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

Classes of Conjugation. Normal Subgroups

Wojciech A. Trybulec
Warsaw University

Summary. Theorems that were not proved in [13] and in [14] 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 normalizator 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 [2] is proved.

MML Identifier: GROUP_3.

WWW: http://mizar.org/JFM/Vol2/group_3.html

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

For simplicity, we use the following convention: x, y are sets, G is a group, a, b, c, g, h are elements of G, A, B, C, D are subsets of G, H, H_1, H_2, H_3 are subgroups of G, n is a natural number, and i is an integer.

One can prove the following 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 a commutative group iff the multiplication of G is commutative.

(3) $\{\mathbf{1}\}_G$ is commutative.

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

(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 set is defined as follows:

(Def. 1) $x \in \mathrm{SubGr}\,G$ iff x is a strict subgroup of G.

Let us consider G. Observe that $\mathrm{SubGr}\,G$ is non empty.
The following propositions are true:

(18)[1] For every strict group G holds $G \in \mathrm{SubGr}\,G$.

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

We now state a number of 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) $a^b = a$ iff $a \cdot b = b \cdot a$.

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

(32)[2] $(a^{-1})^b = (a^b)^{-1}$.

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

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

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

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

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

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

One can prove the following propositions:

(38)[3] $x \in A^B$ iff there exist g, h such that $x = g^h$ and $g \in A$ and $h \in B$.

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

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

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

[1] The propositions (16) and (17) have been removed.
[2] The proposition (31) has been removed.
[3] The proposition (37) has been removed.

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

Let us consider G, A, g. The functor A^g yielding a subset of G is defined by:

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

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

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

We now state a number of propositions:

(50)[4] $x \in A^g$ iff there exists h such that $x = h^g$ and $h \in A$.

(51) $x \in g^A$ iff 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 $(A^{a^{-1}})^a = A$.

(65)[5] G is a commutative group iff for all A, B such that $B \neq \emptyset$ holds $A^B = A$.

(66) G is a commutative group iff for all A, g holds $A^g = A$.

(67) G is a commutative group iff for all A, g such that $A \neq \emptyset$ holds $g^A = \{g\}$.

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

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

We now state a number of propositions:

(70)[6] $x \in H^a$ iff there exists g such that $x = g^a$ and $g \in H$.

[4] The propositions (48) and (49) have been removed.
[5] The proposition (64) has been removed.
[6] The propositions (68) and (69) have been removed.

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

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

(73) For every strict subgroup H of G holds $H^{1_G} = H$.

(74) For every strict subgroup H of G holds $(H^a)^{a^{-1}} = H$ and $(H^{a^{-1}})^a = H$.

(76)[7] $(H_1 \cap H_2)^a = {H_1}^a \cap {H_2}^a$.

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

(78) H is finite iff 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) For every strict subgroup H of G such that $H^a = \{\mathbf{1}\}_G$ holds $H = \{\mathbf{1}\}_G$.

(82) For every group G and for every element a of G holds $(\Omega_G)^a = \Omega_G$.

(83) For every strict subgroup H of G such that $H^a = G$ holds $H = G$.

(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 a commutative group, then for every strict subgroup H of G and for every 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 $a = b^g$.

Next we state three propositions:

(88)[8] a and b are conjugated iff 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.

Let us consider G, a, b. Let us notice that the predicate a and b are conjugated is reflexive and symmetric.

Next we state three propositions:

(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 $a^\bullet$ yields a subset of G and is defined by:

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

The following propositions are true:

(95)[9] $x \in a^\bullet$ iff there exists b such that $b = x$ and a and b are conjugated.

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

[7] The proposition (75) has been removed.
[8] The proposition (87) has been removed.
[9] The proposition (94) has been removed.

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

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

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

(100) $a^\bullet = b^\bullet$ iff $a^\bullet$ meets $b^\bullet$.

(101) $a^\bullet = \{1_G\}$ iff $a = 1_G$.

(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 $A = B^g$.

The following propositions are true:

(104)[10] A and B are conjugated iff 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.

Let us consider G, A, B. Let us notice that the predicate A and B are conjugated is reflexive and symmetric.

Next we state three propositions:

(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 iff a and b are conjugated.

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

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

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

One can prove the following propositions:

(111)[11] $x \in A^\bullet$ iff there exists B such that $x = B$ and A and B are conjugated.

(113)[12] $A \in B^\bullet$ iff 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) $A^\bullet = B^\bullet$ iff $A^\bullet$ 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 the groupoid of $H_1 = {H_2}^g$.

Next we state three propositions:

[10] The proposition (103) has been removed.
[11] The proposition (110) has been removed.
[12] The proposition (112) has been removed.

(121)[13] For all strict subgroups H_1, H_2 of G holds H_1 and H_2 are conjugated iff there exists g such that $H_2 = H_1{}^g$.

(122) For every strict subgroup H_1 of G holds H_1 and H_1 are conjugated.

(123) For all strict subgroups H_1, H_2 of G such that H_1 and H_2 are conjugated holds H_2 and H_1 are conjugated.

Let us consider G and let H_1, H_2 be strict subgroups of G. Let us notice that the predicate H_1 and H_2 are conjugated is reflexive and symmetric.
We now state the proposition

(124) Let H_1, H_2 be strict subgroups of G. Suppose H_1 and H_2 are conjugated and H_2 and H_3 are conjugated. Then H_1 and H_3 are conjugated.

Let us consider G, H. The functor $H^\bullet$ yields a subset of $\mathrm{SubGr}\,G$ and is defined by:

(Def. 12) $x \in H^\bullet$ iff there exists a strict subgroup H_1 of G such that $x = H_1$ and H and H_1 are conjugated.

We now state several propositions:

(127)[14] If $x \in H^\bullet$, then x is a strict subgroup of G.

(128) For all strict subgroups H_1, H_2 of G holds $H_1 \in H_2{}^\bullet$ iff H_1 and H_2 are conjugated.

(129) For every strict subgroup H of G holds $H^g \in H^\bullet$.

(130) For every strict subgroup H of G holds $H \in H^\bullet$.

(131) For all strict subgroups H_1, H_2 of G such that $H_1 \in H_2{}^\bullet$ holds $H_2 \in H_1{}^\bullet$.

(132) For all strict subgroups H_1, H_2 of G holds $H_1{}^\bullet = H_2{}^\bullet$ iff $H_1{}^\bullet$ meets $H_2{}^\bullet$.

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

(134) For every strict subgroup H_1 of G holds H_1 and H_2 are conjugated iff $\overline{H_1}$ and $\overline{H_2}$ are conjugated.

Let us consider G and let I_1 be a subgroup of G. We say that I_1 is normal if and only if:

(Def. 13) For every a holds $I_1{}^a =$ the groupoid of I_1.

Let us consider G. Observe that there exists a subgroup of G which is strict and normal.
Next we state a number of propositions:

(137)[15] $\{\mathbf{1}\}_G$ is normal and Ω_G is normal.

(138) For all strict normal subgroups N_1, N_2 of G holds $N_1 \cap N_2$ is normal.

(139) For every strict subgroup H of G such that G is a commutative group holds H is normal.

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

(141) For every subgroup H of G holds H is a normal subgroup of G iff for every a holds $a \cdot H \subseteq H \cdot a$.

(142) For every subgroup H of G holds H is a normal subgroup of G iff for every a holds $H \cdot a \subseteq a \cdot H$.

[13] The proposition (120) has been removed.
[14] The propositions (125) and (126) have been removed.
[15] The propositions (135) and (136) have been removed.

(143) For every subgroup H of G holds H is a normal subgroup of G iff for every A holds $A \cdot H = H \cdot A$.

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

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

(146) For every strict subgroup H of G holds H is a normal subgroup of G iff $H^\bullet = \{H\}$.

(147) Let H be a strict subgroup of G. Then 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) For all strict normal subgroups N_1, N_2 of G holds $\overline{N_1} \cdot \overline{N_2} = \overline{N_2} \cdot \overline{N_1}$.

(149) Let N_1, N_2 be strict normal subgroups of G. Then there exists a strict normal subgroup N of G such that the carrier of $N = \overline{N_1} \cdot \overline{N_2}$.

(150) For every normal subgroup N of G holds the left cosets of $N =$ the right cosets of N.

(151) Let H be a subgroup of G. Suppose 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 and let us consider A. The functor $\mathrm{N}(A)$ yielding a strict subgroup of G is defined as follows:

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

The following propositions are true:

(154)[16] $x \in \mathrm{N}(A)$ iff 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 there exists a finite set C such that $C = A^\bullet$ and $\mathrm{card}\, C = |\bullet : \mathrm{N}(A)|_{\mathbb{N}}$.

(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 there exists a finite set C such that $C = a^\bullet$ and $\mathrm{card}\, C = |\bullet : \mathrm{N}(\{a\})|_{\mathbb{N}}$.

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

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

Next we state several propositions:

(160)[17] For every strict subgroup H of G holds $x \in \mathrm{N}(H)$ iff there exists h such that $x = h$ and $H^h = H$.

(161) For every strict subgroup H of G holds $\overline{\overline{H^\bullet}} = |\bullet : \mathrm{N}(H)|$.

(162) Let H be a strict subgroup of G. Suppose $H^\bullet$ is finite or the left cosets of $\mathrm{N}(H)$ is finite. Then there exists a finite set C such that $C = H^\bullet$ and $\mathrm{card}\, C = |\bullet : \mathrm{N}(H)|_{\mathbb{N}}$.

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

(164) For every strict group G holds $\mathrm{N}(\{\mathbf{1}\}_G) = G$.

(165) For every strict group G holds $\mathrm{N}(\Omega_G) = G$.

(166) For every finite set X such that $\mathrm{card}\, X = 2$ there exist x, y such that $x \neq y$ and $X = \{x, y\}$.

[16] The propositions (152) and (153) have been removed.

[17] The proposition (159) has been removed.

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/card_1.html`.

[2] Grzegorz Bancerek. Cardinal arithmetics. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/card_2.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] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finset_1.html`.

[8] 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`.

[9] Andrzej Trybulec. Domains and their Cartesian products. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/domain_1.html`.

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

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

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

[13] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_1.html`.

[14] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_2.html`.

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

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

Received August 10, 1990

Published January 2, 2004