FORMALIZED MATHEMATICS
Volume 12, Number 3, 2004
University of Białystok

Properties of Groups[1]

Gijs Geleijnse[2]
Eindhoven University of Technology

Grzegorz Bancerek
Białystok Technical University

Summary. In this article we formalize theorems from Chapter 1 of [7]. Our article covers Theorems 1.5.4, 1.5.5 (inequality on indices), 1.5.6 (equality of indices), Lemma 1.6.1 and several other supporting theorems needed to complete the formalization.

MML Identifier: GROUP_8.

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

For simplicity, we adopt the following rules: G is a strict group, a, b, x, y, z are elements of the carrier of G, H, K are strict subgroups of G, p is a natural number, and A is a subset of the carrier of G.

We now state a number of propositions:

(1) If p is prime and $\mathrm{ord}(G) = p$ and G is finite, then there exists a such that $\mathrm{ord}(a) = p$.

(2) Let a_1, a_2 be elements of the carrier of H and b_1, b_2 be elements of the carrier of G. If $a_1 = b_1$ and $a_2 = b_2$, then $a_1 \cdot a_2 = b_1 \cdot b_2$.

(3) Let a be an element of the carrier of H and b be an element of the carrier of G. If $a = b$, then for every natural number n holds $a^n = b^n$.

(4) Let a be an element of the carrier of H and b be an element of the carrier of G. If $a = b$, then for every integer i holds $a^i = b^i$.

[1]This work has been partially supported by the CALCULEMUS grant HPRN-CT-2000-00102.
[2]The author visited the University of Białystok as a guest.

ISSN 1426–2630

(5) Let a be an element of the carrier of H and b be an element of the carrier of G. If $a = b$ and G is finite, then $\mathrm{ord}(a) = \mathrm{ord}(b)$.

(6) For every element h of the carrier of G such that $h \in H$ holds $H \cdot h \subseteq$ the carrier of H.

(7) For every a such that $a \neq 1_G$ holds $\mathrm{gr}(\{a\}) \neq \{\mathbf{1}\}_G$.

(8) For every integer m holds $(1_G)^m = 1_G$.

(9) For every integer m holds $a^{m \cdot \mathrm{ord}(a)} = 1_G$.

(10) For every a such that a is not of order 0 and for every integer m holds $a^m = a^{m \bmod \mathrm{ord}(a)}$.

(11) If b is not of order 0, then $\mathrm{gr}(\{b\})$ is finite.

(12) If b is of order 0, then b^{-1} is of order 0.

(13) b is of order 0 iff for every integer n such that $b^n = 1_G$ holds $n = 0$.

(14) Let given G. Given a such that $a \neq 1_G$. Then for every H holds $H = G$ or $H = \{\mathbf{1}\}_G$ if and only if the following conditions are satisfied:

(i) G is a cyclic group and finite, and

(ii) there exists a natural number p such that $\mathrm{ord}(G) = p$ and p is prime.

(15) Let x, y, z be elements of the carrier of G and A be a subset of the carrier of G. Then $z \in x \cdot A \cdot y$ if and only if there exists an element a of the carrier of G such that $z = x \cdot a \cdot y$ and $a \in A$.

(16) For every non empty subset A of G and for every element x of the carrier of G holds $\overline{\overline{A}} = \overline{\overline{x^{-1} \cdot A \cdot x}}$.

Let us consider G, H, K. The functor DoubleCosets(H, K) yielding a family of subsets of the carrier of G is defined as follows:

(Def. 1) $A \in$ DoubleCosets(H, K) iff there exists a such that $A = H \cdot a \cdot K$.

We now state two propositions:

(17) $z \in H \cdot x \cdot K$ iff there exist elements g, h of the carrier of G such that $z = g \cdot x \cdot h$ and $g \in H$ and $h \in K$.

(18) For all H, K holds $H \cdot x \cdot K = H \cdot y \cdot K$ or it is not true that there exists z such that $z \in H \cdot x \cdot K$ and $z \in H \cdot y \cdot K$.

In the sequel B, A denote strict subgroups of G and D denotes a strict subgroup of A.

Let us consider G, A. Observe that the left cosets of A is non empty.

Let us consider G and let H be a subgroup of G. We introduce $[G : H]_{\mathbb{N}}$ as a synonym of $|\bullet : H|_{\mathbb{N}}$.

Next we state several propositions:

(19) If $G = A \sqcup B$ and $D = A \cap B$ and G is finite, then $[G : B]_{\mathbb{N}} \geqslant [A : D]_{\mathbb{N}}$.

(20) If G is finite, then $[G : H]_{\mathbb{N}} > 0$.

(21) Let G be a strict group. Suppose G is finite. Let C be a strict subgroup of G and A, B be strict subgroups of C. Suppose $C = A \sqcup B$. Let D be a

strict subgroup of A. Suppose $D = A \cap B$. Let E be a strict subgroup of B. Suppose $E = A \cap B$. Let F be a strict subgroup of C. Suppose $F = A \cap B$. Suppose the left cosets of B is finite and the left cosets of A is finite and $[A : C]_{\mathbb{N}}$ and $[B : C]_{\mathbb{N}}$ are relative prime. Then $[B : C]_{\mathbb{N}} = [D : A]_{\mathbb{N}}$ and $[A : C]_{\mathbb{N}} = [E : B]_{\mathbb{N}}$.

(22) For every element a of the carrier of G such that $a \in H$ and for every integer j holds $a^j \in H$.

(23) For every strict group G such that $G \neq \{\mathbf{1}\}_G$ there exists an element b of the carrier of G such that $b \neq 1_G$.

(24) Let G be a strict group and a be an element of the carrier of G. Suppose $G = \mathrm{gr}(\{a\})$ and $G \neq \{\mathbf{1}\}_G$. Let H be a strict subgroup of G. If $H \neq \{\mathbf{1}\}_G$, then there exists a natural number k such that $0 < k$ and $a^k \in H$.

(25) Let G be a strict cyclic group. Suppose $G \neq \{\mathbf{1}\}_G$. Let H be a strict subgroup of G. If $H \neq \{\mathbf{1}\}_G$, then H is a cyclic group.

Acknowledgments

Thanks to the Mizar Group for their help and hospitality.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[6] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[7] Marshall Hall Jr. *The Theory of Groups.* The Macmillan Company, New York, 1959.
[8] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[9] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[10] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[11] Dariusz Surowik. Cyclic groups and some of their properties - part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[12] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[13] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[14] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[15] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[16] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[17] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[18] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[20] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received May 31, 2004