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

Classes of Conjugation. Normal Subgroups

Wojciech A. Trybulec[1]
Warsaw University

Summary. Theorems that were not proved in [8] and in [9] are discussed. In the article we define notion of conjugation for elements, subsets and subgroups of a group. We define the classes of conjugation. Normal subgroups of a group and normalizer of a subset of a group or of a subgroup are introduced. We also define the set of all subgroups of a group. An auxiliary theorem that belongs rather to [1] is proved.

MML Identifier: `GROUP_3`.

The papers [3], [10], [5], [2], [8], [9], [6], [4], and [7] provide the notation and terminology for this paper. For simplicity we follow a convention: x, y are arbitrary, X denotes a set, G denotes a group, a, b, c, d, g, h denote elements of G, A, B, C, D denote subsets of G, H, H_1, H_2, H_3 denote subgroups of G, n denotes a natural number, and i denotes an integer. Next we state a number of propositions:

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

(2) G is an Abelian group if and only if the operation of G is commutative.

(3) $\{\mathbf{1}\}_G$ is an Abelian group.

(4) If $A \subseteq B$ and $C \subseteq D$, then $A \cdot C \subseteq B \cdot D$.

(5) If $A \subseteq B$, then $a \cdot A \subseteq a \cdot B$ and $A \cdot a \subseteq B \cdot a$.

(6) If H_1 is a subgroup of H_2, then $a \cdot H_1 \subseteq a \cdot H_2$ and $H_1 \cdot a \subseteq H_2 \cdot a$.

(7) $a \cdot H = \{a\} \cdot H$.

(8) $H \cdot a = H \cdot \{a\}$.

(9) $(a \cdot A) \cdot H = a \cdot (A \cdot H)$.

(10) $(A \cdot a) \cdot H = A \cdot (a \cdot H)$.

(11) $(a \cdot H) \cdot A = a \cdot (H \cdot A)$.

(12) $(A \cdot H) \cdot a = A \cdot (H \cdot a)$.

[1]Supported by RPBP.III-24.C1

ISSN 0777–4028

(13) $(H \cdot a) \cdot A = H \cdot (a \cdot A)$.

(14) $(H \cdot A) \cdot a = H \cdot (A \cdot a)$.

(15) $(H_1 \cdot a) \cdot H_2 = H_1 \cdot (a \cdot H_2)$.

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

(Def.1) $x \in \mathrm{SubGr}\, G$ if and only if x is a subgroup of G.

In the sequel D denotes a non-empty set. Next we state four propositions:

(16) If for every x holds $x \in D$ if and only if x is a subgroup of G, then $D = \mathrm{SubGr}\, G$.

(17) $x \in \mathrm{SubGr}\, G$ if and only if x is a subgroup of G.

(18) $G \in \mathrm{SubGr}\, G$.

(19) If G is finite, then $\mathrm{SubGr}\, G$ is finite.

Let us consider G, a, b. The functor a^b yielding an element of G is defined as follows:

(Def.2) $a^b = (b^{-1} \cdot a) \cdot b$.

One can prove the following propositions:

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

(21) If $a^g = b^g$, then $a = b$.

(22) $(1_G)^a = 1_G$.

(23) If $a^b = 1_G$, then $a = 1_G$.

(24) $a^{1_G} = a$.

(25) $a^a = a$.

(26) $(a^a)^{-1} = a$ and $(a^{-1})^a = a^{-1}$.

(27) $a^b = a$ if and only if $a \cdot b = b \cdot a$.

(28) $(a \cdot b)^g = a^g \cdot b^g$.

(29) $(a^g)^h = a^{g \cdot h}$.

(30) $((a^b)^b)^{-1} = a$ and $((a^b)^{-1})^b = a$.

(31) $a^b = c$ if and only if $a = (c^b)^{-1}$.

(32) $(a^{-1})^b = (a^b)^{-1}$.

(33) $(a^n)^b = (a^b)^n$.

(34) $(a^i)^b = (a^b)^i$.

(35) If G is an Abelian group, then $a^b = a$.

(36) If for all a, b holds $a^b = a$, then G is an Abelian group.

Let us consider G, A, B. The functor A^B yielding a subset of G is defined as follows:

(Def.3) $A^B = \{g^h : g \in A \wedge h \in B\}$.

We now state a number of propositions:

(37) $A^B = \{g^h : g \in A \wedge h \in B\}$.

(38) $x \in A^B$ if and only if there exist g, h such that $x = g^h$ and $g \in A$ and $h \in B$.

(39) $A^B \neq \emptyset$ if and only if $A \neq \emptyset$ and $B \neq \emptyset$.

(40) $A^B \subseteq (B^{-1} \cdot A) \cdot B$.

(41) $(A \cdot B)^C \subseteq A^C \cdot B^C$.

(42) $(A^B)^C = A^{B \cdot C}$.

(43) $(A^{-1})^B = (A^B)^{-1}$.

(44) $\{a\}^{\{b\}} = \{a^b\}$.

(45) $\{a\}^{\{b,c\}} = \{a^b, a^c\}$.

(46) $\{a, b\}^{\{c\}} = \{a^c, b^c\}$.

(47) $\{a, b\}^{\{c,d\}} = \{a^c, a^d, b^c, b^d\}$.

We now define two new functors. Let us consider G, A, g. The functor A^g yields a subset of G and is defined as follows:

(Def.4) $A^g = A^{\{g\}}$.

The functor g^A yields a subset of G and is defined by:

(Def.5) $g^A = \{g\}^A$.

Next we state a number of propositions:

(48) $A^g = A^{\{g\}}$.

(49) $g^A = \{g\}^A$.

(50) $x \in A^g$ if and only if there exists h such that $x = h^g$ and $h \in A$.

(51) $x \in g^A$ if and only if there exists h such that $x = g^h$ and $h \in A$.

(52) $g^A \subseteq (A^{-1} \cdot g) \cdot A$.

(53) $(A^B)^g = A^{B \cdot g}$.

(54) $(A^g)^B = A^{g \cdot B}$.

(55) $(g^A)^B = g^{A \cdot B}$.

(56) $(A^a)^b = A^{a \cdot b}$.

(57) $(a^A)^b = a^{A \cdot b}$.

(58) $(a^b)^A = a^{b \cdot A}$.

(59) $A^g = (g^{-1} \cdot A) \cdot g$.

(60) $(A \cdot B)^a \subseteq A^a \cdot B^a$.

(61) $A^{1_G} = A$.

(62) If $A \neq \emptyset$, then $(1_G)^A = \{1_G\}$.

(63) $((A^a)^a)^{-1} = A$ and $((A^a)^{-1})^a = A$.

(64) $A = B^g$ if and only if $B = (A^g)^{-1}$.

(65) G is an Abelian group if and only if for all A, B such that $B \neq \emptyset$ holds $A^B = A$.

(66) G is an Abelian group if and only if for all A, g holds $A^g = A$.

(67) G is an Abelian group if and only if for all A, g such that $A \neq \emptyset$ holds $g^A = \{g\}$.

Let us consider G, H, a. The functor H^a yielding a subgroup of G is defined by:

(Def.6) the carrier of $H^a = \overline{H}^a$.

The following propositions are true:

(68) If the carrier of $H_1 = \overline{H}^a$, then $H_1 = H^a$.

(69) The carrier of $H^a = \overline{H}^a$.

(70) $x \in H^a$ if and only if there exists g such that $x = g^a$ and $g \in H$.

(71) The carrier of $H^a = (a^{-1} \cdot H) \cdot a$.

(72) $(H^a)^b = H^{a \cdot b}$.

(73) $H^{1_G} = H$.

(74) $((H^a)^a)^{-1} = H$ and $((H^a)^{-1})^a = H$.

(75) $H_1 = H_2^a$ if and only if $H_2 = (H_1^a)^{-1}$.

(76) $(H_1 \cap H_2)^a = H_1^a \cap H_2^a$.

(77) $\mathrm{Ord}(H) = \mathrm{Ord}(H^a)$.

(78) H is finite if and only if H^a is finite.

(79) If H is finite, then $\mathrm{ord}(H) = \mathrm{ord}(H^a)$.

(80) $\{\mathbf{1}\}_G^a = \{\mathbf{1}\}_G$.

(81) If $H^a = \{\mathbf{1}\}_G$, then $H = \{\mathbf{1}\}_G$.

(82) ${\Omega_G}^a = G$.

(83) If $H^a = G$, then $H = G$.

(84) $|\bullet : H| = |\bullet : H^a|$.

(85) If the left cosets of H is finite, then $|\bullet : H|_{\mathbb{N}} = |\bullet : H^a|_{\mathbb{N}}$.

(86) If G is an Abelian group, then for all H, a holds $H^a = H$.

Let us consider G, a, b. We say that a and b are conjugated if and only if:

(Def.7) there exists g such that $a = b^g$.

We now state several propositions:

(87) a and b are conjugated if and only if there exists g such that $a = b^g$.

(88) a and b are conjugated if and only if there exists g such that $b = a^g$.

(89) a and a are conjugated.

(90) If a and b are conjugated, then b and a are conjugated.

(91) If a and b are conjugated and b and c are conjugated, then a and c are conjugated.

(92) If a and 1_G are conjugated or 1_G and a are conjugated, then $a = 1_G$.

(93) $a^{\overline{\Omega_G}} = \{b : a \text{ and } b \text{ are conjugated }\}$.

Let us consider G, a. The functor $a^\bullet$ yielding a subset of G is defined by:

(Def.8) $a^\bullet = a^{\overline{\Omega_G}}$.

We now state several propositions:

(94) $a^\bullet = a^{\overline{\Omega_G}}$.

(95) $x \in a^\bullet$ if and only if there exists b such that $b = x$ and a and b are conjugated.

(96) $a \in b^\bullet$ if and only if a and b are conjugated.

(97) $a^g \in a^\bullet$.

(98) $a \in a^\bullet$.

(99) If $a \in b^\bullet$, then $b \in a^\bullet$.

(100) $a^\bullet = b^\bullet$ if and only if $a^\bullet$ meets $b^\bullet$.

(101) $a^\bullet = \{1_G\}$ if and only if $a = 1_G$.

(102) $a^\bullet \cdot A = A \cdot a^\bullet$.

Let us consider G, A, B. We say that A and B are conjugated if and only if:

(Def.9) there exists g such that $A = B^g$.

We now state several propositions:

(103) A and B are conjugated if and only if there exists g such that $A = B^g$.

(104) A and B are conjugated if and only if there exists g such that $B = A^g$.

(105) A and A are conjugated.

(106) If A and B are conjugated, then B and A are conjugated.

(107) If A and B are conjugated and B and C are conjugated, then A and C are conjugated.

(108) $\{a\}$ and $\{b\}$ are conjugated if and only if a and b are conjugated.

(109) If A and $\overline{H_1}$ are conjugated, then there exists H_2 such that the carrier of $H_2 = A$.

Let us consider G, A. The functor $A^\bullet$ yielding a family of subsets of the carrier of G is defined as follows:

(Def.10) $A^\bullet = \{B : A \text{ and } B \text{ are conjugated }\}$.

The following propositions are true:

(110) $A^\bullet = \{B : A \text{ and } B \text{ are conjugated }\}$.

(111) $x \in A^\bullet$ if and only if there exists B such that $x = B$ and A and B are conjugated.

(112) If $x \in A^\bullet$, then x is a subset of G.

(113) $A \in B^\bullet$ if and only if A and B are conjugated.

(114) $A^g \in A^\bullet$.

(115) $A \in A^\bullet$.

(116) If $A \in B^\bullet$, then $B \in A^\bullet$.

(117) $A^\bullet = B^\bullet$ if and only if $A^\bullet$ meets $B^\bullet$.

(118) $\{a\}^\bullet = \{\{b\} : b \in a^\bullet\}$.

(119) If G is finite, then $A^\bullet$ is finite.

Let us consider G, H_1, H_2. We say that H_1 and H_2 are conjugated if and only if:

(Def.11) there exists g such that $H_1 = H_2^g$.

The following propositions are true:

(120) H_1 and H_2 are conjugated if and only if there exists g such that $H_1 = H_2^g$.

(121) H_1 and H_2 are conjugated if and only if there exists g such that $H_2 = H_1^g$.

(122) H_1 and H_1 are conjugated.

(123) If H_1 and H_2 are conjugated, then H_2 and H_1 are conjugated.

(124) If H_1 and H_2 are conjugated and H_2 and H_3 are conjugated, then H_1 and H_3 are conjugated.

In the sequel L denotes a subset of $\mathrm{SubGr}\, G$. Let us consider G, H. The functor $H^\bullet$ yielding a subset of $\mathrm{SubGr}\, G$ is defined as follows:

(Def.12) $x \in H^\bullet$ if and only if there exists H_1 such that $x = H_1$ and H and H_1 are conjugated.

One can prove the following propositions:

(125) If for every x holds $x \in L$ if and only if there exists H such that $x = H$ and H_1 and H are conjugated, then $L = H_1^\bullet$.

(126) $x \in H_1^\bullet$ if and only if there exists H_2 such that $x = H_2$ and H_1 and H_2 are conjugated.

(127) If $x \in H^\bullet$, then x is a subgroup of G.

(128) $H_1 \in H_2^\bullet$ if and only if H_1 and H_2 are conjugated.

(129) $H^g \in H^\bullet$.

(130) $H \in H^\bullet$.

(131) If $H_1 \in H_2^\bullet$, then $H_2 \in H_1^\bullet$.

(132) $H_1^\bullet = H_2^\bullet$ if and only if $H_1^\bullet$ meets $H_2^\bullet$.

(133) If G is finite, then $H^\bullet$ is finite.

(134) H_1 and H_2 are conjugated if and only if $\overline{H_1}$ and $\overline{H_2}$ are conjugated.

Let us consider G. A subgroup of G is called a normal subgroup of G if:

(Def.13) for every a holds $\mathrm{it}^a = \mathrm{it}$.

One can prove the following proposition

(135) If for every a holds $H = H^a$, then H is a normal subgroup of G.

In the sequel N, N_1, N_2 will denote ha normal subgroups of G. We now state a number of propositions:

(136) $N^a = N$.

(137) $\{\mathbf{1}\}_G$ is a normal subgroup of G and Ω_G is a normal subgroup of G.

(138) $N_1 \cap N_2$ is a normal subgroup of G.

(139) If G is an Abelian group, then H is a normal subgroup of G.

(140) H is a normal subgroup of G if and only if for every a holds $a \cdot H = H \cdot a$.

(141) H is a normal subgroup of G if and only if for every a holds $a \cdot H \subseteq H \cdot a$.

(142) H is a normal subgroup of G if and only if for every a holds $H \cdot a \subseteq a \cdot H$.

(143) H is a normal subgroup of G if and only if for every A holds $A \cdot H = H \cdot A$.

(144) H is a normal subgroup of G if and only if for every a holds H is a subgroup of H^a.

(145) H is a normal subgroup of G if and only if for every a holds H^a is a subgroup of H.

(146) H is a normal subgroup of G if and only if $H^\bullet = \{H\}$.

(147) H is a normal subgroup of G if and only if for every a such that $a \in H$ holds $a^\bullet \subseteq \overline{H}$.

(148) $\overline{N_1} \cdot \overline{N_2} = \overline{N_2} \cdot \overline{N_1}$.

(149) There exists N such that the carrier of $N = \overline{N_1} \cdot \overline{N_2}$.

(150) The left cosets of $N =$ the right cosets of N.

(151) If the left cosets of H is finite and $|\bullet : H|_{\mathbb{N}} = 2$, then H is a normal subgroup of G.

Let us consider G, A. The functor $\mathrm{N}(A)$ yielding a subgroup of G is defined by:

(Def.14) the carrier of $\mathrm{N}(A) = \{h : A^h = A\}$.

We now state several propositions:

(152) If the carrier of $H = \{h : A^h = A\}$, then $H = \mathrm{N}(A)$.

(153) The carrier of $\mathrm{N}(A) = \{h : A^h = A\}$.

(154) $x \in \mathrm{N}(A)$ if and only if there exists h such that $x = h$ and $A^h = A$.

(155) $\overline{\overline{A^\bullet}} = |\bullet : \mathrm{N}(A)|$.

(156) If $A^\bullet$ is finite or the left cosets of $\mathrm{N}(A)$ is finite, then $\mathrm{card}\, A^\bullet = |\bullet : \mathrm{N}(A)|_{\mathbb{N}}$.

(157) $\overline{\overline{a^\bullet}} = |\bullet : \mathrm{N}(\{a\})|$.

(158) If $a^\bullet$ is finite or the left cosets of $\mathrm{N}(\{a\})$ is finite, then $\mathrm{card}\, a^\bullet = |\bullet : \mathrm{N}(\{a\})|_{\mathbb{N}}$.

Let us consider G, H. The functor $\mathrm{N}(H)$ yields a subgroup of G and is defined as follows:

(Def.15) $\mathrm{N}(H) = \mathrm{N}(\overline{H})$.

We now state several propositions:

(159) $\mathrm{N}(H) = \mathrm{N}(\overline{H})$.

(160) $x \in \mathrm{N}(H)$ if and only if there exists h such that $x = h$ and $H^h = H$.

(161) $\overline{\overline{H^\bullet}} = |\bullet : \mathrm{N}(H)|$.

(162) If $H^\bullet$ is finite or the left cosets of $\mathrm{N}(H)$ is finite, then $\mathrm{card}\, H^\bullet = |\bullet : \mathrm{N}(H)|_{\mathbb{N}}$.

(163) H is a normal subgroup of G if and only if $\mathrm{N}(H) = G$.

(164) $\mathrm{N}(\{\mathbf{1}\}_G) = G$.

(165) $\mathrm{N}(\Omega_G) = G$.

(166) If X is finite and $\mathrm{card}\, X = 2$, then there exist x, y such that $x \neq y$ and $X = \{x, y\}$.

References

[1] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

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

[5] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[6] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

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

[8] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[9] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.

[10] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.

Received August 10, 1990