FORMALIZED MATHEMATICS
Vol.1, No.5, November–December 1990
Université Catholique de Louvain

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.

The notation and terminology used in this paper are introduced in the following articles: [6], [7], [9], [2], [3], [5], [12], [11], [1], [8], [4], [10], and [13]. We follow the rules: x is arbitrary, m, n are natural numbers, and i, j are integers. Let N be a non-empty subset of $\mathbb{R}$, and let D be a non-empty set, and let f be a function from N into D, and let n be an element of N. Then $f(n)$ is an element of D.

Let D be a non-empty set, and let N be a non-empty subset of $\mathbb{R}$, and let E be a non-empty set, and let f be a function from $[\!: D, N :\!]$ into E, and let h be an element of D, and let n be an element of N. Then $f(h, n)$ is an element of E.

Let us consider i. Then $|i|$ is a natural number.

We consider half group structures which are systems

$\langle$a carrier, an operation$\rangle$,

where the carrier is a non-empty set and the operation is a binary operation on the carrier. In the sequel S denotes a half group structure. Let us consider S. An element of S is an element of the carrier of S.

In the sequel r, s, s_1, s_2, t will be elements of S. Let us consider S, x. The predicate $x \in S$ is defined as follows:

(Def.1) $x \in$ the carrier of S.

The following propositions are true:

(1) $x \in S$ if and only if $x \in$ the carrier of S.

(2) $s \in S$.

ISSN 0777–4028

(3) If $x \in S$, then x is an element of S.

Let us consider S, s_1, s_2. The functor $s_1 \cdot s_2$ yielding an element of S is defined by:

(Def.2) $s_1 \cdot s_2 =$ (the operation of S)(s_1, s_2).

One can prove the following proposition

(4) $s_1 \cdot s_2 =$ (the operation of S)(s_1, s_2).

A half group structure is called a group if:

(Def.3) (i) for all elements f, g, h of it holds $(f \cdot g) \cdot h = f \cdot (g \cdot h)$,

(ii) there exists an element e of it such that for every element h of it holds $h \cdot e = h$ and $e \cdot h = h$ and there exists an element g of it such that $h \cdot g = e$ and $g \cdot h = e$.

We now state three propositions:

(5) If 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) If 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 a group.

(7) $\langle \mathbb{R}, +_{\mathbb{R}} \rangle$ is a group.

We follow a convention: G denotes a group and e, f, g, h denote elements of G. Next we state two propositions:

(8) $(h \cdot g) \cdot f = h \cdot (g \cdot f)$.

(9) There exists e such that for every h holds $h \cdot e = h$ and $e \cdot h = h$ and there exists g such that $h \cdot g = e$ and $g \cdot h = e$.

Let us consider G. The functor 1_G yielding an element of G is defined by:

(Def.4) $h \cdot (1_G) = h$ and $(1_G) \cdot h = h$.

One can prove the following two propositions:

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

(11) $h \cdot (1_G) = h$ and $(1_G) \cdot h = h$.

Let us consider G, h. The functor h^{-1} yields an element of G and is defined as follows:

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

One can prove the following propositions:

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

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

(14) 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) $h \cdot f = g$ if and only if $f = h^{-1} \cdot g$.

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

(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) $g \cdot h = h \cdot g$ if and only if $(g \cdot h)^{-1} = g^{-1} \cdot h^{-1}$.

(27) $g \cdot h = h \cdot g$ if and only if $g^{-1} \cdot h^{-1} = h^{-1} \cdot g^{-1}$.

(28) $g \cdot h = h \cdot g$ if and only if $g \cdot h^{-1} = h^{-1} \cdot g$.

In the sequel u is a unary operation on the carrier of 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) $\cdot_G^{-1}(h) = h^{-1}$.

We now state several propositions:

(29) If for every h holds $u(h) = h^{-1}$, then $u = \cdot_G^{-1}$.

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

(31) The operation of G is associative.

(32) 1_G is a unity w.r.t. the operation of G.

(33) $\mathbf{1}_{\text{the operation of } G} = 1_G$.

(34) The operation of G has a unity.

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

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

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

Let us consider G. The functor power_G yields a function from $[\!:$ the carrier of G, $\mathbb{N}\,:\!]$ into the carrier of G and is defined by:

(Def.7) $\text{power}_G(h, 0) = 1_G$ and for every n holds $\text{power}_G(h, n+1) = \text{power}_G(h, n) \cdot h$.

In the sequel H is a function from $[\!:$ the carrier of G, $\mathbb{N}\,:\!]$ into the carrier of G. We now state three propositions:

(38) If for every h holds $H(h, 0) = 1_G$ and for every n holds $H(h, n+1) = H(h, n) \cdot h$, then $H = \text{power}_G$.

(39) $\text{power}_G(h, 0) = 1_G$.

(40) $\text{power}_G(h, n+1) = \text{power}_G(h, n) \cdot h$.

Let us consider G, n, h. The functor h^n yields an element of G and is defined as follows:

(Def.8) $h^n = \text{power}_G(h, n)$.

We now state a number of propositions:

(41) $h^n = \text{power}_G(h, n)$.

(42) $(1_G)^n = 1_G$.

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

(44) $h^1 = h$.

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

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

(47) $h^2 = 1_G$ if and only if $h^{-1} = h$.

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

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

(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 $(g \cdot h)^n = g^n \cdot h^n$.

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

(Def.9) $h^i = h^{|i|}$ if $0 \leq i$, $h^i = (h^{|i|})^{-1}$, otherwise.

The following propositions are true:

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

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

(57) If $i < 0$, then $h^i = (h^{|i|})^{-1}$.

(58) If $i = n$, then $h^i = h^n$.

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

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

(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 $g^n \cdot h^j = h^j \cdot g^n$.

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

(77) 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 now state two propositions:

(78) h is of order 0 if and only if for every n such that $h^n = 1_G$ holds $n = 0$.

(79) 1_G is not of order 0.

Let us consider G, h. The functor $\mathrm{ord}(h)$ yields a natural number and is defined by:

(Def.11) $\mathrm{ord}(h) = 0$ if h is of order 0, $h^{\mathrm{ord}(h)} = 1_G$ 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.

One can prove the following propositions:

(80) If h is not of order 0 and $h^m = 1_G$ and $m \neq 0$ and for every n such that $h^n = 1_G$ and $n \neq 0$ holds $m \leq n$, then $m = \mathrm{ord}(h)$.

(81) h is of order 0 if and only if $\mathrm{ord}(h) = 0$.

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

(83) If h is not of order 0 and $h^m = 1_G$ and $m \neq 0$, then $\mathrm{ord}(h) \leq m$.

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

(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 as follows:

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

We now state the proposition

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

We now define two new predicates. Let us consider G. We say that G is finite if and only if:

(Def.13) the carrier of G is finite.

We say that G is infinite if and only if G is not finite.

The following proposition is true

(88) G is finite if and only if the carrier of G is finite.

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

(Def.14) $\mathrm{ord}(G) = \mathrm{card}\,(\text{the carrier of } G)$.

Next we state two propositions:

(89) If G is finite, then $\mathrm{ord}(G) = \mathrm{card}\,(\text{the carrier of } G)$.

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

A group is called an Abelian group if:

(Def.15) for all elements a, b of it holds $a \cdot b = b \cdot a$.

We now state two propositions:

(91) If for all h, g holds $h \cdot g = g \cdot h$, then G is an Abelian group.

(92) $\langle \mathbb{R}, +_{\mathbb{R}} \rangle$ is an Abelian group.

In the sequel A is an Abelian group and a, b are elements of A. One can prove the following propositions:

(93) $a \cdot b = b \cdot a$.

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

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

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

(97) $\langle$The carrier of A, the operation of $A, \cdot_A^{-1}, 1_A\rangle$ is an Abelian group.

In the sequel B denotes an Abelian group. We now state two propositions:

(98) $\langle$The carrier of B, the addition of $B\rangle$ is an Abelian group.

(99) $-1 < 0$.

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

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

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

[11] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.

[12] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(**1**):187–190, 1990.

[13] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

Received July 3, 1990