

The Jordan-Hölder Theorem

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. The goal of this article is to formalize the Jordan-Hölder theorem in the context of group with operators as in the book [5]. Accordingly, the article introduces the structure of group with operators and reformulates some theorems on a group already present in the Mizar Mathematical Library. Next, the article formalizes the Zassenhaus butterfly lemma and the Schreier refinement theorem, and defines the composition series.

MML identifier: GROUP_9, version: 7.8.05 4.84.971

The terminology and notation used here are introduced in the following articles: [17], [25], [3], [26], [7], [27], [8], [9], [4], [10], [1], [12], [18], [2], [6], [21], [20], [22], [19], [15], [23], [11], [14], [16], [13], and [24].

1. ACTIONS AND GROUPS WITH OPERATORS

Let O, E be sets. An action of O on E is a function from O into E^E .

Let O, E be sets, let A be an action of O on E , and let I_1 be a set. We say that I_1 is stable under the action of A if and only if:

(Def. 1) For every element o of O and for every function f from E into E such that $o \in O$ and $f = A(o)$ holds $f^\circ I_1 \subseteq I_1$.

Let O, E be sets, let A be an action of O on E , and let X be a subset of E . The stable subset generated by X yields a subset of E and is defined by the conditions (Def. 2).

(Def. 2)(i) $X \subseteq$ the stable subset generated by X ,
(ii) the stable subset generated by X is stable under the action of A , and
(iii) for every subset Y of E such that Y is stable under the action of A and $X \subseteq Y$ holds the stable subset generated by $X \subseteq Y$.

Let O, E be sets, let A be an action of O on E , and let F be a finite sequence of elements of O . The functor $\text{Product}(F, A)$ yields a function from E into E and is defined by:

- (Def. 3)(i) $\text{Product}(F, A) = \text{id}_E$ if $\text{len } F = 0$,
(ii) there exists a finite sequence P_1 of elements of E^E such that $\text{Product}(F, A) = P_1(\text{len } F)$ and $\text{len } P_1 = \text{len } F$ and $P_1(1) = A(F(1))$ and for every natural number n such that $n \neq 0$ and $n < \text{len } F$ there exist functions f, g from E into E such that $f = P_1(n)$ and $g = A(F(n+1))$ and $P_1(n+1) = f \cdot g$, otherwise.

Let O be a set, let G be a group, and let I_1 be an action of O on the carrier of G . We say that I_1 is distributive if and only if:

- (Def. 4) For every element o of O such that $o \in O$ holds $I_1(o)$ is a homomorphism from G to G .

Let O be a set. We consider group structures with operators in O as extensions of groupoid as systems

\langle a carrier, a multiplication, an action \rangle ,

where the carrier is a set, the multiplication is a binary operation on the carrier, and the action is an action of O on the carrier.

Let O be a set. Observe that there exists a group structure with operators in O which is non empty.

Let O be a set and let I_1 be a non empty group structure with operators in O . We say that I_1 is distributive if and only if the condition (Def. 5) is satisfied.

- (Def. 5) Let G be a group and a be an action of O on the carrier of G . Suppose $a =$ the action of I_1 and the groupoid of $G =$ the groupoid of I_1 . Then a is distributive.

Let O be a set. Observe that there exists a non empty group structure with operators in O which is strict, distributive, group-like, and associative.

Let O be a set. A group with operators in O is a distributive group-like associative non empty group structure with operators in O .

Let O be a set, let G be a group with operators in O , and let o be an element of O . The functor $G \hat{\ } o$ yields a homomorphism from G to G and is defined as follows:

- (Def. 6) $G \hat{\ } o = \begin{cases} \text{(the action of } G)(o), & \text{if } o \in O, \\ \text{id}_{\text{the carrier of } G}, & \text{otherwise.} \end{cases}$

Let O be a set and let G be a group with operators in O . A distributive group-like associative non empty group structure with operators in O is said to be a stable subgroup of G if:

- (Def. 7) It is a subgroup of G and for every element o of O holds $\text{it} \hat{\ } o = (G \hat{\ } o) \upharpoonright \text{the carrier of it}$.

Let O be a set and let G be a group with operators in O . Note that there exists a stable subgroup of G which is strict.

Let O be a set and let G be a group with operators in O . The functor $\{\mathbf{1}\}_G$ yields a strict stable subgroup of G and is defined by:

(Def. 8) The carrier of $\{\mathbf{1}\}_G = \{\mathbf{1}_G\}$.

Let O be a set and let G be a group with operators in O . The functor Ω_G yielding a strict stable subgroup of G is defined as follows:

(Def. 9) $\Omega_G =$ the group structure with operators of G .

Let O be a set, let G be a group with operators in O , and let I_1 be a stable subgroup of G . We say that I_1 is normal if and only if:

(Def. 10) For every strict subgroup H of G such that $H =$ the groupoid of I_1 holds H is normal.

Let O be a set and let G be a group with operators in O . Note that there exists a stable subgroup of G which is strict and normal.

Let O be a set, let G be a group with operators in O , and let H be a stable subgroup of G . Observe that there exists a stable subgroup of H which is normal.

Let O be a set and let G be a group with operators in O . Note that $\{\mathbf{1}\}_G$ is normal and Ω_G is normal.

Let O be a set and let G be a group with operators in O . The stable subgroups of G yields a set and is defined as follows:

(Def. 11) For every set x holds $x \in$ the stable subgroups of G iff x is a strict stable subgroup of G .

Let O be a set and let G be a group with operators in O . Observe that the stable subgroups of G is non empty.

Let I_1 be a group. We say that I_1 is simple if and only if:

(Def. 12) I_1 is not trivial and it is not true that there exists a strict normal subgroup H of I_1 such that $H \neq \Omega_{(I_1)}$ and $H \neq \{\mathbf{1}\}_{(I_1)}$.

Let us note that there exists a group which is strict and simple.

Let O be a set and let I_1 be a group with operators in O . We say that I_1 is simple if and only if:

(Def. 13) I_1 is not trivial and it is not true that there exists a strict normal stable subgroup H of I_1 such that $H \neq \Omega_{(I_1)}$ and $H \neq \{\mathbf{1}\}_{(I_1)}$.

Let O be a set. Observe that there exists a group with operators in O which is strict and simple.

Let O be a set, let G be a group with operators in O , and let N be a normal stable subgroup of G . The functor $\text{Cosets } N$ yields a set and is defined by:

(Def. 14) For every strict normal subgroup H of G such that $H =$ the groupoid of N holds $\text{Cosets } N = \text{Cosets } H$.

Let O be a set, let G be a group with operators in O , and let N be a normal stable subgroup of G . The functor $\text{CosOp } N$ yielding a binary operation on $\text{Cosets } N$ is defined by:

(Def. 15) For every strict normal subgroup H of G such that $H =$ the groupoid of N holds $\text{CosOp } N = \text{CosOp } H$.

Let O be a set, let G be a group with operators in O , and let N be a normal stable subgroup of G . The functor $\text{CosAc } N$ yielding an action of O on $\text{Cosets } N$ is defined as follows:

(Def. 16)(i) For every element o of O holds $(\text{CosAc } N)(o) = \{\langle A, B \rangle; A$ ranges over elements of $\text{Cosets } N, B$ ranges over elements of $\text{Cosets } N :$
 $\bigvee_{g,h: \text{element of } G} (g \in A \wedge h \in B \wedge h = (G \frown o)(g))\}$ if O is not empty,
(ii) $\text{CosAc } N = \{\emptyset, \{\text{id}_{\text{Cosets } N}\}\}$, otherwise.

Let O be a set, let G be a group with operators in O , and let N be a normal stable subgroup of G . The functor G/N yields a group structure with operators in O and is defined as follows:

(Def. 17) $G/N = \langle \text{Cosets } N, \text{CosOp } N, \text{CosAc } N \rangle$.

Let O be a set, let G be a group with operators in O , and let N be a normal stable subgroup of G . Note that G/N is non empty and G/N is distributive, group-like, and associative.

Let O be a set, let G, H be groups with operators in O , and let f be a function from G into H . We say that f is homomorphic if and only if:

(Def. 18) For every element o of O and for every element g of G holds $f((G \frown o)(g)) = (H \frown o)(f(g))$.

Let O be a set and let G, H be groups with operators in O . One can check that there exists a function from G into H which is multiplicative and homomorphic.

Let O be a set and let G, H be groups with operators in O . A homomorphism from G to H is a multiplicative homomorphic function from G into H .

Let O be a set, let G, H, I be groups with operators in O , let h be a homomorphism from G to H , and let h_1 be a homomorphism from H to I . Then $h_1 \cdot h$ is a homomorphism from G to I .

Let O be a set, let G, H be groups with operators in O , and let h be a homomorphism from G to H . We say that h is monomorphism if and only if:

(Def. 19) h is one-to-one.

We say that h is epimorphism if and only if:

(Def. 20) $\text{rng } h =$ the carrier of H .

Let O be a set, let G, H be groups with operators in O , and let h be a homomorphism from G to H . We say that h is isomorphism if and only if:

(Def. 21) h is an epimorphism and a monomorphism.

Let O be a set and let G, H be groups with operators in O . We say that G and H are isomorphic if and only if:

(Def. 22) There exists a homomorphism from G to H which is an isomorphism.

Let us note that the predicate G and H are isomorphic is reflexive.

Let O be a set and let G, H be groups with operators in O . Let us note that the predicate G and H are isomorphic is symmetric.

Let O be a set, let G be a group with operators in O , and let N be a normal stable subgroup of G . The canonical homomorphism onto cosets of N yields a homomorphism from G to G/N and is defined by the condition (Def. 23).

(Def. 23) Let H be a strict normal subgroup of G . Suppose $H =$ the groupoid of N . Then the canonical homomorphism onto cosets of $N =$ the canonical homomorphism onto cosets of H .

Let O be a set, let G, H be groups with operators in O , and let g be a homomorphism from G to H . The functor $\text{Ker } g$ yields a strict stable subgroup of G and is defined as follows:

(Def. 24) The carrier of $\text{Ker } g = \{a; a \text{ ranges over elements of } G: g(a) = \mathbf{1}_H\}$.

Let O be a set, let G, H be groups with operators in O , and let g be a homomorphism from G to H . Observe that $\text{Ker } g$ is normal.

Let O be a set, let G, H be groups with operators in O , and let g be a homomorphism from G to H . The functor $\text{Im } g$ yielding a strict stable subgroup of H is defined by:

(Def. 25) The carrier of $\text{Im } g = g^\circ(\text{the carrier of } G)$.

Let O be a set, let G be a group with operators in O , and let H be a stable subgroup of G . The functor \overline{H} yielding a subset of G is defined as follows:

(Def. 26) $\overline{H} =$ the carrier of H .

Let O be a set, let G be a group with operators in O , and let H_1, H_2 be stable subgroups of G . The functor $H_1 \cdot H_2$ yields a subset of G and is defined as follows:

(Def. 27) $H_1 \cdot H_2 = \overline{H_1} \cdot \overline{H_2}$.

Let O be a set, let G be a group with operators in O , and let H_1, H_2 be stable subgroups of G . The functor $H_1 \cap H_2$ yielding a strict stable subgroup of G is defined by:

(Def. 28) The carrier of $H_1 \cap H_2 = \overline{H_1} \cap \overline{H_2}$.

Let us note that the functor $H_1 \cap H_2$ is commutative.

Let O be a set, let G be a group with operators in O , and let A be a subset of G . The stable subgroup of A yielding a strict stable subgroup of G is defined by the conditions (Def. 29).

(Def. 29)(i) $A \subseteq$ the carrier of the stable subgroup of A , and
 (ii) for every strict stable subgroup H of G such that $A \subseteq$ the carrier of H holds the stable subgroup of A is a stable subgroup of H .

Let O be a set, let G be a group with operators in O , and let H_1, H_2 be stable subgroups of G . The functor $H_1 \sqcup H_2$ yielding a strict stable subgroup of G is defined as follows:

(Def. 30) $H_1 \sqcup H_2 =$ the stable subgroup of $\overline{H_1} \cup \overline{H_2}$.

2. SOME THEOREMS ON GROUPS REFORMULATED FOR GROUPS WITH OPERATORS

For simplicity, we follow the rules: x, O are sets, o is an element of O , G, H, I are groups with operators in O , A, B are subsets of G , N is a normal stable subgroup of G , H_1, H_2, H_3 are stable subgroups of G , g_1, g_2 are elements of G , h_1, h_2 are elements of H_1 , and h is a homomorphism from G to H .

One can prove the following propositions:

- (1) If $x \in H_1$, then $x \in G$.
- (2) h_1 is an element of G .
- (3) If $h_1 = g_1$ and $h_2 = g_2$, then $h_1 \cdot h_2 = g_1 \cdot g_2$.
- (4) $\mathbf{1}_G = \mathbf{1}_{(H_1)}$.
- (5) $\mathbf{1}_G \in H_1$.
- (6) If $h_1 = g_1$, then $h_1^{-1} = g_1^{-1}$.
- (7) If $g_1 \in H_1$ and $g_2 \in H_1$, then $g_1 \cdot g_2 \in H_1$.
- (8) If $g_1 \in H_1$, then $g_1^{-1} \in H_1$.
- (9) Suppose that
 - (i) $A \neq \emptyset$,
 - (ii) for all g_1, g_2 such that $g_1 \in A$ and $g_2 \in A$ holds $g_1 \cdot g_2 \in A$,
 - (iii) for every g_1 such that $g_1 \in A$ holds $g_1^{-1} \in A$, and
 - (iv) for all o, g_1 such that $g_1 \in A$ holds $(G \circ o)(g_1) \in A$.
 Then there exists a strict stable subgroup H of G such that the carrier of $H = A$.
- (10) G is a stable subgroup of G .
- (11) Let G_1, G_2, G_3 be groups with operators in O . Suppose G_1 is a stable subgroup of G_2 and G_2 is a stable subgroup of G_3 . Then G_1 is a stable subgroup of G_3 .
- (12) If the carrier of $H_1 \subseteq$ the carrier of H_2 , then H_1 is a stable subgroup of H_2 .
- (13) If for every element g of G such that $g \in H_1$ holds $g \in H_2$, then H_1 is a stable subgroup of H_2 .
- (14) For all strict stable subgroups H_1, H_2 of G such that the carrier of $H_1 =$ the carrier of H_2 holds $H_1 = H_2$.
- (15) $\{\mathbf{1}\}_G = \{\mathbf{1}\}_{(H_1)}$.
- (16) $\{\mathbf{1}\}_G$ is a stable subgroup of H_1 .
- (17) If $\overline{H_1} \cdot \overline{H_2} = \overline{H_2} \cdot \overline{H_1}$, then there exists a strict stable subgroup H of G such that the carrier of $H = \overline{H_1} \cdot \overline{H_2}$.

- (18)(i) For every stable subgroup H of G such that $H = H_1 \cap H_2$ holds the carrier of $H = (\text{the carrier of } H_1) \cap (\text{the carrier of } H_2)$, and
- (ii) for every strict stable subgroup H of G such that the carrier of $H = (\text{the carrier of } H_1) \cap (\text{the carrier of } H_2)$ holds $H = H_1 \cap H_2$.
- (19) For every strict stable subgroup H of G holds $H \cap H = H$.
- (20) $(H_1 \cap H_2) \cap H_3 = H_1 \cap (H_2 \cap H_3)$.
- (21) $\{\mathbf{1}\}_G \cap H_1 = \{\mathbf{1}\}_G$ and $H_1 \cap \{\mathbf{1}\}_G = \{\mathbf{1}\}_G$.
- (22) $\bigcup \text{Cosets } N = \text{the carrier of } G$.
- (23) Let N_1, N_2 be strict normal stable subgroups of G . Then there exists a strict normal stable subgroup N of G such that the carrier of $N = \overline{N_1} \cdot \overline{N_2}$.
- (24) $g_1 \in$ the stable subgroup of A if and only if there exists a finite sequence F of elements of the carrier of G and there exists a finite sequence I of elements of \mathbb{Z} and there exists a subset C of G such that $C =$ the stable subset generated by A and $\text{len } F = \text{len } I$ and $\text{rng } F \subseteq C$ and $\prod(F^I) = g_1$.
- (25) For every strict stable subgroup H of G holds the stable subgroup of $\overline{H} = H$.
- (26) If $A \subseteq B$, then the stable subgroup of A is a stable subgroup of the stable subgroup of B .

The scheme *MeetSbgWOpEx* deals with a set \mathcal{A} , a group \mathcal{B} with operators in \mathcal{A} , and a unary predicate \mathcal{P} , and states that:

There exists a strict stable subgroup H of \mathcal{B} such that the carrier of $H = \bigcap \{A; A \text{ ranges over subsets of } \mathcal{B} :$

$\bigvee_K : \text{strict stable subgroup of } \mathcal{B} (A = \text{the carrier of } K \wedge \mathcal{P}[K])\}$

provided the parameters meet the following requirement:

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

The following propositions are true:

- (27) The carrier of the stable subgroup of $A = \bigcap \{B; B \text{ ranges over subsets of } G: \bigvee_H : \text{strict stable subgroup of } G (B = \text{the carrier of } H \wedge A \subseteq \overline{H})\}$.
- (28) For all strict normal stable subgroups N_1, N_2 of G holds $N_1 \cdot N_2 = N_2 \cdot N_1$.
- (29) $H_1 \sqcup H_2 =$ the stable subgroup of $H_1 \cdot H_2$.
- (30) If $H_1 \cdot H_2 = H_2 \cdot H_1$, then the carrier of $H_1 \sqcup H_2 = H_1 \cdot H_2$.
- (31) For all strict normal stable subgroups N_1, N_2 of G holds the carrier of $N_1 \sqcup N_2 = N_1 \cdot N_2$.
- (32) For all strict normal stable subgroups N_1, N_2 of G holds $N_1 \sqcup N_2$ is a normal stable subgroup of G .
- (33) For every strict stable subgroup H of G holds $\{\mathbf{1}\}_G \sqcup H = H$ and $H \sqcup \{\mathbf{1}\}_G = H$.
- (34) $\Omega_G \sqcup H_1 = \Omega_G$ and $H_1 \sqcup \Omega_G = \Omega_G$.

- (35) H_1 is a stable subgroup of $H_1 \sqcup H_2$ and H_2 is a stable subgroup of $H_1 \sqcup H_2$.
- (36) For every strict stable subgroup H_2 of G holds H_1 is a stable subgroup of H_2 iff $H_1 \sqcup H_2 = H_2$.
- (37) Let H_3 be a strict stable subgroup of G . Suppose H_1 is a stable subgroup of H_3 and H_2 is a stable subgroup of H_3 . Then $H_1 \sqcup H_2$ is a stable subgroup of H_3 .
- (38) Let H_2, H_3 be strict stable subgroups of G . Suppose H_1 is a stable subgroup of H_2 . Then $H_1 \sqcup H_3$ is a stable subgroup of $H_2 \sqcup H_3$.
- (39) For all stable subgroups X, Y of H_1 and for all stable subgroups X', Y' of G such that $X = X'$ and $Y = Y'$ holds $X' \cap Y' = X \cap Y$.
- (40) If N is a stable subgroup of H_1 , then N is a normal stable subgroup of H_1 .
- (41) $H_1 \cap N$ is a normal stable subgroup of H_1 and $N \cap H_1$ is a normal stable subgroup of H_1 .
- (42) For every strict group G with operators in O such that G is trivial holds $\{\mathbf{1}\}_G = G$.
- (43) $\mathbf{1}_{G/N} = \overline{N}$.
- (44) Let M, N be strict normal stable subgroups of G and M_1 be a normal stable subgroup of N . Suppose $M_1 = M$ and M is a stable subgroup of N . Then ${}^N/M_1$ is a normal stable subgroup of G/M .
- (45) $h(\mathbf{1}_G) = \mathbf{1}_H$.
- (46) $h(g_1^{-1}) = h(g_1)^{-1}$.
- (47) $g_1 \in \text{Ker } h$ iff $h(g_1) = \mathbf{1}_H$.
- (48) For every strict normal stable subgroup N of G holds $\text{Ker } h$ (the canonical homomorphism onto cosets of N) = N .
- (49) $\text{rng } h = \text{the carrier of } \text{Im } h$.
- (50) $\text{Im } h$ (the canonical homomorphism onto cosets of N) = G/N .
- (51) Let H be a strict group with operators in O and h be a homomorphism from G to H . Then h is an epimorphism if and only if $\text{Im } h = H$.
- (52) Let H be a strict group with operators in O and h be a homomorphism from G to H . Suppose h is an epimorphism. Let c be an element of H . Then there exists an element a of G such that $h(a) = c$.
- (53) The canonical homomorphism onto cosets of N is an epimorphism.
- (54) The canonical homomorphism onto cosets of $\{\mathbf{1}\}_G$ is an isomorphism.
- (55) If G and H are isomorphic and H and I are isomorphic, then G and I are isomorphic.
- (56) For every strict group G with operators in O holds G and $G/\{\mathbf{1}\}_G$ are isomorphic.

- (57) For every strict group G with operators in O holds G/Ω_G is trivial.
- (58) Let G, H be strict groups with operators in O . If G and H are isomorphic and G is trivial, then H is trivial.
- (59) $G/\text{Ker } h$ and $\text{Im } h$ are isomorphic.
- (60) Let H, F_1, F_2 be strict stable subgroups of G . Suppose F_1 is a normal stable subgroup of F_2 . Then $H \cap F_1$ is a normal stable subgroup of $H \cap F_2$.

3. OTHERS THEOREMS ON ACTIONS AND GROUPS WITH OPERATORS

In the sequel E is a set, A is an action of O on E , C is a subset of G , and N_1 is a normal stable subgroup of H_1 .

One can prove the following propositions:

- (61) Ω_E is stable under the action of A .
- (62) $[\cdot O, \{\text{id}_E\}]$ is an action of O on E .
- (63) Let O be a non empty set, E be a set, o be an element of O , and A be an action of O on E . Then $\text{Product}(\langle o \rangle, A) = A(o)$.
- (64) Let O be a non empty set, E be a set, F_1, F_2 be finite sequences of elements of O , and A be an action of O on E . Then $\text{Product}(F_1 \wedge F_2, A) = \text{Product}(F_1, A) \cdot \text{Product}(F_2, A)$.
- (65) Let F be a finite sequence of elements of O and Y be a subset of E . If Y is stable under the action of A , then $(\text{Product}(F, A))^\circ Y \subseteq Y$.
- (66) Let E be a non empty set, A be an action of O on E , X be a subset of E , and a be an element of E . Suppose X is not empty. Then $a \in$ the stable subset generated by X if and only if there exists a finite sequence F of elements of O and there exists an element x of X such that $(\text{Product}(F, A))(x) = a$.
- (67) For every strict group G there exists a strict group H with operators in O such that $G =$ the groupoid of H .
- (68) The groupoid of H_1 is a strict subgroup of G .
- (69) The groupoid of N is a strict normal subgroup of G .
- (70) If $g_1 \in H_1$, then $(G \wedge o)(g_1) \in H_1$.
- (71) Let O be a set, G, H be groups with operators in O , G' be a strict stable subgroup of G , and f be a homomorphism from G to H . Then there exists a strict stable subgroup H' of H such that the carrier of $H' = f^\circ$ (the carrier of G').
- (72) If B is empty, then the stable subgroup of $B = \{\mathbf{1}\}_G$.
- (73) If $B =$ the carrier of $\text{gr}(C)$, then the stable subgroup of $C =$ the stable subgroup of B .

- (74) Let N' be a normal subgroup of G . Suppose N' = the groupoid of N . Then $G/N' =$ the groupoid of G/N and $\mathbf{1}_{G/N'} = \mathbf{1}_{G/N}$.
- (75) Suppose the carrier of $H_1 =$ the carrier of H_2 . Then the group structure with operators of $H_1 =$ the group structure with operators of H_2 .
- (76) Suppose H_1/N_1 is trivial. Then the group structure with operators of $H_1 =$ the group structure with operators of N_1 .
- (77) If the carrier of $H_1 =$ the carrier of N_1 , then H_1/N_1 is trivial.
- (78) Let G, H be groups with operators in O , N be a stable subgroup of G , H' be a strict stable subgroup of H , and f be a homomorphism from G to H . Suppose $N = \text{Ker } f$. Then there exists a strict stable subgroup G' of G such that
- (i) the carrier of $G' = f^{-1}(\text{the carrier of } H')$, and
 - (ii) if H' is normal, then N is a normal stable subgroup of G' and G' is normal.
- (79) Let G, H be groups with operators in O , N be a stable subgroup of G , G' be a strict stable subgroup of G , and f be a homomorphism from G to H . Suppose $N = \text{Ker } f$. Then there exists a strict stable subgroup H' of H such that
- (i) the carrier of $H' = f^\circ(\text{the carrier of } G')$,
 - (ii) $f^{-1}(\text{the carrier of } H') = \text{the carrier of } G' \sqcup N$, and
 - (iii) if f is an epimorphism and G' is normal, then H' is normal.
- (80) Let G be a strict group with operators in O , N be a strict normal stable subgroup of G , and H be a strict stable subgroup of G/N . Suppose the carrier of $G = (\text{the canonical homomorphism onto cosets of } N)^{-1}(\text{the carrier of } H)$. Then $H = \Omega_{G/N}$.
- (81) Let G be a strict group with operators in O , N be a strict normal stable subgroup of G , and H be a strict stable subgroup of G/N . Suppose the carrier of $N = (\text{the canonical homomorphism onto cosets of } N)^{-1}(\text{the carrier of } H)$. Then $H = \{\mathbf{1}\}_{G/N}$.
- (82) Let G, H be strict groups with operators in O . If G and H are isomorphic and G is simple, then H is simple.
- (83) Let G be a group with operators in O , H be a stable subgroup of G , F_3 be a finite sequence of elements of the carrier of G , F_4 be a finite sequence of elements of the carrier of H , and I be a finite sequence of elements of \mathbb{Z} . If $F_3 = F_4$ and $\text{len } F_3 = \text{len } I$, then $\prod(F_3^I) = \prod(F_4^I)$.
- (84) Let O, E_1, E_2 be sets, A_1 be an action of O on E_1 , A_2 be an action of O on E_2 , and F be a finite sequence of elements of O . Suppose that
- (i) $E_1 \subseteq E_2$, and
 - (ii) for every element o of O and for every function f_1 from E_1 into E_1 and for every function f_2 from E_2 into E_2 such that $f_1 = A_1(o)$ and $f_2 = A_2(o)$

holds $f_1 = f_2 \upharpoonright E_1$.

Then $\text{Product}(F, A_1) = \text{Product}(F, A_2) \upharpoonright E_1$.

- (85) Let N_1, N_2 be strict stable subgroups of H_1 and N'_1, N'_2 be strict stable subgroups of G . If $N_1 = N'_1$ and $N_2 = N'_2$, then $N'_1 \cdot N'_2 = N_1 \cdot N_2$.
- (86) Let N_1, N_2 be strict stable subgroups of H_1 and N'_1, N'_2 be strict stable subgroups of G . If $N_1 = N'_1$ and $N_2 = N'_2$, then $N'_1 \sqcup N'_2 = N_1 \sqcup N_2$.
- (87) Let N_1, N_2 be strict stable subgroups of G . Suppose N_1 is a normal stable subgroup of H_1 and N_2 is a normal stable subgroup of H_1 . Then $N_1 \sqcup N_2$ is a normal stable subgroup of H_1 .
- (88) Let f be a homomorphism from G to H and g be a homomorphism from H to I . Then the carrier of $\text{Ker}(g \cdot f) = f^{-1}$ (the carrier of $\text{Ker } g$).
- (89) Let G' be a stable subgroup of G , H' be a stable subgroup of H , and f be a homomorphism from G to H . Suppose the carrier of $H' = f^\circ$ (the carrier of G') or the carrier of $G' = f^{-1}$ (the carrier of H'). Then $f \upharpoonright$ the carrier of G' is a homomorphism from G' to H' .
- (90) Let G, H be strict groups with operators in O , N, L, G' be strict stable subgroups of G , and f be a homomorphism from G to H . Suppose $N = \text{Ker } f$ and L is a strict normal stable subgroup of G' . Then
- (i) $L \sqcup G' \cap N$ is a normal stable subgroup of G' ,
 - (ii) $L \sqcup N$ is a normal stable subgroup of $G' \sqcup N$, and
 - (iii) for every strict normal stable subgroup N_1 of $G' \sqcup N$ and for every strict normal stable subgroup N_2 of G' such that $N_1 = L \sqcup N$ and $N_2 = L \sqcup G' \cap N$ holds $(G' \sqcup N)/N_1$ and G'/N_2 are isomorphic.

4. THE ZASSENHAUS BUTTERFLY LEMMA

The following propositions are true:

- (91) Let H, K, H', K' be strict stable subgroups of G , J_1 be a normal stable subgroup of $H' \sqcup H \cap K$, and H_4 be a normal stable subgroup of $H \cap K$. Suppose H' is a normal stable subgroup of H and K' is a normal stable subgroup of K and $J_1 = H' \sqcup H \cap K'$ and $H_4 = H' \cap K \sqcup K' \cap H$. Then $(H' \sqcup H \cap K)/J_1$ and $(H \cap K)/H_4$ are isomorphic.
- (92) Let H, K, H', K' be strict stable subgroups of G . Suppose H' is a normal stable subgroup of H and K' is a normal stable subgroup of K . Then $H' \sqcup H \cap K'$ is a normal stable subgroup of $H' \sqcup H \cap K$.
- (93) Let H, K, H', K' be strict stable subgroups of G , J_1 be a normal stable subgroup of $H' \sqcup H \cap K$, and J_2 be a normal stable subgroup of $K' \sqcup K \cap H$. Suppose $J_1 = H' \sqcup H \cap K'$ and $J_2 = K' \sqcup K \cap H'$ and H' is a normal stable subgroup of H and K' is a normal stable subgroup of K . Then $(H' \sqcup H \cap K)/J_1$ and $(K' \sqcup K \cap H)/J_2$ are isomorphic.

5. COMPOSITION SERIES

Let O be a set, let G be a group with operators in O , and let I_1 be a finite sequence of elements of the stable subgroups of G . We say that I_1 is composition series if and only if the conditions (Def. 31) are satisfied.

- (Def. 31)(i) $I_1(1) = \Omega_G$,
(ii) $I_1(\text{len } I_1) = \{\mathbf{1}\}_G$, and
(iii) for every natural number i such that $i \in \text{dom } I_1$ and $i + 1 \in \text{dom } I_1$ and for all stable subgroups H_1, H_2 of G such that $H_1 = I_1(i)$ and $H_2 = I_1(i + 1)$ holds H_2 is a normal stable subgroup of H_1 .

Let O be a set and let G be a group with operators in O . One can verify that there exists a finite sequence of elements of the stable subgroups of G which is composition series.

Let O be a set and let G be a group with operators in O . A composition series of G is a composition series finite sequence of elements of the stable subgroups of G .

Let O be a set, let G be a group with operators in O , and let s_1, s_2 be composition series of G . We say that s_1 is finer than s_2 if and only if:

- (Def. 32) There exists a set x such that $x \subseteq \text{dom } s_1$ and $s_2 = s_1 \cdot \text{Sgm } x$.

Let us note that the predicate s_1 is finer than s_2 is reflexive.

Let O be a set, let G be a group with operators in O , and let I_1 be a composition series of G . We say that I_1 is strictly decreasing if and only if the condition (Def. 33) is satisfied.

- (Def. 33) Let i be a natural number. Suppose $i \in \text{dom } I_1$ and $i + 1 \in \text{dom } I_1$. Let H be a stable subgroup of G and N be a normal stable subgroup of H . If $H = I_1(i)$ and $N = I_1(i + 1)$, then H/N is not trivial.

Let O be a set, let G be a group with operators in O , and let I_1 be a composition series of G . We say that I_1 is Jordan-Hölder if and only if the conditions (Def. 34) are satisfied.

- (Def. 34)(i) I_1 is strictly decreasing, and
(ii) it is not true that there exists a composition series s of G such that $s \neq I_1$ and s is strictly decreasing and finer than I_1 .

Let O be a set, let G_1, G_2 be groups with operators in O , let s_1 be a composition series of G_1 , and let s_2 be a composition series of G_2 . We say that s_1 is equivalent with s_2 if and only if the conditions (Def. 35) are satisfied.

- (Def. 35)(i) $\text{len } s_1 = \text{len } s_2$, and
(ii) for every natural number n such that $n + 1 = \text{len } s_1$ there exists a permutation p of $\text{Seg } n$ such that for every stable subgroup H_1 of G_1 and for every stable subgroup H_2 of G_2 and for every normal stable subgroup N_1 of H_1 and for every normal stable subgroup N_2 of H_2 and for all natural numbers i, j such that $1 \leq i$ and $i \leq n$ and $j = p(i)$ and $H_1 = s_1(i)$ and

$H_2 = s_2(j)$ and $N_1 = s_1(i + 1)$ and $N_2 = s_2(j + 1)$ holds H_1/N_1 and H_2/N_2 are isomorphic.

Let O be a set, let G be a group with operators in O , and let s be a composition series of G . The series of quotients of s yielding a finite sequence is defined as follows:

- (Def. 36)(i) $\text{len } s = \text{len}(\text{the series of quotients of } s) + 1$ and for every natural number i such that $i \in \text{dom}(\text{the series of quotients of } s)$ and for every stable subgroup H of G and for every normal stable subgroup N of H such that $H = s(i)$ and $N = s(i + 1)$ holds (the series of quotients of s)(i) = H/N if $\text{len } s > 1$,
- (ii) the series of quotients of $s = \emptyset$, otherwise.

Let O be a set, let f_1, f_2 be finite sequences, and let p be a permutation of $\text{dom } f_1$. We say that f_1 and f_2 are equivalent under p in O if and only if the conditions (Def. 37) are satisfied.

- (Def. 37)(i) $\text{len } f_1 = \text{len } f_2$, and
- (ii) for all groups H_1, H_2 with operators in O and for all natural numbers i, j such that $i \in \text{dom } f_1$ and $j = p^{-1}(i)$ and $H_1 = f_1(i)$ and $H_2 = f_2(j)$ holds H_1 and H_2 are isomorphic.

For simplicity, we follow the rules: y is a set, s_1, s'_1, s_2, s'_2 are composition series of G , f_3 is a finite sequence of elements of the stable subgroups of G , f_1, f_2 are finite sequences, and i, j, n are natural numbers.

We now state a number of propositions:

- (94) If $i \in \text{dom } s_1$ and $i + 1 \in \text{dom } s_1$ and $s_1(i) = s_1(i + 1)$ and $f_3 = (s_1)_{|i}$, then f_3 is composition series.
- (95) If s_1 is finer than s_2 , then there exists n such that $\text{len } s_1 = \text{len } s_2 + n$.
- (96) If $\text{len } s_2 = \text{len } s_1$ and s_2 is finer than s_1 , then $s_1 = s_2$.
- (97) If s_1 is not empty and s_2 is finer than s_1 , then s_2 is not empty.
- (98) If s_1 is finer than s_2 and Jordan-Hölder and s_2 is Jordan-Hölder, then $s_1 = s_2$.
- (99) If $i \in \text{dom } s_1$ and $i + 1 \in \text{dom } s_1$ and $s_1(i) = s_1(i + 1)$ and $s'_1 = (s_1)_{|i}$ and s_2 is Jordan-Hölder and s_1 is finer than s_2 , then s'_1 is finer than s_2 .
- (100) Suppose $\text{len } s_1 > 1$ and $s_2 \neq s_1$ and s_2 is strictly decreasing and finer than s_1 . Then there exist i, j such that $i \in \text{dom } s_1$ and $i \in \text{dom } s_2$ and $i + 1 \in \text{dom } s_1$ and $i + 1 \in \text{dom } s_2$ and $j \in \text{dom } s_2$ and $i + 1 < j$ and $s_1(i) = s_2(i)$ and $s_1(i + 1) \neq s_2(i + 1)$ and $s_1(i + 1) = s_2(j)$.
- (101) If $i \in \text{dom } s_1$ and $j \in \text{dom } s_1$ and $i \leq j$ and $H_1 = s_1(i)$ and $H_2 = s_1(j)$, then H_2 is a stable subgroup of H_1 .
- (102) If $y \in \text{rng}(\text{the series of quotients of } s_1)$, then y is a strict group with operators in O .

- (103) Suppose $i \in \text{dom}(\text{the series of quotients of } s_1)$ and for every H such that $H = (\text{the series of quotients of } s_1)(i)$ holds H is trivial. Then $i \in \text{dom } s_1$ and $i + 1 \in \text{dom } s_1$ and $s_1(i) = s_1(i + 1)$.
- (104) Suppose $i \in \text{dom } s_1$ and $i + 1 \in \text{dom } s_1$ and $s_1(i) = s_1(i + 1)$ and $s_2 = (s_1)_{\upharpoonright i}$. Then the series of quotients of $s_2 = (\text{the series of quotients of } s_1)_{\upharpoonright i}$.
- (105) Suppose $f_1 = \text{the series of quotients of } s_1$ and $i \in \text{dom } f_1$ and for every H such that $H = f_1(i)$ holds H is trivial. Then $(s_1)_{\upharpoonright i}$ is a composition series of G and for every s_2 such that $s_2 = (s_1)_{\upharpoonright i}$ holds the series of quotients of $s_2 = (f_1)_{\upharpoonright i}$.
- (106) Suppose that
- (i) $f_1 = \text{the series of quotients of } s_1$,
 - (ii) $f_2 = \text{the series of quotients of } s_2$,
 - (iii) $i \in \text{dom } f_1$,
 - (iv) for every H such that $H = f_1(i)$ holds H is trivial, and
 - (v) there exists a permutation p of $\text{dom } f_1$ such that f_1 and f_2 are equivalent under p in O and $j = p^{-1}(i)$.
- Then there exists a permutation p' of $\text{dom}((f_1)_{\upharpoonright i})$ such that $(f_1)_{\upharpoonright i}$ and $(f_2)_{\upharpoonright j}$ are equivalent under p' in O .
- (107) Let G_1, G_2 be groups with operators in O , s_1 be a composition series of G_1 , and s_2 be a composition series of G_2 . If s_1 is empty and s_2 is empty, then s_1 is equivalent with s_2 .
- (108) Let G_1, G_2 be groups with operators in O , s_1 be a composition series of G_1 , and s_2 be a composition series of G_2 . Suppose s_1 is not empty and s_2 is not empty. Then s_1 is equivalent with s_2 if and only if there exists a permutation p of $\text{dom}(\text{the series of quotients of } s_1)$ such that the series of quotients of s_1 and the series of quotients of s_2 are equivalent under p in O .
- (109) Suppose s_1 is finer than s_2 and s_2 is Jordan-Hölder and $\text{len } s_1 > \text{len } s_2$. Then there exists i such that $i \in \text{dom}(\text{the series of quotients of } s_1)$ and for every H such that $H = (\text{the series of quotients of } s_1)(i)$ holds H is trivial.
- (110) Suppose $\text{len } s_1 > 1$. Then s_1 is Jordan-Hölder if and only if for every i such that $i \in \text{dom}(\text{the series of quotients of } s_1)$ holds $(\text{the series of quotients of } s_1)(i)$ is a strict simple group with operators in O .
- (111) Suppose $1 \leq i$ and $i \leq \text{len } s_1 - 1$. Then $s_1(i)$ is a strict stable subgroup of G and $s_1(i + 1)$ is a strict stable subgroup of G .
- (112) If $1 \leq i$ and $i \leq \text{len } s_1 - 1$ and $H_1 = s_1(i)$ and $H_2 = s_1(i + 1)$, then H_2 is a normal stable subgroup of H_1 .
- (113) s_1 is equivalent with s_1 .

- (114) If $\text{len } s_1 \leq 1$ or $\text{len } s_2 \leq 1$ and if $\text{len } s_1 \leq \text{len } s_2$, then s_2 is finer than s_1 .
 (115) If s_1 is equivalent with s_2 and Jordan-Hölder, then s_2 is Jordan-Hölder.

6. THE SCHREIER REFINEMENT THEOREM

Let us consider O, G, s_1, s_2 . Let us assume that $\text{len } s_1 > 1$ and $\text{len } s_2 > 1$. The Schreier series of s_1 and s_2 yielding a composition series of G is defined by the condition (Def. 38).

- (Def. 38) Let k, i, j be natural numbers and H_1, H_2, H_3 be stable subgroups of G . Then
- (i) if $k = (i - 1) \cdot (\text{len } s_2 - 1) + j$ and $1 \leq i$ and $i \leq \text{len } s_1 - 1$ and $1 \leq j$ and $j \leq \text{len } s_2 - 1$ and $H_1 = s_1(i + 1)$ and $H_2 = s_1(i)$ and $H_3 = s_2(j)$, then (the Schreier series of s_1 and s_2)(k) = $H_1 \sqcup H_2 \cap H_3$,
 - (ii) if $k = (\text{len } s_1 - 1) \cdot (\text{len } s_2 - 1) + 1$, then (the Schreier series of s_1 and s_2)(k) = $\{\mathbf{1}\}_G$, and
 - (iii) len (the Schreier series of s_1 and s_2) = $(\text{len } s_1 - 1) \cdot (\text{len } s_2 - 1) + 1$.

Next we state three propositions:

- (116) If $\text{len } s_1 > 1$ and $\text{len } s_2 > 1$, then the Schreier series of s_1 and s_2 is finer than s_1 .
 (117) If $\text{len } s_1 > 1$ and $\text{len } s_2 > 1$, then the Schreier series of s_1 and s_2 is equivalent with the Schreier series of s_2 and s_1 .
 (118) There exist s'_1, s'_2 such that s'_1 is finer than s_1 and s'_2 is finer than s_2 and s'_1 is equivalent with s'_2 .

7. THE JORDAN-HÖLDER THEOREM

One can prove the following proposition

- (119) If s_1 is Jordan-Hölder and s_2 is Jordan-Hölder, then s_1 is equivalent with s_2 .

8. APPENDIX

Next we state several propositions:

- (120) For all binary relations P, R holds $P = \text{rng } P \upharpoonright R$ iff $P^\sim = R^\sim \upharpoonright \text{dom}(P^\sim)$.
 (121) For every set X and for all binary relations P, R holds $P \cdot (R \upharpoonright X) = (X \upharpoonright P) \cdot R$.
 (122) Let n be a natural number, X be a set, and f be a partial function from \mathbb{R} to \mathbb{R} . If $X \subseteq \text{Seg } n$ and $X \subseteq \text{dom } f$ and f is increasing on X and $f^\circ X \subseteq \mathbb{N} \setminus \{0\}$, then $\text{Sgm}(f^\circ X) = f \cdot \text{Sgm } X$.

- (123) Let y be a set and i, n be natural numbers. Suppose $y \subseteq \text{Seg}(n+1)$ and $i \in \text{Seg}(n+1)$ and $i \notin y$. Then there exists x such that $\text{Sgm } x = (\text{Sgm}(\text{Seg}(n+1) \setminus \{i\}))^{-1} \cdot \text{Sgm } y$ and $x \subseteq \text{Seg } n$.
- (124) Let D be a non empty set, f be a finite sequence of elements of D , p be an element of D , and n be an element of \mathbb{N} . If $n \in \text{dom } f$, then $f = (\text{Ins}(f, n, p)) \upharpoonright_{n+1}$.
- (125) Let G, H be groups, F_1 be a finite sequence of elements of the carrier of G , F_2 be a finite sequence of elements of the carrier of H , I be a finite sequence of elements of \mathbb{Z} , and f be a homomorphism from G to H . Suppose for every element k of \mathbb{N} such that $k \in \text{Seg len } F_1$ holds $F_2(k) = f(F_1(k))$ and $\text{len } F_1 = \text{len } I$ and $\text{len } F_2 = \text{len } I$. Then $f(\prod(F_1^I)) = \prod(F_2^I)$.

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. The ordinal numbers. *Formalized Mathematics*, 1(1):91–96, 1990.
- [4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [5] Nicolas Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3*. Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.
- [6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(3):529–536, 1990.
- [7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(2):357–367, 1990.
- [10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.
- [11] Czesław Byliński. Some properties of restrictions of finite sequences. *Formalized Mathematics*, 5(2):241–245, 1996.
- [12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(1):165–167, 1990.
- [13] Katarzyna Jankowska. Transpose matrices and groups of permutations. *Formalized Mathematics*, 2(5):711–717, 1991.
- [14] Jarosław Kotowicz. Properties of real functions. *Formalized Mathematics*, 1(4):781–786, 1990.
- [15] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(1):147–152, 1990.
- [16] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.
- [17] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(1):9–11, 1990.
- [18] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [19] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(5):955–962, 1990.
- [20] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(5):821–827, 1990.
- [21] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(3):569–573, 1990.
- [22] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(5):855–864, 1990.
- [23] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(1):41–47, 1991.
- [24] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(4):573–578, 1991.
- [25] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.

- [26] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.
- [27] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(1):181–186, 1990.

Received April 20, 2007
