

Lattice of \mathbb{Z} -module

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

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the definition of lattice of \mathbb{Z} -module and its properties in the Mizar system [5]. We formally prove that scalar products in lattices are bilinear forms over the field of real numbers \mathbb{R} . We also formalize the definitions of positive definite and integral lattices and their properties. Lattice of \mathbb{Z} -module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [14], and cryptographic systems with lattices [15] and coding theory [9].

MSC: 15A03 15A63 11E39 03B35

Keywords: \mathbb{Z} -lattice; Gram matrix; integral \mathbb{Z} -lattice; positive definite \mathbb{Z} -lattice

MML identifier: ZMODLAT1, version: 8.1.04 5.36.1267

1. DEFINITION OF LATTICES OF \mathbb{Z} -MODULE

Now we state the proposition:

- (1) Let us consider non empty sets D, E , natural numbers n, m , and a matrix M over D of dimension $n \times m$. 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 of dimension $n \times m$.

Let a, b be elements of $\mathbb{F}_{\mathbb{Q}}$ and x, y be rational numbers. We identify $x + y$ with $a + b$ and $x \cdot y$ with $a \cdot b$. Let F be a 1-sorted structure. We consider structures of \mathbb{Z} -lattice over F which extend vector space structures over F and are systems

\langle a carrier, an addition, a zero, a left multiplication,

a scalar product)

where the carrier is a set, the addition is a binary operation on the carrier, the zero is an element of the carrier, the left multiplication is a function from (the carrier of F) \times (the carrier) into the carrier, the scalar product is a function from (the carrier) \times (the carrier) into the carrier of \mathbb{R}_F .

Note that there exists a structure of \mathbb{Z} -lattice over F which is strict and non empty.

Let D be a non empty set, Z be an element of D , a be a binary operation on D , m be a function from (the carrier of F) \times D into D , and s be a function from $D \times D$ into the carrier of \mathbb{R}_F . One can check that $\langle D, a, Z, m, s \rangle$ is non empty.

Let X be a non empty structure of \mathbb{Z} -lattice over \mathbb{Z}^R and x, y be vectors of X . The functor $\langle x, y \rangle$ yielding an element of \mathbb{R}_F is defined by the term

(Def. 1) (the scalar product of X)($\langle x, y \rangle$).

Let x be a vector of X . The functor $\|x\|$ yielding an element of \mathbb{R}_F is defined by the term

(Def. 2) $\langle x, x \rangle$.

Let X be a non empty structure of \mathbb{Z} -lattice over \mathbb{Z}^R . We say that X is \mathbb{Z} -lattice-like if and only if

(Def. 3) for every vector x of X such that for every vector y of X , $\langle x, y \rangle = 0$ holds $x = 0_X$ and for every vectors x, y of X , $\langle x, y \rangle = \langle y, x \rangle$ and for every vectors x, y, z of X and for every element a of \mathbb{Z}^R , $\langle x+y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ and $\langle a \cdot x, y \rangle = a \cdot \langle x, y \rangle$.

Let V be a \mathbb{Z} -module and s be a function from (the carrier of V) \times (the carrier of V) into the carrier of \mathbb{R}_F . The functor $\text{GenLat}(V, s)$ yielding a non empty structure of \mathbb{Z} -lattice over \mathbb{Z}^R is defined by the term

(Def. 4) (the carrier of V , the addition of V , 0_V , the left multiplication of V , s).

Let us note that there exists a non empty structure of \mathbb{Z} -lattice over \mathbb{Z}^R which is vector distributive, scalar distributive, scalar associative, scalar unital, Abelian, add-associative, right zeroed, right complementable, and strict.

Let V be a \mathbb{Z} -module and s be a function from (the carrier of V) \times (the carrier of V) into the carrier of \mathbb{R}_F . One can verify that $\text{GenLat}(V, s)$ is Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, and scalar unital.

Let us consider a \mathbb{Z} -module V and a function s from (the carrier of V) \times (the carrier of V) into the carrier of \mathbb{R}_F . Now we state the propositions:

- (2) $\text{GenLat}(V, s)$ is a submodule of V .
- (3) V is a submodule of $\text{GenLat}(V, s)$.

Note that there exists an Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of \mathbb{Z} -lattice over $\mathbb{Z}^{\mathbb{R}}$ which is free.

Let V be a free \mathbb{Z} -module and s be a function from (the carrier of V) \times (the carrier of V) into the carrier of $\mathbb{R}_{\mathbb{F}}$. Let us observe that $\text{GenLat}(V, s)$ is free and there exists an Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of \mathbb{Z} -lattice over $\mathbb{Z}^{\mathbb{R}}$ which is torsion-free.

Now we state the proposition:

- (4) Let us consider a finite rank, free \mathbb{Z} -module V , and a function s from (the carrier of V) \times (the carrier of V) into the carrier of $\mathbb{R}_{\mathbb{F}}$.

Then $\text{GenLat}(V, s)$ is finite rank. The theorem is a consequence of (2).

Let us note that there exists a free, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of \mathbb{Z} -lattice over $\mathbb{Z}^{\mathbb{R}}$ which is finite rank.

Let V be a finite rank, free \mathbb{Z} -module and s be a function from (the carrier of V) \times (the carrier of V) into the carrier of $\mathbb{R}_{\mathbb{F}}$. Let us note that $\text{GenLat}(V, s)$ is finite rank.

Now we state the proposition:

- (5) Let us consider a finite rank, free \mathbb{Z} -module V , and a function f from (the carrier of $\mathbf{0}_V$) \times (the carrier of $\mathbf{0}_V$) into the carrier of $\mathbb{R}_{\mathbb{F}}$. Suppose $f = (\text{the carrier of } \mathbf{0}_V) \times (\text{the carrier of } \mathbf{0}_V) \mapsto 0_{\mathbb{R}_{\mathbb{F}}}$. Then $\text{GenLat}(\mathbf{0}_V, f)$ is \mathbb{Z} -lattice-like.

PROOF: Set $X = \text{GenLat}(\mathbf{0}_V, f)$. For every vector x of X such that for every vector y of X , $\langle x, y \rangle = 0$ holds $x = 0_X$ by [10, (26)]. For every vectors x, y, z of X and for every element a of $\mathbb{Z}^{\mathbb{R}}$, $\langle x, y \rangle = \langle y, x \rangle$ and $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ and $\langle a \cdot x, y \rangle = a \cdot \langle x, y \rangle$ by [16, (7)], [8, (87)].
□

Note that there exists a non empty structure of \mathbb{Z} -lattice over $\mathbb{Z}^{\mathbb{R}}$ which is \mathbb{Z} -lattice-like and there exists a finite rank, free, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of \mathbb{Z} -lattice over $\mathbb{Z}^{\mathbb{R}}$ which is \mathbb{Z} -lattice-like.

There exists a finite rank, free, \mathbb{Z} -lattice-like, Abelian, add-associative, right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of \mathbb{Z} -lattice over $\mathbb{Z}^{\mathbb{R}}$ which is strict.

A \mathbb{Z} -lattice is a finite rank, free, \mathbb{Z} -lattice-like, Abelian, add-associative,

right zeroed, right complementable, scalar distributive, vector distributive, scalar associative, scalar unital, non empty structure of \mathbb{Z} -lattice over $\mathbb{Z}^{\mathbb{R}}$. Now we state the proposition:

- (6) Let us consider a non trivial, torsion-free \mathbb{Z} -module V , a submodule Z of V , a non zero vector v of V , and a function f from (the carrier of Z) \times (the carrier of Z) into the carrier of $\mathbb{R}_{\mathbb{F}}$. Suppose $Z = \text{Lin}(\{v\})$ and for every vectors v_1, v_2 of Z and for every elements a, b of $\mathbb{Z}^{\mathbb{R}}$ such that $v_1 = a \cdot v$ and $v_2 = b \cdot v$ holds $f(v_1, v_2) = a \cdot b$. Then $\text{GenLat}(Z, f)$ is \mathbb{Z} -lattice-like.

PROOF: Set $L = \text{GenLat}(Z, f)$. L is \mathbb{Z} -lattice-like by [10, (26)], [12, (19)], [10, (1)], [12, (21)]. \square

Observe that there exists a \mathbb{Z} -lattice which is non trivial.

Let V be a torsion-free \mathbb{Z} -module. Let us observe that $\mathbb{Z}\text{-MQVectSp}(V)$ is scalar distributive, vector distributive, scalar associative, scalar unital, add-associative, right zeroed, right complementable, and Abelian as a non empty vector space structure over $\mathbb{F}_{\mathbb{Q}}$.

Now we state the propositions:

- (7) Let us consider a \mathbb{Z} -lattice L , and vectors v, u of L . Then
- (i) $\langle v, -u \rangle = -\langle v, u \rangle$, and
 - (ii) $\langle -v, u \rangle = -\langle v, u \rangle$.
- (8) Let us consider a \mathbb{Z} -lattice L , and vectors v, u, w of L . Then $\langle v, u+w \rangle = \langle v, u \rangle + \langle v, w \rangle$.
- (9) Let us consider a \mathbb{Z} -lattice L , vectors v, u of L , and an element a of $\mathbb{Z}^{\mathbb{R}}$. Then $\langle v, a \cdot u \rangle = a \cdot \langle v, u \rangle$.
- (10) Let us consider a \mathbb{Z} -lattice L , vectors v, u, w of L , and elements a, b of $\mathbb{Z}^{\mathbb{R}}$. Then
- (i) $\langle a \cdot v + b \cdot u, w \rangle = a \cdot \langle v, w \rangle + b \cdot \langle u, w \rangle$, and
 - (ii) $\langle v, a \cdot u + b \cdot w \rangle = a \cdot \langle v, u \rangle + b \cdot \langle v, w \rangle$.

The theorem is a consequence of (8) and (9).

- (11) Let us consider a \mathbb{Z} -lattice L , and vectors v, u, w of L . Then
- (i) $\langle v - u, w \rangle = \langle v, w \rangle - \langle u, w \rangle$, and
 - (ii) $\langle v, u - w \rangle = \langle v, u \rangle - \langle v, w \rangle$.

The theorem is a consequence of (8) and (9).

- (12) Let us consider a \mathbb{Z} -lattice L , and a vector v of L . Then
- (i) $\langle v, 0_L \rangle = 0$, and
 - (ii) $\langle 0_L, v \rangle = 0$.

The theorem is a consequence of (11).

Let X be a \mathbb{Z} -lattice. We say that X is integral if and only if

(Def. 5) for every vectors v, u of X , $\langle v, u \rangle \in \mathbb{Z}$.

Observe that there exists a \mathbb{Z} -lattice which is integral.

Let L be an integral \mathbb{Z} -lattice and v, u be vectors of L . Let us observe that $\langle v, u \rangle$ is integer.

Let v be a vector of L . Let us note that $\|v\|$ is integer.

Now we state the propositions:

(13) Let us consider a \mathbb{Z} -lattice L , a finite subset I of L , and a vector u of L . Suppose for every vector v of L such that $v \in I$ holds $\langle v, u \rangle \in \mathbb{Z}$. Let us consider a vector v of L . If $v \in \text{Lin}(I)$, then $\langle v, u \rangle \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset I of L such that $\bar{I} = \mathbb{S}_1$ and for every vector v of L such that $v \in I$ holds $\langle v, u \rangle \in \mathbb{Z}$ for every vector v of L such that $v \in \text{Lin}(I)$ holds $\langle v, u \rangle \in \mathbb{Z}$. $\mathcal{P}[0]$ by [11, (67)], (12). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [8, (40)], [11, (72)], [1, (44)], [8, (31)]. For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

(14) Let us consider a \mathbb{Z} -lattice L , and a basis I of L . Suppose for every vectors v, u of L such that $v, u \in I$ holds $\langle v, u \rangle \in \mathbb{Z}$. Let us consider vectors v, u of L . Then $\langle v, u \rangle \in \mathbb{Z}$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset I of L such that $\bar{I} = \mathbb{S}_1$ and for every vectors v, u of L such that $v, u \in I$ holds $\langle v, u \rangle \in \mathbb{Z}$ for every vectors v, u of L such that $v, u \in \text{Lin}(I)$ holds $\langle v, u \rangle \in \mathbb{Z}$. $\mathcal{P}[0]$ by [11, (67)], (12). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [8, (40)], [11, (72)], [1, (44)], [8, (31)]. For every natural number n , $\mathcal{P}[n]$ from [3, Sch. 2]. \square

(15) Let us consider a \mathbb{Z} -lattice L , and a basis I of L . Suppose for every vectors v, u of L such that $v, u \in I$ holds $\langle v, u \rangle \in \mathbb{Z}$. Then L is integral.

Let X be a \mathbb{Z} -lattice. We say that X is positive definite if and only if

(Def. 6) for every vector v of X such that $v \neq 0_X$ holds $\|v\| > 0$.

Let us observe that there exists a \mathbb{Z} -lattice which is non trivial, integral, and positive definite.

Let us consider a positive definite \mathbb{Z} -lattice L and a vector v of L . Now we state the propositions:

(16) $\|v\| = 0$ if and only if $v = 0_L$.

(17) $\|v\| \geq 0$. The theorem is a consequence of (12).

Let X be an integral \mathbb{Z} -lattice. We say that X is even if and only if

(Def. 7) for every vector v of X , $\|v\|$ is even.

One can verify that there exists an integral \mathbb{Z} -lattice which is even.

Let L be a \mathbb{Z} -lattice. We introduce the notation $\dim(L)$ as a synonym of $\text{rank } L$.

Let v, u be vectors of L . We say that v, u are orthogonal if and only if

(Def. 8) $\langle v, u \rangle = 0$.

Let us note that the predicate is symmetric.

Let us consider a \mathbb{Z} -lattice L and vectors v, u of L .

Let us assume that v, u are orthogonal. Now we state the propositions:

(18) (i) $v, -u$ are orthogonal, and

(ii) $-v, u$ are orthogonal, and

(iii) $-v, -u$ are orthogonal.

The theorem is a consequence of (7).

(19) $\|v + u\| = \|v\| + \|u\|$. The theorem is a consequence of (8).

(20) $\|v - u\| = \|v\| + \|u\|$. The theorem is a consequence of (11).

Let L be a \mathbb{Z} -lattice.

A \mathbb{Z} -sublattice of L is a \mathbb{Z} -lattice and is defined by

(Def. 9) the carrier of $it \subseteq$ the carrier of L and $0_{it} = 0_L$ and the addition of $it =$ (the addition of L) \upharpoonright (the carrier of it) and the left multiplication of $it =$ (the left multiplication of L) \upharpoonright ((the carrier of $\mathbb{Z}^{\mathbb{R}}$) \times (the carrier of it)) and the scalar product of $it =$ (the scalar product of L) \upharpoonright (the carrier of it).

Now we state the propositions:

(21) Let us consider a \mathbb{Z} -lattice L . Then every \mathbb{Z} -sublattice of L is a submodule of L .

(22) Let us consider an object x , a \mathbb{Z} -lattice L , and \mathbb{Z} -sublattices L_1, L_2 of L . Suppose $x \in L_1$ and L_1 is a \mathbb{Z} -sublattice of L_2 . Then $x \in L_2$. The theorem is a consequence of (21).

(23) Let us consider an object x , a \mathbb{Z} -lattice L , and a \mathbb{Z} -sublattice L_1 of L . If $x \in L_1$, then $x \in L$. The theorem is a consequence of (21).

(24) Let us consider a \mathbb{Z} -lattice L , and a \mathbb{Z} -sublattice L_1 of L . Then every vector of L_1 is a vector of L . The theorem is a consequence of (21).

(25) Let us consider a \mathbb{Z} -lattice L , and \mathbb{Z} -sublattices L_1, L_2 of L . Then $0_{L_1} = 0_{L_2}$.

(26) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , vectors v_1, v_2 of L , and vectors w_1, w_2 of L_1 . If $w_1 = v_1$ and $w_2 = v_2$, then $w_1 + w_2 = v_1 + v_2$. The theorem is a consequence of (21).

- (27) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , a vector v of L , a vector w of L_1 , and an element a of $\mathbb{Z}^{\mathbb{R}}$. If $w = v$, then $a \cdot w = a \cdot v$. The theorem is a consequence of (21).
- (28) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , a vector v of L , and a vector w of L_1 . If $w = v$, then $-w = -v$. The theorem is a consequence of (21).
- (29) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , vectors v_1, v_2 of L , and vectors w_1, w_2 of L_1 . If $w_1 = v_1$ and $w_2 = v_2$, then $w_1 - w_2 = v_1 - v_2$. The theorem is a consequence of (21).
- (30) Let us consider a \mathbb{Z} -lattice L , and a \mathbb{Z} -sublattice L_1 of L . Then $0_L \in L_1$. The theorem is a consequence of (21).
- (31) Let us consider a \mathbb{Z} -lattice L , and \mathbb{Z} -sublattices L_1, L_2 of L . Then $0_{L_1} \in L_2$. The theorem is a consequence of (21).
- (32) Let us consider a \mathbb{Z} -lattice L , and a \mathbb{Z} -sublattice L_1 of L . Then $0_{L_1} \in L$. The theorem is a consequence of (21).
- (33) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , and vectors v_1, v_2 of L . If $v_1, v_2 \in L_1$, then $v_1 + v_2 \in L_1$. The theorem is a consequence of (21).
- (34) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , a vector v of L , and an element a of $\mathbb{Z}^{\mathbb{R}}$. If $v \in L_1$, then $a \cdot v \in L_1$. The theorem is a consequence of (21).
- (35) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , and a vector v of L . If $v \in L_1$, then $-v \in L_1$. The theorem is a consequence of (21).
- (36) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , and vectors v_1, v_2 of L . If $v_1, v_2 \in L_1$, then $v_1 - v_2 \in L_1$. The theorem is a consequence of (21).
- (37) Let us consider a positive definite \mathbb{Z} -lattice L , a non empty set A , an element z of A , a binary operation a on A , a function m from (the carrier of $\mathbb{Z}^{\mathbb{R}} \times A$) into A , and a function s from $A \times A$ into the carrier of \mathbb{R}_F . Suppose A is a linearly closed subset of L and $z = 0_L$ and $a =$ (the addition of L) $\upharpoonright A$ and $m =$ (the left multiplication of L) $\upharpoonright ((\text{the carrier of } \mathbb{Z}^{\mathbb{R}}) \times A)$ and $s =$ (the scalar product of L) $\upharpoonright A$. Then $\langle A, a, z, m, s \rangle$ is a \mathbb{Z} -sublattice of L .
- PROOF: Set $L_1 = \langle A, a, z, m, s \rangle$. Set $V_1 = \langle A, a, z, m \rangle$. L_1 is a submodule of V_1 . L_1 is \mathbb{Z} -lattice-like by [10, (25)], [7, (49)], [10, (28), (29)]. \square
- (38) Let us consider a \mathbb{Z} -lattice L , a \mathbb{Z} -sublattice L_1 of L , vectors w_1, w_2 of L_1 , and vectors v_1, v_2 of L . Suppose $w_1 = v_1$ and $w_2 = v_2$. Then $\langle w_1, w_2 \rangle = \langle v_1, v_2 \rangle$.

Let L be an integral \mathbb{Z} -lattice. Note that every \mathbb{Z} -sublattice of L is integral.

Let L be a positive definite \mathbb{Z} -lattice. Let us observe that every \mathbb{Z} -sublattice of L is positive definite.

Let V, W be vector space structures over $\mathbb{Z}^{\mathbb{R}}$.

An \mathbb{R} -form of V and W is a function from (the carrier of V) \times (the carrier of W) into the carrier of $\mathbb{R}_{\mathbb{F}}$. The functor $\text{NulFrForm}(V, W)$ yielding an \mathbb{R} -form of V and W is defined by the term

(Def. 10) (the carrier of V) \times (the carrier of W) $\mapsto 0_{\mathbb{R}_{\mathbb{F}}}$.

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

(Def. 11) 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 an \mathbb{R} -form of V and W and a be an element of $\mathbb{R}_{\mathbb{F}}$. The functor $a \cdot f$ yielding an \mathbb{R} -form of V and W is defined by

(Def. 12) 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 an \mathbb{R} -form of V and W is defined by

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

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

(Def. 14) $(-1_{\mathbb{R}_{\mathbb{F}}}) \cdot f$.

Let f, g be \mathbb{R} -forms of V and W . The functor $f - g$ yielding an \mathbb{R} -form of V and W is defined by the term

(Def. 15) $f + -g$.

Observe that the functor $f - g$ is defined by

(Def. 16) for every vector v of V and for every vector w of W , $it(v, w) = f(v, w) - g(v, w)$.

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

Now we state the propositions:

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

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

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

(42) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an element a of $\mathbb{R}_{\mathbb{F}}$, and \mathbb{R} -forms f, g of V and 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 $\mathbb{R}_{\mathbb{F}}$, and an \mathbb{R} -form f of V and W . Now we state the propositions:

$$(43) \quad (a + b) \cdot f = a \cdot f + b \cdot f.$$

$$(44) \quad (a \cdot b) \cdot f = a \cdot (b \cdot f).$$

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

Let V be a vector space structure over $\mathbb{Z}^{\mathbb{R}}$.

An \mathbb{R} -functional of V is a function from the carrier of V into the carrier of \mathbb{R}_F . Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$ and f, g be \mathbb{R} -functionals of V . The functor $f + g$ yielding an \mathbb{R} -functional of V is defined by

(Def. 17) for every element x of V , $it(x) = f(x) + g(x)$.

Let f be an \mathbb{R} -functional of V . The functor $-f$ yielding an \mathbb{R} -functional of V is defined by

(Def. 18) for every element x of V , $it(x) = -f(x)$.

Let f, g be \mathbb{R} -functionals of V . The functor $f - g$ yielding an \mathbb{R} -functional of V is defined by the term

(Def. 19) $f - g$.

Let v be an element of \mathbb{R}_F and f be an \mathbb{R} -functional of V . The functor $v \cdot f$ yielding an \mathbb{R} -functional of V is defined by

(Def. 20) for every element x of V , $it(x) = v \cdot f(x)$.

Let V be a vector space structure over $\mathbb{Z}^{\mathbb{R}}$. The functor $0\text{FrFunctional}(V)$ yielding an \mathbb{R} -functional of V is defined by the term

(Def. 21) $\Omega_V \mapsto 0_{\mathbb{R}_F}$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$ and F be an \mathbb{R} -functional of V . We say that F is homogeneous if and only if

(Def. 22) for every vector x of V and for every scalar r of V , $F(r \cdot x) = r \cdot F(x)$.

We say that F is 0-preserving if and only if

(Def. 23) $F(0_V) = 0_{\mathbb{R}_F}$.

Let V be a \mathbb{Z} -module. Note that every \mathbb{R} -functional of V which is homogeneous is also 0-preserving.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$. One can verify that $0\text{FrFunctional}(V)$ is additive and $0\text{FrFunctional}(V)$ is homogeneous and $0\text{FrFunctional}(V)$ is 0-preserving and there exists an \mathbb{R} -functional of V which is additive, homogeneous, and 0-preserving.

Now we state the propositions:

(46) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, and \mathbb{R} -functionals f, g of V . Then $f + g = g + f$.

(47) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, and \mathbb{R} -functionals f, g, h of V . Then $(f + g) + h = f + (g + h)$.

(48) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, and an element x of V . Then $(0\text{FrFunctional}(V))(x) = 0_{\mathbb{R}_F}$.

Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$ and an \mathbb{R} -functional f of V . Now we state the propositions:

(49) $f + 0\text{FrFunctional}(V) = f$.

(50) $f - f = 0\text{FrFunctional}(V)$.

(51) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, an element r of \mathbb{R}_F , and \mathbb{R} -functionals f, g of V . Then $r \cdot (f + g) = r \cdot f + r \cdot g$.

Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, elements r, s of \mathbb{R}_F , and an \mathbb{R} -functional f of V . Now we state the propositions:

(52) $(r + s) \cdot f = r \cdot f + s \cdot f$.

(53) $(r \cdot s) \cdot f = r \cdot (s \cdot f)$.

(54) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, and an \mathbb{R} -functional f of V . Then $1_{\mathbb{R}_F} \cdot f = f$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$ and f, g be additive \mathbb{R} -functionals of V . Observe that $f + g$ is additive.

Let f be an additive \mathbb{R} -functional of V . One can check that $-f$ is additive.

Let v be an element of \mathbb{R}_F . Let us note that $v \cdot f$ is additive.

Let f, g be homogeneous \mathbb{R} -functionals of V . Let us observe that $f + g$ is homogeneous.

Let f be a homogeneous \mathbb{R} -functional of V . Note that $-f$ is homogeneous.

Let v be an element of \mathbb{R}_F . Observe that $v \cdot f$ is homogeneous.

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

(Def. 24) $(\text{curry } f)(v)$.

Let w be a vector of W . The functor $\text{FrFunctionalSAF}(f, w)$ yielding an \mathbb{R} -functional of V is defined by the term

(Def. 25) $(\text{curry}' f)(w)$.

Now we state the propositions:

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

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

(ii) $\text{rng FrFunctionalFAF}(f, v) \subseteq \text{the carrier of } \mathbb{R}_F$, and

(iii) for every vector w of W , $(\text{FrFunctionalFAF}(f, v))(w) = f(v, w)$.

- (56) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -form f of V and W , and a vector w of W . Then
- (i) $\text{dom FrFunctionalSAF}(f, w) = \text{the carrier of } V$, and
 - (ii) $\text{rng FrFunctionalSAF}(f, w) \subseteq \text{the carrier of } \mathbb{R}_{\mathbb{F}}$, and
 - (iii) for every vector v of V , $(\text{FrFunctionalSAF}(f, w))(v) = f(v, w)$.
- (57) Let us consider a non empty vector space structure V over $\mathbb{Z}^{\mathbb{R}}$, and an element x of V . Then $(0\text{FrFunctional}(V))(x) = 0_{\mathbb{R}_{\mathbb{F}}}$.
- (58) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a vector v of V . Then $\text{FrFunctionalFAF}(\text{NulFrForm}(V, W), v) = 0\text{FrFunctional}(W)$. The theorem is a consequence of (55).
- (59) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and a vector w of W . Then $\text{FrFunctionalSAF}(\text{NulFrForm}(V, W), w) = 0\text{FrFunctional}(V)$. The theorem is a consequence of (56).
- (60) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, \mathbb{R} -forms f, g of V and W , and a vector w of W . Then $\text{FrFunctionalSAF}(f + g, w) = \text{FrFunctionalSAF}(f, w) + \text{FrFunctionalSAF}(g, w)$. The theorem is a consequence of (56).
- (61) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, \mathbb{R} -forms f, g of V and W , and a vector v of V . Then $\text{FrFunctionalFAF}(f + g, v) = \text{FrFunctionalFAF}(f, v) + \text{FrFunctionalFAF}(g, v)$. The theorem is a consequence of (55).
- (62) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -form f of V and W , an element a of $\mathbb{R}_{\mathbb{F}}$, and a vector w of W . Then $\text{FrFunctionalSAF}(a \cdot f, w) = a \cdot \text{FrFunctionalSAF}(f, w)$. The theorem is a consequence of (56).
- (63) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -form f of V and W , an element a of $\mathbb{R}_{\mathbb{F}}$, and a vector v of V . Then $\text{FrFunctionalFAF}(a \cdot f, v) = a \cdot \text{FrFunctionalFAF}(f, v)$. The theorem is a consequence of (55).
- (64) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -form f of V and W , and a vector w of W . Then $\text{FrFunctionalSAF}(-f, w) = -\text{FrFunctionalSAF}(f, w)$. The theorem is a consequence of (56).
- (65) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -form f of V and W , and a vector v of V . Then $\text{FrFunctionalFAF}(-f, v) = -\text{FrFunctionalFAF}(f, v)$. The theorem is a consequence of (55).
- (66) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, \mathbb{R} -forms f, g of V and W , and a vector w of W . Then $\text{FrFunctionalSAF}(f -$

$g, w) = \text{FrFunctionalSAF}(f, w) - \text{FrFunctionalSAF}(g, w)$. The theorem is a consequence of (56).

- (67) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, \mathbb{R} -forms f, g of V and W , and a vector v of V . Then $\text{FrFunctionalFAF}(f - g, v) = \text{FrFunctionalFAF}(f, v) - \text{FrFunctionalFAF}(g, v)$. The theorem is a consequence of (55).

Let V, W be non empty vector space structures over $\mathbb{Z}^{\mathbb{R}}$, f be an \mathbb{R} -functional of V , and g be an \mathbb{R} -functional of W . The functor $\text{FrFormFunctional}(f, g)$ yielding an \mathbb{R} -form of V and W is defined by

(Def. 26) for every vector v of V and for every vector w of W , $it(v, w) = f(v) \cdot g(w)$.

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

Then $(\text{FrFormFunctional}(f, 0\text{FrFunctional}(W)))(v, w) = 0_{\mathbb{Z}^{\mathbb{R}}}$.

- (69) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -functional g of W , a vector v of V , and a vector w of W .

Then $(\text{FrFormFunctional}(0\text{FrFunctional}(V), g))(v, w) = 0_{\mathbb{Z}^{\mathbb{R}}}$.

- (70) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and an \mathbb{R} -functional f of V . Then $\text{FrFormFunctional}(f, 0\text{FrFunctional}(W)) = \text{NulFrForm}(V, W)$. The theorem is a consequence of (68).

- (71) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and an \mathbb{R} -functional g of W . Then $\text{FrFormFunctional}(0\text{FrFunctional}(V), g) = \text{NulFrForm}(V, W)$. The theorem is a consequence of (69).

- (72) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -functional f of V , an \mathbb{R} -functional g of W , and a vector v of V . Then $\text{FrFunctionalFAF}(\text{FrFormFunctional}(f, g), v) = f(v) \cdot g$. The theorem is a consequence of (55).

- (73) Let us consider non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an \mathbb{R} -functional f of V , an \mathbb{R} -functional g of W , and a vector w of W . Then $\text{FrFunctionalSAF}(\text{FrFormFunctional}(f, g), w) = g(w) \cdot f$. The theorem is a consequence of (56).

2. BILINEAR FORMS OVER FIELD OF REALS AND THEIR PROPERTIES

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

(Def. 27) for every vector v of V , $\text{FrFunctionalFAF}(f, v)$ is additive.

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

(Def. 28) for every vector w of W , $\text{FrFunctionalSAF}(f, w)$ is additive.

We say that f is homogeneous w.r.t. second argument if and only if
 (Def. 29) for every vector v of V , $\text{FrFunctionalFAF}(f, v)$ is homogeneous.

We say that f is homogeneous w.r.t. first argument if and only if
 (Def. 30) for every vector w of W , $\text{FrFunctionalSAF}(f, w)$ is homogeneous.

Observe that $\text{NulFrForm}(V, W)$ is additive w.r.t. second argument and

$\text{NulFrForm}(V, W)$ is additive w.r.t. first argument and there exists an \mathbb{R} -form of V and W which is additive w.r.t. second argument and additive w.r.t. first argument and $\text{NulFrForm}(V, W)$ is homogeneous w.r.t. second argument and $\text{NulFrForm}(V, W)$ is homogeneous w.r.t. first argument.

There exists an \mathbb{R} -form of V and 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.

An \mathbb{R} -bilinear form of V and 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 \mathbb{R} -form of V and W . Let f be an additive w.r.t. second argument \mathbb{R} -form of V and W and v be a vector of V . One can check that $\text{FrFunctionalFAF}(f, v)$ is additive.

Let f be an additive w.r.t. first argument \mathbb{R} -form of V and W and w be a vector of W . Observe that $\text{FrFunctionalSAF}(f, w)$ is additive.

Let f be a homogeneous w.r.t. second argument \mathbb{R} -form of V and W and v be a vector of V . One can check that $\text{FrFunctionalFAF}(f, v)$ is homogeneous.

Let f be a homogeneous w.r.t. first argument \mathbb{R} -form of V and W and w be a vector of W . Observe that $\text{FrFunctionalSAF}(f, w)$ is homogeneous.

Let f be an \mathbb{R} -functional of V and g be an additive \mathbb{R} -functional of W . Observe that $\text{FrFormFunctional}(f, g)$ is additive w.r.t. second argument.

Let f be an additive \mathbb{R} -functional of V and g be an \mathbb{R} -functional of W . One can check that $\text{FrFormFunctional}(f, g)$ is additive w.r.t. first argument.

Let f be an \mathbb{R} -functional of V and g be a homogeneous \mathbb{R} -functional of W . Observe that $\text{FrFormFunctional}(f, g)$ is homogeneous w.r.t. second argument.

Let f be a homogeneous \mathbb{R} -functional of V and g be an \mathbb{R} -functional of W . One can check that $\text{FrFormFunctional}(f, g)$ is homogeneous w.r.t. first argument.

Let V be a non trivial vector space structure over $\mathbb{Z}^{\mathbb{R}}$, W be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$, and f be an \mathbb{R} -functional of V . One can verify that $\text{FrFormFunctional}(f, g)$ is non trivial and $\text{FrFormFunctional}(f, g)$ is non trivial.

Let F be an \mathbb{R} -functional of V . We say that F is 0-preserving if and only if
 (Def. 31) $F(0_V) = 0_{\mathbb{R}_F}$.

Let V be a \mathbb{Z} -module. One can check that every \mathbb{R} -functional of 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 $0\text{FrFunctional}(V)$ is 0-preserving and there exists an \mathbb{R} -functional of V which is additive, homogeneous, and 0-preserving.

Let V be a non trivial, free \mathbb{Z} -module. Note that there exists an \mathbb{R} -functional of V which is additive, homogeneous, non constant, and non trivial.

(74) Let us consider a non trivial, free \mathbb{Z} -module V , and a non constant, 0-preserving \mathbb{R} -functional f of V . Then there exists a vector v of V such that

- (i) $v \neq 0_V$, and
- (ii) $f(v) \neq 0_{\mathbb{R}_F}$.

Let V, W be non trivial, free \mathbb{Z} -modules, f be a non constant, 0-preserving \mathbb{R} -functional of V , and g be a non constant, 0-preserving \mathbb{R} -functional of W . Note that $\text{FrFormFunctional}(f, g)$ is non constant.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathbb{R}}$.

An \mathbb{R} -linear functional of V is an additive, homogeneous \mathbb{R} -functional of V . Let V, W be non trivial, free \mathbb{Z} -modules. Observe that there exists an \mathbb{R} -form of V and 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 \mathbb{R} -forms of V and W . Let us observe that $f + g$ is additive w.r.t. first argument. Let f, g be additive w.r.t. second argument \mathbb{R} -forms of V and W . One can check that $f + g$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument \mathbb{R} -form of V and W and a be an element of \mathbb{R}_F . Let us observe that $a \cdot f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument \mathbb{R} -form of V and W . Note that $a \cdot f$ is additive w.r.t. second argument.

Let f be an additive w.r.t. first argument \mathbb{R} -form of V and W . Let us observe that $-f$ is additive w.r.t. first argument.

Let f be an additive w.r.t. second argument \mathbb{R} -form of V and W . Let us observe that $-f$ is additive w.r.t. second argument.

Let f, g be additive w.r.t. first argument \mathbb{R} -forms of V and W . Observe that $f - g$ is additive w.r.t. first argument.

Let f, g be additive w.r.t. second argument \mathbb{R} -forms of V and W . One can check that $f - g$ is additive w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument \mathbb{R} -forms of V and W . Observe that $f + g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument \mathbb{R} -forms of V and W . One can verify that $f + g$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument \mathbb{R} -form of V and W and a be an element of \mathbb{R}_F . Observe that $a \cdot f$ is homogeneous w.r.t. first argument.

Let f be a homogeneous w.r.t. second argument \mathbb{R} -form of V and W . One can check that $a \cdot f$ is homogeneous w.r.t. second argument.

Let f be a homogeneous w.r.t. first argument \mathbb{R} -form of V and W . Observe that $-f$ is homogeneous w.r.t. first argument. Let f be a homogeneous w.r.t. second argument \mathbb{R} -form of V and W . Observe that $-f$ is homogeneous w.r.t. second argument.

Let f, g be homogeneous w.r.t. first argument \mathbb{R} -forms of V and W . Let us note that $f - g$ is homogeneous w.r.t. first argument.

Let f, g be homogeneous w.r.t. second argument \mathbb{R} -forms of V and W . One can verify that $f - g$ is homogeneous w.r.t. second argument.

(75) 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 an \mathbb{R} -form f of V and 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 (56).

(76) 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 an \mathbb{R} -form f of V and 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 (55).

(77) 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 \mathbb{R} -form f of V and 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 (75) and (76).

(78) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an additive w.r.t. second argument \mathbb{R} -form f of V and W , and a vector v of V . Then $f(v, 0_W) = 0_{\mathbb{Z}^{\mathbb{R}}}$. The theorem is a consequence of (76).

(79) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, an additive w.r.t. first argument \mathbb{R} -form f of V and W , and a vector w of W . Then $f(0_V, w) = 0_{\mathbb{Z}^{\mathbb{R}}}$. The theorem is a consequence of (75).

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 an \mathbb{R} -form f of V and W . Now we state the propositions:

(80) 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 (56).

- (81) 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 (55).
- (82) 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 \mathbb{R} -form f of V and W , and a vector w of W . Then $f(0_V, w) = 0_{\mathbb{R}_F}$. The theorem is a consequence of (80).
- (83) 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 \mathbb{R} -form f of V and W , and a vector v of V . Then $f(v, 0_W) = 0_{\mathbb{R}_F}$. The theorem is a consequence of (81).
- (84) 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 \mathbb{R} -form f of V and W . Then $f(v - u, w) = f(v, w) - f(u, w)$. The theorem is a consequence of (75) and (80).
- (85) 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 \mathbb{R} -form f of V and W . Then $f(v, w - t) = f(v, w) - f(v, t)$. The theorem is a consequence of (76) and (81).
- (86) Let us consider \mathbb{Z} -modules V, W , vectors v, u of V , vectors w, t of W , and an \mathbb{R} -bilinear form f of V and 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 (84) and (85).
- (87) 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 an \mathbb{R} -bilinear form f of V and 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 (77), (81), and (80).
- (88) 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 an \mathbb{R} -bilinear form f of V and 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 (86), (81), and (80).
- (89) Let us consider right zeroed, non empty vector space structures V, W over $\mathbb{Z}^{\mathbb{R}}$, and an \mathbb{R} -form f of V and 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 , $f(v, w) = 0_{\mathbb{Z}^{\mathbb{R}}}$. The theorem is a consequence of (78) and (79).

3. MATRICES OF BILINEAR FORM OVER FIELD OF REAL NUMBERS

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 an \mathbb{R} -bilinear form of V_1 and V_2 . The functor $\text{Bilinear}(f, b_1, b_2)$ yielding a matrix over \mathbb{R}_F of dimension $\text{len } b_1 \times \text{len } b_2$ is defined by

(Def. 32) 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:

(90) Let us consider a finite rank, free \mathbb{Z} -module V , an \mathbb{R} -linear functional F of V , a finite sequence y of elements of V , a finite sequence x of elements of \mathbb{Z}^R , and finite sequences X, Y of elements of \mathbb{R}_F . 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 $k \in \text{Seg len } x$ 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}^R for every finite sequences X, Y of elements of \mathbb{R}_F 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 $k \in \text{Seg len } x$ 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 [4, (22), (39), (59)], [3, (11)]. $\mathcal{P}[\varepsilon_\alpha]$, where α is the carrier of V by [17, (43)]. For every finite sequence p of elements of V , $\mathcal{P}[p]$ from [6, Sch. 2]. \square

(91) 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 , an \mathbb{R} -bilinear form f of V_1 and 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{R}_F . Suppose $\text{len } X = \text{len } b_2$ and $\text{len } Y = \text{len } b_2$ and for every natural number k such that $k \in \text{Seg len } b_2$ 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 (55) and (90).

(92) Let us consider finite rank, free \mathbb{Z} -modules V_1, V_2 , an ordered basis b_1 of V_1 , an \mathbb{R} -bilinear form f of V_1 and 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{R}_F . Suppose $\text{len } X = \text{len } b_1$ and $\text{len } Y = \text{len } b_1$ and for every natural number k such that $k \in \text{Seg len } b_1$ 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 (56) and (90).

(93) Every matrix over \mathbb{Z}^R is a matrix over \mathbb{R}_F .

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

(Def. 33) M .

Let n, m be natural numbers and M be a matrix over $\mathbb{Z}^{\mathbb{R}}$ of dimension $n \times m$. Note that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a matrix over $\mathbb{R}_{\mathbb{F}}$ of dimension $n \times m$. Let n be a natural number and M be a square matrix over $\mathbb{Z}^{\mathbb{R}}$ of dimension n . Let us note that the functor $\mathbb{Z}2\mathbb{R}(M)$ yields a square matrix over $\mathbb{R}_{\mathbb{F}}$ of dimension n . Now we state the propositions:

- (94) Let us consider natural numbers m, l, n , a matrix S over $\mathbb{Z}^{\mathbb{R}}$ of dimension $l \times m$, a matrix T over $\mathbb{Z}^{\mathbb{R}}$ of dimension $m \times n$, a matrix S_1 over $\mathbb{R}_{\mathbb{F}}$ of dimension $l \times m$, and a matrix T_1 over $\mathbb{R}_{\mathbb{F}}$ of dimension $m \times n$. If $S = S_1$ and $T = T_1$ and $0 < l$ and $0 < m$, then $S \cdot T = S_1 \cdot T_1$.

PROOF: Reconsider $S_3 = S \cdot T$ as a matrix over $\mathbb{Z}^{\mathbb{R}}$ of dimension $l \times n$. Reconsider $S_2 = S_1 \cdot T_1$ as a matrix over $\mathbb{R}_{\mathbb{F}}$ of dimension $l \times n$. For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of S_3 holds $S_{3i,j} = S_{2i,j}$ by [8, (87)], [13, (2), (3), (37)]. \square

- (95) Let us consider a natural number n . Then $I_{\mathbb{Z}^{\mathbb{R}}}^{n \times n} = I_{\mathbb{R}_{\mathbb{F}}}^{n \times n}$.

- (96) 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 an \mathbb{R} -bilinear form f of V_1 and V_2 . Suppose $0 < \text{rank } V_1$. Then $\text{Bilinear}(f, b_1, b_3) = \text{Bilinear}(f, b_1, b_2) \cdot (\mathbb{Z}2\mathbb{R}(\text{AutMt}(\text{id}_{V_2}, b_3, b_2)))^{\text{T}}$.

PROOF: Set $n = \text{len } b_2$. Reconsider $I_2 = \text{AutMt}(\text{id}_{V_2}, b_3, b_2)$ as a square matrix over $\mathbb{Z}^{\mathbb{R}}$ of dimension n . Reconsider $M_1 = \mathbb{Z}2\mathbb{R}(I_2^{\text{T}})$ as a square matrix over $\mathbb{R}_{\mathbb{F}}$ of dimension n . Set $M_2 = \text{Bilinear}(f, b_1, b_2) \cdot M_1$. 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 [8, (87)], [13, (1)], (91). \square

- (97) 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 an \mathbb{R} -bilinear form f of V_1 and V_2 . Suppose $0 < \text{rank } V_1$. Then $\text{Bilinear}(f, b_3, b_2) = \mathbb{Z}2\mathbb{R}(\text{AutMt}(\text{id}_{V_1}, b_3, b_1)) \cdot \text{Bilinear}(f, b_1, b_2)$.

PROOF: Set $n = \text{len } b_3$. Reconsider $I_2 = \text{AutMt}(\text{id}_{V_1}, b_3, b_1)$ as a square matrix over $\mathbb{Z}^{\mathbb{R}}$ of dimension n . Reconsider $M_1 = \mathbb{Z}2\mathbb{R}(I_2)$ as a square matrix over $\mathbb{R}_{\mathbb{F}}$ of dimension n . Set $M_2 = M_1 \cdot \text{Bilinear}(f, b_1, b_2)$. 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 [8, (87)], [4, (1)], [13, (1)], (92). \square

- (98) Let us consider a finite rank, free \mathbb{Z} -module V , ordered bases b_1, b_2 of V , and an \mathbb{R} -bilinear form f of V and V . Suppose $0 < \text{rank } V$. Then $\text{Bilinear}(f, b_2, b_2) = \mathbb{Z}2\mathbb{R}(\text{AutMt}(\text{id}_V, b_2, b_1)) \cdot \text{Bilinear}(f, b_1, b_1) \cdot (\mathbb{Z}2\mathbb{R}(\text{AutMt}(\text{id}_V, b_2, b_1)))^{\text{T}}$. The theorem is a consequence of (97) and (96).

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 $\mathbb{R}_{\mathbb{F}}$ of dimension $\text{rank } V$.

Let us assume that $M = \text{AutMt}(\text{id}_V, b_1, b_2)$. Now we state the propositions:

(99) (i) $\text{Det } M = 1$ and $\text{Det } M^T = 1$, or

(ii) $\text{Det } M = -1$ and $\text{Det } M^T = -1$.

The theorem is a consequence of (94) and (95).

(100) $|\text{Det } M| = 1$. The theorem is a consequence of (99).

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

(101) $\text{Det Bilinear}(f, b_2, b_2) = \text{Det Bilinear}(f, b_1, b_1)$. The theorem is a consequence of (98) and (99).

(102) $|\text{Det Bilinear}(f, b_2, b_2)| = |\text{Det Bilinear}(f, b_1, b_1)|$.

Let V be a finite rank, free \mathbb{Z} -module, f be an \mathbb{R} -bilinear form of V and V , and b be an ordered basis of V . The functor $\text{GramMatrix}(f, b)$ yielding a square matrix over \mathbb{R}_F of dimension $\text{rank } V$ is defined by the term

(Def. 34) $\text{Bilinear}(f, b, b)$.

The functor $\text{GramDet}(f)$ yielding an element of \mathbb{R}_F is defined by

(Def. 35) for every ordered basis b of V , $it = \text{Det GramMatrix}(f, b)$.

Let L be a \mathbb{Z} -lattice. The functor $\text{InnerProduct } L$ yielding an \mathbb{R} -form of L and L is defined by the term

(Def. 36) the scalar product of L .

One can check that $\text{InnerProduct } L$ is additive w.r.t. first argument, homogeneous w.r.t. first argument, additive w.r.t. second argument, and homogeneous w.r.t. second argument.

Let b be an ordered basis of L . The functor $\text{GramMatrix}(b)$ yielding a square matrix over \mathbb{R}_F of dimension $\text{dim}(L)$ is defined by the term

(Def. 37) $\text{GramMatrix}(\text{InnerProduct } L, b)$.

The functor $\text{GramDet}(L)$ yielding an element of \mathbb{R}_F is defined by the term

(Def. 38) $\text{GramDet}(\text{InnerProduct } L)$.

(103) Let us consider an integral \mathbb{Z} -lattice L . Then $\text{InnerProduct } L$ is a bilinear form of L, L .

PROOF: For every object z such that $z \in (\text{the carrier of } L) \times (\text{the carrier of } L)$ holds $(\text{InnerProduct } L)(z) \in \text{the carrier of } \mathbb{Z}^R$. Reconsider $f = \text{InnerProduct } L$ as a form of L, L . For every vector v of L , $f(\cdot, v)$ is additive by [2, (70)], (8). For every vector v of L , $f(\cdot, v)$ is homogeneous by [2, (70)], (9). For every vector v of L , $f(v, \cdot)$ is additive by [2, (69)], (8). For every vector v of L , $f(v, \cdot)$ is homogeneous by [2, (69)], (9). \square

(104) Let us consider an integral \mathbb{Z} -lattice L , and an ordered basis b of L . Then $\text{GramMatrix}(b)$ is a square matrix over \mathbb{Z}^R of dimension $\text{dim}(L)$.

PROOF: For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $\text{GramMatrix}(b)$ holds $(\text{GramMatrix}(b))_{i,j} \in$ the carrier of $\mathbb{Z}^{\mathbb{R}}$ by [8, (87)].

□

Let L be an integral \mathbb{Z} -lattice. Note that $\text{GramDet}(L)$ is integer.

REFERENCES

- [1] Grzegorz Bancerek. Cardinal arithmetics. *Formalized Mathematics*, 1(3):543–547, 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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [5] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Kornilowicz, Roman Matuszewski, Adam Naumowicz, Karol Pał, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.
- [6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(3):529–536, 1990.
- [7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [8] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.
- [9] Wolfgang Ebeling. *Lattices and Codes*. Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.
- [10] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. \mathbb{Z} -modules. *Formalized Mathematics*, 20(1):47–59, 2012. doi:10.2478/v10037-012-0007-z.
- [11] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Quotient module of \mathbb{Z} -module. *Formalized Mathematics*, 20(3):205–214, 2012. doi:10.2478/v10037-012-0024-y.
- [12] Yuichi Futa, Hiroyuki Okazaki, Kazuhisa Nakasho, and Yasunari Shidama. Torsion \mathbb{Z} -module and torsion-free \mathbb{Z} -module. *Formalized Mathematics*, 22(4):277–289, 2014. doi:10.2478/forma-2014-0028.
- [13] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. Matrix of \mathbb{Z} -module. *Formalized Mathematics*, 23(1):29–49, 2015. doi:10.2478/forma-2015-0003.
- [14] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4), 1982.
- [15] Daniele Micciancio and Shafi Goldwasser. Complexity of lattice problems: A cryptographic perspective. *The International Series in Engineering and Computer Science*, 2002.
- [16] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(2):329–334, 1990.
- [17] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(2):291–296, 1990.

Received December 30, 2015