FORMALIZED MATHEMATICS
Vol. 33, No. 1, pp. 71–89, 2025
DOI: 10.2478/forma-2025-0007
e-ISSN: 1898–9934

sciendo
sciendo.com/journal/forma

Semidirect Products of Groups

Alexander M. Nelson
Los Angeles, California
United States of America

Summary. We formalize the semidirect product of groups in Mizar, following §10 of Aschbacher [1]. We also prove the universal property for semidirect products as found in Bourbaki [7, III §2.10] Proposition 27. In an appendix, we define the dihdral group of the regular n-gon and the infinite dihedral group.

MSC: 20E22 68V20

Keywords: semidirect product; subgroup complement; dihedral group

MML identifier: GROUP_24, version: 8.1.15 5.94.1493

1. Preliminaries

Now we state the proposition:

(1) Let us consider natural numbers a, b. If $a < b$ and $b \neq 0$, then $2 \cdot a \operatorname{div} b < 2$.

From now on G, A denote groups and φ denotes a homomorphism from A to AutGroup(G).

Now we state the propositions:

(2) Let us consider a non empty, unital multiplicative magma M. Suppose for every element h of M, there exists an element g of M such that $h \cdot g = \mathbf{1}_M$ and $g \cdot h = \mathbf{1}_M$. Then M is group-like.

(3) Let us consider a group G, and a subgroup H of G. Then the multiplicative magma of H is a strict subgroup of G.

(4) Let us consider a group G, and a normal subgroup N of G. Then the multiplicative magma of N is a strict, normal subgroup of G.

Proof: Reconsider $N_0 =$ the multiplicative magma of N as a strict subgroup of G. For every element g of G, ${N_0}^g = N_0$ by [15, (59)]. □

(5) Let us consider a group G, a subgroup H of G, and a normal subgroup N of G. Suppose N is a subgroup of H. Then the multiplicative magma of N = the multiplicative magma of $(N)_H$. The theorem is a consequence of (4).

Let us consider a group G, subgroups H_1, H_2, K of G, and subgroups K_1, K_2 of K. Now we state the propositions:

(6) Suppose the multiplicative magma of H_1 = the multiplicative magma of K_1 and the multiplicative magma of H_2 = the multiplicative magma of K_2. Then $H_1 \cap H_2 = K_1 \cap K_2$.
PROOF: For every element g of G such that $g \in H_1 \cap H_2$ holds $g \in K_1 \cap K_2$ by [15, (82)]. For every element g of G such that $g \in K_1 \cap K_2$ holds $g \in H_1 \cap H_2$ by [15, (82)]. □

(7) Suppose the multiplicative magma of H_1 = the multiplicative magma of K_1 and the multiplicative magma of H_2 = the multiplicative magma of K_2. Then $H_1 \cdot H_2 = K_1 \cdot K_2$.
PROOF: For every object x, $x \in \overline{H_1} \cdot \overline{H_2}$ iff $x \in \overline{K_1} \cdot \overline{K_2}$ by [15, (43), (42)]. □

Now we state the propositions:

(8) Let us consider a group G, and a subset A of G. Suppose A = the carrier of G. Then $\mathrm{gr}(A)$ = the multiplicative magma of G.

(9) A and the multiplicative magma of A are isomorphic.

(10) Let us consider a group G, a normal subgroup N of G, and elements g_1, g_2 of G. Suppose $g_1 \cdot N = g_2 \cdot N$. Then there exists an element n of G such that

(i) $n \in N$, and

(ii) $g_1 = g_2 \cdot n$.

Let us consider a group G and subgroups H_1, H_2 of G. Now we state the propositions:

(11) (i) $H_1 \cdot H_2 \subseteq$ the carrier of $H_1 \sqcup H_2$, and

(ii) $H_2 \cdot H_1 \subseteq$ the carrier of $H_1 \sqcup H_2$.

(12) If $H_1 \cdot H_2$ = the carrier of $H_1 \sqcup H_2$, then $H_1 \cdot H_2 = H_2 \cdot H_1$.
PROOF: $H_2 \cdot H_1 \subseteq H_1 \cdot H_2$. For every element x of G such that $x \in H_1 \cdot H_2$ holds $x \in H_2 \cdot H_1$ by [15, (51)], [17, (4)], [14, (17)]. □

Now we state the propositions:

(13) Let us consider a group G, subgroups H, K of G, and a subgroup H_3 of K. Suppose the multiplicative magma of H = the multiplicative magma of H_3. Then $\overline{H} = \overline{H_3}$.

(14) Let us consider a group G, and subgroups H, K of G. Suppose H is a subgroup of K. Let us consider a subgroup N of G. If N is a normal subgroup of K, then $N \cdot H = H \cdot N$. The theorem is a consequence of (7).

(15) Let us consider a group G, a subgroup H of G, and a normal subgroup N of G. Suppose N is a subgroup of H. Then the multiplicative magma of N = the multiplicative magma of $(N)_H$. The theorem is a consequence of (4).

(16) Let us consider a group G, and subgroups H_1, N_1, H_2, N_2 of G. Suppose the multiplicative magma of H_1 = the multiplicative magma of H_2 and the multiplicative magma of N_1 = the multiplicative magma of N_2. Then

(i) $H_1 \cdot N_1 = H_2 \cdot N_2$, and

(ii) $H_1 \cap N_1 = H_2 \cap N_2$.

The theorem is a consequence of (3), (7), and (6).

(17) Let us consider a group G, and strict subgroups H, K of G. Suppose $H \neq K$ and K is a subgroup of H. Then there exists an element g of G such that

(i) $g \in H$, and

(ii) $g \notin K$.

2. Automorphism Group Results

Let G, A be groups. One can verify that $\prod$(the support of $\langle A, G \rangle$) is non empty.

Now we state the propositions:

(18) Let us consider groups G_1, G_2, and an element x of $\prod \langle G_1, G_2 \rangle$. Then

(i) $x(1) \in G_1$, and

(ii) $x(2) \in G_2$, and

(iii) $\operatorname{dom} x = \{1, 2\}$.

(19) Let us consider groups G_1, G_2, a subgroup H_1 of G_1, a subgroup H_2 of G_2, and an element h_1 of G_1. Suppose $h_1 \in H_1$. Let us consider an element h_2 of G_2. Suppose $h_2 \in H_2$. Then $\langle h_1, h_2 \rangle \in \prod \langle H_1, H_2 \rangle$.

3. Semidirect Products of Groups

From now on G, A denote groups and φ denotes a homomorphism from A to AutGroup(G).

Now we state the propositions:

(20) Let us consider an element g of G. Then $\varphi(\mathbf{1}_A)(g) = g$.

(21) Let us consider elements a_1, a_2 of A, and an element g of G. Then $\varphi(a_1)(\varphi(a_2)(g)) = (\varphi(a_1 \cdot a_2))(g)$.

(22) Let us consider an element a of A, and an element g of G. Then

(i) $\varphi(a^{-1})(\varphi(a)(g)) = g$, and

(ii) $\varphi(a)(\varphi(a^{-1})(g)) = g$.

The theorem is a consequence of (21) and (20).

Let us consider G, A, and φ. The functor $G \rtimes_\varphi A$ yielding a non empty, strict multiplicative magma is defined by

(Def. 1) the carrier of $it = \prod$(the support of $\langle G, A\rangle$) and for every elements f, g of $\prod$(the support of $\langle G, A\rangle$), there exists a function h and there exists an element a_1 of A and there exists an element g_2 of G such that $h =$ (the multiplication of it)(f, g) and $a_1 = f(2)$ and $g_2 = g(1)$ and $h(1) =$ (the multiplication of G)$(f(1), \varphi(a_1)(g_2))$ and $h(2) =$ (the multiplication of A)$(f(2), g(2))$.

One can check that $G \rtimes_\varphi A$ is constituted functions and every element of $G \rtimes_\varphi A$ is finite sequence-like.

Now we state the propositions:

(23) The carrier of $G \rtimes_\varphi A =$ the carrier of $\prod\langle G, A\rangle$.

(24) Let us consider an element a of A, and an element g of G. Then $\langle g, a\rangle$ is an element of $G \rtimes_\varphi A$.

Let us consider an element x of $G \rtimes_\varphi A$. Now we state the propositions:

(25) (i) $x(1) \in G$, and

(ii) $x(2) \in A$, and

(iii) $\operatorname{dom} x = \{1, 2\}$.

The theorem is a consequence of (23) and (18).

(26) There exists an element g of G and there exists an element a of A such that $x = \langle g, a\rangle$. The theorem is a consequence of (25).

Now we state the propositions:

(27) Let us consider elements x, y of $G \rtimes_\varphi A$, elements a_1, a_2 of A, and elements g_1, g_2, g_3 of G. Suppose $x = \langle g_1, a_1\rangle$ and $y = \langle g_2, a_2\rangle$ and $g_3 =$

$\varphi(a_1)(g_2)$. Then $x \cdot y = \langle g_1 \cdot g_3, a_1 \cdot a_2 \rangle$. The theorem is a consequence of (25).

(28) Let us consider elements x, y of $G \rtimes_\varphi A$, an element a of A, and an element g of G. Suppose $x = \langle g, \mathbf{1}_A \rangle$ and $y = \langle \mathbf{1}_G, a \rangle$. Then $x \cdot y = \langle g, a \rangle$. The theorem is a consequence of (20) and (27).

Let us consider G, A, and φ. One can verify that $G \rtimes_\varphi A$ is unital.

Now we state the propositions:

(29) $\mathbf{1}_{G \rtimes_\varphi A} = \langle \mathbf{1}_G, \mathbf{1}_A \rangle$. The theorem is a consequence of (23).

(30) Let us consider elements x, y of $G \rtimes_\varphi A$, an element a of A, and an element g of G. Suppose $x = \langle g, a \rangle$ and $y = \langle \varphi(a^{-1})(g^{-1}), a^{-1} \rangle$. Then

(i) $x \cdot y = \mathbf{1}_{G \rtimes_\varphi A}$, and

(ii) $y \cdot x = \mathbf{1}_{G \rtimes_\varphi A}$.

The theorem is a consequence of (22), (27), and (29).

Let G, A be groups and φ be a homomorphism from A to AutGroup(G). One can check that $G \rtimes_\varphi A$ is associative and group-like.

Now we state the propositions:

(31) Let us consider an element a of A, an element g of G, and an element x of $G \rtimes_\varphi A$. Suppose $x = \langle g, a \rangle$. Then $x^{-1} = \langle \varphi(a^{-1})(g^{-1}), a^{-1} \rangle$. The theorem is a consequence of (23) and (30).

(32) Let us consider elements g_1, g_2 of G, and elements x, y, z of $G \rtimes_\varphi A$. Suppose $x = \langle g_1, \mathbf{1}_A \rangle$ and $y = \langle g_2, \mathbf{1}_A \rangle$ and $z = \langle g_1 \cdot g_2, \mathbf{1}_A \rangle$. Then $x \cdot y = z$. The theorem is a consequence of (27) and (20).

(33) Let us consider an element g of G, and an element x of $G \rtimes_\varphi A$. Suppose $x = \langle g, \mathbf{1}_A \rangle$. Then $x^{-1} = \langle g^{-1}, \mathbf{1}_A \rangle$. The theorem is a consequence of (31) and (20).

(34) Let us consider an element x of $G \rtimes_\varphi A$, and an element g of G. Suppose $x = \langle g, \mathbf{1}_A \rangle$. Let us consider an integer i. Then $x^i = \langle g^i, \mathbf{1}_A \rangle$.

PROOF: Define $\mathcal{P}[\text{integer}] \equiv x^{\$_1} = \langle g^{\$_1}, \mathbf{1}_A \rangle$. $\mathcal{P}[0]$ by [14, (25)], (29). For every integer i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i-1]$ and $\mathcal{P}[i+1]$ by (33), (23), [14, (33), (32)]. For every integer i, $\mathcal{P}[i]$ from [13, Sch. 4]. □

(35) Let us consider elements a_1, a_2 of A, and elements x, y, z of $G \rtimes_\varphi A$. Suppose $x = \langle \mathbf{1}_G, a_1 \rangle$ and $y = \langle \mathbf{1}_G, a_2 \rangle$ and $z = \langle \mathbf{1}_G, a_1 \cdot a_2 \rangle$. Then $x \cdot y = z$. The theorem is a consequence of (27).

(36) Let us consider an element a of A, and an element x of $G \rtimes_\varphi A$. Suppose $x = \langle \mathbf{1}_G, a \rangle$. Then $x^{-1} = \langle \mathbf{1}_G, a^{-1} \rangle$. The theorem is a consequence of (31).

(37) Let us consider an integer i, an element x of $G \rtimes_\varphi A$, and an element a of A. Suppose $x = \langle \mathbf{1}_G, a \rangle$. Then $x^i = \langle \mathbf{1}_G, a^i \rangle$.

PROOF: Define $\mathcal{P}[\text{integer}] \equiv x^{\$_1} = \langle \mathbf{1}_G, a^{\$_1} \rangle$. $\mathcal{P}[0]$ by [14, (25)], (29). For every integer i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i-1]$ and $\mathcal{P}[i+1]$ by (36), (23), [14, (33), (32)]. For every integer i, $\mathcal{P}[i]$ from [13, Sch. 4]. □

Let us consider G, A, and φ. The functor incl1(G, A, φ) yielding a function from G into $G \rtimes_\varphi A$ is defined by

(Def. 2) for every element g of G, $it(g) = \langle g, \mathbf{1}_A \rangle$.

Aschbacher [1], THEOREM (10.1.2):

Let us consider G, A, and φ. One can check that incl1(G, A, φ) is multiplicative and one-to-one.

The functor incl2(G, A, φ) yielding a function from A into $G \rtimes_\varphi A$ is defined by

(Def. 3) for every element a of A, $it(a) = \langle \mathbf{1}_G, a \rangle$.

Aschbacher [1], THEOREM (10.1.2):

Let us consider G, A, and φ. Observe that incl2(G, A, φ) is multiplicative and one-to-one.

Now we state the proposition:

(38) ASCHBACHER [1], THEOREM (10.1.3):
Im incl1(G, A, φ) is a normal subgroup of $G \rtimes_\varphi A$.
PROOF: For every elements x, g of $G \rtimes_\varphi A$ such that g is an element of Im incl1(G, A, φ) holds $g^x \in$ Im incl1(G, A, φ) by [18, (45)], (26), (31), (27). □

Let us consider A, G, and φ. Observe that Im incl1(G, A, φ) is normal.

Now we state the propositions:

(39) Im incl2$(G, A, \varphi) \cap$ Im incl1$(G, A, \varphi) = \{\mathbf{1}\}_{G \rtimes_\varphi A}$.
PROOF: Set $I_1 =$ Im incl2(G, A, φ). Set $I_2 =$ Im incl1(G, A, φ). Set $S = G \rtimes_\varphi A$. For every object x such that $x \in$ the carrier of $I_1 \cap I_2$ holds $x \in \{\mathbf{1}_S\}$ by [15, (82)], [18, (45)], [5, (77)], (29). □

(40) Let us consider an element x of $G \rtimes_\varphi A$. Then there exists an element g of G and there exists an element a of A such that $(\text{incl1}(G, A, \varphi))(g) \cdot (\text{incl2}(G, A, \varphi))(a) = x$. The theorem is a consequence of (26), (27), and (20).

(41) (Im incl1$(G, A, \varphi)) \cdot$ (Im incl2$(G, A, \varphi)) =$ the carrier of $G \rtimes_\varphi A$.
PROOF: For every element x of $G \rtimes_\varphi A$, $x \in$ (Im incl1$(G, A, \varphi)) \cdot$ (Im incl2$(G, A, \varphi))$ by (40), [18, (45)], [17, (4)]. □

(42) Im incl1$(G, A, \varphi) \sqcup$ Im incl2$(G, A, \varphi) = G \rtimes_\varphi A$. The theorem is a consequence of (41).

Now we state the proposition:

(43) ASCHBACHER [1], THEOREM (10.1.3):
G and $\operatorname{Im}\operatorname{incl1}(G, A, \varphi)$ are isomorphic.

Let us consider an element a of A and an element g of G. Now we state the propositions:

(44) ASCHBACHER [1], THEOREM (10.1.4):
$(\operatorname{incl1}(G, A, \varphi))(g)^{(\operatorname{incl2}(G,A,\varphi))(a)} = \langle \varphi(a^{-1})(g), \mathbf{1}_A \rangle$. The theorem is a consequence of (31) and (27).

(45) $(\operatorname{incl1}(G, A, \varphi))(g)^{(\operatorname{incl2}(G,A,\varphi))(a^{-1})} = \langle \varphi(a)(g), \mathbf{1}_A \rangle$. The theorem is a consequence of (44).

Now we state the proposition:

(46) $G \rtimes_{(A \to \{\mathbf{1}\}_{\operatorname{AutGroup}(G)})} A = \prod \langle G, A \rangle$.
PROOF: Set $S = G \rtimes_{(A \to \{\mathbf{1}\}_{\operatorname{AutGroup}(G)})} A$. The carrier of $S =$ the carrier of $\prod \langle G, A \rangle$. Set $B_1 =$ the multiplication of S. Set $B_2 =$ the multiplication of $\prod \langle G, A \rangle$. Set $U = \prod$(the support of $\langle G, A \rangle$). B_1 is a binary operation on U and B_2 is a binary operation on U. For every elements x, y of $\prod$(the support of $\langle G, A \rangle$), $B_1(x, y) = B_2(x, y)$ by (26), [10, (9)], (27), [11, (29)]. □

4. COMPLEMENTARY SUBGROUPS

Let G, H, N be groups. We say that H, N are complements in G if and only if

(Def. 4) there exists a strict subgroup H_1 of G and there exists a strict, normal subgroup N_1 of G such that $H_1 =$ the multiplicative magma of H and $N_1 =$ the multiplicative magma of N and $H_1 \cdot N_1 =$ the carrier of G and $H_1 \cap N_1 = \{\mathbf{1}\}_G$.

Let G be a group and H, N be subgroups of G. Observe that H, N are complements in G if and only if the condition (Def. 5) is satisfied.

(Def. 5) N is normal and $H \cdot N =$ the carrier of G and $H \cap N = \{\mathbf{1}\}_G$.

Let us consider a group G, subgroups H, K of G, and a subgroup N of G. Now we state the propositions:

(47) Suppose H is a subgroup of K. Then suppose N is a normal subgroup of K. Then H, N are complements in K if and only if $N \cdot H =$ the carrier of K and $H \cap N = \{\mathbf{1}\}_K$. The theorem is a consequence of (3), (4), (7), and (6).

(48) Suppose H is a subgroup of K. Then suppose N is a normal subgroup of K. Then H, N are complements in K if and only if $H \cdot N =$ the carrier of K and $H \cap N = \{\mathbf{1}\}_K$. The theorem is a consequence of (14) and (47).

Let us consider a group G, subgroups H, K of G, and a normal subgroup N of G. Now we state the propositions:

(49) Suppose H is a subgroup of K. Then suppose N is a subgroup of K. Then H, $(N)_K$ are complements in K if and only if $N \cdot H =$ the carrier of K and $H \cap N = \{\mathbf{1}\}_K$. The theorem is a consequence of (3), (15), and (47).

(50) If H is a subgroup of K, then if N is a subgroup of K, then H, N are complements in K iff H, $(N)_K$ are complements in K. The theorem is a consequence of (47) and (49).

Now we state the propositions:

(51) Let us consider a group G, a subgroup K of G, a subgroup H of K, and a normal subgroup N of G. Suppose N is a subgroup of K. Then H, N are complements in K if and only if H, $(N)_K$ are complements in K.

(52) Let us consider a group G, a subgroup H of G, and a normal subgroup N of G. Then H, N are complements in G if and only if $H \sqcup N =$ the multiplicative magma of G and $H \cap N = \{\mathbf{1}\}_G$.
PROOF: If H, N are complements in G, then $H \sqcup N =$ the multiplicative magma of G and $H \cap N = \{\mathbf{1}\}_G$ by [16, (50)], (8). □

Now we state the propositions:

(53) UNIVERSAL PROPERTY OF QUOTIENT GROUPS:
Let us consider groups G_1, G_2, a normal subgroup N of G_1, and a homomorphism f from G_1 to G_2. Suppose N is a subgroup of $\operatorname{Ker} f$. Then there exists a homomorphism $\overline{f}$ from ${}^{G_1}/_N$ to G_2 such that $f = \overline{f} \cdot$(the canonical homomorphism onto cosets of N).
PROOF: Define $\mathcal{P}$[element of ${}^{G_1}/_N$, element of G_2] $\equiv$ there exists an element g of G_1 such that $\$_1 = g \cdot N$ and $\$_2 = f(g)$. For every element x of ${}^{G_1}/_N$, there exists an element y of G_2 such that $\mathcal{P}[x, y]$ by [18, (23)]. Consider $\overline{f}$ being a function from ${}^{G_1}/_N$ into G_2 such that for every element x of ${}^{G_1}/_N$, $\mathcal{P}[x, \overline{f}(x)]$ from [9, Sch. 3]. For every elements x_1, x_2 of ${}^{G_1}/_N$, $\overline{f}(x_1 \cdot x_2) = \overline{f}(x_1) \cdot \overline{f}(x_2)$ by (10), [15, (40)], [18, (41)]. For every element g of G_1, $f(g) = (\overline{f} \cdot (\text{the canonical homomorphism onto cosets of } N))(g)$ by (10), [15, (40)], [18, (41)], [9, (15)]. □

(54) Let us consider groups G_1, G_2, a normal subgroup N_1 of G_1, a normal subgroup N_2 of G_2, and a homomorphism φ from G_1 to G_2. Suppose φ is bijective and φ°(the carrier of N_1) = the carrier of N_2. Then ${}^{G_1}/_{N_1}$ and ${}^{G_2}/_{N_2}$ are isomorphic.
PROOF: For every element g of G_1 such that $g \in N_1$ holds $g \in \operatorname{Ker}$(the canonical homomorphism onto cosets of N_2) $\cdot \varphi$ by [9, (35)], [18, (24)], [15, (113)], [9, (15)]. Consider $\overline{\varphi}$ being a homomorphism from ${}^{G_1}/_{N_1}$ to ${}^{G_2}/_{N_2}$ such that

(the canonical homomorphism onto cosets of N_2) $\cdot\, \varphi = \overline{\varphi} \cdot$ (the canonical homomorphism onto cosets of N_1). For every element y of ${}^{G_2}/_{N_2}$, there exists an element x of ${}^{G_1}/_{N_1}$ such that $\overline{\varphi}(x) = y$ by [18, (21), (62)], [9, (5)], [8, (13)]. For every elements a, b of ${}^{G_1}/_{N_1}$ such that $\overline{\varphi}(a) = \overline{\varphi}(b)$ holds $a = b$ by [18, (21)], [9, (15)], (10), [9, (64)]. □

Let us consider a group G, a subgroup H of G, and a normal subgroup N of G. Now we state the propositions:

(55) Suppose H, N are complements in G. Then there exists a homomorphism φ from H to ${}^{G}/_{N}$ such that

(i) for every element h of H and for every element g of G such that $g = h$ holds $\varphi(h) = g \cdot N$, and

(ii) φ is bijective.

PROOF: Define $\mathcal{P}$[element of H, element of ${}^{G}/_{N}$] ≡ there exists an element g of G such that $g = \$_1$ and $\$_2 = g \cdot N$. For every element x of H, there exists an element y of ${}^{G}/_{N}$ such that $\mathcal{P}[x, y]$ by [15, (42)]. Consider φ being a function from H into ${}^{G}/_{N}$ such that for every element x of H, $\mathcal{P}[x, \varphi(x)]$ from [9, Sch. 3]. For every element h of H and for every element g of G such that $g = h$ holds $\varphi(h) = g \cdot N$. For every elements a, b of H, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ by [15, (42), (43)]. For every element y of ${}^{G}/_{N}$, there exists an element x of H such that $\varphi(x) = y$ by [18, (23)], [17, (4)], [15, (105), (113)]. For every elements a, b of H such that $\varphi(a) = \varphi(b)$ holds $a = b$ by [15, (42), (114), (51)]. □

(56) If H, N are complements in G, then ${}^{G}/_{N}$ and H are isomorphic. The theorem is a consequence of (55).

Now we state the proposition:

(57) Let us consider a group G, subgroups H_1, H_2 of G, and a normal subgroup N of G. Suppose H_1, N are complements in G and H_2, N are complements in G. Then H_1 and H_2 are isomorphic. The theorem is a consequence of (56).

Now we state the propositions:

(58) BOURBAKI [6, I §6.1], COROLLARY TO PROPOSITION 4:
Let us consider a group G, subgroups H, K of G, and a function φ from $\prod\langle H, K\rangle$ into G. Suppose for every elements h, k of G such that $h \in H$ and $k \in K$ holds $\varphi(\langle h, k\rangle) = h \cdot k$. Then φ is one-to-one if and only if $H \cap K = \{\mathbf{1}\}_G$.
PROOF: If φ is one-to-one, then $H \cap K = \{\mathbf{1}\}_G$ by (19), [18, (1)], [15, (65)], (17). If $H \cap K = \{\mathbf{1}\}_G$, then φ is one-to-one by (18), [15, (41)], [5, (2), (44)]. □

(59) Let us consider a group G, and subgroups H, K of G. Then there exists a function φ from $\prod$(the support of $\langle H, K\rangle$) into G such that

(i) for every elements h, k of G such that $h \in H$ and $k \in K$ holds $\varphi(\langle h, k\rangle) = h \cdot k$, and

(ii) φ is one-to-one iff $H \cap K = \{\mathbf{1}\}_G$.

PROOF: Define $\mathcal{P}$[element of $\prod$(the support of $\langle H, K\rangle$), element of G] $\equiv$ there exist elements h, k of G such that $h \in H$ and $k \in K$ and $\$_1 = \langle h, k\rangle$ and $\$_2 = h \cdot k$. For every element x of $\prod$(the support of $\langle H, K\rangle$), there exists an element y of G such that $\mathcal{P}[x, y]$ by (18), [15, (40)], [5, (2), (44)]. Consider φ being a function from $\prod$(the support of $\langle H, K\rangle$) into G such that for every element x of $\prod$(the support of $\langle H, K\rangle$), $\mathcal{P}[x, \varphi(x)]$ from [9, Sch. 3]. For every elements h, k of G such that $h \in H$ and $k \in K$ holds $\varphi(\langle h, k\rangle) = h \cdot k$ by (19), [5, (77)]. □

(60) Let us consider a group G, a subgroup H of G, a strict, normal subgroup N of G, and a homomorphism φ from H to AutGroup(N). Then there exists a function ψ from $N \rtimes_\varphi H$ into G such that

(i) for every elements n, h of G such that $n \in N$ and $h \in H$ holds $\psi(\langle n, h\rangle) = n \cdot h$, and

(ii) ψ is one-to-one iff $N \cap H = \{\mathbf{1}\}_G$.

The theorem is a consequence of (59).

(61) Let us consider a group G, a subgroup H of G, and a normal subgroup N of G. Suppose H, N are complements in G. Then

(i) $H \cdot N =$ the carrier of G, and

(ii) $N \cdot H =$ the carrier of G.

The theorem is a consequence of (52) and (12).

Now we state the proposition:

(62) ASCHBACHER [1], THEOREM 10.2:
Let us consider a group G, a strict, normal subgroup N of G, and a subgroup H of G. Suppose H, N are complements in G. Let us consider a homomorphism α from H to AutGroup(N). Suppose for every elements h, n of G such that $h \in H$ and $n \in N$ for every homomorphism a from N to N such that $a = \alpha(h)$ holds $a(n) = n^{h^{-1}}$. Then there exists a homomorphism β from $N \rtimes_\alpha H$ to G such that

(i) for every elements g_5, g_7 of G and for every element h of H and for every element n of N such that $g_5 = h$ and $g_7 = n$ holds $\beta(\langle n, h\rangle) = g_7 \cdot g_5$, and

(ii) β is bijective.

PROOF: Set $S = N \rtimes_\alpha H$. Consider β being a function from S into G such that for every elements n, h of G such that $n \in N$ and $h \in H$ holds $\beta(\langle n, h\rangle) = n \cdot h$ and (β is one-to-one iff $N \cap H = \{\mathbf{1}\}_G$). For every elements x, y of S, $\beta(x \cdot y) = \beta(x) \cdot \beta(y)$ by (26), [15, (42)], [9, (5)], [10, (1)]. For every elements g_5, g_7 of G and for every element h of H and for every element n of N such that $g_5 = h$ and $g_7 = n$ holds $\beta(\langle n, h\rangle) = g_7 \cdot g_5$. For every element y of G, there exists an element x of S such that $\beta(x) = y$ by (61), [17, (4)], (23). □

Now we state the proposition:

(63) UNIVERSAL PROPERTY OF SEMIDIRECT PRODUCTS (BOURBAKI [7, III §2.10] PROPOSITION 27):
Let us consider groups H, G, a strict group N, a homomorphism f from N to G, a homomorphism g from H to G, and a homomorphism φ from H to AutGroup(N). Suppose for every element n of N for every element h of H, $f(\varphi(h)(n)) = g(h) \cdot f(n) \cdot g(h^{-1})$. Then there exists a homomorphism k from $N \rtimes_\varphi H$ to G such that

(i) $f = k \cdot (\mathrm{incl1}(N, H, \varphi))$, and

(ii) $g = k \cdot (\mathrm{incl2}(N, H, \varphi))$.

PROOF: Set $S = N \rtimes_\varphi H$. Define $\mathcal{P}[\text{element of } S, \text{element of } G] \equiv$ for every element n of N for every element h of H such that $\$_1 = \langle n, h\rangle$ holds $\$_2 = f(n) \cdot g(h)$. For every element x of S, there exists an element y of G such that $\mathcal{P}[x, y]$ by (26), [5, (77)]. Consider k being a function from S into G such that for every element x of S, $\mathcal{P}[x, k(x)]$ from [9, Sch. 3]. For every elements x_1, x_2 of S, $k(x_1 \cdot x_2) = k(x_1) \cdot k(x_2)$ by (26), (27), [18, (31)]. For every element n of N and for every element h of H, $k(\langle n, h\rangle) = f(n) \cdot g(h)$. For every element n of N, $f(n) = (k \cdot (\mathrm{incl1}(N, H, \varphi)))(n)$ by [9, (15)], [18, (31)]. For every element h of H, $g(h) = (k \cdot (\mathrm{incl2}(N, H, \varphi)))(h)$ by [9, (15)], [18, (31)]. □

Let G be a finite, strict group, A be a finite group, and φ be a homomorphism from A to AutGroup(G). One can verify that $G \rtimes_\varphi A$ is finite.

From now on G_1, G_2 denote groups.

Now we state the propositions:

(64) If G_2 is trivial, then for every homomorphism φ from G_1 to G_2, $\varphi = G_1 \to \{\mathbf{1}\}_{G_2}$.

(65) $\mathrm{Aut}(\{\mathbf{1}\}_G) = \{\mathrm{id}_{\{\mathbf{1}\}_G}\}$.
PROOF: For every object x such that $x \in \{\mathrm{id}_{\{\mathbf{1}\}_G}\}$ holds $x \in \mathrm{Aut}(\{\mathbf{1}\}_G)$ by [10, (3)]. For every object x such that $x \in \mathrm{Aut}(\{\mathbf{1}\}_G)$ holds $x \in \{\mathrm{id}_{\{\mathbf{1}\}_G}\}$ by [15, (44)], [18, (31)]. □

(66) If G is strict and trivial, then AutGroup(G) is trivial. The theorem is a consequence of (65).

(67) If G is strict and trivial, then $\varphi = A \to \{\mathbf{1}\}_{\mathrm{AutGroup}(G)}$. The theorem is a consequence of (66) and (64).

(68) If G_1 is trivial, then $\prod\langle G_1, G_2\rangle$ and G_2 are isomorphic.
PROOF: There exists a homomorphism f from $\prod\langle G_1, G_2\rangle$ to G_2 such that f is bijective by (18), [5, (2), (44)], [11, (29)]. □

(69) If G is strict and trivial, then $G \rtimes_\varphi A$ and A are isomorphic. The theorem is a consequence of (66), (64), (46), and (68).

(70) Let us consider finite groups G, A, and a homomorphism φ from A to AutGroup(G). Then $\overline{\overline{G \rtimes_\varphi A}} = \overline{\overline{G}} \cdot \overline{\overline{A}}$.

5. Appendix 1: Results about Cyclic Groups

One can check that every group which is infinite is also non trivial and every group which is trivial is also finite.

Let us consider a non zero natural number n. Now we state the propositions:

(71) The multiplication of $\mathbb{Z}_n^+ = +_n$.

(72) The carrier of $\mathbb{Z}_n^+ = \mathbb{Z}_n$.

Let us observe that $\mathbb{Z}_1^+$ is trivial.

Let n be a non zero natural number. One can verify that $\overline{\overline{\mathbb{Z}_n^+}}$ reduces to n.

Now we state the propositions:

(73) Let us consider a group G. Then G is trivial if and only if for every element x of G, $x = \mathbf{1}_G$.

(74) Let us consider a group G, and a subgroup H of G. Then H is trivial if and only if for every element x of G, $x \in H$ iff $x = \mathbf{1}_G$.
PROOF: If H is trivial, then for every element x of G, $x \in H$ iff $x = \mathbf{1}_G$ by [15, (44)]. For every object x, $x \in$ the carrier of H iff $x = \mathbf{1}_G$ by [15, (40)]. □

Let us consider a non zero natural number n. Now we state the propositions:

(75) $\mathbb{Z}_n^+$ is trivial if and only if $n = 1$.

(76) $\mathbb{Z}_n^+$ is not trivial if and only if $n > 1$.

Let us note that there exists a group which is non trivial, cyclic, strict, and infinite and there exists a group which is non trivial, cyclic, strict, and finite.

Now we state the propositions:

(77) Let us consider an element g of $\mathbb{Z}_2^+$. If $g = 1$, then $g \cdot g = \mathbf{1}_{\mathbb{Z}_2^+}$. The theorem is a consequence of (72) and (71).

(78) Let us consider an object x. Then $x \in \mathbb{Z}_2^+$ if and only if $x = 0$ or $x = 1$.
PROOF: If $x \in \mathbb{Z}_2^+$, then $x = 0$ or $x = 1$ by (72), [2, (50)]. □

(79) Let us consider elements x, y of $\mathbb{Z}_2^+$. Then

(i) if $x = 0$, then $x \cdot y = y$, and

(ii) if $y = 0$, then $x \cdot y = x$, and

(iii) if $x = 1$ and $y = 1$, then $x \cdot y = \mathbf{1}_{\mathbb{Z}_2^+}$.

PROOF: If $x = 0$, then $x \cdot y = y$ by [12, (14)]. If $y = 0$, then $x \cdot y = x$ by [12, (14)]. □

(80) Let us consider non zero natural numbers n, k, and an element g of $\mathbb{Z}_n^+$. If $g = k$, then $g^{-1} = n - k \bmod n$.
PROOF: k, $n - k \bmod n \in \mathbb{Z}_n$ by (72), [13, (57), (58), (3)]. Reconsider $g_2 = n - k \bmod n$ as an element of $\mathbb{Z}_n^+$. $n - k \in \mathbb{N}$ by [4, (44)], [13, (3)]. $g \cdot g_2 = +_n(k, n - k \bmod n)$. □

(81) Let us consider a non zero natural number n, and an element x of $\mathbb{Z}_n^+$. Then $x^{-1} = x^{n-1}$. The theorem is a consequence of (73).

(82) Let us consider a finite group G, and an element x of G. Then $0 < \operatorname{ord}(x) \leqslant \overline{\overline{G}}$.

Let us consider a non zero natural number n and elements g, g_1 of $\mathbb{Z}_n^+$. Now we state the propositions:

(83) If $g_1 = 1$, then there exists a natural number k such that $g = {g_1}^k$ and $g = k \bmod n$. The theorem is a consequence of (72) and (71).

(84) If $g_1 = 1$, then there exists a natural number k such that $k < n$ and $g = {g_1}^k$ and $g = k \bmod n$. The theorem is a consequence of (83).

Now we state the propositions:

(85) Let us consider a group G, an element g of G, and integers i, j. If $g^i = g^j$, then $g^{-i} = g^{-j}$.

(86) Let us consider a non zero natural number n, and an element g_1 of $\mathbb{Z}_n^+$. If $g_1 = 1$, then for every natural number i, ${g_1}^i = i \bmod n$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv {g_1}^{\$_1} = \$_1 \bmod n$. $\mathcal{P}[0]$ by [14, (25)], [12, (14)]. For every natural number i such that $\mathcal{P}[i]$ holds $\mathcal{P}[i + 1]$ by [4, (44), (53)], [12, (14)], [14, (34)]. For every natural number i, $\mathcal{P}[i]$ from [4, Sch. 2]. □

(87) Let us consider a non zero natural number n, and an element g_1 of $\mathbb{Z}_n^+$. Suppose $g_1 = 1$. Let us consider natural numbers i, j. Then ${g_1}^i = {g_1}^j$ if and only if $i \bmod n = j \bmod n$. The theorem is a consequence of (86).

6. Appendix 2: Dihedral Groups

Now we state the proposition:

(88) If A is commutative, then $\cdot_A^{-1}$ is an automorphism of A.

Let G be a strict, commutative group. The functor inversions G yielding a function from $\mathbb{Z}_2^+$ into AutGroup(G) is defined by

(Def. 6) $it(0) = \mathrm{id}_G$ and $it(1) = \cdot_G^{-1}$.

Now we state the proposition:

(89) Let us consider a group G. Then $\cdot_G^{-1} \cdot \cdot_G^{-1} = \mathrm{id}_G$.

Proof: For every element x of the carrier of G, $(\cdot_G^{-1} \cdot \cdot_G^{-1})(x) = (\mathrm{id}_G)(x)$ by [9, (15)]. □

Let us consider a strict, commutative group G and elements a, b of $\mathbb{Z}_2^+$. Now we state the propositions:

(90) Suppose $b = 0$. Then

(i) $(\text{inversions } G)(b) \cdot (\text{inversions } G)(a) = (\text{inversions } G)(a)$, and

(ii) $(\text{inversions } G)(a) \cdot (\text{inversions } G)(b) = (\text{inversions } G)(a)$.

The theorem is a consequence of (78).

(91) If $a = 1$ and $b = 1$, then $(\text{inversions } G)(b) \cdot (\text{inversions } G)(a) = (\text{inversions } G)(a \cdot b)$. The theorem is a consequence of (79) and (89).

Let G be a strict, commutative group. Observe that inversions G is multiplicative.

One can check that the functor inversions G yields a homomorphism from $\mathbb{Z}_2^+$ to AutGroup(G). Let n be a non zero extended natural. The functor Dihedral-group(n) yielding a strict group is defined by

(Def. 7) if $n = +\infty$, then $it = (\mathbb{Z}^+) \rtimes_{(\text{inversions}(\mathbb{Z}^+))} (\mathbb{Z}_2^+)$ and if $n \neq +\infty$, then there exists a non zero natural number n_1 such that $n = n_1$ and $it = (\mathbb{Z}_{n_1}^+) \rtimes_{(\text{inversions}(\mathbb{Z}_{n_1}^+))} (\mathbb{Z}_2^+)$.

Let n be a non zero natural number. Note that the functor Dihedral-group(n) is defined by the term

(Def. 8) $(\mathbb{Z}_n^+) \rtimes_{(\text{inversions}(\mathbb{Z}_n^+))} (\mathbb{Z}_2^+)$.

Now we state the proposition:

(92) Let us consider a non zero natural number n. Then $\overline{\overline{\text{Dihedral-group}(n)}} = 2 \cdot n$. The theorem is a consequence of (70).

Let n be a non zero natural number. One can verify that Dihedral-group(n) is finite.

Let n be a non natural extended natural. One can check that the functor Dihedral-group(n) is defined by the term

(Def. 9) $(\mathbb{Z}^+) \rtimes_{(\text{inversions}(\mathbb{Z}^+))} (\mathbb{Z}_2^+)$.

Now we state the proposition:

(93) Let us consider an element g_1 of $\mathbb{Z}^+$, and an element a_2 of $\mathbb{Z}_2^+$. Suppose $a_2 = 1$. Let us consider elements x, y of Dihedral-group($+\infty$). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}^+}, a_2 \rangle$. Then $y \cdot x = x^{-1} \cdot y$. The theorem is a consequence of (33) and (27).

Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, an element a_2 of $\mathbb{Z}_2^+$, and elements x, y of Dihedral-group(n). Now we state the propositions:

(94) Suppose $a_2 = 1$. Then if $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2 \rangle$, then $y \cdot x = x^{-1} \cdot y$. The theorem is a consequence of (33) and (27).

(95) Suppose $a_2 = 1$. Then if $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2 \rangle$, then $y \cdot x = x^{n-1} \cdot y$. The theorem is a consequence of (33), (81), (34), and (94).

Now we state the propositions:

(96) Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, and an element x of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. Then $x^n = \mathbf{1}_{\text{Dihedral-group}(n)}$. The theorem is a consequence of (34) and (29).

(97) Let us consider a non zero natural number n, and an element g_1 of $\mathbb{Z}_n^+$. Suppose $g_1 = 1$. Let us consider an element x of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. Let us consider a natural number k. If $k \neq 0$ and $k < n$, then $x^k \neq \mathbf{1}_{\text{Dihedral-group}(n)}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ there exists an element g of $\mathbb{Z}_n^+$ such that $g = \$_1 \bmod n$ and $g = {g_1}^{\$_1}$. $\mathcal{P}[0]$ by [12, (14)], [14, (25)]. For every natural number j such that $\mathcal{P}[j]$ holds $\mathcal{P}[j+1]$ by [12, (14)], [14, (35)], [12, (9)], [4, (53), (44)]. For every natural number j, $\mathcal{P}[j]$ from [4, Sch. 2]. Consider g_6 being an element of $\mathbb{Z}_n^+$ such that $g_6 = k \bmod n$ and $g_6 = {g_1}^k$. $x^k = \langle {g_1}^k, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. □

(98) Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, and an element x of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. Then $x^{-1} = x^{n-1}$. The theorem is a consequence of (96).

(99) Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, and an element x of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. Let us consider a natural number j. Then $x^{j-1} = x^{n-j}$.

PROOF: ${g_1}^{j-1} = {g_1}^{n-j}$ by [14, (33)], [12, (9)], [14, (5)]. $x^j = \langle {g_1}^j, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. □

(100) Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, and an element a_2 of $\mathbb{Z}_2^+$. Suppose $a_2 = 1$. Let us consider elements x, y of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2 \rangle$. Then $y \cdot x = x^{-1} \cdot y$. The theorem is a consequence of (98) and (95).

(101) Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, and an element a_2 of $\mathbb{Z}_2^+$. Suppose $a_2 = 1$. Let us consider elements x, y of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+}\rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2\rangle$. Let us consider a natural number i. Then $y \cdot x^i = x^{n-i} \cdot y$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv y \cdot x^{\$_1} = x^{n-\$_1} \cdot y$. $\mathcal{P}[0]$ by [14, (25)], (96). For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [14, (34)], (100), [14, (33)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, an element a_2 of $\mathbb{Z}_2^+$, elements x, y of Dihedral-group(n), and an element z of Dihedral-group(n). Now we state the propositions:

(102) Suppose $g_1 = 1$. Then suppose $a_2 = 1$. Then suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+}\rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2\rangle$. Then there exists a natural number k such that $z = x^k \cdot y$ or $z = x^k$. The theorem is a consequence of (26), (83), (34), (78), and (28).

(103) Suppose $g_1 = 1$. Then suppose $a_2 = 1$. Then suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+}\rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2\rangle$. Then there exists a natural number k such that

(i) $k < n$, and

(ii) $z = x^k \cdot y$ or $z = x^k$.

The theorem is a consequence of (102), (87), and (34).

Now we state the propositions:

(104) Let us consider a non zero natural number n, an element g_1 of $\mathbb{Z}_n^+$, and an element a_2 of $\mathbb{Z}_2^+$. Suppose $a_2 = 1$. Let us consider elements x, y of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+}\rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2\rangle$. Let us consider natural numbers i, j. Then $x^i \cdot y \cdot x^j = x^{n+i-j} \cdot y$. The theorem is a consequence of (101).

(105) Let us consider a non zero natural number n, an element a_2 of $\mathbb{Z}_2^+$, and an element y of Dihedral-group(n). Suppose $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2\rangle$. Then $y \cdot y = \mathbf{1}_{\text{Dihedral-group}(n)}$. The theorem is a consequence of (37) and (29).

(106) (i) Dihedral-group(1) and $\mathbb{Z}_2^+$ are isomorphic, and

(ii) Dihedral-group(1) is commutative.

The theorem is a consequence of (69).

(107) Dihedral-group(2) is commutative.

PROOF: $1 \in \mathbb{Z}_2^+$. Reconsider $g_1 = 1$, $a_2 = 1$ as an element of $\mathbb{Z}_2^+$. Reconsider $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+}\rangle$, $y = \langle \mathbf{1}_{\mathbb{Z}_2^+}, a_2\rangle$ as an element of Dihedral-group(2). For every natural number k such that $k < 2$ holds $x^k \cdot y = y \cdot x^k$ by [4, (23)], [14, (25)], (101). For every natural numbers k_1, k_2, $x^{k_1} \cdot x^{k_2} = x^{k_2} \cdot x^{k_1}$ by [14, (33)]. For every elements z_1, z_2 of Dihedral-group(2), $z_1 \cdot z_2 = z_2 \cdot z_1$. □

(108) Let us consider a non zero natural number n. If $n > 2$, then Dihedral-group(n) is not commutative.

PROOF: $1 \in$ the carrier of $\mathbb{Z}_n^+$. Reconsider $g_1 = 1$ as an element of $\mathbb{Z}_n^+$. $1 \in \mathbb{Z}_2^+$. Reconsider $a_2 = 1$ as an element of $\mathbb{Z}_2^+$. Reconsider $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$, $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2 \rangle$ as an element of Dihedral-group(n). $y \cdot x \neq x \cdot y$ by [14, (34)], (96), (97), [14, (27), (6)]. □

(109) Let us consider a non zero natural number n, and an element g_1 of $\mathbb{Z}_n^+$. Suppose $g_1 = 1$. Let us consider an element a_2 of $\mathbb{Z}_2^+$. Suppose $a_2 = 1$. Let us consider elements x, y, z of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2 \rangle$. Then $z \in$ Z(Dihedral-group(n)) if and only if $y \cdot z = z \cdot y$ and for every natural number i, $x^i \cdot z = z \cdot x^i$. The theorem is a consequence of (102).

(110) Let us consider a non zero natural number n, and an element z of Dihedral-group(n). Then $z \in$ Z(Dihedral-group(n)) if and only if for every element g_1 of $\mathbb{Z}_n^+$ such that $g_1 = 1$ for every element a_2 of $\mathbb{Z}_2^+$ such that $a_2 = 1$ for every elements x, y of Dihedral-group(n) such that $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$ and $y = \langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2 \rangle$ holds $y \cdot z = z \cdot y$ and for every natural number i, $x^i \cdot z = z \cdot x^i$.

PROOF: For every element g of Dihedral-group(n), $z \cdot g = g \cdot z$ by [4, (53)], (106), [4, (44)], (72). □

(111) Z(Dihedral-group(1)) = Dihedral-group(1).

(112) Let us consider an odd, non zero natural number n, and an element g_1 of $\mathbb{Z}_n^+$. Suppose $g_1 = 1$. Let us consider an element x of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. Let us consider a natural number i. If $i < n$, then $i = 0$ or $x^i \neq x^{n-i}$.

PROOF: For every natural number j, ${g_1}^j = j \bmod n$. ${g_1}^i \neq {g_1}^{n-i}$ by [13, (3)]. $x^i \neq \langle {g_1}^{n-i}, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. □

(113) Let us consider an odd natural number n. If $n > 1$, then Z(Dihedral-group(n)) is trivial.

PROOF: For every element z of Dihedral-group(n), $z = \mathbf{1}_{\text{Dihedral-group}(n)}$ iff $z \in$ Z(Dihedral-group(n)) by [15, (46)], [4, (44)], (72), (78). □

Let us consider an even, non zero natural number n, a natural number k, an element g_1 of $\mathbb{Z}_n^+$, and an element x of Dihedral-group(n). Now we state the propositions:

(114) If $n = 2 \cdot k$, then if $g_1 = 1$, then if $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$, then $(x^k)^2 = \mathbf{1}_{\text{Dihedral-group}(n)}$. The theorem is a consequence of (86), (34), and (29).

(115) If $n = 2 \cdot k$, then if $g_1 = 1$, then if $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$, then $x^k \in$ Z(Dihedral-group(n)).

PROOF: $1 \in \mathbb{Z}_2^+$. Reconsider $a_2 = 1$ as an element of $\mathbb{Z}_2^+$. Reconsider $y =$

$\langle \mathbf{1}_{\mathbb{Z}_n^+}, a_2 \rangle$ as an element of Dihedral-group(n). Set $z = x^k$. $y \cdot z = x^{n-k} \cdot y$. For every natural number i, $x^i \cdot z = z \cdot x^i$ by [14, (33)]. □

Now we state the propositions:

(116) Let us consider an even, non zero natural number n, and a natural number k. Suppose $n = 2 \cdot k$ and $n > 2$. Let us consider an element g_1 of $\mathbb{Z}_n^+$. Suppose $g_1 = 1$. Let us consider an element x of Dihedral-group(n). Suppose $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$. Let us consider an element g of Dihedral-group(n). Then $g \in$ Z(Dihedral-group(n)) if and only if $g = \mathbf{1}_{\text{Dihedral-group}(n)}$ or $g = x^k$.

PROOF: $1 \in \mathbb{Z}_2^+$. If $g \in$ Z(Dihedral-group(n)), then $g = \mathbf{1}_{\text{Dihedral-group}(n)}$ or $g = x^k$ by (103), [14, (26)], (104), [14, (33), (34)]. □

(117) Let us consider an even, non zero natural number n. Suppose $n > 2$. Then $\mathbb{Z}_2^+$ and Z(Dihedral-group(n)) are isomorphic.

PROOF: Consider k being a natural number such that $n = 2 \cdot k$. $1 \in \mathbb{Z}_n^+$. Reconsider $g_1 = 1$ as an element of $\mathbb{Z}_n^+$. Reconsider $x = \langle g_1, \mathbf{1}_{\mathbb{Z}_2^+} \rangle$ as an element of Dihedral-group(n). For every object z, $z \in$ the carrier of Z(Dihedral-group(n)) iff $z \in \{\mathbf{1}_{\text{Dihedral-group}(n)}, x^k\}$ by [15, (40)], (116). $\overline{\overline{\text{Z(Dihedral-group}(n))}} = 2$ by (97), [3, (57)]. □

ACKNOWLEDGEMENT: The author would like to dedicate this to his grandparents. "There are only two precious things on earth: the first is love; the second, a long way behind it, is intelligence."

REFERENCES

[1] Michael Aschbacher. *Finite Group Theory*, volume 10. Cambridge University Press, 2000.
[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[3] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.
[4] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[6] Nicolas Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3*. Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.
[7] Nicolas Bourbaki. *General Topology: Chapters 1–4*. Springer Science and Business Media, 2013.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[10] Artur Korniłowicz. On the group of inner automorphisms. *Formalized Mathematics*, 5 (**1**):43–45, 1996.
[11] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, 7(**1**):127–134, 1998.

[12] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[13] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[14] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[15] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**): 855–864, 1990.
[16] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[17] Wojciech A. Trybulec. Commutator and center of a group. *Formalized Mathematics*, 2 (**4**):461–466, 1991.
[18] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

Accepted May 27, 2025