FORMALIZED MATHEMATICS
Vol. 24, No. 1, Pages 37–47, 2016
DOI: 10.1515/forma-2016-0004

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

Divisible $\mathbb{Z}$-modules

Yuichi Futa
Japan Advanced Institute
of Science and Technology
Ishikawa, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the definition of divisible $\mathbb{Z}$-module and its properties in the Mizar system [3]. We formally prove that any non-trivial divisible $\mathbb{Z}$-modules are not finitely-generated. We introduce a divisible $\mathbb{Z}$-module, equivalent to a vector space of a torsion-free $\mathbb{Z}$-module with a coefficient ring $\mathbb{Q}$. $\mathbb{Z}$-modules are important for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [15], cryptographic systems with lattices [16] and coding theory [8].

MSC: 15A03 16D20 13C13 03B35

Keywords: divisible vector; divisible $\mathbb{Z}$-module

MML identifier: ZMODUL08, version: 8.1.04 5.36.1267

1. Divisible Module

Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x + y$ with $a + b$. We identify $x \cdot y$ with $a \cdot b$. Let V be a $\mathbb{Z}$-module and v be a vector of V. We say that v is divisible if and only if

(Def. 1) for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ there exists a vector u of V such that $a \cdot u = v$.

Let us observe that 0_V is divisible and there exists a vector of V which is divisible.

Now we state the propositions:

(1) Let us consider a $\mathbb{Z}$-module V, and divisible vectors v, u of V. Then $v+u$ is divisible.

(2) Let us consider a $\mathbb{Z}$-module V, and a divisible vector v of V. Then $-v$ is divisible.

PROOF: For every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ there exists a vector w of V such that $-v = a \cdot w$ by [9, (6)]. □

(3) Let us consider a $\mathbb{Z}$-module V, a divisible vector v of V, and an element i of $\mathbb{Z}^{\mathrm{R}}$. Then $i \cdot v$ is divisible.

Let V be a $\mathbb{Z}$-module. We say that V is divisible if and only if

(Def. 2) every vector of V is divisible.

Observe that $\mathbf{0}_V$ is divisible and $\mathbb{Z}$-module$\mathbb{Q}$ is divisible and there exists a $\mathbb{Z}$-module which is divisible.

Let V be a $\mathbb{Z}$-module. Let us note that there exists a submodule of V which is divisible and there exists a divisible $\mathbb{Z}$-module which is non finitely generated.

Now we state the propositions:

(4) (The left integer multiplication of $\mathbb{F}_{\mathbb{Q}}) \restriction (\mathbb{Z} \times \mathbb{Z}) =$ the left integer multiplication of $\mathbb{Z}^{\mathrm{R}}$.

PROOF: Set $a =$ (the left integer multiplication of $\mathbb{F}_{\mathbb{Q}}) \restriction (\mathbb{Z} \times \mathbb{Z})$. For every object z such that $z \in \operatorname{dom} a$ holds $a(z) =$ (the left integer multiplication of $\mathbb{Z}^{\mathrm{R}})(z)$ by [5, (49)], [13, (15)], [12, (14)]. □

(5) $\langle$the carrier of $\mathbb{Z}^{\mathrm{R}}$, the addition of $\mathbb{Z}^{\mathrm{R}}$, the zero of $\mathbb{Z}^{\mathrm{R}}$, the left integer multiplication of $\mathbb{Z}^{\mathrm{R}}\rangle$ is a submodule of $\mathbb{Z}$-module$\mathbb{Q}$. The theorem is a consequence of (4).

(6) Let us consider a divisible $\mathbb{Z}$-module V, and a submodule W of V. Then $\mathbb{Z}$-ModuleQuot(V, W) is divisible.

Let us note that there exists a divisible $\mathbb{Z}$-module which is non trivial.

Now we state the proposition:

(7) Let us consider a $\mathbb{Z}$-module V. Then V is divisible if and only if Ω_V is divisible.

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

(8) If v is not torsion, then $\mathrm{Lin}(\{v\})$ is not divisible.

(9) If v is torsion and $v \neq 0_V$, then $\mathrm{Lin}(\{v\})$ is not divisible.

Let V be a non trivial $\mathbb{Z}$-module and v be a non zero vector of V. Observe that $\mathrm{Lin}(\{v\})$ is non divisible and there exists a submodule of V which is non divisible.

Now we state the propositions:

(10) Every non trivial, finitely generated, torsion-free $\mathbb{Z}$-module is not divisible.

Proof: Consider I being a finite subset of V such that I is a basis of V. Consider v being an object such that $v \in I$. v is not divisible by [9, (92)], [12, (19)], [19, (15)], [9, (9)]. □

(11) Let us consider a non trivial, finitely generated, torsion $\mathbb{Z}$-module V. Then there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $i \neq 0$, and

(ii) for every vector v of V, $i \cdot v = 0_V$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset I of V such that $\overline{\overline{I}} = \$_1$ there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0$ and for every vector v of V such that $v \in \mathrm{Lin}(I)$ holds $i \cdot v = 0_V$. $\mathcal{P}[0]$ by [10, (67)], [9, (1)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [7, (40)], [10, (72)], [1, (44)], [7, (31)]. For every natural number n, $\mathcal{P}[n]$ from [2, Sch. 2]. Consider I being a finite subset of V such that $\mathrm{Lin}(I) =$ the vector space structure of V. Consider i being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0$ and for every vector v of V such that $v \in \mathrm{Lin}(I)$ holds $i \cdot v = 0_V$. For every vector v of V, $i \cdot v = 0_V$. □

(12) Let us consider a non trivial, finitely generated, torsion $\mathbb{Z}$-module V, and an element i of $\mathbb{Z}^{\mathrm{R}}$. Suppose $i \neq 0$ and for every vector v of V, $i \cdot v = 0_V$. Then V is not divisible.

(13) Every non trivial, finitely generated, torsion $\mathbb{Z}$-module is not divisible. The theorem is a consequence of (11) and (12).

One can verify that there exists a non trivial, finitely generated, torsion $\mathbb{Z}$-module which is non divisible.

Now we state the proposition:

(14) Every non trivial, finitely generated $\mathbb{Z}$-module is not divisible. The theorem is a consequence of (13), (6), and (10).

Let us note that every non trivial, divisible $\mathbb{Z}$-module is non finitely generated.

Let V be a non trivial, non divisible $\mathbb{Z}$-module. One can verify that there exists a non zero vector of V which is non divisible.

Let V be a non trivial, finite rank, free $\mathbb{Z}$-module. Observe that $\operatorname{rank} V$ is non zero.

Now we state the propositions:

(15) Let us consider a non trivial, free $\mathbb{Z}$-module V, a non zero vector v of V, and a basis I of V. Then there exists a linear combination L of I and there exists a vector u of V such that $v = \sum L$ and $u \in I$ and $L(u) \neq 0$.

Proof: Consider L being a linear combination of I such that $v = \sum L$. The support of $L \neq \emptyset$ by [10, (23)]. Consider u_1 being an object such that

$u_1 \in$ the support of L. Consider u being a vector of V such that $u = u_1$ and $L(u) \neq 0$. $\square$

(16) Let us consider a non trivial, free $\mathbb{Z}$-module V. Then every non zero vector of V is not divisible. The theorem is a consequence of (15).

Let us observe that every non trivial, free $\mathbb{Z}$-module is non divisible.

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

(17) There exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \in \mathbb{N}$, and

(ii) for every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector u of V such that $b > a$ holds $v \neq b \cdot u$.

PROOF: Set $I =$ the basis of V. Consider L being a linear combination of I, w being a vector of V such that $v = \sum L$ and $w \in I$ and $L(w) \neq 0$. Reconsider $a = |L(w)|$ as an element of $\mathbb{Z}^{\mathrm{R}}$. For every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector u of V such that $b > a$ holds $v \neq b \cdot u$ by [10, (64), (31), (53)], [11, (3)]. $\square$

(18) There exists an element a of $\mathbb{Z}^{\mathrm{R}}$ and there exists a vector u of V such that $a \in \mathbb{N}$ and $a \neq 0$ and $v = a \cdot u$ and for every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector w of V such that $b > a$ holds $v \neq b \cdot w$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ there exists a vector u of V and there exists an element k of $\mathbb{Z}^{\mathrm{R}}$ such that $k = \$_1$ and $v = k \cdot u$. Consider a being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $a \in \mathbb{N}$ and for every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector u of V such that $b > a$ holds $v \neq b \cdot u$. There exists a natural number k such that $\mathcal{P}[k]$. Consider a_0 being a natural number such that $\mathcal{P}[a_0]$ and for every natural number n such that $\mathcal{P}[n]$ holds $n \leqslant a_0$ from [2, Sch. 6]. Reconsider $a = a_0$ as an element of $\mathbb{Z}^{\mathrm{R}}$. Consider u being a vector of V such that $v = a \cdot u$. $a \neq 0$ by [9, (1)]. For every element b of $\mathbb{Z}^{\mathrm{R}}$ and for every vector w of V such that $b > a$ holds $v \neq b \cdot w$ by [18, (3)]. $\square$

2. Divisible Module for Torsion-free $\mathbb{Z}$-module

Let V be a torsion-free $\mathbb{Z}$-module. The functor Embedding(V) yielding a strict $\mathbb{Z}$-module is defined by

(Def. 3) the carrier of *it* $=$ rng MorphsZQ(V) and the zero of *it* $=$ zeroCoset(V) and the addition of *it* $=$ addCoset$(V) \restriction$ rng MorphsZQ(V) and the left multiplication of *it* $=$ lmultCoset$(V) \restriction (\mathbb{Z} \times$ rng MorphsZQ$(V))$.

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

(19) (i) every vector of Embedding(V) is a vector of $\mathbb{Z}$-MQVectSp(V), and

(ii) $0_{\mathrm{Embedding}(V)} = 0_{\mathbb{Z}\text{-}\mathrm{MQVectSp}(V)}$, and

(iii) for every vectors x, y of Embedding(V) and for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that $x = v$ and $y = w$ holds $x + y = v + w$, and

(iv) for every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of Embedding(V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$.

Proof: Set $Z = \mathbb{Z}$-MQVectSp(V). Set E = Embedding(V). For every vectors x, y of E and for every vectors v, w of Z such that $x = v$ and $y = w$ holds $x + y = v + w$ by [5, (49)]. For every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of E and for every vector v of Z such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$ by [5, (49)]. □

(20) (i) for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that $v, w \in$ Embedding(V) holds $v + w \in$ Embedding(V), and

(ii) for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $j \in \mathbb{Z}$ and $v \in$ Embedding(V) holds $j \cdot v \in$ Embedding(V).

The theorem is a consequence of (19).

(21) There exists a linear transformation T from V to Embedding(V) such that

(i) T is bijective, and

(ii) T = MorphsZQ(V), and

(iii) for every vector v of V, $T(v) = [\langle v, 1\rangle]_{\mathrm{EQRZM}(V)}$.

The theorem is a consequence of (19).

Now we state the proposition:

(22) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v_1 of Embedding(V). Then there exists a vector v of V such that $(\mathrm{MorphsZQ}(V))(v) = v_1$. The theorem is a consequence of (21).

Let V be a torsion-free $\mathbb{Z}$-module. The functor DivisibleMod(V) yielding a strict $\mathbb{Z}$-module is defined by

(Def. 4) the carrier of *it* = Classes EQRZM(V) and the zero of *it* = zeroCoset(V) and the addition of *it* = addCoset(V) and the left multiplication of *it* = lmultCoset$(V) \restriction (\mathbb{Z} \times \mathrm{Classes\,EQRZM}(V))$.

Now we state the proposition:

(23) Let us consider a torsion-free $\mathbb{Z}$-module V, a vector v of DivisibleMod(V), and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \neq 0$. Then there exists a vector u of DivisibleMod(V) such that $a \cdot u = v$.

Proof: For every vector v of DivisibleMod(V) and for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ there exists a vector u of DivisibleMod(V) such that $a \cdot u = v$ by [5, (49)], [7, (87)]. □

Let V be a torsion-free $\mathbb{Z}$-module. Let us observe that DivisibleMod(V) is divisible.

Now we state the proposition:

(24) Let us consider a torsion-free $\mathbb{Z}$-module V. Then Embedding(V) is a submodule of DivisibleMod(V).

Proof: Set E = Embedding(V). Set D = DivisibleMod(V). For every object x such that $x \in$ the carrier of E holds $x \in$ the carrier of D by [6, (11), (5)]. The left multiplication of E = (the left multiplication of D)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ rng MorphsZQ(V)) by [20, (74)], [7, (96)]. □

Let V be a finitely generated, torsion-free $\mathbb{Z}$-module. One can check that Embedding(V) is finitely generated.

Let V be a non trivial, torsion-free $\mathbb{Z}$-module. Observe that Embedding(V) is non trivial.

Let G be a field, V be a vector space over G, W be a subset of V, and a be an element of G. The functor $a \cdot W$ yielding a subset of V is defined by the term

(Def. 5) $\{a \cdot u$, where u is a vector of $V : u \in W\}$.

Let V be a torsion-free $\mathbb{Z}$-module and r be an element of $\mathbb{F}_{\mathbb{Q}}$. The functor Embedding(r, V) yielding a strict $\mathbb{Z}$-module is defined by

(Def. 6) the carrier of *it* = $r \cdot$rng MorphsZQ(V) and the zero of *it* = zeroCoset(V) and the addition of *it* = addCoset(V) $\restriction$ ($r \cdot$rng MorphsZQ(V)) and the left multiplication of *it* = lmultCoset(V)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ ($r \cdot$ rng MorphsZQ(V))).

Let us consider a torsion-free $\mathbb{Z}$-module V and an element r of $\mathbb{F}_{\mathbb{Q}}$. Now we state the propositions:

(25) (i) every vector of Embedding(r, V) is a vector of $\mathbb{Z}$-MQVectSp(V), and

(ii) $0_{\mathrm{Embedding}(r,V)} = 0_{\mathbb{Z}\text{-MQVectSp}(V)}$, and

(iii) for every vectors x, y of Embedding(r, V) and for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that $x = v$ and $y = w$ holds $x + y = v + w$, and

(iv) for every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of Embedding(r, V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$.

Proof: Set Z = $\mathbb{Z}$-MQVectSp(V). Set E = Embedding(r, V). For every vectors x, y of E and for every vectors v, w of Z such that $x = v$ and

$y = w$ holds $x + y = v + w$ by [5, (49)]. For every element i of $\mathbb{Z}^{\mathrm{R}}$ and for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector x of E and for every vector v of Z such that $i = j$ and $x = v$ holds $i \cdot x = j \cdot v$ by [5, (49)]. □

(26) (i) for every vectors v, w of $\mathbb{Z}$-MQVectSp(V) such that v, $w \in$ Embedding(r, V) holds $v + w \in$ Embedding(r, V), and

(ii) for every element j of $\mathbb{F}_{\mathbb{Q}}$ and for every vector v of $\mathbb{Z}$-MQVectSp(V) such that $j \in \mathbb{Z}$ and $v \in$ Embedding(r, V) holds $j \cdot v \in$ Embedding(r, V).

The theorem is a consequence of (25).

(27) Suppose $r \neq 0_{\mathbb{F}_{\mathbb{Q}}}$. Then there exists a linear transformation T from Embedding(V) to Embedding(r, V) such that

(i) for every element v of $\mathbb{Z}$-MQVectSp(V) such that $v \in$ Embedding(V) holds $T(v) = r \cdot v$, and

(ii) T is bijective.

PROOF: Set $Z = \mathbb{Z}$-MQVectSp(V). Define $\mathcal{F}$(vector of Z) $= r \cdot \$_1$. Consider T being a function from the carrier of Z into the carrier of Z such that for every element x of the carrier of Z, $T(x) = \mathcal{F}(x)$ from [6, Sch. 4]. Set $T_0 = T \restriction$(the carrier of Embedding(V)). For every object y, $y \in \operatorname{rng} T_0$ iff $y \in$ the carrier of Embedding(r, V) by [5, (49)]. T_0 is additive by (19), (20), [5, (49)], (25). For every element x of Embedding(V) and for every element i of $\mathbb{Z}^{\mathrm{R}}$, $T_0(i \cdot x) = i \cdot T_0(x)$ by (19), (20), [5, (49)], (25). For every element v of $\mathbb{Z}$-MQVectSp(V) such that $v \in$ Embedding(V) holds $T_0(v) = r \cdot v$ by [5, (49)]. For every objects x_1, x_2 such that x_1, $x_2 \in$ the carrier of Embedding(V) and $T_0(x_1) = T_0(x_2)$ holds $x_1 = x_2$ by [14, (20)]. □

Now we state the propositions:

(28) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of V. Then $[\langle v, 1 \rangle]_{\mathrm{EQRZM}(V)} \in$ Embedding(V).

(29) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of DivisibleMod (V). Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \neq 0$, and

(ii) $a \cdot v \in$ Embedding(V).

The theorem is a consequence of (28).

Let V be a torsion-free $\mathbb{Z}$-module. One can check that DivisibleMod(V) is torsion-free and Embedding(V) is torsion-free.

Let V be a free $\mathbb{Z}$-module. Let us note that Embedding(V) is free.

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

(30) (i) every vector of $\mathbb{Z}$-MQVectSp(V) is a vector of DivisibleMod(V), and

(ii) every vector of DivisibleMod(V) is a vector of $\mathbb{Z}$-MQVectSp(V), and

(iii) $0_{\mathrm{DivisibleMod}(V)} = 0_{\mathbb{Z}\text{-MQVectSp}(V)}$.

(31) (i) for every vectors x, y of DivisibleMod(V) and for every vectors v, u of $\mathbb{Z}$-MQVectSp(V) such that $x = v$ and $y = u$ holds $x+y = v+u$, and

(ii) for every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a of $\mathbb{Z}^{\mathrm{R}}$ and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ such that $z = w$ and $a = a_1$ holds $a \cdot z = a_1 \cdot w$, and

(iii) for every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ and for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ and $a_1 = a$ and $a \cdot z = a_1 \cdot w$ holds $z = w$, and

(iv) for every vector x of DivisibleMod(V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) and for every element r of $\mathbb{F}_{\mathbb{Q}}$ and for every elements m, n of $\mathbb{Z}^{\mathrm{R}}$ and for every integers m_1, n_1 such that $m = m_1$ and $n = n_1$ and $x = v$ and $r \neq 0_{\mathbb{F}_{\mathbb{Q}}}$ and $n \neq 0$ and $r = \frac{m_1}{n_1}$ there exists a vector y of DivisibleMod(V) such that $x = n \cdot y$ and $r \cdot v = m \cdot y$.

Proof: For every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a of $\mathbb{Z}^{\mathrm{R}}$ and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ such that $z = w$ and $a = a_1$ holds $a \cdot z = a_1 \cdot w$ by [5, (49)], [7, (87)]. For every vector z of DivisibleMod(V) and for every vector w of $\mathbb{Z}$-MQVectSp(V) and for every element a_1 of $\mathbb{F}_{\mathbb{Q}}$ and for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ and $a_1 = a$ and $a \cdot z = a_1 \cdot w$ holds $z = w$ by (30), [9, (8)], [19, (15), (21)]. For every vector x of DivisibleMod(V) and for every vector v of $\mathbb{Z}$-MQVectSp(V) and for every element r of $\mathbb{F}_{\mathbb{Q}}$ and for every elements m, n of $\mathbb{Z}^{\mathrm{R}}$ and for every integers m_1, n_1 such that $m = m_1$ and $n = n_1$ and $x = v$ and $r \neq 0_{\mathbb{F}_{\mathbb{Q}}}$ and $n \neq 0$ and $r = \frac{m_1}{n_1}$ there exists a vector y of DivisibleMod(V) such that $x = n \cdot y$ and $r \cdot v = m \cdot y$. □

Now we state the proposition:

(32) Let us consider a torsion-free $\mathbb{Z}$-module V, and an element r of $\mathbb{F}_{\mathbb{Q}}$. Then Embedding(r, V) is a submodule of DivisibleMod(V). The theorem is a consequence of (25) and (30).

Let V be a finitely generated, torsion-free $\mathbb{Z}$-module and r be an element of $\mathbb{F}_{\mathbb{Q}}$. Observe that Embedding(r, V) is finitely generated.

Let V be a non trivial, torsion-free $\mathbb{Z}$-module and r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. One can verify that Embedding(r, V) is non trivial.

Let V be a torsion-free $\mathbb{Z}$-module and r be an element of $\mathbb{F}_{\mathbb{Q}}$. Observe that Embedding(r, V) is torsion-free.

Let V be a free $\mathbb{Z}$-module and r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. One can check that Embedding(r, V) is free.

Now we state the propositions:

(33) Let us consider a non trivial, free $\mathbb{Z}$-module V, and a vector v of DivisibleMod(V). Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \in \mathbb{N}$, and

(ii) $a \neq 0$, and

(iii) $a \cdot v \in$ Embedding(V), and

(iv) for every element b of $\mathbb{Z}^{\mathrm{R}}$ such that $b \in \mathbb{N}$ and $b < a$ and $b \neq 0$ holds $b \cdot v \notin$ Embedding(V).

Proof: Consider a_1 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $a_1 \neq 0$ and $a_1 \cdot v \in$ Embedding(V). $|a_1| \cdot v \in$ Embedding(V) by (24), [9, (16), (30)]. Define $\mathcal{P}[\text{natural number}] \equiv$ there exists an element n of $\mathbb{Z}^{\mathrm{R}}$ such that $n = \$_1$ and $n \in \mathbb{N}$ and $n \neq 0$ and $n \cdot v \in$ Embedding(V). There exists a natural number k such that $\mathcal{P}[k]$ and for every natural number n such that $\mathcal{P}[n]$ holds $k \leqslant n$ from [2, Sch. 5]. Consider a_0 being a natural number such that $\mathcal{P}[a_0]$ and for every natural number b_0 such that $\mathcal{P}[b_0]$ holds $a_0 \leqslant b_0$. $\square$

(34) Let us consider a finite rank, free $\mathbb{Z}$-module V. Then rank Embedding$(V) =$ rank V. The theorem is a consequence of (21).

Let us consider a finite rank, free $\mathbb{Z}$-module V and a non zero element r of $\mathbb{F}_{\mathbb{Q}}$. Now we state the propositions:

(35) rank Embedding$(r, V) =$ rank Embedding(V). The theorem is a consequence of (27).

(36) rank Embedding$(r, V) =$ rank V. The theorem is a consequence of (35) and (34).

Observe that every non trivial, torsion-free $\mathbb{Z}$-module is infinite.

Now we state the propositions:

(37) Let us consider a $\mathbb{Z}$-module V. Then there exists a subset A of V such that

(i) A is linearly independent, and

(ii) for every vector v of V, there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \in \mathbb{N}$ and $a > 0$ and $a \cdot v \in$ Lin(A).

Proof: Consider A being a subset of V such that $\emptyset \subseteq A$ and A is linearly independent and for every vector v of V, there exists an element a_1 of $\mathbb{Z}^{\mathrm{R}}$ such that $a_1 \neq 0$ and $a_1 \cdot v \in$ Lin(A). For every vector v of V, there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \in \mathbb{N}$ and $a > 0$ and $a \cdot v \in \mathrm{Lin}(A)$ by [17, (2)], [4, (46)], [18, (3)], [9, (16), (38)]. $\square$

(38) Let us consider a non trivial, torsion-free $\mathbb{Z}$-module V, a non zero vector v of V, a subset A of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \in \mathbb{N}$ and A is linearly independent and $a > 0$ and $a \cdot v \in \mathrm{Lin}(A)$. Then there exists a linear combination L of A and there exists a vector u of V such that $a \cdot v = \sum L$ and $u \in A$ and $L(u) \neq 0$.

Proof: Consider L being a linear combination of A such that $a \cdot v = \sum L$. The support of $L \neq \emptyset$ by [10, (23)]. Consider u_1 being an object such that $u_1 \in$ the support of L. Consider u being a vector of V such that $u = u_1$ and $L(u) \neq 0$. $\square$

(39) Let us consider a torsion-free $\mathbb{Z}$-module V, a non zero integer i, and non zero elements r_1, r_2 of $\mathbb{F}_{\mathbb{Q}}$. Suppose $r_2 = \frac{r_1}{i}$. Then $\mathrm{Embedding}(r_1, V)$ is a submodule of $\mathrm{Embedding}(r_2, V)$.

Proof: For every vector x of DivisibleMod(V) such that $x \in \mathrm{Embedding}(r_1, V)$ holds $x \in \mathrm{Embedding}(r_2, V)$ by (27), [6, (11)], (19), [6, (5)]. Embedding (r_1, V) is a submodule of DivisibleMod(V) and $\mathrm{Embedding}(r_2, V)$ is a submodule of DivisibleMod(V). $\square$

(40) Let us consider a finite rank, free $\mathbb{Z}$-module V, and a submodule Z of DivisibleMod(V). Then Z is finitely generated if and only if there exists a non zero element r of $\mathbb{F}_{\mathbb{Q}}$ such that Z is a submodule of $\mathrm{Embedding}(r, V)$. The theorem is a consequence of (32), (29), (19), (27), (31), and (39).

References

[1] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(**3**):543–547, 1990.

[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[3] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[4] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 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. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[8] Wolfgang Ebeling. *Lattices and Codes.* Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.

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

[10] 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.

[11] 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.

[12] Yuichi Futa, Hiroyuki Okazaki, Kazuhisa Nakasho, and Yasunari Shidama. Torsion $\mathbb{Z}$-module and torsion-free $\mathbb{Z}$-module. *Formalized Mathematics*, 22(**4**):277–289, 2014. doi:10.2478/forma-2014-0028.

[13] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Torsion part of $\mathbb{Z}$-module. *Formalized Mathematics*, 23(**4**):297–307, 2015. doi:10.1515/forma-2015-0024.

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

[15] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4), 1982.

[16] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.

[17] Jan Popiołek. Some properties of functions modul and signum. *Formalized Mathematics*, 1(**2**):263–264, 1990.

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

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

[20] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received December 30, 2015