奇数次 Galois 拡大体上の既約ルート格子と符号

東京理科大学大学院　創域理工学研究科　数理科学専攻
比嘉 陸 (Riku HIGA) *

概要

n を奇数、$F/\mathbb{Q}$ を n 次 Galois 拡大とすると、F は self-dual basis をもつ。 F に埋め込めるランク n の既約ルート格子について考えると、$n+1$ が平方数でないとき、格子の体積 (判別式) からルート格子 A_n は F に埋め込めないことがわかる。本講演では F の self-dual basis を用いて、任意の奇数 n に対して、ルート格子 D_n が、$n+1$ が平方数のときに、ルート格子 A_n が、それぞれ構成できることを示す。また、構成したルート格子と符号との対応について議論する。

1　導入

符号理論は、情報の伝達や保存に関する理論で、通信、データ圧縮、誤り訂正、暗号化などの分野で応用されており、数学や情報工学の融合という点でも注目される分野である。一方で、保型形式は、複素解析や数論、表現論など多くの分野で重要な役割を果たしており、最近では量子数理や暗号理論などの分野でも活用されている。その中で 1 変数の保型形式 (楕円モジュラー形式) は数学において極めて重要な研究対象である。符号からモジュラー形式を構成する方法としては、符号から格子を構成し、その格子のテータ関数を利用する方法がある。偶ユニモジュラー格子というとても性質の良い格子はその格子のテータ関数がモジュラー形式となる。2 元符号の場合は重偶自己双対符号という誤り検出・訂正能力の高い符号から格子を構成すると偶ユニモジュラー格子を構成できる。

自己双対符号とユニモジュラー格子の対応は 2 元符号だけでなく、様々な有限環上の符号において研究されており、その際重要になるのが、符号に対応する格子（特に既約ルート格子）がどのような体に埋め込めるのかということである。

代数体においては Ebeling [3] により奇素数 p について A_{p-1} 型ルート格子を $\mathbb{Q}(\zeta_p)$ に、Bayer-Flückiger [1] により D_4、E_6、E_8 がそれぞれ $\mathbb{Q}(\zeta_8)$、$\mathbb{Q}(\zeta_9)$、$\mathbb{Q}(\zeta_{20})$ に、de Araujo、Jorge [2] により、自然数 $n \geq 3$ に対して D_n が $\mathbb{Q}(\zeta_p)$ (p は素数で、$p \equiv 1 \mod n$) に埋め込めることが知られている。

本稿では、奇数次の Galois 拡大体に埋め込める既約ルート格子を決定する。また、そのルート格子と符号との対応により、自己双対符号からユニモジュラー格子を構成する方法を考察する。

* E-mail:6123702@ed.tus.ac.jp

2　主定理

主定理 2.1. n を奇数、$F/\mathbb{Q}$ を n 次 Galois 拡大とする。

(1) $n \geq 5$ に対して、D_n 型の格子 $\Lambda \subset F$ が存在する。
(2) $n+1 \in \mathbb{Q}^{\times 2}$ のとき、A_n 型の格子 $\Lambda \subset F$ が存在する。

主定理 2.2. 主定理 2.1 の格子 Λ と長さ m の Λ^*/Λ-符号 C に対して

$$C = C^{\perp} \Longleftrightarrow \Gamma_C = \Gamma_{C^{\perp}}$$

となる格子 $\Gamma_C \subset F^{\oplus m}$ が存在する。

3　格子と符号

この章では格子と符号の基本事項を述べる。詳細は [3]、[6] を参照。

定義 3.1. Λ をランク n の自由 $\mathbb{Z}$-加群とし、双線型形式 $\langle\ ,\ \rangle : \Lambda \times \Lambda \to \mathbb{R}$ を考える。

1. $\Lambda = (\Lambda, \langle\ ,\ \rangle)$ が**格子**であるとは $\langle\ ,\ \rangle$ が正定値対称双線型形式であることすなわち、$x \in \Lambda \backslash \{0\}$ に対して $\langle x, x\rangle > 0$ であり、かつ $x, y \in \Lambda$ に対して $\langle x, y\rangle = \langle y, x\rangle$ を満たすときを言う。
2. 格子 Λ が**整**であるとは $x, y \in \Lambda$ に対して $\langle x, y\rangle \in \mathbb{Z}$ を満たすことである。
3. 整格子 Λ が**偶**であるとは $x \in \Lambda$ に対して $\langle x, x\rangle \in 2\mathbb{Z}$ を満たすことである。
4. 格子 Λ が A_n 型であるとは Λ が次を満たす基底 $(e_1, \ldots, e_n)$ を持つときを言う。

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

5. 格子 Λ が D_n 型 $(n \geq 4)$ であるとは Λ が次を満たす基底 $(e_1, \ldots, e_n)$ を持つときを言う。

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

6. 格子 Λ が E_n 型 $(n = 6, 7, 8)$ であるとは Λ が次を満たす基底 $(e_1, \ldots, e_n)$ を持つときを言う。

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

7. ランク n の格子 Λ に対して、**双対格子** Λ^* を次で定義する。

$$\Lambda^* := \left\{ x \in \mathbb{R}^{\oplus n} \mid \forall y \in \Lambda, \langle x, y\rangle \in \mathbb{Z} \right\}$$

($\mathbb{R}^{\oplus n} \simeq \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ であり $\langle\ ,\ \rangle$ を $\mathbb{R}^{\oplus n} \times \mathbb{R}^{\oplus n}$ に拡張して考える。)

格子 Λ が整であることと $\Lambda \subset \Lambda^*$ は同値である。本稿では代数体上の整格子について考える。

定義 3.2. F を代数体とする

1. F が**総実**であるとは任意の準同型写像 $F \to \mathbb{C}$ が $\mathbb{R}$ 上に値をとることである。
2. F が **CM** (complex multiplication) であるとは、F が $[F : F^+] = 2$ となる総実な部分体 F^+ をもち、準同型写像 $F \to \mathbb{R}$ を持たないときを言う。

F が CM 体であるとき、$\mathrm{Gal}(F/F^+)$ は複素共役で生成される。

補題 3.3. F は総実または CM 体であるとする。このとき、

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

は正定値対称双線型形式である。

特にすべての F 上の部分 $\mathbb{Z}$-加群 Λ に対して, $(\Lambda, \mathrm{Tr}\,|_{\Lambda\times\Lambda})$ は格子である。

定義 3.4. $\mathbb{Q}$-ベクトル空間 F の基底 $(e_1,\ \ldots,\ e_n)$ が self-dual であるとは

$$\mathrm{Tr}(e_i, e_j) = \delta_{i,j} \quad (\text{クロネッカーのデルタ})$$

を満たすことである。

定理 3.5. 奇数次 Galois 拡大体 $F/\mathbb{Q}$ は self-dual $\mathbb{Q}$-基底を持つ。

Proof. 証明は [4, Theorem 2.1] を参照。 □

定義 3.6. 自然数 $l \geq 2$、$m \geq 1$ をとる。

1. 長さ m の $\mathbb{Z}/l\mathbb{Z}$ 上の**符号** C (または、長さ m の $\mathbb{Z}/l\mathbb{Z}$-符号 C) とは $(\mathbb{Z}/l\mathbb{Z})^{\oplus m}$ 上の $\mathbb{Z}/l\mathbb{Z}$-加群のことである。
2. C の元を**符号語**と言う。
3. 符号語 x の成分が i であるものの数を $n_i(x)$ で表す。
4. 符号語 x の Euclidean 重み $\mathrm{wt}_{\mathrm{E}}(x)$ を

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

   で定義する。
5. $x = (x_1, \cdots, x_m),\ y = (y_1, \cdots, y_m) \in (\mathbb{Z}/l\mathbb{Z})^{\oplus m}$ に対して内積を

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

   で定義する。
6. 長さ m の $\mathbb{Z}/l\mathbb{Z}$-符号 C の**双対符号**を次で定義する。

   $$C^{\perp} := \{x \in (\mathbb{Z}/l\mathbb{Z})^{\oplus m} \mid \forall y \in C,\ x \cdot y = 0\}.$$

7. $\mathbb{Z}/l\mathbb{Z}$-符号 C が**自己双対**であるとは $C = C^{\perp}$ を満たすことである。

4　奇数次 Galois 拡大体上の既約ルート格子

この章では主定理 2.1 を証明する。

4.1　D_n 型格子

n は 5 以上の奇数とし、$F/\mathbb{Q}$ を n 次 Galois 拡大、$(\varepsilon_1,\ \ldots,\ \varepsilon_n)$ を F 上の self-dual $\mathbb{Q}$-基底とする。

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

とすると、

$$(\mathrm{Tr}_{F/\mathbb{Q}}(e_i \cdot e_j)) = \begin{pmatrix} 2 & -1 & & & & \\ -1 & 2 & \ddots & & & \\ & -1 & \ddots & -1 & & \\ & & \ddots & 2 & -1 & -1 \\ & & & -1 & 2 & \\ & & & -1 & & 2 \end{pmatrix}$$

より、$(e_1,\ \ldots,\ e_n)$ を基底とする格子は F 上の D_n 型格子である。

4.2　$A_n(n+1 \in \mathbb{Q}^{\times 2})$ 型格子

$a > 0$ を偶数、$n+1 = a^2$（i.e. n は奇数）、$F/\mathbb{Q}$ を n 次 Galois 拡大、$(\varepsilon_1,\ \ldots,\ \varepsilon_n)$ を F 上の self-dual $\mathbb{Q}$-基底とする。

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

とすると、

$$(\mathrm{Tr}_{F/\mathbb{Q}}(e_i \cdot e_j)) = \begin{pmatrix} 2 & -1 & & & & \\ -1 & 2 & \ddots & & & \\ & -1 & \ddots & -1 & & \\ & & \ddots & 2 & -1 & \\ & & & -1 & 2 & -1 \\ & & & & -1 & 2 \end{pmatrix}$$

となるので、$(e_1,\ \ldots,\ e_n)$ を基底とする格子は F 上の A_n 型格子である。

4.3 E_7 型、A_n 型 $(n+1 \notin \mathbb{Q}^{\times 2})$ 格子

$n > 0$ を奇数、$F/\mathbb{Q}$ を n 次 Galois 拡大、$(\varepsilon_1,\ \ldots,\ \varepsilon_n)$ を F 上の self-dual $\mathbb{Q}$-基底とする。
$\Lambda \subset F$ を $\mathbb{Q}$-基底 $(e_1,\ \ldots,\ e_n)$ を持つ格子とすると、

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

を満たす行列 $A = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{GL}_n(\mathbb{Q})$ が存在し、 $\det A \in \mathbb{Q}$ となる。
つまり

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

を満たす。
ここで、A_n, D_n, E_n 型の格子 Λ は

$$\Lambda^*/\Lambda \simeq \begin{cases} \mathbb{Z}/(n+1)\mathbb{Z} & \Lambda \text{ が } A_n \text{ 型のとき,} \\ (\mathbb{Z}/2\mathbb{Z})^{\oplus 2} & \Lambda \text{ が } D_n \text{ 型かつ } n \text{ が偶数,} \\ \mathbb{Z}/4\mathbb{Z} & \Lambda \text{ が } D_n \text{ 型かつ } n \text{ が奇数,} \\ \mathbb{Z}/(9-n)\mathbb{Z} & \Lambda \text{ が } E_n \text{ 型.} \end{cases}$$

を満たす。(cf.[3]) よって、F 上に E_n 型、A_n 型 $(n+1 \notin \mathbb{Q}^{\times 2})$ の格子は存在しない。

5 D_n 型、A_n 型格子と符号

この章では主定理 2.2 を証明する。

5.1 D_n 型格子と $\mathbb{Z}/4\mathbb{Z}$-符号

n は 5 以上の奇数とし、$F/\mathbb{Q}$ を n 次 Galois 拡大、$(\varepsilon_1,\ \ldots,\ \varepsilon_n)$ を F 上の self-dual $\mathbb{Q}$-基底とする。

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

とし、

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

とすると、

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

となる。

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

とすると、

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

が成り立つ。

$$\begin{bmatrix} e_1 & \cdots & e_n \end{bmatrix} \begin{pmatrix} 0 & -1 & & -1 & 0 \\ 1 & 0 & & \vdots & 0 \\ -1 & 1 & \ddots & 1 & \vdots \\ 1 & -1 & & -1 & \\ -1 & 1 & & 1 & \\ \vdots & -1 & & -1 & \\ 1 & \vdots & & 0 & 0 \\ -1 & 1 & & 1 & -1 \end{pmatrix} = \begin{bmatrix} \varepsilon_1 & \cdots & \varepsilon_n \end{bmatrix} \begin{pmatrix} -1 & & & \\ 1 & \ddots & & \\ & \ddots & -1 & -1 \\ & & 1 & -1 \end{pmatrix}$$

より、Λ は D_n 型格子であり、

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

を満たす。

写像

$$\begin{array}{rccc} \rho\colon & \Lambda^* & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ & \cup & & \cup \\ & \displaystyle\sum_{i=1}^{n} a_i e_i^* & \longmapsto & \left(\displaystyle\sum_{i=1}^{n} a_i \right) \bmod 4 \end{array}$$

と、

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

を考える。

長さ m の $\mathbb{Z}/4\mathbb{Z}$-符号 C に対して、

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

とすると、Γ_C は $(\Lambda^*)^{\oplus m}$ 上の $\mathbb{Z}$-加群であり、$x = (x_i),\ y = (y_i) \in F^{\oplus m}$ に対して、

$$\langle x, y \rangle = \sum_{i=1}^{m} \mathrm{Tr}(x_i y_i)$$

を考えると、Γ_C は格子となる。

$x_i = \sum_{l=1}^{n} x_{il} e_l^*,\ y_i = \sum_{l=1}^{n} y_{il} e_l^* \in \Lambda^*$ とすると、

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

より、

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

となる。

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

であることから、

$x,\ y \in (\Lambda^*)^{\oplus m}$ に対して、

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

が成り立つ。よって、

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

となる。

また、

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

であり、

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

となることから、$x\in(\Lambda^*)^{\oplus m}$ に対して、

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

となる。

以上より次が成り立つ。

定理 5.1. 長さ m の $\mathbb{Z}/4\mathbb{Z}$-符号 C に対して、以下が成り立つ。

1. $$C\subset C^{\perp}\Longleftrightarrow\Gamma_C\subset\Gamma_{C^{\perp}}$$

2. $$C=C^{\perp}\Longleftrightarrow\Gamma_C=\Gamma_{C^{\perp}}$$

3. $$\text{「}\forall x\in C,\ \mathrm{wt}_{\mathrm{E}}(x)\in 8\mathbb{Z}\text{」}\Longleftrightarrow\Gamma_C\text{は偶格子}$$

5.2 A_n 型格子と $\mathbb{Z}/(n+1)\mathbb{Z}$-符号

$a>0$ を偶数、$n+1=a^2$ (i.e. n は奇数)、$F/\mathbb{Q}$ を n 次 Galois 拡大、$(\varepsilon_1,\ \ldots,\ \varepsilon_n)$ を F 上の self-dual $\mathbb{Q}$-基底とする。

D_n 型の時と同様に、

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

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

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

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

$$\begin{array}{rccc} \rho\colon & \Lambda^* & \longrightarrow & \mathbb{Z}/(n+1)\mathbb{Z} \\ & \cup & & \cup \\ & \sum_{i=1}^{n} a_i e_i^* & \longmapsto & \left(\sum_{i=1}^{n} a_i \right) \mod n+1 \end{array}$$

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

$x = (x_i),\ y = (y_i) \in F^{\oplus m}$ に対して、

$$\langle x, y \rangle = \sum_{i=1}^{m} \mathrm{Tr}(x_i y_i)$$

とすると、

定理 5.2. 長さ m の $\mathbb{Z}/(n+1)\mathbb{Z}$-符号 C と、格子 $\Gamma_C = (\rho^{\oplus m})^{-1}(C)$ に対して次が成り立つ。

1. $$C \subset C^{\perp} \Longleftrightarrow \Gamma_C \subset \Gamma_{C^{\perp}}$$

2. $$C = C^{\perp} \Longleftrightarrow \Gamma_C = \Gamma_{C^{\perp}}$$

3. $$「\forall x \in C,\ \mathrm{wt_E}(x) \in 2(n+1)\mathbb{Z}」 \Longleftrightarrow \Gamma_C \text{は偶格子}$$

参考文献

[1] Eva Bayer-Flückiger, *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] Bayer-Flückiger, *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