

Matrix of \mathbb{Z} -module¹

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

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize a matrix of \mathbb{Z} -module and its properties. Specially, we formalize a matrix of a linear transformation of \mathbb{Z} -module, a bilinear form and a matrix of the bilinear form (Gramian matrix). We formally prove that for a finite-rank free \mathbb{Z} -module V , determinant of its Gramian matrix is constant regardless of selection of its basis. \mathbb{Z} -module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattices [22] and coding theory [14]. Some theorems in this article are described by translating theorems in [24], [26] and [19] into theorems of \mathbb{Z} -module.

MSC: 11E39 13C10 03B35

Keywords: matrix of \mathbb{Z} -module; matrix of linear transformation; bilinear form

MML identifier: ZMATRLIN, version: 8.1.04 5.31.1231

The notation and terminology used in this paper have been introduced in the following articles: [6], [1], [7], [5], [8], [13], [30], [9], [10], [2], [41], [34], [23], [31], [28], [27], [17], [42], [24], [25], [4], [11], [18], [39], [40], [35], [38], [21], [36], [37], [12], [15], and [16].

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

1. PRELIMINARIES

From now on x, y, z denote objects, i, j, k, l, n, m denote natural numbers, D, E denote non empty sets, M denotes a matrix over D , and L denotes a matrix over E .

Now we state the proposition:

- (1) Let us consider natural numbers i, j . Suppose $M = L$ and $\langle i, j \rangle \in$ the indices of M . Then $M_{i,j} = L_{i,j}$.

Let us consider a natural number i . Now we state the propositions:

- (2) If $M = L$ and $i \in \text{dom } M$, then $\text{Line}(M, i) = \text{Line}(L, i)$.

PROOF: For every j such that $j \in \text{dom } \text{Line}(M, i)$ holds $\text{Line}(M, i)(j) = \text{Line}(L, i)(j)$ by [12, (87)], (1). \square

- (3) If $M = L$ and $i \in \text{Seg width } M$, then $M_{\square, i} = L_{\square, i}$.

PROOF: For every j such that $j \in \text{dom } M_{\square, i}$ holds $M_{\square, i}(j) = L_{\square, i}(j)$ by [12, (87)], (1). \square

Now we state the propositions:

- (4) Suppose $\text{len } M = \text{len } L$ and $\text{width } M = \text{width } L$ and for every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} = L_{i,j}$. Then $M = L$.

PROOF: M is a matrix over E by [12, (87)]. Reconsider $L_0 = M$ as a matrix over E . For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of L_0 holds $L_{0i,j} = L_{i,j}$. \square

- (5) Let us consider a matrix M over D . Suppose for every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} \in E$. Then M is a matrix over E .

- (6) If $M = L$, then $M^T = L^T$. The theorem is a consequence of (1) and (5).

- (7) Every matrix over \mathbb{Z} is a matrix over \mathbb{R} .

Let M be a matrix over \mathbb{Z} . The functor $\mathbb{Z}2\mathbb{R}(M)$ yielding a matrix over \mathbb{R} is defined by the term

(Def. 1) M .

Let n, m be natural numbers and M be a matrix over \mathbb{Z} of dimension $n \times m$. Let us note that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a matrix over \mathbb{R} of dimension $n \times m$. Let n be a natural number and M be a square matrix over \mathbb{Z} of dimension n . Observe that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a square matrix over \mathbb{R} of dimension n . Let M be a matrix over \mathbb{R} . We say that M is integer if and only if

(Def. 2) M is a matrix over \mathbb{Z} .

One can verify that there exists a matrix over \mathbb{R} which is integer.

Let n, m be natural numbers. Observe that there exists a matrix over \mathbb{R} of dimension $n \times m$ which is integer.

Let M be an integer matrix over \mathbb{R} . The functor $\mathbb{R}2\mathbb{Z}(M)$ yielding a matrix over \mathbb{Z} is defined by the term

(Def. 3) M .

Let n, m be natural numbers and M be an integer matrix over \mathbb{R} of dimension $n \times m$. Let us note that the functor $\mathbb{R}2\mathbb{Z}(M)$ yields a matrix over \mathbb{Z} of dimension $n \times m$. Let n be a natural number and M be an integer square matrix over \mathbb{R} of dimension n . Observe that the functor $\mathbb{R}2\mathbb{Z}(M)$ yields a square matrix over \mathbb{Z} of dimension n . Let n, m be natural numbers. The functor $0_n^{m \times m}$ yielding a matrix over $\mathbb{Z}^{\mathbb{R}}$ of dimension $n \times m$ is defined by the term

(Def. 4) $n \mapsto (m \mapsto 0_{\mathbb{Z}^{\mathbb{R}}})$.

2. SEQUENCES AND MATRICES CONCERNING LINEAR TRANSFORMATIONS

In the sequel k, t, i, j, m, n denote natural numbers, D denotes a non empty set, V denotes a free \mathbb{Z} -module, a denotes an element of $\mathbb{Z}^{\mathbb{R}}$, W denotes an element of V , K_1, K_2, K_3 denote linear combinations of V , and X denotes a subset of V .

Now we state the propositions:

- (8) Suppose X is linearly independent and the support of $K_1 \subseteq X$ and the support of $K_2 \subseteq X$ and the support of $K_3 \subseteq X$ and $\sum K_1 = \sum K_2 + \sum K_3$. Then $K_1 = K_2 + K_3$.
- (9) Suppose X is linearly independent and the support of $K_1 \subseteq X$ and the support of $K_2 \subseteq X$ and $a \neq 0_{\mathbb{Z}^{\mathbb{R}}}$ and $\sum K_1 = a \cdot \sum K_2$. Then $K_1 = a \cdot K_2$.

From now on V denotes a finite rank, free \mathbb{Z} -module, W denotes an element of V , K_1, K_2, K_3 denote linear combinations of V , and X denotes a subset of V .

Now we state the proposition:

- (10) Let us consider a basis b_2 of V . Then there exists a linear combination K of V such that
 - (i) $W = \sum K$, and
 - (ii) the support of $K \subseteq b_2$.

Let V be a finite rank, free \mathbb{Z} -module.

An ordered basis of V is a finite sequence of elements of V and is defined by

(Def. 5) it is one-to-one and $rng\ it$ is a basis of V .

From now on s denotes a finite sequence, V_1, V_2, V_3 denote finite rank, free \mathbb{Z} -modules, f, f_1, f_2 denote functions from V_1 into V_2 , g denotes a function from V_2 into V_3 , b_1 denotes an ordered basis of V_1 , b_2 denotes an ordered basis of V_2 , b_3 denotes an ordered basis of V_3 , v_1, v_2 denote vectors of V_2 , v, w denote elements of V_1 , p_2, F denote finite sequences of elements of V_1 , p_1, d denote finite sequences of elements of \mathbb{Z}^R , and K denotes a linear combination of V_1 .

Now we state the propositions:

- (11) Let us consider an element a of V_1 , a finite sequence F of elements of V_1 , and a finite sequence G of elements of \mathbb{Z}^R . Suppose $\text{len } F = \text{len } G$ and for every k and for every element v of \mathbb{Z}^R such that $k \in \text{dom } F$ and $v = G(k)$ holds $F(k) = v \cdot a$. Then $\sum F = \sum G \cdot a$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence H of elements of V_1 for every finite sequence I of elements of \mathbb{Z}^R such that $\text{len } H = \text{len } I$ and $\text{len } H = \$_1$ and for every k and for every element v of \mathbb{Z}^R such that $k \in \text{dom } H$ and $v = I(k)$ holds $H(k) = v \cdot a$ holds $\sum H = \sum I \cdot a$. For every n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [5, (18)], [3, (12)], [5, (17)], [32, (30)]. $\mathcal{P}[0]$ by [35, (43)], [21, (14)]. For every n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

- (12) Let us consider an element a of V_1 , a finite sequence F of elements of \mathbb{Z}^R , and a finite sequence G of elements of V_1 . Suppose $\text{len } F = \text{len } G$ and for every k such that $k \in \text{dom } F$ holds $G(k) = F_k \cdot a$. Then $\sum G = \sum F \cdot a$. The theorem is a consequence of (11).

Let us consider V_1, p_1 , and p_2 . The functor $\text{lmlt}(p_1, p_2)$ yielding a finite sequence of elements of V_1 is defined by the term

(Def. 6) (the left multiplication of V_1) $^\circ(p_1, p_2)$.

Now we state the propositions:

- (13) If $\text{dom } p_1 = \text{dom } p_2$, then $\text{dom lmlt}(p_1, p_2) = \text{dom } p_1$.
- (14) Let us consider a matrix M over the carrier of V_1 . If $\text{len } M = 0$, then $\sum \sum M = 0_{V_1}$.
- (15) Let us consider a matrix M over the carrier of V_1 of dimension $m + 1 \times 0$. Then $\sum \sum M = 0_{V_1}$.

PROOF: For every k such that $k \in \text{dom } \sum M$ holds $(\sum M)_k = 0_{V_1}$ by [32, (29)], [20, (2)], [35, (43)]. \square

- (16) Let us consider \mathbb{Z} -modules V_1, V_2 , a function f from V_1 into V_2 , and a finite sequence p of elements of V_1 . If f is additive and homogeneous, then $f(\sum p) = \sum(f \cdot p)$.

PROOF: Define $\mathcal{P}[\text{finite sequence of elements of } V_1] \equiv f(\sum \$_1) = \sum(f \cdot \$_1)$. For every finite sequence p of elements of V_1 and for every element w of V_1 such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \hat{\ } \langle w \rangle]$ by [35, (41), (44)], [7, (8)]. For every finite sequence p of elements of V_1 , $\mathcal{P}[p]$ from [8, Sch. 2]. \square

- (17) Let us consider a finite sequence a of elements of \mathbb{Z}^R , and a finite sequence p of elements of V_1 . Suppose $\text{len } p = \text{len } a$. If f is additive and homogeneous, then $f \cdot \text{lmlt}(a, p) = \text{lmlt}(a, f \cdot p)$. The theorem is a consequence of (13).
- (18) Let us consider a finite sequence a of elements of \mathbb{Z}^R . Suppose $\text{len } a = \text{len } b_2$ and g is additive and homogeneous. Then $g(\sum \text{lmlt}(a, b_2)) = \sum \text{lmlt}(a, g \cdot b_2)$. The theorem is a consequence of (16) and (17).
- (19) Let us consider finite sequences F, F_1 of elements of V_1 , a linear combination K of V_1 , and a permutation p of $\text{dom } F$. If $F_1 = F \cdot p$, then $K \cdot F_1 = (K \cdot F) \cdot p$.
- (20) If F is one-to-one and the support of $K \subseteq \text{rng } F$, then $\sum(K \cdot F) = \sum K$.
 PROOF: Reconsider $A = \text{the support of } K \text{ as a subset of } \text{rng } F$. Consider p_1 being a permutation of $\text{dom } F$ such that $(F - A^c) \wedge (F - A) = F \cdot p_1$. Reconsider $G_1 = F - A^c, G_2 = F - A$ as a finite sequence of elements of V_1 . For every k such that $k \in \text{dom}(K \cdot G_2)$ holds $(K \cdot G_2)_k = 0_{V_1}$ by [32, (29), (65)], [15, (1)]. $K \cdot (G_1 \wedge G_2) = (K \cdot F) \cdot p_1$. \square
- (21) Let us consider a set A , and a finite sequence p of elements of V_1 . Suppose $\text{rng } p \subseteq A$. Suppose f_1 is additive and homogeneous and f_2 is additive and homogeneous and for every v such that $v \in A$ holds $f_1(v) = f_2(v)$. Then $f_1(\sum p) = f_2(\sum p)$.
 PROOF: Define \mathcal{P} [finite sequence of elements of V_1] \equiv if $\text{rng } \$1 \subseteq A$, then $f_1(\sum \$1) = f_2(\sum \$1)$. For every finite sequence p of elements of V_1 and for every element x of V_1 such that $\mathcal{P}[p]$ holds $\mathcal{P}[p \wedge \langle x \rangle]$ by [5, (31), (39)], [35, (41), (44)]. $\mathcal{P}[\varepsilon_\alpha]$, where α is the carrier of V_1 by [35, (43)], [15, (1)]. For every finite sequence p of elements of V_1 , $\mathcal{P}[p]$ from [8, Sch. 2]. \square
- (22) Suppose f_1 is additive and homogeneous and f_2 is additive and homogeneous. Let us consider an ordered basis b_1 of V_1 . Suppose $\text{len } b_1 > 0$. If $f_1 \cdot b_1 = f_2 \cdot b_1$, then $f_1 = f_2$. The theorem is a consequence of (20) and (21).
- (23) Let us consider a matrix M_1 over the carrier of V of dimension $n \times k$, and a matrix M_2 over the carrier of V of dimension $m \times k$. Then $\sum(M_1 \wedge M_2) = \sum M_1 \wedge \sum M_2$.
- (24) Let us consider matrices M_1, M_2 over the carrier of V_1 . Then $\sum M_1 + \sum M_2 = \sum(M_1 \wedge M_2)$.
- (25) Let us consider finite sequences P_1, P_2 of elements of V_1 . Suppose $\text{len } P_1 = \text{len } P_2$. Then $\sum(P_1 + P_2) = \sum P_1 + \sum P_2$.
- (26) Let us consider matrices M_1, M_2 over the carrier of V_1 . Suppose $\text{len } M_1 = \text{len } M_2$. Then $\sum \sum M_1 + \sum \sum M_2 = \sum \sum(M_1 \wedge M_2)$. The theorem is a consequence of (25) and (24).

(27) Let us consider a matrix M over the carrier of V_1 . Then $\sum \sum M = \sum \sum M^T$.

PROOF: Define $\mathcal{X}[\text{natural number}] \equiv$ for every matrix M over the carrier of V_1 such that $\text{len } M = \$_1$ holds $\sum \sum M = \sum \sum M^T$. For every finite sequence P of elements of V_1 , $\sum \sum \langle P \rangle = \sum \sum \langle P \rangle^T$ by [5, (38), (6), (39)]. For every n such that $\mathcal{X}[n]$ holds $\mathcal{X}[n+1]$ by [5, (4), (40)], [24, (3), (2), (1)]. $\mathcal{X}[0]$. For every n , $\mathcal{X}[n]$ from [3, Sch. 2]. \square

(28) Let us consider a matrix M over \mathbb{Z}^R of dimension $n \times m$. Suppose $n > 0$ and $m > 0$. Let us consider finite sequences p, d of elements of \mathbb{Z}^R . Suppose $\text{len } p = n$ and $\text{len } d = m$ and for every j such that $j \in \text{dom } d$ holds $d_j = \sum (p \bullet M_{\square, j})$. Let us consider finite sequences b, c of elements of V_1 . Suppose $\text{len } b = m$ and $\text{len } c = n$ and for every i such that $i \in \text{dom } c$ holds $c_i = \sum \text{lmlt}(\text{Line}(M, i), b)$. Then $\sum \text{lmlt}(p, c) = \sum \text{lmlt}(d, b)$.

PROOF: Reconsider $n_1 = n$, $m_1 = m$ as an element of \mathbb{N} . Define $\mathcal{V}(\text{natural number, natural number}) = p_{\$_1} \cdot M_{\$_1, \$_2} \cdot b_{\$_2}$. Consider M_1 being a matrix over the carrier of V_1 of dimension $n_1 \times m_1$ such that for every i and j such that $\langle i, j \rangle \in$ the indices of M_1 holds $M_{1i, j} = \mathcal{V}(i, j)$. $\text{dom lmlt}(d, b) = \text{dom } b$. $\text{dom lmlt}(p, c) = \text{dom } p$. \square

3. DECOMPOSITION OF A VECTOR IN BASIS

Let V be a finite rank, free \mathbb{Z} -module, b_1 be an ordered basis of V , and W be an element of V . The functor $W \rightarrow b_1$ yielding a finite sequence of elements of \mathbb{Z}^R is defined by

(Def. 7) $\text{len } it = \text{len } b_1$ and there exists a linear combination K of V such that $W = \sum K$ and the support of $K \subseteq \text{rng } b_1$ and for every k such that $1 \leq k \leq \text{len } it$ holds $it_k = K(b_{1k})$.

Now we state the propositions:

(29) If $v_1 \rightarrow b_2 = v_2 \rightarrow b_2$, then $v_1 = v_2$.

(30) $v = \sum \text{lmlt}(v \rightarrow b_1, b_1)$. The theorem is a consequence of (13) and (20).

(31) If $\text{len } d = \text{len } b_1$, then $d = \sum \text{lmlt}(d, b_1) \rightarrow b_1$.

PROOF: Define $\mathcal{X}[\text{element of } V_1, \text{element of } \mathbb{Z}^R] \equiv$ if $\$1 \in \text{rng } b_1$, then for every k such that $k \in \text{dom } b_1$ and $b_{1k} = \$1$ holds $\$2 = d_k$ and if $\$1 \notin \text{rng } b_1$, then $\$2 = 0_{\mathbb{Z}^R}$. For every v , there exists an element u of \mathbb{Z}^R such that $\mathcal{X}[v, u]$ by [20, (2)]. Consider K being a function from V_1 into the carrier of \mathbb{Z}^R such that for every v , $\mathcal{X}[v, K(v)]$ from [10, Sch. 3]. \square

(32) Let us consider finite sequences a, d of elements of \mathbb{Z}^R . Suppose $\text{len } a = \text{len } b_1$. Let us consider a natural number j . Suppose $j \in \text{dom } b_2$ and $\text{len } d =$

len b_1 and for every k such that $k \in \text{dom } b_1$ holds $d(k) = (f(b_{1k}) \rightarrow b_2)_j$. If len $b_1 > 0$, then $(\sum \text{lmlt}(a, f \cdot b_1) \rightarrow b_2)_j = \sum(a \bullet d)$.

PROOF: Reconsider $B_3 = f \cdot b_1$ as a finite sequence of elements of V_2 . Define $\mathcal{V}(\text{natural number, natural number}) = (B_{3\$1} \rightarrow b_2)_{\$2}$. Consider M being a matrix over \mathbb{Z}^R of dimension len $b_1 \times$ len b_2 such that for every i and j such that $\langle i, j \rangle \in$ the indices of M holds $M_{i,j} = \mathcal{V}(i, j)$. Define $\mathcal{W}(\text{natural number}) = \sum(a \bullet M_{\square, \$1})$. Consider d_1 being a finite sequence of elements of \mathbb{Z}^R such that len $d_1 =$ len b_2 and for every natural number j such that $j \in \text{dom } d_1$ holds $d_{1j} = \mathcal{W}(j)$ from [33, Sch. 2]. \square

4. MATRICES OF LINEAR TRANSFORMATIONS

Let V_1, V_2 be finite rank, free \mathbb{Z} -modules, f be a function from V_1 into V_2 , b_1 be a finite sequence of elements of V_1 , and b_2 be an ordered basis of V_2 . The functor $\text{AutMt}(f, b_1, b_2)$ yielding a matrix over \mathbb{Z}^R is defined by

(Def. 8) len $it =$ len b_1 and for every k such that $k \in \text{dom } b_1$ holds $it_k = f(b_{1k}) \rightarrow b_2$.

Now we state the propositions:

(33) If len $b_1 = 0$, then $\text{AutMt}(f, b_1, b_2) = \emptyset$.

(34) If len $b_1 > 0$, then width $\text{AutMt}(f, b_1, b_2) =$ len b_2 .

(35) Suppose f_1 is additive and homogeneous and f_2 is additive and homogeneous and $\text{AutMt}(f_1, b_1, b_2) = \text{AutMt}(f_2, b_1, b_2)$ and len $b_1 > 0$. Then $f_1 = f_2$. The theorem is a consequence of (29) and (22).

(36) Let us consider a finite sequence F of elements of \mathbb{R}_F , and a finite sequence G of elements of \mathbb{Z}^R . If $F = G$, then $\sum F = \sum G$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence F of elements of \mathbb{R}_F for every finite sequence G of elements of \mathbb{Z}^R such that len $F = \$1$ and $F = G$ holds $\sum F = \sum G$. $\mathcal{P}[0]$ by [35, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [5, (4)], [9, (3)], [5, (59)], [3, (11)]. For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

(37) Let us consider finite sequences p, q of elements of \mathbb{Z}^R , and finite sequences p_1, q_1 of elements of \mathbb{R}_F . If $p = p_1$ and $q = q_1$, then $p \cdot q = p_1 \cdot q_1$. The theorem is a consequence of (36).

(38) Suppose g is additive and homogeneous and len $b_1 > 0$ and len $b_2 > 0$. Then $\text{AutMt}(g \cdot f, b_1, b_3) = \text{AutMt}(f, b_1, b_2) \cdot \text{AutMt}(g, b_2, b_3)$.

PROOF: width $\text{AutMt}(f, b_1, b_2) =$ len b_2 . width $\text{AutMt}(g \cdot f, b_1, b_3) =$ len b_3 . For every i and j such that $\langle i, j \rangle \in$ the indices of $\text{AutMt}(g \cdot f, b_1, b_3)$ holds $(\text{AutMt}(g \cdot f, b_1, b_3))_{i,j} = (\text{AutMt}(f, b_1, b_2) \cdot \text{AutMt}(g, b_2, b_3))_{i,j}$ by [12, (87)], [32, (29)], (34), [32, (25)]. \square

$$(39) \quad \text{AutMt}(f_1 + f_2, b_1, b_2) = \text{AutMt}(f_1, b_1, b_2) + \text{AutMt}(f_2, b_1, b_2).$$

PROOF: $\text{width AutMt}(f_1, b_1, b_2) = \text{width AutMt}(f_2, b_1, b_2)$. $\text{width AutMt}(f_1 + f_2, b_1, b_2) = \text{width AutMt}(f_1, b_1, b_2)$. For every i and j such that $\langle i, j \rangle \in$ the indices of $\text{AutMt}(f_1 + f_2, b_1, b_2)$ holds $(\text{AutMt}(f_1 + f_2, b_1, b_2))_{i,j} = (\text{AutMt}(f_1, b_1, b_2) + \text{AutMt}(f_2, b_1, b_2))_{i,j}$ by [32, (29)], [12, (87)], (8), [36, (22)]. \square

$$(40) \quad \text{If } a \neq 0_{\mathbb{Z}_R}, \text{ then } \text{AutMt}(a \cdot f, b_1, b_2) = a \cdot \text{AutMt}(f, b_1, b_2).$$

PROOF: $\text{width AutMt}(a \cdot f, b_1, b_2) = \text{width AutMt}(f, b_1, b_2)$. For every i and j such that $\langle i, j \rangle \in$ the indices of $\text{AutMt}(a \cdot f, b_1, b_2)$ holds $(\text{AutMt}(a \cdot f, b_1, b_2))_{i,j} = (a \cdot \text{AutMt}(f, b_1, b_2))_{i,j}$ by [32, (29)], [12, (87)], (9), [5, (1)]. \square

(41) Let us consider non empty sets D, E , natural numbers n, m, i, j , and a matrix M over D of dimension $n \times m$. Suppose $0 < n$ and M is a matrix over E of dimension $n \times m$ and $\langle i, j \rangle \in$ the indices of M . Then $M_{i,j}$ is an element of E .

(42) Let us consider a finite sequence F of elements of \mathbb{R}_F . Suppose for every natural number i such that $i \in \text{dom } F$ holds $F(i) \in \mathbb{Z}$. Then $\sum F \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite sequence F of elements of \mathbb{R}_F such that $\text{len } F = \$_1$ and for every natural number i such that $i \in \text{dom } F$ holds $F(i) \in \mathbb{Z}$ holds $\sum F \in \mathbb{Z}$. $\mathcal{P}[0]$ by [35, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [5, (4)], [9, (3)], [5, (59)], [3, (11)]. For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

(43) Let us consider a natural number i , and an element j of \mathbb{R}_F . Suppose $j \in \mathbb{Z}$. Then $\text{power}_{\mathbb{R}_F}(-\mathbf{1}_{\mathbb{R}_F}, i) \cdot j \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv \text{power}_{\mathbb{R}_F}(-\mathbf{1}_{\mathbb{R}_F}, \$_1) \cdot j \in \mathbb{Z}$. $\mathcal{P}[0]$. 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]. \square

(44) Let us consider natural numbers n, i, j, k, m , and a square matrix M over \mathbb{R}_F of dimension $n + 1$. Suppose $0 < n$ and M is a square matrix over \mathbb{Z} of dimension $n + 1$ and $\langle i, j \rangle \in$ the indices of M and $\langle k, m \rangle \in$ the indices of $\text{Delete}(M, i, j)$. Then $(\text{Delete}(M, i, j))_{k,m}$ is an element of \mathbb{Z} . The theorem is a consequence of (41).

(45) Let us consider natural numbers n, i, j , and a square matrix M over \mathbb{R}_F of dimension $n + 1$. Suppose $0 < n$ and M is a square matrix over \mathbb{Z} of dimension $n + 1$ and $\langle i, j \rangle \in$ the indices of M . Then $\text{Delete}(M, i, j)$ is a square matrix over \mathbb{Z} of dimension n .

PROOF: Set $M_0 = \text{Delete}(M, i, j)$. For every object x such that $x \in \text{rng } M_0$ there exists a finite sequence p of elements of \mathbb{Z} such that $x = p$ and $\text{len } p = n$ by [12, (87)], (44). \square

Let us consider a natural number n and a square matrix M over \mathbb{R}_F of dimension n . Now we state the propositions:

(46) If M is a square matrix over \mathbb{Z} of dimension n , then $\text{Det } M \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every square matrix M over \mathbb{R}_F of dimension n such that M is a square matrix over \mathbb{Z} of dimension n , $\mathcal{P}[n]$ holds $\text{Det } M \in \mathbb{Z}$. $\mathcal{P}[0]$ by [29, (41)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n + 1]$ by [3, (14)], [5, (1)], [27, (27)], [12, (87)]. For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

(47) If M is a square matrix over \mathbb{Z}^R of dimension n , then $\text{Det } M \in \mathbb{Z}$.

Now we state the proposition:

(48) Let us consider a finite rank, free \mathbb{Z} -module V , and a basis I of V . Then there exists an ordered basis J of V such that $\text{rng } J = I$.

Let V be a \mathbb{Z} -module. One can check that id_V is additive and homogeneous.

Now we state the propositions:

(49) Let us consider a finite rank, free \mathbb{Z} -module V , and an ordered basis b of V . Then $\text{len } b = \text{rank } V$.

(50) Let us consider a finite rank, free \mathbb{Z} -module V , and ordered bases b_1, b_2 of V . Then $\text{AutMt}(\text{id}_V, b_1, b_2)$ is a square matrix over \mathbb{Z}^R of dimension $\text{rank } V$. The theorem is a consequence of (49) and (34).

(51) Let us consider a finite rank, free \mathbb{Z} -module V , ordered bases b_1, b_2 of V , and a square matrix M over \mathbb{R}_F of dimension $\text{rank } V$. Suppose $M = \text{AutMt}(\text{id}_V, b_1, b_2)$. Then $\text{Det } M \in \mathbb{Z}$. The theorem is a consequence of (46).

(52) Let us consider a finite rank, free \mathbb{Z} -module V_1 , an ordered basis b_1 of V_1 , and natural numbers i, j . Suppose $i, j \in \text{dom } b_1$. Then

(i) if $i = j$, then $(b_{1i} \rightarrow b_1)(j) = 1$, and

(ii) if $i \neq j$, then $(b_{1i} \rightarrow b_1)(j) = 0$.

(53) Let us consider a finite rank, free \mathbb{Z} -module V , and an ordered basis b_1 of V . Suppose $\text{rank } V > 0$. Then $\text{AutMt}(\text{id}_V, b_1, b_1) = I_{\mathbb{Z}^R}^{(\text{rank } V) \times (\text{rank } V)}$. The theorem is a consequence of (49), (34), (52), and (4).

(54) Let us consider a finite rank, free \mathbb{Z} -module V , and ordered bases b_1, b_2 of V . Suppose $\text{rank } V > 0$. Then $\text{AutMt}(\text{id}_V, b_1, b_2) \cdot \text{AutMt}(\text{id}_V, b_2, b_1) = I_{\mathbb{Z}^R}^{(\text{rank } V) \times (\text{rank } V)}$. The theorem is a consequence of (49), (38), and (53).

(55) Let us consider a finite rank, free \mathbb{Z} -module V , ordered bases b_1, b_2 of V , and a square matrix M over \mathbb{Z}^R of dimension $\text{rank } V$. Suppose $M = \text{AutMt}(\text{id}_V, b_1, b_2)$. Then $|\text{Det } M| = 1$. The theorem is a consequence of (49), (34), and (54).

5. REAL-VALUED FUNCTION OF \mathbb{Z} -MODULE

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$. Observe that there exists a functional in V which is additive, homogeneous, and 0-preserving.

A linear functional in V is an additive, homogeneous functional in V . Now we state the proposition:

(56) Let us consider an element a of $\mathbb{Z}^{\mathbb{R}}$, an add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, and a vector v of V . Then

- (i) $0_{\mathbb{Z}^{\mathbb{R}}} \cdot v = 0_V$, and
- (ii) $a \cdot 0_V = 0_V$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$. Note that there exists a functional in V which is additive and 0-preserving.

Let V be a right zeroed, non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$. Let us note that every functional in V which is additive is also 0-preserving.

Let V be an add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$. Note that every functional in V which is homogeneous is also 0-preserving.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$. Let us observe that 0Functional V is constant and there exists a functional in V which is constant.

Let V be a right zeroed, non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$ and f be a 0-preserving functional in V . Let us note that f is constant if and only if the condition (Def. 9) is satisfied.

(Def. 9) $f = 0\text{Functional } V$.

Let us note that there exists a functional in V which is constant, additive, and 0-preserving.

Let V be a free \mathbb{Z} -module and A, B be subsets of V . Assume $A \subseteq B$ and B is a basis of V . The functor $\text{Proj}(A, B)$ yielding a linear transformation from V to V is defined by

(Def. 10) for every vector v of V , there exist vectors v_6, v_7 of V such that $v_6 \in \text{Lin}(A)$ and $v_7 \in \text{Lin}(B \setminus A)$ and $v = v_6 + v_7$ and $it(v) = v_6$ and for every vectors v, v_6, v_7 of V such that $v_6 \in \text{Lin}(A)$ and $v_7 \in \text{Lin}(B \setminus A)$ and $v = v_6 + v_7$ holds $it(v) = v_6$.

Let B be a basis of V and u be a vector of V . The functor $\text{Coordinate}(u, B)$ yielding a function from V into $\mathbb{Z}^{\mathbb{R}}$ is defined by

(Def. 11) for every vector v of V , there exists a linear combination L_2 of B such that $v = \sum L_2$ and $it(v) = L_2(u)$ and for every vector v of V and for every

linear combination L_3 of B such that $v = \sum L_3$ holds $it(v) = L_3(u)$ and for every vectors v_1, v_2 of V , $it(v_1 + v_2) = it(v_1) + it(v_2)$ and for every vector v of V and for every element r of \mathbb{Z}^R , $it(r \cdot v) = r \cdot it(v)$.

Now we state the propositions:

- (57) Let us consider a free \mathbb{Z} -module V , a basis B of V , and a vector u of V . Then $(\text{Coordinate}(u, B))(0_V) = 0$.
- (58) Let us consider a free \mathbb{Z} -module V , a basis X of V , and a vector v of V . If $v \in X$ and $v \neq 0_V$, then $(\text{Coordinate}(v, X))(v) = 1$.

Let V be a non trivial, free \mathbb{Z} -module. One can verify that there exists a functional in V which is additive, homogeneous, non constant, and non trivial.

Now we state the proposition:

- (59) Let us consider a non trivial, free \mathbb{Z} -module V , and a non constant, 0-preserving functional f in V . Then there exists a vector v of V such that
- (i) $v \neq 0_V$, and
 - (ii) $f(v) \neq 0_{\mathbb{Z}^R}$.

6. BILINEAR FORM OF \mathbb{Z} -MODULE

Let V, W be vector space structures over \mathbb{Z}^R . The functor $\text{NulForm}(V, W)$ yielding a form of V, W is defined by the term

(Def. 12) $(\text{the carrier of } V) \times (\text{the carrier of } W) \mapsto 0_{\mathbb{Z}^R}$.

Let V, W be non empty vector space structures over \mathbb{Z}^R and f, g be forms of V, W . The functor $f + g$ yielding a form of V, W is defined by

(Def. 13) for every vector v of V and for every vector w of W , $it(v, w) = f(v, w) + g(v, w)$.

Let f be a form of V, W and a be an element of \mathbb{Z}^R . The functor $a \cdot f$ yielding a form of V, W is defined by

(Def. 14) for every vector v of V and for every vector w of W , $it(v, w) = a \cdot f(v, w)$.

The functor $-f$ yielding a form of V, W is defined by

(Def. 15) for every vector v of V and for every vector w of W , $it(v, w) = -f(v, w)$.

Note that the functor $-f$ is defined by the term

(Def. 16) $(-1_{\mathbb{Z}^R}) \cdot f$.

Let f, g be forms of V, W . The functor $f - g$ yielding a form of V, W is defined by the term

(Def. 17) $f + -g$.

One can verify that the functor $f - g$ is defined by

(Def. 18) for every vector v of V and for every vector w of W , $it(v, w) = f(v, w) - g(v, w)$.

Let us observe that the functor $f + g$ is commutative.

Now we state the propositions:

(60) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a form f of V, W . Then $f + \text{NulForm}(V, W) = f$.

(61) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and forms f, g, h of V, W . Then $(f + g) + h = f + (g + h)$.

(62) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a form f of V, W . Then $f - f = \text{NulForm}(V, W)$.

(63) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an element a of $\mathbb{Z}^{\mathbb{R}}$, and forms f, g of V, W . Then $a \cdot (f + g) = a \cdot f + a \cdot g$.

Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, elements a, b of $\mathbb{Z}^{\mathbb{R}}$, and a form f of V, W . Now we state the propositions:

(64) $(a + b) \cdot f = a \cdot f + b \cdot f$.

(65) $(a \cdot b) \cdot f = a \cdot (b \cdot f)$.

Now we state the proposition:

(66) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a form f of V, W . Then $1_{\mathbb{Z}^{\mathbb{R}}} \cdot f = f$.

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathbb{R}}$, f be a form of V, W , and v be a vector of V . The functor $f(v, \cdot)$ yielding a functional in W is defined by the term

(Def. 19) $(\text{curry } f)(v)$.

Let w be a vector of W . The functor $f(\cdot, w)$ yielding a functional in V is defined by the term

(Def. 20) $(\text{curry}' f)(w)$.

Now we state the propositions:

(67) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a form f of V, W , and a vector v of V . Then

(i) $\text{dom } f(v, \cdot) = \text{the carrier of } W$, and

(ii) $\text{rng } f(v, \cdot) \subseteq \text{the carrier of } \mathbb{Z}^{\mathbb{R}}$, and

(iii) for every vector w of W , $(f(v, \cdot))(w) = f(v, w)$.

(68) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a form f of V, W , and a vector w of W . Then

(i) $\text{dom } f(\cdot, w) = \text{the carrier of } V$, and

- (ii) $\text{rng } f(\cdot, w) \subseteq \text{the carrier of } \mathbb{Z}^{\mathbb{R}}$, and
- (iii) for every vector v of V , $(f(\cdot, w))(v) = f(v, w)$.

- (69) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a vector v of V . Then $\text{NulForm}(V, W)(v, \cdot) = 0\text{Functional } W$. The theorem is a consequence of (67).
- (70) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a vector w of W . Then $\text{NulForm}(V, W)(\cdot, w) = 0\text{Functional } V$. The theorem is a consequence of (68).
- (71) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, forms f, g of V, W , and a vector w of W . Then $(f + g)(\cdot, w) = f(\cdot, w) + g(\cdot, w)$. The theorem is a consequence of (68).
- (72) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, forms f, g of V, W , and a vector v of V . Then $(f + g)(v, \cdot) = f(v, \cdot) + g(v, \cdot)$. The theorem is a consequence of (67).
- (73) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a form f of V, W , an element a of $\mathbb{Z}^{\mathbb{R}}$, and a vector w of W . Then $(a \cdot f)(\cdot, w) = a \cdot f(\cdot, w)$. The theorem is a consequence of (68).
- (74) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a form f of V, W , an element a of $\mathbb{Z}^{\mathbb{R}}$, and a vector v of V . Then $(a \cdot f)(v, \cdot) = a \cdot f(v, \cdot)$. The theorem is a consequence of (67).
- (75) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a form f of V, W , and a vector w of W . Then $(-f)(\cdot, w) = -f(\cdot, w)$. The theorem is a consequence of (68).
- (76) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a form f of V, W , and a vector v of V . Then $(-f)(v, \cdot) = -f(v, \cdot)$. The theorem is a consequence of (67).
- (77) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, forms f, g of V, W , and a vector w of W . Then $(f - g)(\cdot, w) = f(\cdot, w) - g(\cdot, w)$. The theorem is a consequence of (68).
- (78) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, forms f, g of V, W , and a vector v of V . Then $(f - g)(v, \cdot) = f(v, \cdot) - g(v, \cdot)$. The theorem is a consequence of (67).

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathbb{R}}$, f be a functional in V , and g be a functional in W . The functor $f \otimes g$ yielding a form of V, W is defined by

(Def. 21) for every vector v of V and for every vector w of W , $it(v, w) = f(v) \cdot g(w)$.

Now we state the propositions:

- (79) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a functional f in V , a vector v of V , and a vector w of W . Then $f \otimes (0\text{Functional } W)(v, w) = 0$.
- (80) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a functional g in W , a vector v of V , and a vector w of W . Then $(0\text{Functional } V) \otimes g(v, w) = 0$.
- (81) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a functional f in V . Then $f \otimes (0\text{Functional } W) = \text{NulForm}(V, W)$. The theorem is a consequence of (79).
- (82) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a functional g in W . Then $(0\text{Functional } V) \otimes g = \text{NulForm}(V, W)$. The theorem is a consequence of (80).
- (83) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a functional f in V , a functional g in W , and a vector v of V . Then $f \otimes g(v, \cdot) = f(v) \cdot g$. The theorem is a consequence of (67).
- (84) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a functional f in V , a functional g in W , and a vector w of W . Then $f \otimes g(\cdot, w) = g(w) \cdot f$. The theorem is a consequence of (68).

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathbb{R}}$ and f be a form of V, W . We say that f is additive w.r.t. second argument if and only if

(Def. 22) for every vector v of V , $f(v, \cdot)$ is additive.

We say that f is additive w.r.t. first argument if and only if

(Def. 23) for every vector w of W , $f(\cdot, w)$ is additive.

We say that f is homogeneous w.r.t. second argument if and only if

(Def. 24) for every vector v of V , $f(v, \cdot)$ is homogeneous.

We say that f is homogeneous w.r.t. first argument if and only if

(Def. 25) for every vector w of W , $f(\cdot, w)$ is homogeneous.

One can check that $\text{NulForm}(V, W)$ is additive w.r.t. second argument and $\text{NulForm}(V, W)$ is additive w.r.t. first argument and $\text{NulForm}(V, W)$ is homogeneous w.r.t. second argument and $\text{NulForm}(V, W)$ is homogeneous w.r.t. first argument and there exists a form of V, W which is additive w.r.t. second argument, homogeneous w.r.t. second argument, additive w.r.t. first argument, and homogeneous w.r.t. first argument.

A bilinear form of V, W is an additive w.r.t. first argument, homogeneous w.r.t. first argument, additive w.r.t. second argument, homogeneous w.r.t. second argument form of V, W . Let f be an additive w.r.t. second argument form of V, W and v be a vector of V . Note that $f(v, \cdot)$ is additive.

Let f be an additive w.r.t. first argument form of V , W and w be a vector of W . Let us observe that $f(\cdot, w)$ is additive.

Let f be a homogeneous w.r.t. second argument form of V , W and v be a vector of V . Note that $f(v, \cdot)$ is homogeneous.

Let f be a homogeneous w.r.t. first argument form of V , W and w be a vector of W . Let us observe that $f(\cdot, w)$ is homogeneous.

Let f be a functional in V and g be an additive functional in W . Let us observe that $f \otimes g$ is additive w.r.t. second argument.

Let f be an additive functional in V and g be a functional in W . Note that $f \otimes g$ is additive w.r.t. first argument.

Let f be a functional in V and g be a homogeneous functional in W . Let us observe that $f \otimes g$ is homogeneous w.r.t. second argument.

Let f be a homogeneous functional in V and g be a functional in W . Note that $f \otimes g$ is homogeneous w.r.t. first argument.

Let V be a non trivial vector space structure over $\mathbb{Z}^{\mathbb{R}}$, W be a \mathbb{Z} -module, and f be a functional in V . Note that $f \otimes g$ is non trivial.

Let W be a non trivial \mathbb{Z} -module. One can verify that $f \otimes g$ is non trivial.

Let V , W be non trivial, free \mathbb{Z} -modules, f be a non constant, 0-preserving functional in V , and g be a non constant, 0-preserving functional in W . Let us note that $f \otimes g$ is non constant and there exists a form of V , W which is non trivial, non constant, additive w.r.t. second argument, homogeneous w.r.t. second argument, additive w.r.t. first argument, and homogeneous w.r.t. first argument.

Let V , W be non empty vector space structures over $\mathbb{Z}^{\mathbb{R}}$ and f , g be additive w.r.t. first argument forms of V , W . One can check that $f + g$ is additive w.r.t. first argument.

Let f , g be additive w.r.t. second argument forms of V , W . Let us note that $f + g$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument form of V , W and a be an element of $\mathbb{Z}^{\mathbb{R}}$. One can check that $a \cdot f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument form of V , W . Observe that $a \cdot f$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument form of V , W . One can check that $-f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument form of V , W . One can check that $-f$ is additive w.r.t. second argument.

Let f , g be additive w.r.t. first argument forms of V , W . One can verify that $f - g$ is additive w.r.t. first argument.

Let f , g be additive w.r.t. second argument forms of V , W . Let us note that $f - g$ is additive w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument forms of V, W . One can verify that $f + g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument forms of V, W . Note that $f + g$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument form of V, W and a be an element of $\mathbb{Z}^{\mathbb{R}}$. One can verify that $a \cdot f$ is homogeneous w.r.t. first argument.

Let f be a homogeneous w.r.t. second argument form of V, W . Let us note that $a \cdot f$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument form of V, W . One can verify that $-f$ is homogeneous w.r.t. first argument.

Let f be a homogeneous w.r.t. second argument form of V, W . One can verify that $-f$ is homogeneous w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument forms of V, W . Let us observe that $f - g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument forms of V, W . Note that $f - g$ is homogeneous w.r.t. second argument.

Now we state the propositions:

- (85) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, vectors v, u of V , a vector w of W , and a form f of V, W . If f is additive w.r.t. first argument, then $f(v + u, w) = f(v, w) + f(u, w)$. The theorem is a consequence of (68).
- (86) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a vector v of V , vectors u, w of W , and a form f of V, W . If f is additive w.r.t. second argument, then $f(v, u + w) = f(v, u) + f(v, w)$. The theorem is a consequence of (67).
- (87) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, vectors v, u of V , vectors w, t of W , and an additive w.r.t. first argument, additive w.r.t. second argument form f of V, W . Then $f(v + u, w + t) = f(v, w) + f(v, t) + (f(u, w) + f(u, t))$. The theorem is a consequence of (85) and (86).
- (88) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an additive w.r.t. second argument form f of V, W , and a vector v of V . Then $f(v, 0_W) = 0$. The theorem is a consequence of (86).
- (89) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an additive w.r.t. first argument form f of V, W , and a vector w of W . Then $f(0_V, w) = 0$. The theorem is a consequence of (85).

Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a vector v of V , a vector w of W , an element a of $\mathbb{Z}^{\mathbb{R}}$, and a form f of V, W . Now we state the propositions:

(90) If f is homogeneous w.r.t. first argument, then $f(a \cdot v, w) = a \cdot f(v, w)$.
The theorem is a consequence of (68).

(91) If f is homogeneous w.r.t. second argument, then $f(v, a \cdot w) = a \cdot f(v, w)$.
The theorem is a consequence of (67).

Now we state the propositions:

(92) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a homogeneous w.r.t. first argument form f of V, W , and a vector w of W . Then $f(0_V, w) = 0_{\mathbb{Z}^{\mathbb{R}}}$. The theorem is a consequence of (56) and (90).

(93) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, a homogeneous w.r.t. second argument form f of V, W , and a vector v of V . Then $f(v, 0_W) = 0_{\mathbb{Z}^{\mathbb{R}}}$. The theorem is a consequence of (56) and (91).

(94) Let us consider \mathbb{Z} -modules V, W , vectors v, u of V , a vector w of W , and an additive w.r.t. first argument, homogeneous w.r.t. first argument form f of V, W . Then $f(v - u, w) = f(v, w) - f(u, w)$. The theorem is a consequence of (85) and (90).

(95) Let us consider \mathbb{Z} -modules V, W , a vector v of V , vectors w, t of W , and an additive w.r.t. second argument, homogeneous w.r.t. second argument form f of V, W . Then $f(v, w - t) = f(v, w) - f(v, t)$. The theorem is a consequence of (86) and (91).

(96) Let us consider \mathbb{Z} -modules V, W , vectors v, u of V , vectors w, t of W , and a bilinear form f of V, W . Then $f(v - u, w - t) = f(v, w) - f(v, t) - (f(u, w) - f(u, t))$. The theorem is a consequence of (94) and (95).

(97) Let us consider add-associative, right zeroed, right complementable, vector distributive, scalar distributive, scalar associative, scalar unital, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, vectors v, u of V , vectors w, t of W , elements a, b of $\mathbb{Z}^{\mathbb{R}}$, and a bilinear form f of V, W . Then $f(v + a \cdot u, w + b \cdot t) = f(v, w) + b \cdot f(v, t) + (a \cdot f(u, w) + a \cdot (b \cdot f(u, t)))$. The theorem is a consequence of (87), (91), and (90).

(98) Let us consider \mathbb{Z} -modules V, W , vectors v, u of V , vectors w, t of W , elements a, b of $\mathbb{Z}^{\mathbb{R}}$, and a bilinear form f of V, W . Then $f(v - a \cdot u, w - b \cdot t) = f(v, w) - b \cdot f(v, t) - (a \cdot f(u, w) - a \cdot (b \cdot f(u, t)))$. The theorem is a consequence of (96), (91), and (90).

(99) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a form f of V, W . Suppose f is additive w.r.t. second argument or additive w.r.t. first argument. Then f is constant if and only

if for every vector v of V and for every vector w of W , $f(v, w) = 0$. The theorem is a consequence of (88) and (89).

7. MATRIX OF BILINEAR FORM

Let V_1, V_2 be finite rank, free \mathbb{Z} -modules, b_1 be an ordered basis of V_1 , b_2 be an ordered basis of V_2 , and f be a bilinear form of V_1, V_2 . The functor $\text{Bilinear}(f, b_1, b_2)$ yielding a matrix over $\mathbb{Z}^{\mathbb{R}}$ of dimension $\text{len } b_1 \times \text{len } b_2$ is defined by

(Def. 26) for every natural numbers i, j such that $i \in \text{dom } b_1$ and $j \in \text{dom } b_2$ holds $it_{i,j} = f(b_{1i}, b_{2j})$.

Now we state the propositions:

(100) Let us consider a finite rank, free \mathbb{Z} -module V , a natural number i , an element a_1 of $\mathbb{Z}^{\mathbb{R}}$, an element a_2 of V , a finite sequence p_1 of elements of $\mathbb{Z}^{\mathbb{R}}$, and a finite sequence p_2 of elements of V . Suppose $i \in \text{dom } \text{lmlt}(p_1, p_2)$ and $a_1 = p_1(i)$ and $a_2 = p_2(i)$. Then $(\text{lmlt}(p_1, p_2))(i) = a_1 \cdot a_2$.

(101) Let us consider a finite rank, free \mathbb{Z} -module V , a linear functional F in V , a finite sequence y of elements of V , a finite sequence x of elements of $\mathbb{Z}^{\mathbb{R}}$, and finite sequences X, Y of elements of $\mathbb{Z}^{\mathbb{R}}$. Suppose $X = x$ and $\text{len } y = \text{len } x$ and $\text{len } X = \text{len } Y$ and for every natural number k such that $k \in \text{Seg } \text{len } x$ holds $Y(k) = F(y_k)$. Then $X \cdot Y = F(\sum \text{lmlt}(x, y))$.

PROOF: Define \mathcal{P} [finite sequence of elements of V] \equiv for every finite sequence x of elements of $\mathbb{Z}^{\mathbb{R}}$ for every finite sequences X, Y of elements of $\mathbb{Z}^{\mathbb{R}}$ such that $X = x$ and $\text{len } \$_1 = \text{len } x$ and $\text{len } X = \text{len } Y$ and for every natural number k such that $k \in \text{Seg } \text{len } x$ holds $Y(k) = F(\$_{1k})$ holds $X \cdot Y = F(\sum \text{lmlt}(x, \$_1))$. For every finite sequence y of elements of V and for every element w of V such that $\mathcal{P}[y]$ holds $\mathcal{P}[y \wedge \langle w \rangle]$ by [5, (22), (39), (59)], [3, (11)]. $\mathcal{P}[\varepsilon_\alpha]$, where α is the carrier of V by [35, (43)]. For every finite sequence p of elements of V , $\mathcal{P}[p]$ from [8, Sch. 2]. \square

(102) Let us consider finite rank, free \mathbb{Z} -modules V_1, V_2 , an ordered basis b_2 of V_2 , an ordered basis b_3 of V_2 , a bilinear form f of V_1, V_2 , a vector v_1 of V_1 , a vector v_2 of V_2 , and finite sequences X, Y of elements of $\mathbb{Z}^{\mathbb{R}}$. Suppose $\text{len } X = \text{len } b_2$ and $\text{len } Y = \text{len } b_2$ and for every natural number k such that $k \in \text{Seg } \text{len } b_2$ holds $Y(k) = f(v_1, b_{2k})$ and $X = v_2 \rightarrow b_2$. Then $Y \cdot X = f(v_1, v_2)$. The theorem is a consequence of (67), (101), and (30).

(103) Let us consider finite rank, free \mathbb{Z} -modules V_1, V_2 , an ordered basis b_1 of V_1 , a bilinear form f of V_1, V_2 , a vector v_1 of V_1 , a vector v_2 of V_2 , and finite sequences X, Y of elements of $\mathbb{Z}^{\mathbb{R}}$. Suppose $\text{len } X = \text{len } b_1$ and $\text{len } Y = \text{len } b_1$ and for every natural number k such that $k \in \text{Seg } \text{len } b_1$

holds $Y(k) = f(b_{1k}, v_2)$ and $X = v_1 \rightarrow b_1$. Then $X \cdot Y = f(v_1, v_2)$. The theorem is a consequence of (68), (101), and (30).

- (104) Let us consider finite rank, free \mathbb{Z} -modules V_1, V_2 , an ordered basis b_1 of V_1 , an ordered basis b_2 of V_2 , an ordered basis b_3 of V_2 , and a bilinear form f of V_1, V_2 . Suppose $0 < \text{rank } V_1$. Then $\text{Bilinear}(f, b_1, b_3) = \text{Bilinear}(f, b_1, b_2) \cdot (\text{AutMt}(\text{id}_{V_2}, b_3, b_2))^T$.

PROOF: Set $n = \text{len } b_2$. $\text{len } b_2 = \text{rank } V_2$. $\text{len } b_3 = \text{rank } V_2$. Reconsider $I_1 = \text{AutMt}(\text{id}_{V_2}, b_3, b_2)$ as a square matrix over \mathbb{Z}^R of dimension n . Reconsider $M_1 = I_1^T$ as a square matrix over \mathbb{Z}^R of dimension n . Set $M_2 = \text{Bilinear}(f, b_1, b_2) \cdot M_1$. $0 < \text{len } b_1$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\text{Bilinear}(f, b_1, b_3)$ holds $(\text{Bilinear}(f, b_1, b_3))_{i,j} = M_{2i,j}$ by [12, (87)], [5, (1)], (102). \square

- (105) Let us consider finite rank, free \mathbb{Z} -modules V_1, V_2 , an ordered basis b_1 of V_1 , an ordered basis b_2 of V_2 , an ordered basis b_3 of V_1 , and a bilinear form f of V_1, V_2 . Suppose $0 < \text{rank } V_1$. Then $\text{Bilinear}(f, b_3, b_2) = \text{AutMt}(\text{id}_{V_1}, b_3, b_1) \cdot \text{Bilinear}(f, b_1, b_2)$.

PROOF: Set $n = \text{len } b_3$. $\text{len } b_1 = \text{rank } V_1$. $\text{len } b_3 = \text{rank } V_1$. Reconsider $I_1 = \text{AutMt}(\text{id}_{V_1}, b_3, b_1)$ as a square matrix over \mathbb{Z}^R of dimension n . Reconsider $M_1 = I_1$ as a square matrix over \mathbb{Z}^R of dimension n . Set $M_2 = M_1 \cdot \text{Bilinear}(f, b_1, b_2)$. $0 < \text{len } b_1$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\text{Bilinear}(f, b_3, b_2)$ holds $(\text{Bilinear}(f, b_3, b_2))_{i,j} = M_{2i,j}$ by [12, (87)], [5, (1)], (103). \square

Let us consider a finite rank, free \mathbb{Z} -module V , ordered bases b_1, b_2 of V , and a bilinear form f of V, V . Now we state the propositions:

- (106) Suppose $0 < \text{rank } V$. Then $\text{Bilinear}(f, b_2, b_2) = \text{AutMt}(\text{id}_V, b_2, b_1) \cdot \text{Bilinear}(f, b_1, b_1) \cdot (\text{AutMt}(\text{id}_V, b_2, b_1))^T$. The theorem is a consequence of (49), (50), (105), and (104).

- (107) $|\text{Det Bilinear}(f, b_2, b_2)| = |\text{Det Bilinear}(f, b_1, b_1)|$. The theorem is a consequence of (49), (106), (50), and (55).

REFERENCES

- [1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(2):377–382, 1990.
- [2] Grzegorz Bancerek. Curried and uncurried functions. *Formalized Mathematics*, 1(3):537–541, 1990.
- [3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(1):41–46, 1990.
- [4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(1):91–96, 1990.
- [5] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [6] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(1):175–180, 1990.

- [7] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(4):643–649, 1990.
- [8] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(3):529–536, 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] Wolfgang Ebeling. *Lattices and Codes*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.
- [15] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. \mathbb{Z} -modules. *Formalized Mathematics*, 20(1):47–59, 2012. doi:10.2478/v10037-012-0007-z.
- [16] 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.
- [17] Katarzyna Jankowska. Matrices. Abelian group of matrices. *Formalized Mathematics*, 2(4):475–480, 1991.
- [18] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(5):841–845, 1990.
- [19] Jarosław Kotowicz. Bilinear functionals in vector spaces. *Formalized Mathematics*, 11(1):69–86, 2003.
- [20] Jarosław Kotowicz. Partial functions from a domain to a domain. *Formalized Mathematics*, 1(4):697–702, 1990.
- [21] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(2):335–342, 1990.
- [22] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: a cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.
- [23] Anna Justyna Milewska. The Hahn Banach theorem in the vector space over the field of complex numbers. *Formalized Mathematics*, 9(2):363–371, 2001.
- [24] Robert Milewski. Associated matrix of linear map. *Formalized Mathematics*, 5(3):339–345, 1996.
- [25] Michał Muzalewski. Rings and modules – part II. *Formalized Mathematics*, 2(4):579–585, 1991.
- [26] Bogdan Nowak and Andrzej Trybulec. Hahn-Banach theorem. *Formalized Mathematics*, 4(1):29–34, 1993.
- [27] Karol Pał and Andrzej Trybulec. Laplace expansion. *Formalized Mathematics*, 15(3):143–150, 2007. doi:10.2478/v10037-007-0016-5.
- [28] Christoph Schwarzeweller. The ring of integers, Euclidean rings and modulo integers. *Formalized Mathematics*, 8(1):29–34, 1999.
- [29] Nobuyuki Tamura and Yatsuka Nakamura. Determinant and inverse of matrices of real elements. *Formalized Mathematics*, 15(3):127–136, 2007. doi:10.2478/v10037-007-0014-7.
- [30] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(2):329–334, 1990.
- [31] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [32] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(3):569–573, 1990.
- [33] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(3):575–579, 1990.
- [34] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(5):821–827, 1990.
- [35] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.
- [36] Wojciech A. Trybulec. Linear combinations in vector space. *Formalized Mathematics*, 1

- (5):877–882, 1990.
- [37] Wojciech A. Trybulec. Basis of vector space. *Formalized Mathematics*, 1(5):883–885, 1990.
- [38] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.
- [39] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.
- [40] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(1):181–186, 1990.
- [41] Katarzyna Zawadzka. The sum and product of finite sequences of elements of a field. *Formalized Mathematics*, 3(2):205–211, 1992.
- [42] Katarzyna Zawadzka. The product and the determinant of matrices with entries in a field. *Formalized Mathematics*, 4(1):1–8, 1993.

Received February 18, 2015
