Contents

Formaliz. Math. 23 (**1**)

FORMALIZED MATHEMATICS
Vol. 23, No. 1, Pages 1–14, 2015
DOI: 10.2478/forma-2015-0001

DE GRUYTER OPEN
degruyter.com/view/j/forma

Categorical Pullbacks

Marco Riccardi
Via del Pero 102
54038 Montignoso
Italy

Summary. The main purpose of this article is to introduce the categorical concept of pullback in Mizar. In the first part of this article we redefine hom-sets, monomorphisms, epimorpshisms and isomorphisms [7] within a free-object category [1] and it is shown there that ordinal numbers can be considered as categories. Then the pullback is introduced in terms of its universal property and the Pullback Lemma is formalized [15]. In the last part of the article we formalize the pullback of functors [14] and it is also shown that it is not possible to write an equivalent definition in the context of the previous Mizar formalization of category theory [8].

MSC: 18A30 03B35

Keywords: category pullback; pullback lemma

MML identifier: CAT_7, version: 8.1.03 5.29.1227

The notation and terminology used in this paper have been introduced in the following articles: [2], [8], [17], [18], [6], [13], [9], [10], [3], [11], [20], [21], [16], [19], [4], [5], and [12].

1. Preliminaries

One can verify that every set which is ordinal is also non pair.

Let $\mathscr{C}$ be an empty category structure. Let us note that $\operatorname{Mor}\mathscr{C}$ is empty.

Let $\mathscr{C}$ be a non empty category structure. Note that $\operatorname{Mor}\mathscr{C}$ is non empty.

Let $\mathscr{C}$ be an empty category structure with identities. Let us note that $\operatorname{Ob}\mathscr{C}$ is empty.

Let $\mathscr{C}$ be a non empty category structure with identities. Observe that $\operatorname{Ob}\mathscr{C}$ is non empty.

ISSN 1426–2630(Print), 1898-9934(Online)

Let $\mathscr{C}$ be category structure with identities and a be an object of $\mathscr{C}$. One can check that id-a is identity.

Now we state the propositions:

(1) Let us consider a category structure $\mathscr{C}$, and a morphism f of $\mathscr{C}$. Suppose $\mathscr{C}$ is not empty. Then $f \in$ the carrier of $\mathscr{C}$.

(2) Let us consider category structure $\mathscr{C}$ with identities, and an object a of $\mathscr{C}$. Suppose $\mathscr{C}$ is not empty. Then $a \in$ the carrier of $\mathscr{C}$.

(3) Let us consider a composable category structure $\mathscr{C}$, and morphisms f_1, f_2, f_3 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$ and $f_2 \triangleright f_3$ and f_2 is identity. Then $f_1 \triangleright f_3$.

(4) Let us consider a composable category structure $\mathscr{C}$ with identities, and morphisms f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$. Then

(i) $\operatorname{dom}(f_1 \circ f_2) = \operatorname{dom} f_2$, and

(ii) $\operatorname{cod}(f_1 \circ f_2) = \operatorname{cod} f_1$.

(5) Let us consider a non empty, composable category structure $\mathscr{C}$ with identities, and morphisms f_1, f_2 of $\mathscr{C}$. Then $f_1 \triangleright f_2$ if and only if $\operatorname{dom} f_1 = \operatorname{cod} f_2$.

(6) Let us consider a composable category structure $\mathscr{C}$ with identities, and a morphism f of $\mathscr{C}$. If f is identity, then $\operatorname{dom} f = f$ and $\operatorname{cod} f = f$.

(7) Let us consider a composable category structure $\mathscr{C}$ with identities, and morphisms f_1, f_2 of $\mathscr{C}$. Suppose $f_1 \triangleright f_2$ and f_1 is identity and f_2 is identity. Then $f_1 = f_2$.

Let us consider a non empty, composable category structure $\mathscr{C}$ with identities and morphisms f_1, f_2 of $\mathscr{C}$. Now we state the propositions:

(8) If $\operatorname{dom} f_1 = f_2$, then $f_1 \triangleright f_2$ and $f_1 \circ f_2 = f_1$.

(9) If $f_1 = \operatorname{cod} f_2$, then $f_1 \triangleright f_2$ and $f_1 \circ f_2 = f_2$.

Now we state the propositions:

(10) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{C}_3$, $\mathscr{C}_4$, a functor $\mathcal{F}$ from $\mathscr{C}_1$ to $\mathscr{C}_2$, a functor $\mathcal{G}$ from $\mathscr{C}_2$ to $\mathscr{C}_3$, and a functor $\mathcal{H}$ from $\mathscr{C}_3$ to $\mathscr{C}_4$. Suppose $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{H}$ is covariant. Then $\mathcal{H} \circ (\mathcal{G} \circ \mathcal{F}) = (\mathcal{H} \circ \mathcal{G}) \circ \mathcal{F}$.

(11) Let us consider categories $\mathscr{C}$, $\mathscr{D}$, and a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$. Suppose $\mathcal{F}$ is covariant. Then

(i) $\mathcal{F} \circ \operatorname{id}_{\mathscr{C}} = \mathcal{F}$, and

(ii) $\operatorname{id}_{\mathscr{D}} \circ \mathcal{F} = \mathcal{F}$.

(12) Let us consider composable category structures $\mathscr{C}$, $\mathscr{D}$ with identities. Then $\mathscr{C} \cong \mathscr{D}$ if and only if there exists a functor $\mathcal{F}$ from $\mathscr{C}$ to $\mathscr{D}$ such that $\mathcal{F}$ is covariant and bijective. The theorem is a consequence of (5).

(13) Let us consider empty category structures $\mathscr{C}$, $\mathscr{D}$ with identities. Then $\mathscr{C} \cong \mathscr{D}$.

Let us consider category structures $\mathscr{C}$, $\mathscr{D}$ with identities. Now we state the propositions:

(14) Suppose $\mathscr{C} \cong \mathscr{D}$. Then

(i) $\overline{\overline{\operatorname{Mor}\mathscr{C}}} = \overline{\overline{\operatorname{Mor}\mathscr{D}}}$, and

(ii) $\overline{\overline{\operatorname{Ob}\mathscr{C}}} = \overline{\overline{\operatorname{Ob}\mathscr{D}}}$.

(15) If $\mathscr{C} \cong \mathscr{D}$ and $\mathscr{C}$ is empty, then $\mathscr{D}$ is empty. The theorem is a consequence of (14).

2. HOM-SETS

Let $\mathscr{C}$ be a category structure and a, b be objects of $\mathscr{C}$. The functor $\hom(a, b)$ yielding a subset of $\operatorname{Mor}\mathscr{C}$ is defined by the term

(Def. 1) $\{f$, where f is a morphism of $\mathscr{C}$: there exist morphisms f_1, f_2 of $\mathscr{C}$ such that $a = f_1$ and $b = f_2$ and $f \triangleright f_1$ and $f_2 \triangleright f\}$.

Let $\mathscr{C}$ be a non empty, composable category structure with identities. Observe that the functor $\hom(a, b)$ yields a subset of $\operatorname{Mor}\mathscr{C}$ and is defined by the term

(Def. 2) $\{f$, where f is a morphism of $\mathscr{C}$: $\operatorname{dom} f = a$ and $\operatorname{cod} f = b\}$.

Let $\mathscr{C}$ be a category structure. Assume $\hom(a, b) \neq \emptyset$.

A morphism from a to b is a morphism of $\mathscr{C}$ and is defined by

(Def. 3) $it \in \hom(a, b)$.

Let $\mathscr{C}$ be category structure with identities and a be an object of $\mathscr{C}$. Assume $\hom(a, a) \neq \emptyset$. Observe that the functor id-a yields a morphism from a to a. Let $\mathscr{C}$ be a non empty category structure with identities. Note that $\hom(a, a)$ is non empty.

Let $\mathscr{C}$ be a composable category structure with identities, a, b, c be objects of $\mathscr{C}$, f be a morphism from a to b, and g be a morphism from b to c. Assume $\hom(a, b) \neq \emptyset$ and $\hom(b, c) \neq \emptyset$. The functor $g \cdot f$ yielding a morphism from a to c is defined by the term

(Def. 4) $g \circ f$.

Now we state the propositions:

(16) Let us consider a category structure $\mathscr{C}$, objects a, b of $\mathscr{C}$, and a morphism f from a to b. Suppose $\hom(a, b) \neq \emptyset$. Then there exist morphisms f_1, f_2 of $\mathscr{C}$ such that

(i) $a = f_1$, and

(ii) $b = f_2$, and

(iii) $f \triangleright f_1$, and

(iv) $f_2 \triangleright f$.

(17) Let us consider a composable category structure $\mathscr{C}$ with identities, objects a, b, c of $\mathscr{C}$, a morphism f_1 from a to b, and a morphism f_2 from b to c. Suppose $\hom(a, b) \neq \emptyset$ and $\hom(b, c) \neq \emptyset$. Then $f_2 \triangleright f_1$. The theorem is a consequence of (16) and (3).

(18) Let us consider a composable category structure $\mathscr{C}$ with identities, objects a, b of $\mathscr{C}$, and a morphism f from a to b. Suppose $\hom(a, b) \neq \emptyset$. Then

(i) $f \cdot \text{id-}a = f$, and

(ii) $\text{id-}b \cdot f = f$.

The theorem is a consequence of (17).

(19) Let us consider a non empty, composable category structure $\mathscr{C}$ with identities, and a morphism f of $\mathscr{C}$. Then $f \in \hom(\operatorname{dom} f, \operatorname{cod} f)$.

(20) Let us consider a non empty, composable category structure $\mathscr{C}$ with identities, objects a, b of $\mathscr{C}$, and a morphism f of $\mathscr{C}$. Then $f \in \hom(a, b)$ if and only if $\operatorname{dom} f = a$ and $\operatorname{cod} f = b$.

(21) Let us consider a non empty, composable category structure $\mathscr{C}$ with identities, and an object a of $\mathscr{C}$. Then $a \in \hom(a, a)$. The theorem is a consequence of (6).

(22) Let us consider a composable category structure $\mathscr{C}$ with identities, and objects a, b, c of $\mathscr{C}$. Suppose $\hom(a, b) \neq \emptyset$ and $\hom(b, c) \neq \emptyset$. Then $\hom(a, c) \neq \emptyset$. The theorem is a consequence of (16) and (3).

(23) Let us consider a category $\mathscr{C}$, objects a, b, c, d of $\mathscr{C}$, a morphism f_1 from a to b, a morphism f_2 from b to c, and a morphism f_3 from c to d. Suppose $\hom(a, b) \neq \emptyset$ and $\hom(b, c) \neq \emptyset$ and $\hom(c, d) \neq \emptyset$. Then $f_3 \cdot (f_2 \cdot f_1) = (f_3 \cdot f_2) \cdot f_1$. The theorem is a consequence of (22) and (17).

(24) Let us consider a composable category structure $\mathscr{C}$ with identities, objects a, b, c of $\mathscr{C}$, a morphism f_1 from a to b, and a morphism f_2 from b to c. Suppose $\hom(a, b) \neq \emptyset$ and $\hom(b, c) \neq \emptyset$. Then

(i) if f_1 is identity, then $f_2 \cdot f_1 = f_2$, and

(ii) if f_2 is identity, then $f_2 \cdot f_1 = f_1$.

Proof: $f_2 \triangleright f_1$. If f_1 is identity, then $f_2 \cdot f_1 = f_2$ by [17, (22), (23)]. □

3. MONOMORPHISMS, EPIMORPHISMS AND ISOMORPHISMS

Let $\mathscr{C}$ be a composable category structure with identities, a, b be objects of $\mathscr{C}$, and f be a morphism from a to b. We say that f is monomorphic if and only if

(Def. 5) $\hom(a,b) \neq \emptyset$ and for every object c of $\mathscr{C}$ such that $\hom(c,a) \neq \emptyset$ for every morphisms g_1, g_2 from c to a such that $f \cdot g_1 = f \cdot g_2$ holds $g_1 = g_2$.

We say that f is epimorphic if and only if

(Def. 6) $\hom(a,b) \neq \emptyset$ and for every object c of $\mathscr{C}$ such that $\hom(b,c) \neq \emptyset$ for every morphisms g_1, g_2 from b to c such that $g_1 \cdot f = g_2 \cdot f$ holds $g_1 = g_2$.

Now we state the proposition:

(25) Let us consider a composable category structure $\mathscr{C}$ with identities, objects a, b of $\mathscr{C}$, and a morphism f_1 from a to b. Suppose $\hom(a,b) \neq \emptyset$ and f_1 is identity. Then f_1 is monomorphic. The theorem is a consequence of (24).

Let us consider a category $\mathscr{C}$, objects a, b, c of $\mathscr{C}$, a morphism f_1 from a to b, and a morphism f_2 from b to c. Now we state the propositions:

(26) If f_1 is monomorphic and f_2 is monomorphic, then $f_2 \cdot f_1$ is monomorphic. The theorem is a consequence of (22) and (23).

(27) If $f_2 \cdot f_1$ is monomorphic and $\hom(a,b) \neq \emptyset$ and $\hom(b,c) \neq \emptyset$, then f_1 is monomorphic. The theorem is a consequence of (23).

Let $\mathscr{C}$ be a composable category structure with identities, a, b be objects of $\mathscr{C}$, and f be a morphism from a to b. We say that f is a section if and only if

(Def. 7) $\hom(a,b) \neq \emptyset$ and $\hom(b,a) \neq \emptyset$ and there exists a morphism g from b to a such that $g \cdot f = \mathrm{id}\text{-}a$.

We say that f is a retraction if and only if

(Def. 8) $\hom(a,b) \neq \emptyset$ and $\hom(b,a) \neq \emptyset$ and there exists a morphism g from b to a such that $f \cdot g = \mathrm{id}\text{-}b$.

Now we state the propositions:

(28) Let us consider a category $\mathscr{C}$, objects a, b of $\mathscr{C}$, and a morphism f from a to b. If f is a section, then f is monomorphic. The theorem is a consequence of (23) and (18).

(29) Let us consider a composable category structure $\mathscr{C}$ with identities, objects a, b of $\mathscr{C}$, and a morphism f_1 from a to b. Suppose $\hom(a,b) \neq \emptyset$ and f_1 is identity. Then f_1 is epimorphic. The theorem is a consequence of (24).

Let us consider a category $\mathscr{C}$, objects a, b, c of $\mathscr{C}$, a morphism f_1 from a to b, and a morphism f_2 from b to c. Now we state the propositions:

(30) If f_1 is epimorphic and f_2 is epimorphic, then $f_2 \cdot f_1$ is epimorphic. The theorem is a consequence of (22) and (23).

(31) If $f_2 \cdot f_1$ is epimorphic and $\hom(a, b) \neq \emptyset$ and $\hom(b, c) \neq \emptyset$, then f_2 is epimorphic. The theorem is a consequence of (23).

(32) Let us consider a category $\mathscr{C}$, objects a, b of $\mathscr{C}$, and a morphism f from a to b. If f is a retraction, then f is epimorphic. The theorem is a consequence of (23) and (18).

Let $\mathscr{C}$ be a composable category structure with identities, a, b be objects of $\mathscr{C}$, and f be a morphism from a to b. We say that f is isomorphism if and only if

(Def. 9) $\hom(a, b) \neq \emptyset$ and $\hom(b, a) \neq \emptyset$ and there exists a morphism g from b to a such that $g \cdot f = \mathrm{id}\text{-}a$ and $f \cdot g = \mathrm{id}\text{-}b$.

We say that a and b are isomorphic if and only if

(Def. 10) there exists a morphism f from a to b such that f is isomorphism.

Note that a and b are isomorphic if and only if the condition (Def. 11) is satisfied.

(Def. 11) $\hom(a, b) \neq \emptyset$ and $\hom(b, a) \neq \emptyset$ and there exists a morphism f from a to b and there exists a morphism g from b to a such that $g \cdot f = \mathrm{id}\text{-}a$ and $f \cdot g = \mathrm{id}\text{-}b$.

Now we state the proposition:

(33) Let us consider a category $\mathscr{C}$, objects a, b of $\mathscr{C}$, and a morphism f from a to b. If f is isomorphism, then f is monomorphic and epimorphic. The theorem is a consequence of (28) and (32).

4. Ordinal Numbers as Categories

Let $\mathscr{C}$ be a category structure. We say that $\mathscr{C}$ is a preorder if and only if

(Def. 12) for every objects a, b of $\mathscr{C}$ and for every morphisms f_1, f_2 of $\mathscr{C}$ such that f_1, $f_2 \in \hom(a, b)$ holds $f_1 = f_2$.

Observe that every category structure which is empty is also a preorder and there exists a category structure which is strict and preorder and every composable category structure with identities which is a preorder is also associative.

Let $\mathscr{C}$ be category structure with identities. The functor $\mathrm{RelOb}\,\mathscr{C}$ yielding a binary relation on $\mathrm{Ob}\,\mathscr{C}$ is defined by the term

(Def. 13) $\{\langle a, b\rangle$, where a, b are objects of $\mathscr{C}$: there exists a morphism f of $\mathscr{C}$ such that $f \in \hom(a, b)\}$.

Let $\mathscr{C}$ be an empty category structure with identities. Let us note that $\mathrm{RelOb}\,\mathscr{C}$ is empty.

Now we state the propositions:

(34) Let us consider a composable category structure $\mathscr{C}$ with identities. Then

(i) $\operatorname{dom}\operatorname{RelOb}\mathscr{C} = \operatorname{Ob}\mathscr{C}$, and

(ii) $\operatorname{rng}\operatorname{RelOb}\mathscr{C} = \operatorname{Ob}\mathscr{C}$.

The theorem is a consequence of (6) and (19).

(35) Let us consider composable category structures $\mathscr{C}_1$, $\mathscr{C}_2$ with identities. Suppose $\mathscr{C}_1 \cong \mathscr{C}_2$. Then $\operatorname{RelOb}\mathscr{C}_1$ and $\operatorname{RelOb}\mathscr{C}_2$ are isomorphic. The theorem is a consequence of (15), (34), and (20).

Let $\mathscr{C}$ be a non empty, composable category structure with identities. One can verify that $\operatorname{RelOb}\mathscr{C}$ is non empty.

Now we state the propositions:

(36) Let us consider preorder, composable category structure $\mathscr{C}$ with identities. Suppose $\mathscr{C}$ is not empty. Then there exists a function $\mathcal{F}$ from $\mathscr{C}$ into $\operatorname{RelOb}\mathscr{C}$ such that

(i) $\mathcal{F}$ is bijective, and

(ii) for every morphism f of $\mathscr{C}$, $\mathcal{F}(f) = \langle \operatorname{dom} f, \operatorname{cod} f \rangle$.

PROOF: Reconsider $\mathscr{C}_1 = \mathscr{C}$ as a non empty, composable category structure with identities. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ for every morphism f of $\mathscr{C}_1$ such that $\$_1 = f$ holds $\$_2 = \langle \operatorname{dom} f, \operatorname{cod} f \rangle$. For every element x of the carrier of $\mathscr{C}_1$, there exists an element y of $\operatorname{RelOb}\mathscr{C}_1$ such that $\mathcal{P}[x, y]$. Consider $\mathcal{F}$ being a function from the carrier of $\mathscr{C}_1$ into $\operatorname{RelOb}\mathscr{C}_1$ such that for every element x of the carrier of $\mathscr{C}_1$, $\mathcal{P}[x, \mathcal{F}(x)]$ from [10, Sch. 3]. For every object y such that $y \in \operatorname{RelOb}\mathscr{C}$ holds $y \in \operatorname{rng}\mathcal{F}$ by (20), [9, (3)]. For every objects x_1, x_2 such that x_1, $x_2 \in \operatorname{dom}\mathcal{F}$ and $\mathcal{F}(x_1) = \mathcal{F}(x_2)$ holds $x_1 = x_2$. □

(37) Let us consider an ordinal number O. Then there exists a strict, a preorder category $\mathscr{C}$ such that

(i) $\operatorname{Ob}\mathscr{C} = O$, and

(ii) for every objects o_1, o_2 of $\mathscr{C}$ such that $o_1 \in o_2$ holds $\hom(o_1, o_2) = \{\langle o_1, o_2 \rangle\}$, and

(iii) $\operatorname{RelOb}\mathscr{C} = {}^{\subseteq}_{O}$, and

(iv) $\operatorname{Mor}\mathscr{C} = O \cup \{\langle o_1, o_2 \rangle$, where o_1, o_2 are elements of $O : o_1 \in o_2\}$.

The theorem is a consequence of (6), (20), and (21).

Let O be an ordinal number and $\mathscr{C}$ be a composable category structure with identities. We say that $\mathscr{C}$ is O-ordered if and only if

(Def. 14) $\operatorname{RelOb}\mathscr{C}$ and ${}^{\subseteq}_{O}$ are isomorphic.

Let O be a non empty, ordinal number. Let us observe that every composable category structure with identities which is O-ordered is also non empty.

Let O be an ordinal number. Note that there exists a composable category structure with identities which is strict, O-ordered, and preorder.

Let O be an empty, ordinal number. Let us observe that every composable category structure with identities which is O-ordered is also empty.

Now we state the proposition:

(38) Let us consider ordinal numbers O_1, O_2, a O_1-ordered, a preorder category $\mathscr{C}_1$, and a O_2-ordered, a preorder category $\mathscr{C}_2$. Then $O_1 = O_2$ if and only if $\mathscr{C}_1 \cong \mathscr{C}_2$.

PROOF: If $O_1 = O_2$, then $\mathscr{C}_1 \cong \mathscr{C}_2$ by (13), [4, (39), (41)], (36). If $\mathscr{C}_1 \cong \mathscr{C}_2$, then $O_1 = O_2$ by (35), [4, (42), (40)], [5, (10)]. □

Let O be an ordinal number. The functor $\mathbf{O}$ yielding a strict, O-ordered, a preorder category is defined by the term

(Def. 15) the strict, O-ordered, a preorder category.

Now we state the proposition:

(39) There exists a morphism f of $\mathbf{2}$ such that

(i) f is not identity, and

(ii) $\operatorname{Ob}\mathbf{2} = \{\operatorname{dom} f, \operatorname{cod} f\}$, and

(iii) $\operatorname{Mor}\mathbf{2} = \{\operatorname{dom} f, \operatorname{cod} f, f\}$, and

(iv) $\operatorname{dom} f$, $\operatorname{cod} f$, f are mutually different.

PROOF: Consider $\mathscr{C}$ being a strict, a preorder category such that $\operatorname{Ob}\mathscr{C} = 2$ and for every objects o_1, o_2 of $\mathscr{C}$ such that $o_1 \in o_2$ holds $\hom(o_1, o_2) = \{\langle o_1, o_2\rangle\}$ and $\operatorname{RelOb}\mathscr{C} = \subseteq_2$ and $\operatorname{Mor}\mathscr{C} = 2 \cup \{\langle o_1, o_2\rangle$, where o_1, o_2 are elements of $2 : o_1 \in o_2\}$. $\mathscr{C} \cong \mathbf{2}$. Consider $\mathcal{F}$ being a functor from $\mathscr{C}$ to $\mathbf{2}$, $\mathcal{G}$ being a functor from $\mathbf{2}$ to $\mathscr{C}$ such that $\mathcal{F}$ is covariant and $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \operatorname{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \operatorname{id}_{\mathbf{2}}$. Reconsider $g = \langle 0, 1\rangle$ as a morphism of $\mathscr{C}$. g is not identity by [17, (22)]. Set $f = \mathcal{F}(g)$. f is not identity by [9, (18)], [17, (34)]. $\overline{\overline{\operatorname{Ob}\mathbf{2}}} = \overline{\overline{2}}$. Consider x, y being objects such that $x \neq y$ and $\operatorname{Ob}\mathbf{2} = \{x, y\}$. $\operatorname{dom} f \neq \operatorname{cod} f$. For every object x, $x \in \operatorname{Mor}\mathbf{2}$ iff $x \in \{\operatorname{dom} f, \operatorname{cod} f, f\}$ by [17, (22)], [9, (18)], [17, (34)], [2, (50), (49)]. □

Let $\mathscr{C}$ be a non empty category and f be a morphism of $\mathscr{C}$. The functor $\mathcal{M}_{\mathrm{f}}$ yielding a covariant functor from $\mathbf{2}$ to $\mathscr{C}$ is defined by

(Def. 16) for every morphism g of $\mathbf{2}$ such that g is not identity holds $it(g) = f$.

Now we state the proposition:

(40) Let us consider a non empty category $\mathscr{C}$, and a morphism f of $\mathscr{C}$. Suppose f is identity. Let us consider a morphism g of $\mathbf{2}$. Then $(\mathcal{M}_{\mathrm{f}})(g) = f$.

The theorem is a consequence of (39) and (6).

5. PULLBACKS

Let $\mathscr{C}$ be a category, c, c_1, c_2, d be objects of $\mathscr{C}$, and f_1 be a morphism from c_1 to c. Assume $\hom(c_1, c) \neq \emptyset$. Let f_2 be a morphism from c_2 to c. Assume $\hom(c_2, c) \neq \emptyset$. Let p_1 be a morphism from d to c_1. Assume $\hom(d, c_1) \neq \emptyset$. Let p_2 be a morphism from d to c_2. Assume $\hom(d, c_2) \neq \emptyset$. We say that $\langle d, p_1, p_2 \rangle$ is a pullback of f_1, f_2 if and only if

(Def. 17) $f_1 \cdot p_1 = f_2 \cdot p_2$ and for every object d_1 of $\mathscr{C}$ and for every morphism g_1 from d_1 to c_1 and for every morphism g_2 from d_1 to c_2 such that $\hom(d_1, c_1) \neq \emptyset$ and $\hom(d_1, c_2) \neq \emptyset$ and $f_1 \cdot g_1 = f_2 \cdot g_2$ holds $\hom(d_1, d) \neq \emptyset$ and there exists a morphism h from d_1 to d such that $p_1 \cdot h = g_1$ and $p_2 \cdot h = g_2$ and for every morphism h_1 from d_1 to d such that $p_1 \cdot h_1 = g_1$ and $p_2 \cdot h_1 = g_2$ holds $h = h_1$.

Now we state the proposition:

(41) Let us consider a category $\mathscr{C}$, objects c, c_1, c_2, d, e of $\mathscr{C}$, a morphism f_1 from c_1 to c, a morphism f_2 from c_2 to c, a morphism p_1 from d to c_1, a morphism p_2 from d to c_2, a morphism q_1 from e to c_1, and a morphism q_2 from e to c_2. Suppose $\hom(c_1, c) \neq \emptyset$ and $\hom(c_2, c) \neq \emptyset$ and $\hom(d, c_1) \neq \emptyset$ and $\hom(d, c_2) \neq \emptyset$ and $\hom(e, c_1) \neq \emptyset$ and $\hom(e, c_2) \neq \emptyset$ and $\langle d, p_1, p_2 \rangle$ is a pullback of f_1, f_2 and $\langle e, q_1, q_2 \rangle$ is a pullback of f_1, f_2. Then d and e are isomorphic. The theorem is a consequence of (23) and (18).

Let us consider a category $\mathscr{C}$, objects c, c_1, c_2, d of $\mathscr{C}$, a morphism f_1 from c_1 to c, a morphism f_2 from c_2 to c, a morphism p_1 from d to c_1, and a morphism p_2 from d to c_2. Now we state the propositions:

(42) Suppose $\hom(c_1, c) \neq \emptyset$ and $\hom(c_2, c) \neq \emptyset$ and $\hom(d, c_1) \neq \emptyset$ and $\hom(d, c_2) \neq \emptyset$ and $\langle d, p_1, p_2 \rangle$ is a pullback of f_1, f_2.
Then $\langle d, p_2, p_1 \rangle$ is a pullback of f_2, f_1.

(43) Suppose $\hom(c_1, c) \neq \emptyset$ and $\hom(c_2, c) \neq \emptyset$ and $\hom(d, c_1) \neq \emptyset$ and $\hom(d, c_2) \neq \emptyset$ and $\langle d, p_1, p_2 \rangle$ is a pullback of f_1, f_2 and f_1 is monomorphic. Then p_2 is monomorphic. The theorem is a consequence of (22) and (23).

(44) Suppose $\hom(c_1, c) \neq \emptyset$ and $\hom(c_2, c) \neq \emptyset$ and $\hom(d, c_1) \neq \emptyset$ and $\hom(d, c_2) \neq \emptyset$ and $\langle d, p_1, p_2 \rangle$ is a pullback of f_1, f_2 and f_1 is isomorphism. Then p_2 is isomorphism. The theorem is a consequence of (22), (23), and (18).

(45) Let us consider a category $\mathscr{C}$, objects c_1, c_1, c_2, c_3, c_4, c_5, c_6 of $\mathscr{C}$, a morphism f_1 from c_1 to c_2, a morphism f_2 from c_2 to c_3, a morphism f_3 from c_1 to c_4, a morphism f_4 from c_2 to c_5, a morphism f_5 from

c_3 to c_6, a morphism f_6 from c_4 to c_5, and a morphism f_7 from c_5 to c_6. Suppose $\hom(c_1, c_2) \neq \emptyset$ and $\hom(c_2, c_3) \neq \emptyset$ and $\hom(c_1, c_4) \neq \emptyset$ and $\hom(c_2, c_5) \neq \emptyset$ and $\hom(c_3, c_6) \neq \emptyset$ and $\hom(c_4, c_5) \neq \emptyset$ and $\hom(c_5, c_6) \neq \emptyset$ and $\langle c_2, f_2, f_4\rangle$ is a pullback of f_5, f_7. Then $\langle c_1, f_1, f_3\rangle$ is a pullback of f_4, f_6 if and only if $\langle c_1, f_2 \cdot f_1, f_3\rangle$ is a pullback of $f_5, f_7 \cdot f_6$ and $f_4 \cdot f_1 = f_6 \cdot f_3$. The theorem is a consequence of (22) and (23).

6. Pullbacks of Functors

Let $\mathscr{C}$, $\mathscr{D}$ be categories and $\mathcal{F}$ be a functor from $\mathscr{C}$ to $\mathscr{D}$. We say that $\mathcal{F}$ is monomorphic if and only if

(Def. 18) $\mathcal{F}$ is covariant and for every category $\mathscr{B}$ and for every functors $\mathcal{G}_1$, $\mathcal{G}_2$ from $\mathscr{B}$ to $\mathscr{C}$ such that $\mathcal{G}_1$ is covariant and $\mathcal{G}_2$ is covariant and $\mathcal{F} \circ \mathcal{G}_1 = \mathcal{F} \circ \mathcal{G}_2$ holds $\mathcal{G}_1 = \mathcal{G}_2$.

We say that $\mathcal{F}$ is isomorphism if and only if

(Def. 19) $\mathcal{F}$ is covariant and there exists a functor $\mathcal{G}$ from $\mathscr{D}$ to $\mathscr{C}$ such that $\mathcal{G}$ is covariant and $\mathcal{G} \circ \mathcal{F} = \mathrm{id}_{\mathscr{C}}$ and $\mathcal{F} \circ \mathcal{G} = \mathrm{id}_{\mathscr{D}}$.

Let $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{D}$ be categories and $\mathcal{F}_1$ be a functor from $\mathscr{C}_1$ to $\mathscr{C}$. Assume $\mathcal{F}_1$ is covariant. Let $\mathcal{F}_2$ be a functor from $\mathscr{C}_2$ to $\mathscr{C}$. Assume $\mathcal{F}_2$ is covariant. Let $\mathcal{P}_1$ be a functor from $\mathscr{D}$ to $\mathscr{C}_1$. Assume $\mathcal{P}_1$ is covariant. Let $\mathcal{P}_2$ be a functor from $\mathscr{D}$ to $\mathscr{C}_2$. Assume $\mathcal{P}_2$ is covariant. We say that $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2\rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$ if and only if

(Def. 20) $\mathcal{F}_1 \circ \mathcal{P}_1 = \mathcal{F}_2 \circ \mathcal{P}_2$ and for every category $\mathscr{D}_1$ and for every functor $\mathcal{G}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ and for every functor $\mathcal{G}_2$ from $\mathscr{D}_1$ to $\mathscr{C}_2$ such that $\mathcal{G}_1$ is covariant and $\mathcal{G}_2$ is covariant and $\mathcal{F}_1 \circ \mathcal{G}_1 = \mathcal{F}_2 \circ \mathcal{G}_2$ there exists a functor $\mathcal{H}$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}$ is covariant and $\mathcal{P}_1 \circ \mathcal{H} = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H} = \mathcal{G}_2$ and for every functor $\mathcal{H}_1$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}_1$ is covariant and $\mathcal{P}_1 \circ \mathcal{H}_1 = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H}_1 = \mathcal{G}_2$ holds $\mathcal{H} = \mathcal{H}_1$.

Now we state the proposition:

(46) Let us consider categories $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{D}$, $\mathscr{E}$, a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{C}$, a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{C}$, a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$, a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$, a functor $\mathcal{Q}_1$ from $\mathscr{E}$ to $\mathscr{C}_1$, and a functor $\mathcal{Q}_2$ from $\mathscr{E}$ to $\mathscr{C}_2$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant and $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\mathcal{Q}_1$ is covariant and $\mathcal{Q}_2$ is covariant and $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2\rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$ and $\langle \mathscr{E}, \mathcal{Q}_1, \mathcal{Q}_2\rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$. Then $\mathscr{D} \cong \mathscr{E}$.

Proof: There exists a functor $\mathcal{F}_8$ from $\mathscr{D}$ to $\mathscr{E}$ and there exists a functor $\mathcal{G}_3$ from $\mathscr{E}$ to $\mathscr{D}$ such that $\mathcal{F}_8$ is covariant and $\mathcal{G}_3$ is covariant and $\mathcal{G}_3 \circ \mathcal{F}_8 = \mathrm{id}_{\mathscr{D}}$ and $\mathcal{F}_8 \circ \mathcal{G}_3 = \mathrm{id}_{\mathscr{E}}$ by (10), (11), [17, (35)]. □

Let us consider categories $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{D}$, a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{C}$, a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{C}$, a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$, and a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$. Now we state the propositions:

(47) Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant and $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$.
Then $\langle \mathscr{D}, \mathcal{P}_2, \mathcal{P}_1 \rangle$ is a pullback of $\mathcal{F}_2, \mathcal{F}_1$.

(48) Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant and $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$ and $\mathcal{F}_1$ is monomorphic. Then $\mathcal{P}_2$ is monomorphic.
PROOF: For every category $\mathscr{D}_1$ and for every functors $\mathcal{Q}_1$, $\mathcal{Q}_2$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{Q}_1$ is covariant and $\mathcal{Q}_2$ is covariant and $\mathcal{P}_2 \circ \mathcal{Q}_1 = \mathcal{P}_2 \circ \mathcal{Q}_2$ holds $\mathcal{Q}_1 = \mathcal{Q}_2$ by [17, (35)], (10). □

(49) Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant and $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$ and $\mathcal{F}_1$ is isomorphism. Then $\mathcal{P}_2$ is isomorphism. The theorem is a consequence of (10) and (11).

(50) Let us consider categories $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{C}_3$, $\mathscr{C}_4$, $\mathscr{C}_5$, $\mathscr{C}_6$, a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{C}_2$, a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{C}_3$, a functor $\mathcal{F}_3$ from $\mathscr{C}_1$ to $\mathscr{C}_4$, a functor $\mathcal{F}_4$ from $\mathscr{C}_2$ to $\mathscr{C}_5$, a functor $\mathcal{F}_5$ from $\mathscr{C}_3$ to $\mathscr{C}_6$, a functor $\mathcal{F}_6$ from $\mathscr{C}_4$ to $\mathscr{C}_5$, and a functor $\mathcal{F}_7$ from $\mathscr{C}_5$ to $\mathscr{C}_6$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant and $\mathcal{F}_3$ is covariant and $\mathcal{F}_4$ is covariant and $\mathcal{F}_5$ is covariant and $\mathcal{F}_6$ is covariant and $\mathcal{F}_7$ is covariant and $\langle \mathscr{C}_2, \mathcal{F}_2, \mathcal{F}_4 \rangle$ is a pullback of $\mathcal{F}_5, \mathcal{F}_7$. Then $\langle \mathscr{C}_1, \mathcal{F}_1, \mathcal{F}_3 \rangle$ is a pullback of $\mathcal{F}_4, \mathcal{F}_6$ if and only if $\langle \mathscr{C}_1, \mathcal{F}_2 \circ \mathcal{F}_1, \mathcal{F}_3 \rangle$ is a pullback of $\mathcal{F}_5, \mathcal{F}_7 \circ \mathcal{F}_6$ and $\mathcal{F}_4 \circ \mathcal{F}_1 = \mathcal{F}_6 \circ \mathcal{F}_3$.
PROOF: For every category $\mathscr{D}_1$ and for every functor $\mathcal{G}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_2$ and for every functor $\mathcal{G}_2$ from $\mathscr{D}_1$ to $\mathscr{C}_4$ such that $\mathcal{G}_1$ is covariant and $\mathcal{G}_2$ is covariant and $\mathcal{F}_4 \circ \mathcal{G}_1 = \mathcal{F}_6 \circ \mathcal{G}_2$ there exists a functor $\mathcal{H}$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ such that $\mathcal{H}$ is covariant and $\mathcal{F}_1 \circ \mathcal{H} = \mathcal{G}_1$ and $\mathcal{F}_3 \circ \mathcal{H} = \mathcal{G}_2$ and for every functor $\mathcal{H}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ such that $\mathcal{H}_1$ is covariant and $\mathcal{F}_1 \circ \mathcal{H}_1 = \mathcal{G}_1$ and $\mathcal{F}_3 \circ \mathcal{H}_1 = \mathcal{G}_2$ holds $\mathcal{H} = \mathcal{H}_1$ by [17, (35)], (10). □

(51) Let us consider categories $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$, a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{C}$, and a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{C}$. Suppose $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Then there exists a strict category $\mathscr{D}$ and there exists a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$ and there exists a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$ such that the carrier of $\mathscr{D} = \{\langle f_1, f_2 \rangle$, where f_1 is a morphism of $\mathscr{C}_1, f_2$ is a morphism of $\mathscr{C}_2 : f_1 \in$ the carrier of $\mathscr{C}_1$ and $f_2 \in$ the carrier of $\mathscr{C}_2$ and $\mathcal{F}_1(f_1) = \mathcal{F}_2(f_2)\}$ and the composition of $\mathscr{D} = \{\langle \langle f_1, f_2 \rangle, f_3 \rangle$, where f_1, f_2, f_3 are morphisms of $\mathscr{D} : f_1, f_2, f_3 \in$ the carrier of $\mathscr{D}$ and for every morphisms f_{11}, f_{12}, f_{13} of $\mathscr{C}_1$ and for every morphisms f_{21}, f_{22}, f_{23} of $\mathscr{C}_2$ such that $f_1 = \langle f_{11}, f_{21} \rangle$ and $f_2 = \langle f_{12}, f_{22} \rangle$ and $f_3 = \langle f_{13}, f_{23} \rangle$ holds

$f_{11} \triangleright f_{12}$ and $f_{21} \triangleright f_{22}$ and $f_{13} = f_{11} \circ f_{12}$ and $f_{23} = f_{21} \circ f_{22}\}$ and $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$.

PROOF: Reconsider $c_7 = \{\langle f_1, f_2 \rangle$, where f_1 is a morphism of $\mathscr{C}_1, f_2$ is a morphism of $\mathscr{C}_2 : f_1 \in$ the carrier of $\mathscr{C}_1$ and $f_2 \in$ the carrier of $\mathscr{C}_2$ and $\mathcal{F}_1(f_1) = \mathcal{F}_2(f_2)\}$ as a set. Set $c_8 = \{\langle \langle x_1, x_2 \rangle, x_3 \rangle$, where x_1, x_2, x_3 are elements of $c_7 : x_1, x_2, x_3 \in c_7$ and for every morphisms f_{11}, f_{12}, f_{13} of $\mathscr{C}_1$ and for every morphisms f_{21}, f_{22}, f_{23} of $\mathscr{C}_2$ such that $x_1 = \langle f_{11}, f_{21} \rangle$ and $x_2 = \langle f_{12}, f_{22} \rangle$ and $x_3 = \langle f_{13}, f_{23} \rangle$ holds $f_{11} \triangleright f_{12}$ and $f_{21} \triangleright f_{22}$ and $f_{13} = f_{11} \circ f_{12}$ and $f_{23} = f_{21} \circ f_{22}\}$. For every object x such that $x \in c_8$ holds $x \in (c_7 \times c_7) \times c_7$. For every objects x, y_1, y_2 such that $\langle x, y_1 \rangle$, $\langle x, y_2 \rangle \in c_8$ holds $y_1 = y_2$. Set $\mathscr{D} = \langle c_7, c_8 \rangle$. For every morphisms g_1, g_2 of $\mathscr{D}$ such that $g_1 \triangleright g_2$ there exist morphisms f_{11}, f_{12}, f_{13} of $\mathscr{C}_1$ and there exist morphisms f_{21}, f_{22}, f_{23} of $\mathscr{C}_2$ such that $g_1 = \langle f_{11}, f_{21} \rangle$ and $g_2 = \langle f_{12}, f_{22} \rangle$ and $\mathcal{F}_1(f_{11}) = \mathcal{F}_2(f_{21})$ and $\mathcal{F}_1(f_{12}) = \mathcal{F}_2(f_{22})$ and $f_{11} \triangleright f_{12}$ and $f_{21} \triangleright f_{22}$ and $f_{13} = f_{11} \circ f_{12}$ and $f_{23} = f_{21} \circ f_{22}$ and $g_1 \circ g_2 = \langle f_{13}, f_{23} \rangle$ by (1), [17, (1)], [9, (1)]. For every morphisms g_1, g_2 of $\mathscr{D}$ such that there exist morphisms f_{11}, f_{12} of $\mathscr{C}_1$ and there exist morphisms f_{21}, f_{22} of $\mathscr{C}_2$ such that $g_1 = \langle f_{11}, f_{21} \rangle$ and $g_2 = \langle f_{12}, f_{22} \rangle$ and $\mathcal{F}_1(f_{11}) = \mathcal{F}_2(f_{21})$ and $\mathcal{F}_1(f_{12}) = \mathcal{F}_2(f_{22})$ and $f_{11} \triangleright f_{12}$ and $f_{21} \triangleright f_{22}$ holds $g_1 \triangleright g_2$ by (1), [17, (1)]. For every morphisms g, g_1, g_2 of $\mathscr{D}$ such that $g_1 \triangleright g_2$ holds $g_1 \circ g_2 \triangleright g$ iff $g_2 \triangleright g$. For every morphisms g, g_1, g_2 of $\mathscr{D}$ such that $g_1 \triangleright g_2$ holds $g \triangleright g_1 \circ g_2$ iff $g \triangleright g_1$. For every morphism g_1 of $\mathscr{D}$ such that $g_1 \in$ the carrier of $\mathscr{D}$ there exists a morphism g of $\mathscr{D}$ such that $g \triangleright g_1$ and g is left identity by (2), [17, (31), (32)]. For every morphism g_1 of $\mathscr{D}$ such that $g_1 \in$ the carrier of $\mathscr{D}$ there exists a morphism g of $\mathscr{D}$ such that $g_1 \triangleright g$ and g is right identity by (2), [17, (31), (32)]. For every morphisms g_1, g_2, g_3 of $\mathscr{D}$ such that $g_1 \triangleright g_2$ and $g_2 \triangleright g_3$ and $g_1 \circ g_2 \triangleright g_3$ and $g_1 \triangleright g_2 \circ g_3$ holds $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$. For every object x, $x \in c_8$ iff $x \in \{\langle \langle f_1, f_2 \rangle, f_3 \rangle$, where f_1, f_2, f_3 are morphisms of $\mathscr{D} : f_1, f_2, f_3 \in$ the carrier of $\mathscr{D}$ and for every morphisms f_{11}, f_{12}, f_{13} of $\mathscr{C}_1$ and for every morphisms f_{21}, f_{22}, f_{23} of $\mathscr{C}_2$ such that $f_1 = \langle f_{11}, f_{21} \rangle$ and $f_2 = \langle f_{12}, f_{22} \rangle$ and $f_3 = \langle f_{13}, f_{23} \rangle$ holds $f_{11} \triangleright f_{12}$ and $f_{21} \triangleright f_{22}$ and $f_{13} = f_{11} \circ f_{12}$ and $f_{23} = f_{21} \circ f_{22}\}$. There exists a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$ and there exists a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$ such that $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\mathcal{F}_1 \circ \mathcal{P}_1 = \mathcal{F}_2 \circ \mathcal{P}_2$ and for every category $\mathscr{D}_1$ and for every functor $\mathcal{G}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ and for every functor $\mathcal{G}_2$ from $\mathscr{D}_1$ to $\mathscr{C}_2$ such that $\mathcal{G}_1$ is covariant and $\mathcal{G}_2$ is covariant and $\mathcal{F}_1 \circ \mathcal{G}_1 = \mathcal{F}_2 \circ \mathcal{G}_2$ there exists a functor $\mathcal{H}$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}$ is covariant and $\mathcal{P}_1 \circ \mathcal{H} = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H} = \mathcal{G}_2$ and for every functor $\mathcal{H}_1$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}_1$ is covariant and $\mathcal{P}_1 \circ \mathcal{H}_1 = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H}_1 = \mathcal{G}_2$ holds $\mathcal{H} = \mathcal{H}_1$ by [17, (31)], [9, (13)], (1), [17, (32), (34)]. Consider $\mathcal{P}_1$

being a functor from $\mathscr{D}$ to $\mathscr{C}_1$, $\mathcal{P}_2$ being a functor from $\mathscr{D}$ to $\mathscr{C}_2$ such that $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\mathcal{F}_1 \circ \mathcal{P}_1 = \mathcal{F}_2 \circ \mathcal{P}_2$ and for every category $\mathscr{D}_1$ and for every functor $\mathcal{G}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ and for every functor $\mathcal{G}_2$ from $\mathscr{D}_1$ to $\mathscr{C}_2$ such that $\mathcal{G}_1$ is covariant and $\mathcal{G}_2$ is covariant and $\mathcal{F}_1 \circ \mathcal{G}_1 = \mathcal{F}_2 \circ \mathcal{G}_2$ there exists a functor $\mathcal{H}$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}$ is covariant and $\mathcal{P}_1 \circ \mathcal{H} = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H} = \mathcal{G}_2$ and for every functor $\mathcal{H}_1$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{H}_1$ is covariant and $\mathcal{P}_1 \circ \mathcal{H}_1 = \mathcal{G}_1$ and $\mathcal{P}_2 \circ \mathcal{H}_1 = \mathcal{G}_2$ holds $\mathcal{H} = \mathcal{H}_1$. □

Let $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$ be categories and $\mathcal{F}_1$ be a functor from $\mathscr{C}_1$ to $\mathscr{C}$. Assume $\mathcal{F}_1$ is covariant. Let $\mathcal{F}_2$ be a functor from $\mathscr{C}_2$ to $\mathscr{C}$. Assume $\mathcal{F}_2$ is covariant.

A pullback of $\mathcal{F}_1$, $\mathcal{F}_2$ is a triple object and is defined by

(Def. 21) there exists a strict category $\mathscr{D}$ and there exists a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$ and there exists a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$ such that $it = \langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ and $\mathcal{P}_1$ is covariant and $\mathcal{P}_2$ is covariant and $\langle \mathscr{D}, \mathcal{P}_1, \mathcal{P}_2 \rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$.

Assume $\mathcal{F}_1$ is covariant. Assume $\mathcal{F}_2$ is covariant. The functor $[\![\mathcal{F}_1, \mathcal{F}_2]\!]$ yielding a strict category is defined by the term

(Def. 22) the pullback of $\mathcal{F}_1$, $\mathcal{F}_{2\mathbf{1},3}$.

Assume $\mathcal{F}_1$ is covariant. Assume $\mathcal{F}_2$ is covariant. The functor $\pi_1(\mathcal{F}_1 \boxtimes \mathcal{F}_2)$ yielding a functor from $[\![\mathcal{F}_1, \mathcal{F}_2]\!]$ to $\mathscr{C}_1$ is defined by the term

(Def. 23) the pullback of $\mathcal{F}_1$, $\mathcal{F}_{2\mathbf{2},3}$.

The functor $\pi_2(\mathcal{F}_1 \boxtimes \mathcal{F}_2)$ yielding a functor from $[\![\mathcal{F}_1, \mathcal{F}_2]\!]$ to $\mathscr{C}_2$ is defined by the term

(Def. 24) the pullback of $\mathcal{F}_1$, $\mathcal{F}_{2\mathbf{3},3}$.

Let us consider categories $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$, a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{C}$, and a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{C}$. Let us assume that $\mathcal{F}_1$ is covariant and $\mathcal{F}_2$ is covariant. Now we state the propositions:

(52) (i) $\pi_1(\mathcal{F}_1 \boxtimes \mathcal{F}_2)$ is covariant, and

(ii) $\pi_2(\mathcal{F}_1 \boxtimes \mathcal{F}_2)$ is covariant, and

(iii) $\langle [\![\mathcal{F}_1, \mathcal{F}_2]\!], \pi_1(\mathcal{F}_1 \boxtimes \mathcal{F}_2), \pi_2(\mathcal{F}_1 \boxtimes \mathcal{F}_2) \rangle$ is a pullback of $\mathcal{F}_1, \mathcal{F}_2$.

(53) $[\![\mathcal{F}_1, \mathcal{F}_2]\!] \cong [\![\mathcal{F}_2, \mathcal{F}_1]\!]$. The theorem is a consequence of (52), (47), and (46).

(54) There exist object-categories $\mathscr{C}$, $\mathscr{C}_1$, $\mathscr{C}_2$ and there exists a functor $\mathcal{F}_1$ from $\mathscr{C}_1$ to $\mathscr{C}$ and there exists a functor $\mathcal{F}_2$ from $\mathscr{C}_2$ to $\mathscr{C}$ such that there exists no object-category $\mathscr{D}$ and there exists a functor $\mathcal{P}_1$ from $\mathscr{D}$ to $\mathscr{C}_1$ and there exists a functor $\mathcal{P}_2$ from $\mathscr{D}$ to $\mathscr{C}_2$ such that $\mathcal{F}_1 \cdot \mathcal{P}_1 = \mathcal{F}_2 \cdot \mathcal{P}_2$ and for every object-category $\mathscr{D}_1$ and for every functor $\mathcal{G}_1$ from $\mathscr{D}_1$ to $\mathscr{C}_1$ and for every functor $\mathcal{G}_2$ from $\mathscr{D}_1$ to $\mathscr{C}_2$ such that $\mathcal{F}_1 \cdot \mathcal{G}_1 = \mathcal{F}_2 \cdot \mathcal{G}_2$ there exists a functor $\mathcal{H}$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{P}_1 \cdot \mathcal{H} = \mathcal{G}_1$ and $\mathcal{P}_2 \cdot \mathcal{H} = \mathcal{G}_2$ and for

every functor $\mathcal{H}_1$ from $\mathscr{D}_1$ to $\mathscr{D}$ such that $\mathcal{P}_1 \cdot \mathcal{H}_1 = \mathcal{G}_1$ and $\mathcal{P}_2 \cdot \mathcal{H}_1 = \mathcal{G}_2$ holds $\mathcal{H} = \mathcal{H}_1$. The theorem is a consequence of (39) and (40).

References

[1] Jiri Adamek, Horst Herrlich, and George E. Strecker. *Abstract and Concrete Categories: The Joy of Cats*. Dover Publication, New York, 2009.

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

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

[4] Grzegorz Bancerek. The well ordering relations. *Formalized Mathematics*, 1(**1**):123–129, 1990.

[5] Grzegorz Bancerek. Zermelo theorem and axiom of choice. *Formalized Mathematics*, 1 (**2**):265–267, 1990.

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

[7] Francis Borceaux. *Handbook of Categorical Algebra I. Basic Category Theory*, volume 50 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1994.

[8] Czesław Byliński. Introduction to categories and functors. *Formalized Mathematics*, 1 (**2**):409–420, 1990.

[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 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] F. William Lawvere. Functorial semantics of algebraic theories and some algebraic problems in the context of functorial semantics of algebraic theories. *Reprints in Theory and Applications of Categories*, 5:1–121, 2004.

[15] Saunders Mac Lane. *Categories for the Working Mathematician*, volume 5 of *Graduate Texts in Mathematics*. Springer Verlag, New York, Heidelberg, Berlin, 1971.

[16] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[17] Marco Riccardi. Object-free definition of categories. *Formalized Mathematics*, 21(**3**): 193–205, 2013. doi:10.2478/forma-2013-0021.

[18] Andrzej Trybulec. Enumerated sets. *Formalized Mathematics*, 1(**1**):25–34, 1990.

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

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

[21] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received December 31, 2014

FORMALIZED MATHEMATICS
Vol. 23, No. 1, Pages 15–27, 2015
DOI: 10.2478/forma-2015-0002

DE GRUYTER OPEN
degruyter.com/view/j/forma

Definition and Properties of Direct Sum Decomposition of Groups[1]

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, direct sum decomposition of group is mainly discussed. In the second section, support of element of direct product group is defined and its properties are formalized. It is formalized here that an element of direct product group belongs to its direct sum if and only if support of the element is finite. In the third section, product map and sum map are prepared. In the fourth section, internal and external direct sum are defined. In the last section, an equivalent form of internal direct sum is proved. We referred to [23], [22], [8] and [18] in the formalization.

MSC: 20E34 03B35

Keywords: group theory; direct sum decomposition

MML identifier: GROUP_19, version: 8.1.03 5.29.1227

The notation and terminology used in this paper have been introduced in the following articles: [1], [2], [6], [16], [24], [10], [11], [12], [13], [7], [27], [20], [21], [28], [29], [30], [17], [33], [25], [3], [5], [14], [19], [32], [31], and [15].

1. Miscellanies

Let D be a non empty set and x be an element of D. Observe that the functor $\langle x \rangle$ yields a finite sequence of elements of D. Let I be a set.

[1]This work was supported by JSPS KAKENHI 22300285.

ISSN 1426–2630(Print), 1898-9934(Online)

A family of groups of I is an associative, group-like multiplicative magma family of I. Let G be a group. Note that there exists a subgroup of G which is commutative.

Now we state the proposition:

(1) Let us consider a set I, a family F of groups of I, and an object i. If $i \in I$, then $F(i)$ is a group.

Let I be a set, F be a family of groups of I, and i be an object. Assume $i \in I$. One can verify that the functor $F(i)$ yields a group. One can verify that $\operatorname{sum} F$ is non empty and constituted functions.

Now we state the propositions:

(2) Let us consider a set I, and a function F. Suppose $I = \operatorname{dom} F$ and for every object i such that $i \in I$ holds $F(i)$ is a group. Then F is a family of groups of I.

(3) Let us consider a set I, a family F of groups of I, and an element a of $\prod F$. Then $\operatorname{dom} a = I$.

(4) Let us consider a non empty set I, a family F of groups of I, and an element x of I. Then (the support of F)$(x) = \Omega_{F(x)}$.

(5) Let us consider a non empty set I, a family F of groups of I, a function x, and an element i of I. If $x \in \prod F$, then $x(i) \in F(i)$. The theorem is a consequence of (4).

(6) Let us consider groups G, H, and a subgroup I of H. Then every homomorphism from G to I is a homomorphism from G to H.

2. Support of Element of Direct Product Group

Let I be a set, F be a family of groups of I, and a be a function. The functor $\operatorname{support}(a, F)$ yielding a subset of I is defined by

(Def. 1) for every object i, $i \in it$ iff $a(i) \neq \mathbf{1}_{F(i)}$ and $i \in I$.

Now we state the proposition:

(7) Let us consider a set I, a family F of groups of I, and an element a of $\operatorname{sum} F$. Then there exists a finite subset J of I and there exists a many sorted set b indexed by J such that $J = \operatorname{support}(a, F)$ and $a = \mathbf{1}_{\prod F} + \cdot b$ and for every object j such that $j \in I \setminus J$ holds $a(j) = \mathbf{1}_{F(j)}$ and for every object j such that $j \in J$ holds $a(j) = b(j)$.

Proof: Consider g being an element of $\prod$(the support of F), J being a finite subset of I, b being a many sorted set indexed by J such that $g = \mathbf{1}_{\prod F}$ and $a = g + \cdot b$ and for every set j such that $j \in J$ there exists a group-like, non empty multiplicative magma G such that $G = F(j)$ and

$b(j) \in$ the carrier of G and $b(j) \neq \mathbf{1}_G$. $\operatorname{dom} \mathbf{1}_{\prod F} = I$. For every object j such that $j \in I \setminus J$ holds $a(j) = \mathbf{1}_{F(j)}$ by [13, (11)], [17, (6)]. For every object j, $j \in \operatorname{support}(a, F)$ iff $j \in J$ by [13, (13)]. □

Let I be a set, F be a family of groups of I, and a be an element of $\operatorname{sum} F$. One can verify that $\operatorname{support}(a, F)$ is finite.

Let G be a group and a be a function from I into G. The functor $\operatorname{support} a$ yielding a subset of I is defined by

(Def. 2) for every object i, $i \in it$ iff $a(i) \neq \mathbf{1}_G$ and $i \in I$.

We say that a is finite-support if and only if

(Def. 3) $\operatorname{support} a$ is finite.

Let us observe that there exists a function from I into G which is finite-support. Let a be a finite-support function from I into G. One can verify that $\operatorname{support} a$ is finite.

The functor $\prod a$ yielding an element of G is defined by the term

(Def. 4) $\prod(a \restriction \operatorname{support} a)$.

Now we state the propositions:

(8) Let us consider a set I, a family F of groups of I, and an element a of $\prod F$. Then $a \in \operatorname{sum} F$ if and only if $\operatorname{support}(a, F)$ is finite.

PROOF: Reconsider $J = \operatorname{support}(a, F)$ as a finite subset of I. Set $k = a \restriction J$. Set $x = \mathbf{1}_{\prod F} + \cdot k$. For every set j such that $j \in J$ there exists a group-like, non empty multiplicative magma G such that $G = F(j)$ and $k(j) \in$ the carrier of G and $k(j) \neq \mathbf{1}_G$ by [10, (49)], (5). $\operatorname{dom} x = I$. For every object i such that $i \in \operatorname{dom} x$ holds $x(i) = a(i)$ by [13, (11)], [17, (6)], [13, (13)], [10, (49)]. $x = a$. □

(9) Let us consider a set I, a group G, a family H of groups of I, a function x from I into G, and an element y of $\prod H$. Suppose $x = y$ and for every object i such that $i \in I$ holds $H(i)$ is a subgroup of G. Then $\operatorname{support} x = \operatorname{support}(y, H)$.

PROOF: For every object i such that $i \in I$ holds $\mathbf{1}_{H(i)} = \mathbf{1}_G$ by [28, (44)]. For every object i, $i \in \operatorname{support}(y, H)$ iff $i \in \operatorname{support} x$. □

(10) Let us consider a set I, a group G, a family F of groups of I, and an object a. Suppose $a \in \operatorname{sum} F$ and for every object i such that $i \in I$ holds $F(i)$ is a subgroup of G. Then a is a finite-support function from I into G.

PROOF: Reconsider $b = a$ as an element of $\prod F$. For every object i such that $i \in I$ holds $\Omega_{F(i)} \subseteq \Omega_G$. $\operatorname{dom} b = I$. For every object z such that $z \in \operatorname{rng} b$ holds $z \in \Omega_G$ by (3), (5), [28, (40)]. $\operatorname{support}(b, F) = \operatorname{support} b$. □

(11) Let us consider a non empty set I, and a family F of groups of I. Then $\mathrm{support}(\mathbf{1}_{\prod F}, F)$ is empty.
PROOF: For every object i, $i \notin \mathrm{support}(\mathbf{1}_{\prod F}, F)$ by [17, (6)]. □

(12) Let us consider a non empty set I, a group G, and a function a from I into G. If $a = I \longmapsto \mathbf{1}_G$, then $\mathrm{support}\, a$ is empty.
PROOF: For every object i, $i \notin \mathrm{support}\, a$ by [24, (7)]. □

(13) Let us consider a non empty set I, a group G, and a family F of groups of I. Suppose for every element i of I, $F(i)$ is a subgroup of G. Then $\mathbf{1}_{\prod F} = I \longmapsto \mathbf{1}_G$.
PROOF: $\mathrm{dom}\, \mathbf{1}_{\prod F} = I$. For every object j such that $j \in I$ holds $\mathbf{1}_{\prod F}(j) = (I \longmapsto \mathbf{1}_G)(j)$ by [17, (6)], [24, (7)], [28, (44)]. □

(14) Let us consider a non empty set I, a family F of groups of I, a group G, and a finite-support function x from I into G. Suppose $\mathrm{support}\, x = \emptyset$ and for every object i such that $i \in I$ holds $F(i)$ is a subgroup of G. Then $x = \mathbf{1}_{\prod F}$.
PROOF: For every set i such that $i \in I$ there exists a group-like, non empty multiplicative magma G such that $G = F(i)$ and $x(i) = \mathbf{1}_G$ by [28, (44)]. □

(15) Let us consider a set I, a group G, and a finite-support function x from I into G. If $\mathrm{support}\, x = \emptyset$, then $\prod x = \mathbf{1}_G$.

(16) Let us consider a non empty set I, a group G, and a finite-support function a from I into G. If $a = I \longmapsto \mathbf{1}_G$, then $\prod a = \mathbf{1}_G$. The theorem is a consequence of (12) and (15).

Let us consider a non empty set I, a family F of groups of I, an element x of $\prod F$, an element i of I, and an element g of $F(i)$. Now we state the propositions:

(17) If $x = \mathbf{1}_{\prod F} +\cdot (i, g)$, then $\mathrm{support}(x, F) \subseteq \{i\}$.
PROOF: For every object j such that $j \in \mathrm{support}(x, F)$ holds $j \in \{i\}$ by [20, (1)]. □

(18) If $x = \mathbf{1}_{\prod F} +\cdot (i, g)$ and $g \neq \mathbf{1}_{F(i)}$, then $\mathrm{support}(x, F) = \{i\}$. The theorem is a consequence of (17).

Let us consider a non empty set I, a group G, an element i of I, an element g of G, and a function a from I into G. Now we state the propositions:

(19) If $a = (I \longmapsto \mathbf{1}_G) +\cdot (i, g)$, then $\mathrm{support}\, a \subseteq \{i\}$.
PROOF: For every object j such that $j \in \mathrm{support}\, a$ holds $j \in \{i\}$ by [7, (32)], [24, (7)]. □

(20) If $a = (I \longmapsto \mathbf{1}_G) +\cdot (i, g)$ and $g \neq \mathbf{1}_G$, then $\mathrm{support}\, a = \{i\}$. The theorem is a consequence of (19).

Now we state the propositions:

(21) Let us consider a non empty set I, a group G, a finite-support function a from I into G, an element i of I, and an element g of G. If $a = (I \longmapsto \mathbf{1}_G) +\cdot (i, g)$, then $\prod a = g$. The theorem is a consequence of (20) and (16).

(22) Let us consider a non empty set I, a family F of groups of I, a function x, an element i of I, and an element g of $F(i)$. Suppose $\operatorname{support}(x, F)$ is finite. Then $\operatorname{support}(x +\cdot (i, g), F)$ is finite.

PROOF: Reconsider $y = x +\cdot (i, g)$ as a function. For every object j such that $j \in \operatorname{support}(y, F)$ holds $j \in \operatorname{support}(x, F) \cup \{i\}$ by [7, (32)]. □

(23) Let us consider a non empty set I, a group G, a function a from I into G, an element i of I, and an element g of G. Suppose $\operatorname{support} a$ is finite. Then $\operatorname{support}(a +\cdot (i, g))$ is finite.

PROOF: Reconsider $b = a +\cdot (i, g)$ as a function from I into G. For every object j such that $j \in \operatorname{support} b$ holds $j \in \operatorname{support} a \cup \{i\}$ by [7, (32)]. □

Let us consider a non empty set I, a family F of groups of I, a function x, an element i of I, and an element g of $F(i)$. Now we state the propositions:

(24) If $x \in \prod F$, then $x +\cdot (i, g) \in \prod F$.

PROOF: $\operatorname{dom} x = I$. Set $y = x +\cdot (i, g)$. For every object j such that $j \in \operatorname{dom}$(the support of F) holds $y(j) \in$ (the support of F)(j) by [7, (31)], (4), [7, (32)], [2, (9)]. □

(25) If $x \in \operatorname{sum} F$, then $x +\cdot (i, g) \in \operatorname{sum} F$.

PROOF: Set $y = x +\cdot (i, g)$. $y \in \prod F$. For every object j such that $j \in \operatorname{support}(y, F)$ holds $j \in \operatorname{support}(x, F) \cup \{i\}$ by [7, (32)]. □

Now we state the propositions:

(26) Let us consider a non empty set I, a group G, a finite-support function a from I into G, an element i of I, and an element g of G. Then $a +\cdot (i, g)$ is a finite-support function from I into G. The theorem is a consequence of (23).

(27) Let us consider a non empty set I, a family F of groups of I, an object i, and functions a, b. Suppose $i \in I$ and $\operatorname{dom} a = I$ and $b = a +\cdot (i, \mathbf{1}_{F(i)})$. Then $\operatorname{support}(b, F) = \operatorname{support}(a, F) \setminus \{i\}$.

PROOF: For every object j, $j \in \operatorname{support}(b, F)$ iff $j \in \operatorname{support}(a, F) \setminus \{i\}$ by [15, (11), (48)], [7, (32)], [15, (50)]. □

(28) Let us consider a non empty set I, a group G, an object i, and functions a, b from I into G. Suppose $i \in \operatorname{support} a$ and $b = a +\cdot (i, \mathbf{1}_G)$. Then $\operatorname{support} b = \operatorname{support} a \setminus \{i\}$.

PROOF: For every object j, $j \in \operatorname{support} b$ iff $j \in \operatorname{support} a \setminus \{i\}$ by [15, (11), (48)], [7, (32)], [15, (50)]. □

(29) Let us consider a non empty set I, a family F of groups of I, an object i, an element a of $\operatorname{sum} F$, and a function b. Suppose $i \in \operatorname{support}(a, F)$ and

$b = a +\cdot (i, \mathbf{1}_{F(i)})$. Then $\overline{\overline{\operatorname{support}(b, F)}} = \overline{\overline{\operatorname{support}(a, F)}} - 1$. The theorem is a consequence of (3) and (27).

(30) Let us consider a non empty set I, a group G, an object i, a finite-support function a from I into G, and a function b from I into G. Suppose $i \in \operatorname{support} a$ and $b = a +\cdot (i, \mathbf{1}_G)$. Then $\overline{\overline{\operatorname{support} b}} = \overline{\overline{\operatorname{support} a}} - 1$. The theorem is a consequence of (28).

Let us consider a non empty set I, a family F of groups of I, and elements a, b of $\prod F$.

Let us assume that $\operatorname{support}(a, F)$ misses $\operatorname{support}(b, F)$. Now we state the propositions:

(31) $a +\cdot b \restriction \operatorname{support}(b, F) = a \cdot b$.

PROOF: Reconsider $c = a +\cdot b \restriction \operatorname{support}(b, F)$ as a function. Reconsider $d = a \cdot b$ as an element of $\prod F$. $\operatorname{dom} a = I$. $\operatorname{dom} b = I$. $\operatorname{dom} d = I$. For every object i such that $i \in I$ holds $c(i) = d(i)$ by (5), [13, (11)], [17, (1)], [13, (13)]. □

(32) $a \cdot b = b \cdot a$.

PROOF: Reconsider $c = a \cdot b$ as an element of $\prod F$. Reconsider $d = b \cdot a$ as an element of $\prod F$. $\operatorname{dom} c = I$. $\operatorname{dom} d = I$. For every object i such that $i \in I$ holds $c(i) = d(i)$ by (5), [17, (1)]. □

(33) Let us consider a non empty set I, a family F of groups of I, and an element i of I. Then $\operatorname{ProjGroup}(F, i)$ is a subgroup of $\operatorname{sum} F$.

PROOF: Set $S = \operatorname{ProjGroup}(F, i)$. Set $G = \operatorname{sum} F$. For every object x such that $x \in \Omega_S$ holds $x \in \Omega_G$ by [28, (40)], (17), (8). □

(34) Let us consider a non empty set I, families F, G of groups of I, and functions x, y. Suppose for every object i such that $i \in I$ there exists a homomorphism h_1 from $F(i)$ to $G(i)$ such that $y(i) = h_1(x(i))$. Then $\operatorname{support}(y, G) \subseteq \operatorname{support}(x, F)$.

PROOF: For every object i such that $i \in \operatorname{support}(y, G)$ holds $i \in \operatorname{support}(x, F)$ by [30, (31)]. □

3. Product Map and Sum Map

Let F, G be non-empty, non empty functions and h be a non empty function. Assume $\operatorname{dom} F = \operatorname{dom} G = \operatorname{dom} h$ and for every object i such that $i \in \operatorname{dom} h$ holds $h(i)$ is a function from $F(i)$ into $G(i)$. The functor $\operatorname{ProductMap}(F, G, h)$ yielding a function from $\prod F$ into $\prod G$ is defined by

(Def. 5) for every element x of $\prod F$ and for every object i such that $i \in \operatorname{dom} h$ there exists a function h_1 from $F(i)$ into $G(i)$ such that $h_1 = h(i)$ and $(it(x))(i) = h_1(x(i))$.

Let us consider non-empty, non empty functions F, G and a non empty function h.

Let us assume that $\operatorname{dom} F = \operatorname{dom} G = \operatorname{dom} h$ and for every object i such that $i \in \operatorname{dom} h$ there exists a function h_1 from $F(i)$ into $G(i)$ such that $h_1 = h(i)$ and h_1 is onto. Now we state the propositions:

(35) ProductMap(F, G, h) is onto.

PROOF: Set $p = \text{ProductMap}(F, G, h)$. For every object i such that $i \in \operatorname{dom} h$ holds $h(i)$ is a function from $F(i)$ into $G(i)$. For every object y such that $y \in \prod G$ there exists an object x such that $x \in \prod F$ and $y = p(x)$ by [2, (9)], [11, (11)], [10, (2)]. □

(36) ProductMap(F, G, h) is one-to-one.

PROOF: Set $p = \text{ProductMap}(F, G, h)$. For every object i such that $i \in \operatorname{dom} h$ holds $h(i)$ is a function from $F(i)$ into $G(i)$. For every objects x_1, x_2 such that x_1, $x_2 \in \prod F$ and $p(x_1) = p(x_2)$ holds $x_1 = x_2$ by [2, (9)], [11, (19)], [10, (2)]. □

(37) ProductMap(F, G, h) is bijective. The theorem is a consequence of (35) and (36).

Now we state the proposition:

(38) Let us consider a non empty set I, families F, G of groups of I, a non empty function h, an element x of $\prod F$, and an element y of $\prod G$. Suppose $I = \operatorname{dom} h$ and $y = (\text{ProductMap}(\text{the support of } F, \text{the support of } G, h))(x)$ and for every object i such that $i \in I$ holds $h(i)$ is a homomorphism from $F(i)$ to $G(i)$. Let us consider an object i. Suppose $i \in I$. Then there exists a homomorphism h_1 from $F(i)$ to $G(i)$ such that

(i) $h_1 = h(i)$, and

(ii) $y(i) = h_1(x(i))$.

The theorem is a consequence of (4).

Let I be a non empty set, F, G be families of groups of I, and h be a non empty function. Assume $I = \operatorname{dom} h$ and for every object i such that $i \in I$ holds $h(i)$ is a homomorphism from $F(i)$ to $G(i)$. The functor ProductMap(F, G, h) yielding a homomorphism from $\prod F$ to $\prod G$ is defined by the term

(Def. 6) ProductMap(the support of F, the support of G, h).

Now we state the propositions:

(39) Let us consider a non empty set I, families F, G of groups of I, a non empty function h, an element x of $\prod F$, and an element y of $\prod G$. Suppose $I = \operatorname{dom} h$ and $y = (\text{ProductMap}(F, G, h))(x)$ and for every object i such that $i \in I$ holds $h(i)$ is a homomorphism from $F(i)$ to $G(i)$. Let us consider

an object i. Suppose $i \in I$. Then there exists a homomorphism h_1 from $F(i)$ to $G(i)$ such that

(i) $h_1 = h(i)$, and

(ii) $y(i) = h_1(x(i))$.

The theorem is a consequence of (38).

(40) Let us consider a non empty set I, families F, G of groups of I, and a non empty function h. Suppose $I = \operatorname{dom} h$ and for every object i such that $i \in I$ there exists a homomorphism h_1 from $F(i)$ to $G(i)$ such that $h_1 = h(i)$ and h_1 is bijective. Then $\operatorname{ProductMap}(F, G, h)$ is bijective. The theorem is a consequence of (4) and (37).

Let I be a non empty set, F be a family of groups of I, and i be an element of I. Observe that the functor $\operatorname{ProjGroup}(F, i)$ yields a strict subgroup of $\operatorname{sum} F$. Let F, G be families of groups of I and h be a non empty function. Assume $I = \operatorname{dom} h$ and for every object i such that $i \in I$ holds $h(i)$ is a homomorphism from $F(i)$ to $G(i)$. The functor $\operatorname{SumMap}(F, G, h)$ yielding a homomorphism from $\operatorname{sum} F$ to $\operatorname{sum} G$ is defined by the term

(Def. 7) $\operatorname{ProductMap}(F, G, h) \restriction \operatorname{sum} F$.

Now we state the propositions:

(41) Let us consider a non empty set I, families F, G of groups of I, and a non empty function h. Suppose $I = \operatorname{dom} h$ and for every object i such that $i \in I$ there exists a homomorphism h_1 from $F(i)$ to $G(i)$ such that $h_1 = h(i)$ and h_1 is bijective. Then $\operatorname{SumMap}(F, G, h)$ is bijective.

PROOF: For every object i such that $i \in I$ holds $h(i)$ is a homomorphism from $F(i)$ to $G(i)$. Set $p = \operatorname{ProductMap}(F, G, h)$. Set $s = \operatorname{SumMap}(F, G, h)$. p is bijective. For every object y such that $y \in \Omega_{\operatorname{sum} G}$ holds $y \in \operatorname{rng} s$ by [28, (40)], [30, (61)], (39), [30, (62)]. □

(42) Let us consider a non empty set I, families F, G of groups of I, and a non empty function h. Suppose $I = \operatorname{dom} h$ and for every object i such that $i \in I$ holds $h(i)$ is a homomorphism from $F(i)$ to $G(i)$. Let us consider an element i of I, an element f of $F(i)$, and a homomorphism h_1 from $F(i)$ to $G(i)$. Suppose $h_1 = h(i)$. Then $(\operatorname{SumMap}(F, G, h))((1\operatorname{ProdHom}(F, i))(f)) = (1\operatorname{ProdHom}(G, i))(h_1(f))$.

PROOF: Set $x = (1\operatorname{ProdHom}(F, i))(f)$. Set $y = (\operatorname{SumMap}(F, G, h))(x)$. $\operatorname{dom} y = I$. Consider h_2 being a homomorphism from $F(i)$ to $G(i)$ such that $h_2 = h(i)$ and $y(i) = h_2(x(i))$. For every element j of I such that $j \neq i$ holds $y(j) = \mathbf{1}_{G(j)}$ by [20, (1)], (39), [30, (31)]. □

4. DEFINITION OF INTERNAL AND EXTERNAL DIRECT SUM DECOMPOSITION

Now we state the proposition:

(43) Let us consider a non empty set I, a group G, and an object i. Suppose $i \in I$. Then there exists a family F of groups of I and there exists a homomorphism h from $\operatorname{sum} F$ to G such that h is bijective and $F = (I \longmapsto \{\mathbf{1}\}_G) +\cdot (\{i\} \longmapsto G)$ and for every object j such that $j \in I$ holds $\mathbf{1}_{F(j)} = \mathbf{1}_G$ and for every element x of $\operatorname{sum} F$, $h(x) = x(i)$ and for every element x of $\operatorname{sum} F$, there exists a finite subset J of I and there exists a many sorted set a indexed by J such that $J \subseteq \{i\}$ and $J = \operatorname{support}(x, F)$ and ($\operatorname{support}(x, F) = \emptyset$ or $\operatorname{support}(x, F) = \{i\}$) and $x = \mathbf{1}_{\prod F} +\cdot a$ and for every object j such that $j \in I \setminus J$ holds $x(j) = \mathbf{1}_{F(j)}$ and for every object j such that $j \in J$ holds $x(j) = a(j)$.

PROOF: Set $v = I \longmapsto \{\mathbf{1}\}_G$. Set $w = \{i\} \longmapsto G$. Set $F = v +\cdot w$. For every object j such that $j \in I \setminus \{i\}$ holds $F(j) = \{\mathbf{1}\}_G$ by [24, (7)]. For every object j such that $j \in I$ holds $F(j)$ is a group. For every object j such that $j \in I$ holds $\mathbf{1}_{F(j)} = \mathbf{1}_G$ by [28, (44)]. Define $\mathcal{P}$[element of $\operatorname{sum} F$, element of G] $\equiv \$_2 = \$_1(i)$. For every element x of $\operatorname{sum} F$, there exists an element y of G such that $\mathcal{P}[x, y]$ by [28, (40)], (5), [24, (13), (7)]. Consider h being a function from $\operatorname{sum} F$ into G such that for every element x of $\operatorname{sum} F$, $\mathcal{P}[x, h(x)]$ from [11, Sch. 3]. For every object y such that $y \in \Omega_G$ there exists an object x such that $x \in \Omega_{\operatorname{sum} F}$ and $y = h(x)$ by [24, (7)], (24), (17), (8). For every element x of $\operatorname{sum} F$, $\operatorname{support}(x, F) \subseteq \{i\}$ by [28, (40)], (5), [28, (44)]. For every objects x_1, x_2 such that x_1, $x_2 \in \Omega_{\operatorname{sum} F}$ and $h(x_1) = h(x_2)$ holds $x_1 = x_2$ by [28, (40)], (3), (7), [10, (2)]. For every elements x, y of $\operatorname{sum} F$, $h(x \cdot y) = h(x) \cdot h(y)$ by [28, (40)], (5), [28, (43)], [17, (1)]. For every element x of $\operatorname{sum} F$, there exists a finite subset J of I and there exists a many sorted set a indexed by J such that $J \subseteq \{i\}$ and $J = \operatorname{support}(x, F)$ and ($\operatorname{support}(x, F) = \emptyset$ or $\operatorname{support}(x, F) = \{i\}$) and $x = \mathbf{1}_{\prod F} +\cdot a$ and for every object j such that $j \in I \setminus J$ holds $x(j) = \mathbf{1}_{F(j)}$ and for every object j such that $j \in J$ holds $x(j) = a(j)$ by [15, (31)], (7). □

Let I be a non empty set and G be a group. A direct sum components of G and I is a family of groups of I and is defined by

(Def. 8) there exists a homomorphism h from sum *it* to G such that h is bijective.

Let F be a direct sum components of G and I. We say that F is internal if and only if

(Def. 9) for every element i of I, $F(i)$ is a subgroup of G and there exists a homomorphism h from $\operatorname{sum} F$ to G such that h is bijective and for every

finite-support function x from I into G such that $x \in \operatorname{sum} F$ holds $h(x) = \prod x$.

One can verify that there exists a direct sum components of G and I which is internal.

5. Equivalent Expression of Internal Direct Sum Decomposition

Now we state the propositions:

(44) Let us consider a group G, and a non empty subset A of G. Suppose for every elements x, y of G such that x, $y \in A$ holds $x \cdot y = y \cdot x$. Then $\operatorname{gr}(A)$ is commutative.

PROOF: For every elements x, y of G and for every elements i, j of $\mathbb{Z}$ such that x, $y \in A$ holds $x^i \cdot y^j = y^j \cdot x^i$ by [27, (39)]. For every element y of G and for every element j of $\mathbb{Z}$ such that $y \in A$ for every finite sequence F of elements of G for every finite sequence I of elements of $\mathbb{Z}$ such that $\operatorname{len} F = \operatorname{len} I$ and $\operatorname{rng} F \subseteq A$ holds $\prod F^I \cdot y^j = y^j \cdot \prod F^I$ by [29, (21), (8)], [32, (70)], [6, (4)]. For every elements x, g of G and for every element i of $\mathbb{Z}$ such that $x \in \operatorname{gr}(A)$ and $g \in A$ holds $x \cdot g^i = g^i \cdot x$ by [29, (28)]. For every element x of G such that $x \in \operatorname{gr}(A)$ for every finite sequence F of elements of G for every finite sequence I of elements of $\mathbb{Z}$ such that $\operatorname{len} F = \operatorname{len} I$ and $\operatorname{rng} F \subseteq A$ holds $\prod F^I \cdot x = x \cdot \prod F^I$ by [29, (21), (8)], [32, (70)], [6, (4)]. For every elements x, y of $\operatorname{gr}(A)$, $x \cdot y = y \cdot x$ by [28, (41)], [29, (28)], [28, (43)]. □

(45) Let us consider a group G, a subgroup H of G, a finite sequence a of elements of G, and a finite sequence b of elements of H. If $a = b$, then $\prod a = \prod b$.

PROOF: Define $\mathcal{P}$[natural number] ≡ for every finite sequence a of elements of G for every finite sequence b of elements of H such that $\operatorname{len} a = \$_1$ and $a = b$ holds $\prod a = \prod b$. $\mathcal{P}[0]$ by [29, (8)], [28, (44)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (4), (17)], [26, (55)], [29, (6)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

(46) Let us consider a group G, an element h of G, and a finite sequence F of elements of G. Suppose for every natural number k such that $k \in \operatorname{dom} F$ holds $h \cdot F_k = F_k \cdot h$. Then $h \cdot \prod F = \prod F \cdot h$.

PROOF: Define $\mathcal{P}$[natural number] ≡ for every finite sequence F of elements of G such that $\operatorname{len} F = \$_1$ and for every natural number i such that $i \in \operatorname{dom} F$ holds $h \cdot F_i = F_i \cdot h$ holds $h \cdot \prod F = \prod F \cdot h$. $\mathcal{P}[0]$ by [29, (8)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (4), (17), (5)], [14, (80)]. For every natural number i, $\mathcal{P}[i]$ from [4, Sch. 2]. □

(47) Let us consider a group G, and finite sequences F, F_1, F_2 of elements of G. Suppose $\operatorname{len} F = \operatorname{len} F_1$ and $\operatorname{len} F = \operatorname{len} F_2$ and for every natural numbers i, j such that $i, j \in \operatorname{dom} F$ and $i \neq j$ holds $F_{1i} \cdot F_{2j} = F_{2j} \cdot F_{1i}$ and for every natural number k such that $k \in \operatorname{dom} F$ holds $F(k) = F_{1k} \cdot F_{2k}$. Then $\prod F = \prod F_1 \cdot \prod F_2$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequences F, F_1, F_2 of elements of G such that $\operatorname{len} F = \$_1$ and $\operatorname{len} F = \operatorname{len} F_1$ and $\operatorname{len} F = \operatorname{len} F_2$ and for every natural numbers i, j such that $i, j \in \operatorname{dom} F$ and $i \neq j$ holds $F_{1i} \cdot F_{2j} = F_{2j} \cdot F_{1i}$ and for every natural number k such that $k \in \operatorname{dom} F$ holds $F(k) = F_{1k} \cdot F_{2k}$ holds $\prod F = \prod F_1 \cdot \prod F_2$. $\mathcal{P}[0]$ by [29, (8)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (4), (17), (5)], [14, (80)]. For every natural number i, $\mathcal{P}[i]$ from [4, Sch. 2]. □

(48) Let us consider a group G, and a finite sequence a of elements of G. Suppose for every object i such that $i \in \operatorname{dom} a$ holds $a(i) = \mathbf{1}_G$. Then $\prod a = \mathbf{1}_G$.

PROOF: Set $n = \operatorname{len} a$. $a = n \mapsto \mathbf{1}_G$ by [24, (13)], [9, (57)], [10, (2)]. □

(49) Let us consider a finite set I, a group G, and a (the carrier of G)-valued, total, I-defined function a. Suppose for every object i such that $i \in I$ holds $a(i) = \mathbf{1}_G$. Then $\prod a = \mathbf{1}_G$.

PROOF: Set $c_1 = \operatorname{CFS}(I)$. Set $a_2 = a \cdot c_1$. For every object i such that $i \in \operatorname{dom} a_2$ holds $a_2(i) = \mathbf{1}_G$ by [32, (27)], [10, (3), (12)]. □

(50) Let us consider a finite set A, a non empty set B, and a B-valued, total, A-defined function f. Then $f \cdot \operatorname{CFS}(A)$ is a finite sequence of elements of B.

Let us consider a non empty set I, a group G, a finite-support function a from I into G, and a finite subset W of I. Now we state the propositions:

(51) If $\operatorname{support} a \subseteq W$ and for every elements i, j of I, $a(i) \cdot a(j) = a(j) \cdot a(i)$, then $\prod a = \prod (a \restriction W)$.

PROOF: Reconsider $r = \operatorname{rng} a$ as a non empty subset of G. For every elements x, y of G such that $x, y \in r$ holds $x \cdot y = y \cdot x$ by [11, (113)]. □

(52) Suppose $\operatorname{support} a \subseteq W$. Then there exists a finite-support function a_1 from W into G such that

(i) $a_1 = a \restriction W$, and

(ii) $\operatorname{support} a = \operatorname{support} a_1$, and

(iii) $\prod a = \prod a_1$.

(53) Let us consider a non empty set I, a group G, a family F of groups of I, elements s_1, s_2 of $\operatorname{sum} F$, and finite-support functions x, y, x_3 from I into G. Suppose for every element i of I, $F(i)$ is a subgroup of G and for

every elements i, j of I and for every elements g_1, g_2 of G such that $i \neq j$ and $g_1 \in F(i)$ and $g_2 \in F(j)$ holds $g_1 \cdot g_2 = g_2 \cdot g_1$ and $s_1 = x$ and $s_2 = y$ and $s_1 \cdot s_2 = x_3$. Then $\prod x_3 = \prod x \cdot \prod y$.

PROOF: Reconsider $W = \operatorname{support} x \cup \operatorname{support} y$ as a finite subset of I. For every object i such that $i \in \operatorname{support} x_3$ holds $i \in W$ by (5), [28, (40), (43)], [17, (1)]. For every function a from I into G and for every elements i, j of I such that $a \in \prod F$ holds $a(i) \cdot a(j) = a(j) \cdot a(i)$. $\prod x = \prod (x \restriction W)$. $\prod y = \prod (y \restriction W)$. $\prod x_3 = \prod (x_3 \restriction W)$. Set $c_1 = \mathrm{CFS}(W)$. Reconsider $w_1 = (x \restriction W) \cdot c_1$ as a finite sequence of elements of G. Reconsider $w_3 = (y \restriction W) \cdot c_1$ as a finite sequence of elements of G. Reconsider $w_2 = (x_3 \restriction W) \cdot c_1$ as a finite sequence of elements of G. For every natural numbers i, j such that i, $j \in \operatorname{dom} w_2$ and $i \neq j$ holds $w_{1i} \cdot w_{3j} = w_{3j} \cdot w_{1i}$ by [10, (3), (12), (49)], (5). For every natural number i such that $i \in \operatorname{dom} w_2$ holds $w_2(i) = w_{1i} \cdot w_{3i}$ by [10, (3), (12), (49)], (5). $\prod w_2 = \prod w_1 \cdot \prod w_3$. □

(54) Let us consider a non empty set I, a group G, and a family F of groups of I. Then F is an internal direct sum components of G and I if and only if for every element i of I, $F(i)$ is a subgroup of G and for every elements i, j of I and for every elements g_1, g_2 of G such that $i \neq j$ and $g_1 \in F(i)$ and $g_2 \in F(j)$ holds $g_1 \cdot g_2 = g_2 \cdot g_1$ and for every element y of G, there exists a finite-support function x from I into G such that $x \in \operatorname{sum} F$ and $y = \prod x$ and for every finite-support functions x_1, x_2 from I into G such that x_1, $x_2 \in \operatorname{sum} F$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$.

PROOF: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists a finite-support function x from I into G such that $\$_1 = x$ and $\$_2 = \prod x$. For every element x of $\operatorname{sum} F$, there exists an element y of G such that $\mathcal{P}[x, y]$. Consider h being a function from $\operatorname{sum} F$ into G such that for every element x of $\operatorname{sum} F$, $\mathcal{P}[x, h(x)]$ from [11, Sch. 3]. For every object y such that $y \in \Omega_G$ there exists an object x such that $x \in \Omega_{\operatorname{sum} F}$ and $y = h(x)$. For every objects x_1, x_2 such that x_1, $x_2 \in \Omega_{\operatorname{sum} F}$ and $h(x_1) = h(x_2)$ holds $x_1 = x_2$. For every finite-support function a from I into G such that $a \in \operatorname{sum} F$ holds $h(a) = \prod a$. For every elements x, y of $\operatorname{sum} F$, $h(x \cdot y) = h(x) \cdot h(y)$. □

REFERENCES

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[3] Grzegorz Bancerek. Monoids. *Formalized Mathematics*, 3(**2**):213–225, 1992.
[4] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[5] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[7] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[8] Nicolas Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3*. Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.

[9] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[10] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[11] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[12] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(**1**):245–254, 1990.

[13] 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.

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

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

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

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

[18] Serge Lang. *Algebra*. Springer, 3rd edition, 2005.

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

[20] Hiroyuki Okazaki, Kenichi Arai, and Yasunari Shidama. Normal subgroup of product of groups. *Formalized Mathematics*, 19(**1**):23–26, 2011. doi:10.2478/v10037-011-0004-7.

[21] Hiroyuki Okazaki, Hiroshi Yamazaki, and Yasunari Shidama. Isomorphisms of direct products of finite commutative groups. *Formalized Mathematics*, 21(**1**):65–74, 2013. doi:10.2478/forma-2013-0007.

[22] D. Robinson. *A Course in the Theory of Groups*. Springer New York, 2012.

[23] J.J. Rotman. *An Introduction to the Theory of Groups*. Springer, 1995.

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

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

[26] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

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

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

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

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

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

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

[33] Katarzyna Zawadzka. Solvable groups. *Formalized Mathematics*, 5(**1**):145–147, 1996.

Received December 31, 2014

FORMALIZED MATHEMATICS
Vol. 23, No. 1, Pages 29–49, 2015
DOI: 10.2478/forma-2015-0003

DE GRUYTER OPEN
degruyter.com/view/j/forma

Matrix of $\mathbb{Z}$-module[1]

Yuichi Futa
Japan Advanced Institute
of Science and Technology
Ishikawa, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize a matrix of $\mathbb{Z}$-module and its properties. Specially, we formalize a matrix of a linear transformation of $\mathbb{Z}$-module, a bilinear form and a matrix of the bilinear form (Gramian matrix). We formally prove that for a finite-rank free $\mathbb{Z}$-module V, determinant of its Gramian matrix is constant regardless of selection of its basis. $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattices [22] and coding theory [14]. Some theorems in this article are described by translating theorems in [24], [26] and [19] into theorems of $\mathbb{Z}$-module.

MSC: 11E39 13C10 03B35

Keywords: matrix of Z-module; matrix of linear transformation; bilinear form

MML identifier: `ZMATRLIN`, version: `8.1.04 5.31.1231`

The notation and terminology used in this paper have been introduced in the following articles: [6], [1], [7], [5], [8], [13], [30], [9], [10], [2], [41], [34], [23], [31], [28], [27], [17], [42], [24], [25], [4], [11], [18], [39], [40], [35], [38], [21], [36], [37], [12], [15], and [16].

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

ISSN 1426–2630(Print), 1898-9934(Online)

1. Preliminaries

From now on x, y, z denote objects, i, j, k, l, n, m denote natural numbers, D, E denote non empty sets, M denotes a matrix over D, and L denotes a matrix over E.

Now we state the proposition:

(1) Let us consider natural numbers i, j. Suppose $M = L$ and $\langle i, j \rangle \in$ the indices of M. Then $M_{i,j} = L_{i,j}$.

Let us consider a natural number i. Now we state the propositions:

(2) If $M = L$ and $i \in \operatorname{dom} M$, then $\operatorname{Line}(M, i) = \operatorname{Line}(L, i)$.
Proof: For every j such that $j \in \operatorname{dom} \operatorname{Line}(M, i)$ holds $\operatorname{Line}(M, i)(j) = \operatorname{Line}(L, i)(j)$ by [12, (87)], (1). □

(3) If $M = L$ and $i \in \operatorname{Seg} \operatorname{width} M$, then $M_{\square,i} = L_{\square,i}$.
Proof: For every j such that $j \in \operatorname{dom} M_{\square,i}$ holds $M_{\square,i}(j) = L_{\square,i}(j)$ by [12, (87)], (1). □

Now we state the propositions:

(4) Suppose $\operatorname{len} M = \operatorname{len} L$ and $\operatorname{width} M = \operatorname{width} L$ and for every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} = L_{i,j}$. Then $M = L$.
Proof: M is a matrix over E by [12, (87)]. Reconsider $L_0 = M$ as a matrix over E. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of L_0 holds $L_{0i,j} = L_{i,j}$. □

(5) Let us consider a matrix M over D. Suppose for every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} \in E$. Then M is a matrix over E.

(6) If $M = L$, then $M^{\mathrm{T}} = L^{\mathrm{T}}$. The theorem is a consequence of (1) and (5).

(7) Every matrix over $\mathbb{Z}$ is a matrix over $\mathbb{R}$.

Let M be a matrix over $\mathbb{Z}$. The functor $\mathbb{Z}2\mathbb{R}(M)$ yielding a matrix over $\mathbb{R}$ is defined by the term

(Def. 1) M.

Let n, m be natural numbers and M be a matrix over $\mathbb{Z}$ of dimension $n \times m$. Let us note that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a matrix over $\mathbb{R}$ of dimension $n \times m$. Let n be a natural number and M be a square matrix over $\mathbb{Z}$ of dimension n. Observe that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a square matrix over $\mathbb{R}$ of dimension n. Let M be a matrix over $\mathbb{R}$. We say that M is integer if and only if

(Def. 2) M is a matrix over $\mathbb{Z}$.

One can verify that there exists a matrix over $\mathbb{R}$ which is integer.

Let n, m be natural numbers. Observe that there exists a matrix over $\mathbb{R}$ of dimension $n \times m$ which is integer.

Let M be an integer matrix over $\mathbb{R}$. The functor $\mathbb{R}2\mathbb{Z}(M)$ yielding a matrix over $\mathbb{Z}$ is defined by the term

(Def. 3) M.

Let n, m be natural numbers and M be an integer matrix over $\mathbb{R}$ of dimension $n \times m$. Let us note that the functor $\mathbb{R}2\mathbb{Z}(M)$ yields a matrix over $\mathbb{Z}$ of dimension $n \times m$. Let n be a natural number and M be an integer square matrix over $\mathbb{R}$ of dimension n. Observe that the functor $\mathbb{R}2\mathbb{Z}(M)$ yields a square matrix over $\mathbb{Z}$ of dimension n. Let n, m be natural numbers. The functor $0_n^{m \times m}$ yielding a matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $n \times m$ is defined by the term

(Def. 4) $n \mapsto (m \mapsto 0_{\mathbb{Z}^{\mathrm{R}}})$.

2. Sequences and Matrices Concerning Linear Transformations

In the sequel k, t, i, j, m, n denote natural numbers, D denotes a non empty set, V denotes a free $\mathbb{Z}$-module, a denotes an element of $\mathbb{Z}^{\mathrm{R}}$, W denotes an element of V, K_1, K_2, K_3 denote linear combinations of V, and X denotes a subset of V.

Now we state the propositions:

(8) Suppose X is linearly independent and the support of $K_1 \subseteq X$ and the support of $K_2 \subseteq X$ and the support of $K_3 \subseteq X$ and $\sum K_1 = \sum K_2 + \sum K_3$. Then $K_1 = K_2 + K_3$.

(9) Suppose X is linearly independent and the support of $K_1 \subseteq X$ and the support of $K_2 \subseteq X$ and $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $\sum K_1 = a \cdot \sum K_2$. Then $K_1 = a \cdot K_2$.

From now on V denotes a finite rank, free $\mathbb{Z}$-module, W denotes an element of V, K_1, K_2, K_3 denote linear combinations of V, and X denotes a subset of V.

Now we state the proposition:

(10) Let us consider a basis b_2 of V. Then there exists a linear combination K of V such that

(i) $W = \sum K$, and

(ii) the support of $K \subseteq b_2$.

Let V be a finite rank, free $\mathbb{Z}$-module.

An ordered basis of V is a finite sequence of elements of V and is defined by

(Def. 5) it is one-to-one and rng it is a basis of V.

From now on s denotes a finite sequence, V_1, V_2, V_3 denote finite rank, free $\mathbb{Z}$-modules, f, f_1, f_2 denote functions from V_1 into V_2, g denotes a function from V_2 into V_3, b_1 denotes an ordered basis of V_1, b_2 denotes an ordered basis of V_2, b_3 denotes an ordered basis of V_3, v_1, v_2 denote vectors of V_2, v, w denote elements of V_1, p_2, F denote finite sequences of elements of V_1, p_1, d denote finite sequences of elements of $\mathbb{Z}^{\mathrm{R}}$, and K denotes a linear combination of V_1.

Now we state the propositions:

(11) Let us consider an element a of V_1, a finite sequence F of elements of V_1, and a finite sequence G of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $\operatorname{len} F = \operatorname{len} G$ and for every k and for every element v of $\mathbb{Z}^{\mathrm{R}}$ such that $k \in \operatorname{dom} F$ and $v = G(k)$ holds $F(k) = v \cdot a$. Then $\sum F = \sum G \cdot a$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence H of elements of V_1 for every finite sequence I of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $\operatorname{len} H = \operatorname{len} I$ and $\operatorname{len} H = \$_1$ and for every k and for every element v of $\mathbb{Z}^{\mathrm{R}}$ such that $k \in \operatorname{dom} H$ and $v = I(k)$ holds $H(k) = v \cdot a$ holds $\sum H = \sum I \cdot a$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [5, (18)], [3, (12)], [5, (17)], [32, (30)]. $\mathcal{P}[0]$ by [35, (43)], [21, (14)]. For every n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(12) Let us consider an element a of V_1, a finite sequence F of elements of $\mathbb{Z}^{\mathrm{R}}$, and a finite sequence G of elements of V_1. Suppose $\operatorname{len} F = \operatorname{len} G$ and for every k such that $k \in \operatorname{dom} F$ holds $G(k) = F_k \cdot a$. Then $\sum G = \sum F \cdot a$. The theorem is a consequence of (11).

Let us consider V_1, p_1, and p_2. The functor $\operatorname{lmlt}(p_1, p_2)$ yielding a finite sequence of elements of V_1 is defined by the term

(Def. 6) (the left multiplication of V_1)$^{\circ}(p_1, p_2)$.

Now we state the propositions:

(13) If $\operatorname{dom} p_1 = \operatorname{dom} p_2$, then $\operatorname{dom} \operatorname{lmlt}(p_1, p_2) = \operatorname{dom} p_1$.

(14) Let us consider a matrix M over the carrier of V_1. If $\operatorname{len} M = 0$, then $\sum \sum M = 0_{V_1}$.

(15) Let us consider a matrix M over the carrier of V_1 of dimension $m+1 \times 0$. Then $\sum \sum M = 0_{V_1}$.

PROOF: For every k such that $k \in \operatorname{dom} \sum M$ holds $(\sum M)_k = 0_{V_1}$ by [32, (29)], [20, (2)], [35, (43)]. □

(16) Let us consider $\mathbb{Z}$-modules V_1, V_2, a function f from V_1 into V_2, and a finite sequence p of elements of V_1. If f is additive and homogeneous, then $f(\sum p) = \sum(f \cdot p)$.

PROOF: Define $\mathcal{P}$[finite sequence of elements of V_1] $\equiv f(\sum \$_1) = \sum(f \cdot \$_1)$. For every finite sequence p of elements of V_1 and for every element w of V_1 such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle w \rangle]$ by [35, (41), (44)], [7, (8)]. For every finite sequence p of elements of V_1, $\mathcal{P}[p]$ from [8, Sch. 2]. □

(17) Let us consider a finite sequence a of elements of $\mathbb{Z}^{\mathrm{R}}$, and a finite sequence p of elements of V_1. Suppose $\operatorname{len} p = \operatorname{len} a$. If f is additive and homogeneous, then $f \cdot \operatorname{lmlt}(a, p) = \operatorname{lmlt}(a, f \cdot p)$. The theorem is a consequence of (13).

(18) Let us consider a finite sequence a of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $\operatorname{len} a = \operatorname{len} b_2$ and g is additive and homogeneous. Then $g(\sum \operatorname{lmlt}(a, b_2)) = \sum \operatorname{lmlt}(a, g \cdot b_2)$. The theorem is a consequence of (16) and (17).

(19) Let us consider finite sequences F, F_1 of elements of V_1, a linear combination K of V_1, and a permutation p of $\operatorname{dom} F$. If $F_1 = F \cdot p$, then $K \cdot F_1 = (K \cdot F) \cdot p$.

(20) If F is one-to-one and the support of $K \subseteq \operatorname{rng} F$, then $\sum(K \cdot F) = \sum K$. PROOF: Reconsider $A =$ the support of K as a subset of $\operatorname{rng} F$. Consider p_1 being a permutation of $\operatorname{dom} F$ such that $(F - A^{\mathrm{c}}) \frown (F - A) = F \cdot p_1$. Reconsider $G_1 = F - A^{\mathrm{c}}$, $G_2 = F - A$ as a finite sequence of elements of V_1. For every k such that $k \in \operatorname{dom}(K \cdot G_2)$ holds $(K \cdot G_2)_k = 0_{V_1}$ by [32, (29), (65)], [15, (1)]. $K \cdot (G_1 \frown G_2) = (K \cdot F) \cdot p_1$. □

(21) Let us consider a set A, and a finite sequence p of elements of V_1. Suppose $\operatorname{rng} p \subseteq A$. Suppose f_1 is additive and homogeneous and f_2 is additive and homogeneous and for every v such that $v \in A$ holds $f_1(v) = f_2(v)$. Then $f_1(\sum p) = f_2(\sum p)$.
PROOF: Define $\mathcal{P}$[finite sequence of elements of V_1] $\equiv$ if $\operatorname{rng} \$_1 \subseteq A$, then $f_1(\sum \$_1) = f_2(\sum \$_1)$. For every finite sequence p of elements of V_1 and for every element x of V_1 such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \frown \langle x \rangle]$ by [5, (31), (39)], [35, (41), (44)]. $\mathcal{P}[\varepsilon_\alpha]$, where α is the carrier of V_1 by [35, (43)], [15, (1)]. For every finite sequence p of elements of V_1, $\mathcal{P}[p]$ from [8, Sch. 2]. □

(22) Suppose f_1 is additive and homogeneous and f_2 is additive and homogeneous. Let us consider an ordered basis b_1 of V_1. Suppose $\operatorname{len} b_1 > 0$. If $f_1 \cdot b_1 = f_2 \cdot b_1$, then $f_1 = f_2$. The theorem is a consequence of (20) and (21).

(23) Let us consider a matrix M_1 over the carrier of V of dimension $n \times k$, and a matrix M_2 over the carrier of V of dimension $m \times k$. Then $\sum(M_1 \frown M_2) = \sum M_1 \frown \sum M_2$.

(24) Let us consider matrices M_1, M_2 over the carrier of V_1. Then $\sum M_1 + \sum M_2 = \sum(M_1 \frown M_2)$.

(25) Let us consider finite sequences P_1, P_2 of elements of V_1. Suppose $\operatorname{len} P_1 = \operatorname{len} P_2$. Then $\sum(P_1 + P_2) = \sum P_1 + \sum P_2$.

(26) Let us consider matrices M_1, M_2 over the carrier of V_1. Suppose $\operatorname{len} M_1 = \operatorname{len} M_2$. Then $\sum\sum M_1 + \sum\sum M_2 = \sum\sum(M_1 \frown M_2)$. The theorem is a consequence of (25) and (24).

(27) Let us consider a matrix M over the carrier of V_1. Then $\sum\sum M = \sum\sum M^{\mathrm{T}}$.

PROOF: Define $\mathcal{X}$[natural number] $\equiv$ for every matrix M over the carrier of V_1 such that $\operatorname{len} M = \$_1$ holds $\sum\sum M = \sum\sum M^{\mathrm{T}}$. For every finite sequence P of elements of V_1, $\sum\sum\langle P\rangle = \sum\sum\langle P\rangle^{\mathrm{T}}$ by [5, (38), (6), (39)]. For every n such that $\mathcal{X}[n]$ holds $\mathcal{X}[n+1]$ by [5, (4), (40)], [24, (3), (2), (1)]. $\mathcal{X}[0]$. For every n, $\mathcal{X}[n]$ from [3, Sch. 2]. □

(28) Let us consider a matrix M over $\mathbb{Z}^{\mathrm{R}}$ of dimension $n\times m$. Suppose $n > 0$ and $m > 0$. Let us consider finite sequences p, d of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $\operatorname{len} p = n$ and $\operatorname{len} d = m$ and for every j such that $j \in \operatorname{dom} d$ holds $d_j = \sum(p \bullet M_{\square,j})$. Let us consider finite sequences b, c of elements of V_1. Suppose $\operatorname{len} b = m$ and $\operatorname{len} c = n$ and for every i such that $i \in \operatorname{dom} c$ holds $c_i = \sum \operatorname{lmlt}(\operatorname{Line}(M, i), b)$. Then $\sum \operatorname{lmlt}(p, c) = \sum \operatorname{lmlt}(d, b)$.

PROOF: Reconsider $n_1 = n$, $m_1 = m$ as an element of $\mathbb{N}$. Define $\mathcal{V}$(natural number, natural number) $= p_{\$_1} \cdot M_{\$_1,\$_2} \cdot b_{\$_2}$. Consider M_1 being a matrix over the carrier of V_1 of dimension $n_1\times m_1$ such that for every i and j such that $\langle i, j\rangle \in$ the indices of M_1 holds $M_{1i,j} = \mathcal{V}(i, j)$. $\operatorname{dom}\operatorname{lmlt}(d, b) = \operatorname{dom} b$. $\operatorname{dom}\operatorname{lmlt}(p, c) = \operatorname{dom} p$. □

3. Decomposition of a Vector in Basis

Let V be a finite rank, free $\mathbb{Z}$-module, b_1 be an ordered basis of V, and W be an element of V. The functor $W \to b_1$ yielding a finite sequence of elements of $\mathbb{Z}^{\mathrm{R}}$ is defined by

(Def. 7) $\operatorname{len} it = \operatorname{len} b_1$ and there exists a linear combination K of V such that $W = \sum K$ and the support of $K \subseteq \operatorname{rng} b_1$ and for every k such that $1 \leqslant k \leqslant \operatorname{len} it$ holds $it_k = K(b_{1k})$.

Now we state the propositions:

(29) If $v_1 \to b_2 = v_2 \to b_2$, then $v_1 = v_2$.

(30) $v = \sum \operatorname{lmlt}(v \to b_1, b_1)$. The theorem is a consequence of (13) and (20).

(31) If $\operatorname{len} d = \operatorname{len} b_1$, then $d = \sum \operatorname{lmlt}(d, b_1) \to b_1$.

PROOF: Define $\mathcal{X}$[element of V_1, element of $\mathbb{Z}^{\mathrm{R}}$] $\equiv$ if $\$_1 \in \operatorname{rng} b_1$, then for every k such that $k \in \operatorname{dom} b_1$ and $b_{1k} = \$_1$ holds $\$_2 = d_k$ and if $\$_1 \notin \operatorname{rng} b_1$, then $\$_2 = 0_{\mathbb{Z}^{\mathrm{R}}}$. For every v, there exists an element u of $\mathbb{Z}^{\mathrm{R}}$ such that $\mathcal{X}[v, u]$ by [20, (2)]. Consider K being a function from V_1 into the carrier of $\mathbb{Z}^{\mathrm{R}}$ such that for every v, $\mathcal{X}[v, K(v)]$ from [10, Sch. 3]. □

(32) Let us consider finite sequences a, d of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $\operatorname{len} a = \operatorname{len} b_1$. Let us consider a natural number j. Suppose $j \in \operatorname{dom} b_2$ and $\operatorname{len} d =$

$\operatorname{len} b_1$ and for every k such that $k \in \operatorname{dom} b_1$ holds $d(k) = (f(b_{1k}) \to b_2)_j$. If $\operatorname{len} b_1 > 0$, then $(\sum \operatorname{lmlt}(a, f \cdot b_1) \to b_2)_j = \sum(a \bullet d)$.

PROOF: Reconsider $B_3 = f \cdot b_1$ as a finite sequence of elements of V_2. Define $\mathcal{V}(\text{natural number}, \text{natural number}) = (B_{3\$_1} \to b_2)_{\$_2}$. Consider M being a matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ such that for every i and j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} = \mathcal{V}(i, j)$. Define $\mathcal{W}(\text{natural number}) = \sum(a \bullet M_{\square,\$_1})$. Consider d_1 being a finite sequence of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $\operatorname{len} d_1 = \operatorname{len} b_2$ and for every natural number j such that $j \in \operatorname{dom} d_1$ holds $d_{1j} = \mathcal{W}(j)$ from [33, Sch. 2]. □

4. MATRICES OF LINEAR TRANSFORMATIONS

Let V_1, V_2 be finite rank, free $\mathbb{Z}$-modules, f be a function from V_1 into V_2, b_1 be a finite sequence of elements of V_1, and b_2 be an ordered basis of V_2. The functor $\operatorname{AutMt}(f, b_1, b_2)$ yielding a matrix over $\mathbb{Z}^{\mathrm{R}}$ is defined by

(Def. 8) $\operatorname{len} it = \operatorname{len} b_1$ and for every k such that $k \in \operatorname{dom} b_1$ holds $it_k = f(b_{1k}) \to b_2$.

Now we state the propositions:

(33) If $\operatorname{len} b_1 = 0$, then $\operatorname{AutMt}(f, b_1, b_2) = \emptyset$.

(34) If $\operatorname{len} b_1 > 0$, then $\operatorname{width} \operatorname{AutMt}(f, b_1, b_2) = \operatorname{len} b_2$.

(35) Suppose f_1 is additive and homogeneous and f_2 is additive and homogeneous and $\operatorname{AutMt}(f_1, b_1, b_2) = \operatorname{AutMt}(f_2, b_1, b_2)$ and $\operatorname{len} b_1 > 0$. Then $f_1 = f_2$. The theorem is a consequence of (29) and (22).

(36) Let us consider a finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$, and a finite sequence G of elements of $\mathbb{Z}^{\mathrm{R}}$. If $F = G$, then $\sum F = \sum G$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$ for every finite sequence G of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $\operatorname{len} F = \$_1$ and $F = G$ holds $\sum F = \sum G$. $\mathcal{P}[0]$ by [35, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [5, (4)], [9, (3)], [5, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(37) Let us consider finite sequences p, q of elements of $\mathbb{Z}^{\mathrm{R}}$, and finite sequences p_1, q_1 of elements of $\mathbb{R}_{\mathrm{F}}$. If $p = p_1$ and $q = q_1$, then $p \cdot q = p_1 \cdot q_1$. The theorem is a consequence of (36).

(38) Suppose g is additive and homogeneous and $\operatorname{len} b_1 > 0$ and $\operatorname{len} b_2 > 0$. Then $\operatorname{AutMt}(g \cdot f, b_1, b_3) = \operatorname{AutMt}(f, b_1, b_2) \cdot \operatorname{AutMt}(g, b_2, b_3)$.

PROOF: $\operatorname{width} \operatorname{AutMt}(f, b_1, b_2) = \operatorname{len} b_2$. $\operatorname{width} \operatorname{AutMt}(g \cdot f, b_1, b_3) = \operatorname{len} b_3$. For every i and j such that $\langle i, j \rangle \in$ the indices of $\operatorname{AutMt}(g \cdot f, b_1, b_3)$ holds $(\operatorname{AutMt}(g \cdot f, b_1, b_3))_{i,j} = (\operatorname{AutMt}(f, b_1, b_2) \cdot \operatorname{AutMt}(g, b_2, b_3))_{i,j}$ by [12, (87)], [32, (29)], (34), [32, (25)]. □

(39) $\mathrm{AutMt}(f_1 + f_2, b_1, b_2) = \mathrm{AutMt}(f_1, b_1, b_2) + \mathrm{AutMt}(f_2, b_1, b_2)$.
PROOF: width $\mathrm{AutMt}(f_1, b_1, b_2) = \mathrm{width}\,\mathrm{AutMt}(f_2, b_1, b_2)$. width AutMt $(f_1 + f_2, b_1, b_2) = \mathrm{width}\,\mathrm{AutMt}(f_1, b_1, b_2)$. For every i and j such that $\langle i, j\rangle \in$ the indices of $\mathrm{AutMt}(f_1+f_2, b_1, b_2)$ holds $(\mathrm{AutMt}(f_1+f_2, b_1, b_2))_{i,j} = (\mathrm{AutMt}(f_1, b_1, b_2) + \mathrm{AutMt}(f_2, b_1, b_2))_{i,j}$ by [32, (29)], [12, (87)], (8), [36, (22)]. □

(40) If $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$, then $\mathrm{AutMt}(a \cdot f, b_1, b_2) = a \cdot \mathrm{AutMt}(f, b_1, b_2)$.
PROOF: width $\mathrm{AutMt}(a \cdot f, b_1, b_2) = \mathrm{width}\,\mathrm{AutMt}(f, b_1, b_2)$. For every i and j such that $\langle i, j\rangle \in$ the indices of $\mathrm{AutMt}(a \cdot f, b_1, b_2)$ holds $(\mathrm{AutMt}(a \cdot f, b_1, b_2))_{i,j} = (a \cdot \mathrm{AutMt}(f, b_1, b_2))_{i,j}$ by [32, (29)], [12, (87)], (9), [5, (1)]. □

(41) Let us consider non empty sets D, E, natural numbers n, m, i, j, and a matrix M over D of dimension $n \times m$. Suppose $0 < n$ and M is a matrix over E of dimension $n \times m$ and $\langle i, j\rangle \in$ the indices of M. Then $M_{i,j}$ is an element of E.

(42) Let us consider a finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose for every natural number i such that $i \in \mathrm{dom}\,F$ holds $F(i) \in \mathbb{Z}$. Then $\sum F \in \mathbb{Z}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$ such that $\mathrm{len}\,F = \$_1$ and for every natural number i such that $i \in \mathrm{dom}\,F$ holds $F(i) \in \mathbb{Z}$ holds $\sum F \in \mathbb{Z}$. $\mathcal{P}[0]$ by [35, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [5, (4)], [9, (3)], [5, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(43) Let us consider a natural number i, and an element j of $\mathbb{R}_{\mathrm{F}}$. Suppose $j \in \mathbb{Z}$. Then $\mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, i) \cdot j \in \mathbb{Z}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv \mathrm{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, \$_1) \cdot j \in \mathbb{Z}$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(44) Let us consider natural numbers n, i, j, k, m, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose $0 < n$ and M is a square matrix over $\mathbb{Z}$ of dimension $n+1$ and $\langle i, j\rangle \in$ the indices of M and $\langle k, m\rangle \in$ the indices of $\mathrm{Delete}(M, i, j)$. Then $(\mathrm{Delete}(M, i, j))_{k,m}$ is an element of $\mathbb{Z}$. The theorem is a consequence of (41).

(45) Let us consider natural numbers n, i, j, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose $0 < n$ and M is a square matrix over $\mathbb{Z}$ of dimension $n+1$ and $\langle i, j\rangle \in$ the indices of M. Then $\mathrm{Delete}(M, i, j)$ is a square matrix over $\mathbb{Z}$ of dimension n.
PROOF: Set $M_0 = \mathrm{Delete}(M, i, j)$. For every object x such that $x \in \mathrm{rng}\,M_0$ there exists a finite sequence p of elements of $\mathbb{Z}$ such that $x = p$ and $\mathrm{len}\,p = n$ by [12, (87)], (44). □

Let us consider a natural number n and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Now we state the propositions:

(46) If M is a square matrix over $\mathbb{Z}$ of dimension n, then $\operatorname{Det} M \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $\$_1$ such that M is a square matrix over $\mathbb{Z}$ of dimension $\$_1$ holds $\operatorname{Det} M \in \mathbb{Z}$. $\mathcal{P}[0]$ by [29, (41)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [3, (14)], [5, (1)], [27, (27)], [12, (87)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(47) If M is a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n, then $\operatorname{Det} M \in \mathbb{Z}$.

Now we state the proposition:

(48) Let us consider a finite rank, free $\mathbb{Z}$-module V, and a basis I of V. Then there exists an ordered basis J of V such that $\operatorname{rng} J = I$.

Let V be a $\mathbb{Z}$-module. One can check that id_V is additive and homogeneous.

Now we state the propositions:

(49) Let us consider a finite rank, free $\mathbb{Z}$-module V, and an ordered basis b of V. Then $\operatorname{len} b = \operatorname{rank} V$.

(50) Let us consider a finite rank, free $\mathbb{Z}$-module V, and ordered bases b_1, b_2 of V. Then $\operatorname{AutMt}(\mathrm{id}_V, b_1, b_2)$ is a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\operatorname{rank} V$. The theorem is a consequence of (49) and (34).

(51) Let us consider a finite rank, free $\mathbb{Z}$-module V, ordered bases b_1, b_2 of V, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $\operatorname{rank} V$. Suppose $M = \operatorname{AutMt}(\mathrm{id}_V, b_1, b_2)$. Then $\operatorname{Det} M \in \mathbb{Z}$. The theorem is a consequence of (46).

(52) Let us consider a finite rank, free $\mathbb{Z}$-module V_1, an ordered basis b_1 of V_1, and natural numbers i, j. Suppose $i, j \in \operatorname{dom} b_1$. Then

(i) if $i = j$, then $(b_{1i} \to b_1)(j) = 1$, and

(ii) if $i \neq j$, then $(b_{1i} \to b_1)(j) = 0$.

(53) Let us consider a finite rank, free $\mathbb{Z}$-module V, and an ordered basis b_1 of V. Suppose $\operatorname{rank} V > 0$. Then $\operatorname{AutMt}(\mathrm{id}_V, b_1, b_1) = I_{\mathbb{Z}^{\mathrm{R}}}^{(\operatorname{rank} V)\times(\operatorname{rank} V)}$. The theorem is a consequence of (49), (34), (52), and (4).

(54) Let us consider a finite rank, free $\mathbb{Z}$-module V, and ordered bases b_1, b_2 of V. Suppose $\operatorname{rank} V > 0$. Then $\operatorname{AutMt}(\mathrm{id}_V, b_1, b_2) \cdot \operatorname{AutMt}(\mathrm{id}_V, b_2, b_1) = I_{\mathbb{Z}^{\mathrm{R}}}^{(\operatorname{rank} V)\times(\operatorname{rank} V)}$. The theorem is a consequence of (49), (38), and (53).

(55) Let us consider a finite rank, free $\mathbb{Z}$-module V, ordered bases b_1, b_2 of V, and a square matrix M over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\operatorname{rank} V$. Suppose $M = \operatorname{AutMt}(\mathrm{id}_V, b_1, b_2)$. Then $|\operatorname{Det} M| = 1$. The theorem is a consequence of (49), (34), and (54).

5. Real-valued Function of $\mathbb{Z}$-Module

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Observe that there exists a functional in V which is additive, homogeneous, and 0-preserving.

A linear functional in V is an additive, homogeneous functional in V. Now we state the proposition:

(56) Let us consider an element a of $\mathbb{Z}^{\mathrm{R}}$, an add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structure V over $\mathbb{Z}^{\mathrm{R}}$, and a vector v of V. Then

(i) $0_{\mathbb{Z}^{\mathrm{R}}} \cdot v = 0_V$, and

(ii) $a \cdot 0_V = 0_V$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Note that there exists a functional in V which is additive and 0-preserving.

Let V be a right zeroed, non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Let us note that every functional in V which is additive is also 0-preserving.

Let V be an add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Note that every functional in V which is homogeneous is also 0-preserving.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Let us observe that 0Functional V is constant and there exists a functional in V which is constant.

Let V be a right zeroed, non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$ and f be a 0-preserving functional in V. Let us note that f is constant if and only if the condition (Def. 9) is satisfied.

(Def. 9) $f = 0\mathrm{Functional}\, V$.

Let us note that there exists a functional in V which is constant, additive, and 0-preserving.

Let V be a free $\mathbb{Z}$-module and A, B be subsets of V. Assume $A \subseteq B$ and B is a basis of V. The functor $\mathrm{Proj}(A, B)$ yielding a linear transformation from V to V is defined by

(Def. 10) for every vector v of V, there exist vectors v_6, v_7 of V such that $v_6 \in \mathrm{Lin}(A)$ and $v_7 \in \mathrm{Lin}(B \setminus A)$ and $v = v_6 + v_7$ and $it(v) = v_6$ and for every vectors v, v_6, v_7 of V such that $v_6 \in \mathrm{Lin}(A)$ and $v_7 \in \mathrm{Lin}(B \setminus A)$ and $v = v_6 + v_7$ holds $it(v) = v_6$.

Let B be a basis of V and u be a vector of V. The functor $\mathrm{Coordinate}(u, B)$ yielding a function from V into $\mathbb{Z}^{\mathrm{R}}$ is defined by

(Def. 11) for every vector v of V, there exists a linear combination L_2 of B such that $v = \sum L_2$ and $it(v) = L_2(u)$ and for every vector v of V and for every

linear combination L_3 of B such that $v = \sum L_3$ holds $it(v) = L_3(u)$ and for every vectors v_1, v_2 of V, $it(v_1 + v_2) = it(v_1) + it(v_2)$ and for every vector v of V and for every element r of $\mathbb{Z}^{\mathrm{R}}$, $it(r \cdot v) = r \cdot it(v)$.

Now we state the propositions:

(57) Let us consider a free $\mathbb{Z}$-module V, a basis B of V, and a vector u of V. Then $(\mathrm{Coordinate}(u, B))(0_V) = 0$.

(58) Let us consider a free $\mathbb{Z}$-module V, a basis X of V, and a vector v of V. If $v \in X$ and $v \neq 0_V$, then $(\mathrm{Coordinate}(v, X))(v) = 1$.

Let V be a non trivial, free $\mathbb{Z}$-module. One can verify that there exists a functional in V which is additive, homogeneous, non constant, and non trivial.

Now we state the proposition:

(59) Let us consider a non trivial, free $\mathbb{Z}$-module V, and a non constant, 0-preserving functional f in V. Then there exists a vector v of V such that

(i) $v \neq 0_V$, and

(ii) $f(v) \neq 0_{\mathbb{Z}^{\mathrm{R}}}$.

6. Bilinear Form of $\mathbb{Z}$-Module

Let V, W be vector space structures over $\mathbb{Z}^{\mathrm{R}}$. The functor $\mathrm{NulForm}(V, W)$ yielding a form of V, W is defined by the term

(Def. 12) (the carrier of V) $\times$ (the carrier of W) $\longmapsto 0_{\mathbb{Z}^{\mathrm{R}}}$.

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$ and f, g be forms of V, W. The functor $f + g$ yielding a form of V, W is defined by

(Def. 13) for every vector v of V and for every vector w of W, $it(v, w) = f(v, w) + g(v, w)$.

Let f be a form of V, W and a be an element of $\mathbb{Z}^{\mathrm{R}}$. The functor $a \cdot f$ yielding a form of V, W is defined by

(Def. 14) for every vector v of V and for every vector w of W, $it(v, w) = a \cdot f(v, w)$.

The functor $-f$ yielding a form of V, W is defined by

(Def. 15) for every vector v of V and for every vector w of W, $it(v, w) = -f(v, w)$.

Note that the functor $-f$ is defined by the term

(Def. 16) $(-1_{\mathbb{Z}^{\mathrm{R}}}) \cdot f$.

Let f, g be forms of V, W. The functor $f - g$ yielding a form of V, W is defined by the term

(Def. 17) $f + -g$.

One can verify that the functor $f - g$ is defined by

(Def. 18) for every vector v of V and for every vector w of W, $it(v, w) = f(v, w) - g(v, w)$.

Let us observe that the functor $f + g$ is commutative.

Now we state the propositions:

(60) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a form f of V, W. Then $f + \mathrm{NulForm}(V, W) = f$.

(61) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and forms f, g, h of V, W. Then $(f + g) + h = f + (g + h)$.

(62) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a form f of V, W. Then $f - f = \mathrm{NulForm}(V, W)$.

(63) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an element a of $\mathbb{Z}^{\mathrm{R}}$, and forms f, g of V, W. Then $a \cdot (f + g) = a \cdot f + a \cdot g$.

Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, elements a, b of $\mathbb{Z}^{\mathrm{R}}$, and a form f of V, W. Now we state the propositions:

(64) $(a + b) \cdot f = a \cdot f + b \cdot f$.

(65) $(a \cdot b) \cdot f = a \cdot (b \cdot f)$.

Now we state the proposition:

(66) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a form f of V, W. Then $1_{\mathbb{Z}^{\mathrm{R}}} \cdot f = f$.

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$, f be a form of V, W, and v be a vector of V. The functor $f(v, \cdot)$ yielding a functional in W is defined by the term

(Def. 19) $(\mathrm{curry}\, f)(v)$.

Let w be a vector of W. The functor $f(\cdot, w)$ yielding a functional in V is defined by the term

(Def. 20) $(\mathrm{curry}'\, f)(w)$.

Now we state the propositions:

(67) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a form f of V, W, and a vector v of V. Then

(i) $\mathrm{dom}\, f(v, \cdot) =$ the carrier of W, and

(ii) $\mathrm{rng}\, f(v, \cdot) \subseteq$ the carrier of $\mathbb{Z}^{\mathrm{R}}$, and

(iii) for every vector w of W, $(f(v, \cdot))(w) = f(v, w)$.

(68) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a form f of V, W, and a vector w of W. Then

(i) $\mathrm{dom}\, f(\cdot, w) =$ the carrier of V, and

(ii) $\operatorname{rng} f(\cdot, w) \subseteq$ the carrier of $\mathbb{Z}^{\mathrm{R}}$, and

(iii) for every vector v of V, $(f(\cdot, w))(v) = f(v, w)$.

(69) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a vector v of V. Then $\operatorname{NulForm}(V, W)(v, \cdot) = 0\operatorname{Functional} W$. The theorem is a consequence of (67).

(70) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a vector w of W. Then $\operatorname{NulForm}(V, W)(\cdot, w) = 0\operatorname{Functional} V$. The theorem is a consequence of (68).

(71) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, forms f, g of V, W, and a vector w of W. Then $(f + g)(\cdot, w) = f(\cdot, w) + g(\cdot, w)$. The theorem is a consequence of (68).

(72) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, forms f, g of V, W, and a vector v of V. Then $(f + g)(v, \cdot) = f(v, \cdot) + g(v, \cdot)$. The theorem is a consequence of (67).

(73) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a form f of V, W, an element a of $\mathbb{Z}^{\mathrm{R}}$, and a vector w of W. Then $(a \cdot f)(\cdot, w) = a \cdot f(\cdot, w)$. The theorem is a consequence of (68).

(74) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a form f of V, W, an element a of $\mathbb{Z}^{\mathrm{R}}$, and a vector v of V. Then $(a \cdot f)(v, \cdot) = a \cdot f(v, \cdot)$. The theorem is a consequence of (67).

(75) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a form f of V, W, and a vector w of W. Then $(-f)(\cdot, w) = -f(\cdot, w)$. The theorem is a consequence of (68).

(76) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a form f of V, W, and a vector v of V. Then $(-f)(v, \cdot) = -f(v, \cdot)$. The theorem is a consequence of (67).

(77) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, forms f, g of V, W, and a vector w of W. Then $(f - g)(\cdot, w) = f(\cdot, w) - g(\cdot, w)$. The theorem is a consequence of (68).

(78) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, forms f, g of V, W, and a vector v of V. Then $(f - g)(v, \cdot) = f(v, \cdot) - g(v, \cdot)$. The theorem is a consequence of (67).

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$, f be a functional in V, and g be a functional in W. The functor $f \otimes g$ yielding a form of V, W is defined by

(Def. 21) for every vector v of V and for every vector w of W, $it(v, w) = f(v) \cdot g(w)$.

Now we state the propositions:

(79) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a functional f in V, a vector v of V, and a vector w of W. Then $f \otimes (0\mathrm{Functional}\, W)(v, w) = 0$.

(80) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a functional g in W, a vector v of V, and a vector w of W. Then $(0\mathrm{Functional}\, V) \otimes g(v, w) = 0$.

(81) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a functional f in V. Then $f \otimes (0\mathrm{Functional}\, W) = \mathrm{NulForm}(V, W)$. The theorem is a consequence of (79).

(82) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a functional g in W. Then $(0\mathrm{Functional}\, V) \otimes g = \mathrm{NulForm}(V, W)$. The theorem is a consequence of (80).

(83) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a functional f in V, a functional g in W, and a vector v of V. Then $f \otimes g(v, \cdot) = f(v) \cdot g$. The theorem is a consequence of (67).

(84) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a functional f in V, a functional g in W, and a vector w of W. Then $f \otimes g(\cdot, w) = g(w) \cdot f$. The theorem is a consequence of (68).

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$ and f be a form of V, W. We say that f is additive w.r.t. second argument if and only if

(Def. 22) for every vector v of V, $f(v, \cdot)$ is additive.

We say that f is additive w.r.t. first argument if and only if

(Def. 23) for every vector w of W, $f(\cdot, w)$ is additive.

We say that f is homogeneous w.r.t. second argument if and only if

(Def. 24) for every vector v of V, $f(v, \cdot)$ is homogeneous.

We say that f is homogeneous w.r.t. first argument if and only if

(Def. 25) for every vector w of W, $f(\cdot, w)$ is homogeneous.

One can check that $\mathrm{NulForm}(V, W)$ is additive w.r.t. second argument and $\mathrm{NulForm}(V, W)$ is additive w.r.t. first argument and $\mathrm{NulForm}(V, W)$ is homogeneous w.r.t. second argument and $\mathrm{NulForm}(V, W)$ is homogeneous w.r.t. first argument and there exists a form of V, W which is additive w.r.t. second argument, homogeneous w.r.t. second argument, additive w.r.t. first argument, and homogeneous w.r.t. first argument.

A bilinear form of V, W is an additive w.r.t. first argument, homogeneous w.r.t. first argument, additive w.r.t. second argument, homogeneous w.r.t. second argument form of V, W. Let f be an additive w.r.t. second argument form of V, W and v be a vector of V. Note that $f(v, \cdot)$ is additive.

Let f be an additive w.r.t. first argument form of V, W and w be a vector of W. Let us observe that $f(\cdot, w)$ is additive.

Let f be a homogeneous w.r.t. second argument form of V, W and v be a vector of V. Note that $f(v, \cdot)$ is homogeneous.

Let f be a homogeneous w.r.t. first argument form of V, W and w be a vector of W. Let us observe that $f(\cdot, w)$ is homogeneous.

Let f be a functional in V and g be an additive functional in W. Let us observe that $f \otimes g$ is additive w.r.t. second argument.

Let f be an additive functional in V and g be a functional in W. Note that $f \otimes g$ is additive w.r.t. first argument.

Let f be a functional in V and g be a homogeneous functional in W. Let us observe that $f \otimes g$ is homogeneous w.r.t. second argument.

Let f be a homogeneous functional in V and g be a functional in W. Note that $f \otimes g$ is homogeneous w.r.t. first argument.

Let V be a non trivial vector space structure over $\mathbb{Z}^{\mathrm{R}}$, W be a $\mathbb{Z}$-module, and f be a functional in V. Note that $f \otimes g$ is non trivial.

Let W be a non trivial $\mathbb{Z}$-module. One can verify that $f \otimes g$ is non trivial.

Let V, W be non trivial, free $\mathbb{Z}$-modules, f be a non constant, 0-preserving functional in V, and g be a non constant, 0-preserving functional in W. Let us note that $f \otimes g$ is non constant and there exists a form of V, W which is non trivial, non constant, additive w.r.t. second argument, homogeneous w.r.t. second argument, additive w.r.t. first argument, and homogeneous w.r.t. first argument.

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathrm{R}}$ and f, g be additive w.r.t. first argument forms of V, W. One can check that $f + g$ is additive w.r.t. first argument.

Let f, g be additive w.r.t. second argument forms of V, W. Let us note that $f + g$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument form of V, W and a be an element of $\mathbb{Z}^{\mathrm{R}}$. One can check that $a \cdot f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument form of V, W. Observe that $a \cdot f$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument form of V, W. One can check that $-f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument form of V, W. One can check that $-f$ is additive w.r.t. second argument.

Let f, g be additive w.r.t. first argument forms of V, W. One can verify that $f - g$ is additive w.r.t. first argument.

Let f, g be additive w.r.t. second argument forms of V, W. Let us note that $f - g$ is additive w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument forms of V, W. One can verify that $f + g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument forms of V, W. Note that $f + g$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument form of V, W and a be an element of $\mathbb{Z}^{\mathrm{R}}$. One can verify that $a \cdot f$ is homogeneous w.r.t. first argument.

Let f be a homogeneous w.r.t. second argument form of V, W. Let us note that $a \cdot f$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument form of V, W. One can verify that $-f$ is homogeneous w.r.t. first argument.

Let f be a homogeneous w.r.t. second argument form of V, W. One can verify that $-f$ is homogeneous w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument forms of V, W. Let us observe that $f - g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument forms of V, W. Note that $f - g$ is homogeneous w.r.t. second argument.

Now we state the propositions:

(85) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, vectors v, u of V, a vector w of W, and a form f of V, W. If f is additive w.r.t. first argument, then $f(v + u, w) = f(v, w) + f(u, w)$. The theorem is a consequence of (68).

(86) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a vector v of V, vectors u, w of W, and a form f of V, W. If f is additive w.r.t. second argument, then $f(v, u + w) = f(v, u) + f(v, w)$. The theorem is a consequence of (67).

(87) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, vectors v, u of V, vectors w, t of W, and an additive w.r.t. first argument, additive w.r.t. second argument form f of V, W. Then $f(v + u, w + t) = f(v, w) + f(v, t) + (f(u, w) + f(u, t))$. The theorem is a consequence of (85) and (86).

(88) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an additive w.r.t. second argument form f of V, W, and a vector v of V. Then $f(v, 0_W) = 0$. The theorem is a consequence of (86).

(89) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, an additive w.r.t. first argument form f of V, W, and a vector w of W. Then $f(0_V, w) = 0$. The theorem is a consequence of (85).

Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a vector v of V, a vector w of W, an element a of $\mathbb{Z}^{\mathrm{R}}$, and a form f of V, W. Now we state the propositions:

(90) If f is homogeneous w.r.t. first argument, then $f(a \cdot v, w) = a \cdot f(v, w)$. The theorem is a consequence of (68).

(91) If f is homogeneous w.r.t. second argument, then $f(v, a \cdot w) = a \cdot f(v, w)$. The theorem is a consequence of (67).

Now we state the propositions:

(92) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a homogeneous w.r.t. first argument form f of V, W, and a vector w of W. Then $f(0_V, w) = 0_{\mathbb{Z}^{\mathrm{R}}}$. The theorem is a consequence of (56) and (90).

(93) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, a homogeneous w.r.t. second argument form f of V, W, and a vector v of V. Then $f(v, 0_W) = 0_{\mathbb{Z}^{\mathrm{R}}}$. The theorem is a consequence of (56) and (91).

(94) Let us consider $\mathbb{Z}$-modules V, W, vectors v, u of V, a vector w of W, and an additive w.r.t. first argument, homogeneous w.r.t. first argument form f of V, W. Then $f(v - u, w) = f(v, w) - f(u, w)$. The theorem is a consequence of (85) and (90).

(95) Let us consider $\mathbb{Z}$-modules V, W, a vector v of V, vectors w, t of W, and an additive w.r.t. second argument, homogeneous w.r.t. second argument form f of V, W. Then $f(v, w - t) = f(v, w) - f(v, t)$. The theorem is a consequence of (86) and (91).

(96) Let us consider $\mathbb{Z}$-modules V, W, vectors v, u of V, vectors w, t of W, and a bilinear form f of V, W. Then $f(v - u, w - t) = f(v, w) - f(v, t) - (f(u, w) - f(u, t))$. The theorem is a consequence of (94) and (95).

(97) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, vectors v, u of V, vectors w, t of W, elements a, b of $\mathbb{Z}^{\mathrm{R}}$, and a bilinear form f of V, W. Then $f(v + a \cdot u, w + b \cdot t) = f(v, w) + b \cdot f(v, t) + (a \cdot f(u, w) + a \cdot (b \cdot f(u, t)))$. The theorem is a consequence of (87), (91), and (90).

(98) Let us consider $\mathbb{Z}$-modules V, W, vectors v, u of V, vectors w, t of W, elements a, b of $\mathbb{Z}^{\mathrm{R}}$, and a bilinear form f of V, W. Then $f(v - a \cdot u, w - b \cdot t) = f(v, w) - b \cdot f(v, t) - (a \cdot f(u, w) - a \cdot (b \cdot f(u, t)))$. The theorem is a consequence of (96), (91), and (90).

(99) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathrm{R}}$, and a form f of V, W. Suppose f is additive w.r.t. second argument or additive w.r.t. first argument. Then f is constant if and only

if for every vector v of V and for every vector w of W, $f(v,w)=0$. The theorem is a consequence of (88) and (89).

7. Matrix of Bilinear Form

Let V_1, V_2 be finite rank, free $\mathbb{Z}$-modules, b_1 be an ordered basis of V_1, b_2 be an ordered basis of V_2, and f be a bilinear form of V_1, V_2. The functor $\mathrm{Bilinear}(f,b_1,b_2)$ yielding a matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension $\operatorname{len} b_1 \times \operatorname{len} b_2$ is defined by

(Def. 26) for every natural numbers i, j such that $i \in \operatorname{dom} b_1$ and $j \in \operatorname{dom} b_2$ holds $it_{i,j} = f(b_{1i}, b_{2j})$.

Now we state the propositions:

(100) Let us consider a finite rank, free $\mathbb{Z}$-module V, a natural number i, an element a_1 of $\mathbb{Z}^{\mathrm{R}}$, an element a_2 of V, a finite sequence p_1 of elements of $\mathbb{Z}^{\mathrm{R}}$, and a finite sequence p_2 of elements of V. Suppose $i \in \operatorname{dom} \mathrm{lmlt}(p_1,p_2)$ and $a_1 = p_1(i)$ and $a_2 = p_2(i)$. Then $(\mathrm{lmlt}(p_1,p_2))(i) = a_1 \cdot a_2$.

(101) Let us consider a finite rank, free $\mathbb{Z}$-module V, a linear functional F in V, a finite sequence y of elements of V, a finite sequence x of elements of $\mathbb{Z}^{\mathrm{R}}$, and finite sequences X, Y of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $X = x$ and $\operatorname{len} y = \operatorname{len} x$ and $\operatorname{len} X = \operatorname{len} Y$ and for every natural number k such that $k \in \operatorname{Seg} \operatorname{len} x$ holds $Y(k) = F(y_k)$. Then $X \cdot Y = F(\sum \mathrm{lmlt}(x,y))$.

Proof: Define $\mathcal{P}[\text{finite sequence of elements of } V] \equiv$ for every finite sequence x of elements of $\mathbb{Z}^{\mathrm{R}}$ for every finite sequences X, Y of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $X = x$ and $\operatorname{len} \$_1 = \operatorname{len} x$ and $\operatorname{len} X = \operatorname{len} Y$ and for every natural number k such that $k \in \operatorname{Seg} \operatorname{len} x$ holds $Y(k) = F(\$_{1k})$ holds $X \cdot Y = F(\sum \mathrm{lmlt}(x, \$_1))$. For every finite sequence y of elements of V and for every element w of V such that $\mathcal{P}[y]$ holds $\mathcal{P}[y \frown \langle w \rangle]$ by [5, (22), (39), (59)], [3, (11)]. $\mathcal{P}[\varepsilon_\alpha]$, where α is the carrier of V by [35, (43)]. For every finite sequence p of elements of V, $\mathcal{P}[p]$ from [8, Sch. 2]. □

(102) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_2 of V_2, an ordered basis b_3 of V_2, a bilinear form f of V_1, V_2, a vector v_1 of V_1, a vector v_2 of V_2, and finite sequences X, Y of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $\operatorname{len} X = \operatorname{len} b_2$ and $\operatorname{len} Y = \operatorname{len} b_2$ and for every natural number k such that $k \in \operatorname{Seg} \operatorname{len} b_2$ holds $Y(k) = f(v_1, b_{2k})$ and $X = v_2 \to b_2$. Then $Y \cdot X = f(v_1, v_2)$. The theorem is a consequence of (67), (101), and (30).

(103) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_1 of V_1, a bilinear form f of V_1, V_2, a vector v_1 of V_1, a vector v_2 of V_2, and finite sequences X, Y of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $\operatorname{len} X = \operatorname{len} b_1$ and $\operatorname{len} Y = \operatorname{len} b_1$ and for every natural number k such that $k \in \operatorname{Seg} \operatorname{len} b_1$

holds $Y(k) = f(b_{1k}, v_2)$ and $X = v_1 \to b_1$. Then $X \cdot Y = f(v_1, v_2)$. The theorem is a consequence of (68), (101), and (30).

(104) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_1 of V_1, an ordered basis b_2 of V_2, an ordered basis b_3 of V_2, and a bilinear form f of V_1, V_2. Suppose $0 < \operatorname{rank} V_1$. Then $\operatorname{Bilinear}(f, b_1, b_3) = \operatorname{Bilinear}(f, b_1, b_2) \cdot (\operatorname{AutMt}(\mathrm{id}_{V_2}, b_3, b_2))^{\mathrm{T}}$.

PROOF: Set $n = \operatorname{len} b_2$. $\operatorname{len} b_2 = \operatorname{rank} V_2$. $\operatorname{len} b_3 = \operatorname{rank} V_2$. Reconsider $I_1 = \operatorname{AutMt}(\mathrm{id}_{V_2}, b_3, b_2)$ as a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n. Reconsider $M_1 = {I_1}^{\mathrm{T}}$ as a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n. Set $M_2 = \operatorname{Bilinear}(f, b_1, b_2) \cdot M_1$. $0 < \operatorname{len} b_1$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\operatorname{Bilinear}(f, b_1, b_3)$ holds $(\operatorname{Bilinear}(f, b_1, b_3))_{i,j} = M_{2i,j}$ by [12, (87)], [5, (1)], (102). □

(105) Let us consider finite rank, free $\mathbb{Z}$-modules V_1, V_2, an ordered basis b_1 of V_1, an ordered basis b_2 of V_2, an ordered basis b_3 of V_1, and a bilinear form f of V_1, V_2. Suppose $0 < \operatorname{rank} V_1$. Then $\operatorname{Bilinear}(f, b_3, b_2) = \operatorname{AutMt}(\mathrm{id}_{V_1}, b_3, b_1) \cdot \operatorname{Bilinear}(f, b_1, b_2)$.

PROOF: Set $n = \operatorname{len} b_3$. $\operatorname{len} b_1 = \operatorname{rank} V_1$. $\operatorname{len} b_3 = \operatorname{rank} V_1$. Reconsider $I_1 = \operatorname{AutMt}(\mathrm{id}_{V_1}, b_3, b_1)$ as a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n. Reconsider $M_1 = I_1$ as a square matrix over $\mathbb{Z}^{\mathrm{R}}$ of dimension n. Set $M_2 = M_1 \cdot \operatorname{Bilinear}(f, b_1, b_2)$. $0 < \operatorname{len} b_1$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\operatorname{Bilinear}(f, b_3, b_2)$ holds $(\operatorname{Bilinear}(f, b_3, b_2))_{i,j} = M_{2i,j}$ by [12, (87)], [5, (1)], (103). □

Let us consider a finite rank, free $\mathbb{Z}$-module V, ordered bases b_1, b_2 of V, and a bilinear form f of V, V. Now we state the propositions:

(106) Suppose $0 < \operatorname{rank} V$. Then $\operatorname{Bilinear}(f, b_2, b_2) = \operatorname{AutMt}(\mathrm{id}_V, b_2, b_1) \cdot \operatorname{Bilinear}(f, b_1, b_1) \cdot (\operatorname{AutMt}(\mathrm{id}_V, b_2, b_1))^{\mathrm{T}}$. The theorem is a consequence of (49), (50), (105), and (104).

(107) $|\operatorname{Det} \operatorname{Bilinear}(f, b_2, b_2)| = |\operatorname{Det} \operatorname{Bilinear}(f, b_1, b_1)|$. The theorem is a consequence of (49), (106), (50), and (55).

REFERENCES

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

[2] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(**3**): 537–541, 1990.

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

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

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

[6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[7] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.
[8] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 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] Wolfgang Ebeling. *Lattices and Codes*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.
[15] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.
[16] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Free $\mathbb{Z}$-module. *Formalized Mathematics*, 20(**4**):275–280, 2012. doi:10.2478/v10037-012-0033-x.
[17] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2 (**4**):475–480, 1991.
[18] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[19] Jarosław Kotowicz. Bilinear functionals in vector spaces. *Formalized Mathematics*, 11(**1**): 69–86, 2003.
[20] Jarosław Kotowicz. Partial functions from a domain to a domain. *Formalized Mathematics*, 1(**4**):697–702, 1990.
[21] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[22] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: a cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.
[23] Anna Justyna Milewska. The Hahn Banach theorem in the vector space over the field of complex numbers. *Formalized Mathematics*, 9(**2**):363–371, 2001.
[24] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(**3**):339–345, 1996.
[25] Michał Muzalewski. Rings and modules – part II. *Formalized Mathematics*, 2(**4**):579–585, 1991.
[26] Bogdan Nowak and Andrzej Trybulec. Hahn-Banach theorem. *Formalized Mathematics*, 4(**1**):29–34, 1993.
[27] Karol Pąk and Andrzej Trybulec. Laplace expansion. *Formalized Mathematics*, 15(**3**): 143–150, 2007. doi:10.2478/v10037-007-0016-5.
[28] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[29] Nobuyuki Tamura and Yatsuka Nakamura. Determinant and inverse of matrices of real elements. *Formalized Mathematics*, 15(**3**):127–136, 2007. doi:10.2478/v10037-007-0014-7.
[30] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.
[31] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[32] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.
[33] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[34] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[35] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[36] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1

(**5**):877–882, 1990.

[37] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.

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

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

[40] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

[41] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(**2**):205–211, 1992.

[42] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(**1**):1–8, 1993.

Received February 18, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 1, Pages 51–57, 2015
DOI: 10.2478/forma-2015-0004

DE GRUYTER OPEN
degruyter.com/view/j/forma

σ-ring and σ-algebra of Sets[1]

Noboru Endou
Gifu National College of Technology
Gifu, Japan

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, semiring and semialgebra of sets are formalized so as to construct a measure of a given set in the next step. Although a semiring of sets has already been formalized in [13], that is, strictly speaking, a definition of a quasi semiring of sets suggested in the last few decades [15]. We adopt a classical definition of a semiring of sets here to avoid such a confusion. Ring of sets and algebra of sets have been formalized as non empty preboolean set [23] and field of subsets [18], respectively. In the second section, definitions of a ring and a σ-ring of sets, which are based on a semiring and a ring of sets respectively, are formalized and their related theorems are proved. In the third section, definitions of an algebra and a σ-algebra of sets, which are based on a semialgebra and an algebra of sets respectively, are formalized and their related theorems are proved. In the last section, mutual relationships between σ-ring and σ-algebra of sets are formalized and some related examples are given. The formalization is based on [15], and also referred to [9] and [16].

MSC: 03E30 28A05 03B35

Keywords: semiring of sets; σ-ring of sets; σ-algebra of sets

MML identifier: SRINGS_3, version: 8.1.04 5.31.1231

The notation and terminology used in this paper have been introduced in the following articles: [1], [2], [3], [17], [21], [6], [14], [23], [10], [11], [7], [8], [22], [4], [5], [18], [19], [26], [27], [20], [13], [25], and [12].

[1]This work was supported by JSPS KAKENHI 23500029 and 22300285.

ISSN 1426–2630(Print), 1898-9934(Online)

1. Preliminaries

Now we state the propositions:

(1) Let us consider finite sequences f_1, f_2, and a natural number k. Suppose $k \in \mathrm{Seg}(\mathrm{len}\, f_1 \cdot \mathrm{len}\, f_2)$. Then

(i) $(k -' 1 \bmod \mathrm{len}\, f_2) + 1 \in \mathrm{dom}\, f_2$, and

(ii) $(k -' 1 \,\mathrm{div}\, \mathrm{len}\, f_2) + 1 \in \mathrm{dom}\, f_1$.

(2) Let us consider a non empty, finite set S. Then $\bigcup \mathrm{CFS}(S) = \bigcup S$.

(3) Let us consider an object x. Then $\langle x \rangle$ is a disjoint valued finite sequence.

(4) Let us consider sets x, y, and a finite sequence F. If $F = \langle x, y \rangle$ and x misses y, then F is disjoint valued.

(5) Let us consider finite sequences f_1, f_2. Then there exists a finite sequence f such that

(i) $\bigcup f_1 \cap \bigcup f_2 = \bigcup f$, and

(ii) $\mathrm{dom}\, f = \mathrm{Seg}(\mathrm{len}\, f_1 \cdot \mathrm{len}\, f_2)$, and

(iii) for every natural number i such that $i \in \mathrm{dom}\, f$ holds $f(i) = f_1((i -' 1 \,\mathrm{div}\, \mathrm{len}\, f_2) + 1) \cap f_2((i -' 1 \bmod \mathrm{len}\, f_2) + 1)$.

Proof: For every natural number k such that $k \in \mathrm{Seg}(\mathrm{len}\, f_1 \cdot \mathrm{len}\, f_2)$ holds $(k -' 1 \bmod \mathrm{len}\, f_2) + 1 \in \mathrm{dom}\, f_2$ and $(k -' 1 \,\mathrm{div}\, \mathrm{len}\, f_2) + 1 \in \mathrm{dom}\, f_1$. Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv \$_2 = f_1((\$_1 -' 1 \,\mathrm{div}\, \mathrm{len}\, f_2) + 1) \cap f_2((\$_1 -' 1 \bmod \mathrm{len}\, f_2) + 1)$. Consider f being a finite sequence such that $\mathrm{dom}\, f = \mathrm{Seg}(\mathrm{len}\, f_1 \cdot \mathrm{len}\, f_2)$ and for every natural number k such that $k \in \mathrm{Seg}(\mathrm{len}\, f_1 \cdot \mathrm{len}\, f_2)$ holds $\mathcal{P}[k, f(k)]$ from [6, Sch. 1]. □

(6) Let us consider disjoint valued finite sequences f_1, f_2. Then there exists a disjoint valued finite sequence f such that

(i) $\bigcup f_1 \cap \bigcup f_2 = \bigcup f$, and

(ii) $\mathrm{dom}\, f = \mathrm{Seg}(\mathrm{len}\, f_1 \cdot \mathrm{len}\, f_2)$, and

(iii) for every natural number i such that $i \in \mathrm{dom}\, f$ holds $f(i) = f_1((i -' 1 \,\mathrm{div}\, \mathrm{len}\, f_2) + 1) \cap f_2((i -' 1 \bmod \mathrm{len}\, f_2) + 1)$.

The theorem is a consequence of (5).

(7) Let us consider a set X, and a non empty, \-closed family S of subsets of X. Then $\emptyset \in S$.

Let X be a set. One can check that every family of subsets of X which is non empty and \-closed has also the empty element.

2. Classical Semiring, Ring and σ-ring of Sets

Let I_1 be a set. We say that I_1 is semi \-closed if and only if

(Def. 1) for every sets X, Y such that X, $Y \in I_1$ there exists a disjoint valued finite sequence F of elements of I_1 such that $X \setminus Y = \bigcup F$.

Let X be a set. Let us note that 2^X is semi \-closed and there exists a family of subsets of X which is non empty, semi \-closed, and $\cap$-closed and there exists a family of subsets of X which is semi \-closed and $\cap$-closed and has the empty element.

A semiring of X is a semi \-closed, $\cap$-closed family of subsets of X with the empty element. Now we state the propositions:

(8) Let us consider a set X, a family S of subsets of X, and sets S_1, S_2. Suppose S_1, $S_2 \in S$ and S is semi \-closed. Then there exists a finite subset x of S such that x is a partition of $S_1 \setminus S_2$.

(9) Let us consider a set X, and a non empty family S of subsets of X. Suppose S is semi \-closed. Then S is $\setminus^{\subseteq}_{fp}$-closed. The theorem is a consequence of (8).

(10) Let us consider a set X, and a family S of subsets of X. Suppose S is $\cap_{fp}$-closed and $\setminus^{\subseteq}_{fp}$-closed and has the empty element. Then S is semi \-closed. The theorem is a consequence of (2).

Note that every set which is \-closed is also semi \-closed and $\cap$-closed.

Let X be a set. Observe that there exists a family of subsets of X which is non empty and preboolean and every set which is non empty and preboolean has also the empty element.

Let X be a set and S be a semi \-closed, $\cap$-closed family of subsets of X with the empty element. The ring generated by S yielding a non empty, preboolean family of subsets of X is defined by the term

(Def. 2) $\bigcap\{Z$, where Z is a non empty, preboolean family of subsets of $X : S \subseteq Z\}$.

Now we state the proposition:

(11) Let us consider a set X, and a semi \-closed, $\cap$-closed family P of subsets of X with the empty element. Then $P \subseteq$ the ring generated by P.

Let X be a set and S be a semi \-closed, $\cap$-closed family of subsets of X with the empty element. The functor DisUnion S yielding a non empty family of subsets of X is defined by the term

(Def. 3) $\{A$, where A is a subset of X : there exists a disjoint valued finite sequence F of elements of S such that $A = \bigcup F\}$.

Let us consider a set X and a semi \-closed, $\cap$-closed family S of subsets of X with the empty element. Now we state the propositions:

(12) $S \subseteq \mathrm{DisUnion}\, S$.

(13) $\mathrm{DisUnion}\, S$ is $\cap$-closed. The theorem is a consequence of (6) and (1).

Now we state the proposition:

(14) Let us consider a set X, a semi \-closed, $\cap$-closed family S of subsets of X with the empty element, and sets A, B, P. If $P = \mathrm{DisUnion}\, S$ and A, $B \in P$ and A misses B, then $A \cup B \in P$.

Let us consider a set X, a semi \-closed, $\cap$-closed family S of subsets of X with the empty element, and sets A, B. Now we state the propositions:

(15) If A, $B \in S$, then $B \setminus A \in \mathrm{DisUnion}\, S$.

(16) If $A \in S$ and $B \in \mathrm{DisUnion}\, S$, then $B \setminus A \in \mathrm{DisUnion}\, S$.

PROOF: Reconsider $A_1 = A$ as a subset of X. Consider B_1 being a subset of X such that $B = B_1$ and there exists a disjoint valued finite sequence F of elements of S such that $B_1 = \bigcup F$. Consider g_1 being a disjoint valued finite sequence of elements of S such that $B_1 = \bigcup g_1$. Reconsider $R_1 = \mathrm{DisUnion}\, S$ as a non empty set. Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv \$_2 = g_1(\$_1) \setminus A_1$. For every natural number k such that $k \in \mathrm{Seg\,len}\, g_1$ there exists an element x of R_1 such that $\mathcal{P}[k, x]$ by [10, (3)], (15). Consider g_2 being a finite sequence of elements of R_1 such that $\mathrm{dom}\, g_2 = \mathrm{Seg\,len}\, g_1$ and for every natural number k such that $k \in \mathrm{Seg\,len}\, g_1$ holds $\mathcal{P}[k, g_2(k)]$ from [6, Sch. 5]. For every natural numbers n, m such that n, $m \in \mathrm{dom}\, g_2$ and $n \neq m$ holds $g_2(n)$ misses $g_2(m)$. Set $R = \mathrm{DisUnion}\, S$. Define $\mathcal{H}[\text{natural number}] \equiv \bigcup \mathrm{rng}(g_2 \restriction \$_1) \in R$. For every natural number k such that $\mathcal{H}[k]$ holds $\mathcal{H}[k+1]$ by [4, (13)], [6, (59), (82)], [24, (55)]. For every natural number k, $\mathcal{H}[k]$ from [4, Sch. 2]. □

Now we state the propositions:

(17) Let us consider a set X, a semi \-closed, $\cap$-closed family S of subsets of X with the empty element, and sets A, B, R. Suppose $R = \mathrm{DisUnion}\, S$ and A, $B \in R$ and $A \neq \emptyset$. Then $B \setminus A \in R$.

PROOF: Consider A_1 being a subset of X such that $A = A_1$ and there exists a disjoint valued finite sequence F of elements of S such that $A_1 = \bigcup F$. Consider f_1 being a disjoint valued finite sequence of elements of S such that $A_1 = \bigcup f_1$. Consider B_1 being a subset of X such that $B = B_1$ and there exists a disjoint valued finite sequence F of elements of S such that $B_1 = \bigcup F$. Reconsider $R_1 = R$ as a non empty set. Define $\mathcal{P}[\text{natural number}, \text{object}] \equiv \$_2 = B_1 \setminus f_1(\$_1)$. For every natural number k such that $k \in \mathrm{Seg\,len}\, f_1$ there exists an element x of R_1 such that $\mathcal{P}[k, x]$ by [10, (3)], (16). Consider F being a finite sequence of elements of R_1 such

that $\operatorname{dom} F = \operatorname{Seg}\operatorname{len} f_1$ and for every natural number k such that $k \in \operatorname{Seg}\operatorname{len} f_1$ holds $\mathcal{P}[k, F(k)]$ from [6, Sch. 5]. Define $\mathcal{P}[\text{natural number}] \equiv \bigcap \operatorname{rng}(F\restriction \$_1) \in R$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (82)], [4, (11)], [6, (59)], [24, (55)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

(18) Let us consider a set X, and a semi \-closed, $\cap$-closed family S of subsets of X with the empty element. Then the ring generated by $S = \operatorname{DisUnion} S$. The theorem is a consequence of (13), (17), and (14).

Let X be a set.

A σ-ring of subsets of X is a non empty, preboolean family of subsets of X and is defined by

(Def. 4) for every sequence F of subsets of X such that $\operatorname{rng} F \subseteq it$ holds $\bigcup F \in it$.

Let us observe that every σ-ring of subsets of X is σ-multiplicative.

Let S be a family of subsets of X. The functor σ-ring(S) yielding a σ-ring of subsets of X is defined by

(Def. 5) $S \subseteq it$ and for every set Z such that $S \subseteq Z$ and Z is a σ-ring of subsets of X holds $it \subseteq Z$.

Now we state the proposition:

(19) Let us consider a set X, and a semi \-closed, $\cap$-closed family S of subsets of X with the empty element. Then σ-ring(the ring generated by S) = σ-ring(S). The theorem is a consequence of (11).

3. Semialgebra, Algebra and σ-algebra of Sets

Let X be a set.

A semialgebra of sets of X is a semi \-closed, $\cap$-closed family of subsets of X with the empty element and is defined by

(Def. 6) $X \in it$.

Now we state the proposition:

(20) Let us consider a set X. Then every field of subsets of X is a semialgebra of sets of X.

Let X be a set and S be a semialgebra of sets of X. The field generated by S yielding a non empty field of subsets of X is defined by the term

(Def. 7) $\bigcap\{Z$, where Z is a field of subsets of $X : S \subseteq Z\}$.

Now we state the propositions:

(21) Let us consider a set X, and a semialgebra P of sets of X. Then $P \subseteq$ the field generated by P.

(22) Let us consider a set X, and a semialgebra S of sets of X. Then the field generated by $S = \mathrm{DisUnion}\, S$. The theorem is a consequence of (13), (17), and (14).

(23) Let us consider a non empty set X, and a semialgebra S of sets of X. Then σ(the field generated by S) $= \sigma(S)$. The theorem is a consequence of (21).

4. Mutual Relationships between σ-ring and σ-algebra of Sets

Let us consider a set X and a set S. Now we state the propositions:

(24) If S is a σ-field of subsets of X, then S is a σ-ring of subsets of X.

(25) If S is a σ-ring of subsets of X and $X \in S$, then S is a σ-field of subsets of X.

Let us consider a family S of subsets of $\mathbb{R}$. Now we state the propositions:

(26) Suppose $S = \{I$, where I is a subset of $\mathbb{R} : I$ is left open interval$\}$. Then S is semi $\setminus$-closed and $\cap$-closed and has the empty element. The theorem is a consequence of (10).

(27) Suppose $S = \{I$, where I is a subset of $\mathbb{R} : I$ is right open interval$\}$. Then S is semi $\setminus$-closed and $\cap$-closed and has the empty element. The theorem is a consequence of (4) and (3).

Now we state the proposition:

(28) the set of all I where I is an interval is a semialgebra of sets of $\mathbb{R}$. The theorem is a consequence of (3) and (4).

References

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

[2] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.

[3] Grzegorz Bancerek. Continuous, stable, and linear maps of coherence spaces. *Formalized Mathematics*, 5(**3**):381–393, 1996.

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

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

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

[7] Józef Białas. The σ-additive measure theory. *Formalized Mathematics*, 2(**2**):263–270, 1991.

[8] Józef Białas. Properties of the intervals of real numbers. *Formalized Mathematics*, 3(**2**): 263–269, 1992.

[9] Vladimir Igorevich Bogachev and Maria Aparecida Soares Ruas. *Measure theory*, volume 1. Springer, 2007.

[10] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[11] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

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

[13] Roland Coghetto. Semiring of sets. *Formalized Mathematics*, 22(**1**):79–84, 2014. doi:10.2478/forma-2014-0008.

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

[15] D.F. Goguadze. About the notion of semiring of sets. *Mathematical Notes*, 74:346–351, 2003. ISSN 0001-4346. doi:10.1023/A:1026102701631.

[16] P. R. Halmos. *Measure Theory*. Springer-Verlag, 1974.

[17] Jarosław Kotowicz and Konrad Raczkowski. Coherent space. *Formalized Mathematics*, 3 (**2**):255–261, 1992.

[18] Andrzej Nędzusiak. σ-fields and probability. *Formalized Mathematics*, 1(**2**):401–407, 1990.

[19] Andrzej Nędzusiak. Probability. *Formalized Mathematics*, 1(**4**):745–749, 1990.

[20] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[21] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(**3**):441–444, 1990.

[22] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**): 341–347, 2003.

[23] Andrzej Trybulec and Agata Darmochwał. Boolean domains. *Formalized Mathematics*, 1 (**1**):187–190, 1990.

[24] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

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

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

[27] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received February 18, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 1, Pages 59–65, 2015
DOI: 10.2478/forma-2015-0005

DE GRUYTER OPEN
degruyter.com/view/j/forma

Separability of Real Normed Spaces and Its Basic Properties

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Noboru Endou
Gifu National College of Technology
Gifu, Japan

Summary. In this article, the separability of real normed spaces and its properties are mainly formalized. In the first section, it is proved that a real normed subspace is separable if it is generated by a countable subset. We used here the fact that the rational numbers form a dense subset of the real numbers. In the second section, the basic properties of the separable normed spaces are discussed. It is applied to isomorphic spaces via bounded linear operators and double dual spaces. In the last section, it is proved that the completeness and reflexivity are transferred to sublinear normed spaces. The formalization is based on [34], and also referred to [7], [14] and [16].

MSC: 46B20 46A19 03B35

Keywords: functional analysis; normed linear space; topological vector space

MML identifier: NORMSP_4, version: 8.1.04 5.31.1231

The notation and terminology used in this paper have been introduced in the following articles: [2], [4], [8], [26], [20], [21], [13], [9], [10], [22], [1], [25], [24], [15], [19], [6], [11], [23], [17], [32], [33], [27], [28], [29], [30], [31], [18], and [12].

1. Separability of Real Normed Space

Let X be a real linear space and A be a subset of X. The functor $\mathrm{Sums}_{\mathbb{Q}}\, A$ yielding a subset of X is defined by the term

(Def. 1) $\{\sum l$, where l is a linear combination of $A : \mathrm{rng}\, l \subseteq \mathbb{Q}\}$.

Let us consider a real normed space V and a real normed subspace V_1 of V. Now we state the propositions:

ISSN 1426–2630(Print), 1898-9934(Online)

(1) TopSpaceNorm V_1 is a subspace of TopSpaceNorm V.
PROOF: For every points x, y of MetricSpaceNorm V_1, (the distance of MetricSpaceNorm V_1)(x, y) = (the distance of MetricSpaceNorm V)(x, y) by [28, (16)], [19, (28)]. □

(2) LinearTopSpaceNorm V_1 is a subspace of LinearTopSpaceNorm V. The theorem is a consequence of (1).

Now we state the proposition:

(3) Let us consider a real normed space X, and real normed subspaces Y, Z of X. Suppose there exists a subset A of X such that A = the carrier of Y and $\overline{A}$ = the carrier of Z. Let us consider a subset D_0 of Y, and a subset D of Z. If D_0 is dense and $D_0 = D$, then D is dense.
PROOF: LinearTopSpaceNorm Z is a subspace of LinearTopSpaceNorm X and LinearTopSpaceNorm Y is a subspace of LinearTopSpaceNorm X. For every subset S of Z such that $S \neq \emptyset$ and S is open holds D meets S by [15, (16), (20)], [19, (5), (17), (4)]. □

Let us consider an additive loop structure X and subsets A, B of X. Now we state the propositions:

(4) There exists a function F from $A + B$ into $A \times B$ such that F is one-to-one.
PROOF: Set $D = A + B$. Define $\mathcal{P}$[object, object] ≡ there exist points a, b of X such that $\$_1 = a + b$ and $a \in A$ and $b \in B$ and $\$_2 = \langle a, b \rangle$. For every object x such that $x \in D$ there exists an object y such that $y \in A \times B$ and $\mathcal{P}[x, y]$ by [12, (87)]. Consider F being a function from D into $A \times B$ such that for every object x such that $x \in D$ holds $\mathcal{P}[x, F(x)]$ from [10, Sch. 1]. For every objects x_1, x_2 such that x_1, $x_2 \in \operatorname{dom} F$ and $F(x_1) = F(x_2)$ holds $x_1 = x_2$. □

(5) If A is countable and B is countable, then $A + B$ is countable. The theorem is a consequence of (4).

Now we state the proposition:

(6) Let us consider a non empty additive loop structure X, subsets A, B of X, a linear combination l_1 of A, and a linear combination l_2 of B. Suppose A misses B. Then there exists a linear combination l of $A \cup B$ such that

(i) the support of l = (the support of l_1) ∪ (the support of l_2), and

(ii) $l = l_1 + l_2$.

PROOF: Define $\mathcal{P}$[object, object] ≡ if $\$_1 \in$ the support of l_1, then $\$_2 = l_1(\$_1)$ and if $\$_1 \in$ the support of l_2, then $\$_2 = l_2(\$_1)$ and if $\$_1 \notin$ the support of l_1 and $\$_1 \notin$ the support of l_2, then $\$_2 = 0$. Consider l being a function from the carrier of X into $\mathbb{R}$ such that for every object x such

that $x \in$ the carrier of X holds $\mathcal{P}[x, l(x)]$ from [10, Sch. 1]. Reconsider $T =$ (the support of l_1) $\cup$ (the support of l_2) as a finite subset of X. For every element x of X such that $x \notin T$ holds $l(x) = 0$. For every element v of X, $l(v) = l_1(v) + l_2(v)$. □

Let us consider a non empty additive loop structure X, subsets A, B of X, and a linear combination l of $A \cup B$. Now we state the propositions:

(7) There exists a linear combination l_1 of A such that

(i) the support of $l_1 =$ (the support of l) $\setminus B$, and

(ii) for every element x of X such that $x \in$ the support of l_1 holds $l_1(x) = l(x)$.

PROOF: Reconsider $T_1 =$ (the support of l) $\setminus B$ as a finite subset of X. Define $\mathcal{Q}[\text{object}, \text{object}] \equiv$ if $\$_1 \in T_1$, then $\$_2 = l(\$_1)$ and if $\$_1 \notin T_1$, then $\$_2 = 0$. Consider l_1 being a function from the carrier of X into $\mathbb{R}$ such that for every object x such that $x \in$ the carrier of X holds $\mathcal{Q}[x, l_1(x)]$ from [10, Sch. 1]. □

(8) Suppose A misses B. Then there exists a linear combination l_1 of A and there exists a linear combination l_2 of B such that the support of $l =$ (the support of l_1)$\cup$(the support of l_2) and $l = l_1 + l_2$ and the support of $l_1 =$ (the support of l)$\setminus B$ and the support of $l_2 =$ (the support of l)$\setminus A$. The theorem is a consequence of (7).

Now we state the propositions:

(9) Let us consider a real linear space X, subsets A, B of X, a linear combination l_1 of A, and a linear combination l_2 of B. Suppose $\operatorname{rng} l_1 \subseteq \mathbb{Q}$ and $\operatorname{rng} l_2 \subseteq \mathbb{Q}$ and A misses B. Then there exists a linear combination l of $A \cup B$ such that

(i) the support of $l =$ (the support of l_1) $\cup$ (the support of l_2), and

(ii) $\operatorname{rng} l \subseteq \mathbb{Q}$, and

(iii) $\sum l = \sum l_1 + \sum l_2$.

The theorem is a consequence of (6).

(10) Let us consider a real linear space X, subsets A, B of X, and a linear combination l of $A \cup B$. Suppose $\operatorname{rng} l \subseteq \mathbb{Q}$ and A misses B. Then there exists a linear combination l_1 of A and there exists a linear combination l_2 of B such that $\operatorname{rng} l_1 \subseteq \mathbb{Q}$ and $\operatorname{rng} l_2 \subseteq \mathbb{Q}$ and $\sum l = \sum l_1 + \sum l_2$. The theorem is a consequence of (8).

(11) Let us consider a real linear space X, and finite subsets A, B of X. Suppose A misses B. Then $\operatorname{Sums}_{\mathbb{Q}} A + \operatorname{Sums}_{\mathbb{Q}} B = \operatorname{Sums}_{\mathbb{Q}}(A \cup B)$. The theorem is a consequence of (9) and (10).

Let X be a real linear space and A be a finite subset of X. Observe that $\mathrm{Sums}_{\mathbb{Q}} A$ is countable.

Now we state the proposition:

(12) Let us consider a real linear space X, a sequence x of X, and a finite subset A of X. Suppose $A \subseteq \operatorname{rng} x$. Then there exists a natural number n such that $A \subseteq \operatorname{rng}(x{\restriction}\mathbb{Z}_n)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset A of X such that $\overline{\overline{A}} = \$_1$ and $A \subseteq \operatorname{rng} x$ there exists a natural number n such that $A \subseteq \operatorname{rng}(x{\restriction}\mathbb{Z}_n)$. $\mathcal{P}[0]$. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (44)], [12, (31)], [3, (42)], [10, (11)]. For every natural number k, $\mathcal{P}[k]$ from [5, Sch. 2]. □

Let X be a real linear space and x be a sequence of X. One can verify that $\mathrm{Sums}_{\mathbb{Q}} \operatorname{rng} x$ is countable.

Now we state the propositions:

(13) Let us consider a real normed space X, and a sequence x of X. Then $\mathrm{Sums}_{\mathbb{Q}} \operatorname{rng} x$ is a subset of the carrier of $\mathrm{NLin} \operatorname{rng} x$.

PROOF: Set $D = \mathrm{Sums}_{\mathbb{Q}} \operatorname{rng} x$. For every object z such that $z \in D$ holds $z \in$ the carrier of $\mathrm{NLin} \operatorname{rng} x$ by [30, (14)]. □

(14) Let us consider a real normed space X, and a subset Y of X. Then

(i) the carrier of $\mathrm{NLin}\, Y \subseteq$ the carrier of $\mathrm{ClNLin}(Y)$, and

(ii) there exists a subset Z of X such that $Z =$ the carrier of $\mathrm{NLin}\, Y$ and $\overline{Z} =$ the carrier of $\mathrm{ClNLin}(Y)$.

(15) Let us consider a real normed space X, and a sequence x of X. Then $\mathrm{Sums}_{\mathbb{Q}} \operatorname{rng} x$ is a countable subset of the carrier of $\mathrm{ClNLin}(\operatorname{rng} x)$. The theorem is a consequence of (13) and (14).

(16) Let us consider real numbers z, e. Suppose $0 < e$. Then there exists an element q of $\mathbb{Q}$ such that

(i) $q \neq 0$, and

(ii) $|z - q| < e$.

(17) Let us consider a real normed space X, a point w of X, a real number e, and a linear combination l of $\{w\}$. Suppose $0 < e$. Then there exists a linear combination m of $\{w\}$ such that

(i) the support of $m =$ the support of l, and

(ii) $\operatorname{rng} m \subseteq \mathbb{Q}$, and

(iii) $\|\sum l - \sum m\| < e$.

The theorem is a consequence of (16).

(18) Let us consider a real normed space X, a subset A of X, a real number e, and a linear combination l of A. Suppose $0 < e$. Then there exists a linear combination m of A such that

(i) the support of m = the support of l, and

(ii) $\operatorname{rng} m \subseteq \mathbb{Q}$, and

(iii) $\|\sum l - \sum m\| < e$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every real number e for every linear combination l of A such that $0 < e$ and $\overline{\overline{\text{the support of } l}} = \$_1$ there exists a linear combination m of A such that the support of m = the support of l and $\operatorname{rng} m \subseteq \mathbb{Q}$ and $\|\sum l - \sum m\| < e$. $\mathcal{P}[0]$ by [29, (34), (44), (42)], [30, (2)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [3, (44)], [12, (31)], [3, (42)], (8). For every natural number k, $\mathcal{P}[k]$ from [5, Sch. 2]. □

Let us consider a real normed space X and a sequence x of X. Now we state the propositions:

(19) $\operatorname{Sums}_{\mathbb{Q}} \operatorname{rng} x$ is a dense subset of the carrier of $\operatorname{NLin} \operatorname{rng} x$.

(20) $\operatorname{Sums}_{\mathbb{Q}} \operatorname{rng} x$ is a dense subset of the carrier of $\operatorname{ClNLin}(\operatorname{rng} x)$.

Now we state the proposition:

(21) Let us consider a real normed space X. Suppose there exists a subset D of the carrier of X such that D is dense and countable. Then X is separable.

2. Basic Properties of Separable Spaces

Let X be a real normed space and x be a sequence of X. Let us observe that $\operatorname{ClNLin}(\operatorname{rng} x)$ is separable.

Now we state the propositions:

(22) Let us consider a real normed space X, a real normed subspace Y of X, and a Lipschitzian linear functional L in X. Then $L\restriction$(the carrier of Y) is a Lipschitzian linear functional in Y.

PROOF: Set Y_1 = the carrier of Y. Reconsider $L_1 = L\restriction Y_1$ as a functional in Y. L_1 is additive by [9, (49)], [19, (28)]. L_1 is homogeneous by [9, (49)], [19, (28)]. Consider K being a real number such that $0 \leqslant K$ and for every point x of X, $|L(x)| \leqslant K \cdot \|x\|$. For every point x of Y, $|L_1(x)| \leqslant K \cdot \|x\|$ by [19, (28)], [9, (49)]. □

(23) Let us consider real normed spaces X, Y, a subset A of X, a subset B of Y, and a Lipschitzian linear operator L from X into Y. Suppose L is isomorphism and $B = L^\circ A$. Then A is dense if and only if B is dense.

(24) Let us consider real normed spaces X, Y. Suppose there exists a Lipschitzian linear operator L from X into Y such that L is isomorphism. Then X is separable if and only if Y is separable. The theorem is a consequence of (23).

(25) Let us consider a real normed space X. Suppose X is non trivial and reflexive. Then X is separable if and only if DualSp(DualSp(X)) is separable. The theorem is a consequence of (24).

3. Completeness and Reflexivity of Sublinear Normed Spaces

Now we state the proposition:

(26) Let us consider a real normed space X, and subsets Y, Z of X. Suppose $Z =$ the carrier of Lin(Y). Then the carrier of Lin(Z) $= Z$.

Let us consider a real Banach space X and a subset Y of X. Now we state the propositions:

(27) There exists a subset Z of X such that

(i) $Z =$ the carrier of Lin(Y), and

(ii) ClNLin(Y) $=$ NLin $\overline{Z}$, and

(iii) $\overline{Z}$ is linearly closed, and

(iv) $\overline{Z} \neq \emptyset$.

(28) ClNLin(Y) is a real Banach space. The theorem is a consequence of (27).

(29) If X is reflexive, then ClNLin(Y) is reflexive. The theorem is a consequence of (27).

Acknowledgement: We would like to thank Keiko Narita and Yasunari Shidama.

References

[1] Jonathan Backer, Piotr Rudnicki, and Christoph Schwarzweller. Ring ideals. *Formalized Mathematics*, 9(**3**):565–582, 2001.
[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. König's theorem. *Formalized Mathematics*, 1(**3**):589–593, 1990.
[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] Nicolas Bourbaki. Topological vector spaces: Chapters 1-5. *Springer*, 1981.
[8] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.
[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 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] N. J. Dunford and T. Schwartz. *Linear operators I.* Interscience Publ., 1958.
[15] Noboru Endou, Yasunari Shidama, and Katsumasa Okamura. Baire's category theorem and some spaces generated from real normed space. *Formalized Mathematics*, 14(**4**): 213–219, 2006. doi:10.2478/v10037-006-0024-x.
[16] Andrey Kolmogorov and Sergei Fomin. *Elements of the Theory of Functions and Functional Analysis [Two Volumes in One].* Martino Fine Books, 2012.
[17] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.
[18] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[19] Kazuhisa Nakasho, Yuichi Futa, and Yasunari Shidama. Topological properties of real normed space. *Formalized Mathematics*, 22(**3**):209–223, 2014. doi:10.2478/forma-2014-0024.
[20] Keiko Narita, Noboru Endou, and Yasunari Shidama. Dual spaces and Hahn-Banach theorem. *Formalized Mathematics*, 22(**1**):69–77, 2014. doi:10.2478/forma-2014-0007.
[21] Keiko Narita, Noboru Endou, and Yasunari Shidama. Bidual spaces and reflexivity of real normed spaces. *Formalized Mathematics*, 22(**4**):303–311, 2014. doi:10.2478/forma-2014-0030.
[22] Bogdan Nowak and Andrzej Trybulec. Hahn-Banach theorem. *Formalized Mathematics*, 4(**1**):29–34, 1993.
[23] Beata Padlewska and Agata Darmochwał. Topological spaces and continuous functions. *Formalized Mathematics*, 1(**1**):223–230, 1990.
[24] Jan Popiołek. Real normed space. *Formalized Mathematics*, 2(**1**):111–115, 1991.
[25] Yasunari Shidama. Banach space of bounded linear operators. *Formalized Mathematics*, 12(**1**):39–48, 2004.
[26] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.
[27] Wojciech A. Trybulec. Subspaces and cosets of subspaces in real linear space. *Formalized Mathematics*, 1(**2**):297–301, 1990.
[28] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[29] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.
[30] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(**5**):847–850, 1990.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[33] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.
[34] Kosaku Yoshida. *Functional Analysis.* Springer, 1980.

Received February 26, 2015

FORMALIZED MATHEMATICS
Vol. 23, No. 1, Pages 67–73, 2015
DOI: 10.2478/forma-2015-0006

DE GRUYTER OPEN
degruyter.com/view/j/forma

Equivalent Expressions of Direct Sum Decomposition of Groups[1]

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Hiroshi Yamazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, the equivalent expressions of the direct sum decomposition of groups are mainly discussed. In the first section, we formalize the fact that the internal direct sum decomposition can be defined as normal subgroups and some of their properties. In the second section, we formalize an equivalent form of internal direct sum of commutative groups. In the last section, we formalize that the external direct sum leads an internal direct sum. We referred to [19], [18] [8] and [14] in the formalization.

MSC: 20E34 03B35

Keywords: group theory; direct sum decomposition

MML identifier: GROUP_20, version: 8.1.04 5.31.1231

The notation and terminology used in this paper have been introduced in the following articles: [1], [20], [6], [9], [10], [7], [22], [17], [16], [23], [24], [25], [26], [13], [3], [5], [11], [15], [28], [29], [27], and [12].

1. Internal Direct Sum Decomposition into Normal Subgroups

Let I be a set and G be a group.

A subgroup-family of I and G is a group-family of I and is defined by

(Def. 1) for every object i such that $i \in I$ holds $it(i)$ is a subgroup of G.

[1]This work was supported by JSPS KAKENHI 22300285.

ISSN 1426–2630(Print), 1898-9934(Online)

Let F be a subgroup-family of I and G. We say that F is component commutative if and only if

(Def. 2) for every elements i, j of I and for every elements g_1, g_2 of G such that $i \neq j$ and $g_1 \in F(i)$ and $g_2 \in F(j)$ holds $g_1 \cdot g_2 = g_2 \cdot g_1$.

Let I be a non empty set. One can verify that there exists a subgroup-family of I and G which is component commutative.

Now we state the propositions:

(1) Let us consider a group G, a normal subgroup H of G, and elements x, y of G. Suppose $y \in H$. Then $x \cdot y \cdot x^{-1}$, $x \cdot (y \cdot x^{-1}) \in H$.

(2) Let us consider a non empty set I, a group G, a group-family F of I, and a function x from I into G. Suppose $x \in \prod F$. Then x is a function from I into $\bigcup$(the support of F).

PROOF: For every object z such that $z \in \operatorname{rng} x$ holds $z \in \bigcup$(the support of F) by [10, (11)], [16, (5), (4)], [9, (3)]. □

(3) Let us consider a non empty set I, a group G, a subgroup H of G, a function x from I into G, and a function y from I into H. If $x = y$, then $\operatorname{support} x = \operatorname{support} y$.

PROOF: For every object i, $i \in \operatorname{support} x$ iff $i \in \operatorname{support} y$ by [23, (44)]. □

(4) Let us consider a non empty set I, a group G, and a subgroup H of G. Then every finite-support function from I into H is a finite-support function from I into G. The theorem is a consequence of (3).

(5) Let us consider a non empty set I, a group G, a subgroup H of G, and a finite-support function x from I into G. Suppose $\operatorname{rng} x \subseteq \Omega_H$. Then x is a finite-support function from I into H. The theorem is a consequence of (3).

(6) Let us consider a non empty set I, a group G, a subgroup H of G, a finite-support function x from I into G, and a finite-support function y from I into H. If $x = y$, then $\prod x = \prod y$. The theorem is a consequence of (3).

(7) Let us consider a function f, and sets i, x. Then $f = (f +\cdot (i, x)) +\cdot (i, f(i))$.

(8) Let us consider a non empty set I, a group G, a component commutative subgroup-family F of I and G, finite-support functions x, y from I into G, and an element i of I. Suppose $y = x +\cdot (i, \mathbf{1}_{F(i)})$ and $x \in \prod F$. Then $\prod x = \prod y \cdot x(i) = x(i) \cdot \prod y$.

PROOF: Reconsider $p_2 = y$ as an element of $\prod F$. Reconsider $s_1 = p_2$ as an element of $\operatorname{sum} F$. Set $z = \mathbf{1}_{\prod F} +\cdot (i, x(i))$. Reconsider $s_2 = z$ as an element of $\operatorname{sum} F$. $x = s_1 \cdot s_2$ by [16, (5), (24)], [23, (40)], [7, (31)].

$s_1 \cdot s_2 = s_2 \cdot s_1$ by [16, (27), (17)], [23, (43)], [16, (32)]. □

(9) Let us consider a non empty set I, a group G, a component commutative subgroup-family F of I and G, a subset U of G, an element i of I, and finite-support functions x, y from I into $\mathrm{gr}(U)$. Suppose $y = x +\cdot (i, \mathbf{1}_{F(i)})$ and $x \in \prod F$. Then $\prod x = \prod y \cdot x(i) = x(i) \cdot \prod y$. The theorem is a consequence of (4), (6), and (8).

(10) Let us consider a non empty set I, a group G, a component commutative subgroup-family F of I and G, a subset U of G, a finite-support function y from I into $\mathrm{gr}(U)$, an element i of I, and an element g of $\mathrm{gr}(U)$. Suppose $y \in \prod F$ and $y(i) = \mathbf{1}_{F(i)}$ and $g \in F(i)$. Then $\prod y \cdot g = g \cdot \prod y$. The theorem is a consequence of (7) and (9).

(11) Let us consider a non empty set I, a group G, a component commutative subgroup-family F of I and G, and a subset U of G. Suppose $U = \bigcup(\text{the support of } F)$. Let us consider an element g of G, a finite sequence H of elements of G, and a finite sequence K of elements of $\mathbb{Z}$. Suppose $\mathrm{len}\, H = \mathrm{len}\, K$ and $\mathrm{rng}\, H \subseteq U$ and $\prod H^K = g$. Then there exists a finite-support function f from I into G such that

(i) $f \in \prod F$, and

(ii) $g = \prod f$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every element g of G for every finite sequence H of elements of G for every finite sequence K of elements of $\mathbb{Z}$ such that $\mathrm{len}\, H = \$_1$ and $\mathrm{len}\, H = \mathrm{len}\, K$ and $\mathrm{rng}\, H \subseteq U$ and $\prod H^K = g$ there exists a finite-support function f from I into G such that $f \in \prod F$ and $g = \prod f$. $\mathcal{P}[0]$ by [25, (21)], [16, (12), (13), (16)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [28, (70)], [6, (4)], [21, (55)], [9, (3)]. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. □

(12) Let us consider a non empty set I, a group G, a subgroup-family F of I and G, finite-support functions h, h_0 from I into G, an element i of I, and a subset U_1 of G. Suppose $U_1 = \bigcup((\text{the support of } F) \restriction (I \setminus \{i\}))$ and $h_0 = h +\cdot (i, \mathbf{1}_{F(i)})$ and $h \in \prod F$. Then $\prod h_0 \in \mathrm{gr}(U_1)$.

PROOF: For every object y such that $y \in \mathrm{rng}\, h_0$ holds $y \in \Omega_{\mathrm{gr}(U_1)}$ by [10, (113)], [7, (32)], [16, (5), (4)]. Reconsider $x_0 = h_0$ as a finite-support function from I into $\mathrm{gr}(U_1)$. $\prod x_0 = \prod h_0$. □

(13) Let us consider a non empty set I, a group G, a component commutative subgroup-family F of I and G, and a subset U of G. Suppose $U = \bigcup(\text{the support of } F)$. Let us consider an element g of G. Suppose $g \in \mathrm{gr}(U)$. Then there exists a finite-support function f from I into $\mathrm{gr}(U)$ such that

(i) $f \in \operatorname{sum} F$, and

(ii) $g = \prod f$.

The theorem is a consequence of (11), (2), (5), and (6).

(14) Let us consider a non empty set I, a group G, a component commutative subgroup-family F of I and G, and a subset U of G. Suppose $U = \bigcup$(the support of F). Let us consider an element i of I. Then $F(i)$ is a normal subgroup of $\operatorname{gr}(U)$.

PROOF: Reconsider $F_1 = F(i)$ as a subgroup of $\operatorname{gr}(U)$. For every element a of $\operatorname{gr}(U)$, $a \cdot F_1 \subseteq F_1 \cdot a$ by [23, (103), (42)], (13), [23, (40)]. □

(15) Let us consider a non empty set I, a group G, and a component commutative subgroup-family F of I and G. Suppose for every element i of I, there exists a subset U_1 of G such that $U_1 = \bigcup((\text{the support of } F)\restriction(I \setminus \{i\}))$ and $\Omega_{\operatorname{gr}(U_1)} \cap \Omega_{F(i)} = \{\mathbf{1}_G\}$. Let us consider finite-support functions x_1, x_2 from I into G. If x_1, $x_2 \in \operatorname{sum} F$ and $\prod x_1 = \prod x_2$, then $x_1 = x_2$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite-support functions x_1, x_2 from I into G such that $\overline{\overline{\operatorname{support} x_1}} = \$_1$ and x_1, $x_2 \in \operatorname{sum} F$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$. $\mathcal{P}[0]$ by [16, (15), (14)], [23, (42)], [16, (26)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [23, (42)], [16, (26)], [23, (44)], [16, (30), (25)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

(16) Let us consider a non empty set I, a strict group G, and a group-family F of I. Then F is an internal direct sum components of G and I if and only if for every element i of I, $F(i)$ is a normal subgroup of G and there exists a subset U of G such that $U = \bigcup$(the support of F) and $\operatorname{gr}(U) = G$ and for every element i of I, there exists a subset U_1 of G such that $U_1 = \bigcup((\text{the support of } F)\restriction(I \setminus \{i\}))$ and $\Omega_{\operatorname{gr}(U_1)} \cap \Omega_{F(i)} = \{\mathbf{1}_G\}$.

PROOF: Consider U being a subset of G such that $U = \bigcup$(the support of F) and $\operatorname{gr}(U) = G$. For every elements i, j of I such that $i \neq j$ holds $\Omega_{F(i)} \cap \Omega_{F(j)} = \{\mathbf{1}_G\}$ by [23, (46)], [12, (31)], [28, (62)], [9, (49)]. For every elements i, j of I and for every elements g_1, g_2 of G such that $i \neq j$ and $g_1 \in F(i)$ and $g_2 \in F(j)$ holds $g_1 \cdot g_2 = g_2 \cdot g_1$ by [23, (51)], (1), [22, (17)], [23, (50)]. For every element y of G, there exists a finite-support function x from I into G such that $x \in \operatorname{sum} F$ and $y = \prod x$. For every finite-support functions x_1, x_2 from I into G such that x_1, $x_2 \in \operatorname{sum} F$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$. □

2. INTERNAL DIRECT SUM DECOMPOSITION FOR COMMUTATIVE GROUP

Now we state the proposition:

(17) Let us consider a non empty set I, a commutative group G, and a group-family F of I. Then F is an internal direct sum components of G and I if and only if for every element i of I, $F(i)$ is a subgroup of G and for every elements i, j of I such that $i \neq j$ holds $\Omega_{F(i)} \cap \Omega_{F(j)} = \{\mathbf{1}_G\}$ and for every element y of G, there exists a finite-support function x from I into G such that $x \in \operatorname{sum} F$ and $y = \prod x$ and for every finite-support functions x_1, x_2 from I into G such that x_1, $x_2 \in \operatorname{sum} F$ and $\prod x_1 = \prod x_2$ holds $x_1 = x_2$.

3. EQUIVALENCE BETWEEN INTERNAL AND EXTERNAL DIRECT SUM

Now we state the propositions:

(18) Let us consider a non empty set I, a group G, a subgroup-family F of I and G, a homomorphism h from $\operatorname{sum} F$ to G, and a finite-support function a from I into G. Suppose $a \in \operatorname{sum} F$ and for every element i of I and for every element x of $F(i)$, $h((1\mathrm{ProdHom}(F, i))(x)) = x$. Then $h(a) = \prod a$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite-support function b from I into G such that $b \in \operatorname{sum} F$ holds if $\overline{\overline{\operatorname{support} b}} = \$_1$, then $h(b) = \prod b$. $\mathcal{P}[0]$ by [16, (14)], [23, (44)], [26, (31)], [16, (15)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [16, (25)], [23, (44)], [16, (26)], [23, (40)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. Consider k being a natural number such that $\overline{\overline{\operatorname{support} a}} = k$. □

(19) Let us consider a non empty set I, a group G, and a direct sum components M of G and I. Then there exists a homomorphism f from $\operatorname{sum} M$ to G and there exists an internal direct sum components N of G and I such that f is bijective and for every element i of I, there exists a homomorphism q_1 from $M(i)$ to $N(i)$ such that $q_1 = f \cdot 1\mathrm{ProdHom}(M, i)$ and q_1 is bijective.
PROOF: Consider f being a homomorphism from $\operatorname{sum} M$ to G such that f is bijective. Define $\mathcal{D}(\text{element of } I) = f^{\circ}(\mathrm{ProjGroup}(M, \$_1))$. Consider N being a function such that $\operatorname{dom} N = I$ and for every element i of I such that $i \in I$ holds $N(i) = \mathcal{D}(i)$ from [2, Sch. 2]. For every object i such that $i \in I$ holds $N(i)$ is a strict subgroup of G. Define $\mathcal{E}(\text{element of } I) = f \cdot 1\mathrm{ProdHom}(M, \$_1)$. Consider q being a function such that $\operatorname{dom} q = I$ and for every element i of I such that $i \in I$ holds $q(i) = \mathcal{E}(i)$ from [2, Sch. 2]. Reconsider $r = \mathrm{SumMap}(M, N, q)$ as a homomorphism from $\operatorname{sum} M$ to $\operatorname{sum} N$. Reconsider $s = r^{-1}$ as a homomorphism from $\operatorname{sum} N$ to $\operatorname{sum} M$.

Reconsider $g = f \cdot s$ as a function. For every element i of I and for every element n of $N(i)$, $g((1\mathrm{ProdHom}(N, i))(n)) = n$ by [16, (42)], [23, (40)], [9, (13), (34)]. For every finite-support function a from I into G such that $a \in \operatorname{sum} N$ holds $g(a) = \prod a$. For every element i of I, there exists a homomorphism q_1 from $M(i)$ to $N(i)$ such that $q_1 = f \cdot 1\mathrm{ProdHom}(M, i)$ and q_1 is bijective. □

References

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

[2] Grzegorz Bancerek. Tarski's classes and ranks. *Formalized Mathematics*, 1(**3**):563–567, 1990.

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

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

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

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

[7] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.

[8] Nicolas Bourbaki. *Elements of Mathematics. Algebra I. Chapters 1-3*. Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, 1989.

[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 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] Artur Korniłowicz. The product of the families of the groups. *Formalized Mathematics*, 7(**1**):127–134, 1998.

[14] Serge Lang. *Algebra*. Springer, 3rd edition, 2005.

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

[16] Kazuhisa Nakasho, Hiroshi Yamazaki, Hiroyuki Okazaki, and Yasunari Shidama. Definition and properties of direct sum decomposition of groups. *Formalized Mathematics*, 23 (**1**):15–27, 2015. doi:10.2478/forma-2015-0002.

[17] Hiroyuki Okazaki, Kenichi Arai, and Yasunari Shidama. Normal subgroup of product of groups. *Formalized Mathematics*, 19(**1**):23–26, 2011. doi:10.2478/v10037-011-0004-7.

[18] D. Robinson. *A Course in the Theory of Groups*. Springer New York, 2012.

[19] J.J. Rotman. *An Introduction to the Theory of Groups*. Springer, 1995.

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

[21] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

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

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

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

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

[26] Wojciech A. Trybulec and Michał J. Trybulec. Homomorphisms and isomorphisms of groups. Quotient group. *Formalized Mathematics*, 2(**4**):573–578, 1991.
[27] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.
[29] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received February 26, 2015