JOURNAL OF FORMALIZED MATHEMATICS
Volume 3, Released 1991, Published 2003
Inst. of Computer Science, Univ. of Białystok

Commutator and Center of a Group

Wojciech A. Trybulec
Warsaw University
Białystok

Summary. We introduce the notions of commutators of element, subgroups of a group, commutator of a group and center of a group. We prove P.Hall identity. The article is based on [5].

MML Identifier: GROUP_5.

WWW: http://mizar.org/JFM/Vol3/group_5.html

The articles [8], [16], [3], [1], [2], [4], [14], [9], [10], [6], [12], [15], [11], [13], and [7] provide the notation and terminology for this paper.

1. Preliminaries

The scheme *SubsetFD3* deals with non empty sets $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, a ternary functor $\mathcal{F}$ yielding an element of $\mathcal{B}$, and a ternary predicate $\mathcal{P}$, and states that:

$\{\mathcal{F}(c,d,e); c$ ranges over elements of $\mathcal{A}, d$ ranges over elements of $\mathcal{B}, e$ ranges over elements of $\mathcal{C} : \mathcal{P}[c,d,e]\}$ is a subset of $\mathcal{B}$

for all values of the parameters.

For simplicity, we follow the rules: x is a set, k, n are natural numbers, i is an integer, G is a group, a, b, c, d are elements of G, A, B, C, D are subsets of G, H, H_1, H_2, H_3, H_4 are subgroups of G, N_1, N_2 are normal subgroups of G, F, F_1, F_2 are finite sequences of elements of the carrier of G, and I is a finite sequence of elements of $\mathbb{Z}$.

Next we state several propositions:

(1) $x \in \{\mathbf{1}\}_G$ iff $x = 1_G$.

(2) If $a \in H$ and $b \in H$, then $a^b \in H$.

(3) For every strict normal subgroup N of G such that $a \in N$ holds $a^b \in N$.

(4) $x \in H_1 \cdot H_2$ iff there exist a, b such that $x = a \cdot b$ and $a \in H_1$ and $b \in H_2$.

(5) If $H_1 \cdot H_2 = H_2 \cdot H_1$, then $x \in H_1 \sqcup H_2$ iff there exist a, b such that $x = a \cdot b$ and $a \in H_1$ and $b \in H_2$.

(6) If G is a commutative group, then $x \in H_1 \sqcup H_2$ iff there exist a, b such that $x = a \cdot b$ and $a \in H_1$ and $b \in H_2$.

(7) For all strict normal subgroups N_1, N_2 of G holds $x \in N_1 \sqcup N_2$ iff there exist a, b such that $x = a \cdot b$ and $a \in N_1$ and $b \in N_2$.

(8) For every normal subgroup N of G holds $H \cdot N = N \cdot H$.

Let us consider G, F, a. The functor F^a yields a finite sequence of elements of the carrier of G and is defined as follows:

(Def. 1) $\operatorname{len}(F^a) = \operatorname{len} F$ and for every k such that $k \in \operatorname{dom} F$ holds $F^a(k) = (F_k)^a$.

Next we state several propositions:

(12)[1] $({F_1}^a) \frown {F_2}^a = (F_1 \frown F_2)^a$.

(13) $(\varepsilon_{(\text{the carrier of } G)})^a = \emptyset$.

(14) $\langle a \rangle^b = \langle a^b \rangle$.

(15) $\langle a, b \rangle^c = \langle a^c, b^c \rangle$.

(16) $\langle a, b, c \rangle^d = \langle a^d, b^d, c^d \rangle$.

(17) $\prod (F^a) = (\prod F)^a$.

(18) $(F^a)^I = (F^I)^a$.

2. Commutators

Let us consider G, a, b. The functor $[a, b]$ yields an element of G and is defined by:

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

We now state a number of propositions:

(19) $[a, b] = a^{-1} \cdot b^{-1} \cdot a \cdot b$ and $[a, b] = a^{-1} \cdot (b^{-1} \cdot a) \cdot b$ and $[a, b] = a^{-1} \cdot (b^{-1} \cdot a \cdot b)$ and $[a, b] = a^{-1} \cdot (b^{-1} \cdot (a \cdot b))$ and $[a, b] = a^{-1} \cdot b^{-1} \cdot (a \cdot b)$.

(20) $[a, b] = (b \cdot a)^{-1} \cdot (a \cdot b)$.

(21) $[a, b] = (b^{-1})^a \cdot b$ and $[a, b] = a^{-1} \cdot a^b$.

(22) $[1_G, a] = 1_G$ and $[a, 1_G] = 1_G$.

(23) $[a, a] = 1_G$.

(24) $[a, a^{-1}] = 1_G$ and $[a^{-1}, a] = 1_G$.

(25) $[a, b]^{-1} = [b, a]$.

(26) $[a, b]^c = [a^c, b^c]$.

(27) $[a, b] = (a^{-1})^2 \cdot (a \cdot b^{-1})^2 \cdot b^2$.

(28) $[a \cdot b, c] = [a, c]^b \cdot [b, c]$.

(29) $[a, b \cdot c] = [a, c] \cdot [a, b]^c$.

(30) $[a^{-1}, b] = [b, a]^{a^{-1}}$.

(31) $[a, b^{-1}] = [b, a]^{b^{-1}}$.

(32) $[a^{-1}, b^{-1}] = [a, b]^{(a \cdot b)^{-1}}$ and $[a^{-1}, b^{-1}] = [a, b]^{(b \cdot a)^{-1}}$.

(33) $[a, b^{a^{-1}}] = [b, a^{-1}]$.

(34) $[a^{b^{-1}}, b] = [b^{-1}, a]$.

(35) $[a^n, b] = a^{-n} \cdot (a^b)^n$.

[1] The propositions (9)–(11) have been removed.

(36) $[a,b^n] = (b^a)^{-n} \cdot b^n$.

(37) $[a^i,b] = a^{-i} \cdot (a^b)^i$.

(38) $[a,b^i] = (b^a)^{-i} \cdot b^i$.

(39) $[a,b] = 1_G$ iff $a \cdot b = b \cdot a$.

(40) G is a commutative group iff for all a, b holds $[a,b] = 1_G$.

(41) If $a \in H$ and $b \in H$, then $[a,b] \in H$.

Let us consider G, a, b, c. The functor $[a, b, c]$ yields an element of G and is defined as follows:

(Def. 3) $[a, b, c] = [[a,b],c]$.

The following propositions are true:

(43)[2] $[a, b, 1_G] = 1_G$ and $[a, 1_G, b] = 1_G$ and $[1_G, a, b] = 1_G$.

(44) $[a, a, b] = 1_G$.

(45) $[a, b, a] = [a^b,a]$.

(46) $[b, a, a] = ([b,a^{-1}] \cdot [b,a])^a$.

(47) $[a, b, b^a] = [b,[b,a]]$.

(48) $[a \cdot b,c] = [a,c] \cdot [a, c, b] \cdot [b,c]$.

(49) $[a,b \cdot c] = [a,c] \cdot [a,b] \cdot [a, b, c]$.

(50) $[a, b^{-1}, c]^b \cdot [b, c^{-1}, a]^c \cdot [c, a^{-1}, b]^a = 1_G$.

Let us consider G, A, B. The commutators of A & B yields a subset of G and is defined by:

(Def. 4) The commutators of A & $B = \{[a,b] : a \in A \wedge b \in B\}$.

One can prove the following propositions:

(52)[3] $x \in$ the commutators of A & B iff there exist a, b such that $x = [a,b]$ and $a \in A$ and $b \in B$.

(53) The commutators of $\emptyset_{\text{the carrier of } G}$ & $A = \emptyset$ and the commutators of A & $\emptyset_{\text{the carrier of } G} = \emptyset$.

(54) The commutators of $\{a\}$ & $\{b\} = \{[a,b]\}$.

(55) If $A \subseteq B$ and $C \subseteq D$, then the commutators of A & $C \subseteq$ the commutators of B & D.

(56) G is a commutative group if and only if for all A, B such that $A \neq \emptyset$ and $B \neq \emptyset$ holds the commutators of A & $B = \{1_G\}$.

Let us consider G, H_1, H_2. The commutators of H_1 & H_2 yielding a subset of G is defined by:

(Def. 5) The commutators of H_1 & $H_2 =$ the commutators of $\overline{H_1}$ & $\overline{H_2}$.

One can prove the following propositions:

(58)[4] $x \in$ the commutators of H_1 & H_2 iff there exist a, b such that $x = [a,b]$ and $a \in H_1$ and $b \in H_2$.

(59) $1_G \in$ the commutators of H_1 & H_2.

(60) The commutators of $\{\mathbf{1}\}_G$ & $H = \{1_G\}$ and the commutators of H & $\{\mathbf{1}\}_G = \{1_G\}$.

[2] The proposition (42) has been removed.
[3] The proposition (51) has been removed.
[4] The proposition (57) has been removed.

(61) Let N be a strict normal subgroup of G. Then the commutators of H & $N \subseteq \overline{N}$ and the commutators of N & $H \subseteq \overline{N}$.

(62) Suppose H_1 is a subgroup of H_2 and H_3 is a subgroup of H_4. Then the commutators of H_1 & $H_3 \subseteq$ the commutators of H_2 & H_4.

(63) G is a commutative group iff for all H_1, H_2 holds the commutators of H_1 & $H_2 = \{1_G\}$.

Let us consider G. The commutators of G yielding a subset of G is defined as follows:

(Def. 6) The commutators of $G =$ the commutators of Ω_G & Ω_G.

We now state two propositions:

(65)[5] $x \in$ the commutators of G iff there exist a, b such that $x = [a,b]$.

(66) G is a commutative group iff the commutators of $G = \{1_G\}$.

Let us consider G, A, B. The functor $[A,B]$ yielding a strict subgroup of G is defined by:

(Def. 7) $[A,B] = \mathrm{gr}($the commutators of A & $B)$.

Next we state three propositions:

(68)[6] If $a \in A$ and $b \in B$, then $[a,b] \in [A,B]$.

(69) $x \in [A,B]$ iff there exist F, I such that $\mathrm{len}\,F = \mathrm{len}\,I$ and $\mathrm{rng}\,F \subseteq$ the commutators of A & B and $x = \prod(F^I)$.

(70) If $A \subseteq C$ and $B \subseteq D$, then $[A,B]$ is a subgroup of $[C,D]$.

Let us consider G, H_1, H_2. The functor $[H_1,H_2]$ yielding a strict subgroup of G is defined by:

(Def. 8) $[H_1,H_2] = [\overline{H_1},\overline{H_2}]$.

The following propositions are true:

(72)[7] $[H_1,H_2] = \mathrm{gr}($the commutators of H_1 & $H_2)$.

(73) $x \in [H_1,H_2]$ iff there exist F, I such that $\mathrm{len}\,F = \mathrm{len}\,I$ and $\mathrm{rng}\,F \subseteq$ the commutators of H_1 & H_2 and $x = \prod(F^I)$.

(74) If $a \in H_1$ and $b \in H_2$, then $[a,b] \in [H_1,H_2]$.

(75) If H_1 is a subgroup of H_2 and H_3 is a subgroup of H_4, then $[H_1,H_3]$ is a subgroup of $[H_2,H_4]$.

(76) For every strict normal subgroup N of G holds $[N,H]$ is a subgroup of N and $[H,N]$ is a subgroup of N.

(77) For all strict normal subgroups N_1, N_2 of G holds $[N_1,N_2]$ is a normal subgroup of G.

(78) $[N_1,N_2] = [N_2,N_1]$.

(79) For all strict normal subgroups N_1, N_2, N_3 of G holds $[N_1 \sqcup N_2, N_3] = [N_1,N_3] \sqcup [N_2,N_3]$.

(80) For all strict normal subgroups N_1, N_2, N_3 of G holds $[N_1, N_2 \sqcup N_3] = [N_1,N_2] \sqcup [N_1,N_3]$.

Let G be a group. The functor G^{c} yields a strict normal subgroup of G and is defined as follows:

(Def. 9) $G^{\mathrm{c}} = [\Omega_G,\Omega_G]$.

We now state several propositions:

[5] The proposition (64) has been removed.
[6] The proposition (67) has been removed.
[7] The proposition (71) has been removed.

(82)[8] For every group G holds $G^{c} = \mathrm{gr}(\text{the commutators of } G)$.

(83) Let G be a group. Then $x \in G^{c}$ if and only if there exists a finite sequence F of elements of the carrier of G and there exists I such that $\mathrm{len}\, F = \mathrm{len}\, I$ and $\mathrm{rng}\, F \subseteq$ the commutators of G and $x = \prod(F^{I})$.

(84) For every strict group G and for all elements a, b of G holds $[a,b] \in G^{c}$.

(85) For every strict group G holds G is a commutative group iff $G^{c} = \{\mathbf{1}\}_{G}$.

(86) Let G be a group and H be a strict subgroup of G. Suppose the left cosets of H is finite and $|\bullet : H|_{\mathbb{N}} = 2$. Then G^{c} is a subgroup of H.

3. Center of a Group

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

(Def. 10) The carrier of $\mathrm{Z}(G) = \{a : \bigwedge_{b}\ a \cdot b = b \cdot a\}$.

Next we state several propositions:

(89)[9] $a \in \mathrm{Z}(G)$ iff for every b holds $a \cdot b = b \cdot a$.

(90) $\mathrm{Z}(G)$ is a normal subgroup of G.

(91) For every subgroup H of G such that H is a subgroup of $\mathrm{Z}(G)$ holds H is a normal subgroup of G.

(92) $\mathrm{Z}(G)$ is commutative.

(93) $a \in \mathrm{Z}(G)$ iff $a^{\bullet} = \{a\}$.

(94) For every strict group G holds G is a commutative group iff $\mathrm{Z}(G) = G$.

4. Auxiliary theorems

In the sequel E denotes a non empty set and p, q denote finite sequences of elements of E.

We now state two propositions:

(95) If $k \in \mathrm{dom}\, p$, then $(p \frown q)_{k} = p_{k}$.

(96) If $k \in \mathrm{dom}\, q$, then $(p \frown q)_{\mathrm{len}\, p + k} = q_{k}$.

References

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

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finseq_1.html`.

[3] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[4] Agata Darmochwał. Finite sets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/finset_1.html`.

[5] M. I. Kargapołow and J. I. Mierzlakow. *Podstawy teorii grup*. PWN, Warszawa, 1989.

[6] 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`.

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

[8] The proposition (81) has been removed.

[9] The propositions (87) and (88) have been removed.

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

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

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

[11] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_3.html.

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

[13] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/group_4.html.

[14] Wojciech A. Trybulec. Pigeon hole principle. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_4.html.

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

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

Received May 15, 1991

Published January 2, 2004