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

Commutator and Center of a Group

Wojciech A. Trybulec
Warsaw University

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 [6].

MML Identifier: GROUP_5.

The terminology and notation used in this paper are introduced in the following articles: [9], [4], [1], [3], [5], [10], [7], [14], [16], [2], [12], [8], [15], [11], and [13].

Preliminaries

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

$\{\mathcal{F}(c,d,e) : \mathcal{P}[c,d,e]\}$, where c ranges over elements of $\mathcal{A}$, and d ranges over elements of $\mathcal{B}$, and e ranges over elements of $\mathcal{C}$, is a subset of $\mathcal{B}$
for all values of the parameters.

For simplicity we adopt the following rules: x will be arbitrary, k, n will denote natural numbers, i will denote an integer, G will denote a group, a, b, c, d will denote elements of G, A, B, C, D will denote subsets of G, H, H_1, H_2, H_3, H_4 will denote subgroups of G, N, N_1, N_2, N_3 will denote normal subgroups of G, F, F_1, F_2 will denote finite sequences of elements of the carrier of G, and I will denote a finite sequence of elements of $\mathbb{Z}$. Next we state several propositions:

(1) $x \in \{\mathbf{1}\}_G$ if and only if $x = 1_G$.

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

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

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

ISSN 0777–4028

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

(7) $x \in N_1 \sqcup N_2$ if and only if there exist a, b such that $x = a \cdot b$ and $a \in N_1$ and $b \in N_2$.

(8) $H \cdot N = N \cdot H$.

Let us consider G, F, a. The functor F^a yielding a finite sequence of elements of the carrier of G is defined by:

(Def.1) $\mathrm{len}(F^a) = \mathrm{len}\, F$ and for every k such that $k \in \mathrm{Seg}\,\mathrm{len}\, F$ holds $F^a(k) = (\pi_k F)^a$.

One can prove the following propositions:

(9) If $\mathrm{len}\, F_1 = \mathrm{len}\, F_2$ and for every k such that $k \in \mathrm{Seg}\,\mathrm{len}\, F_2$ holds $F_1(k) = (\pi_k F_2)^a$, then $F_1 = {F_2}^a$.

(10) $\mathrm{len}(F^a) = \mathrm{len}\, F$.

(11) For every k such that $k \in \mathrm{Seg}\,\mathrm{len}\, F$ holds $F^a(k) = (\pi_k F)^a$.

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

(13) $\varepsilon^a_{(\text{the carrier of } G)} = \varepsilon$.

(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) If $\mathrm{len}\, F = \mathrm{len}\, I$, then $(F^a)^I = (F^I)^a$.

Commutators

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

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

One can prove the following propositions:

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

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

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

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

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

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

(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) $[a,b] = 1_G$ if and only if $a \cdot b = b \cdot a$.

(40) G is an Abelian group if and only if 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 $[a,\, b,\, c]$ yielding an element of G is defined by:

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

One can prove the following propositions:

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

(43) $[a,\, b,\, 1_G] = 1_G$ 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 yielding a subset of G is defined as follows:

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

We now state several propositions:

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

(52) $x \in$ the commutators of A & B if and only if 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 an Abelian 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 yields a subset of G and is defined by:

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

Next we state several propositions:

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

(58) $x \in$ the commutators of H_1 & H_2 if and only if 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 & $\{\mathbf{1}\}_G = \{1_G\}$.

(61) The commutators of H & $N \subseteq \overline{N}$ and the commutators of N & $H \subseteq \overline{N}$.

(62) If 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 an Abelian group if and only if 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 by:

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

Next we state three propositions:

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

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

(66) G is an Abelian group if and only if the commutators of $G = \{1_G\}$.

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

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

Next we state four propositions:

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

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

(69) $x \in [A, B]$ if and only if 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 subgroup of G is defined by:

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

Next we state a number of propositions:

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

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

(73) $x \in [H_1, H_2]$ if and only if 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) $[N, H]$ is a subgroup of N and $[H, N]$ is a subgroup of N.

(77) $[N_1, N_2]$ is a normal subgroup of G.

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

(79) $[N_1 \sqcup N_2, N_3] = [N_1, N_3] \sqcup [N_2, N_3]$.

(80) $[N_1, N_2 \sqcup N_3] = [N_1, N_2] \sqcup [N_1, N_3]$.

Let us consider G. The functor G^{c} yields a normal subgroup of G and is defined by:

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

Next we state several propositions:

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

(82) $G^{\mathrm{c}} = \mathrm{gr}$(the commutators of G).

(83) $x \in G^{\mathrm{c}}$ if and only if there exist F, I such that $\mathrm{len}\, F = \mathrm{len}\, I$ and $\mathrm{rng}\, F \subseteq$ the commutators of G and $x = \prod(F^I)$.

(84) $[a, b] \in G^{\mathrm{c}}$.

(85) G is an Abelian group if and only if $G^{\mathrm{c}} = \{\mathbf{1}\}_G$.

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

Center of a Group

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

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

We now state several propositions:

(87) If the carrier of $H = \{a : \bigwedge_b a \cdot b = b \cdot a\}$, then $H = \mathrm{Z}(G)$.

(88) The carrier of $\mathrm{Z}(G) = \{a : \bigwedge_b a \cdot b = b \cdot a\}$.

(89) $a \in \mathrm{Z}(G)$ if and only if for every b holds $a \cdot b = b \cdot a$.

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

(91) If H is a subgroup of $\mathrm{Z}(G)$, then H is a normal subgroup of G.

(92) $\mathrm{Z}(G)$ is an Abelian group.

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

(94) G is an Abelian group if and only if $\mathrm{Z}(G) = G$.

Auxiliary theorems

In the sequel E will be a non-empty set and p, q will be finite sequences of elements of E. The following propositions are true:

(95) If $k \in \mathrm{dom}\, p$ or $k \in \mathrm{Seg}\, \mathrm{len}\, p$, then $\pi_k(p \frown q) = \pi_k p$.

(96) If $k \in \mathrm{dom}\, q$ or $k \in \mathrm{Seg}\, \mathrm{len}\, q$, then $\pi_{\mathrm{len}\, p+k}(p \frown q) = \pi_k q$.

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] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[5] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[6] M. I. Kargapołow and J. I. Mierzlakow. *Podstawy teorii grup.* PWN, Warszawa, 1989.
[7] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[8] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[9] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[10] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[11] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[12] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[13] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[14] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[15] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[16] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

Received May 15, 1991