Isomorphisms of Direct Products of Finite Commutative Groups

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. We have been working on the formalization of groups. In [1], we encoded some theorems concerning the product of cyclic groups. In this article, we present the generalized formalization of [1]. First, we show that every finite commutative group which order is composite number is isomorphic to a direct product of finite commutative groups which orders are relatively prime. Next, we describe finite direct products of finite commutative groups.

MML identifier: GROUP_17

The notation and terminology used in this paper have been introduced in the following articles: [2], [3], [19], [7], [13], [20], [8], [9], [10], [23], [24], [25], [26], [27], [14], [22], [17], [4], [5], [15], [16], [6], [11], [21], [18], [29], [28], and [12].

1. Preliminaries

Now we state the propositions:

(1) Let us consider sets $A, B, A_1, B_1$. Suppose
   (i) $A$ misses $B$, and
   (ii) $A_1 \subseteq A$, and
   (iii) $B_1 \subseteq B$, and
   (iv) $A_1 \cup B_1 = A \cup B$.

   Then

\footnote{The 1st author was supported by JSPS KAKENHI 21240001, and the 3rd author was supported by JSPS KAKENHI 22300285.}
(v) \( A_1 = A \), and
(vi) \( B_1 = B \).

**Proof**: \( A \subseteq A_1 \), \( B \subseteq B_1 \). □

(2) Let us consider non empty finite sets \( H, K \). Then \( \prod (H, K) = \overline{H} \cdot \overline{K} \).

Let us consider bags \( p_2, p_1, f \) of Prime and a natural number \( q \). Now we state the propositions:

(3) If support \( p_2 \) misses support \( p_1 \) and \( f = p_2 + p_1 \) and \( q \in \text{support } p_2 \), then \( p_2(q) = f(q) \).

(4) If support \( p_2 \) misses support \( p_1 \) and \( f = p_2 + p_1 \) and \( q \in \text{support } p_1 \), then \( p_1(q) = f(q) \).

Now we state the propositions:

(5) Let us consider a non zero natural number \( h \) and a prime number \( q \). If \( q \) and \( h \) are not relatively prime, then \( q \mid h \).

(6) Let us consider non zero natural numbers \( h, s \). Suppose a prime number \( q \). Suppose \( q \in \text{support PrimeFactorization}(s) \). Then \( q \) and \( h \) are not relatively prime. Then \( \text{support PrimeFactorization}(s) \subseteq \text{support PrimeFactorization}(h) \). The theorem is a consequence of (5).

(7) Let us consider non zero natural numbers \( h, k, s, t \). Suppose

(i) \( h \) and \( k \) are relatively prime, and
(ii) \( s \cdot t = h \cdot k \), and
(iii) for every prime number \( q \) such that \( q \in \text{support PrimeFactorization}(s) \) holds \( q \) and \( h \) are not relatively prime, and
(iv) for every prime number \( q \) such that \( q \in \text{support PrimeFactorization}(t) \) holds \( q \) and \( k \) are not relatively prime.

Then

(v) \( s = h \), and
(vi) \( t = k \).

The theorem is a consequence of (6), (1), (3), and (4). **Proof**: Set \( p_2 = \text{PrimeFactorization}(s) \). Set \( p_1 = \text{PrimeFactorization}(t) \). For every natural number \( p \) such that \( p \in \text{support PFExp}(h) \) holds \( p = p^{p-\text{count}(h)} \). For every natural number \( p \) such that \( p \in \text{support PFExp}(k) \) holds \( p = p^{p-\text{count}(k)} \). □

Let \( G \) be a non empty multiplicative magma, \( I \) be a finite set, and \( b \) be a (the carrier of \( G \))-valued total \( I \)-defined function. The functor \( \prod b \) yielding an element of \( G \) is defined by

(Def. 1) There exists a finite sequence \( f \) of elements of \( G \) such that

(i) \( it = \prod f \), and
(ii) \( f = b \cdot \text{CFS}(I) \).

Now we state the propositions:

(8) Let us consider a commutative group \( G \), non empty finite sets \( A, B \), a (the carrier of \( G \))-valued total \( A \)-defined function \( F_3 \), a (the carrier of \( G \))-valued total \( B \)-defined function \( F_2 \), and a (the carrier of \( G \))-valued total \( A \cup B \)-defined function \( F_1 \). Suppose

(i) \( A \) misses \( B \), and
(ii) \( F_1 = F_3 + F_2 \).

Then \( \prod F_1 = \prod F_3 \cdot \prod F_2 \).

(9) Let us consider a non empty multiplicative magma \( G \), a set \( q \), an element \( z \) of \( G \), and a (the carrier of \( G \))-valued total \( \{q\} \)-defined function \( f \). If \( f = \{q\} \mapsto \rightarrow z \), then \( \prod f = z \).

2. Direct Product of Finite Commutative Groups

Now we state the propositions:

(10) Let us consider non empty multiplicative magmas \( X, Y \). Then the carrier of \( \prod \langle X, Y \rangle = \prod \langle \text{the carrier of } X, \text{the carrier of } Y \rangle \).

PROOF: Set \( \text{Carr} X = \text{the carrier of } X \). Set \( \text{Carr} Y = \text{the carrier of } Y \). For every element \( a \) such that \( a \in \text{dom the support of } \langle X, Y \rangle \) holds (the support of \( \langle X, Y \rangle \))(\( a \)) = \langle \text{the carrier of } X, \text{the carrier of } Y \rangle(\( a \)). \( \square \)

(11) Let us consider a group \( G \) and normal subgroups \( A, B \) of \( G \). Suppose (the carrier of \( A \)) \( \cap \) (the carrier of \( B \)) = \{1_G\}. Let us consider elements \( a, b \) of \( G \). If \( a \in A \) and \( b \in B \), then \( a \cdot b = b \cdot a \).

(12) Let us consider a group \( G \) and normal subgroups \( A, B \) of \( G \). Suppose

(i) for every element \( x \) of \( G \), there exist elements \( a, b \) of \( G \) such that \( a \in A \) and \( b \in B \) and \( x = a \cdot b \), and
(ii) (the carrier of \( A \)) \( \cap \) (the carrier of \( B \)) = \{1_G\}.

Then there exists a homomorphism \( h \) from \( \prod \langle A, B \rangle \) to \( G \) such that

(iii) \( h \) is bijective, and
(iv) for every elements \( a, b \) of \( G \) such that \( a \in A \) and \( b \in B \) holds \( h(\langle a, b \rangle) = a \cdot b \).

The theorem is a consequence of (11). PROOF: Define \( P[\text{set, set}] \equiv \) there exists an element \( x \) of \( G \) and there exists an element \( y \) of \( G \) such that \( x \in A \) and \( y \in B \) and \( S_1 = \langle x, y \rangle \) and \( S_2 = x \cdot y \). For every element \( z \) of \( \prod \langle A, B \rangle \), there exists an element \( w \) of \( G \) such that \( P[z, w] \). Consider \( h \) being a function from \( \prod \langle A, B \rangle \) into \( G \) such that for every element \( z \) of \( \prod \langle A, B \rangle \), \( P[z, h(z)] \). For every elements \( a, b \) of \( G \) such that \( a \in A \) and \( b \in B \) holds
\( h(\langle a, b \rangle) = a \cdot b \). For every elements \( z, w \) of \( \prod \langle A, B \rangle \), \( h(z \cdot w) = h(z) \cdot h(w) \).

Let us consider a finite commutative group \( G \), a natural number \( m \), and a subset \( A \) of \( G \). Now we state the propositions:

(13) Suppose \( A = \{ x \text{ where } x \text{ is an element of } G : x^m = 1_G \} \). Then

(i) \( A \neq \emptyset \), and

(ii) for every elements \( g_1, g_2 \) of \( G \) such that \( g_1, g_2 \in A \) holds \( g_1 \cdot g_2 \in A \), and

(iii) for every element \( g \) of \( G \) such that \( g \in A \) holds \( g^{-1} \in A \).

(14) Suppose \( A = \{ x \text{ where } x \text{ is an element of } G : x^m = 1_G \} \). Then there exists a strict finite subgroup \( H \) of \( G \) such that

(i) the carrier of \( H = A \), and

(ii) \( H \) is commutative and normal.

Now we state the propositions:

(15) Let us consider a finite commutative group \( G \), a natural number \( m \), and a finite subgroup \( H \) of \( G \). Suppose the carrier of \( H = \{ x \text{ where } x \text{ is an element of } G : x^m = 1_G \} \). Let us consider a prime number \( q \). Suppose \( q \in \text{support PrimeFactorization}(H) \). Then \( q \) and \( m \) are not relatively prime.

(16) Let us consider a finite commutative group \( G \) and natural numbers \( h, k \). Suppose

(i) \( \overline{G} = h \cdot k \), and

(ii) \( h \) and \( k \) are relatively prime.

Then there exist strict finite subgroups \( H, K \) of \( G \) such that

(iii) the carrier of \( H = \{ x \text{ where } x \text{ is an element of } G : x^h = 1_G \} \), and

(iv) the carrier of \( K = \{ x \text{ where } x \text{ is an element of } G : x^k = 1_G \} \), and

(v) \( H \) is normal, and

(vi) \( K \) is normal, and

(vii) for every element \( x \) of \( G \), there exist elements \( a, b \) of \( G \) such that \( a \in H \) and \( b \in K \) and \( x = a \cdot b \), and

(viii) \( (\text{the carrier of } H) \cap (\text{the carrier of } K) = \{ 1_G \} \).

The theorem is a consequence of (14). PROOF: Set \( A = \{ x \text{ where } x \text{ is an element of } G : x^h = 1_G \} \). Set \( B = \{ x \text{ where } x \text{ is an element of } G : x^k = 1_G \} \). \( A \subseteq \text{the carrier of } G \). \( B \subseteq \text{the carrier of } G \). Consider \( H \) being a strict finite subgroup of \( G \) such that the carrier of \( H = A \) and \( H \) is commutative and \( H \) is normal. Consider \( K \) being a strict finite subgroup of \( G \) such that the carrier of \( K = B \) and \( K \) is commutative and \( K \) is
normal. Consider $a, b$ being integers such that $a \cdot h + b \cdot k = 1$. (The carrier of $H$) $\cap$ (the carrier of $K$) $\subseteq \{1_G\}$. For every element $x$ of $G$, there exist elements $s, t$ of $G$ such that $s \in H$ and $t \in K$ and $x = s \cdot t$. □

(17) Let us consider finite groups $H, K$. Then $\prod \langle H, K \rangle = H \cdot K$. The theorem is a consequence of (10) and (2).

(18) Let us consider a finite commutative group $G$ and non zero natural numbers $h, k$. Suppose

(i) $\overline{G} = h \cdot k$, and

(ii) $h$ and $k$ are relatively prime.

Then there exist strict finite subgroups $H, K$ of $G$ such that

(iii) $\overline{H} = h$, and

(iv) $\overline{K} = k$, and

(v) (the carrier of $H$) $\cap$ (the carrier of $K$) $= \{1_G\}$, and

(vi) there exists a homomorphism $F$ from $\prod \langle H, K \rangle$ to $G$ such that $F$ is bijective and for every elements $a, b$ of $G$ such that $a \in H$ and $b \in K$ holds $F((a, b)) = a \cdot b$.

The theorem is a consequence of (16), (12), (17), (15), and (7).

3. Finite Direct Products of Finite Commutative Groups

Let us consider a group $G$, a set $q$, an associative group-like multiplicative magma family $F$ of $\{q\}$, and a function $f$ from $G$ into $\prod F$. Now we state the propositions:

(19) If $F = q \rightarrow G$ and for every element $x$ of $G$, $f(x) = q \rightarrow x$, then $f$ is a homomorphism from $G$ to $\prod F$.

(20) If $F = q \rightarrow G$ and for every element $x$ of $G$, $f(x) = q \rightarrow x$, then $f$ is bijective.

Now we state the propositions:

(21) Let us consider a set $q$, an associative group-like multiplicative magma family $F$ of $\{q\}$, and a group $G$. Suppose $F = q \rightarrow G$. Then there exists a homomorphism $I$ from $G$ to $\prod F$ such that

(i) $I$ is bijective, and

(ii) for every element $x$ of $G$, $I(x) = q \rightarrow x$.

The theorem is a consequence of (19) and (20). Proof: Define $\mathcal{P}[\text{set, set}] \equiv S_2 = q \rightarrow S_1$. For every element $z$ of $G$, there exists an element $w$ of $\prod F$ such that $\mathcal{P}[z, w]$. Consider $I$ being a function from $G$ into $\prod F$ such that for every element $x$ of $G$, $\mathcal{P}[x, I(x)]$. □
Let us consider non empty finite sets $I_0$, $I$, an associative group-like multiplicative magma family $F_0$ of $I_0$, an associative group-like multiplicative magma family $F$ of $I$, groups $H$, $K$, an element $q$ of $I$, an element $k$ of $K$, and a function $g$. Suppose

(i) $g \in$ the carrier of $\prod F_0$, and
(ii) $q \notin I_0$, and
(iii) $I = I_0 \cup \{q\}$, and
(iv) $F = F_0 + (q \rightharpoonup K)$.

Then $g + (q \rightharpoonup k) \in$ the carrier of $\prod F$. Proof: Set $HK = \langle H, K \rangle$. Set $w = g + (q \rightharpoonup k)$. For every element $x$ such that $x \in \text{dom}$ the support of $F$ holds $w(x) \in$ (the support of $F$)$(x)$. □

Let us consider non empty finite sets $I_0$, $I$, an associative group-like multiplicative magma family $F_0$ of $I_0$, an associative group-like multiplicative magma family $F$ of $I$, groups $H$, $K$, an element $q$ of $I$, a function $G_0$ from $H$ into $\prod F_0$, and a function $G$ from $\prod \langle H, K \rangle$ into $\prod F$. Now we state the propositions:

(23) Suppose $G_0$ is a homomorphism from $H$ to $\prod F_0$ and $G_0$ is bijective and $q \notin I_0$ and $I = I_0 \cup \{q\}$ and $F = F_0 + (q \rightharpoonup K)$. Then suppose for every element $h$ of $H$ and for every element $k$ of $K$, there exists a function $g$ such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g + (q \rightharpoonup k)$. Then $G$ is a homomorphism from $\prod \langle H, K \rangle$ to $\prod F$.

(24) Suppose $G_0$ is a homomorphism from $H$ to $\prod F_0$ and $G_0$ is bijective and $q \notin I_0$ and $I = I_0 \cup \{q\}$ and $F = F_0 + (q \rightharpoonup K)$. Then suppose for every element $h$ of $H$ and for every element $k$ of $K$, there exists a function $g$ such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g + (q \rightharpoonup k)$. Then $G$ is bijective.

Now we state the propositions:

(25) Let us consider a set $q$, a multiplicative magma family $F$ of $\{q\}$, and a non empty multiplicative magma $G$. Suppose $F = q \rightharpoonup G$. Let us consider a (the carrier of $G$)-valued total $\{q\}$-defined function $y$. Then

(i) $y \in$ the carrier of $\prod F$, and
(ii) $y(q) \in$ the carrier of $G$, and
(iii) $y = q \rightharpoonup y(q)$.

(26) Let us consider a set $q$, an associative group-like multiplicative magma family $F$ of $\{q\}$, and a group $G$. Suppose $F = q \rightharpoonup G$. Then there exists a homomorphism $H_0$ from $\prod F$ to $G$ such that

(i) $H_0$ is bijective, and
(ii) for every (the carrier of $G$)-valued total $\{q\}$-defined function $x$, $H_0(x) = \prod x$. 

The theorem is a consequence of (21), (25), and (9). Proof: Consider \( I \) being a homomorphism from \( G \) to \( \prod F \) such that \( I \) is bijective and for every element \( x \) of \( G \), \( I(x) = q \leadsto x \). Set \( H_0 = I^{-1} \). For every (the carrier of \( G \))-valued total \( \{q\}\)-defined function \( y \), \( H_0(y) = \prod y \). □

(27) Let us consider non empty finite sets \( I_0, I \), an associative group-like multiplicative magma family \( F_0 \) of \( I_0 \), an associative group-like multiplicative magma family \( F \) of \( I \), groups \( H, K \), an element \( q \) of \( I \), and a homomorphism \( G_0 \) from \( H \) to \( \prod F_0 \). Suppose

(i) \( q \notin I_0 \), and
(ii) \( I = I_0 \cup \{q\} \), and
(iii) \( F = F_0 + \cdot (q \leadsto K) \), and
(iv) \( G_0 \) is bijective.

Then there exists a homomorphism \( G \) from \( \prod \langle H, K \rangle \) to \( \prod F \) such that

(v) \( G \) is bijective, and
(vi) for every element \( h \) of \( H \) and for every element \( k \) of \( K \), there exists a function \( g \) such that \( g = G_0(h) \) and \( G(\langle h, k \rangle) = g + \cdot (q \leadsto k) \).

The theorem is a consequence of (22), (23), and (24). Proof: Set \( HK = \langle H, K \rangle \). Define \( P[\text{set}, \text{set}] \equiv \text{there exists an element } h \text{ of } H \text{ and there exists an element } k \text{ of } K \text{ and there exists a function } g \text{ such that } S_1 = \langle h, k \rangle \text{ and } g = G_0(h) \text{ and } S_2 = g + \cdot (q \leadsto k) \). For every element \( z \) of \( \prod \langle H, K \rangle \), there exists an element \( w \) of the carrier of \( \prod F \) such that \( P[z, w] \).

Consider \( G \) being a function from \( \prod \langle H, K \rangle \) into \( \prod F \) such that for every element \( x \) of \( \prod \langle H, K \rangle \), \( P[x, G(x)] \). For every element \( h \) of \( H \) and for every element \( k \) of \( K \), there exists a function \( g \) such that \( g = G_0(h) \) and \( G(\langle h, k \rangle) = g + \cdot (q \leadsto k) \). □

(28) Let us consider non empty finite sets \( I_0, I \), an associative group-like multiplicative magma family \( F_0 \) of \( I_0 \), an associative group-like multiplicative magma family \( F \) of \( I \), groups \( H, K \), an element \( q \) of \( I \), and a homomorphism \( G_0 \) from \( \prod F_0 \) to \( H \). Suppose

(i) \( q \notin I_0 \), and
(ii) \( I = I_0 \cup \{q\} \), and
(iii) \( F = F_0 + \cdot (q \leadsto K) \), and
(iv) \( G_0 \) is bijective.

Then there exists a homomorphism \( G \) from \( \prod F \) to \( \prod \langle H, K \rangle \) such that

(v) \( G \) is bijective, and
(vi) for every function \( x_0 \) and for every element \( k \) of \( K \) and for every element \( h \) of \( H \) such that \( h = G_0(x_0) \) and \( x_0 \in \prod F_0 \) holds \( G(x_0 + \cdot (q \leadsto k)) = \langle h, k \rangle \).
The theorem is a consequence of (27). \textbf{Proof}: Set $L0 = G0^{-1}$. Consider $L$ being a homomorphism from $\prod \langle H, K \rangle$ to $\prod F$ such that $L$ is bijective and for every element $h$ of $H$ and for every element $k$ of $K$, there exists a function $g$ such that $g = L0(h)$ and $L(\langle h, k \rangle) = g + (q \rightarrow k)$. Set $G = L^{-1}$. For every function $x0$ and for every element $k$ of $K$ and for every element $h$ of $H$ such that $h = G0(x0)$ and $x0 \in \prod F0$ holds $G(x0 + (q \rightarrow k)) = \langle h, k \rangle$. $\square$

29 Let us consider a non empty finite set $I$, an associative group-like multiplicative magma family $F$ of $I$, and a total $I$-defined function $x$. Suppose an element $p$ of $I$. Then $x(p) \in F(p)$. Then $x \in \text{the carrier of } \prod F$.

30 Let us consider non empty finite sets $I0$, $I$, an associative group-like multiplicative magma family $F0$ of $I0$, an associative group-like multiplicative magma family $F$ of $I$, a group $K$, an element $q$ of $I$, and an element $x$ of $\prod F$. Suppose

(i) $q \notin I0$, and

(ii) $I = I0 \cup \{q\}$, and

(iii) $F = F0 + (q \rightarrow K)$.

Then there exists a total $I0$-defined function $x0$ and there exists an element $k$ of $K$ such that $x0 \in \prod F0$ and $x = x0 + (q \rightarrow k)$ and for every element $p$ of $I0$, $x0(p) \in F0(p)$. \textbf{Proof}: Reconsider $y = x$ as a total $I$-defined function. Reconsider $k = y(q)$ as an element of $K$. Reconsider $y0 = y|I0$ as an $I0$-defined function. For every element $i$ of $I0$, $y0(i) \in (\text{the support of } F0)(i)$ and $y0(i) \in F0(i)$. $\square$

31 Let us consider a group $G$, a subgroup $H$ of $G$, a finite sequence $f$ of elements of $G$, and a finite sequence $g$ of elements of $H$. If $f = g$, then $\prod f = \prod g$. \textbf{Proof}: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence $f$ of elements of $G$ for every finite sequence $g$ of elements of $H$ such that $\mathcal{P}[k] \equiv \prod f = \prod g$. For every natural number $k$ such that $\mathcal{P}[k]$ holds $\mathcal{P}[k + 1]$. $\square$

32 Let us consider a non empty finite set $I$, a group $G$, a subgroup $H$ of $G$, a (the carrier of $G$)-valued total $I$-defined function $x$, and a (the carrier of $H$)-valued total $I$-defined function $x0$. If $x = x0$, then $\prod x = \prod x0$. The theorem is a consequence of (31).

33 Let us consider a commutative group $G$, non empty finite sets $I0$, $I$, an element $q$ of $I$, a (the carrier of $G$)-valued total $I$-defined function $x$, a (the carrier of $G$)-valued total $I0$-defined function $x0$, and an element $k$ of $G$. Suppose

(i) $q \notin I0$, and

(ii) $I = I0 \cup \{q\}$, and
(iii) $x = x_0 + (q, q^k)$.

Then $\prod x = \prod x_0 \cdot k$. The theorem is a consequence of (8) and (9). **Proof:**

Reconsider $y = q \cdot k$ as a (the carrier of $G$)-valued total $\{q\}$-defined function. $I_0$ misses $\{q\}$. □

Let us consider a finite commutative group $G$. Now we state the propositions:

(34) Suppose $\overline{G} > 1$. Then there exists a non empty finite set $I$ and there exists an associative group-like commutative multiplicative magma family $F$ of $I$ and there exists a homomorphism $H_0$ from $\prod F$ to $G$ such that $I = \text{support PrimeFactorization}(\overline{G})$ and for every element $p$ of $I$, $F(p)$ is a subgroup of $G$ and $\overline{F(p)} = (\text{PrimeFactorization}(\overline{G}))(p)$ and for every elements $p, q$ of $I$ such that $p \neq q$ holds (the carrier of $F(p)$) $\cap$ (the carrier of $F(q)$) = $\{1_G\}$ and $H_0$ is bijective and for every (the carrier of $G$)-valued total $I$-defined function $x$ such that for every element $p$ of $I$, $x(p) \in F(p)$ holds $x \in \prod F$ and $H_0(x) = \prod x$.

(35) Suppose $\overline{G} > 1$. Then there exists a non empty finite set $I$ and there exists an associative group-like commutative multiplicative magma family $F$ of $I$ such that $I = \text{support PrimeFactorization}(\overline{G})$ and for every element $p$ of $I$, $F(p)$ is a subgroup of $G$ and $\overline{F(p)} = (\text{PrimeFactorization}(\overline{G}))(p)$ and for every elements $p, q$ of $I$ such that $p \neq q$ holds (the carrier of $F(p)$) $\cap$ (the carrier of $F(q)$) = $\{1_G\}$ and for every element $y$ of $G$, there exists a (the carrier of $G$)-valued total $I$-defined function $x$ such that for every element $p$ of $I$, $x(p) \in F(p)$ and $y = \prod x$ and for every (the carrier of $G$)-valued total $I$-defined functions $x_1$, $x_2$ such that for every element $p$ of $I$, $x_1(p) \in F(p)$ and for every element $p$ of $I$, $x_2(p) \in F(p)$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$.

**References**


Received January 31, 2013