FORMALIZED MATHEMATICS
Vol. 23, No. 4, Pages 297–307, 2015
DOI: 10.1515/forma-2015-0024

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

Torsion Part of $\mathbb{Z}$-module

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 in Mizar [7] the definition of "torsion part" of $\mathbb{Z}$-module and its properties. We show $\mathbb{Z}$-module generated by the field of rational numbers as an example of torsion-free non free $\mathbb{Z}$-modules. We also formalize the rank-nullity theorem over finite-rank free $\mathbb{Z}$-modules (previously formalized in [1]). $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [23] and cryptographic systems with lattices [24].

MSC: 15A03 13C12 03B35

Keywords: torsion part of $\mathbb{Z}$-module; torsion-free non free $\mathbb{Z}$-module

MML identifier: ZMODUL07, version: 8.1.04 5.33.1254

The notation and terminology used in this paper have been introduced in the following articles: [27], [8], [2], [29], [6], [13], [9], [10], [17], [30], [22], [28], [25], [4], [5], [11], [20], [38], [39], [32], [37], [21], [33], [34], [35], [36], [12], [14], [15], [16], [26], and [19].

1. Torsion Part of $\mathbb{Z}$-module

From now on x, y, y_1, y_2 denote objects, V denotes a $\mathbb{Z}$-module, W, W_1, W_2 denote submodules of V, u, v denote vectors of V, and i, j, k, n denote elements of $\mathbb{N}$.

Now we state the proposition:

ISSN 1426–2630(Print), 1898-9934(Online)

(1) Let us consider an integer n. Suppose $n \neq 0$ and $n \neq -1$ and $n \neq -2$. Then $\frac{n}{n+1} \notin \mathbb{Z}$.

One can check that there exists an element of $\mathbb{Z}^{\mathrm{R}}$ which is prime and non zero and every element of $\mathbb{Z}^{\mathrm{R}}$ which is prime is also non zero.

Now we state the propositions:

(2) Let us consider a $\mathbb{Z}$-module V, and a subset A of V. Suppose A is linearly independent. Then there exists a subset B of V such that

(i) $A \subseteq B$, and

(ii) B is linearly independent, and

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

PROOF: Define $\mathcal{P}[\text{set}] \equiv$ there exists a subset B of V such that $B = \$_1$ and $A \subseteq B$ and B is linearly independent. Consider Q being a set such that For every set Z, $Z \in Q$ iff $Z \in 2^{\alpha}$ and $\mathcal{P}[Z]$, where α is the carrier of V. Consider X being a set such that $X \in Q$ and for every set Z such that $Z \in Q$ and $Z \neq X$ holds $X \nsubseteq Z$. Consider B being a subset of V such that $B = X$ and $A \subseteq B$ and B is linearly independent. Consider v being a vector of V such that for every element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0$ holds $a \cdot v \notin \mathrm{Lin}(B)$. $B \cup \{v\}$ is linearly independent by [10, (8)], [15, (39), (55)], [31, (61)]. $\square$

(3) Let us consider a $\mathbb{Z}$-module V, a finite subset I of V, and a submodule W of V. Suppose for every vector v of V such that $v \in I$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $a \cdot v \in W$. Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that

(i) $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$, and

(ii) for every vector v of V such that $v \in I$ holds $a \cdot v \in W$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset I of V such that $\overline{\overline{I}} = \$_1$ and for every vector v of V such that $v \in I$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $a \cdot v \in W$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and for every vector v of V such that $v \in I$ holds $a \cdot v \in W$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [37, (41)], [3, (44)], [2, (30)], [14, (37)]. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. $\square$

(4) Let us consider a finite rank, free $\mathbb{Z}$-module V. Then every linearly independent subset of V is finite.

Let V be a finite rank, free $\mathbb{Z}$-module. Let us observe that every subset of V which is linearly independent is also finite.

Let us consider a finite rank, free $\mathbb{Z}$-module V and a linearly independent subset A of V. Now we state the propositions:

(5) There exists a finite, linearly independent subset I of V and there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $A \subseteq I$ and $a \circ V$ is a submodule of $\mathrm{Lin}(I)$.

(6) There exists a finite, linearly independent subset I of V such that

(i) $A \subseteq I$, and

(ii) $\mathrm{rank}\, V = \overline{\overline{I}}$.

The theorem is a consequence of (5).

Now we state the proposition:

(7) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I_1 of W_1. Then there exists a finite, linearly independent subset I of V such that

(i) I is a subset of $W_1 + W_2$, and

(ii) $I_1 \subseteq I$, and

(iii) $\mathrm{rank}(W_1 + W_2) = \mathrm{rank}\,\mathrm{Lin}(I)$.

The theorem is a consequence of (6).

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

(8) Suppose W_2 is a submodule of W_1. Then there exists a finite rank, free submodule W_3 of V such that

(i) $\mathrm{rank}\, W_1 = \mathrm{rank}\, W_2 + \mathrm{rank}\, W_3$, and

(ii) $W_2 \cap W_3 = \mathbf{0}_V$, and

(iii) W_3 is a submodule of W_1.

Proof: Set $I_2 =$ the basis of W_2. Reconsider $J_2 = I_2$ as a subset of W_1. Consider J_1 being a finite, linearly independent subset of W_1 such that $J_2 \subseteq J_1$ and $\mathrm{rank}\, W_1 = \overline{\overline{J_1}}$. Set $J_3 = J_1 \setminus J_2$. Reconsider $I_3 = J_3$ as a subset of V. $W_2 \cap \mathrm{Lin}(I_3) = \mathbf{0}_V$ by [16, (20)], [14, (42)], [18, (23)], [19, (4)]. □

(9) There exists a finite rank, free submodule W_3 of V such that

(i) $\mathrm{rank}(W_1 + W_2) = \mathrm{rank}\, W_1 + \mathrm{rank}\, W_3$, and

(ii) $W_1 \cap W_3 = \mathbf{0}_V$, and

(iii) W_3 is a submodule of $W_1 + W_2$.

PROOF: Set $I_1 =$ the basis of W_1. Consider I being a finite, linearly independent subset of V such that I is a subset of $W_1 + W_2$ and $I_1 \subseteq I$ and $\mathrm{rank}(W_1 + W_2) = \mathrm{rank}\,\mathrm{Lin}(I)$. Set $I_2 = I \setminus I_1$. Reconsider $J_2 = I_2$ as a finite, linearly independent subset of V. $W_1 \cap \mathrm{Lin}(J_2) = \mathbf{0}_V$ by [16, (20)], [14, (42)], [18, (23)], [19, (4)]. □

Now we state the proposition:

(10) Let us consider a finite rank, free $\mathbb{Z}$-module V, and submodules W_1, W_2 of V. Then $\mathrm{rank}(W_1 \cap W_2) \geqslant \mathrm{rank}\,W_1 + \mathrm{rank}\,W_2 - \mathrm{rank}\,V$.

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

(Def. 1) the carrier of $it = \{v$, where v is a vector of $V : v$ is torsion$\}$.

Now we state the propositions:

(11) Let us consider a $\mathbb{Z}$-module V, and a vector v of V. Then v is torsion if and only if $v \in$ torsion-part(V).

(12) Let us consider a $\mathbb{Z}$-module V. Then V is torsion-free if and only if torsion-part$(V) = \mathbf{0}_V$. The theorem is a consequence of (11).

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

Let W be a submodule of V. The functor $\mathbb{Z}$-QMorph(V, W) yielding a linear transformation from V to $\mathbb{Z}$-ModuleQuot(V, W) is defined by

(Def. 2) for every element v of V, $it(v) = v + W$.

One can check that $\mathbb{Z}$-QMorph(V, W) is onto.

Now we state the proposition:

(13) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, a finite sequence s of elements of V, and a finite sequence t of elements of W. Suppose $\mathrm{len}\,s = \mathrm{len}\,t$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\,s$ there exists a vector s_1 of V such that $s_1 = s(i)$ and $t(i) = T(s_1)$. Then $\sum t = T(\sum s)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence s of elements of V for every finite sequence t of elements of W such that $\mathrm{len}\,s = \$_1$ and $\mathrm{len}\,s = \mathrm{len}\,t$ and for every element i of $\mathbb{N}$ such that $i \in \mathrm{dom}\,s$ there exists a vector s_1 of V such that $s_1 = s(i)$ and $t(i) = T(s_1)$ holds $\sum t = T(\sum s)$. $\mathcal{P}[0]$ by [32, (43)], [26, (19)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [6, (59)], [4, (11)], [6, (4)], [9, (3)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

Let V be a finitely generated $\mathbb{Z}$-module and W be a submodule of V. Observe that $\mathbb{Z}$-ModuleQuot(V, W) is finitely generated and

$\mathbb{Z}$-ModuleQuot$(V,$ torsion-part$(V))$ is free.

2. $\mathbb{Z}$-module Generated by the Field of Rational Numbers

The functor $\mathbb{Z}$-module$\mathbb{Q}$ yielding a vector space structure over $\mathbb{Z}^{\mathrm{R}}$ is defined by the term

(Def. 3) $\langle$the carrier of $\mathbb{F}_{\mathbb{Q}}$, the addition of $\mathbb{F}_{\mathbb{Q}}$, the zero of $\mathbb{F}_{\mathbb{Q}}$, the left integer multiplication of $\mathbb{F}_{\mathbb{Q}}\rangle$.

One can verify that $\mathbb{Z}$-module$\mathbb{Q}$ is non empty and $\mathbb{Z}$-module$\mathbb{Q}$ is Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

Now we state the propositions:

(14) Let us consider an element v of $\mathbb{F}_{\mathbb{Q}}$, and a rational number v_1. Suppose $v = v_1$. Let us consider a natural number n. Then $(\text{Nat-mult-left}\,\mathbb{F}_{\mathbb{Q}})(n, v) = n \cdot v_1$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv (\text{Nat-mult-left}\,\mathbb{F}_{\mathbb{Q}})(\$_1, v) = \$_1 \cdot v_1$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. □

(15) Let us consider an integer x, an element v of $\mathbb{F}_{\mathbb{Q}}$, and a rational number v_1. Suppose $v = v_1$. Then (the left integer multiplication of $\mathbb{F}_{\mathbb{Q}})(x, v) = x \cdot v_1$. The theorem is a consequence of (14).

Let us observe that $\mathbb{Z}$-module$\mathbb{Q}$ is torsion-free and $\mathbb{Z}$-module$\mathbb{Q}$ is non trivial.

Now we state the propositions:

(16) Let us consider an element s of $\mathbb{Z}$-module$\mathbb{Q}$. Then $\text{Lin}(\{s\}) \neq \mathbb{Z}$-module$\mathbb{Q}$. The theorem is a consequence of (15) and (1).

(17) Let us consider elements s, t of $\mathbb{Z}$-module$\mathbb{Q}$. If $s \neq t$, then $\{s, t\}$ is not linearly independent. The theorem is a consequence of (15).

Let us observe that $\mathbb{Z}$-module$\mathbb{Q}$ is non free.

Now we state the proposition:

(18) Let us consider a finite subset A of $\mathbb{Z}$-module$\mathbb{Q}$. Then there exists an integer n such that

(i) $n \neq 0$, and

(ii) for every element s of $\mathbb{Z}$-module$\mathbb{Q}$ such that $s \in \text{Lin}(A)$ there exists an integer m such that $s = \frac{m}{n}$.

Proof: Set $S = \mathbb{Z}$-module$\mathbb{Q}$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset A of S such that $\overline{\overline{A}} = \$_1$ there exists an integer n such that $n \neq 0$ and for every element s of S such that $s \in \text{Lin}(A)$ there exists an integer m such that $s = \frac{m}{n}$. $\mathcal{P}[0]$ by [15, (67)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [37, (41)], [3, (44)], [2, (30)], [20, (1)]. For every natural number k, $\mathcal{P}[k]$ from [4, Sch. 2]. □

One can verify that $\mathbb{Z}$-module$\mathbb{Q}$ is non finitely generated.

Now we state the proposition:

(19) Let us consider a finite subset A of $\mathbb{Z}$-module$\mathbb{Q}$. Then $\operatorname{rank}\operatorname{Lin}(A) \leqslant 1$.
PROOF: Set $S = \mathbb{Z}$-module$\mathbb{Q}$. Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset A of S such that $\overline{\overline{A}} = \$_1$ holds $\operatorname{rank}\operatorname{Lin}(A) \leqslant 1$. $\mathcal{P}[0]$ by [15, (67)], [14, (51)], [26, (1)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (31)], [3, (44)], [2, (30)], [15, (72)]. For every natural number n, $\mathcal{P}[n]$ from [4, Sch. 2]. □

3. The Rank-Nullity Theorem

In the sequel V, W denote finite rank, free $\mathbb{Z}$-modules and T denotes a linear transformation from V to W.

Let W be a finite rank, free $\mathbb{Z}$-module, V be a $\mathbb{Z}$-module, and T be a linear transformation from V to W. Observe that $\operatorname{im} T$ is finite rank and free.

The functor $\operatorname{rank} T$ yielding a natural number is defined by the term

(Def. 4) $\operatorname{rank}\operatorname{im} T$.

Let V be a finite rank, free $\mathbb{Z}$-module and W be a $\mathbb{Z}$-module. The functor $\operatorname{nullity} T$ yielding a natural number is defined by the term

(Def. 5) $\operatorname{rank}\ker T$.

Now we state the propositions:

(20) Let us consider a finite rank, free $\mathbb{Z}$-module V, a subset A of V, a linearly independent subset B of V, and a linear transformation T from V to W. Suppose $\operatorname{rank} V = \overline{\overline{B}}$ and A is a basis of $\ker T$ and $A \subseteq B$. Then $T \restriction (B \setminus A)$ is one-to-one.

(21) Let us consider a finite rank, free $\mathbb{Z}$-module V, a subset A of V, a linearly independent subset B of V, a linear transformation T from V to W, and a linear combination l of $B \setminus A$. Suppose $\operatorname{rank} V = \overline{\overline{B}}$ and A is a basis of $\ker T$ and $A \subseteq B$. Then $T(\sum l) = \sum(T \mathbin{@*} l)$. The theorem is a consequence of (20).

(22) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, and a subset A of V. Suppose $A \subseteq$ the carrier of $\ker T$. Then $\operatorname{Lin}(T^\circ A) = \mathbf{0}_W$.

(23) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, and subsets A, B, X of V. Suppose $A \subseteq$ the carrier of $\ker T$ and $X = B \cup A$. Then $\operatorname{Lin}(T^\circ X) = \operatorname{Lin}(T^\circ B)$. The theorem is a consequence of (22).

Let us consider finite rank, free $\mathbb{Z}$-modules V, W and a linear transformation T from V to W. Now we state the propositions:

(24) $\operatorname{rank} V = \operatorname{rank} T + \operatorname{nullity} T$.

PROOF: Set $A =$ the finite basis of $\ker T$. Reconsider $A' = A$ as a subset of V. Consider B' being a finite, linearly independent subset of V, a being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $A' \subseteq B'$ and $a \circ V$ is a submodule of $\operatorname{Lin}(B')$. Reconsider $X = B' \setminus A'$ as a finite subset of B'. Reconsider $C = T^{\circ}X$ as a finite subset of W. $T{\restriction}X$ is one-to-one. C is linearly independent by [26, (60)], (21), [26, (20)], [16, (20)]. Reconsider $a_1 = a \circ \operatorname{im} T$ as a submodule of W. $\operatorname{Lin}(T^{\circ}B') = \operatorname{Lin}(T^{\circ}X)$. For every vector v of W such that $v \in a_1$ holds $v \in \operatorname{Lin}(C)$ by [14, (25)], [26, (23)], [14, (29), (24)]. □

(25) If T is one-to-one, then $\operatorname{rank} V = \operatorname{rank} T$. The theorem is a consequence of (24).

Let V, W be $\mathbb{Z}$-modules and T be a linear transformation from V to W. The functor $\mathbb{Z}$-decom(T) yielding a linear transformation from $\mathbb{Z}$-ModuleQuot$(V, \ker T)$ to $\operatorname{im} T$ is defined by

(Def. 6) *it* is bijective and for every element v of V, *it*$((\mathbb{Z}\text{-QMorph}(V, \ker T))(v)) = T(v)$.

Now we state the propositions:

(26) Let us consider $\mathbb{Z}$-modules V, W, and a linear transformation T from V to W. Then $T = \mathbb{Z}\text{-decom}(T) \cdot \mathbb{Z}\text{-QMorph}(V, \ker T)$.

PROOF: Set $g = \mathbb{Z}\text{-decom}(T) \cdot \mathbb{Z}\text{-QMorph}(V, \ker T)$. For every element z of V, $T(z) = g(z)$ by [10, (15)]. □

(27) Let us consider $\mathbb{Z}$-modules V, U, W, a linear transformation f from V to U, and a linear transformation g from U to W. Then $g \cdot f$ is a linear transformation from V to W.

PROOF: Set $\mathfrak{f} = g \cdot f$. For every elements x, y of V, $\mathfrak{f}(x + y) = \mathfrak{f}(x) + \mathfrak{f}(y)$ by [10, (15)]. For every element a of $\mathbb{Z}^{\mathrm{R}}$ and for every element x of V, $\mathfrak{f}(a \cdot x) = a \cdot \mathfrak{f}(x)$ by [10, (15)]. □

Let V, U, W be $\mathbb{Z}$-modules, f be a linear transformation from V to U, and g be a linear transformation from U to W. One can check that the functor $g \cdot f$ yields a linear transformation from V to W. Now we state the propositions:

(28) Let us consider $\mathbb{Z}$-modules V, W, and a linear transformation f from V to W. Then the carrier of $\ker f = f^{-1}(\{0_W\})$.

PROOF: For every object x, $x \in$ the carrier of $\ker f$ iff $x \in f^{-1}(\{0_W\})$ by [10, (38)]. □

(29) Let us consider $\mathbb{Z}$-modules V, U, W, a linear transformation f from V to U, and a linear transformation g from U to W. Then the carrier of

$\ker g \cdot f = f^{-1}$(the carrier of $\ker g$). The theorem is a consequence of (28).

(30) Let us consider $\mathbb{Z}$-modules V, W, and a linear transformation f from V to W. If f is onto, then $\mathrm{im}\, f = \Omega_W$.

(31) Let us consider a $\mathbb{Z}$-module V, and a submodule W of V. Then $\ker \mathbb{Z}\text{-QMorph}(V, W) = \Omega_W$.
PROOF: Set $f = \mathbb{Z}\text{-QMorph}(V, W)$. Reconsider $W_1 = \Omega_W$ as a strict submodule of V. For every object x, $x \in f^{-1}(\{0_{\mathbb{Z}\text{-ModuleQuot}(V,W)}\})$ iff $x \in$ the carrier of W by [10, (38)], [14, (63)]. $\ker f = W_1$. □

(32) Let us consider a $\mathbb{Z}$-module V, a submodule W of V, a strict submodule W_1 of V, and a vector v of V. If $W_1 = \Omega_W$, then $v + W = v + W_1$.
PROOF: For every object x, $x \in v + W$ iff $x \in v + W_1$ by [14, (72)]. □

(33) Let us consider a $\mathbb{Z}$-module V, a submodule W of V, a strict submodule W_1 of V, and an object A. If $W_1 = \Omega_W$, then A is a coset of W iff A is a coset of W_1. The theorem is a consequence of (32).

Let us consider a $\mathbb{Z}$-module V, a submodule W of V, and a strict submodule W_1 of V.

Let us assume that $W_1 = \Omega_W$. Now we state the propositions:

(34) $\mathrm{CosetSet}(V, W) = \mathrm{CosetSet}(V, W_1)$. The theorem is a consequence of (33).

(35) $\mathrm{addCoset}(V, W) = \mathrm{addCoset}(V, W_1)$. The theorem is a consequence of (34) and (32).

(36) $\mathrm{lmultCoset}(V, W) = \mathrm{lmultCoset}(V, W_1)$. The theorem is a consequence of (34) and (32).

(37) $\mathbb{Z}\text{-ModuleQuot}(V, W) = \mathbb{Z}\text{-ModuleQuot}(V, W_1)$. The theorem is a consequence of (34), (35), and (36).

Now we state the propositions:

(38) Let us consider $\mathbb{Z}$-modules V, U, a submodule V_1 of V, a submodule U_1 of U, and a linear transformation f from V to U. Suppose f is onto and the carrier of $V_1 = f^{-1}$(the carrier of U_1). Then there exists a linear transformation F from $\mathbb{Z}\text{-ModuleQuot}(V, V_1)$ to $\mathbb{Z}\text{-ModuleQuot}(U, U_1)$ such that F is bijective. The theorem is a consequence of (37), (29), (31), and (30).

(39) Let us consider a $\mathbb{Z}$-module V, submodules W_1, W_2 of V, a submodule U_1 of $W_1 + W_2$, and a strict submodule U_2 of W_1. Suppose $U_1 = W_2$ and $U_2 = W_1 \cap W_2$. Then there exists a linear transformation F from $\mathbb{Z}\text{-ModuleQuot}(W_1 + W_2, U_1)$ to $\mathbb{Z}\text{-ModuleQuot}(W_1, U_2)$ such that F is bijective.
PROOF: Set $Z_1 = \mathbb{Z}\text{-ModuleQuot}(W_1 + W_2, U_1)$. Set $Z_2 = \mathbb{Z}\text{-ModuleQuot}$

(W_1, U_2). Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element v of $W_1 + W_2$ such that $\$_1 = v$ and $\$_2 = v + U_1$. For every element z of W_1, there exists an element y of Z_1 such that $\mathcal{P}[z, y]$ by [14, (25), (93)]. Consider f being a function from the carrier of W_1 into the carrier of Z_1 such that for every element z of W_1, $\mathcal{P}[z, f(z)]$ from [10, Sch. 3]. f is a linear transformation from W_1 to Z_1 by [14, (25), (28), (29)]. $\ker f = U_2$ by [26, (20)], [14, (63), (94), (46)]. $\operatorname{im} f = \mathbb{Z}\text{-ModuleQuot}(W_1 + W_2, U_1)$ by [14, (92), (93), (28)]. Reconsider $F = \mathbb{Z}\text{-decom}(f)$ as a linear transformation from Z_2 to Z_1. Consider F_1 being a linear transformation from Z_1 to Z_2 such that $F_1 = F^{-1}$ and F_1 is bijective. □

(40) Let us consider a $\mathbb{Z}$-module V, a submodule W_1 of V, a submodule W_2 of W_1, a submodule U_1 of V, and a submodule U_2 of $\mathbb{Z}\text{-ModuleQuot}(V, U_1)$. Suppose $U_1 = W_2$ and $U_2 = \mathbb{Z}\text{-ModuleQuot}(W_1, W_2)$. Then there exists a linear transformation F from $\mathbb{Z}\text{-ModuleQuot}(\mathbb{Z}\text{-ModuleQuot}(V, U_1), U_2)$ to $\mathbb{Z}\text{-ModuleQuot}(V, W_1)$ such that F is bijective.

Proof: Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ there exists an element v of V such that $\$_1 = v + U_1$ and $\$_2 = v + W_1$. For every element z of $\mathbb{Z}\text{-ModuleQuot}(V, U_1)$, there exists an element y of $\mathbb{Z}\text{-ModuleQuot}(V, W_1)$ such that $\mathcal{P}[z, y]$ by [10, (113)]. Consider f being a function from $\mathbb{Z}\text{-ModuleQuot}(V, U_1)$ into $\mathbb{Z}\text{-ModuleQuot}(V, W_1)$ such that for every element z of $\mathbb{Z}\text{-ModuleQuot}(V, U_1)$, $\mathcal{P}[z, f(z)]$ from [10, Sch. 3]. f is a linear transformation from $\mathbb{Z}\text{-ModuleQuot}(V, U_1)$ to $\mathbb{Z}\text{-ModuleQuot}(V, W_1)$ by [14, (58), (24), (68)]. $\ker f = U_2$ by [26, (20)], [14, (63), (24), (28)]. $\operatorname{im} f = \mathbb{Z}\text{-ModuleQuot}(V, W_1)$ by [14, (58), (24), (68)], [10, (38), (41)]. □

Let V be a $\mathbb{Z}$-module and a be a non zero element of $\mathbb{Z}^{\mathrm{R}}$. Let us observe that $\mathbb{Z}\text{-ModuleQuot}(V, a \circ V)$ is torsion.

Now we state the propositions:

(41) Let us consider a trivial $\mathbb{Z}$-module V. Then $\Omega_V = \mathbf{0}_V$.

(42) Let us consider a $\mathbb{Z}$-module V, and a vector v of V. If $v \neq 0_V$, then $\operatorname{Lin}(\{v\})$ is not trivial. The theorem is a consequence of (41).

(43) There exists a $\mathbb{Z}$-module V and there exists an element p of $\mathbb{Z}^{\mathrm{R}}$ such that $p \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $\mathbb{Z}\text{-ModuleQuot}(V, p \circ V)$ is not trivial.

Proof: Reconsider $V = \langle$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 $(\mathbb{Z}^{\mathrm{R}})\rangle$ as a $\mathbb{Z}$-module. Reconsider $p = 2$ as an element of $\mathbb{Z}^{\mathrm{R}}$. $\mathbb{Z}\text{-ModuleQuot}(V, p \circ V)$ is not trivial by [14, (63)], [19, (14)]. □

Note that there exists a torsion $\mathbb{Z}$-module which is non trivial and there exists a $\mathbb{Z}$-module which is non torsion-free.

Let V be a non torsion-free $\mathbb{Z}$-module. Let us note that there exists a vector of V which is non zero and torsion and there exists a finitely generated $\mathbb{Z}$-module which is non trivial.

Now we state the proposition:

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

Observe that every non torsion-free $\mathbb{Z}$-module is non trivial and there exists a finitely generated, torsion-free $\mathbb{Z}$-module which is non trivial.

Let V be a non trivial, finitely generated, torsion-free $\mathbb{Z}$-module and p be a prime element of $\mathbb{Z}^{\rm R}$. Let us note that $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ is non trivial and there exists a torsion $\mathbb{Z}$-module which is finitely generated and there exists a finitely generated, torsion $\mathbb{Z}$-module which is non trivial.

Let V be a non trivial, finitely generated, torsion-free $\mathbb{Z}$-module and p be a prime element of $\mathbb{Z}^{\rm R}$. Note that $\mathbb{Z}$-ModuleQuot$(V, p \circ V)$ is finitely generated and torsion.

Let V be a non torsion $\mathbb{Z}$-module.

One can verify that $\mathbb{Z}$-ModuleQuot$(V, \text{torsion-part}(V))$ is non trivial.

References

[1] Jesse Alama. The rank+nullity theorem. *Formalized Mathematics*, 15(**3**):137–142, 2007. doi:10.2478/v10037-007-0015-6.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

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

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

[5] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.

[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[7] 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.

[8] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.

[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[11] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[12] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[13] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

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

[15] 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.

[16] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Free ℤ-module. *Formalized Mathematics*, 20(**4**):275–280, 2012. doi:10.2478/v10037-012-0033-x.

[17] Yuichi Futa, Hiroyuki Okazaki, Daichi Mizushima, and Yasunari Shidama. Gaussian integers. *Formalized Mathematics*, 21(**2**):115–125, 2013. doi:10.2478/forma-2013-0013.

[18] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Submodule of free ℤ-module. *Formalized Mathematics*, 21(**4**):273–282, 2013. doi:10.2478/forma-2013-0029.

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

[20] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

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

[22] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

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

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

[25] Michał Muzalewski. Rings and modules – part II. *Formalized Mathematics*, 2(**4**):579–585, 1991.

[26] Kazuhisa Nakasho, Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Rank of submodule, linear transformations and linearly independent subsets of ℤ-module. *Formalized Mathematics*, 22(**3**):189–198, 2014. doi:10.2478/forma-2014-0021.

[27] Christoph Schwarzweller. The binomial theorem for algebraic structures. *Formalized Mathematics*, 9(**3**):559–564, 2001.

[28] Christoph Schwarzweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.

[29] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**): 115–122, 1990.

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

[31] Wojciech A. Trybulec. Operations on subspaces in real linear space. *Formalized Mathematics*, 1(**2**):395–399, 1990.

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

[33] Wojciech A. Trybulec. Subspaces and cosets of subspaces in vector space. *Formalized Mathematics*, 1(**5**):865–870, 1990.

[34] Wojciech A. Trybulec. Operations on subspaces in vector space. *Formalized Mathematics*, 1(**5**):871–876, 1990.

[35] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1 (**5**):877–882, 1990.

[36] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(**5**):883–885, 1990.

[37] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

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

[39] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received August 14, 2015
