FORMALIZED MATHEMATICS
Volume 3, Number 1, 1992
Université Catholique de Louvain

Isomorphisms of Cyclic Groups. Some Properties of Cyclic Groups

Dariusz Surowik
Warsaw University
Białystok

Summary. Some theorems and properties of cyclic groups have been proved with special regard to isomorphisms of these groups. Among other things it has been proved that an arbitrary cyclic group is isomorphic with groups of integers with addition or group of integers with addition modulo m. Moreover, it has been proved that two arbitrary cyclic groups of the same order are isomorphic and that the class of cyclic groups is closed in consideration of homomorphism images. Some other properties of groups of this type have been proved too.

MML Identifier: GR_CY_2.

The terminology and notation used in this paper have been introduced in the following articles: [19], [6], [11], [7], [12], [2], [18], [1], [10], [4], [14], [17], [21], [13], [31], [25], [29], [23], [3], [27], [26], [24], [30], [15], [16], [5], [28], [22], [20], [9], and [8]. For simplicity we adopt the following rules: F, G will be groups, G_1 will be a subgroup of G, G_2 will be a cyclic group, H will be a subgroup of G_2, f will be a homomorphism from G to G_2, a, b will be elements of G, g will be an element of G_2, a_1 will be an element of G_1, k, m, n, p, s will be natural numbers, and i, i_1, i_2 will be integers. The following propositions are true:

(1) For all n, m such that $0 < m$ holds $n \bmod m = n - m \cdot (n \div m)$.

(2) If $i_2 > 0$, then $i_1 \bmod i_2 \geq 0$.

(3) If $i_2 > 0$, then $i_1 \bmod i_2 < i_2$.

(4) $i_1 = (i_1 \div i_2) \cdot i_2 + (i_1 \bmod i_2)$.

(5) For all m, n such that $m > 0$ or $n > 0$ there exist i, i_1 such that $i \cdot m + i_1 \cdot n = \gcd(m, n)$.

(6) If $\mathrm{ord}(a) > 1$ and $a = b^k$, then $k \neq 0$.

(7) If G is finite, then $\mathrm{ord}(G) > 0$.

(8) $a \in \mathrm{gr}(\{a\})$.

ISSN 0777–4028

(9) If $a = a_1$, then $\mathrm{gr}(\{a\}) = \mathrm{gr}(\{a_1\})$.

(10) $\mathrm{gr}(\{a\})$ is a cyclic group.

(11) For every strict group G and for every element b of G holds for every element a of G there exists i such that $a = b^i$ if and only if $G = \mathrm{gr}(\{b\})$.

(12) For every strict group G and for every element b of G such that G is finite holds for every element a of G there exists p such that $a = b^p$ if and only if $G = \mathrm{gr}(\{b\})$.

(13) For every strict group G and for every element a of G such that G is finite and $G = \mathrm{gr}(\{a\})$ and for every strict subgroup G_1 of G there exists p such that $G_1 = \mathrm{gr}(\{a^p\})$.

(14) If G is finite and $G = \mathrm{gr}(\{a\})$ and $\mathrm{ord}(G) = n$ and $n = p \cdot s$, then $\mathrm{ord}(a^p) = s$.

(15) If $s \mid k$, then $a^k \in \mathrm{gr}(\{a^s\})$.

(16) If G is finite and $\mathrm{ord}(\mathrm{gr}(\{a^s\})) = \mathrm{ord}(\mathrm{gr}(\{a^k\}))$ and $a^k \in \mathrm{gr}(\{a^s\})$, then $\mathrm{gr}(\{a^s\}) = \mathrm{gr}(\{a^k\})$.

(17) If G is finite and $\mathrm{ord}(G) = n$ and $G = \mathrm{gr}(\{a\})$ and $\mathrm{ord}(G_1) = p$ and $G_1 = \mathrm{gr}(\{a^k\})$, then $n \mid k \cdot p$.

(18) For every strict group G and for every element a of G such that G is finite and $G = \mathrm{gr}(\{a\})$ and $\mathrm{ord}(G) = n$ holds $G = \mathrm{gr}(\{a^k\})$ if and only if $\gcd(k, n) = 1$.

(19) If $G_2 = \mathrm{gr}(\{g\})$ and $g \in H$, then the half group structure of G_2 = the half group structure of H.

(20) If $G_2 = \mathrm{gr}(\{g\})$, then G_2 is finite if and only if there exist i, i_1 such that $i \neq i_1$ and $g^i = g^{i_1}$.

Let us consider n satisfying the condition: $n > 0$. Let h be an element of $\mathbb{Z}_n^+$. The functor ${}^{@}h$ yielding a natural number is defined as follows:

(Def.1) ${}^{@}h = h$.

The following propositions are true:

(21) For every strict cyclic group G_2 such that G_2 is finite and $\mathrm{ord}(G_2) = n$ holds $\mathbb{Z}_n^+$ and G_2 are isomorphic.

(22) For every strict cyclic group G_2 such that G_2 is infinite holds $\mathbb{Z}^+$ and G_2 are isomorphic.

(23) For all strict cyclic groups G_2, H_1 such that H_1 is finite and G_2 is finite and $\mathrm{ord}(H_1) = \mathrm{ord}(G_2)$ holds H_1 and G_2 are isomorphic.

(24) For all strict groups F, G such that F is finite and G is finite and $\mathrm{ord}(F) = p$ and $\mathrm{ord}(G) = p$ and p is prime holds F and G are isomorphic.

(25) For all strict groups F, G such that F is finite and G is finite and $\mathrm{ord}(F) = 2$ and $\mathrm{ord}(G) = 2$ holds F and G are isomorphic.

(26) For every strict group G such that G is finite and $\mathrm{ord}(G) = 2$ and for every strict subgroup H of G holds $H = \{\mathbf{1}\}_G$ or $H = G$.

(27) For every strict group G such that G is finite and $\mathrm{ord}(G) = 2$ holds G is a cyclic group.

(28) For every strict group G such that G is finite and G is a cyclic group and $\mathrm{ord}(G) = n$ and for every p such that $p \mid n$ there exists a strict subgroup G_1 of G such that $\mathrm{ord}(G_1) = p$ and for every strict subgroup G_3 of G such that $\mathrm{ord}(G_3) = p$ holds $G_3 = G_1$.

Let us note that every group which is cyclic is also Abelian.

We now state two propositions:

(29) If $G_2 = \mathrm{gr}(\{g\})$, then for all G, f such that $g \in \mathrm{Im}\, f$ holds f is an epimorphism.

(30) For every strict cyclic group G_2 such that G_2 is finite and $\mathrm{ord}(G_2) = n$ and there exists k such that $n = 2 \cdot k$ there exists an element g_1 of G_2 such that $\mathrm{ord}(g_1) = 2$ and for every element g_2 of G_2 such that $\mathrm{ord}(g_2) = 2$ holds $g_1 = g_2$.

Let us consider G. Then $\mathrm{Z}(G)$ is a strict normal subgroup of G.

One can prove the following propositions:

(31) For every strict cyclic group G_2 such that G_2 is finite and $\mathrm{ord}(G_2) = n$ and there exists k such that $n = 2 \cdot k$ there exists a subgroup H of G_2 such that $\mathrm{ord}(H) = 2$ and H is a cyclic group.

(32) For every strict group G and for every homomorphism g from G to F such that G is a cyclic group holds $\mathrm{Im}\, g$ is a cyclic group.

(33) For all strict groups G, F such that G and F are isomorphic but G is a cyclic group or F is a cyclic group holds G is a cyclic group and F is a cyclic group.

References

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

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

[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 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. Semigroup operations on finite subsets. *Formalized Mathematics*, 1(**4**):651–656, 1990.

[9] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[11] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.

[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[13] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[14] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.
[15] Dariusz Surowik. Cyclic groups and some of their properties - part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[16] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.
[17] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[18] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.
[19] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[20] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[21] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[22] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[23] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[24] Wojciech A. Trybulec. Commutator and center of a group. *Formalized Mathematics*, 2(**4**):461–466, 1991.
[25] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[26] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[27] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[28] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[29] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[30] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received June 5, 1992