Embedded Lattice and Properties of Gram Matrix

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in Mizar\cite{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\cite{16} and cryptographic systems with lattice\cite{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 \(\text{rng } F = A\) and \(F_1\) is one-to-one and \(\text{rng } F_1 = A\). Then \(\sum (L \cdot F) = \sum (L \cdot F_1)\).

Proof: Define \(G[\text{object, object}] \equiv \{s_2\} = F^{-1}(\{F_1(s_1)\})\). For every object \(x\) such that \(x \in \text{dom } F\) there exists an object \(y\) such that \(y \in \text{dom } F\) and \(G[x, y]\) by \([6, (74)]\). Consider \(f\) being a function from \(\text{dom } F\) into \(\text{dom } F\) such that for every object \(x\) such that \(x \in \text{dom } F\) holds \(G[x, f(x)]\) from \([7, \text{Sch.~1}]\). \(\text{rng } f = \text{dom } F\) by \([6, (59), (82)], [8, (18)]\). \(f\) is one-to-one by \([8, (31)], [6, (91)], [8, (3)]\). \(\Box\)

This work was supported by JSPS KAKENHI Grant Number JP15K00183.

© 2017 University of Białystok

CC-BY-SA License ver. 3.0 or later

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

Brought to you by | Biblioteka Uniwersytecka w Białymstoku

Authenticated

Download Date | 6/5/17 10:36 AM
Let us consider a ring $K$, a left module $V$ over $K$, and a finite subset $\mathcal{A}$ of $V$. Then $\mathcal{A}$ is linearly independent if and only if for every linear combination $L$ of $\mathcal{A}$ such that there exists a finite sequence $F$ of elements of the carrier of $V$ such that $F$ is one-to-one and $\text{rng} F = \mathcal{A}$ and $\sum (L \cdot F) = 0_V$ holds the support of $L = \emptyset$.

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

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 $\text{rng} b$ 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 $\text{len} r = \text{len} b$ and $\text{len} r_1 = \text{len} b$ and for every natural number $i$ such that $i \in \text{dom} r_1$ holds $r_1(i) = r_i \cdot b_i$ and $\sum r_1 = 0_V$ holds $r = \text{Seg} \text{len} r \mapsto 0_K$.

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

Let us consider a ring $K$, a left module $V$ over $K$, and a finite subset $\mathcal{A}$ of $V$. Then $\mathcal{A}$ 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 $\text{rng} b = \mathcal{A}$ and for every finite sequence $r$ of elements of $K$ and for every finite sequence $r_1$ of elements of $V$ such that $\text{len} r = \text{len} b$ and $\text{len} r_1 = \text{len} b$ and for every natural number $i$ such that $i \in \text{dom} r_1$ holds $r_1(i) = r_i \cdot b_i$ and $\sum r_1 = 0_V$ holds $r = \text{Seg} \text{len} r \mapsto 0_K$. 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 $\text{ScProductEM}(L)$ yielding a function from (the carrier of $\text{Embedding}(L)$) $\times$ (the carrier of $\text{Embedding}(L)$) into the carrier of $\mathbb{R}_F$ is defined by

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

Now we state the proposition:
(5) Let us consider a $\mathbb{Z}$-lattice $L$. Then

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

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

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

**Proof:** Set $Z = \text{Embedding}(L)$. Set $f = \text{ScProductEM}(L)$. 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 $\mathbb{Z}^R$, $f(x + y, z) = f(x, z) + f(y, z)$ and $f(a \cdot x, y) = a \cdot f(x, y)$ by [10] (22), (19). □

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

(Def. 3) for every vectors $v_1, u_1$ of $\text{DivisibleMod}(L)$ and for every vectors $v, u$ of $\text{Embedding}(L)$ and for every elements $a, b$ of $\mathbb{Z}^R$ and for every elements $a_1, b_1$ of $\mathbb{R}_F$ 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$(v_1, u_1) = a_1^{-1} \cdot b_1^{-1} \cdot (\text{ScProductEM}(L))(v, u)$.

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

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

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

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

**Proof:** Set $D = \text{DivisibleMod}(L)$. Set $f = \text{ScProductDM}(L)$. 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 $\mathbb{Z}^R$, $f(x + y, z) = f(x, z) + f(y, z)$ and $f(i \cdot x, y) = i \cdot f(x, y)$ by \cite{10} (29), \cite{11} (29), (28), \cite{18} (11)].

(7) $\text{ScProductEM}(L) = \text{ScProductDM}(L) \upharpoonright \text{rng MorphsZQ}(L)$.

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

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

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

(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 (the carrier of $\mathbb{Z}^R \times A$ into $A$, and a function $s_1$ from $A \times A$ into the carrier of $\mathbb{R}_F$. Suppose $A$ is a linearly closed subset of $\text{DivisibleMod}(L)$ and $z = 0_{\text{DivisibleMod}(L)}$ and $a_1 = (\text{the addition of } \text{DivisibleMod}(L)) \upharpoonright A$ and $m_1 = (\text{the left multiplication of } \text{DivisibleMod}(L)) \upharpoonright ((\text{the carrier of } \mathbb{Z}^R) \times A)$. Then $\langle A, a_1, z, m_1, s_1 \rangle$ is a submodule of $\text{DivisibleMod}(L)$.

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

\begin{enumerate}
  \item (\text{ScProductDM}(L))(\overline{v}, u) = - (\text{ScProductDM}(L))(v, u), and
  \item (\text{ScProductDM}(L))(u, \overline{v}) = - (\text{ScProductDM}(L))(u, v).
\end{enumerate}

The theorem is a consequence of (6).

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

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

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

\begin{enumerate}
  \item (\text{ScProductDM}(L))(0_{\text{DivisibleMod}(L)}, v) = 0, and
  \item (\text{ScProductDM}(L))(v, 0_{\text{DivisibleMod}(L)}) = 0.
\end{enumerate}

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

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

\cite{10} (29), \cite{11} (29), (28), \cite{18} (11).
that $u \in I$ holds $(\text{ScProductDM}(L))(v, u) = 0$. Let us consider a vector $u$

of $\text{DivisibleMod}(L)$. Then $(\text{ScProductDM}(L))(v, u) = 0$.

PROOF: Define $\mathcal{P}[\text{natural number}] \equiv$ for every finite subset $I$ of Embedding

$(L)$ such that $\overline{I} = \$1$ and $I$ is linearly independent and for every vector $u$

of $\text{DivisibleMod}(L)$ such that $u \in I$ holds $(\text{ScProductDM}(L))(v, u) = 0$. $\mathcal{P}[0]$ 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 $[3, \text{Sch. 2}]$. For

every vector $w$ of $\text{DivisibleMod}(L)$, $(\text{ScProductDM}(L))(v, w) = 0$ by $[10,$

(29)], (6). $\Box$

(16) Let us consider a $\mathbb{Z}$-lattice $L$, a vector $v$ of $\text{DivisibleMod}(L)$, and a basis $I$

of Embedding($L$). Suppose for every vector $u$ of $\text{DivisibleMod}(L)$ such that $u \in I$ holds $(\text{ScProductDM}(L))(v, u) = 0$. Then $v = 0_{\text{DivisibleMod}(L)}$. 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 $u \in \text{Lin}(\{v\})$. 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 $v \in \text{Lin}(\{v\})$.

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

2. EMBEDDING OF LATTICE

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

(Def. 4) the carrier of $it = \text{rng MorphsZQ}(L)$ and the zero of $it = \text{zeroCoset}(L)$ and

the addition of $it = \text{addCoset}(L) \upharpoonright \text{rng MorphsZQ}(L)$ and the left

multiplication of $it = \text{lmultCoset}(L) \upharpoonright ((\text{the carrier of } \mathbb{Z}^R) \times \text{rng MorphsZQ}

(L))$ and the scalar product of $it = \text{ScProductEM}(L)$.

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

(Def. 5) the carrier of $it = r \cdot \text{rng MorphsZQ}(L)$ and the zero of $it = \text{zeroCoset}(L)$ and

the addition of $it = \text{addCoset}(L) \upharpoonright (r \cdot \text{rng MorphsZQ}(L))$ and the left

multiplication of $it = \text{lmultCoset}(L) \upharpoonright ((\text{the carrier of } \mathbb{Z}^R) \times (r \cdot \text{rng MorphsZQ}

(L)))$ and the scalar product of $it = \text{ScProductDM}(L) \upharpoonright (r \cdot \text{rng MorphsZQ}

(L))$. 

Brought to you by | Biblioteka Uniwersytecka w Białymstoku
Authenticated
Download Date | 6/5/17 10:36 AM
Let $L$ be a non trivial $\mathbb{Z}$-lattice. One can verify that $\text{EMLat}(L)$ is non trivial.
Let $r$ be a non zero element of $\mathbb{F}_q$. One can verify that $\text{EMLat}(r, L)$ is non trivial. Let $L$ be an integral $\mathbb{Z}$-lattice. Observe that $\text{EMLat}(L)$ is integral.

Now we state the propositions:

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

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

(22) Let us consider a $\mathbb{Z}$-lattice $L$, a non zero element $r$ of $\mathbb{F}_q$, elements $m$, $n$ of $\mathbb{Z}^R$, elements $m, n_1$ of $\mathbb{Z}$, and a vector $v$ of $\text{EMLat}(r, L)$. 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 $\text{EMLat}(L)$ 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 $\mathbb{F}_q$, vectors $v, u$ of $\text{EMLat}(r, L)$, and vectors $x, y$ of $\text{EMLat}(L)$. 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 $\mathbb{F}_q$, a rational number $a$, and vectors $v, u$ of $\text{EMLat}(r, L)$. Suppose $r = a$.
Then $a^{-1}.a^{-1}.\langle v, u \rangle \in \mathbb{Z}$. The theorem is a consequence of (22) and (23).

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

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

Now we state the proposition:

(25) Let us consider a positive definite $\mathbb{Z}$-lattice $L$, and a vector $v$ of $\text{DivisibleMod}(L)$. Then $\langle v, v \rangle = 0$ if and only if $v = 0_{\text{DivisibleMod}(L)}$.
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 $\mathbb{Z}^R$. Now we state the propositions:

(26) Suppose $Z$ is a submodule of $\text{DivisibleMod}(L)$ and the scalar product of $Z = \text{ScProductDM}(L)$ \upharpoonright (the carrier of $Z$). Then $Z$ is $\mathbb{Z}$-lattice-like.

**Proof:** For every vectors $x, y$ of $Z$, (the scalar product of $Z$)$\langle x, y \rangle = (\text{ScProductDM}(L))(x, y)$ by \cite[49]{6}. $Z$ is $\mathbb{Z}$-lattice-like by \cite[25]{11}, (25), (26), (25), (6). \quad \square

(27) Suppose $Z$ is a finitely generated submodule of $\text{DivisibleMod}(L)$ and the scalar product of $Z = \text{ScProductDM}(L)$ \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 $\text{EMLat}(L) = \text{Embedding}(L)$.

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

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

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

(33) Suppose the vector space structure of $L$ is 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 $L$ is the vector space structure of $E$ and $I = J$. Then $\text{Lin}(I) = \text{Lin}(J)$. 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 $L$ is 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 $L$ is the vector space structure of $E$. Then $\text{rank } L = \text{rank } E$. 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 $\text{MorphsZQ}(L)^{\circ} I$ is a basis of $\text{Embedding}(L)$.

(38) $I$ is a basis of $L$ if and only if $\text{MorphsZQ}(L)^{\circ} I$ is a basis of $\text{EMLat}(L)$. 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 $\text{MorphsZQ}(L) \cdot b$ is an ordered basis of $\text{Embedding}(L)$. 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 $E$. The theorem is a consequence of (37).
Suppose the vector space structure of $L$ is 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 $\text{MorphsZQ}(L) \cdot b$ is an ordered basis of $\text{EMLat}(L)$. The theorem is a consequence of (39), (28), and (40).

(42) Let us consider a $\mathbb{Z}$-lattice $L$. Then $\text{rank } L = \text{rank } \text{EMLat}(L)$. 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 $\text{EMLat}(L)$ if and only if $x$ is a vector of $\text{Embedding}(L)$. The theorem is a consequence of (28).

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

Let $v, u$ be vectors of $\text{DivisibleMod}(L)$.
One can verify that $(\text{ScProductDM}(L))(v, u)$ is rational.

3. Properties of Gram Matrix

Let $V$ be a vector space structure over $\mathbb{Z}^\mathbb{R}$ 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 $\mathbb{Z}^\mathbb{R}$. Let us observe that $\text{NulFrForm}(V, V)$ 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 $\text{InnerProduct } L$ 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 $\text{GramMatrix}(f, b)$ is symmetric.

Now we state the propositions:

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

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

PROOF: For every natural numbers $i, j$ such that $\langle i, j \rangle$ is the indices of $\text{GramMatrix}(b)$ holds $(\text{GramMatrix}(b))_{i,j} \in \text{the carrier of } \mathbb{F}_Q$ by $\mathbb{S}$ (87).
\[\Box\]

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

Let us consider a natural number $i$. Then \( \text{power}_{\mathbb{R}_F}(-1_{\mathbb{R}_F}, i) \cdot j = \text{power}_{\mathbb{F}_Q}(-1_{\mathbb{F}_Q}, i) \cdot k. \)

Let us consider a natural number $n$. Then \( \text{power}_{\mathbb{R}_F}(-1_{\mathbb{R}_F}, n) \cdot j = \text{power}_{\mathbb{F}_Q}(-1_{\mathbb{F}_Q}, n) \cdot k. \)

 Proof: Define \( \mathcal{P}[\text{natural number}] \equiv \) for every finite sequence \( F \) of elements of \( \mathbb{F}_Q \) such that \( \text{len} F = n \) 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. □

Proof: Define \( \mathcal{P}[\text{natural number}] \equiv \) for every finite sequence \( F \) of elements of \( \mathbb{F}_Q \) such that \( \text{len} F = n \) and for every natural number \( i \) such that \( i \in \text{dom} F \) holds \( F(i) \in \mathbb{F}_Q. \) Then \( \sum F \in \mathbb{F}_Q. \)

Let us consider natural numbers \( n, i, j, k, m, \) a square matrix \( M \) over \( \mathbb{F}_F \) of dimension \( n+1, \) and a square matrix \( L \) over \( \mathbb{F}_Q \) 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 \( \text{Delete}(M, i, j). \) Then \( \langle \text{Delete}(M, i, j) \rangle_{k,m} = \langle \text{Delete}(L, i, j) \rangle_{k,m}. \)

Proof: Define \( \mathcal{P}[\text{natural number}] \equiv \) for every finite sequence \( F \) of elements of \( \mathbb{F}_Q \) such that \( \text{len} F = n \) and for every natural number \( i \) such that \( i \in \text{dom} F \) holds \( F(i) \in \mathbb{F}_Q. \) Then \( \sum F \in \mathbb{F}_Q. \)

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

Let us consider natural numbers \( n, i, j, k, m, \) a square matrix \( M \) over \( \mathbb{F}_F \) of dimension \( n+1. \) Suppose \( 0 < n \) and \( M \) is a square matrix over \( \mathbb{F}_Q \) of dimension \( n+1 \) and \( \langle i, j \rangle \in \) the indices of \( M. \) Then \( \text{Delete}(M, i, j) = \text{Delete}(L, i, j). \) The theorem is a consequence of (50).

Let us consider a natural number \( n, i, j, k, m, \) a square matrix \( M \) over \( \mathbb{F}_F \) of dimension \( n+1. \) Suppose \( 0 < n \) and \( M \) is a square matrix over \( \mathbb{F}_Q \) of dimension \( n+1 \) and \( \langle i, j \rangle \in \) the indices of \( M. \) Then \( \text{Delete}(M, i, j) \) is a square matrix over \( \mathbb{F}_Q \) of dimension \( n. \) The theorem is a consequence of (52).

Let us consider a natural number \( n, i, j, k, m, \) a square matrix \( M \) over \( \mathbb{F}_F \) of dimension \( n+1. \) Suppose \( 0 < n \) and \( M \) is a square matrix over \( \mathbb{F}_Q \) of dimension \( n+1 \) and \( \langle i, j \rangle \in \) the indices of \( M. \) Then \( \text{Delete}(M, i, j) \) is a square matrix over \( \mathbb{F}_Q \) of dimension \( n. \) The theorem is a consequence of (52).
dimension \(n\), and a square matrix \(H\) over \(\mathbb{F}_Q\) of dimension \(n\). If \(M = H\), then \(\text{Det} M = \text{Det} H\).

**Proof:** Define \(\mathcal{P}[\text{natural number}] \equiv \) for every square matrix \(M\) over \(\mathbb{R}_F\) of dimension \(s_1\) for every square matrix \(H\) over \(\mathbb{F}_Q\) of dimension \(s_1\) such that \(M = H\) holds \(\text{Det} M = \text{Det} H\). \(\mathcal{P}[0] \) 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 \(\mathbb{R}_F\) of dimension \(n\). Suppose \(M\) is a square matrix over \(\mathbb{F}_Q\) of dimension \(n\). Then \(\text{Det} M \in \mathbb{F}_Q\).

**Proof:** Reconsider \(D_1 = \text{Delete}(M, i, j)\) as a square matrix over \(\mathbb{R}_F\) of dimension \(n\). \(\text{Det} D_1 \in \mathbb{F}_Q\) by (53), (55), \([21]\) (41)]. \(\text{power}_{\mathbb{R}_F}(-1_{\mathbb{R}_F}, i+j) \in \mathbb{F}_Q\). □

(56) Let us consider natural numbers \(n, i, j\), and a square matrix \(M\) over \(\mathbb{R}_F\) of dimension \(n + 1\). Suppose \(M\) is a square matrix over \(\mathbb{F}_Q\) of dimension \(n + 1\) and \(\{i, j\} \in \) the indices of \(M\). Then \(\text{Cofactor}(M, i, j) \in \mathbb{F}_Q\).

**Proof:** Reconsider \(D_1 = \text{Delete}(M, i, j)\) as a square matrix over \(\mathbb{R}_F\) of dimension \(n\). \(\text{Det} D_1 \in \mathbb{F}_Q\) by (53), (55), \([21]\) (41)]. \(\text{power}_{\mathbb{R}_F}(-1_{\mathbb{R}_F}, i+j) \in \mathbb{F}_Q\). □

(57) Let us consider a rational \(\mathbb{Z}\)-lattice \(L\), and an ordered basis \(b\) of \(L\). Then \(\text{Det} \text{GramMatrix}(b) \in \mathbb{F}_Q\). 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 \(\mathcal{P}[\text{natural number}] \equiv \) for every vector \(u\) of \(L\) for every finite subset \(J\) of \(L\) such that \(J \subseteq I\) and \(\overline{J} = \{1\} \cup u \in \text{Lin}(J)\) 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 \(n \in \text{dom} b\) holds \(\langle b_n, v \rangle = \langle b_n, w \rangle\). Then \(v = w\).

**Proof:** Reconsider \(I = \text{rng} b\) 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 \(\mathbb{F}_Q\) of dimension \(n\). Suppose \(M\) is without repeated line. Then \(\text{Det} M \neq 0_{\mathbb{F}_Q}\) if and only if \(\text{lines}(M)\) is linearly independent.
(61) Let us consider a positive definite \( Z \)-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 \( Z \)-lattice \( L \), an ordered basis \( b \) of \( L \), and vectors \( v, w \) of \( L \). Suppose for every natural number \( n \) such that \( n \in \text{dom} \ b \) 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 \( Z \)-lattice \( L \), an ordered basis \( b \) of \( EMLat(L) \), and vectors \( v, w \) of \( \text{DivisibleMod}(L) \). Now we state the propositions:

(63) If for every natural number \( n \) such that \( n \in \text{dom} \ b \) holds

\[
(\text{ScProductDM}(L))(b_n, v) = (\text{ScProductDM}(L))(b_n, w), \text{ then } v = w.
\]

**Proof:** Consider \( i \) being an element of \( Z^R \) such that \( i \neq 0 \) and \( i \cdot v \in \text{Embedding}(L) \). Consider \( j \) being an element of \( Z^R \) such that \( j \neq 0 \) and \( j \cdot w \in \text{Embedding}(L) \). Reconsider \( i_1 = i \cdot v \) as a vector of \( EMLat(L) \). Reconsider \( j_1 = j \cdot w \) as a vector of \( EMLat(L) \). \( EMLat(L) \) is a submodule of \( \text{DivisibleMod}(L) \). For every natural number \( n \) such that \( n \in \text{dom} \ b \) 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 \( n \in \text{dom} \ b \) holds

\[
(\text{ScProductDM}(L))(v, b_n) = (\text{ScProductDM}(L))(w, b_n), \text{ then } v = w.
\]

**Proof:** For every natural number \( n \) such that \( n \in \text{dom} \ b \) holds

\[
(\text{ScProductDM}(L))(b_n, v) = (\text{ScProductDM}(L))(b_n, w) \text{ by (20), [11, (24)], (6).} \]

□

(65) Let us consider a non trivial, rational, positive definite \( Z \)-lattice \( L \), an element \( v \) of \( L \), a finite sequence \( b \) of elements of \( L \), and a finite sequence \( s \) of elements of \( \mathbb{F}_Q \). Suppose \( \text{len} \ b = \text{len} \ s \) and for every natural number \( n \) such that \( n \in \text{dom} \ s \) holds \( s(n) = \langle b_n, v \rangle \). Then \( \langle \sum b, v \rangle = \sum s \).

**Proof:** Define \( P[\text{natural number}] \equiv \) for every finite sequence \( F \) of elements of \( L \) for every finite sequence \( F_1 \) of elements of \( \mathbb{F}_Q \) such that \( \text{len} \ F = \$1 \) and \( \text{len} \ F_1 = \text{len} \ F \) and for every natural number \( i \) such that \( i \in \text{dom} \ F_1 \) holds \( F_1(i) = \langle F_i, v \rangle \) holds \( \sum F; v \) holds \( \sum F_1. P[0] \) by [24, (43)], [9, (12)]. For every natural number \( n \) such that \( P[n] \) holds \( P[n+1] \) by [4, (4)], [6, (3)], [4, (59)], [3, (11)]. For every natural number \( n \), \( P[n] \) from [3, Sch. 2]. □

(66) Let us consider a natural number \( n \), and a finite sequence \( r \) of elements of \( \mathbb{F}_Q \). Suppose \( \text{len} \ r = n \). Then there exists an integer \( K \) and there exists a finite sequence \( K_2 \) of elements of \( Z^R \) such that \( K \neq 0 \) and \( \text{len} \ K_2 = n \) and for every natural number \( i \) such that \( i \in \text{dom} \ K_2 \) 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 \( i \in \text{Seg} \ n \) holds \( K \cdot r_i \in \mathbb{Z} \). Define \( Q[\text{natural}}
number, object] ≡ $\exists_2 = K \cdot r_{S_1}$. For every natural number $i$ such that $i \in \text{Seg} n$ there exists an element $x$ of the carrier of $\mathbb{Z}^R$ such that $Q[i, x]$. Consider $K_2$ being a finite sequence of elements of the carrier of $\mathbb{Z}^R$ such that $\text{dom} K_2 = \text{Seg} n$ and for every natural number $k$ such that $k \in \text{Seg} n$ holds $Q[k, K_2(k)]$ from $\text{[4, Sch. 5]}. \square$

(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 $j \in \text{Seg} i$ 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 $j \in \text{Seg} i$ 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 $i \in \text{Seg} n$. 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) $\text{len} s_1 = \text{len} s$, and

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

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

\textbf{PROOF:} Define $P[\text{natural number}] \equiv$ for every finite sequence $s$ of elements of the $n$-dimension vector space over $K$ such that $\text{len} s = S_1$ there exists a finite sequence $s_1$ of elements of $K$ such that $\text{len} s_1 = \text{len} s$ and $(\sum s)(i) = \sum s_1$ and for every natural number $k$ such that $k \in \text{dom} s_1$ holds $s_1(k) = s_k(i)$. $P[0]$ by $[22] (7)$, $[24] (43)$. For every natural number $k$ such that $P[k]$ holds $P[k + 1]$ by $[4] (4)$, $[6] (3)$, $[4] (59)$, $[3] (11)$. For every natural number $k$, $P[k]$ from $[3] \text{Sch. 2]}. \square$

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

\textbf{PROOF:} Reconsider $M = \text{GramMatrix}(b)$ as a square matrix over $\mathbb{F}_Q$ of dimension rank $L$. Det $M = 0_{\mathbb{F}_Q}$. $M$ is one-to-one by $[13] (49)$, $[8] (87)$, (59). Reconsider $M_1 = M$ as a finite sequence of elements of the rank $L$-dimension vector space over $\mathbb{F}_Q$. Consider $r$ being a finite sequence of elements of $\mathbb{F}_Q$, $r_1$ being a finite sequence of elements of the rank $L$-dimension vector space over $\mathbb{F}_Q$ such that $\text{len} r = \text{rank} L$ and $\text{len} r_1 = \text{rank} L$ and for every natural number $i$ such that $i \in \text{dom} r_1$ holds $r_1(i) = r_i \cdot M_{i_1}$ and $\sum r_1 = 0_{\alpha}$ and $r \neq \text{Seg} \text{len} r \longmapsto 0_{\mathbb{F}_Q}$, where $\alpha$ is the rank $L$-dimension vector space over $\mathbb{F}_Q$. Consider $K$ being an integer, $K_2$ being a finite sequence of elements of $\mathbb{Z}^R$ such that $K \neq 0$ and $\text{len} K_2 = \text{rank} L$ and for every natural number $i$ such that $i \in \text{dom} K_2$ holds $K_2(i) = K \cdot r_i$. Reconsider $K_1 = K$ as an element of $\mathbb{F}_Q$. Define $P[\text{natural number, object}] \equiv$
there exists an element $r_2$ of the rank $L$-dimension vector space over $\mathbb{F}_Q$ such that $r_2 = r_1(\$1)$ and $\$2 = K_1 \cdot r_2$. For every natural number $k$ such that $k \in \text{Seg rank } L$ there exists an element $x$ of the carrier of the rank $L$-dimension vector space over $\mathbb{F}_Q$ such that $\text{dom } K_3 = \text{Seg rank } L$ and for every natural number $k$ such that $k \in \text{Seg rank } L$ holds $P[k, K_3(k)]$ from [4, Sch. 5]. For every natural number $i$ such that $i \in \text{dom } K_3$ there exists an element $M_2$ of the rank $L$-dimension vector space over $\mathbb{F}_Q$ and there exists an element $K_5$ of $\mathbb{F}_Q$ 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 $\mathbb{F}_Q$ such that $k \in \text{dom } K_3$ and $v = r_1(k)$ holds $K_3(k) = K_1 \cdot v$.

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**


Received March 17, 2017