JOURNAL OF FORMALIZED MATHEMATICS
Volume 3, Released 1991, Published 2003
Inst. of Computer Science, Univ. of Białystok

Cyclic Groups and Some of Their Properties — Part I

Dariusz Surowik
Warsaw University
Białystok

Summary. Some properties of finite groups are proved. The notion of cyclic group is defined next, some cyclic groups are given, for example the group of integers with addition operations. Chosen properties of cyclic groups are proved next.

MML Identifier: GR_CY_1.

WWW: http://mizar.org/JFM/Vol3/gr_cy_1.html

The articles [16], [9], [24], [4], [3], [17], [25], [7], [11], [8], [15], [1], [10], [6], [18], [13], [2], [19], [23], [12], [21], [22], [14], [20], and [5] provide the notation and terminology for this paper.

For simplicity, we use the following convention: i_1 is an element of $\mathbb{Z}$, j_1, j_2 are integers, p, s, g, k, n, m are natural numbers, G is a group, a, b are elements of G, and I is a finite sequence of elements of $\mathbb{Z}$.

Next we state several propositions:

(1) $m \bmod n = (n \cdot k + m) \bmod n$.

(2) $(p+s) \bmod n = ((p \bmod n) + s) \bmod n$.

(3) $(p+s) \bmod n = (p + (s \bmod n)) \bmod n$.

(4) If $k < n$, then $k \bmod n = k$.

(5) $n \bmod n = 0$.

(6) $0 = 0 \bmod n$.

Let n be a natural number. Let us assume that $n > 0$. The functor $\mathbb{Z}_n$ yielding a non empty subset of $\mathbb{N}$ is defined by:

(Def. 1) $\mathbb{Z}_n = \{p : p < n\}$.

Next we state three propositions:

(10)[1] For all natural numbers n, s such that $n > 0$ holds $s \in \mathbb{Z}_n$ iff $s < n$.

(12)[2] For every natural number n such that $n > 0$ holds $0 \in \mathbb{Z}_n$.

(13) $\mathbb{Z}_1 = \{0\}$.

The binary operation $+_{\mathbb{Z}}$ on $\mathbb{Z}$ is defined as follows:

[1] The propositions (7)–(9) have been removed.
[2] The proposition (11) has been removed.

(Def. 2) For all elements i_1, i_2 of $\mathbb{Z}$ holds $(+_{\mathbb{Z}})(i_1, i_2) = +_{\mathbb{R}}(i_1, i_2)$.

The following propositions are true:

(14) For all j_1, j_2 holds $(+_{\mathbb{Z}})(j_1, j_2) = j_1 + j_2$.

(15) For every i_1 such that $i_1 = 0$ holds i_1 is a unity w.r.t. $+_{\mathbb{Z}}$.

(16) $\mathbf{1}_{+_{\mathbb{Z}}} = 0$.

(17) $+_{\mathbb{Z}}$ has a unity.

(18) $+_{\mathbb{Z}}$ is commutative.

(19) $+_{\mathbb{Z}}$ is associative.

Let F be a finite sequence of elements of $\mathbb{Z}$. The functor $\sum F$ yielding an integer is defined by:

(Def. 3) $\sum F = +_{\mathbb{Z}} \circledast F$.

Next we state a number of propositions:

(20) $\sum(I \frown \langle i_1 \rangle) = \sum I +^{@} i_1$.

(21) $\sum \langle i_1 \rangle = i_1$.

(22) $\sum(\varepsilon_{\mathbb{Z}}) = 0$.

(24)[3] For every finite sequence I of elements of $\mathbb{Z}$ holds $\prod((\mathrm{len}\, I \mapsto a)^I) = a^{\sum I}$.

(25) $b \in \mathrm{gr}(\{a\})$ iff there exists j_1 such that $b = a^{j_1}$.

(26) If G is finite, then a is not of order 0.

(27) If G is finite, then $\mathrm{ord}(a) = \mathrm{ord}(\mathrm{gr}(\{a\}))$.

(28) If G is finite, then $\mathrm{ord}(a) \mid \mathrm{ord}(G)$.

(29) If G is finite, then $a^{\mathrm{ord}(G)} = 1_G$.

(30) If G is finite, then $(a^n)^{-1} = a^{\mathrm{ord}(G) - (n \bmod \mathrm{ord}(G))}$.

(31) For every strict group G such that $\mathrm{ord}(G) > 1$ there exists an element a of G such that $a \neq 1_G$.

(32) Let G be a strict group. Suppose G is finite and $\mathrm{ord}(G) = p$ and p is prime. Let H be a strict subgroup of G. Then $H = \{\mathbf{1}\}_G$ or $H = G$.

(33) $\langle \mathbb{Z}, +_{\mathbb{Z}} \rangle$ is associative and group-like.

The strict group $\mathbb{Z}^+$ is defined by:

(Def. 4) $\mathbb{Z}^+ = \langle \mathbb{Z}, +_{\mathbb{Z}} \rangle$.

Let us consider n. Let us assume that $n > 0$. The functor $+_n$ yields a binary operation on $\mathbb{Z}_n$ and is defined as follows:

(Def. 5) For all elements k, l of $\mathbb{Z}_n$ holds $+_n(k, l) = (k + l) \bmod n$.

One can prove the following proposition

(34) For every n such that $n > 0$ holds $\langle \mathbb{Z}_n, +_n \rangle$ is associative and group-like.

[3] The proposition (23) has been removed.

Let us consider n. Let us assume that $n > 0$. The functor $\mathbb{Z}^+_n$ yields a strict group and is defined as follows:

(Def. 6) $\mathbb{Z}^+_n = \langle \mathbb{Z}_n, +_n \rangle$.

Next we state two propositions:

(35) $1_{\mathbb{Z}^+} = 0$.

(36) For every n such that $n > 0$ holds $1_{\mathbb{Z}^+_n} = 0$.

Let h be an element of $\mathbb{Z}^+$. The functor ${}^@h$ yielding an integer is defined as follows:

(Def. 7) ${}^@h = h$.

Let h be an integer. The functor ${}^@h$ yielding an element of $\mathbb{Z}^+$ is defined as follows:

(Def. 8) ${}^@h = h$.

One can prove the following proposition

(37) For every element h of $\mathbb{Z}^+$ holds $h^{-1} = -{}^@h$.

In the sequel h denotes an element of $\mathbb{Z}^+$.
Next we state two propositions:

(38) For every h such that $h = 1$ and for every k holds $h^k = k$.

(39) For all h, j_1 such that $h = 1$ holds $j_1 = h^{j_1}$.

Let I_1 be a group. We say that I_1 is cyclic if and only if:

(Def. 9) There exists an element a of I_1 such that the groupoid of $I_1 = \mathrm{gr}(\{a\})$.

One can check that there exists a group which is strict and cyclic.
We now state several propositions:

(40) $\{\mathbf{1}\}_G$ is cyclic.

(41) G is a cyclic group if and only if there exists an element a of G such that for every element b of G there exists j_1 such that $b = a^{j_1}$.

(42) Suppose G is finite. Then G is a cyclic group if and only if there exists an element a of G such that for every element b of G there exists n such that $b = a^n$.

(43) Let G be a strict group. Suppose G is finite. Then G is a cyclic group if and only if there exists an element a of G such that $\mathrm{ord}(a) = \mathrm{ord}(G)$.

(44) For every strict subgroup H of G such that G is finite and a cyclic group holds H is a cyclic group.

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

(46) For every n such that $n > 0$ there exists an element g of $\mathbb{Z}^+_n$ such that for every element b of $\mathbb{Z}^+_n$ there exists j_1 such that $b = g^{j_1}$.

One can verify that every group which is cyclic is also commutative.
The following propositions are true:

(48)[4] $\mathbb{Z}^+$ is cyclic.

(49) For every n such that $n > 0$ holds $\mathbb{Z}^+_n$ is a cyclic group.

(50) $\mathbb{Z}^+$ is a commutative group.

(51) For every n such that $n > 0$ holds $\mathbb{Z}^+_n$ is a commutative group.

[4] The proposition (47) has been removed.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/card_1.html`.

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

[3] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/ordinal1.html`.

[4] Grzegorz Bancerek. Sequences of ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/ordinal2.html`.

[5] 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`.

[6] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/binop_1.html`.

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

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

[9] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/zfmisc_1.html`.

[10] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finset_1.html`.

[11] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/real_1.html`.

[12] 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`.

[13] 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`.

[14] Andrzej Trybulec. Binary operations applied to functions. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funcop_1.html`.

[15] Andrzej Trybulec. Semilattice operations on finite subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/setwiseo.html`.

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

[17] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

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

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

[20] Wojciech A. Trybulec. Binary operations on finite sequences. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finsop_1.html`.

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

[22] 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`.

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

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

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

Received November 22, 1991

Published January 2, 2004