

# Submodule of free $\mathbb{Z}$ -module<sup>1</sup>

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 free  $\mathbb{Z}$ -module and its property. In particular, we formalize the vector space of rational field corresponding to a free  $\mathbb{Z}$ -module and prove formally that submodules of a free  $\mathbb{Z}$ -module are free.  $\mathbb{Z}$ -module is necessary for lattice problems - LLL (Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattice [20]. Some theorems in this article are described by translating theorems in [11] into theorems of  $\mathbb{Z}$ -module, however their proofs are different.

MSC: 13C10 15A03 03B35

Keywords: free  $\mathbb{Z}$ -module; submodule of free  $\mathbb{Z}$ -module

MML identifier: ZMODUL04, version: 8.1.02 5.22.1194

The notation and terminology used in this paper have been introduced in the following articles: [6], [1], [24], [22], [5], [12], [7], [8], [16], [25], [19], [23], [21], [3], [4], [9], [17], [30], [32], [31], [26], [29], [18], [27], [28], [33], [10], [13], [14], and [15].

## 1. VECTOR SPACE OF RATIONAL FIELD GENERATED BY A FREE $\mathbb{Z}$ -MODULE

From now on  $V$  denotes a  $\mathbb{Z}$ -module and  $W, W_1, W_2$  denote submodules of  $V$ .

Let us consider a  $\mathbb{Z}$ -module  $V$ , submodules  $W_1, W_2$  of  $V$ , and submodules  $W_5, W_6$  of  $W_1 + W_2$ . Now we state the propositions:

- (1) If  $W_5 = W_1$  and  $W_6 = W_2$ , then  $W_1 + W_2 = W_5 + W_6$ .
- (2) If  $W_5 = W_1$  and  $W_6 = W_2$ , then  $W_1 \cap W_2 = W_5 \cap W_6$ .

---

<sup>1</sup>This work was supported by JSPS KAKENHI 21240001 and 22300285.

Let  $V$  be a  $\mathbb{Z}$ -module. Note that (the carrier of  $V$ )  $\times (\mathbb{Z} \setminus \{0\})$  is non empty.

Assume  $V$  is cancelable on multiplication. The functor  $\text{EQRZM}(V)$  yielding an equivalence relation of (the carrier of  $V$ )  $\times (\mathbb{Z} \setminus \{0\})$  is defined by

- (Def. 1) Let us consider elements  $S, T$ . Then  $\langle S, T \rangle \in it$  if and only if  $S, T \in (\text{the carrier of } V) \times (\mathbb{Z} \setminus \{0\})$  and there exist elements  $z_1, z_2$  of  $V$  and there exist integers  $i_1, i_2$  such that  $S = \langle z_1, i_1 \rangle$  and  $T = \langle z_2, i_2 \rangle$  and  $i_1 \neq 0$  and  $i_2 \neq 0$  and  $i_2 \cdot z_1 = i_1 \cdot z_2$ .

Now we state the proposition:

- (3) Let us consider a  $\mathbb{Z}$ -module  $V$ , elements  $z_1, z_2$  of  $V$ , and integers  $i_1, i_2$ . Suppose  $V$  is cancelable on multiplication. Then  $\langle \langle z_1, i_1 \rangle, \langle z_2, i_2 \rangle \rangle \in \text{EQRZM}(V)$  if and only if  $i_1 \neq 0$  and  $i_2 \neq 0$  and  $i_2 \cdot z_1 = i_1 \cdot z_2$ .

Let  $V$  be a  $\mathbb{Z}$ -module. Assume  $V$  is cancelable on multiplication. The functor  $\text{addCoset } V$  yielding a binary operation on  $\text{Classes EQRZM}(V)$  is defined by

- (Def. 2) Let us consider elements  $A, B$ . Suppose  $A, B \in \text{Classes EQRZM}(V)$ . Let us consider elements  $z_1, z_2$  of  $V$  and integers  $i_1, i_2$ . Suppose

- (i)  $i_1 \neq 0$ , and
- (ii)  $i_2 \neq 0$ , and
- (iii)  $A = [\langle z_1, i_1 \rangle]_{\text{EQRZM}(V)}$ , and
- (iv)  $B = [\langle z_2, i_2 \rangle]_{\text{EQRZM}(V)}$ .

Then  $it(A, B) = [\langle i_2 \cdot z_1 + i_1 \cdot z_2, i_1 \cdot i_2 \rangle]_{\text{EQRZM}(V)}$ .

Assume  $V$  is cancelable on multiplication. The functor  $\text{zeroCoset } V$  yielding an element of  $\text{Classes EQRZM}(V)$  is defined by

- (Def. 3) Let us consider an integer  $i$ . Suppose  $i \neq 0$ . Then  $it = [\langle 0_V, i \rangle]_{\text{EQRZM}(V)}$ .

Assume  $V$  is cancelable on multiplication. The functor  $\text{lmultCoset } V$  yielding a function from (the carrier of  $\mathbb{F}_{\mathbb{Q}}$ )  $\times \text{Classes EQRZM}(V)$  into  $\text{Classes EQRZM}(V)$  is defined by

- (Def. 4) Let us consider an element  $q$  and an element  $A$ . Suppose

- (i)  $q \in \mathbb{Q}$ , and
- (ii)  $A \in \text{Classes EQRZM}(V)$ .

Let us consider integers  $m, n, i$  and an element  $z$  of  $V$ . Suppose

- (iii)  $n \neq 0$ , and
- (iv)  $q = \frac{m}{n}$ , and
- (v)  $i \neq 0$ , and
- (vi)  $A = [\langle z, i \rangle]_{\text{EQRZM}(V)}$ .

Then  $it(q, A) = [\langle m \cdot z, n \cdot i \rangle]_{\text{EQRZM}(V)}$ .

Now we state the propositions:

- (4) Let us consider a  $\mathbb{Z}$ -module  $V$ , an element  $z$  of  $V$ , and integers  $i, n$ . Suppose

- (i)  $i \neq 0$ , and
- (ii)  $n \neq 0$ , and
- (iii)  $V$  is cancelable on multiplication.

Then  $[\langle z, i \rangle]_{\text{EQRZM}(V)} = [\langle n \cdot z, n \cdot i \rangle]_{\text{EQRZM}(V)}$ . The theorem is a consequence of (3).

- (5) Let us consider a  $\mathbb{Z}$ -module  $V$  and an element  $v$  of  $\langle \text{Classes EQRZM}(V), \text{addCoset } V, \text{zeroCoset } V, \text{lmultCoset } V \rangle$ . Suppose  $V$  is cancelable on multiplication. Then there exists an integer  $i$  and there exists an element  $z$  of  $V$  such that  $i \neq 0$  and  $v = [\langle z, i \rangle]_{\text{EQRZM}(V)}$ .

Let  $V$  be a  $\mathbb{Z}$ -module. Assume  $V$  is cancelable on multiplication. The functor  $\text{ZMQVectSp}(V)$  yielding a vector space over  $\mathbb{F}_{\mathbb{Q}}$  is defined by the term

(Def. 5)  $\langle \text{Classes EQRZM}(V), \text{addCoset } V, \text{zeroCoset } V, \text{lmultCoset } V \rangle$ .

Assume  $V$  is cancelable on multiplication. The functor  $\text{MorphsZQ}(V)$  yielding a function from  $V$  into  $\text{ZMQVectSp}(V)$  is defined by

- (Def. 6) (i)  $it$  is one-to-one, and
- (ii) for every element  $v$  of  $V$ ,  $it(v) = [\langle v, 1 \rangle]_{\text{EQRZM}(V)}$ , and
  - (iii) for every elements  $v, w$  of  $V$ ,  $it(v + w) = it(v) + it(w)$ , and
  - (iv) for every element  $v$  of  $V$  and for every integer  $i$  and for every element  $q$  of  $\mathbb{F}_{\mathbb{Q}}$  such that  $i = q$  holds  $it(i \cdot v) = q \cdot it(v)$ , and
  - (v)  $it(0_V) = 0_{\text{ZMQVectSp}(V)}$ .

Now we state the propositions:

- (6) Let us consider a  $\mathbb{Z}$ -module  $V$ . Suppose  $V$  is cancelable on multiplication. Let us consider a finite sequence  $s$  of elements of  $V$  and a finite sequence  $t$  of elements of  $\text{ZMQVectSp}(V)$ . Suppose

- (i)  $\text{len } s = \text{len } t$ , and
- (ii) for every element  $i$  of  $\mathbb{N}$  such that  $i \in \text{dom } s$  there exists a vector  $s_1$  of  $V$  such that  $s_1 = s(i)$  and  $t(i) = (\text{MorphsZQ}(V))(s_1)$ .

Then  $\sum t = (\text{MorphsZQ}(V))(\sum s)$ . PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv$  for every finite sequence  $s$  of elements of  $V$  for every finite sequence  $t$  of elements of  $\text{ZMQVectSp}(V)$  such that  $\text{len } s = \text{len } t$  and for every element  $i$  of  $\mathbb{N}$  such that  $i \in \text{dom } s$  there exists a vector  $s_1$  of  $V$  such that  $s_1 = s(i)$  and  $t(i) = (\text{MorphsZQ}(V))(s_1)$  holds  $\sum t = (\text{MorphsZQ}(V))(\sum s)$ .  $\mathcal{P}[0]$  by [26, (43)]. For every natural number  $k$  such that  $\mathcal{P}[k]$  holds  $\mathcal{P}[k+1]$  by [5, (59)], [3, (11)], [5, (4)]. For every natural number  $k$ ,  $\mathcal{P}[k]$  from [3, Sch. 2].  $\square$

- (7) Let us consider a  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ , a  $z$  linear combination  $l$  of  $I$ , and a linear combination  $l_5$  of  $I_6$ . Suppose

- (i)  $V$  is cancelable on multiplication, and
- (ii)  $I_6 = (\text{MorphsZQ}(V))^\circ I$ , and
- (iii)  $l = l_5 \cdot \text{MorphsZQ}(V)$ .

Then  $\sum l_5 = (\text{MorphsZQ}(V))(\sum l)$ . The theorem is a consequence of (6).

- (8) Let us consider a  $\mathbb{Z}$ -module  $V$ , a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ , and a linear combination  $l_5$  of  $I_6$ . Then there exists an integer  $m$  and there exists an element  $a$  of  $\mathbb{F}_\mathbb{Q}$  such that  $m \neq 0$  and  $m = a$  and  $\text{rng}(a \cdot l_5) \subseteq \mathbb{Z}$ . PROOF: Define  $\mathcal{P}[\text{natural number}] \equiv$  for every linear combination  $l_5$  of  $I_6$  such that  $\overline{\text{the support of } l_5} = \$1$  there exists an integer  $m$  and there exists an element  $a$  of  $\mathbb{F}_\mathbb{Q}$  such that  $m \neq 0$  and  $m = a$  and  $\text{rng}(a \cdot l_5) \subseteq \mathbb{Z}$ .  $\mathcal{P}[0]$  by [27, (28)], [8, (113)], [27, (3)]. For every natural number  $n$  such that  $\mathcal{P}[n]$  holds  $\mathcal{P}[n+1]$  by [2, (44)], [10, (31)], [2, (42)]. For every natural number  $n$ ,  $\mathcal{P}[n]$  from [3, Sch. 2].  $\square$

- (9) Let us consider a  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ , and a linear combination  $l_5$  of  $I_6$ . Suppose

- (i)  $V$  is cancelable on multiplication, and
- (ii)  $I_6 = (\text{MorphsZQ}(V))^\circ I$ .

Then there exists an integer  $m$  and there exists an element  $a$  of  $\mathbb{F}_\mathbb{Q}$  and there exists a  $z$  linear combination  $l$  of  $I$  such that  $m \neq 0$  and  $m = a$  and  $l = (a \cdot l_5) \cdot \text{MorphsZQ}(V)$  and  $(\text{MorphsZQ}(V))^{-1}(\text{the support of } l_5) = \text{the support of } l$ . The theorem is a consequence of (8). PROOF: Consider  $m$  being an integer,  $a$  being an element of  $\mathbb{F}_\mathbb{Q}$  such that  $m \neq 0$  and  $m = a$  and  $\text{rng}(a \cdot l_5) \subseteq \mathbb{Z}$ . Reconsider  $l = (a \cdot l_5) \cdot \text{MorphsZQ}(V)$  as an element of  $\mathbb{Z}^{\text{the carrier of } V}$ . Set  $T = \{v, \text{ where } v \text{ is an element of } V : l(v) \neq 0\}$ . Set  $F = \text{MorphsZQ}(V)$ .  $T \subseteq F^{-1}(\text{the support of } l_5)$  by [7, (13)], [8, (38)].  $F^{-1}(\text{the support of } l_5) \subseteq T$  by [8, (38)], [7, (13)].  $\square$

- (10) Let us consider a  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ , a linear combination  $l_5$  of  $I_6$ , an integer  $m$ , an element  $a$  of  $\mathbb{F}_\mathbb{Q}$ , and a  $z$  linear combination  $l$  of  $I$ . Suppose

- (i)  $V$  is cancelable on multiplication, and
- (ii)  $I_6 = (\text{MorphsZQ}(V))^\circ I$ , and
- (iii)  $m \neq 0$ , and
- (iv)  $m = a$ , and
- (v)  $l = (a \cdot l_5) \cdot \text{MorphsZQ}(V)$ .

Then  $a \cdot \sum l_5 = (\text{MorphsZQ}(V))(\sum l)$ . The theorem is a consequence of (7).

(11) Let us consider a  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , and a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ . Suppose

- (i)  $V$  is cancelable on multiplication, and
- (ii)  $I_6 = (\text{MorphsZQ}(V))^\circ I$ , and
- (iii)  $I$  is linearly independent.

Then  $I_6$  is linearly independent. The theorem is a consequence of (9) and (10).

(12) Let us consider a  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , a  $\mathbb{Z}$  linear combination  $l$  of  $I$ , and a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ . Suppose

- (i)  $V$  is cancelable on multiplication, and
- (ii)  $I_6 = (\text{MorphsZQ}(V))^\circ I$ .

Then there exists a linear combination  $l_5$  of  $I_6$  such that

- (iii)  $l = l_5 \cdot \text{MorphsZQ}(V)$ , and
- (iv) the support of  $l_5 = (\text{MorphsZQ}(V))^\circ$  the support of  $l$ .

PROOF: Reconsider  $I_0 = \text{the support of } l \text{ as a finite subset of } V$ . Reconsider  $I_7 = (\text{MorphsZQ}(V))^\circ I_0$  as a finite subset of  $\text{ZMQVectSp}(V)$ . Define  $\mathcal{P}[\text{element}, \text{element}] \equiv \$1 \in I_7$  and there exists an element  $v$  of  $V$  such that  $v \in I_0$  and  $\$1 = (\text{MorphsZQ}(V))(v)$  and  $\$2 = l(v)$  or  $\$1 \notin I_7$  and  $\$2 = 0_{\mathbb{F}_Q}$ . For every element  $x$  such that  $x \in \text{the carrier of } \text{ZMQVectSp}(V)$  there exists an element  $y$  such that  $y \in \mathbb{Q}$  and  $\mathcal{P}[x, y]$  by [8, (64)]. Consider  $l_5$  being a function from the carrier of  $\text{ZMQVectSp}(V)$  into  $\mathbb{Q}$  such that for every element  $x$  such that  $x \in \text{the carrier of } \text{ZMQVectSp}(V)$  holds  $\mathcal{P}[x, l_5(x)]$  from [8, Sch. 1]. The support of  $l_5 \subseteq I_7$ . For every element  $x$  such that  $x \in \text{dom } l$  holds  $l(x) = (l_5 \cdot \text{MorphsZQ}(V))(x)$  by [8, (35), (19)], [7, (12)].  $I_7 \subseteq \text{the support of } l_5$  by [8, (64)], [7, (12)], [14, (8)].  $\square$

(13) Let us consider a free  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ , a  $\mathbb{Z}$  linear combination  $l$  of  $I$ , and an integer  $i$ . Suppose

- (i)  $i \neq 0$ , and
- (ii)  $I_6 = (\text{MorphsZQ}(V))^\circ I$ .

Then  $[\{\sum l, i\}]_{\text{EQRZM}(V)} \in \text{Lin}(I_6)$ . The theorem is a consequence of (12) and (7).

Let us consider a free  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , and a subset  $I_6$  of  $\text{ZMQVectSp}(V)$ . Now we state the propositions:

- (14) If  $I_6 = (\text{MorphsZQ}(V))^\circ I$ , then  $\overline{I} = \overline{I_6}$ .
- (15) If  $I_6 = (\text{MorphsZQ}(V))^\circ I$  and  $I$  is a basis of  $V$ , then  $I_6$  is a basis of  $\text{ZMQVectSp}(V)$ .

Let  $V$  be a finite-rank free  $\mathbb{Z}$ -module. Note that  $\text{ZMQVectSp}(V)$  is finite dimensional.

Now we state the propositions:

- (16) Let us consider a finite-rank free  $\mathbb{Z}$ -module  $V$ . Then  $\text{rank } V = \dim(\text{ZMQVectSp}(V))$ . The theorem is a consequence of (15) and (14).
- (17) Let us consider a free  $\mathbb{Z}$ -module  $V$  and finite subsets  $I, A$  of  $V$ . Suppose
  - (i)  $I$  is a basis of  $V$ , and
  - (ii)  $\overline{I} + 1 = \overline{A}$ .

Then  $A$  is linearly dependent. The theorem is a consequence of (15), (11), and (14).

- (18) Let us consider a free  $\mathbb{Z}$ -module  $V$  and subsets  $A, B$  of  $V$ . If  $A$  is linearly dependent and  $A \subseteq B$ , then  $B$  is linearly dependent.
- (19) Let us consider a free  $\mathbb{Z}$ -module  $V$  and subsets  $D, A$  of  $V$ . Suppose
  - (i)  $D$  is basis of  $V$  and finite, and
  - (ii)  $\overline{D} \subset \overline{A}$ .

Then  $A$  is linearly dependent. The theorem is a consequence of (17) and (18).

- (20) Let us consider a free  $\mathbb{Z}$ -module  $V$  and subsets  $I, A$  of  $V$ . Suppose
  - (i)  $I$  is basis of  $V$  and finite, and
  - (ii)  $A$  is linearly independent.

Then  $\overline{A} \subseteq \overline{I}$ .

## 2. SUBMODULE OF FREE $\mathbb{Z}$ -MODULE

Now we state the proposition:

- (21) Let us consider a  $\mathbb{Z}$ -module  $V$ . If  $\Omega_V$  is free, then  $V$  is free.

Let us consider a  $\mathbb{Z}$ -module  $V$ , submodules  $W_1, W_2$  of  $V$ , and strict submodules  $W_3, W_4$  of  $V$ . Now we state the propositions:

- (22) If  $W_3 = \Omega_{W_1}$  and  $W_4 = \Omega_{W_2}$ , then  $W_3 + W_4 = W_1 + W_2$ .
- (23) If  $W_3 = \Omega_{W_1}$  and  $W_4 = \Omega_{W_2}$ , then  $W_3 \cap W_4 = W_1 \cap W_2$ .

Now we state the propositions:

- (24) Let us consider a  $\mathbb{Z}$ -module  $V$  and a strict submodule  $W$  of  $V$ . Suppose  $W \neq \mathbf{0}_V$ . Then there exists a vector  $v$  of  $V$  such that
  - (i)  $v \in W$ , and
  - (ii)  $v \neq 0_V$ .

- (25) Let us consider a subset  $A$  of  $V$  and  $z$  linear combinations  $l_1, l_2$  of  $A$ . Suppose  $(\text{the support of } l_1) \cap (\text{the support of } l_2) = \emptyset$ . Then the support of  $l_1 + l_2 = (\text{the support of } l_1) \cup (\text{the support of } l_2)$ . PROOF:  $(\text{The support of } l_1) \cup (\text{the support of } l_2) \subseteq \text{the support of } l_1 + l_2$  by [14, (8)].  $\square$
- (26) Let us consider subsets  $A_1, A_2$  of  $V$  and a  $z$  linear combination  $l$  of  $A_1 \cup A_2$ . Suppose  $A_1 \cap A_2 = \emptyset$ . Then there exists a  $z$  linear combination  $l_1$  of  $A_1$  and there exists a  $z$  linear combination  $l_2$  of  $A_2$  such that  $l = l_1 + l_2$ . PROOF: Define  $\mathcal{P}[\text{element}, \text{element}] \equiv$  if  $\$1$  is a vector of  $V$ , then  $\$1 \in A_1$  and  $\$2 = l(\$1)$  or  $\$1 \notin A_1$  and  $\$2 = 0$ . For every element  $x$  such that  $x \in \text{the carrier of } V$  there exists an element  $y$  such that  $y \in \mathbb{Z}$  and  $\mathcal{P}[x, y]$ . There exists a function  $l_1$  from the carrier of  $V$  into  $\mathbb{Z}$  such that for every element  $x$  such that  $x \in \text{the carrier of } V$  holds  $\mathcal{P}[x, l_1(x)]$  from [8, Sch. 1]. Consider  $l_1$  being a function from the carrier of  $V$  into  $\mathbb{Z}$  such that for every element  $x$  such that  $x \in \text{the carrier of } V$  holds  $\mathcal{P}[x, l_1(x)]$ . For every element  $x$  such that  $x \in \text{the support of } l_1$  holds  $x \in A_1$  by [14, (8)]. Define  $\mathcal{Q}[\text{element}, \text{element}] \equiv$  if  $\$1$  is a vector of  $V$ , then  $\$1 \in A_2$  and  $\$2 = l(\$1)$  or  $\$1 \notin A_2$  and  $\$2 = 0$ . For every element  $x$  such that  $x \in \text{the carrier of } V$  there exists an element  $y$  such that  $y \in \mathbb{Z}$  and  $\mathcal{Q}[x, y]$ . There exists a function  $l_2$  from the carrier of  $V$  into  $\mathbb{Z}$  such that for every element  $x$  such that  $x \in \text{the carrier of } V$  holds  $\mathcal{Q}[x, l_2(x)]$  from [8, Sch. 1]. Consider  $l_2$  being a function from the carrier of  $V$  into  $\mathbb{Z}$  such that for every element  $x$  such that  $x \in \text{the carrier of } V$  holds  $\mathcal{Q}[x, l_2(x)]$ . For every element  $x$  such that  $x \in \text{the support of } l_2$  holds  $x \in A_2$  by [14, (8)]. For every vector  $v$  of  $V$ ,  $l(v) = (l_1 + l_2)(v)$ .  $\square$
- (27) Let us consider a  $\mathbb{Z}$ -module  $V$ , free submodules  $W_1, W_2$  of  $V$ , a basis  $I_1$  of  $W_1$ , and a basis  $I_2$  of  $W_2$ . If  $V$  is the direct sum of  $W_1$  and  $W_2$ , then  $I_1 \cap I_2 = \emptyset$ .

Let us consider a  $\mathbb{Z}$ -module  $V$ , free submodules  $W_1, W_2$  of  $V$ , a basis  $I_1$  of  $W_1$ , a basis  $I_2$  of  $W_2$ , and a subset  $I$  of  $V$ . Now we state the propositions:

- (28) If  $V$  is the direct sum of  $W_1$  and  $W_2$  and  $I = I_1 \cup I_2$ , then  $\text{Lin}(I) =$  the  $\mathbb{Z}$ -module structure of  $V$ .
- (29) If  $V$  is the direct sum of  $W_1$  and  $W_2$  and  $I = I_1 \cup I_2$ , then  $I$  is linearly independent.

Let us consider a  $\mathbb{Z}$ -module  $V$  and free submodules  $W_1, W_2$  of  $V$ . Now we state the propositions:

- (30) If  $V$  is the direct sum of  $W_1$  and  $W_2$ , then  $V$  is free.
- (31) If  $W_1 \cap W_2 = \mathbf{0}_V$ , then  $W_1 + W_2$  is free.

Let us consider a free  $\mathbb{Z}$ -module  $V$ , a basis  $I$  of  $V$ , and a vector  $v$  of  $V$ . Now we state the propositions:

- (32) If  $v \in I$ , then  $\text{Lin}(I \setminus \{v\})$  is free and  $\text{Lin}(\{v\})$  is free.

- (33) If  $v \in I$ , then  $V$  is the direct sum of  $\text{Lin}(I \setminus \{v\})$  and  $\text{Lin}(\{v\})$ .

Let  $V$  be a finite-rank free  $\mathbb{Z}$ -module. One can verify that every submodule of  $V$  is free.

Now we state the propositions:

- (34) Let us consider a  $\mathbb{Z}$ -module  $V$ , a submodule  $W$  of  $V$ , and free submodules  $W_1, W_2$  of  $V$ . Suppose
- (i)  $W_1 \cap W_2 = \mathbf{0}_V$ , and
  - (ii) the  $\mathbb{Z}$ -module structure of  $W = W_1 + W_2$ .

Then  $W$  is free. The theorem is a consequence of (31).

- (35) Let us consider a prime number  $p$  and a free  $\mathbb{Z}$ -module  $V$ .

If  $\text{Z}_M\text{QvectSp}(V, p)$  is finite dimensional, then  $V$  is finite-rank.

- (36) Let us consider a prime number  $p$ , a  $\mathbb{Z}$ -module  $V$ , an element  $s$  of  $V$ , an integer  $a$ , and an element  $b$  of  $\text{GF}(p)$ . Suppose  $b = a \bmod p$ . Then  $b \cdot \text{ZMtoMQV}(V, p, s) = \text{ZMtoMQV}(V, p, a \cdot s)$ .

- (37) Let us consider a prime number  $p$ , a free  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , a subset  $I_6$  of  $\text{Z}_M\text{QvectSp}(V, p)$ , and a  $\mathbb{Z}$ -linear combination  $l$  of  $I$ . Suppose  $I_6 = \{\text{ZMtoMQV}(V, p, u), \text{ where } u \text{ is a vector of } V : u \in I\}$ . Then  $\text{ZMtoMQV}(V, p, \sum l) \in \text{Lin}(I_6)$ .

- (38) Let us consider a prime number  $p$ , a free  $\mathbb{Z}$ -module  $V$ , a subset  $I$  of  $V$ , and a subset  $I_6$  of  $\text{Z}_M\text{QvectSp}(V, p)$ . Suppose

- (i)  $\text{Lin}(I) = \text{the } \mathbb{Z}\text{-module structure of } V$ , and
- (ii)  $I_6 = \{\text{ZMtoMQV}(V, p, u), \text{ where } u \text{ is a vector of } V : u \in I\}$ .

Then  $\text{Lin}(I_6) = \text{the vector space structure of } \text{Z}_M\text{QvectSp}(V, p)$ . The theorem is a consequence of (37). PROOF: For every element  $v_3$  of  $\text{Z}_M\text{QvectSp}(V, p)$ ,  $v_3 \in \text{Lin}(I_6)$  by [15, (22)], [14, (64)].  $\square$

- (39) Let us consider a finitely-generated free  $\mathbb{Z}$ -module  $V$ . Then there exists a finite subset  $A$  of  $V$  such that  $A$  is a basis of  $V$ . The theorem is a consequence of (38). PROOF: Set  $p = \text{the prime number}$ . Consider  $B$  being a finite subset of  $V$  such that  $\text{Lin}(B) = \text{the } \mathbb{Z}\text{-module structure of } V$ . Set  $B_1 = \{\text{ZMtoMQV}(V, p, u), \text{ where } u \text{ is a vector of } V : u \in B\}$ . Define  $\mathcal{F}(\text{element of } V) = \text{ZMtoMQV}(V, p, \$1)$ . Consider  $f$  being a function from the carrier of  $V$  into  $\text{Z}_M\text{QvectSp}(V, p)$  such that for every element  $x$  of  $V$ ,  $f(x) = \mathcal{F}(x)$  from [8, Sch. 4]. For every element  $y$  such that  $y \in B_1$  there exists an element  $x$  such that  $x \in \text{dom}(f|B)$  and  $y = (f|B)(x)$  by [30, (62)], [7, (47)]. Consider  $I_6$  being a basis of  $\text{Z}_M\text{QvectSp}(V, p)$  such that  $I_6 \subseteq B_1$ .  $\square$

One can verify that every finitely-generated free  $\mathbb{Z}$ -module is finite-rank and every finite-rank free  $\mathbb{Z}$ -module is finitely-generated.

Now we state the proposition:

- (40) Let us consider a finite-rank free  $\mathbb{Z}$ -module  $V$  and a subset  $A$  of  $V$ . If  $A$  is linearly independent, then  $A$  is finite. The theorem is a consequence of (19).

Let  $V$  be a  $\mathbb{Z}$ -module and  $W_1, W_2$  be finite-rank free submodules of  $V$ . One can check that  $W_1 \cap W_2$  is free.

Note that  $W_1 \cap W_2$  is finite-rank.

Let  $V$  be a finite-rank free  $\mathbb{Z}$ -module. Note that every submodule of  $V$  is finite-rank.

## REFERENCES

- [1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(2):377–382, 1990.
- [2] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(3):543–547, 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. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(2):357–367, 1990.
- [10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.
- [11] Jing-Chao Chen. The Steinitz theorem and the dimension of a real linear space. *Formalized Mathematics*, 6(3):411–415, 1997.
- [12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(1):165–167, 1990.
- [13] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama.  $\mathbb{Z}$ -modules. *Formalized Mathematics*, 20(1):47–59, 2012. doi:10.2478/v10037-012-0007-z.
- [14] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Quotient module of  $\mathbb{Z}$ -module. *Formalized Mathematics*, 20(3):205–214, 2012. doi:10.2478/v10037-012-0024-y.
- [15] 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.
- [16] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Gaussian integers. *Formalized Mathematics*, 21(2):115–125, 2013. doi:10.2478/forma-2013-0013.
- [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] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(5):829–832, 1990.
- [20] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: a cryptographic perspective. 2002.
- [21] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(3):339–345, 1996.
- [22] Konrad Raczkowski and Paweł Sadowski. Equivalence relations and classes of abstraction. *Formalized Mathematics*, 1(3):441–444, 1990.
- [23] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(1):29–34, 1999.
- [24] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(1):115–122, 1990.
- [25] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.

- [26] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.
- [27] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(5):877–882, 1990.
- [28] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(5):883–885, 1990.
- [29] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.
- [30] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.
- [31] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(1):181–186, 1990.
- [32] Edmund Woronowicz and Anna Zalewska. Properties of binary relations. *Formalized Mathematics*, 1(1):85–89, 1990.
- [33] Mariusz Żynel. The Steinitz theorem and the dimension of a vector space. *Formalized Mathematics*, 5(3):423–428, 1996.

*Received December 31, 2013*

---