FORMALIZED MATHEMATICS
Vol. **20**, No. **4**, Pages 343–347, **2012**
DOI: 10.2478/v10037-012-0038-5

VERSITA
versita.com/fm/

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 $I(x) = \langle x \rangle$.

ISSN 1426–2630(p), 1898-9934(e)

Let G, F be non empty Abelian group yielding finite sequences. Note that $G \frown F$ 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 $\prod(X \frown Y)$ 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 $I(x, y) = x_1 \frown y_1$.

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

(i) for every set x holds x is an element of $\prod\langle G, F\rangle$ 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 $\prod\langle G, F\rangle$ 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) $0_{\prod\langle G, F\rangle} = \langle 0_G, 0_F\rangle$, and

(iv) for every element x of $\prod\langle G, F\rangle$ 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 $\prod(X \frown Y)$ 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 $I(\langle x, y\rangle) = x_1 \frown y_1$.

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

(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 $\prod(X \frown \langle Y\rangle)$ 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 $I(x, y) = x_1 \frown y_1$.

(11) Let n be a non zero natural number. Then the additive loop structure of $(\mathbb{Z}_n^{\mathrm{R}})$ 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) $\mathbb{Z}/n\mathbb{Z} =$ the additive loop structure of $(\mathbb{Z}_n^{\mathrm{R}})$.

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 $\operatorname{dom} \overline{X}$ holds $z_1(j) =$ (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 $j \in \operatorname{dom} m$ holds $x \bmod \prod m \bmod m(j) = x \bmod m(j)$.

(14) Let m be a CR-sequence and X be a sequence of groups. Suppose $\operatorname{len} m = \operatorname{len} X$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ 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 $x \in$ the carrier of $\mathbb{Z}/(\prod m)\mathbb{Z}$, then $I(x) = \operatorname{mod}(x, m)$.

(15) Let X, Y be non empty sets. Then there exists a function I from $X \times Y$ into $X \times \prod\langle Y\rangle$ 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 $\overline{\overline{\prod\langle X\rangle}} = \overline{\overline{X}}$.

(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 $\prod(X \frown \langle Y\rangle)$ 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 $\langle y \rangle = y_1$ and $I(x, y) = x_1 \frown y_1$.

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

(19) Let m be a CR-sequence and X be a sequence of groups. Suppose $\operatorname{len} m = \operatorname{len} X$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ 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 $\overline{\overline{\text{the carrier of } \prod X}} = \prod m$.

(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) $\operatorname{len} m = \operatorname{len} X$,

(ii) for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ 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 $x \in$ the carrier of $\mathbb{Z}/(\prod m)\mathbb{Z}$ holds $I(x) = \operatorname{mod}(x, m)$.

Then I is one-to-one.

(21) Let m be a CR-sequence and X be a sequence of groups. Suppose $\operatorname{len} m = \operatorname{len} X$ and for every element i of $\mathbb{N}$ such that $i \in \operatorname{dom} X$ 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 $x \in$ the carrier of $\mathbb{Z}/(\prod m)\mathbb{Z}$ holds $I(x) = \operatorname{mod}(x, m)$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[13] Artur Korniłowicz. On the real valued functions. *Formalized Mathematics*, 13(**1**):181–187, 2005.
[14] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[15] Anna Lango and Grzegorz Bancerek. Product of families of groups and vector spaces. *Formalized Mathematics*, 3(**2**):235–240, 1992.
[16] Hiroyuki Okazaki, Noboru Endou, and Yasunari Shidama. Cartesian products of family of real linear spaces. *Formalized Mathematics*, 19(**1**):51–59, 2011, doi: 10.2478/v10037-011-0009-2.
[17] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[18] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**):247–252, 2008, doi:10.2478/v10037-008-0029-8.
[19] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[21] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[22] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[23] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received August 27, 2012