathbb{F}_q}$. 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 $\text{Im}f$ yields a strict subfield of $S$. Let $F$ be a field with characteristic 0. Let us note that $\text{canHom}_{\mathbb{Q}}(\text{PrimeField } F)$ is onto.

Now we state the propositions:

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

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

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

(104) Let us consider a field $F$ with characteristic 0, and a field $E$. If $F$ includes $E$, then $E$ includes $\mathbb{F}_q$. 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 $i \ast 1_R = (i \mod p) \ast 1_R$. The theorem is a consequence of (67) and (62).

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

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

Note that $\text{canHom}_{\mathbb{Z}}/p(F)$ is unity-preserving.
Let $F$ be a field with characteristic $p$. One can verify that $\text{canHom}\mathbb{Z}/p(F)$ is additive and multiplicative and every field with characteristic $p$ is $(\mathbb{Z}/p)$-monomorphically 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 $f = \text{canHom}\mathbb{Z}/p(F)$.

Proof: Set $g = \text{canHom}\mathbb{Z}/p(F)$. 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 $0 \leq k < p_1$ holds if $\mathcal{P}[k]$, then $\mathcal{P}[k + 1]$ by [34, (13), (44)], [29, (14), (7)]. For every element $k$ of $\mathbb{N}$ such that $0 \leq k \leq p_1$ holds if $\mathcal{P}[k]$ 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 $f = \text{id}_{\mathbb{Z}/p}$. The theorem is a consequence of (106).

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

(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 $\text{char}(F) = 0$ if and only if $\text{PrimeField } F$ and $\mathbb{F}_q$ 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 $\text{char}(F) = p$ if and only if $\text{PrimeField } F$ 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 $\mathbb{F}_q$ 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

Characteristic of rings. Prime fields


Received August 14, 2015