FORMALIZED MATHEMATICS
Vol. 20, No. 3, Pages 205–214, 2012
DOI: 10.2478/v10037-012-0024-y

VERSITA
versita.com/fm/

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

Yuichi Futa
Shinshu University
Nagano, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article we formalize a quotient module of $\mathbb{Z}$-module and a vector space constructed by the quotient module. We formally prove that for a $\mathbb{Z}$-module V and a prime number p, a quotient module V/pV has the structure of a vector space over $\mathbb{F}_p$. $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattices [14]. Some theorems in this article are described by translating theorems in [20] and [19] into theorems of $\mathbb{Z}$-module.

MML identifier: `ZMODUL02`, version: `7.14.01 4.183.1153`

The terminology and notation used here have been introduced in the following articles: [4], [1], [16], [3], [21], [9], [5], [6], [18], [13], [15], [17], [2], [7], [11], [24], [25], [22], [20], [23], [12], [8], and [10].

1. Quotient Module of $\mathbb{Z}$-module and Vector Space

For simplicity, we follow the rules: x is a set, V is a $\mathbb{Z}$-module, u, v are vectors of V, F, G, H are finite sequences of elements of V, i is an element of $\mathbb{N}$, and f, g are sequences of V.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $a \cdot V$ yielding a non empty subset of V is defined by:

(Def. 1) $a \cdot V = \{a \cdot v : v$ ranges over elements of $V\}$.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $\mathrm{Zero}(a, V)$ yielding an element of $a \cdot V$ is defined as follows:

(Def. 2) $\mathrm{Zero}(a, V) = 0_V$.

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

ISSN 1426–2630(p), 1898-9934(e)

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $\mathrm{Add}(a, V)$ yielding a function from $(a \cdot V) \times (a \cdot V)$ into $a \cdot V$ is defined by:

(Def. 3) $\mathrm{Add}(a, V) = (\text{the addition of } V)\restriction((a \cdot V) \times (a \cdot V))$.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $\mathrm{Mult}(a, V)$ yielding a function from $\mathbb{Z} \times (a \cdot V)$ into $a \cdot V$ is defined by:

(Def. 4) $\mathrm{Mult}(a, V) = (\text{the external multiplication of } V)\restriction(\mathbb{Z} \times (a \cdot V))$.

Let V be a $\mathbb{Z}$-module and let a be an integer number. The functor $a \circ V$ yields a submodule of V and is defined as follows:

(Def. 5) $a \circ V = \langle a \cdot V, \mathrm{Zero}(a, V), \mathrm{Add}(a, V), \mathrm{Mult}(a, V) \rangle$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{CosetSet}(V, W)$ yields a non empty family of subsets of V and is defined as follows:

(Def. 6) $\mathrm{CosetSet}(V, W) = \{A : A \text{ ranges over cosets of } W\}$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{addCoset}(V, W)$ yields a binary operation on $\mathrm{CosetSet}(V, W)$ and is defined as follows:

(Def. 7) For all elements A, B of $\mathrm{CosetSet}(V, W)$ and for all vectors a, b of V such that $A = a + W$ and $B = b + W$ holds $(\mathrm{addCoset}(V, W))(A, B) = a + b + W$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{zeroCoset}(V, W)$ yielding an element of $\mathrm{CosetSet}(V, W)$ is defined by:

(Def. 8) $\mathrm{zeroCoset}(V, W) = \text{the carrier of } W$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathrm{lmultCoset}(V, W)$ yields a function from $\mathbb{Z} \times \mathrm{CosetSet}(V, W)$ into $\mathrm{CosetSet}(V, W)$ and is defined as follows:

(Def. 9) For every integer z and for every element A of $\mathrm{CosetSet}(V, W)$ and for every vector a of V such that $A = a + W$ holds $(\mathrm{lmultCoset}(V, W))(z, A) = z \cdot a + W$.

Let V be a $\mathbb{Z}$-module and let W be a submodule of V. The functor $\mathbb{Z}\text{-ModuleQuot}(V, W)$ yields a strict $\mathbb{Z}$-module and is defined by the conditions (Def. 10).

(Def. 10)(i) The carrier of $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathrm{CosetSet}(V, W)$,

(ii) the addition of $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathrm{addCoset}(V, W)$,

(iii) $0_{\mathbb{Z}\text{-ModuleQuot}(V, W)} = \mathrm{zeroCoset}(V, W)$, and

(iv) the external multiplication of $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathrm{lmultCoset}(V, W)$.

The following propositions are true:

(1) Let p be an integer, V be a $\mathbb{Z}$-module, W be a submodule of V, and x be a vector of $\mathbb{Z}\text{-ModuleQuot}(V, W)$. If $W = p \circ V$, then $p \cdot x = 0_{\mathbb{Z}\text{-ModuleQuot}(V, W)}$.

(2) Let p, i be integers, V be a $\mathbb{Z}$-module, W be a submodule of V, and x be a vector of $\mathbb{Z}$-ModuleQuot(V, W). If $p \neq 0$ and $W = p \circ V$, then $i \cdot x = (i \bmod p) \cdot x$.

(3) Let p, q be integers, V be a $\mathbb{Z}$-module, W be a submodule of V, and v be a vector of V. Suppose $W = p \circ V$ and $p > 1$ and $q > 1$ and p and q are relative prime. If $q \cdot v = 0_V$, then $v + W = 0_{\mathbb{Z}\text{-ModuleQuot}(V,W)}$.

Let p be a prime number and let V be a $\mathbb{Z}$-module. The functor MultModpV(V, p) yields a function from (the carrier of GF(p)) $\times$ (the carrier of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$) into the carrier of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ and is defined by the condition (Def. 11).

(Def. 11) Let a be an element of GF(p), i be an integer, and x be an element of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$. If $a = i \bmod p$, then (MultModpV(V, p))$(a, x) = (i \bmod p) \cdot x$.

Let p be a prime number and let V be a $\mathbb{Z}$-module. The functor $\mathbb{Z}$-MQVectSp(V, p) yielding a non empty strict vector space structure over GF(p) is defined by:

(Def. 12) $\mathbb{Z}$-MQVectSp(V, p) = $\langle$the carrier of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$, the addition of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$, the zero of $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$, MultModpV$(V, p)\rangle$.

Let p be a prime number and let V be a $\mathbb{Z}$-module. Observe that $\mathbb{Z}$-MQVectSp(V, p) is scalar distributive, vector distributive, scalar associative, scalar unital, add-associative, right zeroed, right complementable, and Abelian.

Let p be a prime number, let V be a $\mathbb{Z}$-module, and let v be a vector of V. The functor $\mathbb{Z}$-MtoMQV(V, p, v) yields a vector of $\mathbb{Z}$-MQVectSp(V, p) and is defined as follows:

(Def. 13) $\mathbb{Z}$-MtoMQV$(V, p, v) = v + p \circ V$.

Let X be a $\mathbb{Z}$-module. The functor MultINT$*\,X$ yielding a function from (the carrier of $(\mathbb{Z}^{\mathrm{R}})$) $\times$ (the carrier of X) into the carrier of X is defined by:

(Def. 14) MultINT$*\,X$ = the external multiplication of X.

Let X be a $\mathbb{Z}$-module. The functor PreNorms X yielding a non empty strict vector space structure over $\mathbb{Z}^{\mathrm{R}}$ is defined by:

(Def. 15) PreNorms X = $\langle$the carrier of X, the addition of X, the zero of X, MultINT$*\,X\rangle$.

Let X be a $\mathbb{Z}$-module. Observe that PreNorms X is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$. The functor MultINT$*\,X$ yielding a function from $\mathbb{Z} \times$ the carrier of X into the carrier of X is defined as follows:

(Def. 16) MultINT$*\,X$ = the left multiplication of X.

Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$. The functor PreNorms X yields a non empty strict $\mathbb{Z}$-module structure and is defined as follows:

(Def. 17) PreNorms $X = \langle$the carrier of X, the zero of X, the addition of X, MultINT$*\,X\rangle$.

Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$. Note that PreNorms X is Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

We now state four propositions:

(4) Let X be a $\mathbb{Z}$-module, v, w be elements of X, and v_1, w_1 be elements of PreNorms X. If $v = v_1$ and $w = w_1$, then $v + w = v_1 + w_1$ and $v - w = v_1 - w_1$.

(5) Let X be a $\mathbb{Z}$-module, v be an element of X, v_1 be an element of PreNorms X, a be an integer, and a_1 be an element of $\mathbb{Z}^{\mathrm{R}}$. If $v = v_1$ and $a = a_1$, then $a \cdot v = a_1 \cdot v_1$.

(6) Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$, v, w be elements of X, and v_1, w_1 be elements of PreNorms X. If $v = v_1$ and $w = w_1$, then $v + w = v_1 + w_1$ and $v - w = v_1 - w_1$.

(7) Let X be a left module over $\mathbb{Z}^{\mathrm{R}}$, v be an element of X, v_1 be an element of PreNorms X, a be an element of $\mathbb{Z}^{\mathrm{R}}$, and a_1 be an integer. If $v = v_1$ and $a = a_1$, then $a \cdot v = a_1 \cdot v_1$.

2. Linear Combination of $\mathbb{Z}$-module

Let V be a non empty zero structure. An element of $\mathbb{Z}^{\text{the carrier of } V}$ is said to be a $\mathbb{Z}$-linear combination of V if:

(Def. 18) There exists a finite subset T of V such that for every element v of V such that $v \notin T$ holds it$(v) = 0$.

In the sequel K, L, L_1, L_2, L_3 denote $\mathbb{Z}$-linear combinations of V.

Let V be a non empty additive loop structure and let L be a $\mathbb{Z}$-linear combination of V. The support of L yielding a finite subset of V is defined by:

(Def. 19) The support of $L = \{v \in V\colon L(v) \neq 0\}$.

Next we state the proposition

(8) Let V be a non empty additive loop structure, L be a $\mathbb{Z}$-linear combination of V, and v be an element of V. Then $L(v) = 0$ if and only if $v \notin$ the support of L.

Let V be a non empty additive loop structure. The functor $\mathbb{Z}$-ZeroLC V yields a $\mathbb{Z}$-linear combination of V and is defined by:

(Def. 20) The support of $\mathbb{Z}$-ZeroLC $V = \emptyset$.

One can prove the following proposition

(9) For every non empty additive loop structure V and for every element v of V holds $(\mathbb{Z}\text{-ZeroLC}\,V)(v) = 0$.

Let V be a non empty additive loop structure and let A be a subset of V. A $\mathbb{Z}$-linear combination of V is said to be a $\mathbb{Z}$-linear combination of A if:

(Def. 21) The support of it $\subseteq A$.

For simplicity, we adopt the following convention: a, b are integers, G, H_1, H_2, F, F_1, F_2, F_3 are finite sequences of elements of V, A, B are subsets of V, v_1, v_2, v_3, u_1, u_2, u_3 are vectors of V, f is a function from the carrier of V into $\mathbb{Z}$, i is an element of $\mathbb{N}$, and l, l_1, l_2 are $\mathbb{Z}$-linear combinations of A.

One can prove the following propositions:

(10) If $A \subseteq B$, then l is a $\mathbb{Z}$-linear combination of B.

(11) $\mathbb{Z}\text{-ZeroLC}\,V$ is a $\mathbb{Z}$-linear combination of A.

(12) For every $\mathbb{Z}$-linear combination l of $\emptyset_{\text{the carrier of } V}$ holds $l = \mathbb{Z}\text{-ZeroLC}\,V$.

Let us consider V, F, f. The functor $f \cdot F$ yields a finite sequence of elements of V and is defined by:

(Def. 22) $\operatorname{len}(f \cdot F) = \operatorname{len} F$ and for every i such that $i \in \operatorname{dom}(f \cdot F)$ holds $(f \cdot F)(i) = f(F_i) \cdot F_i$.

Next we state several propositions:

(13) If $i \in \operatorname{dom} F$ and $v = F(i)$, then $(f \cdot F)(i) = f(v) \cdot v$.

(14) $f \cdot \varepsilon_{(\text{the carrier of } V)} = \varepsilon_{(\text{the carrier of } V)}$.

(15) $f \cdot \langle v \rangle = \langle f(v) \cdot v \rangle$.

(16) $f \cdot \langle v_1, v_2 \rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2 \rangle$.

(17) $f \cdot \langle v_1, v_2, v_3 \rangle = \langle f(v_1) \cdot v_1, f(v_2) \cdot v_2, f(v_3) \cdot v_3 \rangle$.

Let us consider V, L. The functor $\sum L$ yielding an element of V is defined by:

(Def. 23) There exists F such that F is one-to-one and $\operatorname{rng} F =$ the support of L and $\sum L = \sum (L \cdot F)$.

Next we state several propositions:

(18) $A \neq \emptyset$ and A is linearly closed iff for every l holds $\sum l \in A$.

(19) $\sum \mathbb{Z}\text{-ZeroLC}\,V = 0_V$.

(20) For every $\mathbb{Z}$-linear combination l of $\emptyset_{\text{the carrier of } V}$ holds $\sum l = 0_V$.

(21) For every $\mathbb{Z}$-linear combination l of $\{v\}$ holds $\sum l = l(v) \cdot v$.

(22) If $v_1 \neq v_2$, then for every $\mathbb{Z}$-linear combination l of $\{v_1, v_2\}$ holds $\sum l = l(v_1) \cdot v_1 + l(v_2) \cdot v_2$.

(23) If the support of $L = \emptyset$, then $\sum L = 0_V$.

(24) If the support of $L = \{v\}$, then $\sum L = L(v) \cdot v$.

(25) If the support of $L = \{v_1, v_2\}$ and $v_1 \neq v_2$, then $\sum L = L(v_1) \cdot v_1 + L(v_2) \cdot v_2$.

Let V be a non empty additive loop structure and let L_1, L_2 be $\mathbb{Z}$-linear combinations of V. Let us observe that $L_1 = L_2$ if and only if:

(Def. 24) For every element v of V holds $L_1(v) = L_2(v)$.

Let V be a non empty additive loop structure and let L_1, L_2 be $\mathbb{Z}$-linear combinations of V. Then $L_1 + L_2$ is a $\mathbb{Z}$-linear combination of V and it can be characterized by the condition:

(Def. 25) For every element v of V holds $(L_1 + L_2)(v) = L_1(v) + L_2(v)$.

Let us observe that the functor $L_1 + L_2$ is commutative.

The following propositions are true:

(26) The support of $L_1 + L_2 \subseteq$ (the support of L_1) $\cup$ (the support of L_2).

(27) Suppose L_1 is a $\mathbb{Z}$-linear combination of A and L_2 is a $\mathbb{Z}$-linear combination of A. Then $L_1 + L_2$ is a $\mathbb{Z}$-linear combination of A.

(28) $L_1 + (L_2 + L_3) = (L_1 + L_2) + L_3$.

Let us consider V, a, L. Note that $L + \mathbb{Z}\text{-ZeroLC}\,V$ reduces to L.

The functor $a \cdot L$ yielding a $\mathbb{Z}$-linear combination of V is defined as follows:

(Def. 26) For every v holds $(a \cdot L)(v) = a \cdot L(v)$.

We now state several propositions:

(29) If $a \neq 0$, then the support of $a \cdot L =$ the support of L.

(30) $0 \cdot L = \mathbb{Z}\text{-ZeroLC}\,V$.

(31) If L is a $\mathbb{Z}$-linear combination of A, then $a \cdot L$ is a $\mathbb{Z}$-linear combination of A.

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

(33) $a \cdot (L_1 + L_2) = a \cdot L_1 + a \cdot L_2$.

(34) $a \cdot (b \cdot L) = (a \cdot b) \cdot L$.

Let us consider V, L. One can check that $1 \cdot L$ reduces to L.

The functor $-L$ yielding a $\mathbb{Z}$-linear combination of V is defined as follows:

(Def. 27) $-L = (-1) \cdot L$.

Let us note that the functor $-L$ is involutive.

We now state four propositions:

(35) $(-L)(v) = -L(v)$.

(36) If $L_1 + L_2 = \mathbb{Z}\text{-ZeroLC}\,V$, then $L_2 = -L_1$.

(37) The support of $-L =$ the support of L.

(38) If L is a $\mathbb{Z}$-linear combination of A, then $-L$ is a $\mathbb{Z}$-linear combination of A.

Let us consider V, L_1, L_2. The functor $L_1 - L_2$ yields a $\mathbb{Z}$-linear combination of V and is defined as follows:

(Def. 28) $L_1 - L_2 = L_1 + -L_2$.

The following four propositions are true:

(39) $(L_1 - L_2)(v) = L_1(v) - L_2(v)$.

(40) The support of $L_1 - L_2 \subseteq$ (the support of L_1) $\cup$ (the support of L_2).

(41) Suppose L_1 is a $\mathbb{Z}$-linear combination of A and L_2 is a $\mathbb{Z}$-linear combination of A. Then $L_1 - L_2$ is a $\mathbb{Z}$-linear combination of A.

(42) $L - L = \mathbb{Z}\text{-ZeroLC}\, V$.

Let us consider V. The functor LC_V yielding a set is defined by:

(Def. 29) $x \in \mathrm{LC}_V$ iff x is a $\mathbb{Z}$-linear combination of V.

Let us consider V. One can verify that LC_V is non empty.

In the sequel e, e_1, e_2 denote elements of LC_V.

Let us consider V, e. The functor ${}^{@}e$ yielding a $\mathbb{Z}$-linear combination of V is defined by:

(Def. 30) ${}^{@}e = e$.

Let us consider V, L. The functor ${}^{@}L$ yielding an element of LC_V is defined by:

(Def. 31) ${}^{@}L = L$.

Let us consider V. The functor $+_{\mathrm{LC}_V}$ yields a binary operation on LC_V and is defined as follows:

(Def. 32) For all e_1, e_2 holds $+_{\mathrm{LC}_V}(e_1, e_2) = ({}^{@}e_1) + {}^{@}e_2$.

Let us consider V. The functor $\cdot_{\mathrm{LC}_V}$ yields a function from $\mathbb{Z} \times \mathrm{LC}_V$ into LC_V and is defined by:

(Def. 33) For all a, e holds $\cdot_{\mathrm{LC}_V}(\langle a, e\rangle) = a \cdot ({}^{@}e)$.

Let us consider V. The functor LC-$\mathbb{Z}$-Module V yielding a $\mathbb{Z}$-module structure is defined as follows:

(Def. 34) $\text{LC-}\mathbb{Z}\text{-Module}\, V = \langle \mathrm{LC}_V, {}^{@}\mathbb{Z}\text{-ZeroLC}\, V, +_{\mathrm{LC}_V}, \cdot_{\mathrm{LC}_V} \rangle$.

Let us consider V. One can check that LC-$\mathbb{Z}$-Module V is strict and non empty.

Let us consider V. Observe that LC-$\mathbb{Z}$-Module V is Abelian, add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, and scalar unital.

Next we state several propositions:

(43) The carrier of $\text{LC-}\mathbb{Z}\text{-Module}\, V = \mathrm{LC}_V$.

(44) $0_{\text{LC-}\mathbb{Z}\text{-Module}\, V} = \mathbb{Z}\text{-ZeroLC}\, V$.

(45) The addition of $\text{LC-}\mathbb{Z}\text{-Module}\, V = +_{\mathrm{LC}_V}$.

(46) The external multiplication of $\text{LC-}\mathbb{Z}\text{-Module}\, V = \cdot_{\mathrm{LC}_V}$.

(47) ${L_1}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} + {L_2}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = L_1 + L_2$.

(48) $a \cdot L^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = a \cdot L$.

(49) $-L^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = -L$.

(50) ${L_1}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} - {L_2}^{\text{LC-}\mathbb{Z}\text{-Module}\, V} = L_1 - L_2$.

Let us consider V, A. The functor LC-$\mathbb{Z}$-Module A yielding a strict submodule of LC-$\mathbb{Z}$-Module V is defined by:

(Def. 35) The carrier of LC-$\mathbb{Z}$-Module $A = \{l\}$.

3. Linearly Independent Subset of $\mathbb{Z}$-module

For simplicity, we use the following convention: W, W_1, W_2, W_3 are submodules of V, v, v_1 are vectors of V, C is a subset of V, T is a finite subset of V, L, L_1, L_2 are $\mathbb{Z}$-linear combinations of V, l is a $\mathbb{Z}$-linear combination of A, and G is a finite sequence of elements of the carrier of V.

One can prove the following propositions:

(51) $f \cdot (F \frown G) = (f \cdot F) \frown (f \cdot G)$.

(52) $\sum(L_1 + L_2) = \sum L_1 + \sum L_2$.

(53) $\sum(a \cdot L) = a \cdot \sum L$.

(54) $\sum(-L) = -\sum L$.

(55) $\sum(L_1 - L_2) = \sum L_1 - \sum L_2$.

Let us consider V, A. We say that A is linearly independent if and only if:

(Def. 36) For every l such that $\sum l = 0_V$ holds the support of $l = \emptyset$.

Let us consider V, A. We introduce A is linearly dependent as an antonym of A is linearly independent.

We now state three propositions:

(56) If $A \subseteq B$ and B is linearly independent, then A is linearly independent.

(57) If A is linearly independent, then $0_V \notin A$.

(58) $\emptyset_{\text{the carrier of } V}$ is linearly independent.

Let us consider V. Observe that there exists a subset of V which is linearly independent.

One can prove the following proposition

(59) If V inherits cancelable on multiplication, then $\{v\}$ is linearly independent iff $v \neq 0_V$.

Let us consider V. Note that $\{0_V\}$ is linearly dependent as a subset of V.

One can prove the following propositions:

(60) If $\{v_1, v_2\}$ is linearly independent, then $v_1 \neq 0_V$.

(61) $\{v, 0_V\}$ is linearly dependent.

(62) Suppose V inherits cancelable on multiplication. Then $v_1 \neq v_2$ and $\{v_1, v_2\}$ is linearly independent if and only if $v_2 \neq 0_V$ and for all a, b such that $b \neq 0$ holds $b \cdot v_1 \neq a \cdot v_2$.

(63) Suppose V inherits cancelable on multiplication. Then $v_1 \neq v_2$ and $\{v_1, v_2\}$ is linearly independent if and only if for all a, b such that $a \cdot v_1 + b \cdot v_2 = 0_V$ holds $a = 0$ and $b = 0$.

Let us consider V, A. The functor $\mathrm{Lin}(A)$ yielding a strict submodule of V is defined as follows:

(Def. 37) The carrier of $\mathrm{Lin}(A) = \{\sum l\}$.

The following propositions are true:

(64) $x \in \mathrm{Lin}(A)$ iff there exists l such that $x = \sum l$.

(65) If $x \in A$, then $x \in \mathrm{Lin}(A)$.

(66) $x \in \mathbf{0}_V$ iff $x = 0_V$.

(67) $\mathrm{Lin}(\emptyset_{\text{the carrier of } V}) = \mathbf{0}_V$.

(68) If $\mathrm{Lin}(A) = \mathbf{0}_V$, then $A = \emptyset$ or $A = \{0_V\}$.

(69) For every strict $\mathbb{Z}$-module V and for every subset A of V such that $A =$ the carrier of V holds $\mathrm{Lin}(A) = V$.

(70) If $A \subseteq B$, then $\mathrm{Lin}(A)$ is a submodule of $\mathrm{Lin}(B)$.

(71) For every strict $\mathbb{Z}$-module V and for all subsets A, B of V such that $\mathrm{Lin}(A) = V$ and $A \subseteq B$ holds $\mathrm{Lin}(B) = V$.

(72) $\mathrm{Lin}(A \cup B) = \mathrm{Lin}(A) + \mathrm{Lin}(B)$.

(73) $\mathrm{Lin}(A \cap B)$ is a submodule of $\mathrm{Lin}(A) \cap \mathrm{Lin}(B)$.

4. Theorems Related to Submodule

One can prove the following propositions:

(74) If W_1 is a submodule of W_3, then $W_1 \cap W_2$ is a submodule of W_3.

(75) If W_1 is a submodule of W_2 and a submodule of W_3, then W_1 is a submodule of $W_2 \cap W_3$.

(76) If W_1 is a submodule of W_3 and W_2 is a submodule of W_3, then $W_1 + W_2$ is a submodule of W_3.

(77) If W_1 is a submodule of W_2, then W_1 is a submodule of $W_2 + W_3$.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[3] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[4] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[5] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[6] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[7] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012, doi: 10.2478/v10037-012-0007-z.

[11] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**):841–845, 1990.
[12] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[13] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[14] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective (the international series in engineering and computer science). 2002.
[15] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[16] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[17] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[18] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[19] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(**5**):847–850, 1990.
[20] Wojciech A. Trybulec. Linear combinations in real linear space. *Formalized Mathematics*, 1(**3**):581–588, 1990.
[21] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[22] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[23] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[24] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[25] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received May 7, 2012