FORMALIZED MATHEMATICS
Vol.2, No.4, September–October 1991
Université Catholique de Louvain

Homomorphisms and Isomorphisms of Groups. Quotient Group

Wojciech A. Trybulec
Warsaw University

Michał J. Trybulec
Warsaw University

Summary. Quotient group, homomorphisms and isomorphisms of groups are introduced. The so called isomorphism theorems are proved following [7].

MML Identifier: GROUP_6.

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

(1) For all non-empty sets A, B and for every function f from A into B holds f is one-to-one if and only if for all elements a, b of A such that $f(a) = f(b)$ holds $a = b$.

Let G be a group, and let A be a subgroup of G. We see that the subgroup of A is a subgroup of G.

Let G be a group, and let A be a subgroup of G. We see that the normal subgroup of A is a subgroup of A.

Let G be a group. Then $\{\mathbf{1}\}_G$ is a normal subgroup of G. Then Ω_G is a normal subgroup of G.

For simplicity we adopt the following rules: n is a natural number, i is an integer, G, H, I are groups, A, B are subgroups of G, N, M are normal subgroups of G, a, a_1, a_2, a_3, b are elements of G, c is an element of H, f is a function from the carrier of G into the carrier of H, x is arbitrary, and A_1, A_2 are subsets of G. One can prove the following propositions:

(2) For every subgroup X of A and for every element x of A such that $x = a$ holds $x \cdot X = a \cdot X$ **qua** a subgroup of G and $X \cdot x = (X$ **qua** a subgroup of $G) \cdot a$.

(3) For all subgroups X, Y of A holds $(X$ **qua** a subgroup of $G) \cap Y$ **qua** a subgroup of $G = X \cap Y$.

ISSN 0777–4028

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

(5) If $b \in N$, then $b^a \in N$.

(6) $a \cdot A \cdot A = a \cdot A$ and $a \cdot (A \cdot A) = a \cdot A$ and $A \cdot A \cdot a = A \cdot a$ and $A \cdot (A \cdot a) = A \cdot a$.

(7) If $A_1 = \{[a, b]\}$, then $G^{c} = \mathrm{gr}(A_1)$.

(8) G^{c} is a subgroup of B if and only if for all a, b holds $[a, b] \in B$.

(9) If N is a subgroup of B, then N is a normal subgroup of B.

Let us consider G, B, M. Let us assume that M is a subgroup of B. The functor $(M)_B$ yielding a normal subgroup of B is defined as follows:

(Def.1) $(M)_B = M$.

One can prove the following proposition

(10) $B \cap N$ is a normal subgroup of B and $N \cap B$ is a normal subgroup of B.

Let us consider G, B, N. Then $B \cap N$ is a normal subgroup of B.

Let us consider G, N, B. Then $N \cap B$ is a normal subgroup of B.

A group is trivial if:

(Def.2) there exists x such that the carrier of it $= \{x\}$.

One can prove the following propositions:

(11) $\{\mathbf{1}\}_G$ is trivial.

(12) G is trivial if and only if $\mathrm{ord}(G) = 1$ and G is finite.

(13) If G is trivial, then $\{\mathbf{1}\}_G = G$.

Let us consider G, N. The functor $\mathrm{Cosets}\, N$ yielding a non-empty set is defined by:

(Def.3) $\mathrm{Cosets}\, N =$ the left cosets of N.

In the sequel W_1, W_2 denote elements of $\mathrm{Cosets}\, N$. One can prove the following propositions:

(14) $\mathrm{Cosets}\, N =$ the left cosets of N and $\mathrm{Cosets}\, N =$ the right cosets of N.

(15) If $x \in \mathrm{Cosets}\, N$, then there exists a such that $x = a \cdot N$ and $x = N \cdot a$.

(16) $a \cdot N \in \mathrm{Cosets}\, N$ and $N \cdot a \in \mathrm{Cosets}\, N$.

(17) If $x \in \mathrm{Cosets}\, N$, then x is a subset of G.

(18) If $A_1 \in \mathrm{Cosets}\, N$ and $A_2 \in \mathrm{Cosets}\, N$, then $A_1 \cdot A_2 \in \mathrm{Cosets}\, N$.

Let us consider G, N. The functor $\mathrm{CosOp}\, N$ yields a binary operation on $\mathrm{Cosets}\, N$ and is defined by:

(Def.4) for all W_1, W_2, A_1, A_2 such that $W_1 = A_1$ and $W_2 = A_2$ holds $(\mathrm{CosOp}\, N)(W_1, W_2) = A_1 \cdot A_2$.

In the sequel O is a binary operation on $\mathrm{Cosets}\, N$. One can prove the following two propositions:

(19) If for all W_1, W_2, A_1, A_2 such that $W_1 = A_1$ and $W_2 = A_2$ holds $O(W_1, W_2) = A_1 \cdot A_2$, then $O = \mathrm{CosOp}\, N$.

(20) For all W_1, W_2, A_1, A_2 such that $W_1 = A_1$ and $W_2 = A_2$ holds $(\mathrm{CosOp}\,N)(W_1, W_2) = A_1 \cdot A_2$.

Let us consider G, N. The functor ${}^{G}/_{N}$ yields a half group structure and is defined as follows:

(Def.5) ${}^{G}/_{N} = \langle \mathrm{Cosets}\,N, \mathrm{CosOp}\,N \rangle$.

One can prove the following propositions:

(21) ${}^{G}/_{N} = \langle \mathrm{Cosets}\,N, \mathrm{CosOp}\,N \rangle$.

(22) The carrier of ${}^{G}/_{N} = \mathrm{Cosets}\,N$.

(23) The operation of ${}^{G}/_{N} = \mathrm{CosOp}\,N$.

In the sequel S, T_1, T_2 denote elements of ${}^{G}/_{N}$. Let us consider G, N, S. The functor ${}^{@}S$ yields a subset of G and is defined by:

(Def.6) ${}^{@}S = S$.

One can prove the following two propositions:

(24) $({}^{@}T_1) \cdot ({}^{@}T_2) = T_1 \cdot T_2$.

(25) ${}^{@}T_1 \cdot T_2 = ({}^{@}T_1) \cdot ({}^{@}T_2)$.

Let us consider G, N. Then ${}^{G}/_{N}$ is a group.

In the sequel S will denote an element of ${}^{G}/_{N}$. The following propositions are true:

(26) There exists a such that $S = a \cdot N$ and $S = N \cdot a$.

(27) $N \cdot a$ is an element of ${}^{G}/_{N}$ and $a \cdot N$ is an element of ${}^{G}/_{N}$ and $\overline{N}$ is an element of ${}^{G}/_{N}$.

(28) $x \in {}^{G}/_{N}$ if and only if there exists a such that $x = a \cdot N$ and $x = N \cdot a$.

(29) $1_{{}^{G}/_{N}} = \overline{N}$.

(30) If $S = a \cdot N$, then $S^{-1} = a^{-1} \cdot N$.

(31) If the left cosets of N is finite, then ${}^{G}/_{N}$ is finite.

(32) $\mathrm{Ord}({}^{G}/_{N}) = |\bullet : N|$.

(33) If the left cosets of N is finite, then $\mathrm{ord}({}^{G}/_{N}) = |\bullet : N|_{\mathbb{N}}$.

(34) If M is a subgroup of B, then ${}^{B}/_{(M)_B}$ is a subgroup of ${}^{G}/_{M}$.

(35) If M is a subgroup of N, then ${}^{N}/_{(M)_N}$ is a normal subgroup of ${}^{G}/_{M}$.

(36) ${}^{G}/_{N}$ is an Abelian group if and only if G^{c} is a subgroup of N.

Let us consider G, H. A function from the carrier of G into the carrier of H is called a homomorphism from G to H if:

(Def.7) $\mathrm{it}(a \cdot b) = \mathrm{it}(a) \cdot \mathrm{it}(b)$.

One can prove the following proposition

(37) If for all a, b holds $f(a \cdot b) = f(a) \cdot f(b)$, then f is a homomorphism from G to H.

In the sequel g, h will be homomorphisms from G to H, g_1 will be a homomorphism from H to G, and h_1 will be a homomorphism from H to I. One can prove the following propositions:

(38) $\operatorname{dom} g =$ the carrier of G and $\operatorname{rng} g \subseteq$ the carrier of H.

(39) $g(a \cdot b) = g(a) \cdot g(b)$.

(40) $g(1_G) = 1_H$.

(41) $g(a^{-1}) = g(a)^{-1}$.

(42) $g(a^b) = g(a)^{g(b)}$.

(43) $g([a, b]) = [g(a), g(b)]$.

(44) $g([a_1, a_2, a_3]) = [g(a_1), g(a_2), g(a_3)]$.

(45) $g(a^n) = g(a)^n$.

(46) $g(a^i) = g(a)^i$.

(47) $\mathrm{id}_{(\text{the carrier of } G)}$ is a homomorphism from G to G.

(48) $h_1 \cdot h$ is a homomorphism from G to I.

Let us consider G, H, I, h, h_1. Then $h_1 \cdot h$ is a homomorphism from G to I.

Let us consider G, H, g. Then $\operatorname{rng} g$ is a subset of H.

Let us consider G, H. The functor $G \to \{\mathbf{1}\}_H$ yields a homomorphism from G to H and is defined by:

(Def.8) for every a holds $(G \to \{\mathbf{1}\}_H)(a) = 1_H$.

The following proposition is true

(49) $h_1 \cdot (G \to \{\mathbf{1}\}_H) = G \to \{\mathbf{1}\}_I$ and $(H \to \{\mathbf{1}\}_I) \cdot h = G \to \{\mathbf{1}\}_I$.

Let us consider G, N. The canonical homomorphism onto cosets of N yielding a homomorphism from G to ${}^G/_N$ is defined as follows:

(Def.9) for every a holds (the canonical homomorphism onto cosets of N)$(a) = a \cdot N$.

Let us consider G, H, g. The functor $\operatorname{Ker} g$ yields a normal subgroup of G and is defined by:

(Def.10) the carrier of $\operatorname{Ker} g = \{a : g(a) = 1_H\}$.

The following three propositions are true:

(50) $a \in \operatorname{Ker} h$ if and only if $h(a) = 1_H$.

(51) $\operatorname{Ker}(G \to \{\mathbf{1}\}_H) = G$.

(52) Ker(the canonical homomorphism onto cosets of N) $= N$.

Let us consider G, H, g. The functor $\operatorname{Im} g$ yields a subgroup of H and is defined as follows:

(Def.11) the carrier of $\operatorname{Im} g = g^\circ$ (the carrier of G).

Next we state a number of propositions:

(53) $\operatorname{rng} g =$ the carrier of $\operatorname{Im} g$.

(54) $x \in \operatorname{Im} g$ if and only if there exists a such that $x = g(a)$.

(55) $\operatorname{Im} g = \operatorname{gr}(\operatorname{rng} g)$.

(56) $\operatorname{Im}(G \to \{\mathbf{1}\}_H) = \{\mathbf{1}\}_H$.

(57) Im(the canonical homomorphism onto cosets of N) $= {}^G/_N$.

(58) h is a homomorphism from G to $\operatorname{Im} h$.

(59) If G is finite, then $\mathrm{Im}\, g$ is finite.

(60) If G is an Abelian group, then $\mathrm{Im}\, g$ is an Abelian group.

(61) $\mathrm{Ord}(\mathrm{Im}\, g) \leq \mathrm{Ord}(G)$.

(62) If G is finite, then $\mathrm{ord}(\mathrm{Im}\, g) \leq \mathrm{ord}(G)$.

We now define two new predicates. Let us consider G, H, h. We say that h is a monomorphism if and only if:

(Def.12) h is one-to-one.

We say that h is an epimorphism if and only if:

(Def.13) $\mathrm{rng}\, h =$ the carrier of H.

We now state several propositions:

(63) If h is a monomorphism and $c \in \mathrm{Im}\, h$, then $h(h^{-1}(c)) = c$.

(64) If h is a monomorphism, then $h^{-1}(h(a)) = a$.

(65) If h is a monomorphism, then h^{-1} is a homomorphism from $\mathrm{Im}\, h$ to G.

(66) h is a monomorphism if and only if $\mathrm{Ker}\, h = \{\mathbf{1}\}_G$.

(67) h is an epimorphism if and only if $\mathrm{Im}\, h = H$.

(68) If h is an epimorphism, then for every c there exists a such that $h(a) = c$.

(69) The canonical homomorphism onto cosets of N is an epimorphism.

Let us consider G, H, h. We say that h is an isomorphism if and only if:

(Def.14) h is an epimorphism and h is a monomorphism.

One can prove the following propositions:

(70) h is an isomorphism if and only if $\mathrm{rng}\, h =$ the carrier of H and h is one-to-one.

(71) If h is an isomorphism, then $\mathrm{dom}\, h =$ the carrier of G and $\mathrm{rng}\, h =$ the carrier of H.

(72) If h is an isomorphism, then h^{-1} is a homomorphism from H to G.

(73) If h is an isomorphism and $g_1 = h^{-1}$, then g_1 is an isomorphism.

(74) If h is an isomorphism and h_1 is an isomorphism, then $h_1 \cdot h$ is an isomorphism.

(75) The canonical homomorphism onto cosets of $\{\mathbf{1}\}_G$ is an isomorphism.

Let us consider G, H. We say that G and H are isomorphic if and only if:

(Def.15) there exists h such that h is an isomorphism.

We now state a number of propositions:

(76) G and G are isomorphic.

(77) If G and H are isomorphic, then H and G are isomorphic.

(78) If G and H are isomorphic and H and I are isomorphic, then G and I are isomorphic.

(79) If h is a monomorphism, then G and $\mathrm{Im}\, h$ are isomorphic.

(80) If G is trivial and H is trivial, then G and H are isomorphic.

(81) $\{\mathbf{1}\}_G$ and $\{\mathbf{1}\}_H$ are isomorphic.

(82) G and ${}^{G}/_{\{\mathbf{1}\}_G}$ are isomorphic and ${}^{G}/_{\{\mathbf{1}\}_G}$ and G are isomorphic.

(83) ${}^{G}/_{\Omega_G}$ is trivial.

(84) If G and H are isomorphic, then $\mathrm{Ord}(G) = \mathrm{Ord}(H)$.

(85) If G and H are isomorphic but G is finite or H is finite, then G is finite and H is finite.

(86) If G and H are isomorphic but G is finite or H is finite, then $\mathrm{ord}(G) = \mathrm{ord}(H)$.

(87) If G and H are isomorphic but G is trivial or H is trivial, then G is trivial and H is trivial.

(88) If G and H are isomorphic but G is an Abelian group or H is an Abelian group, then G is an Abelian group and H is an Abelian group.

(89) ${}^{G}/_{\mathrm{Ker}\, g}$ and $\mathrm{Im}\, g$ are isomorphic and $\mathrm{Im}\, g$ and ${}^{G}/_{\mathrm{Ker}\, g}$ are isomorphic.

(90) There exists a homomorphism h from ${}^{G}/_{\mathrm{Ker}\, g}$ to $\mathrm{Im}\, g$ such that h is an isomorphism and $g = h\cdot$ the canonical homomorphism onto cosets of $\mathrm{Ker}\, g$.

(91) For every normal subgroup J of ${}^{G}/_{M}$ such that $J = {}^{N}/_{(M)_N}$ and M is a subgroup of N holds ${}^{({}^{G}/_{M})}/_{J}$ and ${}^{G}/_{N}$ are isomorphic.

(92) ${}^{(B \sqcup N)}/_{(N)_{B \sqcup N}}$ and ${}^{B}/_{(B \cap N)}$ are isomorphic.

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] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[6] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[7] M. I. Kargapołow and J. I. Mierzlakow. *Podstawy teorii grup*. PWN, Warszawa, 1989.
[8] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[9] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.
[10] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[11] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[12] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[13] Wojciech A. Trybulec. Commutator and center of a group. *Formalized Mathematics*, 2(**4**):461–466, 1991.
[14] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[15] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[16] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.

Received October 3, 1991