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  
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], [5], [11], [7], [8], [24], [18], [25], [26], [27], [28], [13], [23], [16], [21], [3], [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 $\text{Ordset}(G)$ yielding a subset of $\mathbb{N}$ is defined by the term (Def. 1) the set of all $\text{ord}(a)$ where $a$ is an element of $G$.

One can check that $\text{Ordset}(G)$ 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 $\text{ord}(g) = \text{sup} \text{Ordset}(G)$.

1This work was supported by JSPS KAKENHI 22300285.
(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 $b \in \text{gr} \{a\}$ 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) $\text{gr} \{a\} = n$, and
   
   (ii) $n = p \cdot s$.
   
   Then $\text{ord}(a^p) = s$.

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

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

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

Now we state the proposition:

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

Let $G$ be a strict commutative group and $x$ be an element of $\text{SubGr}(G)$. The functor $\text{NormSp}_{\mathbb{R}}(x)$ 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 $J = f^{-1}(\text{the carrier of } K)$. PROOF: Reconsider $I_3 = f^{-1}(\text{the carrier of } K)$ 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 $J = f^{-1}(\text{the carrier of } K)$. □

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

   (i) $\text{ord}(d) = p$, and
   
   (ii) $p$ is prime, and
   
   (iii) $x \in \text{gr} \{d\}$.
   
   Then

   (iv) $x = 1_G$, or
   
   (v) $\text{gr} \{x\} = \text{gr} \{d\}$. 
The theorem is a consequence of (8). Proof: If \( \text{gr}(\{x\}) = \{1\}_{\text{gr}(d)} \), then \( x = 1_G \) 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 \( K \)) = \( \{1_G\} \). Then (the canonical homomorphism onto cosets of \( H \))(the carrier of \( K \)) is one-to-one. Proof: Set \( f = \) the canonical homomorphism onto cosets of \( H \). For every elements \( x_1, x_2 \) such that \( x_1, x_2 \in \text{dom}g \) 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 \( \text{gr}(\{f(a)\}) = f^\# \) the carrier of \( \text{gr}(\{a\}) \).

(13) \( \text{ord}(f(a)) \leq \text{ord}(a) \).

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

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 \( f \mid \) the carrier of \( H \) is a homomorphism from \( H \) to \( F \). Proof: Reconsider \( g = f \mid \) 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 \( f \mid \) the carrier of \( \text{gr}(\{a\}) \) is one-to-one. Then \( \text{ord}(f(a)) = \text{ord}(a) \). 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) \( \overline{G} = p^m \), and

(ii) \( a \neq 1_G \).

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

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

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

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

References

012-0038-5.


Received October 7, 2013