FORMALIZED MATHEMATICS
Vol. 25, No. 1, Pages 73–86, 2017
DOI: 10.1515/forma-2017-0007

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

Embedded Lattice and Properties of Gram Matrix[1]

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in Mizar [14] the definition of embedding of lattice and its properties. We formally define an inner product on an embedded module. We also formalize properties of Gram matrix. We formally prove that an inverse of Gram matrix for a rational lattice exists. Lattice of $\mathbb{Z}$-module is necessary for lattice problems, LLL (Lenstra, Lenstra and Lovász) base reduction algorithm [16] and cryptographic systems with lattice [17].

MSC: 15A09 15A63 03B35

Keywords: $\mathbb{Z}$-lattice; Gram matrix; rational $\mathbb{Z}$-lattice

MML identifier: ZMODLAT2, version: 8.1.05 5.40.1289

1. Inner Product of Embedded Module

Now we state the propositions:

(1) Let us consider a ring K, a left module V over K, a function L from the carrier of V into the carrier of K, a subset A of V, and finite sequences F, F_1 of elements of the carrier of V. Suppose F is one-to-one and $\operatorname{rng} F = A$ and F_1 is one-to-one and $\operatorname{rng} F_1 = A$. Then $\sum(L \cdot F) = \sum(L \cdot F_1)$.
Proof: Define $\mathcal{G}[\text{object}, \text{object}] \equiv \{\$_2\} = F^{-1}(\{F_1(\$_1)\})$. For every object x such that $x \in \operatorname{dom} F$ there exists an object y such that $y \in \operatorname{dom} F$ and $\mathcal{G}[x, y]$ by [6, (74)]. Consider f being a function from $\operatorname{dom} F$ into $\operatorname{dom} F$ such that for every object x such that $x \in \operatorname{dom} F$ holds $\mathcal{G}[x, f(x)]$ from [7, Sch. 1]. $\operatorname{rng} f = \operatorname{dom} F$ by [6, (59), (82)], [8, (18)]. f is one-to-one by [8, (31)], [6, (91)], [8, (3)]. □

[1]This work was supported by JSPS KAKENHI Grant Number JP15K00183.

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

(2) Let us consider a ring K, a left module V over K, and a finite subset A of V. Then A is linearly independent if and only if for every linear combination L of A such that there exists a finite sequence F of elements of the carrier of V such that F is one-to-one and $\operatorname{rng} F = A$ and $\sum(L \cdot F) = 0_V$ holds the support of $L = \emptyset$.

PROOF: For every linear combination L of A such that $\sum L = 0_V$ holds the support of $L = \emptyset$ by [22, (13)], [26, (13)], [24, (41)]. □

(3) Let us consider a ring K, a left module V over K, and a finite sequence b of elements of V. Suppose b is one-to-one. Then $\operatorname{rng} b$ is linearly independent if and only if for every finite sequence r of elements of K and for every finite sequence r_1 of elements of V such that $\operatorname{len} r = \operatorname{len} b$ and $\operatorname{len} r_1 = \operatorname{len} b$ and for every natural number i such that $i \in \operatorname{dom} r_1$ holds $r_1(i) = r_i \cdot b_i$ and $\sum r_1 = 0_V$ holds $r = \operatorname{Seg} \operatorname{len} r \longmapsto 0_K$.

PROOF: For every linear combination L of $\operatorname{rng} b$ such that there exists a finite sequence F of elements of the carrier of V such that F is one-to-one and $\operatorname{rng} F = \operatorname{rng} b$ and $\sum(L \cdot F) = 0_V$ holds the support of $L = \emptyset$ by [29, (27)], [23, (29)], [6, (13)], (1). □

(4) Let us consider a ring K, a left module V over K, and a finite subset A of V. Then A is linearly independent if and only if there exists a finite sequence b of elements of V such that b is one-to-one and $\operatorname{rng} b = A$ and for every finite sequence r of elements of K and for every finite sequence r_1 of elements of V such that $\operatorname{len} r = \operatorname{len} b$ and $\operatorname{len} r_1 = \operatorname{len} b$ and for every natural number i such that $i \in \operatorname{dom} r_1$ holds $r_1(i) = r_i \cdot b_i$ and $\sum r_1 = 0_V$ holds $r = \operatorname{Seg} \operatorname{len} r \longmapsto 0_K$. The theorem is a consequence of (3).

Let V be a non trivial, free $\mathbb{Z}$-module. Let us note that every basis of V is non empty.

Let I_1 be a $\mathbb{Z}$-lattice. We say that I_1 is rational if and only if

(Def. 1) for every vectors v, u of I_1, $\langle v, u \rangle \in \mathbb{Q}$.

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

Let L be a rational $\mathbb{Z}$-lattice and v, u be vectors of L. Note that $\langle v, u \rangle$ is rational and every integral $\mathbb{Z}$-lattice is rational.

Let L be a $\mathbb{Z}$-lattice. The functor ScProductEM(L) yielding a function from (the carrier of Embedding(L)) $\times$ (the carrier of Embedding(L)) into the carrier of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 2) for every vectors v, u of L and for every vectors v_1, u_1 of Embedding(L) such that $v_1 = (\text{MorphsZQ}(L))(v)$ and $u_1 = (\text{MorphsZQ}(L))(u)$ holds $it(v_1, u_1) = \langle v, u \rangle$.

Now we state the proposition:

(5) Let us consider a $\mathbb{Z}$-lattice L. Then

(i) for every vector x of Embedding(L) such that for every vector y of Embedding(L), (ScProductEM(L))$(x, y) = 0$ holds $x = 0_{\text{Embedding}(L)}$, and

(ii) for every vectors x, y of Embedding(L), (ScProductEM(L))$(x, y) =$ (ScProductEM(L))(y, x), and

(iii) for every vectors x, y, z of Embedding(L) and for every element a of $\mathbb{Z}^{\mathrm{R}}$, (ScProductEM(L))$(x + y, z) =$ (ScProductEM(L))$(x, z) +$ (ScProductEM(L))(y, z) and (ScProductEM(L))$(a \cdot x, y) =$ $a \cdot$ (ScProductEM(L))(x, y).

PROOF: Set $Z =$ Embedding(L). Set $f =$ ScProductEM(L). For every vector x of Z such that for every vector y of Z, $f(x, y) = 0$ holds $x = 0_{\text{Embedding}(L)}$ by [10, (22)], [7, (4)]. For every vectors x, y of Z, $f(x, y) = f(y, x)$ by [10, (22)]. For every vectors x, y, z of Z and for every element a of $\mathbb{Z}^{\mathrm{R}}$, $f(x + y, z) = f(x, z) + f(y, z)$ and $f(a \cdot x, y) = a \cdot f(x, y)$ by [10, (22), (19)]. □

Let L be a $\mathbb{Z}$-lattice. The functor ScProductDM(L) yielding a function from (the carrier of DivisibleMod(L))$\times$(the carrier of DivisibleMod(L)) into the carrier of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 3) for every vectors v_1, u_1 of DivisibleMod(L) and for every vectors v, u of Embedding(L) and for every elements a, b of $\mathbb{Z}^{\mathrm{R}}$ and for every elements a_1, b_1 of $\mathbb{R}_{\mathrm{F}}$ such that $a = a_1$ and $b = b_1$ and $a_1 \neq 0$ and $b_1 \neq 0$ and $v = a \cdot v_1$ and $u = b \cdot u_1$ holds $it(v_1, u_1) = {a_1}^{-1} \cdot {b_1}^{-1} \cdot$ (ScProductEM(L))(v, u).

Let us consider a $\mathbb{Z}$-lattice L. Now we state the propositions:

(6) (i) for every vector x of DivisibleMod(L) such that for every vector y of DivisibleMod(L), (ScProductDM(L))$(x, y) = 0$ holds $x = 0_{\text{DivisibleMod}(L)}$, and

(ii) for every vectors x, y of DivisibleMod(L), (ScProductDM(L))$(x, y) =$ (ScProductDM(L))(y, x), and

(iii) for every vectors x, y, z of DivisibleMod(L) and for every element a of $\mathbb{Z}^{\mathrm{R}}$, (ScProductDM(L))$(x + y, z) =$ (ScProductDM(L))$(x, z) +$ (ScProductDM(L))(y, z) and (ScProductDM(L))$(a \cdot x, y) =$ $a \cdot$ (ScProductDM(L))(x, y).

PROOF: Set $D =$ DivisibleMod(L). Set $f =$ ScProductDM(L). For every vector x of D such that for every vector y of D, $f(x, y) = 0$ holds $x = 0_D$ by [10, (29)], [11, (24)], [15, (25)], (5). For every vectors x, y of D, $f(x, y) = f(y, x)$ by [10, (29)], (5). For every vectors x, y, z of D and for every

element i of $\mathbb{Z}^{\mathrm{R}}$, $f(x+y,z)=f(x,z)+f(y,z)$ and $f(i\cdot x,y)=i\cdot f(x,y)$ by [10, (29)], [11, (29), (28)], [18, (11)]. □

(7) $\mathrm{ScProductEM}(L)=\mathrm{ScProductDM}(L)\upharpoonright \mathrm{rng}\,\mathrm{MorphsZQ}(L)$.
PROOF: Reconsider $s=\mathrm{ScProductDM}(L)\upharpoonright \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ as a function from $\mathrm{rng}\,\mathrm{MorphsZQ}(L)\times \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. For every object x such that $x\in \mathrm{rng}\,\mathrm{MorphsZQ}(L)\times \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ holds $(\mathrm{ScProductEM}(L))(x)=s(x)$ by [11, (24)], [6, (49)], [8, (87)]. □

(8) Let us consider a $\mathbb{Z}$-lattice L, vectors v_1, v_2 of $\mathrm{DivisibleMod}(L)$, and vectors u_1, u_2 of $\mathrm{Embedding}(L)$. Suppose $v_1=u_1$ and $v_2=u_2$. Then $(\mathrm{ScProductEM}(L))(u_1,u_2)=(\mathrm{ScProductDM}(L))(v_1,v_2)$.

(9) Let us consider a $\mathbb{Z}$-lattice L, an element r of $\mathbb{F}_{\mathbb{Q}}$, and vectors v, u of $\mathrm{Embedding}(r,L)$. Then $(\mathrm{ScProductDM}(L)\upharpoonright(\text{the carrier of }\mathrm{Embedding}(r,L)))(v,u)=(\mathrm{ScProductDM}(L))(v,u)$.

(10) Let us consider a $\mathbb{Z}$-lattice L, a non empty set A, an element z of A, a binary operation a_1 on A, a function m_1 from $(\text{the carrier of }\mathbb{Z}^{\mathrm{R}})\times A$ into A, and a function s_1 from $A\times A$ into the carrier of $\mathbb{R}_{\mathrm{F}}$. Suppose A is a linearly closed subset of $\mathrm{DivisibleMod}(L)$ and $z=0_{\mathrm{DivisibleMod}(L)}$ and $a_1=(\text{the addition of }\mathrm{DivisibleMod}(L))\upharpoonright A$ and $m_1=(\text{the left multiplication of }\mathrm{DivisibleMod}(L))\upharpoonright((\text{the carrier of }\mathbb{Z}^{\mathrm{R}})\times A)$. Then $\langle A,a_1,z,m_1,s_1\rangle$ is a submodule of $\mathrm{DivisibleMod}(L)$.

(11) Let us consider a $\mathbb{Z}$-lattice L, and vectors v, u of $\mathrm{DivisibleMod}(L)$. Then

(i) $(\mathrm{ScProductDM}(L))(-v,u)=-(\mathrm{ScProductDM}(L))(v,u)$, and

(ii) $(\mathrm{ScProductDM}(L))(u,-v)=-(\mathrm{ScProductDM}(L))(u,v)$.

The theorem is a consequence of (6).

(12) Let us consider a $\mathbb{Z}$-lattice L, and vectors v, u, w of $\mathrm{DivisibleMod}(L)$. Then $(\mathrm{ScProductDM}(L))(v,u+w)=(\mathrm{ScProductDM}(L))(v,u)+(\mathrm{ScProductDM}(L))(v,w)$. The theorem is a consequence of (6).

(13) Let us consider a $\mathbb{Z}$-lattice L, vectors v, u of $\mathrm{DivisibleMod}(L)$, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Then $(\mathrm{ScProductDM}(L))(v,a\cdot u)=a\cdot(\mathrm{ScProductDM}(L))(v,u)$. The theorem is a consequence of (6).

(14) Let us consider a $\mathbb{Z}$-lattice L, and a vector v of $\mathrm{DivisibleMod}(L)$. Then

(i) $(\mathrm{ScProductDM}(L))(0_{\mathrm{DivisibleMod}(L)},v)=0$, and

(ii) $(\mathrm{ScProductDM}(L))(v,0_{\mathrm{DivisibleMod}(L)})=0$.

The theorem is a consequence of (6) and (11).

(15) Let us consider a $\mathbb{Z}$-lattice L, a vector v of $\mathrm{DivisibleMod}(L)$, and a basis I of $\mathrm{Embedding}(L)$. Suppose for every vector u of $\mathrm{DivisibleMod}(L)$ such

that $u \in I$ holds $(\mathrm{ScProductDM}(L))(v,u) = 0$. Let us consider a vector u of DivisibleMod(L). Then $(\mathrm{ScProductDM}(L))(v,u) = 0$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset I of Embedding (L) such that $\overline{\overline{I}} = \$_1$ and I is linearly independent and for every vector u of DivisibleMod(L) such that $u \in I$ holds $(\mathrm{ScProductDM}(L))(v,u) = 0$ for every vector w of DivisibleMod(L) such that $w \in \mathrm{Lin}(I)$ holds $(\mathrm{ScProductDM}(L))(v,w) = 0$. $\mathcal{P}[0]$ by [12, (67), (66)], (14). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [28, (41)], [2, (44)], [1, (30)], [8, (31)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. For every vector w of DivisibleMod(L), $(\mathrm{ScProductDM}(L))(v,w) = 0$ by [10, (29)], (6). □

(16) Let us consider a $\mathbb{Z}$-lattice L, a vector v of DivisibleMod(L), and a basis I of Embedding(L). Suppose for every vector u of DivisibleMod(L) such that $u \in I$ holds $(\mathrm{ScProductDM}(L))(v,u) = 0$. Then $v = 0_{\mathrm{DivisibleMod}(L)}$. The theorem is a consequence of (15) and (6).

(17) Let us consider a ring R, a left module V over R, a vector v of V, and an object u. Suppose $u \in \mathrm{Lin}(\{v\})$. Then there exists an element i of R such that $u = i \cdot v$.

(18) Let us consider a ring R, a left module V over R, and a vector v of V. Then $v \in \mathrm{Lin}(\{v\})$.

(19) Let us consider a ring R, a left module V over R, a vector v of V, and an element i of R. Then $i \cdot v \in \mathrm{Lin}(\{v\})$.

2. EMBEDDING OF LATTICE

Let L be a $\mathbb{Z}$-lattice. The functor $\mathrm{EMLat}(L)$ yielding a strict $\mathbb{Z}$-lattice is defined by

(Def. 4) the carrier of $it = \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ and the zero of $it = \mathrm{zeroCoset}(L)$ and the addition of $it = \mathrm{addCoset}(L) \restriction \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ and the left multiplication of $it = \mathrm{lmultCoset}(L) \restriction ((\text{the carrier of } \mathbb{Z}^{\mathrm{R}}) \times \mathrm{rng}\,\mathrm{MorphsZQ}(L))$ and the scalar product of $it = \mathrm{ScProductEM}(L)$.

Let r be an element of $\mathbb{F}_{\mathbb{Q}}$. The functor $\mathrm{EMLat}(r, L)$ yielding a strict $\mathbb{Z}$-lattice is defined by

(Def. 5) the carrier of $it = r \cdot \mathrm{rng}\,\mathrm{MorphsZQ}(L)$ and the zero of $it = \mathrm{zeroCoset}(L)$ and the addition of $it = \mathrm{addCoset}(L) \restriction (r \cdot \mathrm{rng}\,\mathrm{MorphsZQ}(L))$ and the left multiplication of $it = \mathrm{lmultCoset}(L) \restriction ((\text{the carrier of } \mathbb{Z}^{\mathrm{R}}) \times (r \cdot \mathrm{rng}\,\mathrm{MorphsZQ}(L)))$ and the scalar product of $it = \mathrm{ScProductDM}(L) \restriction (r \cdot \mathrm{rng}\,\mathrm{MorphsZQ}(L))$.

Let L be a non trivial $\mathbb{Z}$-lattice. One can verify that $\mathrm{EMLat}(L)$ is non trivial.

Let r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. One can verify that $\mathrm{EMLat}(r, L)$ is non trivial. Let L be an integral $\mathbb{Z}$-lattice. Observe that $\mathrm{EMLat}(L)$ is integral.

Now we state the propositions:

(20) Let us consider a $\mathbb{Z}$-lattice L.
Then $\mathrm{EMLat}(L)$ is a submodule of $\mathrm{DivisibleMod}(L)$.

(21) Let us consider a $\mathbb{Z}$-lattice L, and an element r of $\mathbb{F}_{\mathbb{Q}}$. Then $\mathrm{EMLat}(r, L)$ is a submodule of $\mathrm{DivisibleMod}(L)$.

(22) Let us consider a $\mathbb{Z}$-lattice L, a non zero element r of $\mathbb{F}_{\mathbb{Q}}$, elements m, n of $\mathbb{Z}^{\mathrm{R}}$, elements m, n_1 of $\mathbb{Z}$, and a vector v of $\mathrm{EMLat}(r, L)$. Suppose $m = m$ and $n = n_1$ and $r = \frac{m}{n_1}$ and $n_1 \neq 0$. Then there exists a vector x of $\mathrm{EMLat}(L)$ such that $n \cdot v = m \cdot x$. The theorem is a consequence of (20) and (21).

(23) Let us consider a $\mathbb{Z}$-lattice L, an element r of $\mathbb{F}_{\mathbb{Q}}$, vectors v, u of $\mathrm{EMLat}(r, L)$, and vectors x, y of $\mathrm{EMLat}(L)$. If $v = x$ and $u = y$, then $\langle v, u\rangle = \langle x, y\rangle$. The theorem is a consequence of (9) and (7).

(24) Let us consider an integral $\mathbb{Z}$-lattice L, a non zero element r of $\mathbb{F}_{\mathbb{Q}}$, a rational number a, and vectors v, u of $\mathrm{EMLat}(r, L)$. Suppose $r = a$. Then $a^{-1} \cdot a^{-1} \cdot \langle v, u\rangle \in \mathbb{Z}$. The theorem is a consequence of (22) and (23).

Let L be a positive definite $\mathbb{Z}$-lattice. One can verify that $\mathrm{EMLat}(L)$ is positive definite.

Let r be a non zero element of $\mathbb{F}_{\mathbb{Q}}$. Let us observe that $\mathrm{EMLat}(r, L)$ is positive definite.

Now we state the proposition:

(25) Let us consider a positive definite $\mathbb{Z}$-lattice L, and a vector v of $\mathrm{DivisibleMod}(L)$. Then $(\mathrm{ScProductDM}(L))(v, v) = 0$ if and only if $v = 0_{\mathrm{DivisibleMod}(L)}$. The theorem is a consequence of (6) and (7).

Let us consider a positive definite $\mathbb{Z}$-lattice L and a non empty structure of $\mathbb{Z}$-lattice Z over $\mathbb{Z}^{\mathrm{R}}$. Now we state the propositions:

(26) Suppose Z is a submodule of $\mathrm{DivisibleMod}(L)$ and the scalar product of $Z = \mathrm{ScProductDM}(L) \upharpoonright$ (the carrier of Z). Then Z is $\mathbb{Z}$-lattice-like.
Proof: For every vectors x, y of Z, (the scalar product of $Z)(x, y) = (\mathrm{ScProductDM}(L))(x, y)$ by [6, (49)]. Z is $\mathbb{Z}$-lattice-like by [11, (25), (26)], (25), (6). □

(27) Suppose Z is a finitely generated submodule of $\mathrm{DivisibleMod}(L)$ and the scalar product of $Z = \mathrm{ScProductDM}(L) \upharpoonright$ (the carrier of Z). Then Z is a $\mathbb{Z}$-lattice.

(28) Let us consider a $\mathbb{Z}$-lattice L.

Then the vector space structure of $\mathrm{EMLat}(L) = \mathrm{Embedding}(L)$.

(29) Let us consider $\mathbb{Z}$-modules L, E. Suppose the vector space structure of $L =$ the vector space structure of E. Then L is a submodule of E.

(30) Let us consider $\mathbb{Z}$-modules E, L, a subset I of L, a subset J of E, and a linear combination K of J. Suppose $I = J$ and the vector space structure of $L =$ the vector space structure of E. Then K is a linear combination of I.

Let us consider $\mathbb{Z}$-modules E, L, a linear combination K of E, and a linear combination H of L. Now we state the propositions:

(31) Suppose $K = H$ and the vector space structure of $L =$ the vector space structure of E. Then the support of $K =$ the support of H.

(32) Suppose $K = H$ and the vector space structure of $L =$ the vector space structure of E. Then $\sum K = \sum H$. The theorem is a consequence of (29).

Let us consider $\mathbb{Z}$-modules L, E, a subset I of L, and a subset J of E. Now we state the propositions:

(33) Suppose the vector space structure of $L =$ the vector space structure of E and $I = J$. Then I is linearly independent if and only if J is linearly independent. The theorem is a consequence of (30) and (32).

(34) Suppose the vector space structure of $L =$ the vector space structure of E and $I = J$. Then $\mathrm{Lin}(I) = \mathrm{Lin}(J)$. The theorem is a consequence of (29).

(35) Let us consider free $\mathbb{Z}$-modules L, E, a subset I of L, and a subset J of E. Suppose the vector space structure of $L =$ the vector space structure of E and $I = J$. Then I is a basis of L if and only if J is a basis of E. The theorem is a consequence of (33) and (34).

(36) Let us consider finite rank, free $\mathbb{Z}$-modules L, E. Suppose the vector space structure of $L =$ the vector space structure of E. Then $\operatorname{rank} L = \operatorname{rank} E$. The theorem is a consequence of (35).

Let us consider a $\mathbb{Z}$-lattice L and a subset I of L. Now we state the propositions:

(37) I is a basis of L if and only if $(\mathrm{MorphsZQ}(L))^{\circ} I$ is a basis of $\mathrm{Embedding}(L)$.

(38) I is a basis of L if and only if $(\mathrm{MorphsZQ}(L))^{\circ} I$ is a basis of $\mathrm{EMLat}(L)$. The theorem is a consequence of (37), (28), and (35).

(39) Let us consider a $\mathbb{Z}$-lattice L, and a finite sequence b of elements of L. Then b is an ordered basis of L if and only if $\mathrm{MorphsZQ}(L) \cdot b$ is an ordered basis of $\mathrm{Embedding}(L)$. The theorem is a consequence of (37).

(40) Let us consider a $\mathbb{Z}$-lattice L, a finite rank, free $\mathbb{Z}$-module E, a finite sequence I of elements of L, and a finite sequence J of elements of E.

Suppose the vector space structure of L = the vector space structure of E and $I = J$. Then I is an ordered basis of L if and only if J is an ordered basis of E. The theorem is a consequence of (35).

(41) Let us consider a $\mathbb{Z}$-lattice L, and a finite sequence b of elements of L. Then b is an ordered basis of L if and only if $\mathrm{MorphsZQ}(L)\cdot b$ is an ordered basis of $\mathrm{EMLat}(L)$. The theorem is a consequence of (39), (28), and (40).

(42) Let us consider a $\mathbb{Z}$-lattice L. Then $\operatorname{rank} L = \operatorname{rank} \mathrm{EMLat}(L)$. The theorem is a consequence of (28) and (36).

(43) Let us consider a $\mathbb{Z}$-lattice L, and an object x. Then x is a vector of $\mathrm{EMLat}(L)$ if and only if x is a vector of $\mathrm{Embedding}(L)$. The theorem is a consequence of (28).

Let L be a rational $\mathbb{Z}$-lattice and v, u be vectors of $\mathrm{EMLat}(L)$. One can check that $(\mathrm{ScProductEM}(L))(v, u)$ is rational.

Let v, u be vectors of $\mathrm{DivisibleMod}(L)$.

One can verify that $(\mathrm{ScProductDM}(L))(v, u)$ is rational.

3. Properties of Gram Matrix

Let V be a vector space structure over $\mathbb{Z}^{\mathrm{R}}$ and f be an $\mathbb{R}$-form of V and V. We say that f is symmetric if and only if

(Def. 6) for every vectors v, w of V, $f(v, w) = f(w, v)$.

Let V be a non empty vector space structure over $\mathbb{Z}^{\mathrm{R}}$. Let us observe that $\mathrm{NulFrForm}(V, V)$ is symmetric and there exists an $\mathbb{R}$-form of V and V which is symmetric and there exists an $\mathbb{R}$-bilinear form of V and V which is symmetric.

Let L be a $\mathbb{Z}$-lattice. Let us observe that $\mathrm{InnerProduct}\, L$ is symmetric.

Let V be a finite rank, free $\mathbb{Z}$-module, f be a symmetric $\mathbb{R}$-bilinear form of V and V, and b be an ordered basis of V. Let us note that $\mathrm{GramMatrix}(f, b)$ is symmetric.

Now we state the propositions:

(44) Let us consider a rational $\mathbb{Z}$-lattice L, and vectors v, u of $\mathrm{DivisibleMod}(L)$. Then $(\mathrm{ScProductDM}(L))(v, u) \in \mathbb{F}_{\mathbb{Q}}$.

(45) Let us consider a rational $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $\mathrm{GramMatrix}(b)$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L)$.

Proof: For every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of $\mathrm{GramMatrix}(b)$ holds $(\mathrm{GramMatrix}(b))_{i,j} \in$ the carrier of $\mathbb{F}_{\mathbb{Q}}$ by [8, (87)]. □

(46) Let us consider a finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$, and a finite sequence G of elements of $\mathbb{F}_{\mathbb{Q}}$. If $F = G$, then $\sum F = \sum G$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$ for every finite sequence G of elements of $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{len} F = \$_1$ and $F = G$ holds $\sum F = \sum G$. $\mathcal{P}[0]$ by [24, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(47) Let us consider a natural number i, an element j of $\mathbb{R}_{\mathrm{F}}$, and an element k of $\mathbb{F}_{\mathbb{Q}}$. Suppose $j = k$. Then $\operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, i) \cdot j = \operatorname{power}_{\mathbb{F}_{\mathbb{Q}}}(-\mathbf{1}_{\mathbb{F}_{\mathbb{Q}}}, i) \cdot k$. PROOF: Define $\mathcal{P}$[natural number] $\equiv \operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, \$_1) \cdot j = \operatorname{power}_{\mathbb{F}_{\mathbb{Q}}}(-\mathbf{1}_{\mathbb{F}_{\mathbb{Q}}}, \$_1) \cdot k$. $\mathcal{P}[0]$. 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]. □

(48) Let us consider a finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$. Suppose for every natural number i such that $i \in \operatorname{dom} F$ holds $F(i) \in \mathbb{F}_{\mathbb{Q}}$. Then $\sum F \in \mathbb{F}_{\mathbb{Q}}$. PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of $\mathbb{R}_{\mathrm{F}}$ such that $\operatorname{len} F = \$_1$ and for every natural number i such that $i \in \operatorname{dom} F$ holds $F(i) \in \mathbb{F}_{\mathbb{Q}}$ holds $\sum F \in \mathbb{F}_{\mathbb{Q}}$. $\mathcal{P}[0]$ by [24, (43)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(49) Let us consider a natural number i. Then $\operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, i) \in \mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (47).

(50) Let us consider natural numbers n, i, j, k, m, a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$, and a square matrix L over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$. Suppose $0 < n$ and $M = L$ and $\langle i, j \rangle \in$ the indices of M and $\langle k, m \rangle \in$ the indices of $\operatorname{Delete}(M, i, j)$. Then $(\operatorname{Delete}(M, i, j))_{k,m} = (\operatorname{Delete}(L, i, j))_{k,m}$.

(51) Let us consider natural numbers n, i, j, k, m, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose $0 < n$ and M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$ and $\langle i, j \rangle \in$ the indices of M and $\langle k, m \rangle \in$ the indices of $\operatorname{Delete}(M, i, j)$. Then $(\operatorname{Delete}(M, i, j))_{k,m}$ is an element of $\mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (50).

(52) Let us consider natural numbers n, i, j, a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$, and a square matrix L over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$. Suppose $0 < n$ and $M = L$ and $\langle i, j \rangle \in$ the indices of M. Then $\operatorname{Delete}(M, i, j) = \operatorname{Delete}(L, i, j)$. The theorem is a consequence of (50).

(53) Let us consider natural numbers n, i, j, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose $0 < n$ and M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$ and $\langle i, j \rangle \in$ the indices of M. Then $\operatorname{Delete}(M, i, j)$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. The theorem is a consequence of (52).

(54) Let us consider a natural number n, a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of

dimension n, and a square matrix H over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. If $M = H$, then $\operatorname{Det} M = \operatorname{Det} H$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $\$_1$ for every square matrix H over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\$_1$ such that $M = H$ holds $\operatorname{Det} M = \operatorname{Det} H$. $\mathcal{P}[0]$ by [21, (41)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [3, (14)], [20, (27)], [8, (87)], [13, (1)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(55) Let us consider a natural number n, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Suppose M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. Then $\operatorname{Det} M \in \mathbb{F}_{\mathbb{Q}}$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $\$_1$ such that M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\$_1$ holds $\operatorname{Det} M \in \mathbb{F}_{\mathbb{Q}}$. $\mathcal{P}[0]$ by [21, (41)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [3, (14)], [20, (27)], [8, (87)], [13, (41)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(56) Let us consider natural numbers n, i, j, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension $n+1$. Suppose M is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $n+1$ and $\langle i, j\rangle \in$ the indices of M. Then $\operatorname{Cofactor}(M, i, j) \in \mathbb{F}_{\mathbb{Q}}$.

PROOF: Reconsider $D_1 = \operatorname{Delete}(M, i, j)$ as a square matrix over $\mathbb{R}_{\mathrm{F}}$ of dimension n. $\operatorname{Det} D_1 \in \mathbb{F}_{\mathbb{Q}}$ by (53), (55), [21, (41)]. $\operatorname{power}_{\mathbb{R}_{\mathrm{F}}}(-\mathbf{1}_{\mathbb{R}_{\mathrm{F}}}, i+j) \in \mathbb{F}_{\mathbb{Q}}$. □

(57) Let us consider a rational $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $\operatorname{Det} \operatorname{GramMatrix}(b) \in \mathbb{F}_{\mathbb{Q}}$. The theorem is a consequence of (45) and (55).

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

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every vector u of L for every finite subset J of L such that $J \subseteq I$ and $\overline{\overline{J}} = \$_1$ and $u \in \operatorname{Lin}(J)$ holds $\langle u, v\rangle = \langle u, w\rangle$. $\mathcal{P}[0]$ by [27, (9)], [25, (35)], [9, (12)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [28, (41)], [2, (44)], [1, (30)], [27, (7)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(59) Let us consider a positive definite $\mathbb{Z}$-lattice L, an ordered basis b of L, and vectors v, w of L. Suppose for every natural number n such that $n \in \operatorname{dom} b$ holds $\langle b_n, v\rangle = \langle b_n, w\rangle$. Then $v = w$.

PROOF: Reconsider $I = \operatorname{rng} b$ as a basis of L. For every vector u of L such that $u \in I$ holds $\langle u, v\rangle = \langle u, w\rangle$ by [5, (10)]. $\langle v - w, v\rangle = \langle v - w, w\rangle$. □

(60) Let us consider a natural number n, and a square matrix M over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. Suppose M is without repeated line. Then $\operatorname{Det} M \neq 0_{\mathbb{F}_{\mathbb{Q}}}$ if and only if lines(M) is linearly independent.

(61) Let us consider a positive definite $\mathbb{Z}$-lattice L, a basis I of L, and vectors v, w of L. Suppose for every vector u of L such that $u \in I$ holds $\langle v, u\rangle = \langle w, u\rangle$. Let us consider a vector u of L. Then $\langle v, u\rangle = \langle w, u\rangle$. The theorem is a consequence of (58).

(62) Let us consider a positive definite $\mathbb{Z}$-lattice L, an ordered basis b of L, and vectors v, w of L. Suppose for every natural number n such that $n \in \operatorname{dom} b$ holds $\langle v, b_n\rangle = \langle w, b_n\rangle$. Then $v = w$. The theorem is a consequence of (59).

Let us consider a positive definite $\mathbb{Z}$-lattice L, an ordered basis b of $\mathrm{EMLat}(L)$, and vectors v, w of $\mathrm{DivisibleMod}(L)$. Now we state the propositions:

(63) If for every natural number n such that $n \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(b_n, v) = (\mathrm{ScProductDM}(L))(b_n, w)$, then $v = w$.
PROOF: Consider i being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $i \neq 0$ and $i \cdot v \in \mathrm{Embedding}(L)$. Consider j being an element of $\mathbb{Z}^{\mathrm{R}}$ such that $j \neq 0$ and $j \cdot w \in \mathrm{Embedding}(L)$. Reconsider $i_1 = i \cdot v$ as a vector of $\mathrm{EMLat}(L)$. Reconsider $j_1 = j \cdot w$ as a vector of $\mathrm{EMLat}(L)$. $\mathrm{EMLat}(L)$ is a submodule of $\mathrm{DivisibleMod}(L)$. For every natural number n such that $n \in \operatorname{dom} b$ holds $\langle b_n, j \cdot i_1\rangle = \langle b_n, i \cdot j_1\rangle$ by [11, (24)], (6), (8). $j \cdot i_1 = i \cdot j_1$. □

(64) If for every natural number n such that $n \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(v, b_n) = (\mathrm{ScProductDM}(L))(w, b_n)$, then $v = w$.
PROOF: For every natural number n such that $n \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(b_n, v) = (\mathrm{ScProductDM}(L))(b_n, w)$ by (20), [11, (24)], (6). □

(65) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice L, an element v of L, a finite sequence b of elements of L, and a finite sequence s of elements of $\mathbb{F}_{\mathbb{Q}}$. Suppose $\operatorname{len} b = \operatorname{len} s$ and for every natural number n such that $n \in \operatorname{dom} s$ holds $s(n) = \langle b_n, v\rangle$. Then $\langle \sum b, v\rangle = \sum s$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence F of elements of L for every finite sequence F_1 of elements of $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{len} F = \$_1$ and $\operatorname{len} F = \operatorname{len} F_1$ and for every natural number i such that $i \in \operatorname{dom} F_1$ holds $F_1(i) = \langle F_i, v\rangle$ holds $\langle \sum F, v\rangle = \sum F_1$. $\mathcal{P}[0]$ by [24, (43)], [9, (12)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(66) Let us consider a natural number n, and a finite sequence r of elements of $\mathbb{F}_{\mathbb{Q}}$. Suppose $\operatorname{len} r = n$. Then there exists an integer K and there exists a finite sequence K_2 of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $K \neq 0$ and $\operatorname{len} K_2 = n$ and for every natural number i such that $i \in \operatorname{dom} K_2$ holds $K_2(i) = K \cdot r_i$.
PROOF: Consider K being an integer such that $K \neq 0$ and for every natural number i such that $i \in \operatorname{Seg} n$ holds $K \cdot r_i \in \mathbb{Z}$. Define $\mathcal{Q}$[natural

number, object] $\equiv$ \$2 $= K \cdot r_{\$_1}$. For every natural number i such that $i \in \operatorname{Seg} n$ there exists an element x of the carrier of $\mathbb{Z}^{\mathrm{R}}$ such that $\mathcal{Q}[i, x]$. Consider K_2 being a finite sequence of elements of the carrier of $\mathbb{Z}^{\mathrm{R}}$ such that $\operatorname{dom} K_2 = \operatorname{Seg} n$ and for every natural number k such that $k \in \operatorname{Seg} n$ holds $\mathcal{Q}[k, K_2(k)]$ from [4, Sch. 5]. □

(67) Let us consider natural numbers i, j, a field K, elements a, a_1 of K, and an element R of the i-dimension vector space over K. If $j \in \operatorname{Seg} i$ and $a_1 = R(j)$, then $(a \cdot R)(j) = a \cdot a_1$.

(68) Let us consider natural numbers i, j, a field K, elements a_1, b_2 of K, and elements A, B of the i-dimension vector space over K. Suppose $j \in \operatorname{Seg} i$ and $a_1 = A(j)$ and $b_2 = B(j)$. Then $(A + B)(j) = a_1 + b_2$.

(69) Let us consider a field K, and natural numbers n, i. Suppose $i \in \operatorname{Seg} n$. Let us consider a finite sequence s of elements of the n-dimension vector space over K. Then there exists a finite sequence s_1 of elements of K such that

(i) $\operatorname{len} s_1 = \operatorname{len} s$, and

(ii) $(\sum s)(i) = \sum s_1$, and

(iii) for every natural number k such that $k \in \operatorname{dom} s_1$ holds $s_1(k) = s_k(i)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite sequence s of elements of the n-dimension vector space over K such that $\operatorname{len} s =$ \$1 there exists a finite sequence s_1 of elements of K such that $\operatorname{len} s_1 = \operatorname{len} s$ and $(\sum s)(i) = \sum s_1$ and for every natural number k such that $k \in \operatorname{dom} s_1$ holds $s_1(k) = s_k(i)$. $\mathcal{P}[0]$ by [22, (7)], [24, (43)]. For every natural number k such that $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number k, $\mathcal{P}[k]$ from [3, Sch. 2]. □

(70) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $\operatorname{Det} \operatorname{GramMatrix}(b) \neq 0_{\mathbb{R}_{\mathrm{F}}}$.

Proof: Reconsider $M = \operatorname{GramMatrix}(b)$ as a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\operatorname{rank} L$. $\operatorname{Det} M = 0_{\mathbb{F}_{\mathbb{Q}}}$. M is one-to-one by [13, (49)], [8, (87)], (59). Reconsider $M_1 = M$ as a finite sequence of elements of the $\operatorname{rank} L$-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$. Consider r being a finite sequence of elements of $\mathbb{F}_{\mathbb{Q}}$, r_1 being a finite sequence of elements of the $\operatorname{rank} L$-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{len} r = \operatorname{rank} L$ and $\operatorname{len} r_1 = \operatorname{rank} L$ and for every natural number i such that $i \in \operatorname{dom} r_1$ holds $r_1(i) = r_i \cdot M_{1i}$ and $\sum r_1 = 0_\alpha$ and $r \neq \operatorname{Seg} \operatorname{len} r \longmapsto 0_{\mathbb{F}_{\mathbb{Q}}}$, where α is the $\operatorname{rank} L$-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$. Consider K being an integer, K_2 being a finite sequence of elements of $\mathbb{Z}^{\mathrm{R}}$ such that $K \neq 0$ and $\operatorname{len} K_2 = \operatorname{rank} L$ and for every natural number i such that $i \in \operatorname{dom} K_2$ holds $K_2(i) = K \cdot r_i$. Reconsider $K_1 = K$ as an element of $\mathbb{F}_{\mathbb{Q}}$. Define $\mathcal{P}$[natural number, object] $\equiv$

there exists an element r_2 of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $r_2 = r_1(\$_1)$ and $\$_2 = K_1 \cdot r_2$. For every natural number k such that $k \in \operatorname{Seg}\operatorname{rank} L$ there exists an element x of the carrier of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $\mathcal{P}[k, x]$. Consider K_3 being a finite sequence of elements of the carrier of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $\operatorname{dom} K_3 = \operatorname{Seg}\operatorname{rank} L$ and for every natural number k such that $k \in \operatorname{Seg}\operatorname{rank} L$ holds $\mathcal{P}[k, K_3(k)]$ from [4, Sch. 5]. For every natural number i such that $i \in \operatorname{dom} K_3$ there exists an element M_2 of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ and there exists an element K_5 of $\mathbb{F}_{\mathbb{Q}}$ such that $M_2 = M_1(i)$ and $K_5 = K_2(i)$ and $K_3(i) = K_5 \cdot M_2$. For every natural number k and for every element v of the rank L-dimension vector space over $\mathbb{F}_{\mathbb{Q}}$ such that $k \in \operatorname{dom} K_3$ and $v = r_1(k)$ holds $K_3(k) = K_1 \cdot v$. $K_2 \neq \operatorname{Seg}\operatorname{len} K_2 \longmapsto 0_{\mathbb{Z}^{\mathrm{R}}}$ by [22, (7)]. Set $S = \sum K_3$. For every natural number n such that $n \in \operatorname{dom} b$ holds $S(n) = 0_{\mathbb{Z}^{\mathrm{R}}}$ by [22, (7)]. Define $\mathcal{Q}[\text{natural number}, \text{object}] \equiv \$_2 = K_{2\$_1} \cdot b_{\$_1}$. Consider K_4 being a finite sequence of elements of the carrier of L such that $\operatorname{dom} K_4 = \operatorname{Seg}\operatorname{rank} L$ and for every natural number k such that $k \in \operatorname{Seg}\operatorname{rank} L$ holds $\mathcal{Q}[k, K_4(k)]$ from [4, Sch. 5]. For every natural number n such that $n \in \operatorname{dom} b$ holds $S(n) = \langle \sum K_4, b_n \rangle$ by (69), [19, (102)], [8, (87)], (67). For every natural number n such that $n \in \operatorname{dom} b$ holds $\langle 0_L, b_n \rangle = \langle \sum K_4, b_n \rangle$ by [9, (12)]. $\sum K_4 = 0_L$. $\operatorname{rng} b$ is linearly dependent. □

Let L be a non trivial, rational, positive definite $\mathbb{Z}$-lattice and b be an ordered basis of L. Let us observe that GramMatrix(b) is invertible.

REFERENCES

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

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

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

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

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

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

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

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

[9] Yuichi Futa and Yasunari Shidama. Lattice of $\mathbb{Z}$-module. *Formalized Mathematics*, 24 (**1**):49–68, 2016. doi:10.1515/forma-2016-0005.

[10] Yuichi Futa and Yasunari Shidama. Divisible $\mathbb{Z}$-modules. *Formalized Mathematics*, 24 (**1**):37–47, 2016. doi:10.1515/forma-2016-0004.

[11] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathe-*

matics, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[12] 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.

[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] Adam Grabowski, Artur Korniłowicz, and Adam Naumowicz. Four decades of Mizar. *Journal of Automated Reasoning*, 55(3):191–198, 2015. doi:10.1007/s10817-015-9345-1.

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

[16] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982. doi:10.1007/BF01457454.

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

[18] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(**1**):3–11, 1991.

[19] Karol Pąk. Basic properties of the rank of matrices over a field. *Formalized Mathematics*, 15(**4**):199–211, 2007. doi:10.2478/v10037-007-0024-5.

[20] Karol Pąk and Andrzej Trybulec. Laplace expansion. *Formalized Mathematics*, 15(**3**): 143–150, 2007. doi:10.2478/v10037-007-0016-5.

[21] 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.

[22] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1 (**2**):329–334, 1990.

[23] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

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

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

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

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

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

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

Received March 17, 2017