FORMALIZED MATHEMATICS
Vol. 25, No. 2, Pages 157–169, 2017
DOI: 10.1515/forma-2017-0015

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

Dual Lattice of $\mathbb{Z}$-module Lattice[1]

Yuichi Futa
Tokyo University of Technology
Tokyo, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

Summary. In this article, we formalize in Mizar [5] the definition of dual lattice and their properties. We formally prove that a set of all dual vectors in a rational lattice has the construction of a lattice. We show that a dual basis can be calculated by elements of an inverse of the Gram Matrix. We also formalize a summation of inner products and their properties. Lattice of $\mathbb{Z}$-module is necessary for lattice problems, LLL(Lenstra, Lenstra and Lovász) base reduction algorithm and cryptographic systems with lattice [20], [10] and [19].

MSC: 15A03 15A09 03B35

Keywords: $\mathbb{Z}$-lattice; dual lattice of $\mathbb{Z}$-lattice; dual basis of $\mathbb{Z}$-lattice

MML identifier: ZMODLAT3, version: 8.1.06 5.43.1297

1. Summation of Inner Products

Now we state the proposition:

(1) Let us consider a rational $\mathbb{Z}$-lattice L, and a $\mathbb{Z}$-lattice L_1. Suppose L_1 is a submodule of DivisibleMod(L) and the scalar product of L_1 = ScProductDM$(L) \restriction$ (the carrier of L_1). Then L_1 is rational.

Proof: For every vectors v, u of L_1, $\langle v, u \rangle \in \mathbb{Q}$ by [14, (25)], [7, (49)]. $\square$

Let L be a rational $\mathbb{Z}$-lattice. Observe that EMLat(L) is rational.

Let r be an element of $\mathbb{F}_{\mathbb{Q}}$. Let us note that EMLat(r, L) is rational.

Let L be a $\mathbb{Z}$-lattice, F be a finite sequence of elements of L, f be a function from L into $\mathbb{Z}^{\mathrm{R}}$, and v be a vector of L. The functor ScFS(v, f, F) yielding a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$ is defined by

[1] This work was supported by JSPS KAKENHI grant number JP15K00183.

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

(Def. 1) $\operatorname{len} it = \operatorname{len} F$ and for every natural number i such that $i \in \operatorname{dom} it$ holds $it(i) = \langle v, f(F_i) \cdot F_i \rangle$.

Now we state the propositions:

(2) Let us consider a $\mathbb{Z}$-lattice L, a function f from L into $\mathbb{Z}^{\mathrm{R}}$, a finite sequence F of elements of L, vectors v, u of L, and a natural number i. Suppose $i \in \operatorname{dom} F$ and $u = F(i)$. Then $(\mathrm{ScFS}(v, f, F))(i) = \langle v, f(u) \cdot u \rangle$.

(3) Let us consider a $\mathbb{Z}$-lattice L, a function f from L into $\mathbb{Z}^{\mathrm{R}}$, and vectors v, u of L. Then $\mathrm{ScFS}(v, f, \langle u \rangle) = \langle \langle v, f(u) \cdot u \rangle \rangle$.

(4) Let us consider a $\mathbb{Z}$-lattice L, a function f from L into $\mathbb{Z}^{\mathrm{R}}$, finite sequences F, G of elements of L, and a vector v of L. Then $\mathrm{ScFS}(v, f, F \frown G) = \mathrm{ScFS}(v, f, F) \frown \mathrm{ScFS}(v, f, G)$.

Let L be a $\mathbb{Z}$-lattice, l be a linear combination of L, and v be a vector of L. The functor $\mathrm{SumSc}(v, l)$ yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 2) there exists a finite sequence F of elements of L such that F is one-to-one and $\operatorname{rng} F =$ the support of l and $it = \sum \mathrm{ScFS}(v, l, F)$.

Now we state the propositions:

(5) Let us consider a $\mathbb{Z}$-lattice L, and a vector v of L. Then $\mathrm{SumSc}(v, \mathbf{0}_{\mathrm{LC}_L}) = 0_{\mathbb{R}_{\mathrm{F}}}$.

(6) Let us consider a $\mathbb{Z}$-lattice L, a vector v of L, and a linear combination l of $\emptyset_\alpha$. Then $\mathrm{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$, where α is the carrier of L. The theorem is a consequence of (5).

(7) Let us consider a $\mathbb{Z}$-lattice L, a vector v of L, and a linear combination l of L. Suppose the support of $l = \emptyset$. Then $\mathrm{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (5).

(8) Let us consider a $\mathbb{Z}$-lattice L, vectors v, u of L, and a linear combination l of $\{u\}$. Then $\mathrm{SumSc}(v, l) = \langle v, l(u) \cdot u \rangle$. The theorem is a consequence of (5) and (3).

(9) Let us consider a $\mathbb{Z}$-lattice L, a vector v of L, and linear combinations l_1, l_2 of L. Then $\mathrm{SumSc}(v, l_1 + l_2) = \mathrm{SumSc}(v, l_1) + \mathrm{SumSc}(v, l_2)$.

Proof: Set $A = (($the support of $l_1 + l_2) \cup ($the support of $l_1)) \cup ($the support of $l_2)$. Set $C_1 = A \setminus ($the support of $l_1)$. Consider p being a finite sequence such that $\operatorname{rng} p = C_1$ and p is one-to-one. Set $C_3 = A \setminus ($the support of $l_1 + l_2)$. Consider r being a finite sequence such that $\operatorname{rng} r = C_3$ and r is one-to-one. Set $C_2 = A \setminus ($the support of $l_2)$. Consider q being a finite sequence such that $\operatorname{rng} q = C_2$ and q is one-to-one. Consider F being a finite sequence of elements of L such that F is one-to-one and $\operatorname{rng} F =$ the support of $l_1 + l_2$ and $\mathrm{SumSc}(w, l_1 + l_2) = \sum \mathrm{ScFS}(w, l_1 + l_2, F)$. Set $F_1 = F \frown r$. Consider G being a finite sequence of elements of L such that G is one-to-one and rng G = the support of l_1 and $\mathrm{SumSc}(w, l_1) = \sum \mathrm{ScFS}(w, l_1, G)$. Set $G_3 = G \frown p$. rng F misses rng r. rng G misses rng p. Define $\mathcal{F}$(natural number) $= F_1 \leftarrow (G_3(\$_1))$. Consider P being a finite sequence such that len P = len F_1 and for every natural number k such that $k \in \mathrm{dom}\, P$ holds $P(k) = \mathcal{F}(k)$ from [4, Sch. 2]. rng $P \subseteq$ dom F_1 by [22, (29)], [23, (8)]. dom $F_1 \subseteq$ rng P by [7, (33)], [27, (28), (36)], [7, (39)]. Set $g = \mathrm{ScFS}(w, l_1, G_3)$. Set $f = \mathrm{ScFS}(w, l_1 + l_2, F_1)$. Consider H being a finite sequence of elements of L such that H is one-to-one and rng H = the support of l_2 and $\sum \mathrm{ScFS}(w, l_2, H) = \mathrm{SumSc}(w, l_2)$. Set $H_1 = H \frown q$. rng H misses rng q. Define $\mathcal{F}$(natural number) $= H_1 \leftarrow (G_3(\$_1))$. Consider R being a finite sequence such that len R = len H_1 and for every natural number k such that $k \in \mathrm{dom}\, R$ holds $R(k) = \mathcal{F}(k)$ from [4, Sch. 2]. rng $R \subseteq$ dom H_1 by [22, (29)], [23, (8)]. dom $H_1 \subseteq$ rng R by [7, (33)], [27, (28), (36)], [7, (39)]. Set $h = \mathrm{ScFS}(w, l_2, H_1)$. $\sum h = \sum(\mathrm{ScFS}(w, l_2, H) \frown \mathrm{ScFS}(w, l_2, q))$. $\sum g = \sum(\mathrm{ScFS}(w, l_1, G) \frown \mathrm{ScFS}(w, l_1, p))$. Reconsider $H_2 = h \cdot R$ as a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$. $\sum f = \sum(\mathrm{ScFS}(w, l_1 + l_2, F) \frown \mathrm{ScFS}(w, l_1 + l_2, r))$. Define $\mathcal{F}$(natural number) $= g_{\$_1} + H_{2\$_1}$. Consider I being a finite sequence such that len I = len G_3 and for every natural number k such that $k \in \mathrm{dom}\, I$ holds $I(k) = \mathcal{F}(k)$ from [4, Sch. 2]. rng $I \subseteq$ the carrier of $\mathbb{R}_{\mathrm{F}}$. □

(10) Let us consider a $\mathbb{Z}$-lattice L, a linear combination l of L, and a vector v of L. Then $\langle v, \sum l \rangle = \mathrm{SumSc}(v, l)$.

PROOF: Define $\mathcal{P}$[natural number] $\equiv$ for every $\mathbb{Z}$-lattice L for every linear combination l of L for every vector v of L such that $\overline{\overline{\text{the support of } l}} = \$_1$ holds $\langle v, \sum l \rangle = \mathrm{SumSc}(v, l)$. $\mathcal{P}[0]$ by [24, (19)], [11, (12)], (7). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [2, (44)], [9, (31)], [2, (42)], [24, (7)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

Let L be a $\mathbb{Z}$-lattice, F be a finite sequence of elements of DivisibleMod(L), f be a function from DivisibleMod(L) into $\mathbb{Z}^{\mathrm{R}}$, and v be a vector of DivisibleMod(L). The functor ScFS(v, f, F) yielding a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 3) len it = len F and for every natural number i such that $i \in \mathrm{dom}\, it$ holds $it(i) = (\mathrm{ScProductDM}(L))(v, f(F_i) \cdot F_i)$.

Now we state the propositions:

(11) Let us consider a $\mathbb{Z}$-lattice L, a function f from DivisibleMod(L) into $\mathbb{Z}^{\mathrm{R}}$, a finite sequence F of elements of DivisibleMod(L), vectors v, u of DivisibleMod(L), and a natural number i. Suppose $i \in \mathrm{dom}\, F$ and $u = F(i)$. Then $(\mathrm{ScFS}(v, f, F))(i) = (\mathrm{ScProductDM}(L))(v, f(u) \cdot u)$.

(12) Let us consider a $\mathbb{Z}$-lattice L, a function f from DivisibleMod(L) into

$\mathbb{Z}^{\mathrm{R}}$, and vectors v, u of DivisibleMod(L).
Then $\mathrm{ScFS}(v, f, \langle u \rangle) = \langle (\mathrm{ScProductDM}(L))(v, f(u) \cdot u) \rangle$.

(13) Let us consider a $\mathbb{Z}$-lattice L, a function f from DivisibleMod(L) into $\mathbb{Z}^{\mathrm{R}}$, finite sequences F, G of elements of DivisibleMod(L), and a vector v of DivisibleMod(L). Then $\mathrm{ScFS}(v, f, F \frown G) = \mathrm{ScFS}(v, f, F) \frown \mathrm{ScFS}(v, f, G)$.

Let L be a $\mathbb{Z}$-lattice, l be a linear combination of DivisibleMod(L), and v be a vector of DivisibleMod(L). The functor SumSc(v, l) yielding an element of $\mathbb{R}_{\mathrm{F}}$ is defined by

(Def. 4) there exists a finite sequence F of elements of DivisibleMod(L) such that F is one-to-one and $\mathrm{rng}\, F =$ the support of l and $it = \sum \mathrm{ScFS}(v, l, F)$.

Now we state the propositions:

(14) Let us consider a $\mathbb{Z}$-lattice L, and a vector v of DivisibleMod(L). Then $\mathrm{SumSc}(v, \mathbf{0}_{\mathrm{LC}_{\mathrm{DivisibleMod}(L)}}) = 0_{\mathbb{R}_{\mathrm{F}}}$.

(15) Let us consider a $\mathbb{Z}$-lattice L, a vector v of DivisibleMod(L), and a linear combination l of $\emptyset_{\alpha}$. Then $\mathrm{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$, where α is the carrier of DivisibleMod(L). The theorem is a consequence of (14).

(16) Let us consider a $\mathbb{Z}$-lattice L, a vector v of DivisibleMod(L), and a linear combination l of DivisibleMod(L). Suppose the support of $l = \emptyset$. Then $\mathrm{SumSc}(v, l) = 0_{\mathbb{R}_{\mathrm{F}}}$. The theorem is a consequence of (14).

(17) Let us consider a $\mathbb{Z}$-lattice L, vectors v, u of DivisibleMod(L), and a linear combination l of $\{u\}$. Then $\mathrm{SumSc}(v, l) = (\mathrm{ScProductDM}(L))(v, l(u) \cdot u)$. The theorem is a consequence of (14) and (12).

(18) Let us consider a $\mathbb{Z}$-lattice L, a vector v of DivisibleMod(L), and linear combinations l_1, l_2 of DivisibleMod(L). Then $\mathrm{SumSc}(v, l_1 + l_2) = \mathrm{SumSc}(v, l_1) + \mathrm{SumSc}(v, l_2)$.

PROOF: Set $A =$ ((the support of $l_1 + l_2$) $\cup$ (the support of l_1)) $\cup$ (the support of l_2). Set $C_1 = A \setminus$ (the support of l_1). Consider p being a finite sequence such that $\mathrm{rng}\, p = C_1$ and p is one-to-one. Set $C_3 = A \setminus$ (the support of $l_1 + l_2$). Consider r being a finite sequence such that $\mathrm{rng}\, r = C_3$ and r is one-to-one. Set $C_2 = A \setminus$ (the support of l_2). Consider q being a finite sequence such that $\mathrm{rng}\, q = C_2$ and q is one-to-one. Consider F being a finite sequence of elements of DivisibleMod(L) such that F is one-to-one and $\mathrm{rng}\, F =$ the support of $l_1 + l_2$ and $\mathrm{SumSc}(w, l_1 + l_2) = \sum \mathrm{ScFS}(w, l_1 + l_2, F)$. Set $F_1 = F \frown r$. Consider G being a finite sequence of elements of DivisibleMod(L) such that G is one-to-one and $\mathrm{rng}\, G =$ the support of l_1 and $\mathrm{SumSc}(w, l_1) = \sum \mathrm{ScFS}(w, l_1, G)$. Set $G_3 = G \frown p$. $\mathrm{rng}\, F$ misses $\mathrm{rng}\, r$. $\mathrm{rng}\, G$ misses $\mathrm{rng}\, p$. Define $\mathcal{F}(\text{natural number}) = F_1 \leftarrow (G_3(\$_1))$. Consider P being a finite sequence such that $\mathrm{len}\, P = \mathrm{len}\, F_1$ and for every natural number k such that $k \in \mathrm{dom}\, P$ holds $P(k) = \mathcal{F}(k)$ from

[4, Sch. 2]. $\operatorname{rng} P \subseteq \operatorname{dom} F_1$ by [22, (29)], [23, (8)]. $\operatorname{dom} F_1 \subseteq \operatorname{rng} P$ by [7, (33)], [27, (28), (36)], [7, (39)]. Set $g = \mathrm{ScFS}(w, l_1, G_3)$. Set $f = \mathrm{ScFS}(w, l_1 + l_2, F_1)$. Consider H being a finite sequence of elements of DivisibleMod(L) such that H is one-to-one and $\operatorname{rng} H =$ the support of l_2 and $\sum \mathrm{ScFS}(w, l_2, H) = \mathrm{SumSc}(w, l_2)$. Set $H_1 = H \frown q$. $\operatorname{rng} H$ misses $\operatorname{rng} q$. Define $\mathcal{F}$(natural number) $= H_1 \leftarrow (G_3(\$_1))$. Consider R being a finite sequence such that $\operatorname{len} R = \operatorname{len} H_1$ and for every natural number k such that $k \in \operatorname{dom} R$ holds $R(k) = \mathcal{F}(k)$ from [4, Sch. 2]. $\operatorname{rng} R \subseteq \operatorname{dom} H_1$ by [22, (29)], [23, (8)]. $\operatorname{dom} H_1 \subseteq \operatorname{rng} R$ by [7, (33)], [27, (28), (36)], [7, (39)]. Set $h = \mathrm{ScFS}(w, l_2, H_1)$. $\sum h = \sum(\mathrm{ScFS}(w, l_2, H) \frown \mathrm{ScFS}(w, l_2, q))$. $\sum g = \sum(\mathrm{ScFS}(w, l_1, G) \frown \mathrm{ScFS}(w, l_1, p))$. Reconsider $H_2 = h \cdot R$ as a finite sequence of elements of $\mathbb{R}_{\mathrm{F}}$. $\sum f = \sum(\mathrm{ScFS}(w, l_1 + l_2, F) \frown \mathrm{ScFS}(w, l_1 + l_2, r))$. Define $\mathcal{F}$(natural number) $= g_{\$_1} + H_{2\$_1}$. Consider I being a finite sequence such that $\operatorname{len} I = \operatorname{len} G_3$ and for every natural number k such that $k \in \operatorname{dom} I$ holds $I(k) = \mathcal{F}(k)$ from [4, Sch. 2]. $\operatorname{rng} I \subseteq$ the carrier of $\mathbb{R}_{\mathrm{F}}$. □

(19) Let us consider a $\mathbb{Z}$-lattice L, a linear combination l of DivisibleMod(L), and a vector v of DivisibleMod(L). Then $(\mathrm{ScProductDM}(L))(v, \sum l) = \mathrm{SumSc}(v, l)$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every $\mathbb{Z}$-lattice L for every linear combination l of DivisibleMod(L) for every vector v of DivisibleMod(L) such that $\overline{\overline{\text{the support of } l}} = \$_1$ holds $(\mathrm{ScProductDM}(L))(v, \sum l) = \mathrm{SumSc}(v, l)$. $\mathcal{P}[0]$ by [24, (19)], [12, (14)], (16). For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [2, (44)], [9, (31)], [2, (42)], [24, (7)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(20) 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. Suppose $M = H$ and M is invertible. Then

(i) H is invertible, and

(ii) $M^{\smile} = H^{\smile}$.

Proof: For every natural numbers i, j such that $\langle i, j \rangle \in$ the indices of $M^{\smile}$ holds $M^{\smile}{}_{i,j} = H^{\smile}{}_{i,j}$ by [9, (87)], [12, (52), (54), (47)]. □

(21) Let us consider a natural number n, and a square matrix M over $\mathbb{R}_{\mathrm{F}}$ of dimension n. Suppose M is square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension n and invertible. Then $M^{\smile}$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension n. The theorem is a consequence of (20).

(22) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then $(\mathrm{GramMatrix}(b))^{\smile}$ is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L)$. The theorem is a consequence of (21).

(23) Let us consider a finite subset X of $\mathbb{Q}$. Then there exists an element a of $\mathbb{Z}$ such that

(i) $a \neq 0$, and

(ii) for every element r of $\mathbb{Q}$ such that $r \in X$ holds $a \cdot r \in \mathbb{Z}$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset X of $\mathbb{Q}$ such that $\overline{\overline{X}} = \$_1$ there exists an element a of $\mathbb{Z}$ such that $a \neq 0$ and for every element r of $\mathbb{Q}$ such that $r \in X$ holds $a \cdot r \in \mathbb{Z}$. $\mathcal{P}[0]$. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [26, (41)], [2, (44)], [1, (30)], [17, (1)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. $\square$

(24) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice L, and an ordered basis b of L. Then there exists an element a of $\mathbb{R}_{\rm F}$ such that

(i) a is an element of $\mathbb{Z}^{\rm R}$, and

(ii) $a \neq 0$, and

(iii) $a \cdot (\mathrm{GramMatrix}(b))^{\smile}$ is a square matrix over $\mathbb{Z}^{\rm R}$ of dimension $\dim(L)$.

Proof: Set $G = (\mathrm{GramMatrix}(b))^{\smile}$. For every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of G holds $G_{i,j} \in$ the carrier of $\mathbb{F}_{\mathbb{Q}}$ by [9, (87)], [7, (3)]. Define $\mathcal{F}$(natural number, natural number) $= G_{\$_1,\$_2}$. Set $D_3 = \{\mathcal{F}(u, v)$, where u is an element of $\mathbb{N}, v$ is an element of $\mathbb{N} : u \in \mathrm{Seg\,len}\, G$ and $v \in \mathrm{Seg\,width}\, G\}$. D_3 is finite from [21, Sch. 22]. $\{G_{i,j}$, where i, j are natural numbers : $\langle i, j\rangle \in$ the indices of $G\} \subseteq D_3$ by [9, (87)]. $\{G_{i,j}$, where i, j are natural numbers : $\langle i, j\rangle \in$ the indices of $G\} \subseteq$ the carrier of $\mathbb{F}_{\mathbb{Q}}$. Reconsider $X = \{G_{i,j}$, where i, j are natural numbers : $\langle i, j\rangle \in$ the indices of $G\}$ as a finite subset of $\mathbb{F}_{\mathbb{Q}}$. Consider a being an element of $\mathbb{Z}$ such that $a \neq 0$ and for every element r of $\mathbb{Q}$ such that $r \in X$ holds $a \cdot r \in \mathbb{Z}$. For every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of $a \cdot G$ holds $(a \cdot G)_{i,j} \in$ the carrier of $\mathbb{Z}^{\rm R}$. $\square$

(25) Let us consider a non trivial, rational, positive definite $\mathbb{Z}$-lattice L, an ordered basis b of $\mathrm{EMLat}(L)$, and a natural number i. Suppose $i \in \mathrm{dom}\, b$. Then there exists a vector v of $\mathrm{DivisibleMod}(L)$ such that

(i) $(\mathrm{ScProductDM}(L))(b_i, v) = 1$, and

(ii) for every natural number j such that $i \neq j$ and $j \in \mathrm{dom}\, b$ holds $(\mathrm{ScProductDM}(L))(b_j, v) = 0$.

Proof: Consider a being an element of $\mathbb{R}_{\rm F}$ such that a is an element of $\mathbb{Z}^{\rm R}$ and $a \neq 0$ and $a \cdot (\mathrm{GramMatrix}(b))^{\smile}$ is a square matrix over $\mathbb{Z}^{\rm R}$ of dimension $\dim(L)$. For every natural number j such that $i \neq j$ and $j \in \mathrm{dom}\, b$ holds $\mathrm{Line}(a \cdot (\mathrm{GramMatrix}(b))^{\smile}, i) \cdot (\mathrm{GramMatrix}(b))_{\square,j} = 0$ by [9, (87)]. Reconsider $I = \mathrm{rng}\, b$ as a basis of $\mathrm{EMLat}(L)$. Define

$\mathcal{P}$[object, object] $\equiv$ if $\$_1 \in I$, then for every natural number n such that $n = b^{-1}(\$_1)$ and $n \in \operatorname{dom} b$ holds $\$_2 = (a \cdot (\mathrm{GramMatrix}(b))^{\smile})_{i,n}$ and if $\$_1 \notin I$, then $\$_2 = 0_{\mathbb{Z}^{\mathrm{R}}}$. For every element x of EMLat(L), there exists an element y of $\mathbb{Z}^{\mathrm{R}}$ such that $\mathcal{P}[x, y]$ by [7, (32)], [9, (87)], [16, (1)]. Consider l being a function from EMLat(L) into $\mathbb{Z}^{\mathrm{R}}$ such that for every element x of EMLat(L), $\mathcal{P}[x, l(x)]$ from [8, Sch. 3]. Reconsider $a_2 = a$ as an element of $\mathbb{Z}^{\mathrm{R}}$. For every natural number k such that $1 \leqslant k \leqslant \operatorname{len} \mathrm{ScFS}(b_i, l, b)$ holds $(\mathrm{Line}(a \cdot (\mathrm{GramMatrix}(b))^{\smile}, i) \bullet (\mathrm{GramMatrix}(b))_{\square,i})(k) = (\mathrm{ScFS}(b_i, l, b))(k)$ by [22, (25)], [7, (3), (34)], [6, (72)]. The support of $l \subseteq \operatorname{rng} b$. For every natural number j such that $i \neq j$ and $j \in \operatorname{dom} b$ holds $\langle b_j, \sum l \rangle = 0$ by [6, (72)], [22, (25)], [7, (3), (34)]. Consider u being a vector of DivisibleMod(L) such that $a_2 \cdot u = \sum l$. For every natural number j such that $i \neq j$ and $j \in \operatorname{dom} b$ holds $(\mathrm{ScProductDM}(L))(b_j, u) = 0$ by [14, (24)], [12, (13), (8)]. □

2. Dual Lattice

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

A dual of L is a vector of DivisibleMod(L) and is defined by

(Def. 5) for every vector v of DivisibleMod(L) such that $v \in \mathrm{Embedding}(L)$ holds $(\mathrm{ScProductDM}(L))(it, v) \in \mathbb{Z}^{\mathrm{R}}$.

Now we state the propositions:

(26) Let us consider a $\mathbb{Z}$-lattice L. Then $0_{\mathrm{DivisibleMod}(L)}$ is a dual of L.

(27) Let us consider a $\mathbb{Z}$-lattice L, and duals v, u of L. Then $v + u$ is a dual of L.

Proof: For every vector x of DivisibleMod(L) such that $x \in \mathrm{Embedding}(L)$ holds $(\mathrm{ScProductDM}(L))(v + u, x) \in \mathbb{Z}^{\mathrm{R}}$ by [12, (6)]. □

(28) Let us consider a $\mathbb{Z}$-lattice L, a dual v of L, and an element a of $\mathbb{Z}^{\mathrm{R}}$. Then $a \cdot v$ is a dual of L.

Proof: For every vector x of DivisibleMod(L) such that $x \in \mathrm{Embedding}(L)$ holds $(\mathrm{ScProductDM}(L))(a \cdot v, x) \in \mathbb{Z}^{\mathrm{R}}$ by [12, (6)]. □

Let L be a $\mathbb{Z}$-lattice. The functor DualSet(L) yielding a non empty subset of DivisibleMod(L) is defined by the term

(Def. 6) the set of all v where v is a dual of L.

Note that DualSet(L) is linearly closed.

The functor DualLatMod(L) yielding a strict, non empty structure of $\mathbb{Z}$-lattice over $\mathbb{Z}^{\mathrm{R}}$ is defined by

(Def. 7) the carrier of *it* = DualSet(L) and the addition of *it* = (the addition of DivisibleMod(L)) $\restriction$ DualSet(L) and the zero of *it* = $0_{\mathrm{DivisibleMod}(L)}$ and the left multiplication of *it* = (the left multiplication of DivisibleMod(L))$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ DualSet(L)) and the scalar product of *it* = ScProductDM(L)$\restriction$(DualSet(L) $\times$ DualSet(L)).

Now we state the propositions:

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

(30) 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 (ScProductDM(L))$(v, u) \in \mathbb{Z}^{\mathrm{R}}$. Then v is a dual of L.
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 (ScProductDM(L))$(v, u) \in \mathbb{Z}^{\mathrm{R}}$ for every vector w of DivisibleMod(L) such that $w \in \mathrm{Lin}(I)$ holds (ScProductDM(L))$(v, w) \in \mathbb{Z}^{\mathrm{R}}$. $\mathcal{P}[0]$ by [15, (67), (66)], [12, (6)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [26, (41)], [2, (44)], [1, (30)], [9, (31)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

Let L be a rational, positive definite $\mathbb{Z}$-lattice and I be a basis of EMLat(L). The functor DualBasis(I) yielding a subset of DivisibleMod(L) is defined by

(Def. 8) for every vector v of DivisibleMod(L), $v \in$ *it* iff there exists a vector u of EMLat(L) such that $u \in I$ and (ScProductDM(L))$(u, v) = 1$ and for every vector w of EMLat(L) such that $w \in I$ and $u \neq w$ holds (ScProductDM(L))$(w, v) = 0$.

The functor B2DB(I) yielding a function from I into DualBasis(I) is defined by

(Def. 9) dom *it* = I and rng *it* = DualBasis(I) and for every vector v of EMLat(L) such that $v \in I$ holds (ScProductDM(L))$(v, it(v)) = 1$ and for every vector w of EMLat(L) such that $w \in I$ and $v \neq w$ holds (ScProductDM(L))$(w, it(v)) = 0$.

Observe that B2DB(I) is onto and one-to-one.

Now we state the proposition:

(31) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, and a basis I of EMLat(L). Then $\overline{\overline{I}} = \overline{\overline{\mathrm{DualBasis}(I)}}$.

Let L be a rational, positive definite $\mathbb{Z}$-lattice and I be a basis of EMLat(L). Note that DualBasis(I) is finite.

Let L be a non trivial, rational, positive definite $\mathbb{Z}$-lattice.

Note that DualBasis(I) is non empty.

Now we state the propositions:

(32) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, a basis I of $\mathrm{EMLat}(L)$, a vector v of $\mathrm{DivisibleMod}(L)$, and a linear combination l of $\mathrm{DualBasis}(I)$. If $v \in I$, then $(\mathrm{ScProductDM}(L))(v, \sum l) = l((\mathrm{B2DB}(I))(v))$. The theorem is a consequence of (19), (17), and (18).

(33) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, a basis I of $\mathrm{EMLat}(L)$, and a vector v of $\mathrm{DivisibleMod}(L)$. If v is a dual of L, then $v \in \mathrm{Lin}(\mathrm{DualBasis}(I))$.
Proof: Set $f = (\mathrm{B2DB}(I))^{-1}$. Define $\mathcal{P}[\text{object}, \text{object}] \equiv$ if $\$_1 \in \mathrm{DualBasis}(I)$, then $\$_2 = (\mathrm{ScProductDM}(L))(f(\$_1), v)$ and if $\$_1 \notin \mathrm{DualBasis}(I)$, then $\$_2 = 0_{\mathbb{Z}^{\mathrm{R}}}$. For every object x such that $x \in$ the carrier of $\mathrm{DivisibleMod}(L)$ there exists an object y such that $y \in$ the carrier of $\mathbb{Z}^{\mathrm{R}}$ and $\mathcal{P}[x, y]$ by [7, (33), (3)], [13, (24)], [14, (25)]. Consider l being a function from $\mathrm{DivisibleMod}(L)$ into the carrier of $\mathbb{Z}^{\mathrm{R}}$ such that for every object x such that $x \in$ the carrier of $\mathrm{DivisibleMod}(L)$ holds $\mathcal{P}[x, l(x)]$ from [8, Sch. 1]. The support of $l \subseteq \mathrm{DualBasis}(I)$ by [24, (2)]. Consider b being a finite sequence such that $\mathrm{rng}\, b = I$ and b is one-to-one. For every natural number n such that $n \in \mathrm{dom}\, b$ holds $(\mathrm{ScProductDM}(L))(b_n, v) = (\mathrm{ScProductDM}(L))(b_n, \sum l)$ by [12, (20)], [14, (25)], [7, (3)], [18, (14)]. $\square$

Let L be a rational, positive definite $\mathbb{Z}$-lattice and I be a basis of $\mathrm{EMLat}(L)$. Let us note that $\mathrm{DualBasis}(I)$ is linearly independent.

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

(Def. 10) the carrier of $it = \mathrm{DualSet}(L)$ and $0_{it} = 0_{\mathrm{DivisibleMod}(L)}$ and the addition of $it =$ (the addition of $\mathrm{DivisibleMod}(L)$) $\restriction$ (the carrier of it) and the left multiplication of $it =$ (the left multiplication of $\mathrm{DivisibleMod}(L)$)$\restriction$((the carrier of $\mathbb{Z}^{\mathrm{R}}$) $\times$ (the carrier of it)) and the scalar product of $it = \mathrm{ScProductDM}(L) \restriction$ (the carrier of it).

Now we state the propositions:

(34) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, and a vector v of $\mathrm{DivisibleMod}(L)$. Then $v \in \mathrm{DualLat}(L)$ if and only if v is a dual of L.

(35) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L. Then $\mathrm{DualLat}(L)$ is a submodule of $\mathrm{DivisibleMod}(L)$.

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

(36) Every basis of $\mathrm{EMLat}(L)$ is a basis of $\mathrm{Embedding}(L)$.

(37) Every basis of $\mathrm{Embedding}(L)$ is a basis of $\mathrm{EMLat}(L)$.

(38) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, a basis I of $\mathrm{EMLat}(L)$, and a vector v of $\mathrm{DivisibleMod}(L)$. If $v \in \mathrm{DualBasis}(I)$, then

v is a dual of L.

PROOF: Consider u being a vector of EMLat(L) such that $u \in I$ and (ScProductDM(L))(u, v) = 1 and for every vector w of EMLat(L) such that $w \in I$ and $u \neq w$ holds (ScProductDM(L))(w, v) = 0. Reconsider $J = I$ as a basis of Embedding(L). For every vector w of DivisibleMod(L) such that $w \in J$ holds (ScProductDM(L))(v, w) $\in \mathbb{Z}^{\mathrm{R}}$ by [12, (6)]. □

(39) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, and a basis I of EMLat(L). Then DualBasis(I) is a basis of DualLat(L).

PROOF: Reconsider D = DualLat(L) as a submodule of DivisibleMod(L). For every vector v of DivisibleMod(L) such that $v \in$ DualBasis(I) holds $v \in$ the carrier of DualLat(L). For every vector v of DivisibleMod(L) such that $v \in$ the vector space structure of D holds $v \in$ Lin(DualBasis(I)). For every vector v of DivisibleMod(L) such that $v \in$ Lin(DualBasis(I)) holds $v \in$ the vector space structure of D by [25, (7)], (36), (32), [7, (3)]. □

(40) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, an ordered basis b of EMLat(L), and a basis I of EMLat(L). Suppose $I = \operatorname{rng} b$. Then B2DB(I) $\cdot\, b$ is an ordered basis of DualLat(L). The theorem is a consequence of (39).

(41) Let us consider a positive definite, finite rank, free $\mathbb{Z}$-lattice L, an ordered basis b of L, and an ordered basis e of EMLat(L). Suppose e = MorphsZQ(L) $\cdot\, b$. Then GramMatrix(InnerProduct L, b) = GramMatrix (InnerProduct EMLat(L), e).

PROOF: For every natural numbers i, j such that $\langle i, j\rangle \in$ the indices of GramMatrix(InnerProduct L, b) holds (GramMatrix(InnerProduct L, b))$_{i,j}$ = (GramMatrix(InnerProduct EMLat(L), e))$_{i,j}$ by [9, (87)], [7, (13)]. □

(42) Let us consider a positive definite, finite rank, free $\mathbb{Z}$-lattice L. Then GramDet(InnerProduct L) = GramDet(InnerProduct EMLat(L)). The theorem is a consequence of (41).

(43) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L. Then rank L = rank DualLat(L). The theorem is a consequence of (39) and (31).

(44) Let us consider an integral, positive definite $\mathbb{Z}$-lattice L. Then EMLat(L) is a $\mathbb{Z}$-sublattice of DualLat(L).

PROOF: DualLat(L) is a submodule of DivisibleMod(L). For every vector v of DivisibleMod(L) such that $v \in$ EMLat(L) holds $v \in$ DualLat(L) by (36), [12, (28), (8)], (30). □

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

PROOF: Set $I = \operatorname{rng} b$. For every vectors v, u of L such that v, $u \in I$ holds

$\langle v, u \rangle \in \mathbb{Z}$ by [6, (10)], [16, (49)], [9, (87)], [16, (1)]. □

(46) 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 $\langle v, u \rangle \in \mathbb{Q}$. Let us consider a vector v of L. If $v \in \mathrm{Lin}(I)$, then $\langle v, u \rangle \in \mathbb{Q}$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset I of L such that $\overline{\overline{I}} = \$_1$ and for every vector v of L such that $v \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$ for every vector v of L such that $v \in \mathrm{Lin}(I)$ holds $\langle v, u \rangle \in \mathbb{Q}$. $\mathcal{P}[0]$ by [15, (67)], [11, (12)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [9, (40)], [15, (72)], [2, (44)], [9, (31)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(47) 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 $\langle v, u \rangle \in \mathbb{Q}$. Let us consider vectors v, u of L. Then $\langle v, u \rangle \in \mathbb{Q}$.

Proof: Define $\mathcal{P}$[natural number] $\equiv$ for every finite subset I of L such that $\overline{\overline{I}} = \$_1$ and for every vectors v, u of L such that v, $u \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$ for every vectors v, u of L such that v, $u \in \mathrm{Lin}(I)$ holds $\langle v, u \rangle \in \mathbb{Q}$. $\mathcal{P}[0]$ by [15, (67)], [11, (12)]. For every natural number n such that $\mathcal{P}[n]$ holds $\mathcal{P}[n+1]$ by [9, (40)], [15, (72)], [2, (44)], [9, (31)]. For every natural number n, $\mathcal{P}[n]$ from [3, Sch. 2]. □

(48) 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 $\langle v, u \rangle \in \mathbb{Q}$. Then L is rational. The theorem is a consequence of (47).

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

Proof: Set $I = \mathrm{rng}\, b$. For every vectors v, u of L such that v, $u \in I$ holds $\langle v, u \rangle \in \mathbb{Q}$ by [6, (10)], [16, (49)], [9, (87)], [16, (1)]. □

Let L be a rational, positive definite $\mathbb{Z}$-lattice. One can check that DualLat(L) is rational.

Now we state the propositions:

(50) Let us consider a rational $\mathbb{Z}$-lattice L, a $\mathbb{Z}$-lattice L_1, and an ordered basis b of L_1. Suppose L_1 is a submodule of DivisibleMod(L) and the scalar product of L_1 = ScProductDM$(L) \restriction$ (the carrier of L_1). Then GramMatrix(InnerProduct L_1, b) is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L_1)$. The theorem is a consequence of (1).

(51) Let us consider a rational, positive definite $\mathbb{Z}$-lattice L, and an ordered basis b of DualLat(L). Then GramMatrix(InnerProduct DualLat$(L), b$) is a square matrix over $\mathbb{F}_{\mathbb{Q}}$ of dimension $\dim(L)$. The theorem is a consequence of (35), (43), and (50).

(52) Let us consider a positive definite $\mathbb{Z}$-lattice L, and a $\mathbb{Z}$-lattice L_1. Suppose L_1 is a submodule of DivisibleMod(L) and the scalar product of L_1 = ScProductDM(L) $\upharpoonright$ (the carrier of L_1). Then L_1 is positive definite.

PROOF: For every vector v of L_1 such that $v \neq 0_{L_1}$ holds $\|v\| > 0$ by [14, (25)], [7, (49)], [13, (29)], [12, (13), (6), (8)]. □

Let L be a rational, positive definite $\mathbb{Z}$-lattice. Note that DualLat(L) is positive definite.

Let L be a non trivial, rational, positive definite $\mathbb{Z}$-lattice. Let us note that DualLat(L) is non trivial.

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] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, 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. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

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

[10] Wolfgang Ebeling. *Lattices and Codes.* Advanced Lectures in Mathematics. Springer Fachmedien Wiesbaden, 2013.

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

[12] Yuichi Futa and Yasunari Shidama. Embedded lattice and properties of Gram matrix. *Formalized Mathematics*, 25(**1**):73–86, 2017. doi:10.1515/forma-2017-0007.

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

[14] Yuichi Futa, Hiroyuki Okazaki, and Yasunari Shidama. $\mathbb{Z}$-modules. *Formalized Mathematics*, 20(**1**):47–59, 2012. doi:10.2478/v10037-012-0007-z.

[15] 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.

[16] 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.

[17] Andrzej Kondracki. Basic properties of rational numbers. *Formalized Mathematics*, 1(**5**): 841–845, 1990.

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

[19] 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.

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

[21] Andrzej Trybulec. Function domains and Frænkel operator. *Formalized Mathematics*, 1(**3**):495–500, 1990.

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

[23] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.

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

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

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

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

Received June 27, 2017

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.