FORMALIZED MATHEMATICS
Vol. 22, No. 3, Pages 189–198, 2014
DOI: 10.2478/forma-2014-0021

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

Rank of Submodule, Linear Transformations and Linearly Independent Subsets of ℤ-module[1]

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

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 some basic facts of ℤ-module. In the first section, we discuss the rank of submodule of ℤ-module and its properties. Especially, we formally prove that the rank of any ℤ-module is equal to or more than that of its submodules, and vice versa, and that there exists a submodule with any given rank that satisfies the above condition. In the next section, we mention basic facts of linear transformations between two ℤ-modules. In this section, we define homomorphism between two ℤ-modules and deal with kernel and image of homomorphism. In the last section, we formally prove some basic facts about linearly independent subsets and linear combinations. These formalizations are based on [9](p.191-242), [23](p.117-172) and [2](p.17-35).

MSC: 13C10 15A04 03B35

Keywords: free Z-module; rank of Z-module; homomorphism of Z-module; linearly independent; linear combination

MML identifier: ZMODUL05, version: 8.1.04 5.32.1234

The notation and terminology used in this paper have been introduced in the following articles: [3], [25], [10], [7], [18], [26], [12], [13], [14], [8], [24], [28], [27], [6], [15], [32], [33], [29], [16], [31], [22], [17], [19], [20], and [21].

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

1. Rank of Submodule of $\mathbb{Z}$-module

From now on V, W denote $\mathbb{Z}$-modules.

Let V be a $\mathbb{Z}$-module and A be a finite subset of V. One can verify that $\mathrm{Lin}(A)$ is finitely-generated.

Now we state the proposition:

(1) Let us consider a finite rank, free $\mathbb{Z}$-module V. Then $\mathrm{rank}\, V = 0$ if and only if $\Omega_V = \mathbf{0}_V$.

Let V be a finite rank, free $\mathbb{Z}$-module. One can verify that there exists a basis of V which is finite and every basis of V is finite.

Now we state the propositions:

(2) Let us consider a finite rank, free $\mathbb{Z}$-module V and a submodule W of V. Then $\mathrm{rank}\, W \leqslant \mathrm{rank}\, V$.

(3) Let us consider a $\mathbb{Z}$-module V and a finite, linearly independent subset A of V. Then $\overline{\overline{A}} = \mathrm{rank}\, \mathrm{Lin}(A)$.

Let us consider a finite rank, free $\mathbb{Z}$-module V. Now we state the propositions:

(4) $\mathrm{rank}\, V = \mathrm{rank}\, \Omega_V$. The theorem is a consequence of (3).

(5) $\mathrm{rank}\, V = 1$ if and only if there exists a vector v of V such that $v \neq 0_V$ and $\Omega_V = \mathrm{Lin}(\{v\})$.

(6) $\mathrm{rank}\, V = 2$ if and only if there exist vectors u, v of V such that $u \neq v$ and $\{u, v\}$ is linearly independent and $\Omega_V = \mathrm{Lin}(\{u, v\})$.

Now we state the proposition:

(7) Let us consider a finite rank, free $\mathbb{Z}$-module V, a submodule W of V, and a natural number n. Then $n \leqslant \mathrm{rank}\, V$ if and only if there exists a strict, free submodule W of V such that $\mathrm{rank}\, W = n$.

Let V be a finite rank, free $\mathbb{Z}$-module and n be a natural number. The set of n-submodules of V yielding a set is defined by

(Def. 1) for every object x, $x \in it$ iff there exists a strict, free submodule W of V such that $W = x$ and $\mathrm{rank}\, W = n$.

Let us consider a finite rank, free $\mathbb{Z}$-module V and a natural number n. Now we state the propositions:

(8) If $n \leqslant \mathrm{rank}\, V$, then the set of n-submodules of V is not empty.

(9) If $\mathrm{rank}\, V < n$, then the set of n-submodules of $V = \emptyset$. The theorem is a consequence of (2).

Now we state the propositions:

(10) Let us consider a finite rank, free $\mathbb{Z}$-module V, a submodule W of V, and a natural number n. Then the set of n-submodules of $W \subseteq$ the set of n-submodules of V.

(11) Let us consider finite sequences F, G of elements of $\mathbb{Z}$ and an integer v. Suppose $\operatorname{len} F = \operatorname{len} G + 1$ and $G = F \restriction \operatorname{dom} G$ and $v = F(\operatorname{len} F)$. Then $\sum F = \sum G + v$.

(12) Let us consider finite sequences F, G of elements of $\mathbb{Z}$. Suppose $\operatorname{rng} F = \operatorname{rng} G$ and F is one-to-one and G is one-to-one. Then $\sum F = \sum G$.

Let T be a finite subset of the carrier of $\mathbb{Z}^{\mathrm{R}}$. The functor $\sum T$ yielding an element of $\mathbb{Z}^{\mathrm{R}}$ is defined by

(Def. 2) there exists a finite sequence F of elements of $\mathbb{Z}$ such that $\operatorname{rng} F = T$ and F is one-to-one and $it = \sum F$.

The propositions (13)-(15) has been removed.

The definition (Def. 3) has been removed.

Let V, W be $\mathbb{Z}$-modules. Note that there exists a function from V into W which is additive and homogeneous.

Now we state the propositions:

(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 $\mathcal{P}[\text{finite sequence of elements of } V_1] \equiv f(\sum \$_1) = \sum(f \cdot \$_1)$. 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 [29, (41), (44)], [10, (8)]. For every finite sequence p of elements of V_1, $\mathcal{P}[p]$ from [11, Sch. 2]. $\square$

(17) Let us consider a free $\mathbb{Z}$-module V. If Ω_V is finite, then $\Omega_V = \mathbf{0}_V$.

2. BASIC FACTS OF LINEAR TRANSFORMATIONS

Let V, W be $\mathbb{Z}$-modules.

A linear transformation from V to W is an additive, homogeneous function from V into W. In the sequel T denotes a linear transformation from V to W.

Now we state the propositions:

(18) Let us consider elements x, y of V. Then $T(x) - T(y) = T(x - y)$.

(19) $T(0_V) = 0_W$.

Let V, W be $\mathbb{Z}$-modules and T be a linear transformation from V to W. The functor $\ker T$ yielding a strict submodule of V is defined by

(Def. 4) $\Omega_{it} = \{u, \text{ where } u \text{ is an element of } V : T(u) = 0_W\}$.

Now we state the proposition:

(20) Let us consider an element x of V. Then $x \in \ker T$ if and only if $T(x) = 0_W$.

Let V, W be $\mathbb{Z}$-modules and T be a linear transformation from V to W. The functor $\operatorname{im} T$ yielding a strict submodule of W is defined by

(Def. 5) $\Omega_{it} = T^{\circ}(\Omega_V)$.

Now we state the propositions:

(21) $0_V \in \ker T$. The theorem is a consequence of (20).

(22) Let us consider a subset X of V. Then $T^{\circ}X$ is a subset of $\operatorname{im} T$.

(23) Let us consider an element y of W. Then $y \in \operatorname{im} T$ if and only if there exists an element x of V such that $y = T(x)$.

(24) Let us consider an element x of $\ker T$. Then $T(x) = 0_W$. The theorem is a consequence of (20).

(25) If T is one-to-one, then $\ker T = \mathbf{0}_V$.
PROOF: Reconsider $Z = \mathbf{0}_V$ as a submodule of $\ker T$. For every element v of $\ker T$, $v \in Z$ by [1, (7)], (19), [19, (25)], (20). □

(26) Let us consider a finite rank, free $\mathbb{Z}$-module V. Then $\operatorname{rank} \mathbf{0}_V = 0$. The theorem is a consequence of (1).

(27) Let us consider elements x, y of V. If $T(x) = T(y)$, then $x - y \in \ker T$. The theorem is a consequence of (18) and (20).

(28) Let us consider a subset A of V and elements x, y of V. If $x - y \in \operatorname{Lin}(A)$, then $x \in \operatorname{Lin}(A \cup \{y\})$.

3. Some Basic Facts about Linearly Independent Subsets and Linear Combinations

Now we state the propositions:

(29) Let us consider a subset X of V. If V is a submodule of W, then X is a subset of W.

(30) Every subset of V is a subset of $\operatorname{Lin}(A)$.
PROOF: For every object x such that $x \in A$ holds $x \in$ the carrier of $\operatorname{Lin}(A)$ by [20, (65)]. □

(31) Let us consider a $\mathbb{Z}$-module V. Then every linearly independent subset of V is a basis of $\operatorname{Lin}(A)$. The theorem is a consequence of (30).

(32) Let us consider a finite rank, free $\mathbb{Z}$-module V, a subset A of V, and an element x of V. Suppose $x \in \operatorname{Lin}(A)$ and $x \notin A$. Then $A \cup \{x\}$ is linearly dependent. The theorem is a consequence of (31).

Let V be a finite rank, free $\mathbb{Z}$-module, W be a $\mathbb{Z}$-module, and T be a linear transformation from V to W. Let us note that $\ker T$ is finite rank and free.

From now on T denotes a linear transformation from V to W.

Now we state the propositions:

(33) Let us consider a finite rank, free $\mathbb{Z}$-module V, a subset A of V, a basis B of V, and a linear transformation T from V to W. Suppose A is a basis of $\ker T$ and $A \subseteq B$. Then $T\restriction(B \setminus A)$ is one-to-one. The theorem is a consequence of (27), (28), and (32).

(34) Let us consider a subset A of V, a linear combination l of A, an element x of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Then $l +\cdot (x, a)$ is a linear combination of $A \cup \{x\}$.
PROOF: Set $m = l +\cdot (x, a)$. $\operatorname{rng} m \subseteq$ the carrier of $\mathbb{Z}^{\mathrm{R}}$ by [13, (92)], [8, (31)], [12, (3)], [8, (32)]. Set $T =$ (the support of l)$\cup\{x\}$. For every element v of V such that $v \notin T$ holds $m(v) = 0_{\mathbb{Z}^{\mathrm{R}}}$ by [8, (32)]. The support of $m \subseteq T$ by [8, (32)]. □

In the sequel l denotes a linear combination of V.

Let V be a $\mathbb{Z}$-module. One can check that there exists a subset of V which is linearly dependent.

Let l be a linear combination of V and A be a subset of V. The functor $l[A]$ yielding a linear combination of A is defined by the term

(Def. 6) $l\restriction A +\cdot (A^{\mathrm{c}} \longmapsto 0_{\mathbb{Z}^{\mathrm{R}}})$.

Now we state the proposition:

(35) $l = l[$the support of $l]$.
PROOF: Set $f = l\restriction$(the support of l). Set $g =$ (the support of $l)^{\mathrm{c}} \longmapsto 0_{\mathbb{Z}^{\mathrm{R}}}$. Set $m = f +\cdot g$. For every object x such that $x \in \operatorname{dom} l$ holds $l(x) = m(x)$ by [12, (49)], [26, (7)]. □

Let us consider a subset A of V and an element v of V. Now we state the propositions:

(36) If $v \in A$, then $l[A](v) = l(v)$.

(37) If $v \notin A$, then $l[A](v) = 0_{\mathbb{Z}^{\mathrm{R}}}$.

Now we state the proposition:

(38) Let us consider subsets A, B of V and a linear combination l of B. If $A \subseteq B$, then $l = l[A] + l[B \setminus A]$. The theorem is a consequence of (37) and (36).

Let V be a $\mathbb{Z}$-module, l be a linear combination of V, and X be a subset of V. Let us note that $l^{\circ}X$ is finite.

Now we state the proposition:

(39) Let us consider a subset X of V. Suppose X misses the support of l. Then $l^{\circ}X \subseteq \{0_{\mathbb{Z}^{\mathrm{R}}}\}$.

Let V, W be $\mathbb{Z}$-modules, l be a linear combination of V, T be a linear transformation from V to W, and w be an element of W. The functor $\mathrm{CFS}(l, T, w)$ yielding a (the carrier of $\mathbb{Z}^{\mathrm{R}}$)-valued finite sequence is defined by the term

(Def. 7) $l \cdot \mathrm{CFS}(T^{-1}(\{w\}) \cap (\text{the support of } l))$.

From now on V, W denote $\mathbb{Z}$-modules, l denotes a linear combination of V, and T denotes a linear transformation from V to W.

Now we state the proposition:

(40) Let us consider non empty sets V, W, a finite sequence f, and a function l from V into W. Suppose $\mathrm{rng}\, f \subseteq V$. Then $l \cdot f$ is W-valued and finite sequence-like.

Let V, W be non empty sets, f be a V-valued finite sequence, and l be a function from V into W. One can check that $l \cdot f$ is W-valued and finite sequence-like.

Let A be a finite subset of V. Let us note that $l \cdot \mathrm{CFS}(A)$ is W-valued and finite sequence-like.

Let V be a $\mathbb{Z}$-module and l be a linear combination of V. One can check that $l \cdot \mathrm{CFS}(A)$ is (the carrier of $\mathbb{Z}^{\mathrm{R}}$)-valued and finite sequence-like.

Now we state the propositions:

(41) Let us consider non empty sets V, W, V-valued finite sequences f, g, and a function l from V into W. Then $l \cdot (f \frown g) = l \cdot f \frown (l \cdot g)$.

(42) Let us consider a $\mathbb{Z}$-module V, finite subsets A, B of V, a linear combination l of V, and finite sequences l_0, l_1, l_2 of elements of $\mathbb{Z}^{\mathrm{R}}$. Suppose $A \cap B = \emptyset$ and $l_0 = l \cdot \mathrm{CFS}(A \cup B)$ and $l_1 = l \cdot \mathrm{CFS}(A)$ and $l_2 = l \cdot \mathrm{CFS}(B)$. Then $\sum l_0 = \sum l_1 + \sum l_2$. The theorem is a consequence of (43).

(43) Let us consider a $\mathbb{Z}$-module V, a finite subset A of V, and linear combinations l, l_0 of V. Suppose $l\restriction(\text{the support of } l_0) = l_0\restriction(\text{the support of } l_0)$ and the support of $l_0 \subseteq$ the support of l and $A \subseteq$ the support of l_0. Then $\sum(l \cdot \mathrm{CFS}(A)) = \sum(l_0 \cdot \mathrm{CFS}(A))$.

Let V, W be $\mathbb{Z}$-modules, l be a linear combination of V, and T be a linear transformation from V to W. The functor $T \oplus l$ yielding a linear combination of W is defined by

(Def. 8) the support of $it \subseteq T^{\circ}(\text{the support of } l)$ and for every element w of W, $it(w) = \sum \mathrm{CFS}(l, T, w)$.

Now we state the propositions:

(44) $T \oplus l$ is a linear combination of $T^{\circ}(\text{the support of } l)$.

(45) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, a vector s of W, a subset A of V, and a linear combination l of A. Suppose for every vector v of V such that $v \in$ the support of l holds $T(v) = s$. Then $T(\sum l) = \sum \mathrm{CFS}(l, T, s) \cdot s$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every subset A of V for every linear combination l of A such that $\overline{\overline{\text{the support of } l}} = \$_1$ and for every vector v of V such that $v \in$ the support of l holds $T(v) = s$ holds $T(\sum l) = \sum \mathrm{CFS}(l, T, s) \cdot s$. $\mathcal{P}[0]$ by [20, (23)], [19, (1)], [29, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (44)], [17, (31)], [4, (42)], [13, (8)]. For every natural number n, $\mathcal{P}[n]$ from [5, Sch. 2]. □

(46) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, a subset A of V, a linear combination l of A, and a linear combination T_1 of T°(the support of l). If $T_1 = T \oplus l$, then $T(\sum l) = \sum T_1$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every subset A of V for every linear combination l of A for every linear combination T_1 of T°(the support of l) such that $T_1 = T \oplus l$ and $\overline{\overline{T^\circ(\text{the support of } l)}} = \$_1$ holds $T(\sum l) = \sum T_1$. $\mathcal{P}[0]$ by [20, (23)], [19, (1)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (44)], [17, (31)], [4, (42)], [13, (8)]. For every natural number n, $\mathcal{P}[n]$ from [5, Sch. 2]. □

Let us consider linear combinations l, m of V.

Let us assume that the support of l misses the support of m. Now we state the propositions:

(47) The support of $l + m$ = (the support of l) $\cup$ (the support of m).

Proof: (The support of l) $\cup$ (the support of m) $\subseteq$ the support of $l + m$ by [30, (22)], [20, (8)]. □

(48) The support of $l - m$ = (the support of l) $\cup$ (the support of m). The theorem is a consequence of (47).

Now we state the propositions:

(49) Let us consider a $\mathbb{Z}$-module V, a subset A of V, and linear combinations l_1, l_2 of A. Suppose the support of l_1 misses the support of l_2. Then the support of $l_1 - l_2$ = (the support of l_1) $\cup$ (the support of l_2). The theorem is a consequence of (47).

(50) Let us consider a free $\mathbb{Z}$-module V and subsets A, B of V. Suppose $A \subseteq B$ and B is a basis of V. Then V is the direct sum of $\mathrm{Lin}(A)$ and $\mathrm{Lin}(B \setminus A)$.

Proof: $\mathrm{Lin}(A) \cap \mathrm{Lin}(B \setminus A) = \mathbf{0}_V$ by [19, (54), (94)], [20, (64)], [22, (19)]. $\Omega_V = \mathrm{Lin}(A) + \mathrm{Lin}(B \setminus A)$ by [21, (14)], [20, (64)], (38), [20, (52)]. □

(51) Let us consider a subset A of V, a linear combination l of A, and an element v of V. Suppose $T{\restriction}A$ is one-to-one and $v \in A$. Then there exists a subset X of V such that

(i) X misses A, and

(ii) $T^{-1}(\{T(v)\}) = \{v\} \cup X$.

Proof: Set $X = T^{-1}(\{T(v)\}) \setminus \{v\}$. X misses A by [1, (7)], [32, (62)], [12, (49)]. $\{v\} \subseteq T^{-1}(\{T(v)\})$ by [1, (7)]. □

(52) Let us consider a subset X of V. Suppose X misses the support of l and $X \neq \emptyset$. Then $l^{\circ}X = \{0_{\mathbb{Z}^{\mathrm{R}}}\}$. The theorem is a consequence of (39).

(53) Let us consider an element w of W. Suppose $w \in$ the support of $T \oplus l$. Then $T^{-1}(\{w\})$ meets the support of l.

(54) Let us consider an element v of V. Suppose $T \restriction$(the support of l) is one-to-one and $v \in$ the support of l. Then $(T \oplus l)(T(v)) = l(v)$.

PROOF: For every object x, $x \in T^{-1}(\{T(v)\}) \cap$(the support of l) iff $x \in \{v\}$ by [13, (38)], [12, (49)], [32, (57)]. □

(55) Let us consider a finite sequence G of elements of V. Suppose $\operatorname{rng} G =$ the support of l and $T \restriction$(the support of l) is one-to-one. Then $T \cdot (l \cdot G) = (T \oplus l) \cdot (T \cdot G)$.

PROOF: Reconsider $R = (T \oplus l) \cdot (T \cdot G)$ as a finite sequence of elements of W. Reconsider $L = T \cdot (l \cdot G)$ as a finite sequence of elements of W. For every natural number k such that $1 \leqslant k \leqslant \operatorname{len} L$ holds $L(k) = R(k)$ by [12, (13), (3)], (54), [1, (7)]. □

(56) Suppose $T \restriction$(the support of l) is one-to-one. Then T°(the support of l) = the support of $T \oplus l$.

PROOF: T°(the support of l) $\subseteq$ the support of $T \oplus l$ by (54), [20, (8)]. □

(57) Let us consider a finite rank, free $\mathbb{Z}$-module V, a subset A of V, a basis B of V, a linear transformation T from V to W, and a linear combination l of $B \setminus A$. Suppose A is a basis of $\ker T$ and $A \subseteq B$. Then $T(\sum l) = \sum(T \oplus l)$. The theorem is a consequence of (33), (56), (55), and (16).

(58) Let us consider a subset X of V. Suppose X is linearly dependent. Then there exists a linear combination l of X such that

(i) the support of $l \neq \emptyset$, and

(ii) $\sum l = 0_V$.

Let V, W be $\mathbb{Z}$-modules, X be a subset of V, T be a linear transformation from V to W, and l be a linear combination of $T^{\circ}X$. Assume $T \restriction X$ is one-to-one. The functor $T\#l$ yielding a linear combination of X is defined by the term

(Def. 9) $l \cdot T {+\cdot} (X^{\mathrm{c}} \longmapsto 0_{\mathbb{Z}^{\mathrm{R}}})$.

Now we state the propositions:

(59) Let us consider a subset X of V, a linear combination l of $T^{\circ}X$, and an element v of V. If $v \in X$ and $T \restriction X$ is one-to-one, then $(T\#l)(v) = l(T(v))$.

(60) Let us consider a subset X of V and a linear combination l of $T^{\circ}X$. If $T \restriction X$ is one-to-one, then $T \oplus T\#l = l$. The theorem is a consequence of (53), (54), and (59).

References

[1] Jesse Alama. The rank+nullity theorem. *Formalized Mathematics*, 15(**3**):137–142, 2007. doi:10.2478/v10037-007-0015-6.

[2] Michael Francis Atiyah and Ian Grant Macdonald. *Introduction to Commutative Algebra*, volume 2. Addison-Wesley Reading, 1969.

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

[4] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 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] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

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

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

[10] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

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

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

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

[14] 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.

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

[16] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

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

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

[19] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. ℤ-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[20] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Quotient module of ℤ-module. *Formalized Mathematics*, 20(**3**):205–214, 2012. doi:10.2478/v10037-012-0024-y.

[21] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Free ℤ-module. *Formalized Mathematics*, 20(**4**):275–280, 2012. doi:10.2478/v10037-012-0033-x.

[22] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

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

[24] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.

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

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

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

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

[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.

[30] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1 (**5**):877–882, 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.

Received July 10, 2014