

# Subgroup and Cosets of Subgroups

Wojciech A. Trybulec<sup>1</sup>  
Warsaw University

**Summary.** We introduce notion of subgroup, coset of a subgroup, sets of left and right cosets of a subgroup. We define multiplication of two subset of a group, subset of reverse elements of a group, intersection of two subgroups. We define the notion of an index of a subgroup and prove Lagrange theorem which states that in a finite group the order of the group equals the order of a subgroup multiplied by the index of the subgroup. Some theorems that belong rather to [1] are proved.

MML Identifier: GROUP\_2.

The papers [9], [6], [3], [4], [1], [11], [10], [12], [5], [8], [7], and [2] provide the notation and terminology for this paper. Let  $D$  be a non-empty set. Then  $\emptyset_D$  is a subset of  $D$ . Then  $\Omega_D$  is a subset of  $D$ .

For simplicity we adopt the following convention:  $x$  is arbitrary,  $X, Y, Z$  are sets,  $k$  is a natural number,  $G, G_1, G_2, G_3$  are groups, and  $a, b, g, g_1, g_2, h$  are elements of  $G$ . Let us consider  $G$ . A subset of  $G$  is a subset of the carrier of  $G$ .

In the sequel  $A, B, C$  denote subsets of  $G$ . The following propositions are true:

- (1) If  $x \in A$ , then  $x \in G$ .
- (2) If  $x \in A$ , then  $x$  is an element of  $G$ .
- (3) If  $G$  is finite, then  $A$  is finite.

Let us consider  $G, A$ . The functor  $A^{-1}$  yielding a subset of  $G$  is defined by:

(Def.1)  $A^{-1} = \{g^{-1} : g \in A\}$ .

Next we state several propositions:

- (4)  $A^{-1} = \{g^{-1} : g \in A\}$ .
- (5)  $x \in A^{-1}$  if and only if there exists  $g$  such that  $x = g^{-1}$  and  $g \in A$ .
- (6)  $\{g\}^{-1} = \{g^{-1}\}$ .

---

<sup>1</sup>Supported by RPBP.III-24.C1

- (7)  $\{g, h\}^{-1} = \{g^{-1}, h^{-1}\}$ .
- (8)  $(\emptyset_{\text{the carrier of } G})^{-1} = \emptyset$ .
- (9)  $(\Omega_{\text{the carrier of } G})^{-1} = \text{the carrier of } G$ .
- (10)  $A \neq \emptyset$  if and only if  $A^{-1} \neq \emptyset$ .

Let us consider  $G, A, B$ . The functor  $A \cdot B$  yielding a subset of  $G$  is defined as follows:

$$\text{(Def.2)} \quad A \cdot B = \{g \cdot h : g \in A \wedge h \in B\}.$$

One can prove the following propositions:

- (11)  $A \cdot B = \{g \cdot h : g \in A \wedge h \in B\}$ .
- (12)  $x \in A \cdot B$  if and only if there exist  $g, h$  such that  $x = g \cdot h$  and  $g \in A$  and  $h \in B$ .
- (13)  $A \neq \emptyset$  and  $B \neq \emptyset$  if and only if  $A \cdot B \neq \emptyset$ .
- (14)  $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ .
- (15)  $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$ .
- (16)  $A \cdot (B \cup C) = A \cdot B \cup A \cdot C$ .
- (17)  $(A \cup B) \cdot C = A \cdot C \cup B \cdot C$ .
- (18)  $A \cdot (B \cap C) \subseteq (A \cdot B) \cap (A \cdot C)$ .
- (19)  $(A \cap B) \cdot C \subseteq (A \cdot C) \cap (B \cdot C)$ .
- (20)  $\emptyset_{\text{the carrier of } G} \cdot A = \emptyset$  and  $A \cdot \emptyset_{\text{the carrier of } G} = \emptyset$ .
- (21) If  $A \neq \emptyset$ , then  $\Omega_{\text{the carrier of } G} \cdot A = \text{the carrier of } G$  and  $A \cdot \Omega_{\text{the carrier of } G} = \text{the carrier of } G$ .
- (22)  $\{g\} \cdot \{h\} = \{g \cdot h\}$ .
- (23)  $\{g\} \cdot \{g_1, g_2\} = \{g \cdot g_1, g \cdot g_2\}$ .
- (24)  $\{g_1, g_2\} \cdot \{g\} = \{g_1 \cdot g, g_2 \cdot g\}$ .
- (25)  $\{g, h\} \cdot \{g_1, g_2\} = \{g \cdot g_1, g \cdot g_2, h \cdot g_1, h \cdot g_2\}$ .
- (26) If for all  $g_1, g_2$  such that  $g_1 \in A$  and  $g_2 \in A$  holds  $g_1 \cdot g_2 \in A$  and for every  $g$  such that  $g \in A$  holds  $g^{-1} \in A$ , then  $A \cdot A = A$ .
- (27) If for every  $g$  such that  $g \in A$  holds  $g^{-1} \in A$ , then  $A^{-1} = A$ .
- (28) If for all  $a, b$  such that  $a \in A$  and  $b \in B$  holds  $a \cdot b = b \cdot a$ , then  $A \cdot B = B \cdot A$ .
- (29) If  $G$  is an Abelian group, then  $A \cdot B = B \cdot A$ .
- (30) If  $G$  is an Abelian group, then  $(A \cdot B)^{-1} = A^{-1} \cdot B^{-1}$ .

We now define two new functors. Let us consider  $G, g, A$ . The functor  $g \cdot A$  yields a subset of  $G$  and is defined as follows:

$$\text{(Def.3)} \quad g \cdot A = \{g\} \cdot A.$$

The functor  $A \cdot g$  yielding a subset of  $G$  is defined as follows:

$$\text{(Def.4)} \quad A \cdot g = A \cdot \{g\}.$$

Next we state a number of propositions:

- (31)  $g \cdot A = \{g\} \cdot A.$   
 (32)  $A \cdot g = A \cdot \{g\}.$   
 (33)  $x \in g \cdot A$  if and only if there exists  $h$  such that  $x = g \cdot h$  and  $h \in A.$   
 (34)  $x \in A \cdot g$  if and only if there exists  $h$  such that  $x = h \cdot g$  and  $h \in A.$   
 (35)  $(g \cdot A) \cdot B = g \cdot (A \cdot B).$   
 (36)  $(A \cdot g) \cdot B = A \cdot (g \cdot B).$   
 (37)  $(A \cdot B) \cdot g = A \cdot (B \cdot g).$   
 (38)  $(g \cdot h) \cdot A = g \cdot (h \cdot A).$   
 (39)  $(g \cdot A) \cdot h = g \cdot (A \cdot h).$   
 (40)  $(A \cdot g) \cdot h = A \cdot (g \cdot h).$   
 (41)  $\emptyset_{\text{the carrier of } G} \cdot a = \emptyset$  and  $a \cdot \emptyset_{\text{the carrier of } G} = \emptyset.$   
 (42)  $\Omega_{\text{the carrier of } G} \cdot a = \text{the carrier of } G$  and  $a \cdot \Omega_{\text{the carrier of } G} = \text{the carrier of } G.$   
 (43)  $(1_G) \cdot A = A$  and  $A \cdot (1_G) = A.$   
 (44) If  $G$  is an Abelian group, then  $g \cdot A = A \cdot g.$

Let us consider  $G$ . A group is said to be a subgroup of  $G$  if:

- (Def.5) the carrier of it  $\subseteq$  the carrier of  $G$  and the operation of it = (the operation of  $G$ )  $\upharpoonright$  [ the carrier of it, the carrier of it ].

One can prove the following proposition

- (45) If the carrier of  $G_1 \subseteq$  the carrier of  $G_2$  and the operation of  $G_1 =$  (the operation of  $G_2$ )  $\upharpoonright$  [ the carrier of  $G_1$ , the carrier of  $G_1$  ], then  $G_1$  is a subgroup of  $G_2.$

We follow the rules:  $I, H, H_1, H_2, H_3$  will be subgroups of  $G$  and  $h, h_1, h_2$  will be elements of  $H$ . One can prove the following propositions:

- (46) The carrier of  $H \subseteq$  the carrier of  $G.$   
 (47) The operation of  $H =$  (the operation of  $G$ )  $\upharpoonright$  [ the carrier of  $H$ , the carrier of  $H$  ].  
 (48) If  $G$  is finite, then  $H$  is finite.  
 (49) If  $x \in H$ , then  $x \in G.$   
 (50)  $h \in G.$   
 (51)  $h$  is an element of  $G.$   
 (52) If  $h_1 = g_1$  and  $h_2 = g_2$ , then  $h_1 \cdot h_2 = g_1 \cdot g_2.$   
 (53)  $1_H = 1_G.$   
 (54)  $1_{H_1} = 1_{H_2}.$   
 (55)  $1_G \in H.$   
 (56)  $1_{H_1} \in H_2.$   
 (57) If  $h = g$ , then  $h^{-1} = g^{-1}.$   
 (58)  $\cdot_H^{-1} = \cdot_G^{-1} \upharpoonright$  (the carrier of  $H$ ).  
 (59) If  $g_1 \in H$  and  $g_2 \in H$ , then  $g_1 \cdot g_2 \in H.$

- (60) If  $g \in H$ , then  $g^{-1} \in H$ .
- (61) If  $A \neq \emptyset$  and for all  $g_1, g_2$  such that  $g_1 \in A$  and  $g_2 \in A$  holds  $g_1 \cdot g_2 \in A$  and for every  $g$  such that  $g \in A$  holds  $g^{-1} \in A$ , then there exists  $H$  such that the carrier of  $H = A$ .
- (62) If  $G$  is an Abelian group, then  $H$  is an Abelian group.

Let  $G$  be an Abelian group. We see that the subgroup of  $G$  is an Abelian group.

We now state several propositions:

- (63)  $G$  is a subgroup of  $G$ .
- (64) If  $G_1$  is a subgroup of  $G_2$  and  $G_2$  is a subgroup of  $G_1$ , then  $G_1 = G_2$ .
- (65) If  $G_1$  is a subgroup of  $G_2$  and  $G_2$  is a subgroup of  $G_3$ , then  $G_1$  is a subgroup of  $G_3$ .
- (66) If the carrier of  $H_1 \subseteq$  the carrier of  $H_2$ , then  $H_1$  is a subgroup of  $H_2$ .
- (67) If for every  $g$  such that  $g \in H_1$  holds  $g \in H_2$ , then  $H_1$  is a subgroup of  $H_2$ .
- (68) If the carrier of  $H_1 =$  the carrier of  $H_2$ , then  $H_1 = H_2$ .
- (69) If for every  $g$  holds  $g \in H_1$  if and only if  $g \in H_2$ , then  $H_1 = H_2$ .

Let us consider  $G, H_1, H_2$ . Let us note that one can characterize the predicate  $H_1 = H_2$  by the following (equivalent) condition:

- (Def.6) for every  $g$  holds  $g \in H_1$  if and only if  $g \in H_2$ .

The following two propositions are true:

- (70) If the carrier of  $H =$  the carrier of  $G$ , then  $H = G$ .
- (71) If for every  $g$  holds  $g \in H$ , then  $H = G$ .

Let us consider  $G$ . The functor  $\{\mathbf{1}\}_G$  yields a subgroup of  $G$  and is defined by:

- (Def.7) the carrier of  $\{\mathbf{1}\}_G = \{1_G\}$ .

Let us consider  $G$ . The functor  $\Omega_G$  yielding a subgroup of  $G$  is defined as follows:

- (Def.8)  $\Omega_G = G$ .

The following propositions are true:

- (72) If the carrier of  $H = \{1_G\}$ , then  $H = \{\mathbf{1}\}_G$ .
- (73) The carrier of  $\{\mathbf{1}\}_G = \{1_G\}$ .
- (74)  $\Omega_G = G$ .
- (75)  $\{\mathbf{1}\}_H = \{\mathbf{1}\}_G$ .
- (76)  $\{\mathbf{1}\}_{H_1} = \{\mathbf{1}\}_{H_2}$ .
- (77)  $\{\mathbf{1}\}_G$  is a subgroup of  $H$ .
- (78)  $H$  is a subgroup of  $\Omega_G$ .
- (79)  $G$  is a subgroup of  $\Omega_G$ .
- (80)  $\{\mathbf{1}\}_G$  is finite.

- (81)  $\text{ord}(\{\mathbf{1}\}_G) = 1$ .  
 (82) If  $H$  is finite and  $\text{ord}(H) = 1$ , then  $H = \{\mathbf{1}\}_G$ .  
 (83)  $\text{Ord}(H) \leq \text{Ord}(G)$ .  
 (84) If  $G$  is finite, then  $\text{ord}(H) \leq \text{ord}(G)$ .  
 (85) If  $G$  is finite and  $\text{ord}(G) = \text{ord}(H)$ , then  $H = G$ .

Let us consider  $G, H$ . The functor  $\overline{H}$  yields a subset of  $G$  and is defined by:

(Def.9)  $\overline{H}$  = the carrier of  $H$ .

The following propositions are true:

- (86)  $\overline{H}$  = the carrier of  $H$ .  
 (87)  $\overline{H} \neq \emptyset$ .  
 (88)  $x \in \overline{H}$  if and only if  $x \in H$ .  
 (89) If  $g_1 \in \overline{H}$  and  $g_2 \in \overline{H}$ , then  $g_1 \cdot g_2 \in \overline{H}$ .  
 (90) If  $g \in \overline{H}$ , then  $g^{-1} \in \overline{H}$ .  
 (91)  $\overline{H} \cdot \overline{H} = \overline{H}$ .  
 (92)  $\overline{H}^{-1} = \overline{H}$ .  
 (93)  $\overline{H_1} \cdot \overline{H_2} = \overline{H_2} \cdot \overline{H_1}$  if and only if there exists  $H$  such that the carrier of  $H = \overline{H_1} \cdot \overline{H_2}$ .  
 (94) If  $G$  is an Abelian group, then there exists  $H$  such that the carrier of  $H = \overline{H_1} \cdot \overline{H_2}$ .

Let us consider  $G, H_1, H_2$ . The functor  $H_1 \cap H_2$  yields a subgroup of  $G$  and is defined as follows:

(Def.10) the carrier of  $H_1 \cap H_2 = \overline{H_1} \cap \overline{H_2}$ .

One can prove the following propositions:

- (95) If the carrier of  $H = \overline{H_1} \cap \overline{H_2}$ , then  $H = H_1 \cap H_2$ .  
 (96) The carrier of  $H_1 \cap H_2 = \overline{H_1} \cap \overline{H_2}$ .  
 (97)  $H = H_1 \cap H_2$  if and only if the carrier of  $H = (\text{the carrier of } H_1) \cap (\text{the carrier of } H_2)$ .  
 (98)  $\overline{H_1 \cap H_2} = \overline{H_1} \cap \overline{H_2}$ .  
 (99)  $x \in H_1 \cap H_2$  if and only if  $x \in H_1$  and  $x \in H_2$ .  
 (100)  $H \cap H = H$ .  
 (101)  $H_1 \cap H_2 = H_2 \cap H_1$ .  
 (102)  $(H_1 \cap H_2) \cap H_3 = H_1 \cap (H_2 \cap H_3)$ .  
 (103)  $\{\mathbf{1}\}_G \cap H = \{\mathbf{1}\}_G$  and  $H \cap \{\mathbf{1}\}_G = \{\mathbf{1}\}_G$ .  
 (104)  $H \cap \Omega_G = H$  and  $\Omega_G \cap H = H$ .  
 (105)  $\Omega_G \cap \Omega_G = G$ .  
 (106)  $H_1 \cap H_2$  is a subgroup of  $H_1$  and  $H_1 \cap H_2$  is a subgroup of  $H_2$ .  
 (107)  $H_1$  is a subgroup of  $H_2$  if and only if  $H_1 \cap H_2 = H_1$ .  
 (108) If  $H_1$  is a subgroup of  $H_2$ , then  $H_1 \cap H_3$  is a subgroup of  $H_2$ .

(109) If  $H_1$  is a subgroup of  $H_2$  and  $H_1$  is a subgroup of  $H_3$ , then  $H_1$  is a subgroup of  $H_2 \cap H_3$ .

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

(111) If  $H_1$  is finite or  $H_2$  is finite, then  $H_1 \cap H_2$  is finite.

We now define two new functors. Let us consider  $G, H, A$ . The functor  $A \cdot H$  yielding a subset of  $G$  is defined as follows:

(Def.11)  $A \cdot H = A \cdot \overline{H}$ .

The functor  $H \cdot A$  yields a subset of  $G$  and is defined as follows:

(Def.12)  $H \cdot A = \overline{H} \cdot A$ .

One can prove the following propositions:

(112)  $A \cdot H = A \cdot \overline{H}$ .

(113)  $H \cdot A = \overline{H} \cdot A$ .

(114)  $x \in A \cdot H$  if and only if there exist  $g_1, g_2$  such that  $x = g_1 \cdot g_2$  and  $g_1 \in A$  and  $g_2 \in H$ .

(115)  $x \in H \cdot A$  if and only if there exist  $g_1, g_2$  such that  $x = g_1 \cdot g_2$  and  $g_1 \in H$  and  $g_2 \in A$ .

(116)  $(A \cdot B) \cdot H = A \cdot (B \cdot H)$ .

(117)  $(A \cdot H) \cdot B = A \cdot (H \cdot B)$ .

(118)  $(H \cdot A) \cdot B = H \cdot (A \cdot B)$ .

(119)  $(A \cdot H_1) \cdot H_2 = A \cdot (H_1 \cdot \overline{H_2})$ .

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

(121)  $(H_1 \cdot \overline{H_2}) \cdot A = H_1 \cdot (H_2 \cdot A)$ .

(122) If  $G$  is an Abelian group, then  $A \cdot H = H \cdot A$ .

We now define two new functors. Let us consider  $G, H, a$ . The functor  $a \cdot H$  yielding a subset of  $G$  is defined as follows:

(Def.13)  $a \cdot H = a \cdot \overline{H}$ .

The functor  $H \cdot a$  yielding a subset of  $G$  is defined by:

(Def.14)  $H \cdot a = \overline{H} \cdot a$ .

The following propositions are true:

(123)  $a \cdot H = a \cdot \overline{H}$ .

(124)  $H \cdot a = \overline{H} \cdot a$ .

(125)  $x \in a \cdot H$  if and only if there exists  $g$  such that  $x = a \cdot g$  and  $g \in H$ .

(126)  $x \in H \cdot a$  if and only if there exists  $g$  such that  $x = g \cdot a$  and  $g \in H$ .

(127)  $(a \cdot b) \cdot H = a \cdot (b \cdot H)$ .

(128)  $(a \cdot H) \cdot b = a \cdot (H \cdot b)$ .

(129)  $(H \cdot a) \cdot b = H \cdot (a \cdot b)$ .

(130)  $a \in a \cdot H$  and  $a \in H \cdot a$ .

(131)  $a \cdot H \neq \emptyset$  and  $H \cdot a \neq \emptyset$ .

(132)  $(1_G) \cdot H = \overline{H}$  and  $H \cdot (1_G) = \overline{H}$ .

- (133)  $\{\mathbf{1}\}_G \cdot a = \{a\}$  and  $a \cdot \{\mathbf{1}\}_G = \{a\}$ .
- (134)  $a \cdot \Omega_G =$  the carrier of  $G$  and  $\Omega_G \cdot a =$  the carrier of  $G$ .
- (135) If  $G$  is an Abelian group, then  $a \cdot H = H \cdot a$ .
- (136)  $a \in H$  if and only if  $a \cdot H = \overline{H}$ .
- (137)  $a \cdot H = b \cdot H$  if and only if  $b^{-1} \cdot a \in H$ .
- (138)  $a \cdot H = b \cdot H$  if and only if  $a \cdot H$  meets  $b \cdot H$ .
- (139)  $(a \cdot b) \cdot H \subseteq (a \cdot H) \cdot (b \cdot H)$ .
- (140)  $\overline{H} \subseteq (a \cdot H) \cdot (a^{-1} \cdot H)$  and  $\overline{H} \subseteq (a^{-1} \cdot H) \cdot (a \cdot H)$ .
- (141)  $a^2 \cdot H \subseteq (a \cdot H) \cdot (a \cdot H)$ .
- (142)  $a \in H$  if and only if  $H \cdot a = \overline{H}$ .
- (143)  $H \cdot a = H \cdot b$  if and only if  $b \cdot a^{-1} \in H$ .
- (144)  $H \cdot a = H \cdot b$  if and only if  $H \cdot a$  meets  $H \cdot b$ .
- (145)  $(H \cdot a) \cdot b \subseteq (H \cdot a) \cdot (H \cdot b)$ .
- (146)  $\overline{H} \subseteq (H \cdot a) \cdot (H \cdot a^{-1})$  and  $\overline{H} \subseteq (H \cdot a^{-1}) \cdot (H \cdot a)$ .
- (147)  $H \cdot a^2 \subseteq (H \cdot a) \cdot (H \cdot a)$ .
- (148)  $a \cdot (H_1 \cap H_2) = (a \cdot H_1) \cap (a \cdot H_2)$ .
- (149)  $(H_1 \cap H_2) \cdot a = (H_1 \cdot a) \cap (H_2 \cdot a)$ .
- (150) There exists  $H_1$  such that the carrier of  $H_1 = (a \cdot H_2) \cdot a^{-1}$ .
- (151)  $a \cdot H \approx b \cdot H$ .
- (152)  $a \cdot H \approx H \cdot b$ .
- (153)  $H \cdot a \approx H \cdot b$ .
- (154)  $\overline{H} \approx a \cdot H$  and  $\overline{H} \approx H \cdot a$ .
- (155)  $\text{Ord}(H) = \overline{a \cdot H}$  and  $\text{Ord}(H) = \overline{H \cdot a}$ .
- (156) If  $H$  is finite, then  $\text{ord}(H) = \text{card}(a \cdot H)$  and  $\text{ord}(H) = \text{card}(H \cdot a)$ .

The scheme *SubFamComp* deals with a set  $\mathcal{A}$ , a family  $\mathcal{B}$  of subsets of  $\mathcal{A}$ , a family  $\mathcal{C}$  of subsets of  $\mathcal{A}$ , and a unary predicate  $\mathcal{P}$ , and states that:

$$\mathcal{B} = \mathcal{C}$$

provided the parameters meet the following requirements:

- for every subset  $X$  of  $\mathcal{A}$  holds  $X \in \mathcal{B}$  if and only if  $\mathcal{P}[X]$ ,
- for every subset  $X$  of  $\mathcal{A}$  holds  $X \in \mathcal{C}$  if and only if  $\mathcal{P}[X]$ .

We now define two new functors. Let us consider  $G, H$ . The left cosets of  $H$  yielding a family of subsets of the carrier of  $G$  is defined as follows:

(Def.15)  $A \in$  the left cosets of  $H$  if and only if there exists  $a$  such that  $A = a \cdot H$ .

The right cosets of  $H$  yielding a family of subsets of the carrier of  $G$  is defined by:

(Def.16)  $A \in$  the right cosets of  $H$  if and only if there exists  $a$  such that  $A = H \cdot a$ .

In the sequel  $F$  denotes a family of subsets of the carrier of  $G$ . One can prove the following propositions:

(157) If for every  $A$  holds  $A \in F$  if and only if there exists  $a$  such that  $A = a \cdot H$ , then  $F =$  the left cosets of  $H$ .

- (158) If for every  $A$  holds  $A \in F$  if and only if there exists  $a$  such that  $A = H \cdot a$ , then  $F =$  the right cosets of  $H$ .
- (159)  $A \in$  the left cosets of  $H$  if and only if there exists  $a$  such that  $A = a \cdot H$ .
- (160)  $A \in$  the right cosets of  $H$  if and only if there exists  $a$  such that  $A = H \cdot a$ .
- (161) If  $x \in$  the left cosets of  $H$  or  $x \in$  the right cosets of  $H$ , then  $x$  is a subset of  $G$ .
- (162)  $x \in$  the left cosets of  $H$  if and only if there exists  $a$  such that  $x = a \cdot H$ .
- (163)  $x \in$  the right cosets of  $H$  if and only if there exists  $a$  such that  $x = H \cdot a$ .
- (164) If  $G$  is finite, then the right cosets of  $H$  is finite and the left cosets of  $H$  is finite.
- (165)  $\overline{H} \in$  the left cosets of  $H$  and  $\overline{H} \in$  the right cosets of  $H$ .
- (166) The left cosets of  $H \approx$  the right cosets of  $H$ .
- (167)  $\bigcup$ (The left cosets of  $H$ ) = the carrier of  $G$  and  $\bigcup$ (the right cosets of  $H$ ) = the carrier of  $G$ .
- (168) The left cosets of  $\{\mathbf{1}\}_G = \{\{a\}\}$ .
- (169) The right cosets of  $\{\mathbf{1}\}_G = \{\{a\}\}$ .
- (170) If the left cosets of  $H = \{\{a\}\}$ , then  $H = \{\mathbf{1}\}_G$ .
- (171) If the right cosets of  $H = \{\{a\}\}$ , then  $H = \{\mathbf{1}\}_G$ .
- (172) The left cosets of  $\Omega_G = \{\text{the carrier of } G\}$  and the right cosets of  $\Omega_G = \{\text{the carrier of } G\}$ .
- (173) If the left cosets of  $H = \{\text{the carrier of } G\}$ , then  $H = G$ .
- (174) If the right cosets of  $H = \{\text{the carrier of } G\}$ , then  $H = G$ .

Let us consider  $G, H$ . The functor  $|\bullet : H|$  yielding a cardinal number is defined by:

(Def.17)  $|\bullet : H| = \overline{\overline{\text{the left cosets of } H}}$ .

We now state the proposition

(175)  $|\bullet : H| = \overline{\overline{\text{the left cosets of } H}}$  and  $|\bullet : H| = \overline{\overline{\text{the right cosets of } H}}$ .

Let us consider  $G, H$ . Let us assume that the left cosets of  $H$  is finite. The functor  $|\bullet : H|_{\mathbb{N}}$  yielding a natural number is defined as follows:

(Def.18)  $|\bullet : H|_{\mathbb{N}} = \text{card}(\text{the left cosets of } H)$ .

Next we state the proposition

(176) If the left cosets of  $H$  is finite, then  $|\bullet : H|_{\mathbb{N}} = \text{card}(\text{the left cosets of } H)$  and  $|\bullet : H|_{\mathbb{N}} = \text{card}(\text{the right cosets of } H)$ .

Let  $D$  be a non-empty set, and let  $d$  be an element of  $D$ . Then  $\{d\}$  is an element of  $\text{Fin } D$ .

The following two propositions are true:

(177) If  $G$  is finite, then  $\text{ord}(G) = \text{ord}(H) \cdot |\bullet : H|_{\mathbb{N}}$ .

(178) If  $G$  is finite, then  $\text{ord}(H) \mid \text{ord}(G)$ .

In the sequel  $J$  will denote a subgroup of  $H$ . One can prove the following propositions:



- (179) If  $G$  is finite and  $I = J$ , then  $|\bullet : I|_{\mathbb{N}} = |\bullet : J|_{\mathbb{N}} \cdot |\bullet : H|_{\mathbb{N}}$ .
- (180)  $|\bullet : \Omega_G|_{\mathbb{N}} = 1$ .
- (181) If the left cosets of  $H$  is finite and  $|\bullet : H|_{\mathbb{N}} = 1$ , then  $H = G$ .
- (182)  $|\bullet : \{\mathbf{1}\}_G| = \text{Ord}(G)$ .
- (183) If  $G$  is finite, then  $|\bullet : \{\mathbf{1}\}_G|_{\mathbb{N}} = \text{ord}(G)$ .
- (184) If  $G$  is finite and  $|\bullet : H|_{\mathbb{N}} = \text{ord}(G)$ , then  $H = \{\mathbf{1}\}_G$ .
- (185) If the left cosets of  $H$  is finite and  $|\bullet : H| = \text{Ord}(G)$ , then  $G$  is finite and  $H = \{\mathbf{1}\}_G$ .
- (186) If  $X$  is finite and for every  $Y$  such that  $Y \in X$  holds  $Y$  is finite and  $\text{card } Y = k$  and for every  $Z$  such that  $Z \in X$  and  $Y \neq Z$  holds  $Y \approx Z$  and  $Y$  misses  $Z$ , then  $\text{card}(\bigcup X) = k \cdot \text{card } X$ .
- (187) If  $Y$  is finite and  $X \subseteq Y$  and  $\text{card } X = \text{card } Y$ , then  $X = Y$ .

## 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] 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] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(1):165–167, 1990.
- [6] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(1):147–152, 1990.
- [7] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(1):115–122, 1990.
- [8] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(1):25–34, 1990.
- [9] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(1):9–11, 1990.
- [10] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1(1):187–190, 1990.
- [11] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(5):821–827, 1990.

- [12] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.

*Received July 23, 1990*

---