JOURNAL OF FORMALIZED MATHEMATICS
Volume 4, Released 1992, Published 2003
Inst. of Computer Science, Univ. of Białystok

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`.

WWW: `http://mizar.org/JFM/Vol4/gr_cy_2.html`

The articles [8], [16], [17], [3], [4], [9], [6], [1], [10], [12], [14], [5], [11], [13], [15], [7], and [2] provide the notation and terminology for this paper.

For simplicity, we adopt the following convention: F, G are groups, G_1 is a subgroup of G, G_2 is a cyclic group, H is a subgroup of G_2, f is a homomorphism from G to G_2, a, b are elements of G, g is an element of G_2, a_1 is an element of G_1, k, m, n, p, s are natural numbers, and i, i_1, i_2 are integers.

One can prove the following propositions:

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

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

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

(4) If $i_2 \neq 0$, then $i_1 = (i_1 \div i_2) \cdot i_2 + (i_1 \bmod i_2)$.

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

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

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

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

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

(13) Let G be a strict group and a be an element of G. Suppose G is finite and $G = \mathrm{gr}(\{a\})$. Let G_1 be a strict subgroup of G. Then 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) Let G be a strict group and a be an element of G. Suppose G is finite and $G = \mathrm{gr}(\{a\})$ and $\mathrm{ord}(G) = n$. Then $G = \mathrm{gr}(\{a^k\})$ if and only if $\gcd(k,n) = 1$.

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

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

Let us consider n. Let us assume that $n > 0$. Let h be an element of $\mathbb{Z}_n^+$. The functor ${}^{@}h$ yielding a natural number is defined by:

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

Next we state a number of propositions:

(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) Let F, G be strict groups. Suppose F is finite and G is finite and $\mathrm{ord}(F) = p$ and $\mathrm{ord}(G) = p$ and p is prime. Then 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) Let G be a strict group. Suppose G is finite and a cyclic group and $\mathrm{ord}(G) = n$. Let given p. Suppose $p \mid n$. Then 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 $G_3 = G_1$.

(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) Let G_2 be a strict cyclic group. Suppose G_2 is finite and $\mathrm{ord}(G_2) = n$ and there exists k such that $n = 2 \cdot k$. Then 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. One can check that $\mathrm{Z}(G)$ is normal.

The following propositions are true:

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

(32) Let G be a strict group and g be a homomorphism from G to F. If G is a cyclic group, then $\mathrm{Im}\, g$ is a cyclic group.

(33) Let G, F be strict groups. Suppose G and F are isomorphic but G is a cyclic group or F is a cyclic group. Then G is a cyclic group and F is a cyclic group.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/finseq_1.html.

[3] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_1.html.

[4] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[5] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/vectsp_1.html.

[6] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_2.html.

[7] Dariusz Surowik. Cyclic groups and some of their properties — part I. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/gr_cy_1.html.

[8] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. http://mizar.org/JFM/Axiomatics/tarski.html.

[9] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/int_1.html.

[10] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/rlvect_1.html.

[11] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_3.html.

[12] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_1.html.

[13] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_4.html.

[14] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_2.html.

[15] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Journal of Formalized Mathematics*, 3, 1991. http://mizar.org/JFM/Vol3/group_6.html.

[16] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/subset_1.html.

[17] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/relat_1.html.

Received June 5, 1992

Published January 2, 2004