FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 207–211, 2013
DOI: 10.2478/forma-2013-0022

VERSITA
degruyter.com/view/j/forma

Isomorphisms of Direct Products of Cyclic Groups of Prime Power Order

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Yasunari Shidama[1]
Shinshu University
Nagano, Japan

Summary. In this paper we formalized some theorems concerning the cyclic groups of prime power order. We formalize that every commutative cyclic group of prime power order is isomorphic to a direct product of family of cyclic groups [1], [18].

MSC: 13D99 06A75 03B35

Keywords: formalization of the commutative cyclic group; prime power set

MML identifier: GROUP_18, version: 8.1.02 5.19.1189

The notation and terminology used in this paper have been introduced in the following articles: [2], [20], [6], [11], [7], [8], [24], [18], [25], [26], [27], [28], [13], [23], [16], [21], [3], [4], [15], [5], [9], [22], [17], [12], [30], [31], [14], [29], and [10].

1. Basic Properties of Cyclic Groups of Prime Power Order

Let G be a finite group. The functor $\mathrm{Ordset}(G)$ yielding a subset of $\mathbb{N}$ is defined by the term

(Def. 1) the set of all $\mathrm{ord}(a)$ where a is an element of G.

One can check that $\mathrm{Ordset}(G)$ is finite and non empty.

Now we state the propositions:

(1) Let us consider a finite group G. Then there exists an element g of G such that $\mathrm{ord}(g) = \sup \mathrm{Ordset}(G)$.

[1]This work was supported by JSPS KAKENHI 22300285.

ISSN 1426–2630(Print), 1898-9934(Online)

(2) Let us consider a strict group G and a strict normal subgroup N of G. If G is commutative, then ${}^{G}/_{N}$ is commutative.

(3) Let us consider a finite group G and elements a, b of G. Then $b \in \mathrm{gr}(\{a\})$ if and only if there exists an element p of $\mathbb{N}$ such that $b = a^p$.

(4) Let us consider a finite group G, an element a of G, and elements n, p, s of $\mathbb{N}$. Suppose

(i) $\overline{\overline{\mathrm{gr}(\{a\})}} = n$, and

(ii) $n = p \cdot s$.

Then $\mathrm{ord}(a^p) = s$.

Let us consider an element k of $\mathbb{N}$, a finite group G, and an element a of G. Now we state the propositions:

(5) $\mathrm{gr}(\{a\}) = \mathrm{gr}(\{a^k\})$ if and only if $\gcd(k, \mathrm{ord}(a)) = 1$.

(6) If $\gcd(k, \mathrm{ord}(a)) = 1$, then $\mathrm{ord}(a) = \mathrm{ord}(a^k)$.

(7) $\mathrm{ord}(a) \mid k \cdot \mathrm{ord}(a^k)$.

Now we state the proposition:

(8) Let us consider a group G and elements a, b of G. Suppose $b \in \mathrm{gr}(\{a\})$. Then $\mathrm{gr}(\{b\})$ is a strict subgroup of $\mathrm{gr}(\{a\})$.

Let G be a strict commutative group and x be an element of $\mathrm{SubGr}\, G$. The functor $\mathrm{NormSp}_{\mathbb{R}}(x)$ yielding a normal strict subgroup of G is defined by the term

(Def. 2) x.

Now we state the propositions:

(9) Let us consider groups G, H, a subgroup K of H, and a homomorphism f from G to H. Then there exists a strict subgroup J of G such that the carrier of $J = f^{-1}$(the carrier of K). PROOF: Reconsider $I_3 = f^{-1}$(the carrier of K) as a non empty subset of the carrier of G. For every elements g_1, g_2 of G such that g_1, $g_2 \in I_3$ holds $g_1 \cdot g_2 \in I_3$ by [8, (38)], [25, (50)]. For every element g of G such that $g \in I_3$ holds $g^{-1} \in I_3$ by [8, (38)], [25, (51)], [28, (32)]. Consider J being a strict subgroup of G such that the carrier of $J = f^{-1}$(the carrier of K). $\square$

(10) Let us consider a natural number p, a finite group G, and elements x, d of G. Suppose

(i) $\mathrm{ord}(d) = p$, and

(ii) p is prime, and

(iii) $x \in \mathrm{gr}(\{d\})$.

Then

(iv) $x = \mathbf{1}_G$, or

(v) $\mathrm{gr}(\{x\}) = \mathrm{gr}(\{d\})$.

The theorem is a consequence of (8). PROOF: If $\mathrm{gr}(\{x\}) = \{\mathbf{1}\}_{\mathrm{gr}(\{d\})}$, then $x = \mathbf{1}_G$ by [19, (2)], [25, (44)]. □

(11) Let us consider a group G and normal subgroups H, K of G. Suppose (the carrier of H) $\cap$ (the carrier of K) $= \{\mathbf{1}_G\}$. Then (the canonical homomorphism onto cosets of H)$\restriction$(the carrier of K) is one-to-one. PROOF: Set $f =$ the canonical homomorphism onto cosets of H. Set $g = f\restriction$the carrier of K. For every elements x_1, x_2 such that $x_1, x_2 \in \mathrm{dom}\, g$ and $g(x_1) = g(x_2)$ holds $x_1 = x_2$ by [30, (57)], [7, (49)], [25, (46), (103), (51)]. □

Let us consider finite commutative groups G, F, an element a of G, and a homomorphism f from G to F. Now we state the propositions:

(12) The carrier of $\mathrm{gr}(\{f(a)\}) = f^{\circ}$the carrier of $\mathrm{gr}(\{a\})$.

(13) $\mathrm{ord}(f(a)) \leqslant \mathrm{ord}(a)$.

(14) If f is one-to-one, then $\mathrm{ord}(f(a)) = \mathrm{ord}(a)$.

Now we state the propositions:

(15) Let us consider groups G, F, a subgroup H of G, and a homomorphism f from G to F. Then $f\restriction$the carrier of H is a homomorphism from H to F. PROOF: Reconsider $g = f\restriction$the carrier of H as a function from the carrier of H into the carrier of F. For every elements a, b of H, $g(a \cdot b) = g(a) \cdot g(b)$ by [25, (40)], [7, (49)], [25, (43)]. □

(16) Let us consider finite commutative groups G, F, an element a of G, and a homomorphism f from G to F. Suppose $f\restriction$the carrier of $\mathrm{gr}(\{a\})$ is one-to-one. Then $\mathrm{ord}(f(a)) = \mathrm{ord}(a)$. The theorem is a consequence of (15) and (14).

(17) Let us consider a finite commutative group G, a prime number p, a natural number m, and an element a of G. Suppose

(i) $\overline{\overline{G}} = p^m$, and

(ii) $a \neq \mathbf{1}_G$.

Then there exists a natural number n such that $\mathrm{ord}(a) = p^{n+1}$.

(18) Let us consider a prime number p and natural numbers j, m, k. If $m = p^k$ and $p \nmid j$, then $\gcd(j, m) = 1$.

2. Isomorphism of Cyclic Groups of Prime Power Order

Let us consider a strict finite commutative group G, a prime number p, and a natural number m. Now we state the propositions:

(19) Suppose $\overline{\overline{G}} = p^m$. Then there exists a normal strict subgroup K of G and there exist natural numbers n, k and there exists an element g of G such that $\mathrm{ord}(g) = \sup \mathrm{Ordset}(G)$ and K is finite and commutative and

(the carrier of K) $\cap$ (the carrier of $\mathrm{gr}(\{g\})$) $= \{\mathbf{1}_G\}$ and for every element x of G, there exist elements b_1, a_1 of G such that $b_1 \in K$ and $a_1 \in \mathrm{gr}(\{g\})$ and $x = b_1 \cdot a_1$ and $\mathrm{ord}(g) = p^n$ and $k = m - n$ and $n \leqslant m$ and $\overline{\overline{K}} = p^k$ and there exists a homomorphism F from $\prod\langle K, \mathrm{gr}(\{g\})\rangle$ to G such that F is bijective and for every elements a, b of G such that $a \in K$ and $b \in \mathrm{gr}(\{g\})$ holds $F(\langle a, b\rangle) = a \cdot b$.

(20) Suppose $\overline{\overline{G}} = p^m$. Then there exists a non zero natural number k and there exists a k-element finite sequence a of elements of G and there exists a k-element finite sequence I_2 of elements of $\mathbb{N}$ and there exists an associative group-like commutative multiplicative magma family F of $\mathrm{Seg}\,k$ and there exists a homomorphism H_1 from $\prod F$ to G such that for every natural number i such that $i \in \mathrm{Seg}\,k$ there exists an element a_2 of G such that $a_2 = a(i)$ and $F(i) = \mathrm{gr}(\{a_2\})$ and $\mathrm{ord}(a_2) = p^{I_2(i)}$ and for every natural number i such that $1 \leqslant i \leqslant k - 1$ holds $I_2(i) \leqslant I_2(i+1)$ and for every elements p, q of $\mathrm{Seg}\,k$ such that $p \neq q$ holds (the carrier of $F(p)$) $\cap$ (the carrier of $F(q)$) $= \{\mathbf{1}_G\}$ and H_1 is bijective and for every (the carrier of G)-valued total $\mathrm{Seg}\,k$-defined function x such that for every element p of $\mathrm{Seg}\,k$, $x(p) \in F(p)$ holds $x \in \prod F$ and $H_1(x) = \prod x$.

(21) Suppose $\overline{\overline{G}} = p^m$. Then there exists a non zero natural number k and there exists a k-element finite sequence a of elements of G and there exists a k-element finite sequence I_2 of elements of $\mathbb{N}$ and there exists an associative group-like commutative multiplicative magma family F of $\mathrm{Seg}\,k$ such that for every natural number i such that $i \in \mathrm{Seg}\,k$ there exists an element a_2 of G such that $a_2 = a(i)$ and $F(i) = \mathrm{gr}(\{a_2\})$ and $\mathrm{ord}(a_2) = p^{I_2(i)}$ and for every natural number i such that $1 \leqslant i \leqslant k - 1$ holds $I_2(i) \leqslant I_2(i+1)$ and for every elements p, q of $\mathrm{Seg}\,k$ such that $p \neq q$ holds (the carrier of $F(p)$) $\cap$ (the carrier of $F(q)$) $= \{\mathbf{1}_G\}$ and for every element y of G, there exists a (the carrier of G)-valued total $\mathrm{Seg}\,k$-defined function x such that for every element p of $\mathrm{Seg}\,k$, $x(p) \in F(p)$ and $y = \prod x$ and for every (the carrier of G)-valued total $\mathrm{Seg}\,k$-defined functions x_1, x_2 such that for every element p of $\mathrm{Seg}\,k$, $x_1(p) \in F(p)$ and for every element p of $\mathrm{Seg}\,k$, $x_2(p) \in F(p)$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$.

References

[1] Kenichi Arai, Hiroyuki Okazaki, and Yasunari Shidama. Isomorphisms of direct products of finite cyclic groups. *Formalized Mathematics*, 20(**4**):343–347, 2012. doi:10.2478/v10037-012-0038-5.

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

[3] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.

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

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

[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite

sequences. *Formalized Mathematics*, 1(**1**):107–114, 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] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[13] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, 7(**1**):127–134, 1998.
[14] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.
[15] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[16] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[17] Beata Madras. Product of family of universal algebras. *Formalized Mathematics*, 4(**1**): 103–108, 1993.
[18] Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama. Isomorphisms of direct products of finite commutative groups. *Formalized Mathematics*, 21(**1**):65–74, 2013. doi:10.2478/forma-2013-0007.
[19] Dariusz Surowik. Isomorphisms of cyclic groups. Some properties of cyclic groups. *Formalized Mathematics*, 3(**1**):29–32, 1992.
[20] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.
[21] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.
[22] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[23] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[24] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[25] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**): 855–864, 1990.
[26] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[27] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[28] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.
[29] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[30] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[31] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received October 7, 2013