FORMALIZED MATHEMATICS
Vol. 22, No. 4, Pages 277–289, 2014
DOI: 10.2478/forma-2014-0028

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

Torsion $\mathbb{Z}$-module and Torsion-free $\mathbb{Z}$-module[1]

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

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Kazuhisa Nakasho
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize a torsion $\mathbb{Z}$-module and a torsion-free $\mathbb{Z}$-module. Especially, we prove formally that finitely generated torsion-free $\mathbb{Z}$-modules are finite rank free. We also formalize properties related to rank of finite rank free $\mathbb{Z}$-modules. The notion of $\mathbb{Z}$-module is necessary for solving lattice problems, LLL (Lenstra, Lenstra, and Lovász) base reduction algorithm [20], cryptographic systems with lattice [21], and coding theory [11].

MSC: 13C10 15A04 03B35

Keywords: free Z-module; rank of Z-module; homomorphism of Z-module; linearly independent; linear combination

MML identifier: ZMODUL06, version: 8.1.04 5.32.1237

The notation and terminology used in this paper have been introduced in the following articles: [24], [5], [1], [26], [10], [6], [7], [15], [28], [27], [25], [3], [4], [8], [17], [33], [34], [29], [32], [18], [31], [9], [12], [13], [14], and [22].

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

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

1. Torsion $\mathbb{Z}$-module and Torsion-free $\mathbb{Z}$-module

Now we state the proposition:

(1) Let us consider a $\mathbb{Z}$-module V, and a submodule W of V. Then $1_{\mathbb{Z}^{\mathrm{R}}} \circ W = \Omega_W$.

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

(2) $W_1 \cap W_2$ is a submodule of $(W_1 + W_3) \cap W_2$.
PROOF: For every vector v of V such that $v \in W_1 \cap W_2$ holds $v \in (W_1 + W_3) \cap W_2$ by [12, (94), (93)]. $\square$

(3) If $W_1 \cap W_2 \neq \mathbf{0}_V$, then $(W_1 + W_3) \cap W_2 \neq \mathbf{0}_V$.

(4) Let us consider a $\mathbb{Z}$-module V, and linearly independent subsets I, I_1 of V. If $I_1 \subseteq I$, then $\mathrm{Lin}(I \setminus I_1) \cap \mathrm{Lin}(I_1) = \mathbf{0}_V$.

From now on V denotes a $\mathbb{Z}$-module, W denotes a submodule of V, v, u denote vectors of V, and i denotes an element of $\mathbb{Z}^{\mathrm{R}}$. Let V be a $\mathbb{Z}$-module and v be a vector of V. We say that v is torsion if and only if

(Def. 1) there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $i \cdot v = 0_V$.

One can verify that 0_V is torsion.

Now we state the propositions:

(5) If v is torsion and u is torsion, then $v + u$ is torsion.

(6) If v is torsion, then $-v$ is torsion.

(7) If v is torsion and u is torsion, then $v - u$ is torsion.

(8) If v is torsion, then $i \cdot v$ is torsion.

(9) Let us consider a vector v of V, and a vector w of W. If $v = w$, then v is torsion iff w is torsion.

Let V be a $\mathbb{Z}$-module. One can verify that there exists a vector of V which is torsion.

Now we state the propositions:

(10) If v is not torsion, then $-v$ is not torsion.

(11) If v is not torsion and $i \neq 0$, then $i \cdot v$ is not torsion.

(12) v is not torsion if and only if $\{v\}$ is linearly independent.
PROOF: If v is not torsion, then $\{v\}$ is linearly independent by [9, (33)], [13, (24)]. If $\{v\}$ is linearly independent, then v is not torsion by [14, (1)], [13, (8), (29), (53)]. $\square$

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

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

Let us note that $\mathbf{0}_V$ is torsion and there exists a $\mathbb{Z}$-module which is torsion.

Now we state the propositions:

(13) Let us consider an element v of $\mathbb{Z}^{\mathrm{R}}$, and an integer v_1. Suppose $v = v_1$. Let us consider a natural number n. Then (Nat-mult-left $\mathbb{Z}^{\mathrm{R}})(n, v) = n \cdot v_1$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv (\text{Nat-mult-left}\,\mathbb{Z}^{\mathrm{R}})(\$_1, v) = \$_1 \cdot v_1$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(14) Let us consider an element x of $\mathbb{Z}^{\mathrm{R}}$, an element v of $\mathbb{Z}^{\mathrm{R}}$, and an integer v_1. Suppose $v = v_1$. Then (the left integer multiplication of $(\mathbb{Z}^{\mathrm{R}}))(x, v) = x \cdot v_1$. The theorem is a consequence of (13).

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

Let V be a non torsion $\mathbb{Z}$-module. Let us observe that there exists a vector of V which is non torsion.

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

(Def. 3) for every vector v of V such that $v \neq 0_V$ holds v is not torsion.

Now we state the proposition:

(15) V is cancelable on multiplication if and only if V is torsion-free.

One can verify that every cancelable on multiplication $\mathbb{Z}$-module is torsion-free and every torsion-free $\mathbb{Z}$-module is cancelable on multiplication and every free $\mathbb{Z}$-module is torsion-free and there exists a $\mathbb{Z}$-module which is torsion-free and free.

Now we state the proposition:

(16) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of V. Then v is torsion if and only if $v = 0_V$.

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

Let V be a $\mathbb{Z}$-module. Observe that $\mathbf{0}_V$ is trivial and every non trivial, torsion-free $\mathbb{Z}$-module is non torsion and there exists a $\mathbb{Z}$-module which is trivial.

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

Now we state the proposition:

(17) v is not torsion if and only if $\mathrm{Lin}(\{v\})$ is free and $v \neq 0_V$. The theorem is a consequence of (12) and (9).

Let V be a non torsion $\mathbb{Z}$-module and v be a non torsion vector of V. Let us note that $\mathrm{Lin}(\{v\})$ is free.

Now we state the propositions:

(18) Let us consider a $\mathbb{Z}$-module V, a subset A of V, and a vector v of V. If A is linearly independent and $v \in A$, then v is not torsion. The theorem

is a consequence of (12).

(19) Let us consider an object u. Suppose $u \in \mathrm{Lin}(\{v\})$. Then there exists an element i of $\mathbb{Z}^{\mathrm{R}}$ such that $u = i \cdot v$.

(20) $v \in \mathrm{Lin}(\{v\})$.

(21) $i \cdot v \in \mathrm{Lin}(\{v\})$.

(22) $\mathrm{Lin}(\{0_V\}) = \mathbf{0}_V$.

PROOF: For every object x, $x \in \mathrm{Lin}(\{0_V\})$ iff $x \in \mathbf{0}_V$ by [13, (64), (21)], [12, (1)], [13, (66)]. □

Let V be a torsion-free $\mathbb{Z}$-module and v be a vector of V. Let us note that $\mathrm{Lin}(\{v\})$ is free. Now we state the propositions:

(23) Let us consider subsets A_1, A_2 of V. Suppose A_1 is linearly independent and A_2 is linearly independent and $A_1 \cap A_2 = \emptyset$ and $A_1 \cup A_2$ is linearly dependent. Then $\mathrm{Lin}(A_1) \cap \mathrm{Lin}(A_2) \neq \mathbf{0}_V$.

(24) Let us consider a $\mathbb{Z}$-module V, a free submodule W of V, a subset I of V, and a vector v of V. Suppose I is linearly independent and $\mathrm{Lin}(I) = \Omega_W$ and $v \in I$. Then

(i) $\Omega_W = \mathrm{Lin}(I \setminus \{v\}) + \mathrm{Lin}(\{v\})$, and

(ii) $\mathrm{Lin}(I \setminus \{v\}) \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$, and

(iii) $\mathrm{Lin}(I \setminus \{v\})$ is free, and

(iv) $\mathrm{Lin}(\{v\})$ is free, and

(v) $v \neq 0_V$.

PROOF: v is not torsion. $\mathrm{Lin}(I \setminus \{v\}) \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$ by [16, (24)], [12, (94)], [13, (64), (23), (10)]. □

(25) Let us consider a $\mathbb{Z}$-module V, and a free submodule W of V. Then there exists a subset A of V such that

(i) A is subset of W and linearly independent, and

(ii) $\mathrm{Lin}(A) = \Omega_W$.

(26) Let us consider a $\mathbb{Z}$-module V, and a finite rank, free submodule W of V. Then there exists a finite subset A of V such that

(i) A is finite subset of W and linearly independent, and

(ii) $\mathrm{Lin}(A) = \Omega_W$, and

(iii) $\overline{\overline{A}} = \mathrm{rank}\, W$.

Let us consider a torsion-free $\mathbb{Z}$-module V and vectors v_1, v_2 of V.

Let us assume that $v_1 \neq 0_V$ and $v_2 \neq 0_V$ and $\mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\}) \neq \mathbf{0}_V$. Now we state the propositions:

(27) There exists a vector u of V such that

(i) $u \neq 0_V$, and

(ii) $\mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{u\})$.

Proof: Consider x being a vector of V such that $x \in \mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\})$ and $x \neq 0_V$. Consider i_3 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_3 \cdot v_1$. Consider i_4 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_4 \cdot v_2$. Consider i_1, i_2 being integers such that $i_3 = (\gcd(i_3, i_4)) \cdot i_1$ and $i_4 = (\gcd(i_3, i_4)) \cdot i_2$ and i_1 and i_2 are relatively prime. Reconsider $I_1 = i_1$, $I_2 = i_2$ as an element of $\mathbb{Z}^{\mathrm{R}}$. $I_1 \cdot v_1 \in \mathrm{Lin}(\{v_1\})$ and $I_2 \cdot v_2 \in \mathrm{Lin}(\{v_2\})$. For every vector y of V such that $y \in \mathrm{Lin}(\{I_1 \cdot v_1\})$ holds $y \in \mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\})$ by (19), [12, (37)]. $\mathrm{Lin}(\{I_1 \cdot v_1\}) = \mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\})$ by [12, (46), (94)], (19), [12, (37), (36)]. □

(28) There exists a vector u of V such that

(i) $u \neq 0_V$, and

(ii) $\mathrm{Lin}(\{v_1\}) + \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{u\})$.

Proof: Consider x being a vector of V such that $x \neq 0_V$ and $\mathrm{Lin}(\{v_1\}) \cap \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{x\})$. Consider i_1 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_1 \cdot v_1$. Consider i_2 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x = i_2 \cdot v_2$. $\gcd(|i_1|, |i_2|) = 1$ by [19, (5)], [23, (2)], [12, (1)], [3, (25)]. Consider j_1, j_2 being elements of $\mathbb{Z}^{\mathrm{R}}$ such that $i_1 \cdot j_1 + i_2 \cdot j_2 = 1$. Reconsider $J_1 = j_1$, $J_2 = j_2$ as an element of $\mathbb{Z}^{\mathrm{R}}$. Reconsider $u = J_1 \cdot v_2 + J_2 \cdot v_1$ as a vector of V. $\mathrm{Lin}(\{v_1\}) + \mathrm{Lin}(\{v_2\}) = \mathrm{Lin}(\{u\})$ by (19), [12, (37), (92), (36)]. □

(29) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and vectors v, u of V. Suppose $v \neq 0_V$ and $u \neq 0_V$ and $W \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$ and $(W + \mathrm{Lin}(\{u\})) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\mathrm{Lin}(\{u\}) \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$. Then there exist vectors w_1, w_2 of V such that

(i) $w_1 \neq 0_V$, and

(ii) $w_2 \neq 0_V$, and

(iii) $W + \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\}) = W + \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$, and

(iv) $W \cap \mathrm{Lin}(\{w_1\}) \neq \mathbf{0}_V$, and

(v) $(W + \mathrm{Lin}(\{w_1\})) \cap \mathrm{Lin}(\{w_2\}) = \mathbf{0}_V$, and

(vi) u, $v \in \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$, and

(vii) w_1, $w_2 \in \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$.

Proof: Consider x being a vector of V such that $x \in (W + \mathrm{Lin}(\{u\})) \cap \mathrm{Lin}(\{v\})$ and $x \neq 0_V$. Consider x_1, x_2 being vectors of V such that $x_1 \in W$ and $x_2 \in \mathrm{Lin}(\{u\})$ and $x = x_1 + x_2$. Consider i_4 being an element of $\mathbb{Z}^{\mathrm{R}}$

such that $x = i_4 \cdot v$. Consider i_3 being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $x_2 = i_3 \cdot u$. Consider i_2, i_1 being integers such that $i_4 = (\gcd(i_4, i_3)) \cdot i_2$ and $i_3 = (\gcd(i_4, i_3)) \cdot i_1$ and i_2 and i_1 are relatively prime. Consider J_4, J_3 being elements of $\mathbb{Z}^{\mathrm{R}}$ such that $i_2 \cdot J_4 + i_1 \cdot J_3 = 1$. Reconsider $j_4 = J_4$, $j_3 = J_3$ as an element of $\mathbb{Z}^{\mathrm{R}}$. Set $w_1 = i_2 \cdot v - i_1 \cdot u$. Set $w_2 = j_4 \cdot u + j_3 \cdot v$. $w_1 \neq 0_V$ by [29, (21)], [12, (37)], (20), [12, (94), (1)]. Reconsider $i_6 = \gcd(i_4, i_3)$ as an element of $\mathbb{Z}^{\mathrm{R}}$. $i_6 \cdot w_1 \in W$ by [12, (8)]. $W \cap \mathrm{Lin}(\{w_1\}) \neq \mathbf{0}_V$ by [12, (37)], (20), [12, (94)], [13, (66)]. $u = i_2 \cdot w_2 - j_3 \cdot w_1$ by [12, (8)], [29, (29), (28), (15)]. $v = j_4 \cdot w_1 + i_1 \cdot w_2$ by [12, (8)], [29, (28), (15)]. $u \in \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ by [12, (37)], (20), [12, (38), (92)]. $v \in \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ by [12, (37)], (20), [12, (92)]. $w_1 \in \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ by [12, (37)], (20), [12, (38), (92)]. $w_2 \in \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ by [12, (37)], (20), [12, (92)]. For every object x such that $x \in W + \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ holds $x \in W + \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ by [12, (92)], (19), [12, (37), (36), (96)]. For every object x such that $x \in W + \mathrm{Lin}(\{w_1\}) + \mathrm{Lin}(\{w_2\})$ holds $x \in W + \mathrm{Lin}(\{u\}) + \mathrm{Lin}(\{v\})$ by [12, (92)], (19), [12, (37), (36), (96)]. $w_2 \neq 0_V$ by [29, (6)], [12, (37)], (20), [12, (38), (94), (1)]. $(W + \mathrm{Lin}(\{w_1\})) \cap \mathrm{Lin}(\{w_2\}) = \mathbf{0}_V$ by [16, (24)], [12, (94), (92)], (19). $\square$

(30) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and a vector v of V. Suppose $v \neq 0_V$ and $W \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $W + \mathrm{Lin}(\{v\})$ is free.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodule W of V for every vector v of V such that $v \neq 0_V$ and $W \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\operatorname{rank} W = \$_1 + 1$ holds $W + \mathrm{Lin}(\{v\})$ is free. $\mathcal{P}[0]$ by [22, (5)], [12, (25)], [14, (20)], [16, (22), (23)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [16, (33)], [12, (25)], [14, (20)], [12, (97), (51), (94)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. Set $r_1 = \operatorname{rank} W$. $r_1 - 1$ is a natural number by [22, (1)], [12, (51)], [16, (23)], [12, (107)]. $\square$

Let V be a torsion-free $\mathbb{Z}$-module, v be a vector of V, and W be a finite rank, free submodule of V. Let us note that $W + \mathrm{Lin}(\{v\})$ is free.

Let V be a $\mathbb{Z}$-module and W be a finitely generated submodule of V. One can verify that $W + \mathrm{Lin}(\{v\})$ is finitely generated.

Let W_1, W_2 be finitely generated submodules of V. Observe that $W_1 + W_2$ is finitely generated. Now we state the proposition:

(31) Let us consider a $\mathbb{Z}$-module V, a submodule W of V, submodules W_6, W_8 of W, and submodules W_1, W_2 of V. If $W_6 = W_1$ and $W_8 = W_2$, then $W_6 + W_8 = W_1 + W_2$.

PROOF: Reconsider $S = W_6 + W_8$ as a strict submodule of V. For every vector v of V, $v \in S$ iff $v \in W_1 + W_2$ by [12, (92), (28)]. $\square$

Let V be a torsion-free $\mathbb{Z}$-module and U_1, U_2 be finite rank, free submodules of V. Note that U_1+U_2 is free and every finitely generated, torsion-free $\mathbb{Z}$-module is free.

2. Rank of Finite Rank Free $\mathbb{Z}$-module

Now we state the propositions:

(32) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose $W_1 \cap W_2 = \mathbf{0}_V$. Then $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_1 + \operatorname{rank} W_2$.

(33) Let us consider a finite rank, free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose V is the direct sum of W_1 and W_2. Then $\operatorname{rank} V = \operatorname{rank} W_1 + \operatorname{rank} W_2$. The theorem is a consequence of (32).

(34) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Then $\operatorname{rank}(W_1 \cap W_2) \leqslant \operatorname{rank} W_1$.

(35) Let us consider a torsion-free $\mathbb{Z}$-module V, and a vector v of V. If $v \neq 0_V$, then $\operatorname{rank} \operatorname{Lin}(\{v\}) = 1$.

(36) Let us consider a $\mathbb{Z}$-module V. Then $\operatorname{rank} \mathbf{0}_V = 0$.

(37) Let us consider a torsion-free $\mathbb{Z}$-module V, and vectors v, u of V. Suppose $v \neq 0_V$ and $u \neq 0_V$ and $\operatorname{Lin}(\{v\}) \cap \operatorname{Lin}(\{u\}) \neq \mathbf{0}_V$. Then $\operatorname{rank}(\operatorname{Lin}(\{v\}) + \operatorname{Lin}(\{u\})) = 1$. The theorem is a consequence of (28).

(38) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and a vector v of V. Suppose $v \neq 0_V$ and $W \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $\operatorname{rank}(W + \operatorname{Lin}(\{v\})) = \operatorname{rank} W$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodule W of V for every vector v of V such that $v \neq 0_V$ and $W \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\operatorname{rank} W = \$_1 + 1$ holds $\operatorname{rank}(W + \operatorname{Lin}(\{v\})) = \operatorname{rank} W$. $\mathcal{P}[0]$ by [22, (5)], [12, (25), (26), (42)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (26), (24), [9, (31)], [2, (44)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. Set $r_1 = \operatorname{rank} W$. $r_1 - 1$ is a natural number by [22, (1)], [12, (51)], [16, (23)], [12, (107)]. $\square$

(39) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a vector v of V. Suppose $W_1 \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $W_2 \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. The theorem is a consequence of (19).

(40) Let us consider $\mathbb{Z}$-modules V, W, a linear transformation T from V to W, and a subset A of V. Then $T^{\circ}(\text{the carrier of } \operatorname{Lin}(A)) \subseteq$ the carrier of $\operatorname{Lin}(T^{\circ} A)$.

PROOF: For every object y such that $y \in T^\circ$(the carrier of $\mathrm{Lin}(A)$) holds $y \in$ the carrier of $\mathrm{Lin}(T^\circ A)$ by [7, (65)], [13, (64)], [22, (44), (46)]. $\square$

Let us consider $\mathbb{Z}$-modules X, Y and a linear transformation L from X to Y. Now we state the propositions:

(41) $L(0_X) = 0_Y$.

(42) If L is bijective, then there exists a linear transformation K from Y to X such that $K = L^{-1}$ and K is bijective.

PROOF: Reconsider $K = L^{-1}$ as a function from Y into X. K is additive by [7, (113)], [6, (34)]. For every element r of $\mathbb{Z}^{\mathrm{R}}$ and for every element x of Y, $K(r \cdot x) = r \cdot K(x)$ by [7, (113)], [6, (34)]. $\square$

(43) Let us consider $\mathbb{Z}$-modules X, Y, a linear combination l of X, and a linear transformation L from X to Y. If L is bijective, then $L \mathbin{@*} l = l \cdot L^{-1}$.

PROOF: Reconsider $K = L^{-1}$ as a function from Y into X. For every element a of Y, $(L \mathbin{@*} l)(a) = (l \cdot K)(a)$ by [6, (35)], [7, (35)], [6, (12), (34)]. $\square$

(44) Let us consider $\mathbb{Z}$-modules X, Y, a subset X_0 of X, a linear transformation L from X to Y, and a linear combination l of $L^\circ X_0$. Suppose $X_0 =$ the carrier of X and L is one-to-one. Then $L\#l = l \cdot L$.

(45) Let us consider $\mathbb{Z}$-modules X, Y, a subset A of X, and a linear transformation L from X to Y. Suppose L is bijective. Then A is linearly independent if and only if $L^\circ A$ is linearly independent. The theorem is a consequence of (42).

(46) Let us consider $\mathbb{Z}$-modules X, Y, a subset A of X, and a linear transformation T from X to Y. Suppose T is bijective. Then T°(the carrier of $\mathrm{Lin}(A)$) = the carrier of $\mathrm{Lin}(T^\circ A)$. The theorem is a consequence of (40) and (42).

(47) Let us consider a $\mathbb{Z}$-module Y, and a subset A of Y. Then $\mathrm{Lin}(A)$ is a strict submodule of Ω_Y.

(48) Let us consider $\mathbb{Z}$-modules X, Y, and a linear transformation T from X to Y. If T is bijective, then X is free iff Y is free. The theorem is a consequence of (42).

(49) Let us consider free $\mathbb{Z}$-modules X, Y, a linear transformation T from X to Y, and a subset A of X. Suppose T is bijective. Then A is a basis of X if and only if $T^\circ A$ is a basis of Y. The theorem is a consequence of (42).

(50) Let us consider free $\mathbb{Z}$-modules X, Y, and a linear transformation T from X to Y. If T is bijective, then X is finite rank iff Y is finite rank. The theorem is a consequence of (42).

(51) Let us consider finite rank, free $\mathbb{Z}$-modules X, Y, and a linear transfor-

mation T from X to Y. If T is bijective, then $\operatorname{rank} X = \operatorname{rank} Y$.

PROOF: For every basis I of X, $\operatorname{rank} Y = \overline{\overline{I}}$ by [1, (5), (33)], (49). $\square$

(52) Let us consider a $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. If $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$, then $\operatorname{rank}(a \circ W) = \operatorname{rank} W$.

PROOF: Define $\mathcal{P}[\text{element of } W, \text{object}] \equiv \$_2 = a \cdot \$_1$. For every element x of W, there exists an element y of $a \circ W$ such that $\mathcal{P}[x, y]$. Consider F being a function from W into $a \circ W$ such that for every element x of W, $\mathcal{P}[x, F(x)]$ from [7, Sch. 3]. For every objects x_1, x_2 such that x_1, $x_2 \in$ the carrier of W and $F(x_1) = F(x_2)$ holds $x_1 = x_2$ by [12, (10)]. For every object y such that $y \in$ the carrier of $a \circ W$ holds $y \in \operatorname{rng} F$ by [7, (4)]. F is additive by [12, (28)]. For every element r of $\mathbb{Z}^{\mathrm{R}}$ and for every element x of W, $F(r \cdot x) = r \cdot F(x)$ by [12, (29)]. $\square$

(53) Let us consider a $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2, W_3 of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $W_3 = a \circ W_1$. Then $\operatorname{rank}(W_3 \cap W_2) = \operatorname{rank}(W_1 \cap W_2)$.

PROOF: $W_3 \cap W_2$ is a submodule of $W_1 \cap W_2$ by [12, (105), (42)], [13, (75)]. $a \circ (W_1 \cap W_2)$ is a submodule of $W_3 \cap W_2$ by [12, (42), (25), (94)]. $\operatorname{rank}(W_1 \cap W_2) \leqslant \operatorname{rank}(W_3 \cap W_2)$. $\square$

(54) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2, W_3 of V, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Suppose $a \neq 0_{\mathbb{Z}^{\mathrm{R}}}$ and $W_3 = a \circ W_1$. Then $\operatorname{rank}(W_3 + W_2) = \operatorname{rank}(W_1 + W_2)$.

PROOF: For every vector v of V such that $v \in W_3 + W_2$ holds $v \in W_1 + W_2$ by [12, (92)]. For every vector v of V such that $v \in a \circ (W_1 + W_2)$ holds $v \in W_3 + W_2$ by [12, (25), (92), (29)]. $\operatorname{rank}(W_1 + W_2) \leqslant \operatorname{rank}(W_3 + W_2)$. $\square$

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

(55) Suppose for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodules W_1, W_2 of V for every basis I of W_1 such that for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\operatorname{rank} W_1 = \$_1$ holds $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (25)], [14, (15)], [13, (56)], [14, (20)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(56) Suppose $\operatorname{rank}(W_1 \cap W_2) < \operatorname{rank} W_1$. Then there exists a vector v of V such that

(i) $v \in I$, and

(ii) $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) = \mathbf{0}_V$.

(57) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I of W_1. Suppose $\mathrm{rank}(W_1 \cap W_2) = \mathrm{rank}\, W_1$. Let us consider a vector v of V. If $v \in I$, then $(W_1 \cap W_2) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. The theorem is a consequence of (24), (32), and (35).

(58) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I of W_1. Suppose for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $\mathrm{rank}(W_1 + W_2) = \mathrm{rank}\, W_2$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodules W_1, W_2 of V for every basis I of W_1 such that for every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\mathrm{rank}\, W_1 = \$_1$ holds $\mathrm{rank}(W_1 + W_2) = \mathrm{rank}\, W_2$. $\mathcal{P}[0]$ by [22, (1)], [12, (51), (42)], [16, (22)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (25)], [14, (15)], [13, (56)], [14, (20)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(59) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose $\mathrm{rank}(W_1 \cap W_2) = \mathrm{rank}\, W_1$. Then $\mathrm{rank}(W_1 + W_2) = \mathrm{rank}\, W_2$. The theorem is a consequence of (57) and (58).

(60) Let us consider a field G, a vector space V over G, and a subset A of V. If A is linearly independent, then A is a basis of $\mathrm{Lin}(A)$.

(61) Let us consider a cancelable on multiplication, finite rank, free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Then $\mathrm{rank}(W_1 + W_2) + \mathrm{rank}(W_1 \cap W_2) = \mathrm{rank}\, W_1 + \mathrm{rank}\, W_2$.
PROOF: Consider I_1 being a finite subset of V such that I_1 is finite subset of W_1 and linearly independent and $\mathrm{Lin}(I_1) = \Omega_{W_1}$ and $\overline{\overline{I_1}} = \mathrm{rank}\, W_1$. Consider I_2 being a finite subset of V such that I_2 is finite subset of W_2 and linearly independent and $\mathrm{Lin}(I_2) = \Omega_{W_2}$ and $\overline{\overline{I_2}} = \mathrm{rank}\, W_2$. Consider I_4 being a finite subset of V such that I_4 is finite subset of $W_1 + W_2$ and linearly independent and $\mathrm{Lin}(I_4) = \Omega_{W_1+W_2}$ and $\overline{\overline{I_4}} = \mathrm{rank}(W_1 + W_2)$. Consider I_3 being a finite subset of V such that I_3 is finite subset of $W_1 \cap W_2$ and linearly independent and $\mathrm{Lin}(I_3) = \Omega_{W_1 \cap W_2}$ and $\overline{\overline{I_3}} = \mathrm{rank}(W_1 \cap W_2)$. Set $I_6 = (\mathrm{MorphsZQ}\, V)^\circ I_1$. Set $I_8 = (\mathrm{MorphsZQ}\, V)^\circ I_2$. Set $I_5 = (\mathrm{MorphsZQ}\, V)^\circ I_4$. Set $I_7 = (\mathrm{MorphsZQ}\, V)^\circ I_3$. For every vector v of Z MQ VectSp V, $v \in \mathrm{Lin}(I_6) + \mathrm{Lin}(I_8)$ iff $v \in \mathrm{Lin}(I_5)$ by [30, (1)], [31, (7)], [16, (9), (10)]. For every vector v of Z MQ VectSp V, $v \in \mathrm{Lin}(I_6) \cap \mathrm{Lin}(I_8)$ iff $v \in \mathrm{Lin}(I_7)$ by [30, (3)], [31, (7)], [16, (9), (10)]. □

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:

(62) $\mathrm{rank}(W_1 + W_2) + \mathrm{rank}(W_1 \cap W_2) = \mathrm{rank}\, W_1 + \mathrm{rank}\, W_2$.
PROOF: Set $W_5 = W_1 + W_2$. Reconsider $W_4 = W_1$ as a finite rank, free

submodule of W_5. Reconsider $W_7 = W_2$ as a finite rank, free submodule of W_5. $\mathrm{rank}(W_4 + W_7) + \mathrm{rank}(W_4 \cap W_7) = \mathrm{rank}\, W_4 + \mathrm{rank}\, W_7$. For every vector v of V, $v \in W_4 + W_7$ iff $v \in W_1 + W_2$ by [12, (92), (25), (28)]. For every vector v of V, $v \in W_4 \cap W_7$ iff $v \in W_1 \cap W_2$ by [12, (94)]. □

(63) If $\mathrm{rank}(W_1 + W_2) = \mathrm{rank}\, W_2$, then $\mathrm{rank}(W_1 \cap W_2) = \mathrm{rank}\, W_1$. The theorem is a consequence of (62).

(64) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a vector v of V. Suppose $v \neq 0_V$ and $W_1 \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$ and $(W_1 + W_2) \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$. Then $\mathrm{rank}((W_1 + \mathrm{Lin}(\{v\})) \cap W_2) = \mathrm{rank}(W_1 \cap W_2)$.
PROOF: For every vector u of V such that $u \in W_1 \cap W_2$ holds $u \in (W_1 + \mathrm{Lin}(\{v\})) \cap W_2$ by [12, (94), (93)]. There exists a vector u of V such that $u \in (W_1 + \mathrm{Lin}(\{v\})) \cap W_2$ and $u \notin W_1 \cap W_2$ by [12, (44)], [22, (2)]. Consider u being a vector of V such that $u \in (W_1 + \mathrm{Lin}(\{v\})) \cap W_2$ and $u \notin W_1 \cap W_2$. Consider u_1, u_2 being vectors of V such that $u_1 \in W_1$ and $u_2 \in \mathrm{Lin}(\{v\})$ and $u = u_1 + u_2$. □

Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and a vector v of V.

Let us assume that $v \neq 0_V$ and $W \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. Now we state the propositions:

(65) $\mathrm{rank}(W \cap \mathrm{Lin}(\{v\})) = 1$.
PROOF: $\mathrm{rank}\, \mathrm{Lin}(\{v\}) = 1$. $\mathrm{rank}(W \cap \mathrm{Lin}(\{v\})) \neq 0$ by [22, (1)], [12, (51)]. □

(66) There exists a vector u of V such that

(i) $u \neq 0_V$, and

(ii) $W \cap \mathrm{Lin}(\{v\}) = \mathrm{Lin}(\{u\})$.

The theorem is a consequence of (65).

(67) Let us consider a torsion-free $\mathbb{Z}$-module V, a finite rank, free submodule W of V, and vectors u, v of V. Suppose $W \cap \mathrm{Lin}(\{v\}) = \mathbf{0}_V$ and $(W + \mathrm{Lin}(\{u\})) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $W \cap \mathrm{Lin}(\{u\}) = \mathbf{0}_V$. The theorem is a consequence of (19).

(68) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a vector v of V. Suppose $\mathrm{rank}(W_1 \cap W_2) = \mathrm{rank}\, W_1$ and $(W_1 + W_2) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. Then $W_2 \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$.
PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite rank, free submodules W_1, W_2 of V for every vector v of V such that $\mathrm{rank}(W_1 \cap W_2) = \mathrm{rank}\, W_1$ and $(W_1 + W_2) \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$ and $\mathrm{rank}\, W_1 = \$_1$ holds $W_2 \cap \mathrm{Lin}(\{v\}) \neq \mathbf{0}_V$. $\mathcal{P}[0]$ by [22, (1)], [12, (51), (42)], [16, (22)]. For every natural number

n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by (26), [14, (20), (16)], (24). For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(69) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2, W_3 of V. Suppose $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$ and W_3 is a submodule of W_1. Then $\operatorname{rank}(W_3 + W_2) = \operatorname{rank} W_2$.

PROOF: For every vector v of V such that $v \in W_3 + W_2$ holds $v \in W_1 + W_2$ by [12, (92), (23)]. $\square$

(70) Let us consider a torsion-free $\mathbb{Z}$-module V, finite rank, free submodules W_1, W_2 of V, and a basis I of W_1. Suppose $\operatorname{rank}(W_1 + W_2) = \operatorname{rank} W_2$. Let us consider a vector v of V. If $v \in I$, then $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$.

PROOF: For every vector v of V such that $v \in I$ holds $(W_1 \cap W_2) \cap \operatorname{Lin}(\{v\}) \neq \mathbf{0}_V$ by [14, (15)], [13, (57), (65)], [9, (31)]. $\square$

(71) Let us consider a torsion-free $\mathbb{Z}$-module V, and finite rank, free submodules W_1, W_2 of V. Suppose $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$. Then there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \circ W_1$ is a submodule of W_2.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite rank, free submodules W_1, W_2 of V such that $\operatorname{rank}(W_1 \cap W_2) = \operatorname{rank} W_1$ and $\operatorname{rank} W_1 = \$_1$ there exists an element a of $\mathbb{Z}^{\mathrm{R}}$ such that $a \circ W_1$ is a submodule of W_2. $\mathcal{P}[0]$ by [22, (1)], [12, (55)], (1). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [12, (25)], [14, (15)], [13, (56)], [14, (20)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

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] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[8] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[9] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[10] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[11] Wolfgang Ebeling. *Lattices and Codes.* Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.
[12] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.
[13] 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.

[14] 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.

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

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

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

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

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

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

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

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

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

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

[28] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

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

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

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

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

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

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

Received November 29, 2014