

Free \mathbb{Z} -module¹

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 free \mathbb{Z} -module and its rank. We formally prove that for a free finite rank \mathbb{Z} -module V , the number of elements in its basis, that is a rank of the \mathbb{Z} -module, is constant regardless of the selection of its basis. \mathbb{Z} -module is necessary for lattice problems, LLL(Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattice [15]. Some theorems in this article are described by translating theorems in [21] and [8] into theorems of \mathbb{Z} -module.

MML identifier: ZMODUL03, version: 8.0.01 5.3.1162

The papers [17], [1], [3], [9], [4], [5], [23], [20], [14], [18], [16], [19], [2], [6], [12], [27], [28], [25], [26], [13], [24], [22], [7], [10], and [11] provide the terminology and notation for this paper.

1. FREE \mathbb{Z} -MODULE

In this paper V is a \mathbb{Z} -module, v is a vector of V , and W is a submodule of V . Let us note that there exists a \mathbb{Z} -module which is non trivial.

Let V be a \mathbb{Z} -module. One can verify that there exists a finite subset of V which is linearly independent.

Let K be a field, let V be a non empty vector space structure over K , let L be a linear combination of V , and let v be a vector of V . Then $L(v)$ is an element of K .

Next we state two propositions:

- (1) Let u be a vector of V . Then there exists a z linear combination l of V such that $l(u) = 1$ and for every vector v of V such that $v \neq u$ holds $l(v) = 0$.

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

- (2) Let G be a \mathbb{Z} -module, i be an element of \mathbb{Z} , w be an element of \mathbb{Z} , and v be an element of G . Suppose $G = \langle \text{the carrier of } (\mathbb{Z}^{\mathbb{R}}), \text{ the zero of } (\mathbb{Z}^{\mathbb{R}}), \text{ the addition of } (\mathbb{Z}^{\mathbb{R}}), \text{ the left integer multiplication of } (\mathbb{Z}^{\mathbb{R}}) \rangle$ and $v = w$. Then $i \cdot v = i \cdot w$.

Let I_1 be a \mathbb{Z} -module. We say that I_1 is free if and only if:

- (Def. 1) There exists a subset A of I_1 such that A is linearly independent and $\text{Lin}(A) = \text{the } \mathbb{Z}\text{-module structure of } I_1$.

Let us consider V . One can check that $\mathbf{0}_V$ is free.

One can verify that there exists a \mathbb{Z} -module which is strict and free.

Let V be a \mathbb{Z} -module. One can verify that there exists a submodule of V which is strict and free.

Let V be a free \mathbb{Z} -module. A subset of V is called a basis of V if:

- (Def. 2) It is linearly independent and $\text{Lin}(it) = \text{the } \mathbb{Z}\text{-module structure of } V$.

One can verify that every free \mathbb{Z} -module inherits cancelable on multiplication.

Let us observe that there exists a non trivial \mathbb{Z} -module which is free.

In the sequel K_1, K_2 denote z linear combinations of V and X denotes a subset of V .

We now state a number of propositions:

- (3) If X is linearly independent and the support of $K_1 \subseteq X$ and the support of $K_2 \subseteq X$ and $\sum K_1 = \sum K_2$, then $K_1 = K_2$.
- (4) Let V be a free \mathbb{Z} -module and A be a subset of V . Suppose A is linearly independent. Then there exists a subset B of V such that $A \subseteq B$ and B is linearly independent and for every vector v of V there exists an integer a such that $a \cdot v \in \text{Lin}(B)$.
- (5) Let L be a z linear combination of V , F, G be finite sequences of elements of V , and P be a permutation of $\text{dom } F$. If $G = F \cdot P$, then $\sum(L \cdot F) = \sum(L \cdot G)$.
- (6) Let L be a z linear combination of V and F be a finite sequence of elements of V . If the support of L misses $\text{rng } F$, then $\sum(L \cdot F) = \mathbf{0}_V$.
- (7) Let F be a finite sequence of elements of V . Suppose F is one-to-one. Let L be a z linear combination of V . If the support of $L \subseteq \text{rng } F$, then $\sum(L \cdot F) = \sum L$.
- (8) Let L be a z linear combination of V and F be a finite sequence of elements of V . Then there exists a z linear combination K of V such that the support of $K = \text{rng } F \cap (\text{the support of } L)$ and $L \cdot F = K \cdot F$.
- (9) Let L be a z linear combination of V , A be a subset of V , and F be a finite sequence of elements of V . Suppose $\text{rng } F \subseteq \text{the carrier of } \text{Lin}(A)$. Then there exists a z linear combination K of A such that $\sum(L \cdot F) = \sum K$.

- (10) Let L be a \mathbb{Z} linear combination of V and A be a subset of V . Suppose the support of $L \subseteq$ the carrier of $\text{Lin}(A)$. Then there exists a \mathbb{Z} linear combination K of A such that $\sum L = \sum K$.
- (11) Let L be a \mathbb{Z} linear combination of V . Suppose the support of $L \subseteq$ the carrier of W . Let K be a \mathbb{Z} linear combination of W . Suppose $K = L$ on the carrier of W . Then the support of $L =$ the support of K and $\sum L = \sum K$.
- (12) Let K be a \mathbb{Z} linear combination of W . Then there exists a \mathbb{Z} linear combination L of V such that the support of $K =$ the support of L and $\sum K = \sum L$.
- (13) Let L be a \mathbb{Z} linear combination of V . Suppose the support of $L \subseteq$ the carrier of W . Then there exists a \mathbb{Z} linear combination K of W such that the support of $K =$ the support of L and $\sum K = \sum L$.
- (14) For every free \mathbb{Z} -module V and for every basis I of V and for every vector v of V holds $v \in \text{Lin}(I)$.
- (15) For every subset A of W such that A is linearly independent holds A is a linearly independent subset of V .
- (16) Let A be a subset of V . Suppose A is linearly independent and $A \subseteq$ the carrier of W . Then A is a linearly independent subset of W .
- (17) Let V be a \mathbb{Z} -module and A be a subset of V . Suppose A is linearly independent. Let v be a vector of V . If $v \in A$, then for every subset B of V such that $B = A \setminus \{v\}$ holds $v \notin \text{Lin}(B)$.
- (18) Let V be a free \mathbb{Z} -module, I be a basis of V , and A be a non empty subset of V . Suppose A misses I . Let B be a subset of V . If $B = I \cup A$, then B is linearly dependent.
- (19) For every subset A of V such that $A \subseteq$ the carrier of W holds $\text{Lin}(A)$ is a submodule of W .
- (20) For every subset A of V and for every subset B of W such that $A = B$ holds $\text{Lin}(A) = \text{Lin}(B)$.

Let V be a \mathbb{Z} -module and let A be a linearly independent subset of V . One can check that $\text{Lin}(A)$ is free.

Let V be a free \mathbb{Z} -module. Observe that Ω_V is strict and free.

2. FINITE RANK FREE \mathbb{Z} -MODULE

Let I_1 be a free \mathbb{Z} -module. We say that I_1 is finite-rank if and only if:

(Def. 3) There exists a finite subset of I_1 which is a basis of I_1 .

Let us consider V . Note that $\mathbf{0}_V$ is finite-rank.

Let us note that there exists a free \mathbb{Z} -module which is strict and finite-rank.

Let V be a \mathbb{Z} -module. Note that there exists a free submodule of V which is strict and finite-rank.

Let V be a \mathbb{Z} -module and let A be a finite linearly independent subset of V . One can check that $\text{Lin}(A)$ is finite-rank.

Let V be a \mathbb{Z} -module. We say that V is finitely-generated if and only if:

(Def. 4) There exists a finite subset A of V such that $\text{Lin}(A) =$ the \mathbb{Z} -module structure of V .

Let us consider V . One can verify that $\mathbf{0}_V$ is finitely-generated.

Let us mention that there exists a \mathbb{Z} -module which is strict, finitely-generated, and free.

Let V be a finite-rank free \mathbb{Z} -module. Observe that every basis of V is finite.

3. RANK OF A FINITE RANK FREE \mathbb{Z} -MODULE

The following propositions are true:

- (21) Let p be a prime number, V be a free \mathbb{Z} -module, I be a basis of V , and u_1, u_2 be vectors of V . If $u_1 \neq u_2$ and $u_1, u_2 \in I$, then $\text{ZMtoMQV}(V, p, u_1) \neq \text{ZMtoMQV}(V, p, u_2)$.
- (22) Let p be a prime number, V be a \mathbb{Z} -module, Z_1 be a vector space over $\text{GF}(p)$, and v_1 be a vector of Z_1 . If $Z_1 = \text{Z}_M\text{QvectSp}(V, p)$, then there exists a vector v of V such that $v_1 = \text{ZMtoMQV}(V, p, v)$.
- (23) Let p be a prime number, V be a \mathbb{Z} -module, I be a subset of V , and l_1 be a linear combination of $\text{Z}_M\text{QvectSp}(V, p)$. Then there exists a z linear combination l of I such that for every vector v of V if $v \in I$, then there exists a vector w of V such that $w \in I$ and $w \in \text{ZMtoMQV}(V, p, v)$ and $l(w) = l_1(\text{ZMtoMQV}(V, p, v))$.
- (24) Let p be a prime number, V be a free \mathbb{Z} -module, I be a basis of V , and l_1 be a linear combination of $\text{Z}_M\text{QvectSp}(V, p)$. Then there exists a z linear combination l of I such that for every vector v of V if $v \in I$, then $l(v) = l_1(\text{ZMtoMQV}(V, p, v))$.
- (25) Let p be a prime number, V be a free \mathbb{Z} -module, I be a basis of V , and X be a non empty subset of $\text{Z}_M\text{QvectSp}(V, p)$. Suppose $X = \{\text{ZMtoMQV}(V, p, u); u \text{ ranges over vectors of } V: u \in I\}$. Then there exists a function F from X into the carrier of V such that for every vector u of V such that $u \in I$ holds $F(\text{ZMtoMQV}(V, p, u)) = u$ and F is one-to-one and $\text{dom } F = X$ and $\text{rng } F = I$.
- (26) Let p be a prime number, V be a free \mathbb{Z} -module, and I be a basis of V . Then $\overline{\{\text{ZMtoMQV}(V, p, u); u \text{ ranges over vectors of } V: u \in I\}} = \overline{I}$.
- (27) For every prime number p and for every free \mathbb{Z} -module V holds $\text{ZMtoMQV}(V, p, \mathbf{0}_V) = \mathbf{0}_{\text{Z}_M\text{QvectSp}(V, p)}$.
- (28) Let p be a prime number, V be a free \mathbb{Z} -module, and s, t be elements of V . Then $\text{ZMtoMQV}(V, p, s) + \text{ZMtoMQV}(V, p, t) = \text{ZMtoMQV}(V, p, s+t)$.

- (29) Let p be a prime number, V be a free \mathbb{Z} -module, s be a finite sequence of elements of V , and t be a finite sequence of elements of $Z_MQVectSp(V, p)$. Suppose $\text{len } s = \text{len } t$ 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 $t(i) = ZMtoMQV(V, p, s_1)$. Then $\sum t = ZMtoMQV(V, p, \sum s)$.
- (30) Let p be a prime number, V be a free \mathbb{Z} -module, s be an element of V , a be an integer, and b be an element of $GF(p)$. If $a = b$, then $b \cdot ZMtoMQV(V, p, s) = ZMtoMQV(V, p, a \cdot s)$.
- (31) Let p be a prime number, V be a free \mathbb{Z} -module, I be a basis of V , l be a z linear combination of I , I_2 be a subset of $Z_MQVectSp(V, p)$, and l_1 be a linear combination of I_2 . Suppose $I_2 = \{ZMtoMQV(V, p, u); u \text{ ranges over vectors of } V: u \in I\}$ and for every vector v of V such that $v \in I$ holds $l(v) = l_1(ZMtoMQV(V, p, v))$. Then $\sum l_1 = ZMtoMQV(V, p, \sum l)$.
- (32) Let p be a prime number, V be a free \mathbb{Z} -module, I be a basis of V , and I_2 be a subset of $Z_MQVectSp(V, p)$. If $I_2 = \{ZMtoMQV(V, p, u); u \text{ ranges over vectors of } V: u \in I\}$, then I_2 is linearly independent.
- (33) Let p be a prime number, V be a free \mathbb{Z} -module, I be a subset of V , and I_2 be a subset of $Z_MQVectSp(V, p)$. Suppose $I_2 = \{ZMtoMQV(V, p, u); u \text{ ranges over vectors of } V: u \in I\}$. Let s be a finite sequence of elements of V . Suppose that 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 $ZMtoMQV(V, p, s_1) \in \text{Lin}(I_2)$. Then $ZMtoMQV(V, p, \sum s) \in \text{Lin}(I_2)$.
- (34) Let p be a prime number, V be a free \mathbb{Z} -module, I be a basis of V , I_2 be a subset of $Z_MQVectSp(V, p)$, and l be a z linear combination of I . If $I_2 = \{ZMtoMQV(V, p, u); u \text{ ranges over vectors of } V: u \in I\}$, then $ZMtoMQV(V, p, \sum l) \in \text{Lin}(I_2)$.
- (35) Let p be a prime number, V be a free \mathbb{Z} -module, I be a basis of V , and I_2 be a subset of $Z_MQVectSp(V, p)$. If $I_2 = \{ZMtoMQV(V, p, u); u \text{ ranges over vectors of } V: u \in I\}$, then I_2 is a basis of $Z_MQVectSp(V, p)$.

Let p be a prime number and let V be a finite-rank free \mathbb{Z} -module. Observe that $Z_MQVectSp(V, p)$ is finite dimensional.

Next we state the proposition

- (36) For every finite-rank free \mathbb{Z} -module V and for all bases A, B of V holds $\overline{A} = \overline{B}$.

Let V be a finite-rank free \mathbb{Z} -module. The functor $\text{rank } V$ yields a natural number and is defined as follows:

(Def. 5) For every basis I of V holds $\text{rank } V = \overline{I}$.

The following proposition is true

- (37) For every prime number p and for every finite-rank free \mathbb{Z} -module V holds $\text{rank } V = \text{dim}(Z_MQVectSp(V, p))$.

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. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [6] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(2):357–367, 1990.
- [7] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.
- [8] Jing-Chao Chen. The Steinitz theorem and the dimension of a real linear space. *Formalized Mathematics*, 6(3):411–415, 1997.
- [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] 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.
- [12] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(5):841–845, 1990.
- [13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(2):335–342, 1990.
- [14] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(5):829–832, 1990.
- [15] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective (the international series in engineering and computer science). 2002.
- [16] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(3):339–345, 1996.
- [17] Michał Muzalewski and Wojciech Skaba. From loops to abelian multiplicative groups with zero. *Formalized Mathematics*, 1(5):833–840, 1990.
- [18] Christoph Schwarzeweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(1):29–34, 1999.
- [19] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(4):341–347, 2003.
- [20] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [21] Wojciech A. Trybulec. Basis of real linear space. *Formalized Mathematics*, 1(5):847–850, 1990.
- [22] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(5):883–885, 1990.
- [23] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(5):821–827, 1990.
- [24] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1(5):877–882, 1990.
- [25] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.
- [26] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.
- [27] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.
- [28] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(1):181–186, 1990.

Received August 6, 2012
