GALOIS TRACE FORMS OF TYPE A_n, D_n, E_n FOR ODD n AND CODES

RIKU HIGA

Abstract. Let $F/\mathbb{Q}$ be a Galois extension of odd degree, then F has a self-dual basis over $\mathbb{Q}$. In this note, we construct A_n, D_n-lattices that can be embedded in F from the basis. Furthermore, we report a method for constructing unimodular lattices from these lattices and the correspondence with codes.

1. Introduction

For every odd prime number p, Ebeling [3, Ch. 5] constructed a Hilbert modular theta function over $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ by constructing an even unimodular lattice from the fractional ideal of $\mathbb{Q}(\zeta_p)$ generated by $(1-\zeta_p)^{-(p-3)/2}$ which is a lattice of type A_{p-1}.

In order to generalize Ebeling's construction to more general even root lattices, especially irreducible ones of type A_n, D_n, E_n, it is natural to ask which lattices can be realized as ideal lattices over number fields. In [9], the following result is obtained.

Theorem 1.1. *Let n be an odd positive integer and $F/\mathbb{Q}$ be a Galois extension of degree n. Then, there exist no fractional ideals $\Lambda \subset F$ such that $(\Lambda, \mathrm{Tr}|_{\Lambda\times\Lambda})$ are of type A_n, D_n, E_n.*

This leads us to the following question:

Question 1.2. *Let n be an odd positive integer.*

Can one find a totally real F of degree n and a sub $\mathbb{Z}$-module Λ of F such that the lattice $(\Lambda, \mathrm{Tr}|_{\Lambda\times\Lambda})$ is of type A_n, D_n, E_n?

Every Galois extension of odd degree has a self-dual basis (see [4, Theorem 2.1]). Using the basis, we gain the following Theorem 1.3. This is the first main result of this note.

Theorem 1.3. *Let n be an odd positive integer and $F/\mathbb{Q}$ be a Galois extension of degree n.*

1. *There exists a lattice $\Lambda \subset F$ of type A_n such that $n+1 \in \mathbb{Q}^{\times 2}$ or of type D_n.*
2. *There exist no $\mathbb{Z}$-modules $\Lambda \subset F$ such that $(\Lambda, \mathrm{Tr}|_{\Lambda\times\Lambda})$ are of type A_n for $n+1 \notin \mathbb{Q}^{\times 2}$ or of type E_7.*

In addition to the result, we give the following Theorem 1.4.

Theorem 1.4. *Let $\Lambda \subset F$ be a Theorem 1.3 (1)'s lattice, and let C be a Λ^*/Λ-code of length m. If C is self-dual, there exists the unimodular lattice which lies between $(\Lambda)^{\oplus m}$ and $(\Lambda^*)^{\oplus m}$.*

The organization of this note is as follows. In §2, we recall some basic definitions. In §3, we give a proof of Theorem 1.3. In §4, we give a proof of Theorem 1.4.

Notation. In this paper, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the ring of integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively.

A subfield F of $\mathbb{C}$ is called a number field if its degree $[F : \mathbb{Q}]$ over $\mathbb{Q}$ is finite.

2. Basic definitions

First, we recall some basic definitions. For details, see e.g. [3, Ch. 1].

Definition 2.1. Let Λ be a free $\mathbb{Z}$-module of rank n and $\langle\ ,\ \rangle : \Lambda \times \Lambda \to \mathbb{R}$ be a bilinear form.

(1) A pair $\Lambda = (\Lambda, \langle\ ,\ \rangle)$ is called a lattice if $\langle\ ,\ \rangle$ is positive-definite and symmetric, that is, $\langle x, x\rangle > 0$ for every $x \in \Lambda \setminus \{0\}$ and $\langle x, y\rangle = \langle y, x\rangle$ for every $x, y \in \Lambda$.
(2) A lattice Λ is called integral if $\langle x, y\rangle \in \mathbb{Z}$ for every $x, y \in \Lambda$.
(3) An integral lattice Λ is called even if $\langle x, x\rangle \in 2\mathbb{Z}$ for every $x \in \Lambda$, and odd otherwise.
(4) A lattice Λ is called of type A_n if Λ has a basis $(e_1, \dots, e_n)$ such that

$$\langle e_i, e_j\rangle = \begin{cases} 2 & \text{if } |j-i| = 0, \text{ i.e., } j = i, \\ -1 & \text{if } |j-i| = 1, \\ 0 & \text{if } |j-i| \geq 2. \end{cases}$$

(5) A lattice Λ is called of type D_n $(n \geq 4)$ if Λ has a basis $(e_1, \dots, e_n)$ such that

$$\langle e_i, e_j\rangle = \begin{cases} 2 & \text{if } |j-i| = 0, \text{ i.e., } j = i, \\ -1 & \text{if } (|j-i| = 1 \text{ and } \{i,j\} \neq \{n-1, n\}) \text{ or } \{i,j\} = \{n-2, n\}, \\ 0 & \text{if } (|j-i| \geq 2 \text{ and } \{i,j\} \neq \{n-2, n\}) \text{ or } \{i,j\} = \{n-1, n\}. \end{cases}$$

(6) A lattice Λ is called of type E_n $(n = 6, 7, 8)$

$$\langle e_i, e_j\rangle = \begin{cases} 2 & \text{if } |j-i| = 0, \text{ i.e., } j = i, \\ -1 & \text{if } (|j-i| = 1 \text{ and } \{i,j\} \neq \{n-1, n\}) \text{ or } \{i,j\} = \{n-3, n\}, \\ 0 & \text{if } (|j-i| \geq 2 \text{ and } \{i,j\} \neq \{n-3, n\}) \text{ or } \{i,j\} = \{n-1, n\}. \end{cases}$$

(7) For a lattice Λ of rank n, its dual lattice Λ^* is defined by

$$\Lambda^* := \left\{ x \in \mathbb{R}^{\oplus n} \;\middle|\; \langle x, y\rangle \in \mathbb{Z} \text{ for every } y \in \Lambda \right\},$$

where $\mathbb{R}^{\oplus n} \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ and we extend $\langle\ ,\ \rangle$ $\mathbb{R}$-bilinearly to $\mathbb{R}^{\oplus n} \times \mathbb{R}^{\oplus n}$.

Note that a lattice Λ is integral if and only if $\Lambda \subset \Lambda^*$. We are interested in integral lattices arise as submodules of certain number fields.

Definition 2.2. Let F be a number field. F is called totally real if every field homomorphism $F \to \mathbb{C}$ has the image in $\mathbb{R}$.

Lemma 2.3. *Suppose that F is a totally real. Then, the bilinear form*

$$\mathrm{Tr} = \mathrm{Tr}_F : F \times F \to \mathbb{Q}; (x, y) \mapsto \mathrm{Tr}_{F/\mathbb{Q}}(xy)$$

is positive-definite and symmetric. In particular, for every sub $\mathbb{Z}$-module Λ of F, the pair $(\Lambda, \mathrm{Tr}\,|_{\Lambda\times\Lambda})$ is a lattice.

Let K be a field, and let F be a finite Galois extension of K. Set $n = [F : K]$.

Definition 2.4. A basis $(e_1,\ \dots,\ e_n)$ of the K-vector space F is said to be self-dual if

$$\mathrm{Tr}(e_i, e_j) = \delta_{i,j} \quad \text{(Kronecker delta)}.$$

Theorem 2.5. *If $[L : K]$ is odd, then L has a self-dual basis over K.*

Proof. This was proved in [4, Theorem 2.1]. □

Definition 2.6. Let $n \geq 2$ and $m \geq 1$ be an integer.

(1) A code C of length m over $\mathbb{Z}/n\mathbb{Z}$ (or a $\mathbb{Z}/n\mathbb{Z}$-code C of length m) is a $\mathbb{Z}/n\mathbb{Z}$-submodule of $(\mathbb{Z}/n\mathbb{Z})^{\oplus m}$.
(2) The elements of C are called codewords.
(3) The number of coordinates i in a codeword x is denoted by $n_i(x)$
(4) The Euclidean weight $\mathrm{wt}_{\mathrm{E}}(x)$ of a codeword x is defined by

$$\mathrm{wt}_{\mathrm{E}}(x) := (1^2)n_1(x) + \cdots + (n^2)n_n(x).$$

(5) The inner product of $x = (x_1, \cdots, x_m),\ y = (y_1, \cdots, y_m)$ in $(\mathbb{Z}/n\mathbb{Z})^{\oplus m}$ is given by

$$x \cdot y := \sum_{i=1}^{m} x_i y_i \ .$$

(6) The dual code of a $\mathbb{Z}/n\mathbb{Z}$-code C of length m is defined by

$$C^{\perp} := \{x \in (\mathbb{Z}/n\mathbb{Z})^{\oplus m} \mid x \cdot y = 0 \text{ for every } y \in C\}.$$

(7) A $\mathbb{Z}/n\mathbb{Z}$-code C is called self-dual if $C = C^{\perp}$

3. Constructions of lattices of type A_n, D_n from self-dual basis

We determine which irreducible even root lattices as $\mathbb{Z}$-module can be embedded in Galois extension of odd degree.

In this section, let $F/\mathbb{Q}$ be a Galois extension of odd degree n, $\Lambda \subset F$ be an integral lattice with basis $(e_1, \ \ldots, \ e_n)$, and $(\varepsilon_1, \ \ldots, \ \varepsilon_n)$ be a self-dual $\mathbb{Q}$-basis of F.

Then

$$e_i = \sum_{j=1}^{n} a_{ij} \varepsilon_j,$$

and the matrix $A = (a_{ij})_{1 \le i,j \le n}$ is in $\mathrm{GL}_n(\mathbb{Q})$, which means in particular that $\det A \in \mathbb{Q}$.

Thus,

$$\begin{aligned} \#(\Lambda^*/\Lambda) &= \det(\mathrm{Tr}(e_i \cdot e_j))_{1 \le i,j \le n} \\ &= \det(A \ (\mathrm{Tr}(\varepsilon_i \cdot \varepsilon_j))_{1 \le i,j \le n} \ {}^{\mathrm{t}}A) \\ &= (\det A)^2 \in \mathbb{Q}^{\times 2} \ . \end{aligned}$$

We summarize the information of Λ^*/Λ for Λ is of type A_n, D_n, E_n:

$$\Lambda^*/\Lambda \simeq \begin{cases} \mathbb{Z}/(n+1)\mathbb{Z} & \text{if } \Lambda \text{ is of type } A_n, \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 2} & \text{if } \Lambda \text{ is of type } D_n \text{ for even } n, \\ \mathbb{Z}/4\mathbb{Z} & \text{if } \Lambda \text{ is of type } D_n \text{ for odd } n, \\ \mathbb{Z}/(9-n)\mathbb{Z} & \text{if } \Lambda \text{ is of type } E_n. \end{cases}$$

In particular, there exist no $\mathbb{Z}$-modules $\Lambda \subset F$ such that $(\Lambda, \mathrm{Tr}\,|_{\Lambda \times \Lambda})$ are of type A_n for $n+1 \notin \mathbb{Q}^{\times 2}$ or of type E_7.

3.1. **Lattices of type D_n.**

We construct the lattice of type D_n in F.

Let

$$e_i = \begin{cases} -\varepsilon_i + \varepsilon_{i+1} & (1 \le i \le n-1), \\ -\varepsilon_{n-1} - \varepsilon_n & (i = n). \end{cases}$$

Then $(\Lambda, \mathrm{Tr}\,|_{\Lambda \times \Lambda})$ with basis $(e_1, \ldots, e_n)$ is lattice of type D_n.

3.2. **Lattices of type A_n ($n+1 \in \mathbb{Q}^{\times 2}$).** We construct the lattice of type A_n in F.

Suppose that a is an even positive integer, and $n+1 = a^2$ (i.e. n is odd integer).

Let

$$e_i = \begin{cases} -\varepsilon_i + \varepsilon_{i+1} & (1 \le i \le n-2), \\ -\varepsilon_{n-1} - \varepsilon_n & (i = n-1), \\ \frac{1}{a-1}(\varepsilon_1 + \cdots + \varepsilon_{n-1} + (a-2)\varepsilon_n) & (i = n). \end{cases}$$

Then $(\Lambda, \mathrm{Tr}\,|_{\Lambda\times\Lambda})$ with basis $(e_1, \ldots, e_n)$ is lattice of type A_n.

By summarizing the results of this section, we have the following Theorem 3.1.

Theorem 3.1. *Let F be a Galois extension over $\mathbb{Q}$ of odd degree n.*

(1) *There exists a lattice $\Lambda \subset F$ of type A_n such that $n+1 \in \mathbb{Q}^{\times 2}$ or of type D_n.*
(2) *There exist no $\mathbb{Z}$-modules $\Lambda \subset F$ such that $(\Lambda, \mathrm{Tr}\,|_{\Lambda\times\Lambda})$ are of type A_n for $n+1 \notin \mathbb{Q}^{\times 2}$ or of type E_7.*

4. Lattices from codes

In this section, we construct the unimodular lattice from the lattice of type A_n or D_n.

4.1. **D_n and $\mathbb{Z}/4\mathbb{Z}$.** We consider lattices of type D_n and $\mathbb{Z}/4\mathbb{Z}$-codes.

Suppose that n is an odd integer, $F/\mathbb{Q}$ is a Galois extension of degree n, and $(\varepsilon_1, \cdots, \varepsilon_n)$ is a self-dual $\mathbb{Q}$-basis of F.

We define

$$e_i = \begin{cases} \varepsilon_i + \varepsilon_{i+1} & (1 \le i \le n-1), \\ \varepsilon_n + \varepsilon_1 & (i = n), \end{cases}$$

and

$$\begin{aligned} e_i^* &= \frac{1}{2}\varepsilon_i + (\frac{1}{2}\varepsilon_{i+1} - \frac{1}{2}\varepsilon_{i+2} + \cdots + \frac{1}{2}\varepsilon_{i-2} - \frac{1}{2}\varepsilon_{i-1}) \\ &= \frac{1}{4}\left(\sum_{l=0}^{n-1}(-1)^l(n-2l)e_{i+l}\right). \end{aligned}$$

Then,

$$\mathrm{Tr}_{F/\mathbb{Q}}(e_i^* \cdot e_j) = \delta_{ij} \quad \text{(Kronecker delta)}.$$

Let

$$\Lambda = \left\{ \sum_{i=1}^{n} a_i e_i \;\middle|\; a_i \in \mathbb{Z} \right\}.$$

Hence,

$$\Lambda^* = \left\{ \sum_{i=1}^{n} a_i e_i^* \;\middle|\; a_i \in \mathbb{Z} \right\}.$$

Let

$$A = \begin{pmatrix} 0 & -1 & & -1 & 0 \\ 1 & 0 & & \vdots & 0 \\ -1 & 1 & \ddots & 1 & \vdots \\ 1 & -1 & & -1 & \\ -1 & 1 & & 1 & \\ \vdots & -1 & & -1 & \\ 1 & \vdots & & 0 & 0 \\ -1 & 1 & & 1 & -1 \end{pmatrix}.$$

Thus,

$$A \in \mathrm{SL}_n(\mathbb{Z}),$$

and

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} A = \begin{bmatrix} \varepsilon_1 & \cdots & \varepsilon_n \end{bmatrix} \begin{pmatrix} -1 & & & \\ 1 & \ddots & & \\ & \ddots & -1 & -1 \\ & & 1 & -1 \end{pmatrix}.$$

Hence $(\Lambda, \mathrm{Tr}\,|_{\Lambda\times\Lambda})$ is the lattice of type D_n, and

$$\Lambda^*/\Lambda \cong \mathbb{Z}/4\mathbb{Z}.$$

We consider

$$\begin{array}{cccc} \rho^{\oplus m}\colon & (\Lambda^*)^{\oplus m} & \longrightarrow & (\mathbb{Z}/4\mathbb{Z})^{\oplus m} \\ & \cup & & \cup \\ & \left(\displaystyle\sum_{j=1}^{n} a_{ij} e_j^*\right)_{1\le i\le m} & \longmapsto & \left(\rho\left(\displaystyle\sum_{j=1}^{n} a_{ij}\right)\right)_{1\le i\le m.} \end{array}$$

For $\mathbb{Z}/4\mathbb{Z}$-code C of length m, let

$$\Gamma_C = (\rho^{\oplus m})^{-1}(C),$$

and let

$$\langle x, y\rangle = \sum_{i=1}^{m} \mathrm{Tr}(x_i y_i) \quad (\text{for every } x = (x_i),\ y = (y_i) \in F^{\oplus m}).$$

Then, $(\Gamma_C, \langle\ ,\ \rangle)$ is a lattice.

Let $x = (x_i)_{1\le i\le m},\ y = (y_i)_{1\le i\le m} \in (\Lambda^*)^{\oplus m}$, and let $x_i = \sum_{l=1}^{n} x_{il} e_l^*,\ y_i = \sum_{l=1}^{n} y_{il} e_l^*$. Then,

$$\sum_{l=1}^{n} y_{il} e_l^* = \sum_{l=1}^{n} \frac{1}{4} \left(\sum_{j=0}^{n-1} (-1)^j (n-2j) y_{i(l-j)} \right) e_l,$$

and

$$\begin{aligned}
\mathrm{Tr}(x_iy_i) &= \sum_{l=1}^{n}\frac{1}{4}x_{il}\left(\sum_{j=0}^{n-1}(-1)^j(n-2j)y_{i(l-j)}\right)\\
&= \frac{1}{4}n\left(\sum_{l=1}^{n}x_{il}\right)\left(\sum_{l=1}^{n}y_{il}\right)-\frac{1}{4}n\left(\sum_{l=1}^{n}x_{il}\right)\left(\sum_{l=1}^{n}y_{il}\right)+\sum_{l=1}^{n}\frac{1}{4}x_{il}\left(\sum_{j=0}^{n-1}(-1)^j(n-2j)y_{i(l-j)}\right)\\
&= \frac{1}{4}n\left(\sum_{l=1}^{n}x_{il}\right)\left(\sum_{l=1}^{n}y_{il}\right)+\sum_{l=1}^{n}\frac{1}{4}x_{il}\left(\sum_{j=0}^{n-1}-ny_{i(l-j)}+\sum_{j=0}^{n-1}(-1)^j(n-2j)y_{i(l-j)}\right)\\
&= \frac{1}{4}n\left(\sum_{l=1}^{n}x_{il}\right)\left(\sum_{l=1}^{n}y_{il}\right)+\sum_{l=1}^{n}\frac{1}{4}x_{il}\left(\sum_{j=0}^{(n-1)/2}(-4j)y_{i(l-2j)}-\sum_{j=1}^{(n-1)/2}(2(n+1)-4j)y_{i(l-2j+1)}\right).
\end{aligned}$$

By

$$\sum_{j=0}^{(n-1)/2}(-4j)y_{i(l-2j)}-\sum_{j=1}^{(n-1)/2}(2(n+1)-4j)y_{i(l-2j+1)}\in 4\mathbb{Z},$$

we get the following Lemma 4.1.

Lemma 4.1. *For every $x,\ y\in(\Lambda^*)^{\oplus m}$,*

$$\langle x,y\rangle\in\mathbb{Z}\Longleftrightarrow\frac{1}{4}\sum_{i=1}^{m}\left(\sum_{l=1}^{n}x_{il}\right)\left(\sum_{l=1}^{n}y_{il}\right)\in\mathbb{Z}\Longleftrightarrow\rho^{\oplus m}(x)\cdot\rho^{\oplus m}(y)=0.$$

Lemma 4.1 shows that

$$\Gamma_{C^\perp}=\Gamma_C^*.$$

Moreover, by

$$\mathrm{Tr}(x_ix_i)=\frac{1}{4}n\left(\sum_{l=1}^{n}x_{il}\right)\left(\sum_{l=1}^{n}x_{il}\right)+\sum_{l=1}^{n}\frac{1}{4}x_{il}\left(\sum_{j=0}^{(n-1)/2}(-4j)x_{i(l-2j)}-\sum_{j=1}^{(n-1)/2}(2(n+1)-4j)x_{i(l-2j+1)}\right)$$

and,

$$\begin{aligned}
&\sum_{l=1}^{n}\frac{1}{4}x_{il}\left(\sum_{j=0}^{(n-1)/2}(-4j)x_{i(l-2j)}-\sum_{j=1}^{(n-1)/2}(2(n+1)-4j)x_{i(l-2j+1)}\right)\\
=\ &\sum_{l=1}^{n}\frac{1}{4}(-4\cdot 0)x_{il}x_{il}\\
&+\sum_{\substack{1\le s<l\le n\\ l-s\in 2\mathbb{Z}}}\frac{1}{4}\left(-4\frac{l-s}{2}-\left(2(n+1)-4\frac{n+1-(l-s)}{2}\right)\right)x_{il}x_{is}\\
&+\sum_{\substack{1\le s<l\le n\\ l-s\notin 2\mathbb{Z}}}\frac{1}{4}\left(-4\frac{n-(l-s)}{2}-\left(2(n+1)-4\frac{(l-s)+1}{2}\right)\right)x_{il}x_{is}\\
=\ &\sum_{\substack{l>s\\ l-s\in 2\mathbb{Z}}}(s-l)x_{il}x_{is}\in 2\mathbb{Z},
\end{aligned}$$

we get the following Lemma 4.2

Lemma 4.2. *For every* $x \in (\Lambda^*)^{\oplus m}$,

$$\langle x, x\rangle \in 2\mathbb{Z} \Longleftrightarrow \frac{1}{4}\sum_{i=1}^{m}\left(\sum_{l=1}^{n} x_{il}\right)\left(\sum_{l=1}^{n} x_{il}\right) \in 2\mathbb{Z} \Longleftrightarrow \mathrm{wt_E}(\rho^{\oplus m}(x)) \in 8\mathbb{Z}.$$

From Lemma 4.1 and Lemma 4.2, we get the following result.

Theorem 4.3. *Let C be a $\mathbb{Z}/4\mathbb{Z}$-code.*

(1) $$C \subset C^{\perp} \Longleftrightarrow \Gamma_C \subset \Gamma_{C^{\perp}},$$

(2) $$C = C^{\perp} \Longleftrightarrow \Gamma_C = \Gamma_{C^{\perp}}\ ,$$

(3) $$\mathrm{wt_E}(x) \in 8\mathbb{Z} \textit{ for every } x \in C \Longleftrightarrow \Gamma_C \textit{ is even.}$$

4.2. A_n **and** $\mathbb{Z}/(n+1)\mathbb{Z}$**.** We consider lattices of type A_n and $\mathbb{Z}/(n+1)\mathbb{Z}$-codes.

Suppose that a is an even positive integer, and $n+1 = a^2$ (i.e. n is odd integer), $F/\mathbb{Q}$ is a Galois extension of degree n, and $(\varepsilon_1, \cdots, \varepsilon_n)$ is a self-dual $\mathbb{Q}$-basis of F.

We define

$$e_i = \begin{cases} \frac{1}{a-1}\left(-(a-1)\varepsilon_i - 2\varepsilon_n + \sum_{l=1}^{n}\varepsilon_l\right) & (1 \le i \le n-1), \\ \frac{1}{a-1}\left((a-1)\varepsilon_i - 2\varepsilon_n + \sum_{l=1}^{n}\varepsilon_l\right) & (i = n), \end{cases}$$

and

$$e_i^* = \begin{cases} \frac{1}{a(a-1)}\left(-a(a-1)\varepsilon_i - 2\varepsilon_n + \sum_{l=1}^{n}\varepsilon_l\right) & (1 \le i \le n-1), \\ \frac{1}{a(a-1)}\left(a(a-1)\varepsilon_i - 2\varepsilon_n + \sum_{l=1}^{n}\varepsilon_l\right) & (i = n). \end{cases}$$

Then,

$$\mathrm{Tr}_{F/\mathbb{Q}}(e_i^* \cdot e_j) = \delta_{ij} \quad \text{(Kronecker delta)}.$$

Let

$$\Lambda = \left\{\sum_{i=1}^{n} a_i e_i \mid a_i \in \mathbb{Z}\right\}.$$

Hence,

$$\Lambda^* = \left\{\sum_{i=1}^{n} a_i e_i^* \mid a_i \in \mathbb{Z}\right\}.$$

Let

$$A = \begin{pmatrix} 1 & & & \\ -1 & \ddots & & \\ & \ddots & 1 & \\ & & -1 & 1 \end{pmatrix}.$$

Thus,

$$A \in \mathrm{SL}_n(\mathbb{Z}),$$

and

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} A = \begin{bmatrix} \varepsilon_1 & \cdots & \varepsilon_n \end{bmatrix} \begin{pmatrix} -1 & & & & \frac{1}{a-1} \\ 1 & \ddots & & & \vdots \\ & \ddots & -1 & & \\ & & 1 & -1 & \frac{1}{a-1} \\ & & & -1 & \frac{a-2}{a-1} \end{pmatrix}.$$

Hence $(\Lambda, \mathrm{Tr}\,|_{\Lambda\times\Lambda})$ is the lattice of type A_n, and

$$\Lambda^*/\Lambda \cong \mathbb{Z}/(n+1)\mathbb{Z}.$$

We consider

$$\begin{array}{cccc} \rho^{\oplus m}\colon & (\Lambda^*)^{\oplus m} & \longrightarrow & (\mathbb{Z}/(n+1)\mathbb{Z})^{\oplus m} \\ & \cup & & \cup \\ & \left(\sum_{j=1}^{n} a_{ij} e_j^*\right)_{1\le i\le m} & \longmapsto & \left(\rho\left(\sum_{j=1}^{n} a_{ij}\right)\right)_{1\le i\le m.} \end{array}$$

For $\mathbb{Z}/(n+1)\mathbb{Z}$-code C of length m, let

$$\Gamma_C = (\rho^{\oplus m})^{-1}(C),$$

and let

$$\langle x, y\rangle = \sum_{i=1}^{m} \mathrm{Tr}(x_i y_i) \quad (\text{for every } x = (x_i),\ y = (y_i) \in F^{\oplus m}).$$

Then, $(\Gamma_C, \langle\ ,\ \rangle)$ is a lattice.

Let $x = (x_i)_{1\le i\le m},\ y = (y_i)_{1\le i\le m} \in (\Lambda^*)^{\oplus m}$, and let $x_i = \sum_{l=1}^{n} x_{il} e_l^*,\ y_i = \sum_{l=1}^{n} y_{il} e_l^*$. Then,

$$\begin{aligned} \mathrm{Tr}(x_i y_i) &= \mathrm{Tr}\left(\left(\sum_{l=1}^{n} x_{il} e_l^*\right)\left(\sum_{l=1}^{n} y_{il} e_l^*\right)\right) \\ &= \mathrm{Tr}\left(\left(\sum_{l=1}^{n} x_{il} e_l^*\right)\left(\sum_{l=1}^{n}\left(y_{il} - \frac{1}{a^2}\sum_{j=1}^{n} y_{ij}\right) e_l\right)\right) \\ &= \sum_{l=1}^{n} x_{il}\left(y_{il} - \frac{1}{a^2}\sum_{j=1}^{n} y_{ij}\right) \\ &= -\frac{1}{n+1}\left(\sum_{l=1}^{n} x_{il}\right)\left(\sum_{j=1}^{n} y_{ij}\right) + \sum_{l=1}^{n} x_{il} y_{il}. \end{aligned}$$

Thus, we get the following Lemma 4.4.

Lemma 4.4. *For every $x,\ y \in (\Lambda^*)^{\oplus m}$,*

$$\langle x, y\rangle \in \mathbb{Z} \Longleftrightarrow \frac{1}{n+1}\sum_{i=1}^{m}\left(\sum_{l=1}^{n} x_{il}\right)\left(\sum_{l=1}^{n} y_{il}\right) \in \mathbb{Z} \Longleftrightarrow \rho^{\oplus m}(x)\cdot\rho^{\oplus m}(y) = 0.$$

Lemma 4.1 shows that

$$\Gamma_{C^\perp} = \Gamma_C^*.$$

Moreover, we have

$$\begin{aligned}\langle x, x\rangle &= -\frac{1}{n+1}\sum_{i=1}^{m}\left(\sum_{l=1}^{n} x_{il}\right)\left(\sum_{l=1}^{n} x_{il}\right) + \sum_{i=1}^{m}\sum_{l=1}^{n} x_{il}x_{il} \\ &= \frac{n}{n+1}\sum_{i=1}^{m}\left(\sum_{l=1}^{n} x_{il}\right)\left(\sum_{l=1}^{n} x_{il}\right) - \sum_{i=1}^{m}\sum_{1\le l<s\le n} 2x_{il}x_{is}.\end{aligned}$$

Then, we get the following Lemma 4.5.

Lemma 4.5. *For every* $x \in (\Lambda^*)^{\oplus m}$,

$$\langle x, x\rangle \in 2\mathbb{Z} \Longleftrightarrow \frac{1}{n+1}\sum_{i=1}^{m}\left(\sum_{l=1}^{n} x_{il}\right)\left(\sum_{l=1}^{n} x_{il}\right) \in \mathbb{Z} \Longleftrightarrow \mathrm{wt_E}(\rho^{\oplus m}(x)) \in 2(n+1)\mathbb{Z}$$

From Lemma 4.4 and Lemma 4.5, the following result holds.

Theorem 4.6. *Let* C *be a* $\mathbb{Z}/(n+1)\mathbb{Z}$*-code.*

(1) $$C \subset C^\perp \Longleftrightarrow \Gamma_C \subset \Gamma_{C^\perp},$$
(2) $$C = C^\perp \Longleftrightarrow \Gamma_C = \Gamma_{C^\perp},$$
(3) $$\mathrm{wt_E}(\rho^{\oplus m}(x)) \in 2(n+1)\mathbb{Z} \text{ for every } x \in C \Longleftrightarrow \Gamma_C \text{ is even.}$$

References

[1] Eva Bayer-Fluckiger, *Lattices and number fields*, Algebraic geometry: Hirzebruch 70 (Warsaw, 1998), Contemp. Math., vol. 241, Amer. Math. Soc., Providence, RI, 1999, pp. 69–84, DOI 10.1090/conm/241/03628. MR1718137

[2] Robson R. de Araujo and Grasiele C. Jorge, *Constructions of full diversity* D_n*-lattices for all* n, Rocky Mountain J. Math. **50** (2020), no. 4, 1137–1150, DOI 10.1216/rmj.2020.50.1137. MR4154799

[3] Wolfgang Ebeling, *Lattices and codes*, 3rd ed., Advanced Lectures in Mathematics, Springer Spektrum, Wiesbaden, 2013. A course partially based on lectures by Friedrich Hirzebruch. MR2977354

[4] Eva Bayer-Fluckiger, *Self-dual normal bases*, Indagationes Mathematicae (Proceedings) **92** (1989), no. 4, 379-383, DOI https://doi.org/10.1016/1385-7258(89)90002-4.

[5] Vladimir L. Popov and Yuri G. Zarhin, *Root lattices in number fields*, Bull. Math. Sci. **11** (2021), no. 3, Paper No. 2050021, 22, DOI 10.1142/S1664360720500216. MR4354460

[6] Masaaki Harada, *Self-dual Z4-codes and Hadamard matrices*, Discrete Mathematics **245** (2002), no. 1, 273-278, DOI https://doi.org/10.1016/S0012-365X(01)00310-7.

[7] E. M. Rains and N. J. A. Sloane, *Self-Dual Codes* (2002), available at `math/0208001`.

[8] Riku Higa, [*Construction of* A_3*-root lattices from codes*] *Fugo kara kosei sareru koshi de* A_3*-root koshi wo kosei suru hoho ni tsuite*, Tokyo University of Science, master thesis (japanese).

[9] Riku Higa and Yoshinosuke Hirakawa, *Galois trace forms of type* A_n, D_n, E_n *for odd* n (2023), available at `2307.06612`.

[10] Pierre Samuel, *Algebraic theory of numbers*, Houghton Mifflin Co., Boston, Mass., 1970. Translated from the French by Allan J. Silberger. MR0265266

[11] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237

(Riku Higa) Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, 2641, Yamazaki, Noda, Chiba, Japan

Email address: `6123702@ed.tus.ac.jp, 6121510@ed.tus.ac.jp`