Quotient Module of $\mathbb{Z}$-module

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

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

(Def. 2) Zero$(a, V) = 0_V$.

This work was supported by JSPS KAKENHI 22300285.
Let $V$ be a $\mathbb{Z}$-module and let $a$ be an integer number. The functor $\text{Add}(a,V)$ yielding a function from $(a \cdot V) \times (a \cdot V)$ into $a \cdot V$ is defined by:

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

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

(Def. 4) \quad \text{Mult}(a,V) = (\text{the external multiplication of } V)|(\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) \quad a \circ V = \langle \langle a \cdot V, \text{Zero}(a,V), \text{Add}(a,V), \text{Mult}(a,V) \rangle \rangle.$

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

(Def. 6) \quad \text{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 $\text{addCoset}(V,W)$ yields a binary operation on $\text{CosetSet}(V,W)$ and is defined as follows:

(Def. 7) \quad \text{For all elements } A, B \text{ of } \text{CosetSet}(V,W) \text{ and for all vectors } a, b \text{ of } V \text{ such that } A = a + W \text{ and } B = b + W \text{ holds } \text{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 $\text{zeroCoset}(V,W)$ yielding an element of $\text{CosetSet}(V,W)$ is defined by:

(Def. 8) \quad \text{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 $\text{lmultCoset}(V,W)$ yields a function from $\mathbb{Z} \times \text{CosetSet}(V,W)$ into $\text{CosetSet}(V,W)$ and is defined as follows:

(Def. 9) \quad \text{For every integer } z \text{ and for every element } A \text{ of } \text{CosetSet}(V,W) \text{ and for every vector } a \text{ of } V \text{ such that } A = a + W \text{ holds } \text{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 $\text{Z-ModuleQuot}(V,W)$ yields a strict $\mathbb{Z}$-module and is defined by the conditions (Def. 10).

(Def. 10)(i) \quad \text{The carrier of } \text{Z-ModuleQuot}(V,W) = \text{CosetSet}(V,W),$
(ii) \quad \text{the addition of } \text{Z-ModuleQuot}(V,W) = \text{addCoset}(V,W),$
(iii) \quad 0_{\text{Z-ModuleQuot}(V,W)} = \text{zeroCoset}(V,W), \text{ and}$
(iv) \quad \text{the external multiplication of } \text{Z-ModuleQuot}(V,W) = \text{lmultCoset}(V,W).$

The following propositions are true:

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

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 $v + W = 0_{\text{Z-ModuleQuot}(V,W)}$.

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

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

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

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

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

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

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

(Def. 14) $\text{MultINT}^* X = \text{the external multiplication of } X$.

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

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

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

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

(Def. 16) $\text{MultINT}^* X = \text{the left multiplication of } X$. 
Let $X$ be a left module over $\mathbb{Z}^R$. The functor PreNorms $X$ yields a non empty strict $\mathbb{Z}$-module structure and is defined as follows:

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

Let $X$ be a left module over $\mathbb{Z}^R$. 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 $\mathbb{Z}^R$. 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 $\mathbb{Z}^R$, $v, w$ 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 $\mathbb{Z}^R$, $v$ be an element of $X$, $v_1$ be an element of PreNorms $X$, $a$ be an element of $\mathbb{Z}^R$, 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 $\mathbb{Z}$ 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 $v \not\in T$ 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 $L = \{ v \in V: L(v) \neq 0 \}$.

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 $v \not\in$ 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
For every non empty additive loop structure $V$ and for every element $v$ of $V$ holds $(Z\text{-ZeroLC } V)(v) = 0$.

Let $V$ be a non empty additive loop structure and let $A$ be a subset of $V$. A $Z$-linear combination of $V$ is said to be a $Z$-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 $Z$-linear combinations of $A$.

One can prove the following propositions:

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

(11) $Z$-ZeroLC $V$ is a $Z$-linear combination of $A$.

(12) For every $Z$-linear combination $l$ of $\emptyset\text{the carrier of } V$ holds $l = Z$-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) $\text{len}(f \cdot F) = \text{len } F$ and for every $i$ such that $i \in \text{dom}(f \cdot F)$ holds $(f \cdot F)(i) = f(F_i) \cdot F_i$.

Next we state several propositions:

(13) If $i \in \text{dom } F$ 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) $f \cdot \langle v, v \rangle = \langle f(v) \cdot v \rangle$.

(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 $\text{rng } F = \text{the support of } L$ 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) $\sum Z\text{-ZeroLC } V = 0_V$.

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

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

(22) If $v_1 \neq v_2$, then for every $Z$-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 $L_1 + L_2 \subseteq \text{(the support of } L_1 \cup \text{the support of } L_2)$. 
(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 $L + \mathbb{Z}$-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 $a \cdot L = \text{the support of } L$.

(30) $0 \cdot L = \mathbb{Z}$-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 $L_1 + L_2 = \mathbb{Z}$-ZeroLC $V$, then $L_2 = -L_1$.

(37) The support of $-L = \text{the support of } L$.

(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 \(L_1 - L_2 \subseteq (\text{the support of } L_1) \cup (\text{the support of } L_2)\).

(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{Zero}\(\mathbb{Z}\)-LC\(V\).

Let us consider \(V\). The functor \(\text{LC}\(V\) yielding a set is defined by:

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

Let us consider \(V\). One can verify that \(\text{LC}\(V\) is non empty.

In the sequel \(e, e_1, e_2\) denote elements of \(\text{LC}\(V\).

Let us consider \(V, e\). The functor \(\overline{\cdot} e\) yielding a \(\mathbb{Z}\)-linear combination of \(V\) is defined by:

(Def. 30) \(\overline{\cdot} e = e\).

Let us consider \(V, L\). The functor \(\overline{\cdot} L\) yielding an element of \(\text{LC}\(V\) is defined by:

(Def. 31) \(\overline{\cdot} L = L\).

Let us consider \(V\). The functor \(+_{\text{LC}\(V\)}\) yields a binary operation on \(\text{LC}\(V\) and is defined as follows:

(Def. 32) For all \(e_1, e_2\) holds \(+_{\text{LC}\(V\)}(e_1, e_2) = (\overline{\cdot} e_1) + (\overline{\cdot} e_2)\).

Let us consider \(V\). The functor \(\cdot_{\text{LC}\(V\)}\) yields a function from \(\mathbb{Z} \times \text{LC}\(V\) into \(\text{LC}\(V\) and is defined by:

(Def. 33) For all \(a, e\) holds \(\cdot_{\text{LC}\(V\}}(\langle a, e \rangle) = a \cdot (\overline{\cdot} e)\).

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

(Def. 34) \(\text{LC-\(Z\)-\text{Module}}\(V = \langle \text{LC}\(V, \overline{\cdot} \text{Z-}\text{Zero}\(\text{LC}\(V, +_{\text{LC}\(V)}\cdot_{\text{LC}\(V}\rangle\).

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

Let us consider \(V\). Observe that \(\text{LC-\(Z\)-\text{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-\(Z\)-\text{Module}}\(V = \text{LC}\(V\).

(44) \(0_{\text{LC-\(Z\)-\text{Module}}\(V = \text{Z-}\text{Zero}\(\text{LC}\(V\).

(45) The addition of \(\text{LC-\(Z\)-\text{Module}}\(V = +_{\text{LC}\(V\).

(46) The external multiplication of \(\text{LC-\(Z\)-\text{Module}}\(V = \cdot_{\text{LC}\(V\).

(47) \(L_1 +_{\text{LC-\(Z\)-\text{Module}}\(V + L_2 +_{\text{LC-\(Z\)-\text{Module}}\(V = L_1 + L_2\).

(48) \(a \cdot L +_{\text{LC-\(Z\)-\text{Module}}\(V = a \cdot L\).

(49) \(-L +_{\text{LC-\(Z\)-\text{Module}}\(V = -L\).

(50) \(L_1 +_{\text{LC-\(Z\)-\text{Module}}\(V - L_2 +_{\text{LC-\(Z\)-\text{Module}}\(V = L_1 - L_2\).
Let us consider \( V, A \). The functor \( \text{LC-} \mathbb{Z} \text{-Module} A \) yielding a strict submodule of \( \text{LC-} \mathbb{Z} \text{-Module} V \) is defined by:

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

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) \( f \cdot (F \circ G) = (f \cdot F) \circ (f \cdot G) \).
(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 \( 0 \vDash A \).
(58) \( \emptyset \) 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 \( v \neq 0 \).

Let us consider \( V \). Note that \( \{ 0 \vDash \} \) is linearly dependent as a subset of \( V \).

One can prove the following propositions:

(60) If \( \{ v_1, v_2 \} \) is linearly independent, then \( v_1 \neq 0 \).
(61) \( \{ v, 0 \vDash \} \) 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 \( v_2 \neq 0 \) 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 \( a \cdot v_1 + b \cdot v_2 = 0 \vDash \) holds \( a = 0 \) and \( b = 0 \).
Let us consider $V$, $A$. The functor $\text{Lin}(A)$ yielding a strict submodule of $V$ is defined as follows:

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

The following propositions are true:

(64) $x \in \text{Lin}(A)$ iff there exists $l$ such that $x = \sum l$.
(65) If $x \in A$, then $x \in \text{Lin}(A)$.
(66) $x \in 0_V$ iff $x = 0_V$.
(67) $\text{Lin}(\emptyset)$, the carrier of $V$, $= 0_V$.
(68) If $\text{Lin}(A) = 0_V$, then $A = \emptyset$ or $A = \{0_V\}$.
(69) For every strict $\mathbb{Z}$-module $V$ and every subset $A$ of $V$ such that $A = \text{the carrier of } V$ holds $\text{Lin}(A) = V$.
(70) If $A \subseteq B$, then $\text{Lin}(A)$ is a submodule of $\text{Lin}(B)$.
(71) For every strict $\mathbb{Z}$-module $V$ and for all subsets $A$, $B$ of $V$ such that $\text{Lin}(A) = V$ and $A \subseteq B$ holds $\text{Lin}(B) = V$.
(72) $\text{Lin}(A \cup B) = \text{Lin}(A) + \text{Lin}(B)$.
(73) $\text{Lin}(A \cap B)$ is a submodule of $\text{Lin}(A) \cap \text{Lin}(B)$.

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

Received May 7, 2012