Isomorphisms of Direct Products of Finite Commutative Groups[1]

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. We have been working on the formalization of groups. In [1], we encoded some theorems concerning the product of cyclic groups. In this article, we present the generalized formalization of [1]. First, we show that every finite commutative group which order is composite number is isomorphic to a direct product of finite commutative groups which orders are relatively prime. Next, we describe finite direct products of finite commutative groups.

MML identifier: `GROUP_17`, version: `8.1.01 5.9.1172`

The notation and terminology used in this paper have been introduced in the following articles: [2], [3], [19], [7], [13], [20], [8], [9], [10], [23], [24], [25], [26], [27], [14], [22], [17], [4], [5], [15], [16], [6], [11], [21], [18], [29], [28], and [12].

1. Preliminaries

Now we state the propositions:

(1) Let us consider sets A, B, A_1, B_1. Suppose

   (i) A misses B, and

   (ii) $A_1 \subseteq A$, and

   (iii) $B_1 \subseteq B$, and

   (iv) $A_1 \cup B_1 = A \cup B$.

   Then

(v) $A_1 = A$, and

(vi) $B_1 = B$.

PROOF: $A \subseteq A_1$. $B \subseteq B_1$. $\square$

(2) Let us consider non empty finite sets H, K. Then $\overline{\overline{\prod \langle H, K \rangle}} = \overline{\overline{H}} \cdot \overline{\overline{K}}$.

Let us consider bags p_2, p_1, f of Prime and a natural number q. Now we state the propositions:

(3) If support p_2 misses support p_1 and $f = p_2 + p_1$ and $q \in$ support p_2, then $p_2(q) = f(q)$.

(4) If support p_2 misses support p_1 and $f = p_2 + p_1$ and $q \in$ support p_1, then $p_1(q) = f(q)$.

Now we state the propositions:

(5) Let us consider a non zero natural number h and a prime number q. If q and h are not relatively prime, then $q \mid h$.

(6) Let us consider non zero natural numbers h, s. Suppose a prime number q. Suppose $q \in$ support PrimeFactorization(s). Then q and h are not relatively prime. Then support PrimeFactorization$(s) \subseteq$ support PrimeFactorization(h). The theorem is a consequence of (5).

(7) Let us consider non zero natural numbers h, k, s, t. Suppose

(i) h and k are relatively prime, and

(ii) $s \cdot t = h \cdot k$, and

(iii) for every prime number q such that $q \in$ support PrimeFactorization(s) holds q and h are not relatively prime, and

(iv) for every prime number q such that $q \in$ support PrimeFactorization(t) holds q and k are not relatively prime.

Then

(v) $s = h$, and

(vi) $t = k$.

The theorem is a consequence of (6), (1), (3), and (4). PROOF: Set $p_2 =$ PrimeFactorization(s). Set $p_1 =$ PrimeFactorization(t). For every natural number p such that $p \in$ support PFExp(h) holds $p_2(p) = p^{p\text{-count}(h)}$. For every natural number p such that $p \in$ support PFExp(k) holds $p_1(p) = p^{p\text{-count}(k)}$. $\square$

Let G be a non empty multiplicative magma, I be a finite set, and b be a (the carrier of G)-valued total I-defined function. The functor $\prod b$ yielding an element of G is defined by

(Def. 1) There exists a finite sequence f of elements of G such that

(i) $it = \prod f$, and

(ii) $f = b \cdot \text{CFS}(I)$.

Now we state the propositions:

(8) Let us consider a commutative group G, non empty finite sets A, B, a (the carrier of G)-valued total A-defined function F_3, a (the carrier of G)-valued total B-defined function F_2, and a (the carrier of G)-valued total $A \cup B$-defined function F_1. Suppose

    (i) A misses B, and

    (ii) $F_1 = F_3 + \cdot F_2$.

    Then $\prod F_1 = \prod F_3 \cdot \prod F_2$.

(9) Let us consider a non empty multiplicative magma G, a set q, an element z of G, and a (the carrier of G)-valued total $\{q\}$-defined function f. If $f = q \longmapsto z$, then $\prod f = z$.

2. Direct Product of Finite Commutative Groups

Now we state the propositions:

(10) Let us consider non empty multiplicative magmas X, Y. Then the carrier of $\prod\langle X, Y \rangle = \prod\langle$the carrier of X, the carrier of $Y \rangle$. Proof: Set $Carr X =$ the carrier of X. Set $Carr Y =$ the carrier of Y. For every element a such that $a \in \text{dom}$ the support of $\langle X, Y \rangle$ holds (the support of $\langle X, Y \rangle)(a) = \langle$the carrier of X, the carrier of $Y \rangle(a)$. $\square$

(11) Let us consider a group G and normal subgroups A, B of G. Suppose (the carrier of $A) \cap$ (the carrier of $B) = \{\mathbf{1}_G\}$. Let us consider elements a, b of G. If $a \in A$ and $b \in B$, then $a \cdot b = b \cdot a$.

(12) Let us consider a group G and normal subgroups A, B of G. Suppose

    (i) for every element x of G, there exist elements a, b of G such that $a \in A$ and $b \in B$ and $x = a \cdot b$, and

    (ii) (the carrier of $A) \cap$ (the carrier of $B) = \{\mathbf{1}_G\}$.

    Then there exists a homomorphism h from $\prod\langle A, B \rangle$ to G such that

    (iii) h is bijective, and

    (iv) for every elements a, b of G such that $a \in A$ and $b \in B$ holds $h(\langle a, b \rangle) = a \cdot b$.

    The theorem is a consequence of (11). Proof: Define $\mathcal{P}[\text{set}, \text{set}] \equiv$ there exists an element x of G and there exists an element y of G such that $x \in A$ and $y \in B$ and $\$_1 = \langle x, y \rangle$ and $\$_2 = x \cdot y$. For every element z of $\prod\langle A, B \rangle$, there exists an element w of G such that $\mathcal{P}[z, w]$. Consider h being a function from $\prod\langle A, B \rangle$ into G such that for every element z of $\prod\langle A, B \rangle$, $\mathcal{P}[z, h(z)]$. For every elements a, b of G such that $a \in A$ and $b \in B$ holds

$h(\langle a, b \rangle) = a \cdot b$. For every elements z, w of $\prod \langle A, B \rangle$, $h(z \cdot w) = h(z) \cdot h(w)$.
□

Let us consider a finite commutative group G, a natural number m, and a subset A of G. Now we state the propositions:

(13)   Suppose $A = \{x$ where x is an element of $G : x^m = \mathbf{1}_G\}$. Then

    (i) $A \neq \emptyset$, and

    (ii) for every elements g_1, g_2 of G such that g_1, $g_2 \in A$ holds $g_1 \cdot g_2 \in A$, and

    (iii) for every element g of G such that $g \in A$ holds $g^{-1} \in A$.

(14)   Suppose $A = \{x$ where x is an element of $G : x^m = \mathbf{1}_G\}$. Then there exists a strict finite subgroup H of G such that

    (i) the carrier of $H = A$, and

    (ii) H is commutative and normal.

Now we state the propositions:

(15)   Let us consider a finite commutative group G, a natural number m, and a finite subgroup H of G. Suppose the carrier of $H = \{x$ where x is an element of $G : x^m = \mathbf{1}_G\}$. Let us consider a prime number q. Suppose $q \in \text{support PrimeFactorization}(\overline{\overline{H}})$. Then q and m are not relatively prime.

(16)   Let us consider a finite commutative group G and natural numbers h, k. Suppose

    (i) $\overline{\overline{G}} = h \cdot k$, and

    (ii) h and k are relatively prime.

Then there exist strict finite subgroups H, K of G such that

    (iii) the carrier of $H = \{x$ where x is an element of $G : x^h = \mathbf{1}_G\}$, and

    (iv) the carrier of $K = \{x$ where x is an element of $G : x^k = \mathbf{1}_G\}$, and

    (v) H is normal, and

    (vi) K is normal, and

    (vii) for every element x of G, there exist elements a, b of G such that $a \in H$ and $b \in K$ and $x = a \cdot b$, and

    (viii) (the carrier of H) $\cap$ (the carrier of K) $= \{\mathbf{1}_G\}$.

The theorem is a consequence of (14). PROOF: Set $A = \{x$ where x is an element of $G : x^h = \mathbf{1}_G\}$. Set $B = \{x$ where x is an element of $G : x^k = \mathbf{1}_G\}$. $A \subseteq$ the carrier of G. $B \subseteq$ the carrier of G. Consider H being a strict finite subgroup of G such that the carrier of $H = A$ and H is commutative and H is normal. Consider K being a strict finite subgroup of G such that the carrier of $K = B$ and K is commutative and K is

normal. Consider a, b being integers such that $a \cdot h + b \cdot k = 1$. (The carrier of $H) \cap$ (the carrier of $K) \subseteq \{\mathbf{1}_G\}$. For every element x of G, there exist elements s, t of G such that $s \in H$ and $t \in K$ and $x = s \cdot t$. $\square$

(17) Let us consider finite groups H, K. Then $\overline{\overline{\prod\langle H, K\rangle}} = \overline{\overline{H}} \cdot \overline{\overline{K}}$. The theorem is a consequence of (10) and (2).

(18) Let us consider a finite commutative group G and non zero natural numbers h, k. Suppose

   (i) $\overline{\overline{G}} = h \cdot k$, and

   (ii) h and k are relatively prime.

   Then there exist strict finite subgroups H, K of G such that

   (iii) $\overline{\overline{H}} = h$, and

   (iv) $\overline{\overline{K}} = k$, and

   (v) (the carrier of $H) \cap$ (the carrier of $K) = \{\mathbf{1}_G\}$, and

   (vi) there exists a homomorphism F from $\prod\langle H, K\rangle$ to G such that F is bijective and for every elements a, b of G such that $a \in H$ and $b \in K$ holds $F(\langle a, b\rangle) = a \cdot b$.

   The theorem is a consequence of (16), (12), (17), (15), and (7).

3. Finite Direct Products of Finite Commutative Groups

   Let us consider a group G, a set q, an associative group-like multiplicative magma family F of $\{q\}$, and a function f from G into $\prod F$. Now we state the propositions:

(19) If $F = q\longmapsto G$ and for every element x of G, $f(x) = q\longmapsto x$, then f is a homomorphism from G to $\prod F$.

(20) If $F = q\dashmapsto G$ and for every element x of G, $f(x) = q\longmapsto x$, then f is bijective.

   Now we state the propositions:

(21) Let us consider a set q, an associative group-like multiplicative magma family F of $\{q\}$, and a group G. Suppose $F = q\longmapsto G$. Then there exists a homomorphism I from G to $\prod F$ such that

   (i) I is bijective, and

   (ii) for every element x of G, $I(x) = q\longmapsto x$.

   The theorem is a consequence of (19) and (20). Proof: Define $\mathcal{P}[\text{set}, \text{set}] \equiv \$_2 = q\longmapsto\$_1$. For every element z of G, there exists an element w of $\prod F$ such that $\mathcal{P}[z, w]$. Consider I being a function from G into $\prod F$ such that for every element x of G, $\mathcal{P}[x, I(x)]$. $\square$

(22)   Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, an element k of K, and a function g. Suppose

   (i) $g \in$ the carrier of $\prod F_0$, and

   (ii) $q \notin I_0$, and

   (iii) $I = I_0 \cup \{q\}$, and

   (iv) $F = F_0 + \cdot (q \longmapsto K)$.

   Then $g + \cdot (q \longmapsto k) \in$ the carrier of $\prod F$. PROOF: Set $HK = \langle H, K \rangle$. Set $w = g + \cdot (q \longmapsto k)$. For every element x such that $x \in \operatorname{dom}$ the support of F holds $w(x) \in$ (the support of $F)(x)$. □

   Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, a function G_0 from H into $\prod F_0$, and a function G from $\prod \langle H, K \rangle$ into $\prod F$. Now we state the propositions:

(23)   Suppose G_0 is a homomorphism from H to $\prod F_0$ and G_0 is bijective and $q \notin I_0$ and $I = I_0 \cup \{q\}$ and $F = F_0 + \cdot (q \longmapsto K)$. Then suppose for every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g + \cdot (q \longmapsto k)$. Then G is a homomorphism from $\prod \langle H, K \rangle$ to $\prod F$.

(24)   Suppose G_0 is a homomorphism from H to $\prod F_0$ and G_0 is bijective and $q \notin I_0$ and $I = I_0 \cup \{q\}$ and $F = F_0 + \cdot (q \longmapsto K)$. Then suppose for every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g + \cdot (q \longmapsto k)$. Then G is bijective.

   Now we state the propositions:

(25)   Let us consider a set q, a multiplicative magma family F of $\{q\}$, and a non empty multiplicative magma G. Suppose $F = q \longmapsto G$. Let us consider a (the carrier of G)-valued total $\{q\}$-defined function y. Then

   (i) $y \in$ the carrier of $\prod F$, and

   (ii) $y(q) \in$ the carrier of G, and

   (iii) $y = q \longmapsto y(q)$.

(26)   Let us consider a set q, an associative group-like multiplicative magma family F of $\{q\}$, and a group G. Suppose $F = q \longmapsto G$. Then there exists a homomorphism H_0 from $\prod F$ to G such that

   (i) H_0 is bijective, and

   (ii) for every (the carrier of G)-valued total $\{q\}$-defined function x, $H_0(x) = \prod x$.

The theorem is a consequence of (21), (25), and (9). PROOF: Consider I being a homomorphism from G to $\prod F$ such that I is bijective and for every element x of G, $I(x) = q \dashmapsto x$. Set $H_0 = I^{-1}$. For every (the carrier of G)-valued total $\{q\}$-defined function y, $H_0(y) = \prod y$. $\square$

(27)   Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, and a homomorphism G_0 from H to $\prod F_0$. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $F = F_0 + \cdot(q \longmapsto K)$, and

(iv) G_0 is bijective.

Then there exists a homomorphism G from $\prod \langle H, K \rangle$ to $\prod F$ such that

(v) G is bijective, and

(vi) for every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g + \cdot(q \longmapsto k)$.

The theorem is a consequence of (22), (23), and (24). PROOF: Set $HK = \langle H, K \rangle$. Define $\mathcal{P}[\text{set}, \text{set}] \equiv$ there exists an element h of H and there exists an element k of K and there exists a function g such that $\$_1 = \langle h, k \rangle$ and $g = G_0(h)$ and $\$_2 = g + \cdot(q \longmapsto k)$. For every element z of $\prod \langle H, K \rangle$, there exists an element w of the carrier of $\prod F$ such that $\mathcal{P}[z, w]$. Consider G being a function from $\prod \langle H, K \rangle$ into $\prod F$ such that for every element x of $\prod \langle H, K \rangle$, $\mathcal{P}[x, G(x)]$. For every element h of H and for every element k of K, there exists a function g such that $g = G_0(h)$ and $G(\langle h, k \rangle) = g + \cdot(q \longmapsto k)$. $\square$

(28)   Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, groups H, K, an element q of I, and a homomorphism G_0 from $\prod F_0$ to H. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $F = F_0 + \cdot(q \longmapsto K)$, and

(iv) G_0 is bijective.

Then there exists a homomorphism G from $\prod F$ to $\prod \langle H, K \rangle$ such that

(v) G is bijective, and

(vi) for every function x_0 and for every element k of K and for every element h of H such that $h = G_0(x_0)$ and $x_0 \in \prod F_0$ holds $G(x_0 + \cdot(q \longmapsto k)) = \langle h, k \rangle$.

The theorem is a consequence of (27). PROOF: Set $L0 = G_0{}^{-1}$. Consider L being a homomorphism from $\prod\langle H, K\rangle$ to $\prod F$ such that L is bijective and for every element h of H and for every element k of K, there exists a function g such that $g = L0(h)$ and $L(\langle h, k\rangle) = g + \cdot(q \longmapsto k)$. Set $G = L^{-1}$. For every function x_0 and for every element k of K and for every element h of H such that $h = G_0(x_0)$ and $x_0 \in \prod F_0$ holds $G(x_0 + \cdot(q \longmapsto k)) = \langle h, k\rangle$. $\square$

(29)   Let us consider a non empty finite set I, an associative group-like multiplicative magma family F of I, and a total I-defined function x. Suppose an element p of I. Then $x(p) \in F(p)$. Then $x \in$ the carrier of $\prod F$.

(30)   Let us consider non empty finite sets I_0, I, an associative group-like multiplicative magma family F_0 of I_0, an associative group-like multiplicative magma family F of I, a group K, an element q of I, and an element x of $\prod F$. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $F = F_0 + \cdot(q \longmapsto K)$.

Then there exists a total I_0-defined function x_0 and there exists an element k of K such that $x_0 \in \prod F_0$ and $x = x_0 + \cdot(q \longmapsto k)$ and for every element p of I_0, $x_0(p) \in F_0(p)$. PROOF: Reconsider $y = x$ as a total I-defined function. Reconsider $k = y(q)$ as an element of K. Reconsider $y0 = y{\upharpoonright}I_0$ as an I_0-defined function. For every element i of I_0, $y0(i) \in$ (the support of F_0)(i) and $y0(i) \in F_0(i)$. $\square$

(31)   Let us consider a group G, a subgroup H of G, a finite sequence f of elements of G, and a finite sequence g of elements of H. If $f = g$, then $\prod f = \prod g$. PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence f of elements of G for every finite sequence g of elements of H such that $\$_1 = \operatorname{len} f$ and $f = g$ holds $\prod f = \prod g$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$. $\square$

(32)   Let us consider a non empty finite set I, a group G, a subgroup H of G, a (the carrier of G)-valued total I-defined function x, and a (the carrier of H)-valued total I-defined function x_0. If $x = x_0$, then $\prod x = \prod x_0$. The theorem is a consequence of (31).

(33)   Let us consider a commutative group G, non empty finite sets I_0, I, an element q of I, a (the carrier of G)-valued total I-defined function x, a (the carrier of G)-valued total I_0-defined function x_0, and an element k of G. Suppose

(i) $q \notin I_0$, and

(ii) $I = I_0 \cup \{q\}$, and

(iii) $x = x_0 + \cdot (q \dot{\longmapsto} k)$.

Then $\prod x = \prod x_0 \cdot k$. The theorem is a consequence of (8) and (9). Proof: Reconsider $y = q \dot{\longmapsto} k$ as a (the carrier of G)-valued total $\{q\}$-defined function. I_0 misses $\{q\}$. $\square$

Let us consider a finite commutative group G. Now we state the propositions:

(34) Suppose $\overline{\overline{G}} > 1$. Then there exists a non empty finite set I and there exists an associative group-like commutative multiplicative magma family F of I and there exists a homomorphism H_0 from $\prod F$ to G such that $I = \text{support PrimeFactorization}(\overline{\overline{G}})$ and for every element p of I, $F(p)$ is a subgroup of G and $\overline{\overline{F(p)}} = (\text{PrimeFactorization}(\overline{\overline{G}}))(p)$ and for every elements p, q of I such that $p \neq q$ holds (the carrier of $F(p)$)$\cap$(the carrier of $F(q)$) = $\{\mathbf{1}_G\}$ and H_0 is bijective and for every (the carrier of G)-valued total I-defined function x such that for every element p of I, $x(p) \in F(p)$ holds $x \in \prod F$ and $H_0(x) = \prod x$.

(35) Suppose $\overline{\overline{G}} > 1$. Then there exists a non empty finite set I and there exists an associative group-like commutative multiplicative magma family F of I such that $I = \text{support PrimeFactorization}(\overline{\overline{G}})$ and for every element p of I, $F(p)$ is a subgroup of G and $\overline{\overline{F(p)}} = (\text{PrimeFactorization}(\overline{\overline{G}}))(p)$ and for every elements p, q of I such that $p \neq q$ holds (the carrier of $F(p)$)$\cap$ (the carrier of $F(q)$) = $\{\mathbf{1}_G\}$ and for every element y of G, there exists a (the carrier of G)-valued total I-defined function x such that for every element p of I, $x(p) \in F(p)$ and $y = \prod x$ and for every (the carrier of G)-valued total I-defined functions x_1, x_2 such that for every element p of I, $x_1(p) \in F(p)$ and for every element p of I, $x_2(p) \in F(p)$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$.

References

[1] Kenichi Arai, Hiroyuki Okazaki, and Yasunari Shidama. Isomorphisms of direct products of finite cyclic groups. *Formalized Mathematics*, 20(**4**):343–347, 2012. doi:10.2478/v10037-012-0038-5.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.

[4] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.

[5] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[6] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[7] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[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] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[11] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[12] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[13] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[14] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, 7(**1**):127–134, 1998.

[15] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[16] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[17] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[18] Beata Madras. Product of family of universal algebras. *Formalized Mathematics*, 4(**1**): 103–108, 1993.

[19] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.

[20] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[21] Andrzej Trybulec. Many sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.

[22] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

[24] Wojciech A. Trybulec. Subgroup and cosets of subgroups. *Formalized Mathematics*, 1(**5**): 855–864, 1990.

[25] Wojciech A. Trybulec. Classes of conjugation. Normal subgroups. *Formalized Mathematics*, 1(**5**):955–962, 1990.

[26] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.

[27] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.

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

[29] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

————