JOURNAL OF FORMALIZED MATHEMATICS
Volume 2, Released 1990, Published 2003
Inst. of Computer Science, Univ. of Białystok

Groups

Wojciech A. Trybulec
Warsaw University

Summary. Notions of group and abelian group are introduced. The power of an element of a group, order of group and order of an element of a group are defined. Basic theorems concerning those notions are presented.

MML Identifier: GROUP_1.

WWW: http://mizar.org/JFM/Vol2/group_1.html

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

For simplicity, we use the following convention: m, n are natural numbers, i, j are integers, S is a non empty groupoid, and r, s, s_1, s_2, t are elements of S.

Let i be an integer. Then $|i|$ is a natural number.

Let A be a non empty set and let m be a binary operation on A. One can check that $\langle A, m\rangle$ is non empty.

Let I_1 be a non empty groupoid. We say that I_1 is unital if and only if:

(Def. 1) There exists an element e of I_1 such that for every element h of I_1 holds $h \cdot e = h$ and $e \cdot h = h$.

We say that I_1 is group-like if and only if the condition (Def. 3) is satisfied.

(Def. 3)[1] There exists an element e of I_1 such that for every element h of I_1 holds $h \cdot e = h$ and $e \cdot h = h$ and there exists an element g of I_1 such that $h \cdot g = e$ and $g \cdot h = e$.

Let us observe that every non empty groupoid which is group-like is also unital.

One can check that there exists a non empty groupoid which is strict, group-like, and associative.

A group is a group-like associative non empty groupoid.

The following propositions are true:

(5)[2] Suppose for all r, s, t holds $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ and there exists t such that for every s_1 holds $s_1 \cdot t = s_1$ and $t \cdot s_1 = s_1$ and there exists s_2 such that $s_1 \cdot s_2 = t$ and $s_2 \cdot s_1 = t$. Then S is a group.

(6) Suppose for all r, s, t holds $(r \cdot s) \cdot t = r \cdot (s \cdot t)$ and for all r, s holds there exists t such that $r \cdot t = s$ and there exists t such that $t \cdot r = s$. Then S is associative and group-like.

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

In the sequel G denotes a group-like non empty groupoid and e, h denote elements of G.

Let G be a unital non empty groupoid. The functor 1_G yielding an element of G is defined as follows:

[1] The definition (Def. 2) has been removed.
[2] The propositions (1)–(4) have been removed.

(Def. 4) For every element h of G holds $h \cdot 1_G = h$ and $1_G \cdot h = h$.

The following proposition is true

(10)[3] If for every h holds $h \cdot e = h$ and $e \cdot h = h$, then $e = 1_G$.

In the sequel G denotes a group and f, g, h denote elements of G.
Let us consider G, h. The functor h^{-1} yielding an element of G is defined as follows:

(Def. 5) $h \cdot h^{-1} = 1_G$ and $h^{-1} \cdot h = 1_G$.

The following propositions are true:

(12)[4] If $h \cdot g = 1_G$ and $g \cdot h = 1_G$, then $g = h^{-1}$.

(14)[5] If $h \cdot g = h \cdot f$ or $g \cdot h = f \cdot h$, then $g = f$.

(15) If $h \cdot g = h$ or $g \cdot h = h$, then $g = 1_G$.

(16) $(1_G)^{-1} = 1_G$.

(17) If $h^{-1} = g^{-1}$, then $h = g$.

(18) If $h^{-1} = 1_G$, then $h = 1_G$.

(19) $(h^{-1})^{-1} = h$.

(20) If $h \cdot g = 1_G$ or $g \cdot h = 1_G$, then $h = g^{-1}$ and $g = h^{-1}$.

(21) $h \cdot f = g$ iff $f = h^{-1} \cdot g$.

(22) $f \cdot h = g$ iff $f = g \cdot h^{-1}$.

(23) There exists f such that $g \cdot f = h$.

(24) There exists f such that $f \cdot g = h$.

(25) $(h \cdot g)^{-1} = g^{-1} \cdot h^{-1}$.

(26) $g \cdot h = h \cdot g$ iff $(g \cdot h)^{-1} = g^{-1} \cdot h^{-1}$.

(27) $g \cdot h = h \cdot g$ iff $g^{-1} \cdot h^{-1} = h^{-1} \cdot g^{-1}$.

(28) $g \cdot h = h \cdot g$ iff $g \cdot h^{-1} = h^{-1} \cdot g$.

Let us consider G. The functor $\cdot_G^{-1}$ yields a unary operation on the carrier of G and is defined by:

(Def. 6) $\cdot_G^{-1}(h) = h^{-1}$.

Next we state several propositions:

(31)[6] For every associative non empty groupoid G holds the multiplication of G is associative.

(32) For every unital non empty groupoid G holds 1_G is a unity w.r.t. the multiplication of G.

(33) For every unital non empty groupoid G holds $\mathbf{1}_{\text{the multiplication of } G} = 1_G$.

(34) For every unital non empty groupoid G holds the multiplication of G has a unity.

(35) $\cdot_G^{-1}$ is an inverse operation w.r.t. the multiplication of G.

[3] The propositions (8) and (9) have been removed.
[4] The proposition (11) has been removed.
[5] The proposition (13) has been removed.
[6] The propositions (29) and (30) have been removed.

(36) The multiplication of G has an inverse operation.

(37) The inverse operation w.r.t. the multiplication of $G = \cdot_G^{-1}$.

Let G be a unital non empty groupoid. The functor power_G yielding a function from $[:$the carrier of G, $\mathbb{N}:]$ into the carrier of G is defined by:

(Def. 7) For every element h of G holds $\mathrm{power}_G(h, 0) = 1_G$ and for every n holds $\mathrm{power}_G(h, n+1) = \mathrm{power}_G(h, n) \cdot h$.

Let us consider G, i, h. The functor h^i yields an element of G and is defined by:

(Def. 8) $h^i = \begin{cases} \mathrm{power}_G(h, |i|), \text{ if } 0 \leq i, \\ \mathrm{power}_G(h, |i|)^{-1}, \text{ otherwise.} \end{cases}$

Let us consider G, n, h. Then h^n can be characterized by the condition:

(Def. 9) $h^n = \mathrm{power}_G(h, n)$.

Next we state a number of propositions:

(42)[7] $(1_G)^n = 1_G$.

(43) $h^0 = 1_G$.

(44) $h^1 = h$.

(45) $h^2 = h \cdot h$.

(46) $h^3 = h \cdot h \cdot h$.

(47) $h^2 = 1_G$ iff $h^{-1} = h$.

(48) $h^{n+m} = h^n \cdot h^m$.

(49) $h^{n+1} = h^n \cdot h$ and $h^{n+1} = h \cdot h^n$.

(50) $h^{n \cdot m} = (h^n)^m$.

(51) $(h^{-1})^n = (h^n)^{-1}$.

(52) If $g \cdot h = h \cdot g$, then $g \cdot h^n = h^n \cdot g$.

(53) If $g \cdot h = h \cdot g$, then $g^n \cdot h^m = h^m \cdot g^n$.

(54) If $g \cdot h = h \cdot g$, then $(g \cdot h)^n = g^n \cdot h^n$.

(55) If $0 \leq i$, then $h^i = h^{|i|}$.

(56) If $0 \not\leq i$, then $h^i = (h^{|i|})^{-1}$.

(59)[8] If $i = 0$, then $h^i = 1_G$.

(60) If $i \leq 0$, then $h^i = (h^{|i|})^{-1}$.

(61) $(1_G)^i = 1_G$.

(62) $h^{-1} = h^{-1}$.

(63) $h^{i+j} = h^i \cdot h^j$.

(64) $h^{n+j} = h^n \cdot h^j$.

(65) $h^{i+m} = h^i \cdot h^m$.

[7] The propositions (38)–(41) have been removed.
[8] The propositions (57) and (58) have been removed.

(66) $h^{j+1} = h^j \cdot h$ and $h^{j+1} = h \cdot h^j$.

(67) $h^{i \cdot j} = (h^i)^j$.

(68) $h^{n \cdot j} = (h^n)^j$.

(69) $h^{i \cdot m} = (h^i)^m$.

(70) $h^{-i} = (h^i)^{-1}$.

(71) $h^{-n} = (h^n)^{-1}$.

(72) $(h^{-1})^i = (h^i)^{-1}$.

(73) If $g \cdot h = h \cdot g$, then $(g \cdot h)^i = g^i \cdot h^i$.

(74) If $g \cdot h = h \cdot g$, then $g^i \cdot h^j = h^j \cdot g^i$.

(75) If $g \cdot h = h \cdot g$, then $g^n \cdot h^j = h^j \cdot g^n$.

(77)[9] If $g \cdot h = h \cdot g$, then $g \cdot h^i = h^i \cdot g$.

Let us consider G, h. We say that h is of order 0 if and only if:

(Def. 10) If $h^n = 1_G$, then $n = 0$.

We introduce h is of order 0 as a synonym of h is of order 0. We introduce h is not of order 0 as an antonym of h is of order 0.

One can prove the following proposition

(79)[10] 1_G is not of order 0.

Let us consider G, h. The functor $\mathrm{ord}(h)$ yielding a natural number is defined as follows:

(Def. 11)(i) $\mathrm{ord}(h) = 0$ if h is of order 0,

(ii) $h^{\mathrm{ord}(h)} = 1_G$ and $\mathrm{ord}(h) \neq 0$ and for every m such that $h^m = 1_G$ and $m \neq 0$ holds $\mathrm{ord}(h) \leq m$, otherwise.

Next we state four propositions:

(82)[11] $h^{\mathrm{ord}(h)} = 1_G$.

(84)[12] $\mathrm{ord}(1_G) = 1$.

(85) If $\mathrm{ord}(h) = 1$, then $h = 1_G$.

(86) If $h^n = 1_G$, then $\mathrm{ord}(h) \mid n$.

Let us consider G. The functor $\mathrm{Ord}(G)$ yielding a cardinal number is defined by:

(Def. 12) $\mathrm{Ord}(G) = \overline{\overline{\text{the carrier of } G}}$.

Let S be a 1-sorted structure. We say that S is finite if and only if:

(Def. 13) The carrier of S is finite.

We introduce S is infinite as an antonym of S is finite.

Let us consider G. Let us assume that G is finite. The functor $\mathrm{ord}(G)$ yields a natural number and is defined as follows:

[9] The proposition (76) has been removed.
[10] The proposition (78) has been removed.
[11] The propositions (80) and (81) have been removed.
[12] The proposition (83) has been removed.

(Def. 14) There exists a finite set B such that $B =$ the carrier of G and $\mathrm{ord}(G) = \mathrm{card}\, B$.

One can prove the following proposition

(90)[13] If G is finite, then $\mathrm{ord}(G) \geq 1$.

One can verify that there exists a group which is strict and commutative.
One can prove the following proposition

(92)[14] $\langle \mathbb{R}, +_{\mathbb{R}} \rangle$ is a commutative group.

In the sequel A denotes a commutative group and a, b denote elements of A.
The following three propositions are true:

(94)[15] $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

(95) $(a \cdot b)^{n} = a^{n} \cdot b^{n}$.

(96) $(a \cdot b)^{i} = a^{i} \cdot b^{i}$.

Let A be a non empty set, let m be a binary operation on A, and let u be an element of A. One can check that $\langle A, m, u \rangle$ is non empty.
The following proposition is true

(97) $\langle$the carrier of A, the multiplication of A, $1_A\rangle$ is Abelian, add-associative, right zeroed, and right complementable.

In the sequel B denotes an Abelian group.
We now state the proposition

(98) $\langle$the carrier of B, the addition of $B\rangle$ is a commutative group.

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

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

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

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

[7] Czesław Byliński. Binary operations applied to finite sequences. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/finseqop.html`.

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

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

[10] 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`.

[11] Jan Popiołek. Some properties of functions modul and signum. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/absvalue.html`.

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

[13] The propositions (87)–(89) have been removed.
[14] The proposition (91) has been removed.
[15] The proposition (93) has been removed.

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

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

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

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

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

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

Received July 3, 1990

Published January 2, 2004