FORMALIZED MATHEMATICS
Vol.2,No.5, November–December 1991
Université Catholique de Louvain

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`.

The articles [19], [7], [12], [8], [13], [2], [3], [16], [6], [5], [18], [1], [11], [4], [15], [28], [17], [21], [14], [23], [27], [22], [25], [26], [24], [20], [10], and [9] provide the notation and terminology for this paper. For simplicity we adopt the following rules: i_1 denotes an element of $\mathbb{Z}$, j_1 denotes an integer, p, s, k, n, l, m denote natural numbers, x is arbitrary, G denotes a group, a, b denote elements of G, and I denotes a finite sequence of elements of $\mathbb{Z}$. We now state several propositions:

(1) For every n such that $n > 0$ holds $m \bmod n = (n \cdot k + m) \bmod n$.

(2) For every n such that $n > 0$ holds $(p+s) \bmod n = ((p \bmod n)+s) \bmod n$.

(3) For every n such that $n > 0$ holds $(p+s) \bmod n = (p+(s \bmod n)) \bmod n$.

(4) For every k such that $k < n$ holds $k \bmod n = k$.

(5) For every n such that $n > 0$ holds $n \bmod n = 0$.

(6) For every n such that $n > 0$ holds $0 = 0 \bmod n$.

(7) If $k + l = m$, then $l \leq m$.

(8) For all k, l, m such that $l = m$ and $m = k + l$ holds $k = 0$.

Let us consider n satisfying the condition: $n > 0$. The functor $\mathbb{Z}_n$ yields a non-empty subset of $\mathbb{N}$ and is defined by:

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

We now state several propositions:

ISSN 0777–4028

(9) For every n such that $n > 0$ holds if $x \in \mathbb{Z}_n$, then x is a natural number.
(10) For every n such that $n > 0$ holds $s \in \mathbb{Z}_n$ if and only if $s < n$.
(11) For every n such that $n > 0$ holds $\mathbb{Z}_n \subseteq \mathbb{N}$.
(12) For every 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 by:

(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 integers i_1, i_2 holds $(+_{\mathbb{Z}})(i_1, i_2) = i_1 + i_2$.
(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 $\sum F$ yields an integer and is defined by:

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

Next we state several propositions:

(20) $\sum(I \frown \langle i_1 \rangle) = \sum I + {}^{@}i_1$.
(21) $\sum \langle i_1 \rangle = i_1$.
(22) $\sum(\varepsilon_{\mathbb{Z}}) = 0$.
(23) For all non-empty sets D, D_1 holds $\varepsilon_D = \varepsilon_{D_1}$.
(24) For every finite sequence I of elements of $\mathbb{Z}$ holds $\prod((\operatorname{len} I \longmapsto a)^I) = a^{\sum I}$.

Let G be a group, and let a be an element of G. Then $\{a\}$ is a subset of G.

We now state several propositions:

(25) $b \in \operatorname{gr}(\{a\})$ if and only if 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 $\operatorname{ord}(a) = \operatorname{ord}(\operatorname{gr}(\{a\}))$.
(28) If G is finite, then $\operatorname{ord}(a) \mid \operatorname{ord}(G)$.
(29) If G is finite, then $a^{\operatorname{ord}(G)} = 1_G$.
(30) If G is finite, then $(a^n)^{-1} = a^{\operatorname{ord}(G) - (n \bmod \operatorname{ord}(G))}$.
(31) For every strict group G such that $\operatorname{ord}(G) > 1$ there exists an element a of G such that $a \neq 1_G$.
(32) For every strict group G such that G is finite and $\operatorname{ord}(G) = p$ and p is prime and for every strict subgroup H of G holds $H = \{\mathbf{1}\}_G$ or $H = G$.
(33) $\langle \mathbb{Z}, +_{\mathbb{Z}} \rangle$ is a group.

The group $\mathbb{Z}^+$ is defined as follows:

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

Let D be a non-empty set, and let D_1 be a non-empty subset of D, and let D_2 be a non-empty subset of D_1. We see that the element of D_2 is an element of D_1.

Let us consider n satisfying the condition: $n > 0$. The functor $+_n$ yielding a binary operation on $\mathbb{Z}_n$ is defined by:

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

Next we state the proposition

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

Let us consider n satisfying the condition: $n > 0$. The functor $\mathbb{Z}_n^+$ yields a strict group and is defined by:

(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 ${}^{@}h$ yields an integer and 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) ${}^{@}h = h$.

The following proposition is true

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

In the sequel G_1 will denote a subgroup of $\mathbb{Z}^+$ and h will denote 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 $j_1 = h^{j_1}$.

A strict group is said to be a cyclic group if:

(Def.9) there exists an element a of it such that it $= \mathrm{gr}(\{a\})$.

One can prove the following propositions:

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

(41) For every strict group G holds 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) For every strict group G such that G is finite holds 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) For every strict group G such that G is finite holds 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 G is a cyclic group and H is a subgroup of G 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 $b = g^{j_1}$.

(47) If G is a cyclic group, then G is an Abelian group.

(48) $\mathbb{Z}^+$ is a cyclic group.

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

(50) $\mathbb{Z}^+$ is an Abelian group.

(51) For every n such that $n > 0$ holds $\mathbb{Z}_n^+$ is an Abelian 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. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

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

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

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

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

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

[14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[15] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

[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. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[24] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[25] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[26] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[27] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[28] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received November 22, 1991