Isomorphisms of Direct Products of Finite Cyclic Groups

Kenichi Arai  
Tokyo University of Science  
Chiba, Japan

Hiroyuki Okazaki  
Shinshu University  
Nagano, Japan

Yasunari Shidama  
Shinshu University  
Nagano, Japan

Summary. In this article, we formalize that every finite cyclic group is isomorphic to a direct product of finite cyclic groups which orders are relative prime. This theorem is closely related to the Chinese Remainder theorem ([18]) and is a useful lemma to prove the basis theorem for finite abelian groups and the fundamental theorem of finite abelian groups. Moreover, we formalize some facts about the product of a finite sequence of abelian groups.

MML identifier: GROUP_14, version: 8.0.01 5.4.1165

The notation and terminology used in this paper are introduced in the following articles: [5], [1], [2], [4], [11], [6], [7], [20], [17], [18], [19], [3], [8], [13], [15], [16], [12], [23], [21], [10], [22], [14], and [9].

Let $G$ be an Abelian add-associative right zeroed right complementable non empty additive loop structure. Note that $\langle G \rangle$ is non empty and Abelian group yielding as a finite sequence.

Let $G, F$ be Abelian add-associative right zeroed right complementable non empty additive loop structures. Note that $\langle G, F \rangle$ is non empty and Abelian group yielding as a finite sequence.

We now state the proposition

(1) Let $X$ be an Abelian group. Then there exists a homomorphism $I$ from $X$ to $\prod\langle X \rangle$ such that $I$ is bijective and for every element $x$ of $X$ holds $I(x) = \langle x \rangle$. 
Let $G$, $F$ be non empty Abelian group yielding finite sequences. Note that $G \cap F$ is Abelian group yielding.

One can prove the following propositions:

(2) Let $X$, $Y$ be Abelian groups. Then there exists a homomorphism $I$ from $X \times Y$ to $\prod \langle X,Y \rangle$ such that $I$ is bijective and for every element $x$ of $X$ and for every element $y$ of $Y$ holds $I(x,y) = \langle x,y \rangle$.

(3) Let $X$, $Y$ be sequences of groups. Then there exists a homomorphism $I$ from $\prod X \times \prod Y$ to $\prod (X \cap Y)$ such that

(i) $I$ is bijective, and

(ii) for every element $x$ of $\prod X$ and for every element $y$ of $\prod Y$ there exist finite sequences $x_1$, $y_1$ such that $x = x_1$ and $y = y_1$ and $I(x,y) = x_1 \cap y_1$.

(4) Let $G$, $F$ be Abelian groups. Then

(i) for every set $x$ holds $x$ is an element of $\prod (G,F)$ iff there exists an element $x_1$ of $G$ and there exists an element $x_2$ of $F$ such that $x = \langle x_1, x_2 \rangle$,

(ii) for all elements $x$, $y$ of $\prod (G,F)$ and for all elements $x_1$, $y_1$ of $G$ and for all elements $x_2$, $y_2$ of $F$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $x + y = \langle x_1 + y_1, x_2 + y_2 \rangle$,

(iii) $0_{\prod (G,F)} = \langle 0_G, 0_F \rangle$, and

(iv) for every element $x$ of $\prod (G,F)$ and for every element $x_1$ of $G$ and for every element $x_2$ of $F$ such that $x = \langle x_1, x_2 \rangle$ holds $-x = \langle-x_1, -x_2 \rangle$.

(5) Let $G$, $F$ be Abelian groups. Then

(i) for every set $x$ holds $x$ is an element of $G \times F$ iff there exists an element $x_1$ of $G$ and there exists an element $x_2$ of $F$ such that $x = \langle x_1, x_2 \rangle$,

(ii) for all elements $x$, $y$ of $G \times F$ and for all elements $x_1$, $y_1$ of $G$ and for all elements $x_2$, $y_2$ of $F$ such that $x = \langle x_1, x_2 \rangle$ and $y = \langle y_1, y_2 \rangle$ holds $x + y = \langle x_1 + y_1, x_2 + y_2 \rangle$,

(iii) $0_{G \times F} = \langle 0_G, 0_F \rangle$, and

(iv) for every element $x$ of $G \times F$ and for every element $x_1$ of $G$ and for every element $x_2$ of $F$ such that $x = \langle x_1, x_2 \rangle$ holds $-x = \langle-x_1, -x_2 \rangle$.

(6) Let $G$, $H$, $I$ be groups, $h$ be a homomorphism from $G$ to $H$, and $h_1$ be a homomorphism from $H$ to $I$. Then $h_1 \cdot h$ is a homomorphism from $G$ to $I$.

Let $G$, $H$, $I$ be groups, let $h$ be a homomorphism from $G$ to $H$, and let $h_1$ be a homomorphism from $H$ to $I$. Then $h_1 \cdot h$ is a homomorphism from $G$ to $I$.

One can prove the following propositions:

(7) Let $G$, $H$ be groups and $h$ be a homomorphism from $G$ to $H$. If $h$ is bijective, then $h^{-1}$ is a homomorphism from $H$ to $G$.

(8) Let $X$, $Y$ be sequences of groups. Then there exists a homomorphism $I$ from $\prod \langle \prod X, \prod Y \rangle$ to $\prod (X \cap Y)$ such that

(i) $I$ is bijective, and
(ii) For every element \( x \) of \( \prod X \) and for every element \( y \) of \( \prod Y \) there exist finite sequences \( x_1, y_1 \) such that \( x = x_1 \) and \( y = y_1 \) and \( I(\langle x, y \rangle) = x_1 \sim y_1 \).

(9) Let \( X, Y \) be Abelian groups. Then there exists a homomorphism \( I \) from \( X \times Y \) to \( X \times \prod(Y) \) such that \( I \) is bijective and for every element \( x \) of \( X \) and for every element \( y \) of \( Y \) holds \( I(x, y) = \langle x, \langle y \rangle \rangle \).

(10) Let \( X \) be a sequence of groups and \( Y \) be an Abelian group. Then there exists a homomorphism \( I \) from \( \prod X \times Y \) to \( \prod(X \upharpoonright \langle Y \rangle) \) such that

(i) \( I \) is bijective, and

(ii) for every element \( x \) of \( \prod X \) and for every element \( y \) of \( Y \) there exist finite sequences \( x_1, y_1 \) such that \( x = x_1 \) and \( \langle y \rangle = y_1 \) and \( I(x, y) = x_1 \sim y_1 \).

(11) Let \( n \) be a non zero natural number. Then the additive loop structure of \((\mathbb{Z}/n\mathbb{Z})\) is non empty, Abelian, right complementable, add-associative, and right zeroed.

Let \( n \) be a natural number. The functor \( \mathbb{Z}/n\mathbb{Z} \) yields an additive loop structure and is defined by:

(Def. 1) \( \mathbb{Z}/n\mathbb{Z} \) is the additive loop structure of \((\mathbb{Z}/n\mathbb{Z})\).

Let \( n \) be a non zero natural number. Observe that \( \mathbb{Z}/n\mathbb{Z} \) is non empty and strict.

Let \( n \) be a non zero natural number. Note that \( \mathbb{Z}/n\mathbb{Z} \) is Abelian, right complementable, add-associative, and right zeroed.

Next we state a number of propositions:

(12) Let \( X \) be a sequence of groups, \( x, y, z \) be elements of \( \prod X \), and \( x_1, y_1, z_1 \) be finite sequences. Suppose \( x = x_1 \) and \( y = y_1 \) and \( z = z_1 \). Then \( z = x + y \) if and only if for every element \( j \) of \( \text{dom} \ X \) holds \( z_1(j) = (\text{the addition of } X(j))(x_1(j), y_1(j)) \).

(13) For every CR-sequence \( m \) and for every natural number \( j \) and for every integer \( x \) such that \( j \in \text{dom} \ m \) holds \( x \mod \prod m \mod m(j) = x \mod m(j) \).

(14) Let \( m \) be a CR-sequence and \( X \) be a sequence of groups. Suppose \( \text{len} \ m = \text{len} \ X \) and for every element \( i \) of \( \mathbb{N} \) such that \( i \in \text{dom} \ X \) there exists a non zero natural number \( m_1 \) such that \( m_1 = m(i) \) and \( X(i) = \mathbb{Z}/m_1\mathbb{Z} \). Then there exists a homomorphism \( I \) from \( \mathbb{Z}/(\prod m)\mathbb{Z} \) to \( \prod X \) such that for every integer \( x \) if \( x \in \text{carrier of } \mathbb{Z}/(\prod m)\mathbb{Z} \), then \( I(x) = \text{mod}(x, m) \).

(15) Let \( X, Y \) be non empty sets. Then there exists a function \( I \) from \( X \times Y \) into \( X \times \prod(Y) \) such that \( I \) is one-to-one and onto and for all sets \( x, y \) such that \( x \in X \) and \( y \in Y \) holds \( I(x, y) = \langle x, \langle y \rangle \rangle \).

(16) For every non empty set \( X \) holds \( \prod(X) = X \).

(17) Let \( X \) be a non-empty non empty finite sequence and \( Y \) be a non empty set. Then there exists a function \( I \) from \( \prod X \times Y \) into \( \prod(X \upharpoonright \langle Y \rangle) \) such that

(i) \( I \) is one-to-one and onto, and
(ii) for all sets \( x, y \) such that \( x \in \prod X \) and \( y \in Y \) there exist finite sequences \( x_1, y_1 \) such that \( x = x_1 \) and \((y) = y_1\) and \( I(x, y) = x_1 \sim y_1\).

(18) Let \( m \) be a finite sequence of elements of \( \mathbb{N} \) and \( X \) be a non-empty non empty finite sequence. Suppose \( \text{len } m = \text{len } X \) and for every element \( i \) of \( \mathbb{N} \) such that \( i \in \text{dom } X \) holds \( \prod X(i) = m(i) \). Then \( \prod X = \prod m \).

(19) Let \( m \) be a CR-sequence and \( X \) be a sequence of groups. Suppose \( \text{len } m = \text{len } X \) and for every element \( i \) of \( \mathbb{N} \) such that \( i \in \text{dom } X \) there exists a non zero natural number \( m_1 \) such that \( m_1 = m(i) \) and \( X(i) = \mathbb{Z}/m_1 \mathbb{Z} \). Then the carrier of \( \prod X = \prod m \).

(20) Let \( m \) be a CR-sequence, \( X \) be a sequence of groups, and \( I \) be a function from \( \mathbb{Z}/(\prod m)\mathbb{Z} \) into \( \prod X \). Suppose that

(i) \( \text{len } m = \text{len } X \),

(ii) for every element \( i \) of \( \mathbb{N} \) such that \( i \in \text{dom } X \) there exists a non zero natural number \( m_1 \) such that \( m_1 = m(i) \) and \( X(i) = \mathbb{Z}/m_1 \mathbb{Z} \), and

(iii) for every integer \( x \) such that \( x \in \text{carrier of } \mathbb{Z}/(\prod m)\mathbb{Z} \) holds \( I(x) = \text{mod}(x, m) \).

Then \( I \) is one-to-one.

(21) Let \( m \) be a CR-sequence and \( X \) be a sequence of groups. Suppose \( \text{len } m = \text{len } X \) and for every element \( i \) of \( \mathbb{N} \) such that \( i \in \text{dom } X \) there exists a non zero natural number \( m_1 \) such that \( m_1 = m(i) \) and \( X(i) = \mathbb{Z}/m_1 \mathbb{Z} \). Then there exists a homomorphism \( I \) from \( \mathbb{Z}/(\prod m)\mathbb{Z} \) to \( \prod X \) such that \( I \) is bijective and for every integer \( x \) such that \( x \in \text{carrier of } \mathbb{Z}/(\prod m)\mathbb{Z} \) holds \( I(x) = \text{mod}(x, m) \).

References


Received August 27, 2012