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

Lattice of Subgroups of a Group. Frattini Subgroup

Wojciech A. Trybulec
Warsaw University

Summary. We define the notion of a subgroup generated by a set of element of a group and two closely connected notions. Namely lattice of subgroups and Frattini subgroup. The operations in the lattice are the intersection of subgroups (introduced in [21]) and multiplication of subgroups which result is defined as a subgroup generated by a sum of carriers of the two subgroups. In order to define Frattini subgroup and to prove theorems concerning it we introduce notion of maximal subgroup and non-generating element of the group (see [9, page 30]). Frattini subgroup is defined as in [9] as an intersection of all maximal subgroups. We show that an element of the group belongs to Frattini subgroup of the group if and only if it is a non-generating element. We also prove theorems that should be proved in [1] but are not.

MML Identifier: `GROUP_4`.

WWW: `http://mizar.org/JFM/Vol2/group_4.html`

The articles [13], [8], [22], [16], [2], [3], [14], [11], [23], [6], [7], [4], [19], [20], [5], [15], [10], [21], [17], [24], [18], [12], and [1] provide the notation and terminology for this paper.

Let D be a non empty set, let F be a finite sequence of elements of D, and let X be a set. Then $F - X$ is a finite sequence of elements of D.

The scheme *MeetSbgEx* deals with a group $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

> There exists a strict subgroup H of $\mathcal{A}$ such that the carrier of $H = \bigcap\{A; A$ ranges over subsets of $\mathcal{A} : \bigvee_{K:\ \text{strict subgroup of}\ \mathcal{A}}\ (A = \text{the carrier of}\ K\ \wedge\ \mathcal{P}[K])\}$

provided the following condition is satisfied:

- There exists a strict subgroup H of $\mathcal{A}$ such that $\mathcal{P}[H]$.

For simplicity, we adopt the following convention: X is a set, k, n are natural numbers, i, i_1, i_2, i_3, j are integers, G is a group, a, b, c are elements of G, A, B are subsets of G, H, H_1, H_2, H_3 are subgroups of G, h is an element of H, F, F_1, F_2 are finite sequences of elements of the carrier of G, and I, I_1, I_2 are finite sequences of elements of $\mathbb{Z}$.

The scheme *SubgrSep* deals with a group $\mathcal{A}$ and a unary predicate $\mathcal{P}$, and states that:

> There exists X such that $X \subseteq \mathrm{SubGr}\,\mathcal{A}$ and for every strict subgroup H of $\mathcal{A}$ holds $H \in X$ iff $\mathcal{P}[H]$

for all values of the parameters.

Let us consider i. The functor ${}^{@}i$ yielding an element of $\mathbb{Z}$ is defined by:

(Def. 2)[1] ${}^{@}i = i$.

We now state four propositions:

(3)[2] If $a = h$, then $a^n = h^n$.

(4) If $a = h$, then $a^i = h^i$.

[1] The definition (Def. 1) has been removed.
[2] The propositions (1) and (2) have been removed.

(5) If $a \in H$, then $a^n \in H$.

(6) If $a \in H$, then $a^i \in H$.

Let G be a non empty groupoid and let F be a finite sequence of elements of the carrier of G. The functor $\prod F$ yielding an element of G is defined as follows:

(Def. 3) $\prod F =$ the multiplication of $G \odot F$.

The following propositions are true:

(8)[3] Let G be an associative unital non empty groupoid and F_1, F_2 be finite sequences of elements of the carrier of G. Then $\prod(F_1 \frown F_2) = \prod F_1 \cdot \prod F_2$.

(9) Let G be a unital non empty groupoid, F be a finite sequence of elements of the carrier of G, and a be an element of G. Then $\prod(F \frown \langle a \rangle) = \prod F \cdot a$.

(10) Let G be an associative unital non empty groupoid, F be a finite sequence of elements of the carrier of G, and a be an element of G. Then $\prod(\langle a \rangle \frown F) = a \cdot \prod F$.

(11) For every unital non empty groupoid G holds $\prod(\varepsilon_{(\text{the carrier of } G)}) = 1_G$.

(12) For every non empty groupoid G and for every element a of G holds $\prod\langle a \rangle = a$.

(13) For every non empty groupoid G and for all elements a, b of G holds $\prod\langle a, b \rangle = a \cdot b$.

(14) $\prod\langle a, b, c \rangle = a \cdot b \cdot c$ and $\prod\langle a, b, c \rangle = a \cdot (b \cdot c)$.

(15) $\prod(n \mapsto a) = a^n$.

(16) $\prod(F - \{1_G\}) = \prod F$.

(17) If $\operatorname{len} F_1 = \operatorname{len} F_2$ and for every k such that $k \in \operatorname{dom} F_1$ holds $F_2((\operatorname{len} F_1 - k) + 1) = ((F_1)_k)^{-1}$, then $\prod F_1 = (\prod F_2)^{-1}$.

(18) If G is a commutative group, then for every permutation P of $\operatorname{dom} F_1$ such that $F_2 = F_1 \cdot P$ holds $\prod F_1 = \prod F_2$.

(19) If G is a commutative group and F_1 is one-to-one and F_2 is one-to-one and $\operatorname{rng} F_1 = \operatorname{rng} F_2$, then $\prod F_1 = \prod F_2$.

(20) If G is a commutative group and $\operatorname{len} F = \operatorname{len} F_1$ and $\operatorname{len} F = \operatorname{len} F_2$ and for every k such that $k \in \operatorname{dom} F$ holds $F(k) = (F_1)_k \cdot (F_2)_k$, then $\prod F = \prod F_1 \cdot \prod F_2$.

(21) If $\operatorname{rng} F \subseteq \overline{H}$, then $\prod F \in H$.

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

(Def. 4) $\operatorname{len}(F^I) = \operatorname{len} F$ and for every k such that $k \in \operatorname{dom} F$ holds $F^I(k) = (F_k)^{@(I_k)}$.

Next we state several propositions:

(25)[4] If $\operatorname{len} F_1 = \operatorname{len} I_1$ and $\operatorname{len} F_2 = \operatorname{len} I_2$, then $(F_1 \frown F_2)^{I_1 \frown I_2} = (F_1{}^{I_1}) \frown F_2{}^{I_2}$.

(26) If $\operatorname{rng} F \subseteq \overline{H}$, then $\prod(F^I) \in H$.

(27) $(\varepsilon_{(\text{the carrier of } G)})^{\varepsilon_{\mathbb{Z}}} = \emptyset$.

(28) $\langle a \rangle^{\langle @i \rangle} = \langle a^i \rangle$.

---

[3] The proposition (7) has been removed.

[4] The propositions (22)–(24) have been removed.

(29) $\langle a,b\rangle^{\langle @i,@j\rangle} = \langle a^i, b^j\rangle$.

(30) $\langle a,b,c\rangle^{\langle @i_1,@i_2,@i_3\rangle} = \langle a^{i_1}, b^{i_2}, c^{i_3}\rangle$.

(31) $F^{\mathrm{len}\,F\mapsto(@1)} = F$.

(32) $F^{\mathrm{len}\,F\mapsto(@0)} = \mathrm{len}\,F \mapsto 1_G$.

(33) If $\mathrm{len}\,I = n$, then $(n \mapsto 1_G)^I = n \mapsto 1_G$.

Let us consider G, A. The functor $\mathrm{gr}(A)$ yields a strict subgroup of G and is defined by the conditions (Def. 5).

(Def. 5)(i) $A \subseteq$ the carrier of $\mathrm{gr}(A)$, and

(ii) for every strict subgroup H of G such that $A \subseteq$ the carrier of H holds $\mathrm{gr}(A)$ is a subgroup of H.

One can prove the following propositions:

(37)[5] $a \in \mathrm{gr}(A)$ iff there exist F, I such that $\mathrm{len}\,F = \mathrm{len}\,I$ and $\mathrm{rng}\,F \subseteq A$ and $\prod(F^I) = a$.

(38) If $a \in A$, then $a \in \mathrm{gr}(A)$.

(39) $\mathrm{gr}(\emptyset_{\text{the carrier of } G}) = \{\mathbf{1}\}_G$.

(40) For every strict subgroup H of G holds $\mathrm{gr}(\overline{H}) = H$.

(41) If $A \subseteq B$, then $\mathrm{gr}(A)$ is a subgroup of $\mathrm{gr}(B)$.

(42) $\mathrm{gr}(A \cap B)$ is a subgroup of $\mathrm{gr}(A) \cap \mathrm{gr}(B)$.

(43) The carrier of $\mathrm{gr}(A) = \bigcap\{B : \bigvee_{H:\ \text{strict subgroup of } G} (B = \text{the carrier of } H \wedge A \subseteq \overline{H})\}$.

(44) $\mathrm{gr}(A) = \mathrm{gr}(A \setminus \{1_G\})$.

Let us consider G, a. We say that a is generating if and only if:

(Def. 6) It is not true that for every A such that $\mathrm{gr}(A) =$ the groupoid of G holds $\mathrm{gr}(A \setminus \{a\}) =$ the groupoid of G.

One can prove the following proposition

(46)[6] 1_G is non generating.

Let us consider G, H. We say that H is maximal if and only if the conditions (Def. 7) are satisfied.

(Def. 7)(i) The groupoid of $H \neq$ the groupoid of G, and

(ii) for every strict subgroup K of G such that the groupoid of $H \neq K$ and H is a subgroup of K holds $K =$ the groupoid of G.

Next we state the proposition

(48)[7] Let G be a strict group, H be a strict subgroup of G, and a be an element of G. If H is maximal and $a \notin H$, then $\mathrm{gr}(\overline{H} \cup \{a\}) = G$.

Let G be a group. The functor $\Phi(G)$ yielding a strict subgroup of G is defined as follows:

[5] The propositions (34)–(36) have been removed.
[6] The proposition (45) has been removed.
[7] The proposition (47) has been removed.

(Def. 8)(i) The carrier of $\Phi(G) = \bigcap\{A; A$ ranges over subsets of G: $\bigvee_{H:\text{ strict subgroup of } G}$ $(A =$ the carrier of $H \wedge H$is maximal$)\}$ if there exists a strict subgroup of G which is maximal,

(ii) $\Phi(G) =$ the groupoid of G, otherwise.

Next we state several propositions:

(52)[8] Let G be a group. Suppose there exists a strict subgroup of G which is maximal. Then $a \in \Phi(G)$ if and only if for every strict subgroup H of G such that H is maximal holds $a \in H$.

(53) Let G be a group and a be an element of G. If for every strict subgroup H of G holds H is not maximal, then $a \in \Phi(G)$.

(54) For every group G and for every strict subgroup H of G such that H is maximal holds $\Phi(G)$ is a subgroup of H.

(55) For every strict group G holds the carrier of $\Phi(G) = \{a; a$ ranges over elements of G: a is non generating$\}$.

(56) For every strict group G and for every element a of G holds $a \in \Phi(G)$ iff a is non generating.

Let us consider G, H_1, H_2. The functor $H_1 \cdot H_2$ yielding a subset of G is defined by:

(Def. 9) $H_1 \cdot H_2 = \overline{H_1} \cdot \overline{H_2}$.

Next we state several propositions:

(57) $H_1 \cdot H_2 = \overline{H_1} \cdot \overline{H_2}$ and $H_1 \cdot H_2 = H_1 \cdot \overline{H_2}$ and $H_1 \cdot H_2 = \overline{H_1} \cdot H_2$.

(58) $H \cdot H = \overline{H}$.

(59) $(H_1 \cdot H_2) \cdot H_3 = H_1 \cdot (H_2 \cdot H_3)$.

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

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

(62) $(A \cdot H_1) \cdot H_2 = A \cdot (H_1 \cdot H_2)$.

(63) $(H_1 \cdot H_2) \cdot A = H_1 \cdot (H_2 \cdot A)$.

(64) For all strict normal subgroups N_1, N_2 of G holds $N_1 \cdot N_2 = N_2 \cdot N_1$.

(65) If G is a commutative group, then $H_1 \cdot H_2 = H_2 \cdot H_1$.

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

(Def. 10) $H_1 \sqcup H_2 = \mathrm{gr}(\overline{H_1} \cup \overline{H_2})$.

Next we state a number of propositions:

(67)[9] $a \in H_1 \sqcup H_2$ iff there exist F, I such that $\mathrm{len}\, F = \mathrm{len}\, I$ and $\mathrm{rng}\, F \subseteq \overline{H_1} \cup \overline{H_2}$ and $a = \prod(F^I)$.

(68) $H_1 \sqcup H_2 = \mathrm{gr}(H_1 \cdot H_2)$.

(69) If $H_1 \cdot H_2 = H_2 \cdot H_1$, then the carrier of $H_1 \sqcup H_2 = H_1 \cdot H_2$.

(70) If G is a commutative group, then the carrier of $H_1 \sqcup H_2 = H_1 \cdot H_2$.

(71) For all strict normal subgroups N_1, N_2 of G holds the carrier of $N_1 \sqcup N_2 = N_1 \cdot N_2$.

(72) For all strict normal subgroups N_1, N_2 of G holds $N_1 \sqcup N_2$ is a normal subgroup of G.

---

[8] The propositions (49)–(51) have been removed.

[9] The proposition (66) has been removed.

(73) For every strict subgroup H of G holds $H \sqcup H = H$.

(74) $H_1 \sqcup H_2 = H_2 \sqcup H_1$.

(75) $(H_1 \sqcup H_2) \sqcup H_3 = H_1 \sqcup (H_2 \sqcup H_3)$.

(76) For every strict subgroup H of G holds $\{\mathbf{1}\}_G \sqcup H = H$ and $H \sqcup \{\mathbf{1}\}_G = H$.

(77) $\Omega_G \sqcup H = \Omega_G$ and $H \sqcup \Omega_G = \Omega_G$.

(78) H_1 is a subgroup of $H_1 \sqcup H_2$ and H_2 is a subgroup of $H_1 \sqcup H_2$.

(79) For every strict subgroup H_2 of G holds H_1 is a subgroup of H_2 iff $H_1 \sqcup H_2 = H_2$.

(80) If H_1 is a subgroup of H_2, then H_1 is a subgroup of $H_2 \sqcup H_3$.

(81) Let H_3 be a strict subgroup of G. Suppose H_1 is a subgroup of H_3 and H_2 is a subgroup of H_3. Then $H_1 \sqcup H_2$ is a subgroup of H_3.

(82) For all strict subgroups H_3, H_2 of G such that H_1 is a subgroup of H_2 holds $H_1 \sqcup H_3$ is a subgroup of $H_2 \sqcup H_3$.

(83) $H_1 \cap H_2$ is a subgroup of $H_1 \sqcup H_2$.

(84) For every strict subgroup H_2 of G holds $H_1 \cap H_2 \sqcup H_2 = H_2$.

(85) For every strict subgroup H_1 of G holds $H_1 \cap (H_1 \sqcup H_2) = H_1$.

(86) For all strict subgroups H_1, H_2 of G holds $H_1 \sqcup H_2 = H_2$ iff $H_1 \cap H_2 = H_1$.

In the sequel S_1, S_2 denote elements of $\mathrm{SubGr}\, G$.

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

(Def. 11) For all S_1, S_2, H_1, H_2 such that $S_1 = H_1$ and $S_2 = H_2$ holds $(\mathrm{SubJoin}\, G)(S_1, S_2) = H_1 \sqcup H_2$.

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

(Def. 12) For all S_1, S_2, H_1, H_2 such that $S_1 = H_1$ and $S_2 = H_2$ holds $(\mathrm{SubMeet}\, G)(S_1, S_2) = H_1 \cap H_2$.

Let G be a group. The functor $\mathbb{L}_G$ yielding a strict lattice is defined by:

(Def. 13) $\mathbb{L}_G = \langle \mathrm{SubGr}\, G, \mathrm{SubJoin}\, G, \mathrm{SubMeet}\, G \rangle$.

Next we state three propositions:

(92)[10] For every group G holds the carrier of $\mathbb{L}_G = \mathrm{SubGr}\, G$.

(93) For every group G holds the join operation of $\mathbb{L}_G = \mathrm{SubJoin}\, G$.

(94) For every group G holds the meet operation of $\mathbb{L}_G = \mathrm{SubMeet}\, G$.

Let G be a group. Note that $\mathbb{L}_G$ is lower-bounded and upper-bounded.

One can prove the following propositions:

(98)[11] For every group G holds $\perp_{\mathbb{L}_G} = \{\mathbf{1}\}_G$.

(99) For every group G holds $\top_{\mathbb{L}_G} = \Omega_G$.

In the sequel k, l, m, n are natural numbers.

One can prove the following propositions:

[10] The propositions (87)–(91) have been removed.

[11] The propositions (95)–(97) have been removed.

(100) $n \bmod 2 = 0$ or $n \bmod 2 = 1$.

(101) For all natural numbers k, n holds $k \cdot n \bmod k = 0$.

(102) If $k > 1$, then $1 \bmod k = 1$.

(103) If $k \bmod n = 0$ and $l = k - m \cdot n$, then $l \bmod n = 0$.

In the sequel k, n, l denote natural numbers.
We now state four propositions:

(104) If $n \neq 0$ and $k \bmod n = 0$ and $l < n$, then $(k+l) \bmod n = l$.

(105) If $k \bmod n = 0$, then $(k+l) \bmod n = l \bmod n$.

(106) If $n \neq 0$ and $k \bmod n = 0$, then $(k+l) \div n = (k \div n) + (l \div n)$.

(107) If $k \neq 0$, then $k \cdot n \div k = n$.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/nat_1.html.

[2] Grzegorz Bancerek. The ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal1.html.

[3] Grzegorz Bancerek. Sequences of ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/ordinal2.html.

[4] 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.

[5] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/binop_1.html.

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

[7] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/funct_2.html.

[8] Czesław Byliński. Some basic properties of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/zfmisc_1.html.

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

[10] 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.

[11] Beata Padlewska. Families of sets. *Journal of Formalized Mathematics*, 1, 1989. http://mizar.org/JFM/Vol1/setfam_1.html.

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

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

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

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

[16] Wojciech A. Trybulec. Binary operations on finite sequences. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finsop_1.html.

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

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

[19] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Journal of Formalized Mathematics*, 2, 1990. http://mizar.org/JFM/Vol2/finseq_3.html.

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

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

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

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

[24] Stanisław Żukowski. Introduction to lattice theory. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/lattices.html`.

Received August 22, 1990

Published January 2, 2004