FORMALIZED MATHEMATICS
Vol.2, No.1, January–February 1991
Université Catholique de Louvain

Lattice of Subgroups of a Group. Frattini Subgroup

Wojciech A. Trybulec[1]
Warsaw University

Summary. We define the notion of a subgroup generated by a set of elements of a group and two closely connected notions, namely lattice of subgroups and the Frattini subgroup. The operations on the lattice are the intersection of subgroups (introduced in [18]) 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 the Frattini subgroup and to prove theorems concerning it we introduce notion of maximal subgroup and non-generating element of the group (see page 30 in [6]). The Frattini subgroup is defined as in [6] as an intersection of all maximal subgroups. We show that an element of the group belongs to the 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.

The notation and terminology used here are introduced in the following articles: [3], [13], [4], [11], [20], [10], [19], [8], [16], [5], [17], [2], [15], [18], [14], [12], [21], [7], [9], and [1]. Let D be a non-empty set, and 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.

In this article we present several logical schemes. The scheme *SubsetD* deals with a non-empty set $\mathcal{A}$, and a unary predicate $\mathcal{P}$, and states that:

$\{d : \mathcal{P}[d]\}$, where d is an element of $\mathcal{A}$, is a subset of $\mathcal{A}$

for all values of the parameters.

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

there exists a subgroup H of $\mathcal{A}$ such that the carrier of $H = \bigcap\{A : \bigvee_K [A =$ the carrier of $K \wedge \mathcal{P}[K]]\}$, where A is a subset of $\mathcal{A}$, and K is a subgroup of $\mathcal{A}$

provided the parameters have the following property:

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

ISSN 0777–4028

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

For simplicity we adopt the following rules: X denotes a set, k, l, m, n denote natural numbers, i, i_1, i_2, i_3, j denote integers, G denotes a group, a, b, c denote elements of G, A, B denote subsets of G, H, H_1, H_2, H_3, K denote subgroups of G, N_1, N_2 denote normal subgroups of G, h denotes an element of H, F, F_1, F_2 denote finite sequences of elements of the carrier of G, and I, I_1, I_2 denote 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 subgroup H of $\mathcal{A}$ holds $H \in X$ if and only if $\mathcal{P}[H]$

for all values of the parameters.

Let i be an element of $\mathbb{Z}$. The functor $@i$ yields an integer and is defined by:

(Def.1) $@i = i$.

We now state the proposition

(1) For every element i of $\mathbb{Z}$ holds $@i = i$.

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

(Def.2) $@i = i$.

Next we state several propositions:

(2) $@i = i$.

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

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

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

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

Let us consider G, F. The functor $\prod F$ yielding an element of G is defined as follows:

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

Next we state a number of propositions:

(7) $\prod F = $ the operation of $G \odot F$.

(8) $\prod(F_1 \frown F_2) = \prod F_1 \cdot \prod F_2$.

(9) $\prod(F \frown \langle a \rangle) = \prod F \cdot a$.

(10) $\prod(\langle a \rangle \frown F) = a \cdot \prod F$.

(11) $\prod \varepsilon_{\text{the carrier of } G} = 1_G$.

(12) $\prod \langle a \rangle = a$.

(13) $\prod \langle a, b \rangle = a \cdot b$.

(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) $\prod(n \longmapsto a) = a^n$.

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

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

(18) If G is an Abelian group, then for every permutation P of $\mathrm{Seg}(\mathrm{len}\, F_1)$ such that $F_2 = F_1 \cdot P$ holds $\prod F_1 = \prod F_2$.

(19) If G is an Abelian group and F_1 is one-to-one and F_2 is one-to-one and $\mathrm{rng}\, F_1 = \mathrm{rng}\, F_2$, then $\prod F_1 = \prod F_2$.

(20) If G is an Abelian group and $\mathrm{len}\, F = \mathrm{len}\, F_1$ and $\mathrm{len}\, F = \mathrm{len}\, F_2$ and for every k such that $k \in \mathrm{Seg}(\mathrm{len}\, F)$ holds $F(k) = \pi_k F_1 \cdot \pi_k F_2$, then $\prod F = \prod F_1 \cdot \prod F_2$.

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

Let us consider G, I, F. Let us assume that $\mathrm{len}\, F = \mathrm{len}\, I$. The functor F^I yields a finite sequence of elements of the carrier of G and is defined as follows:

(Def.4) $\mathrm{len}(F^I) = \mathrm{len}\, F$ and for every k such that $k \in \mathrm{Seg}(\mathrm{len}\, F)$ holds $(F^I)(k) = \pi_k F^{@(\pi_k I)}$.

One can prove the following propositions:

(22) If $\mathrm{len}\, F = \mathrm{len}\, I$ and $\mathrm{len}\, F_1 = \mathrm{len}\, F$ and for every k such that $k \in \mathrm{Seg}(\mathrm{len}\, F)$ holds $F_1(k) = \pi_k F^{@(\pi_k I)}$, then $F_1 = F^I$.

(23) If $\mathrm{len}\, F = \mathrm{len}\, I$, then for every k such that $k \in \mathrm{Seg}(\mathrm{len}\, F)$ holds $(F^I)(k) = \pi_k F^{@(\pi_k I)}$.

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

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

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

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

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

(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) $F^{\mathrm{len}\, F \longmapsto @(+1)} = F$.

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

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

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

(Def.5) $A \subseteq$ the carrier of $\mathrm{gr}(A)$ and for every H such that $A \subseteq$ the carrier of H holds $\mathrm{gr}(A)$ is a subgroup of H.

We now state a number of propositions:

(34) If $A \subseteq$ the carrier of H_1 and for every H_2 such that $A \subseteq$ the carrier of H_2 holds H_1 is a subgroup of H_2, then $H_1 = \mathrm{gr}(A)$.

(35) $A \subseteq$ the carrier of $\mathrm{gr}(A)$.

(36) If $A \subseteq$ the carrier of H, then $\mathrm{gr}(A)$ is a subgroup of H.

(37) $a \in \mathrm{gr}(A)$ if and only if 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) $\mathrm{gr}(\overline{H}) = H$.

(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 $\mathrm{gr}(A) = \bigcap\{B : \bigvee_H[B =$ the carrier of $H \wedge A \subseteq \overline{H}]\}$.

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

We now define two new predicates. Let us consider G, a. We say that a is non-generating if and only if:

(Def.6) for every A such that $\mathrm{gr}(A) = G$ holds $\mathrm{gr}(A \setminus \{a\}) = G$.

a is generating stands for a is not non-generating.

We now state the proposition

(46)[2] 1_G is non-generating.

Let us consider G, H. We say that H is maximal if and only if:

(Def.7) $H \neq G$ and for every K such that $H \neq K$ and H is a subgroup of K holds $K = G$.

Next we state the proposition

(48)[3] If H is maximal and $a \notin H$, then $\mathrm{gr}(\overline{H} \cup \{a\}) = G$.

Let us consider G. The functor $\Phi(G)$ yields a subgroup of G and is defined as follows:

(Def.8) the carrier of $\Phi(G) = \bigcap\{A : \bigvee_H[A =$ the carrier of $H \wedge$ H is maximal $]\}$ if there exists H such that H is maximal, $\Phi(G) = G$, otherwise.

We now state several propositions:

(49) If there exists H such that H is maximal and the carrier of $H = \bigcap\{A : \bigvee_K[A =$ the carrier of $K \wedge$ K is maximal $]\}$, then $H = \Phi(G)$.

(50) If for every H holds H is not maximal, then $\Phi(G) = G$.

(51) If there exists H such that H is maximal, then the carrier of $\Phi(G) = \bigcap\{A : \bigvee_K[A =$ the carrier of $K \wedge$ K is maximal $]\}$.

(52) If there exists H such that H is maximal, then $a \in \Phi(G)$ if and only if for every H such that H is maximal holds $a \in H$.

(53) If for every H holds H is not maximal, then $a \in \Phi(G)$.

(54) If H is maximal, then $\Phi(G)$ is a subgroup of H.

(55) The carrier of $\Phi(G) = \{a : a$ is non-generating $\}$.

(56) $a \in \Phi(G)$ if and only if 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 as follows:

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

The following propositions are true:

(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 $H_1 \cdot H_2 = \overline{H_1} \cdot H_2$.

[2]The proposition (45) was either repeated or obvious.
[3]The proposition (47) was either repeated or obvious.

(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) $N_1 \cdot N_2 = N_2 \cdot N_1$.

(65) If G is an Abelian 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 subgroup of G is defined as follows:

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

One can prove the following propositions:

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

(67) $a \in H_1 \sqcup H_2$ if and only if 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 an Abelian group, then the carrier of $H_1 \sqcup H_2 = H_1 \cdot H_2$.

(71) The carrier of $N_1 \sqcup N_2 = N_1 \cdot N_2$.

(72) $N_1 \sqcup N_2$ is a normal subgroup of G.

(73) $H \sqcup H = H$.

(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) $\{\mathbf{1}\}_G \sqcup H = H$ and $H \sqcup \{\mathbf{1}\}_G = H$.

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

(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) H_1 is a subgroup of H_2 if and only if $H_1 \sqcup H_2 = H_2$.

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

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

(85) $H_1 \cap (H_1 \sqcup H_2) = H_1$.

(86) $H_1 \sqcup H_2 = H_2$ if and only if $H_1 \cap H_2 = H_1$.

In the sequel S_1, S_2 are elements of $\mathrm{SubGr}\, G$ and o is a binary operation on $\mathrm{SubGr}\, G$. 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 $(\mathrm{SubJoin}\, G)(S_1,\, S_2) = H_1 \sqcup H_2$.

Next we state two propositions:

(87) If for all S_1, S_2, H_1, H_2 such that $S_1 = H_1$ and $S_2 = H_2$ holds $o(S_1,\, S_2) = H_1 \sqcup H_2$, then $o = \mathrm{SubJoin}\, G$.

(88) If $H_1 = S_1$ and $H_2 = S_2$, then $\mathrm{SubJoin}\, G(S_1,\, S_2) = H_1 \sqcup H_2$.

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

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

One can prove the following two propositions:

(89) If for all S_1, S_2, H_1, H_2 such that $S_1 = H_1$ and $S_2 = H_2$ holds $o(S_1,\, S_2) = H_1 \cap H_2$, then $o = \mathrm{SubMeet}\, G$.

(90) If $H_1 = S_1$ and $H_2 = S_2$, then $\mathrm{SubMeet}\, G(S_1,\, S_2) = H_1 \cap H_2$.

Let us consider G. The functor $\mathbb{L}_G$ yielding a lattice is defined as follows:

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

One can prove the following propositions:

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

(92) The carrier of $\mathbb{L}_G = \mathrm{SubGr}\, G$.

(93) The join operation of $\mathbb{L}_G = \mathrm{SubJoin}\, G$.

(94) The meet operation of $\mathbb{L}_G = \mathrm{SubMeet}\, G$.

(95) $\mathbb{L}_G$ is a lower bound lattice.

(96) $\mathbb{L}_G$ is an upper bound lattice.

(97) $\mathbb{L}_G$ is a bound lattice.

(98) $\perp_{\mathbb{L}_G} = \{\mathbf{1}\}_G$.

(99) $\top_{\mathbb{L}_G} = \Omega_G$.

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

(101) $k \cdot n \bmod k = 0$ and $k \cdot n \bmod n = 0$.

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

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

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

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

(106) If $n \neq 0$ and $k \bmod n = 0$ and $l \bmod n = 0$, 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. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[3] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[4] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[5] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 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] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.
[9] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[10] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.
[11] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[12] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[13] Wojciech A. Trybulec. Binary operations on finite sequences. *Formalized Mathematics*, 1(**5**):979–981, 1990.
[14] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.
[15] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[16] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[17] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[18] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**):855–864, 1990.
[19] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[20] Zinaida Trybulec and Halina Święczkowska. Boolean properties of sets. *Formalized Mathematics*, 1(**1**):17–23, 1990.
[21] Stanisław Żukowski. Introduction to lattice theory. *Formalized Mathematics*, 1(**1**):215–222, 1990.

Received August 22, 1990