Orthogonal decompositions of integral trace forms of certain algebraic number fields via Bezoutians

大竹 秀一 (Shuichi OTAKE)・早稲田大学基幹理工学部

概要

有限次代数体 K やその整数環上には, 有理数体 $\mathbb{Q}$ 上の trace 写像が定める二次形式が付随しており, K の trace form 或いは integral trace form と呼ばれる. 本稿では, K が円分体や, ある種の trinomial から定まる場合に, その integral trace form の 有理整数環 $\mathbb{Z}$ 上の直交分解や, p 進整数環 $\mathbb{Z}_p$ 上の標準形に関する結果を紹介する.

1 Introduction

K を有限次代数体とし, K の $\mathbb{Q}$ 上の最小多項式を $f(x)$ とする; $K \simeq \mathbb{Q}[x]/(f(x))$. このとき, 写像

$$\mathrm{Tr}_{K/\mathbb{Q}} : K \times K \to \mathbb{Q}\ ;\ (\alpha, \beta) \to \mathrm{trace}_{K/\mathbb{Q}}(\alpha\beta)$$

は K 上の symmetric $\mathbb{Q}$-bilinear form を定めるが, これを K あるいは f の trace form と呼び, symmetric $\mathbb{Q}$-bilinear form space $(K, \mathrm{Tr}_{K/\mathbb{Q}})$ を Tr_K または Tr_f と表すことにする. また, $\mathrm{Tr}_{K/\mathbb{Q}}$ を K の整数環 O_K に制限すると, トレースの性質から値は有理整数環 $\mathbb{Z}$ に取ることが分かり, O_K 上の symmetric $\mathbb{Z}$-bilinear form $\mathrm{tr}_{K/\mathbb{Q}}$ が定まる. これを K あるいは f の integral trace form と呼び, symmetric $\mathbb{Z}$-bilinear form module $(O_K, \mathrm{tr}_{K/\mathbb{Q}})$ を tr_K または tr_f と表す. 以下, tr_f の $\mathbb{Z}_p$ への係数拡大を $\mathrm{tr}_{K,p}$ または $\mathrm{tr}_{f,p}$ と表す.

一般に, trace form あるいは integral trace form の本格的な研究は, O. Taussky [**?**] から始まったとされており, その後 Conner-Perlis [**?**] や Serre [**?**] 等により, 興味深い問題の提出や, Galois cohomology との関連から Galois の逆問題への応用等がなされ, 現在までの研究の道筋がつけられた. 数多くある (integral) trace form に関連する話題のうち, 本稿で扱う問題は次のものである.

Problem 1.1　symmetric $\mathbb{Q}$ ($\mathbb{Z}$)-bilinear form のうち, (integral) trace form から定まるものを全て決定せよ. または, 全ての (integral) trace form を具体的に計算せよ.

本稿の目的は, [**?**], [**?**] に基づき, 円分体の integral trace form と, ある種の trinomial から定まる integral trace form に関し, その $\mathbb{Z}$ 上の直交分解と, p 進整数環 $\mathbb{Z}_p$ 上の標準形の具体的な明示式を紹介をすることである.

最後に記号の準備をしておく ([**?**] 参照). R を単位的可換環とし, (X_1, β_1), (X_2, β_2) を symmetric R-bilinear form module とする. (X_1, β_1) と (X_2, β_2) が symmetric R-bilinear form module として同型となるとき, $(X_1, \beta_1) \simeq_R (X_2, \beta_2)$ (または単に $X_1 \simeq_R X_2$) と表し, (X_1, β_1) と (X_2, β_2) の (symmetric R-bilinear form module としての) 直和を $(X_1, \beta_1) \oplus (X_2, \beta_2)$ (または単に $X_1 \oplus X_2$) と表す. 特に, 0 以上の整数 $m \in \mathbb{Z}_{\geq 0}$ に対し, $m \times (X_1, \beta_1)$ (または単に $m \times X_1$) で, (X_1, β_1) の m 個の直和を表す;

$$m \times (X_1, \beta_1) = m \times X_1 := \begin{cases} \underbrace{X_1 \oplus \cdots \oplus X_1}_{m} & m \geq 1, \\ \langle 0 \rangle & m = 0. \end{cases}$$

次に, (X_1, β_1) と (X_2, β_2) のテンソル積を $(X_1, \beta_1) \otimes (X_2, \beta_2)$ (または単に $X_1 \otimes X_2$) と表す. また, R 係数の $n \times n$ 対称行列 M に対し, M が定める R^n 上の symmetric R-bilinear form module を $\langle M \rangle_R$ と表すものとし, 記号の簡単のため, $\langle a \rangle X_1 := \langle [a] \rangle \otimes X_1$ ($\forall a \in R$) とおく. 特に, G, H で以下の空間を表す;

$$G = \left\langle \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \right\rangle_R,\ H = \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle_R.$$

2 Relationships between (integral) trace forms and Bezoutian forms

$f_1(x)$, $f_2(x) \in R[x]$ を R 上の多項式とし, $n \geq \max\{\deg f_1, \deg f_2\}$ を満たす整数 n に対し,

$$B_n(f_1, f_2) := \frac{f_1(x)f_2(y) - f_1(y)f_2(x)}{x-y} = \sum_{i,j=1}^{n} \alpha_{ij} x^{i-1} y^{j-1} \in R[x,y],$$
$$M_n(f_1, f_2) := [\alpha_{ij}]_{1 \leq i,j \leq n}$$

とおく. このとき, $M_n(f_1, f_2)$ は R 係数の対称行列となり, R^n 上の symmetric R-bilinear form を定める. この symmetric R-bilinear form を f_1 と f_2 の Bezoutian form (Bezout の二次形式) と呼ぶ. 以後, $M_n(f_1) := M_n(f_1, f_1')$ (f_1' は f_1 の形式的な微分) と表す. Bezoutian form (Bezout の二次形式) に関しては, 高木 [**?**], Krein-Naimark [**?**] に優れた解説がある. 本稿で述べる結果は全て, 次の定理により (integral) trace form を Bezoutian form と見ることにより得られる結果であることを注意しておく.

Theorem 2.1　$K = \mathbb{Q}(\theta)$ を n 次の代数体とし, θ の $\mathbb{Q}$ 上の最小多項式を $f(x)$ とおく. このとき, $\mathrm{Tr}_K \simeq_{\mathbb{Q}} \langle M_n(f) \rangle_{\mathbb{Q}}$. ここで, θ を適当に整数倍して $f(x) \in \mathbb{Z}[x]$ としておくと, $\mathrm{tr}_K \simeq_{\mathbb{Z}} \langle M_n(f) \rangle_{\mathbb{Z}}$ となるための必要十分条件は, 1, θ, $\cdots$, θ^{n-1} が K の整基底をなすことである. 特に, この条件が成り立つときは, $\mathrm{tr}_{K,p} \simeq_{\mathbb{Z}_p} \langle M_n(f) \rangle_{\mathbb{Z}_p}$ である.

3 Main results for cyclotomic fields

以後, 1 の原始 n 乗根 ζ_n に対し, $\mathrm{tr}_n := \mathrm{tr}_{\mathbb{Q}(\zeta_n)}$ とおく. 一般性を失うことなく, n が偶数ならば 4 で割れていると仮定する. また, $I^{(r)}$ で集合 $\{0,1\}$ の r 個の直積を, $\mathbf{i}^{(r)} = (i_1, i_2, \cdots, i_r)$ で $I^{(r)}$ の任意の元を表すものとする.

Theorem 3.1　n を 3 以上の整数とし, その素因数分解を $n = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ とし, $n' = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ とおく.

(i)　$e = 0$ のとき,

$$\mathrm{tr}_n \simeq_{\mathbb{Z}} \bigoplus_{\mathbf{i}^{(r)} \in I^{(r)}} \langle (-1)^{\sum_{m=1}^r i_m} n \prod_{m=1}^{r} p_m^{i_m} \rangle X_n^{(\mathbf{i}^{(r)})}.$$

ここで,

$$X_n^{(\mathbf{i}^{(r)})} = \langle 1 \rangle \oplus \big(\prod_{m=1}^{r} p_m^{e_m - 1}(p_m - 2)^{i_m + 1} - 1 \big)/2 \times H.$$

(ii)　$e \geq 2$ のとき,

$$\mathrm{tr}_n \simeq_{\mathbb{Z}} \begin{cases} \langle 2^{e-1} \rangle \big(\langle 1 \rangle \oplus \langle -1 \rangle \oplus (2^{e-2} - 1) \times H \big), & n' = 1, \\ \bigoplus_{\mathbf{i}^{(r)} \in I^{(r)}} \langle (-1)^{\sum_{m=1}^r i_m} (n/2) \prod_{m=1}^r p_m^{i_m} \rangle Y_n^{(\mathbf{i}^{(r)})}, & n' > 1. \end{cases}$$

ここで,

$$Y_n^{(\mathbf{i}^{(r)})} = \langle 1 \rangle \oplus \langle -1 \rangle \oplus \big(2^{e-2} \prod_{m=1}^{r} p_m^{e_m - 1}(p_m - 2)^{i_m + 1} - 1 \big) \times H.$$

次に, $\mathrm{tr}_{n,p} := \mathrm{tr}_{\mathbb{Q}(\zeta_n),p}$ の標準形に関する結果を述べる. そのため, 以下では $\varphi(*)$ で Euler's totient function を, D_n で円分体 $\mathbb{Q}(\zeta_n)$ の判別式をそれぞれ表すものとする. また, p を奇素数とする時, 任意の p 進単数 $a \in \mathbb{Z}_p^\times$ に対し,

$$u_{a,p} := \begin{cases} 1, & a \in (\mathbb{Z}_p^\times)^2, \\ u_p, & a \notin (\mathbb{Z}_p^\times)^2 \end{cases}$$

とおく. ここで, u_p は p を法として平方非剰余となる正の整数のうち, 最小のものを表す. 他方, $p = 2$ の時は, $u_{a,2}$ ($a \in \mathbb{Z}_2^\times$) を次のように定義する;

$$u_{a,2} = \begin{cases} 1 & a \in (\mathbb{Z}_2^\times)^2, \\ 3 & a \in 3(\mathbb{Z}_2^\times)^2, \\ 5 & a \in 5(\mathbb{Z}_2^\times)^2, \\ 7 & a \in 7(\mathbb{Z}_2^\times)^2. \end{cases}$$

Theorem 3.2　p を奇素数とする．また, n を 3 以上の整数とし, $n = p^e n'$ $(e \geq 0,\ p \nmid n')$ と表す．

(1)　$e = 0$ のとき,

$$\mathrm{tr}_{n,p} \simeq_{\mathbb{Z}_p} (\varphi(n) - 1) \times \langle 1 \rangle \oplus \langle u_{D_n,p} \rangle.$$

(2)　$e \geq 1$ のとき,

$$\mathrm{tr}_{n,p} \simeq_{\mathbb{Z}_p} \langle p^{e-1} \rangle \big((n_1 \times \langle 1 \rangle) \oplus \langle u_{a_1,p} \rangle \big) \oplus \langle p^e \rangle \big((n_2 \times \langle 1 \rangle) \oplus \langle u_{a_2,p} \rangle \big).$$

ここで,

$$a_1 = \begin{cases} (-1)^{1+(p^{e-1}-1)/2}, & n' = 1, \\ D_{n'}, & n' > 1, \end{cases} \quad a_2 = \begin{cases} (-1)^{(p^{e-1}(p-2)-1)/2}, & n' = 1, \\ D_{n'}, & n' > 1 \end{cases}$$

かつ

$$n_1 = \varphi(n')p^{e-1} - 1, \quad n_2 = \varphi(n')p^{e-1}(p-2) - 1.$$

Theorem 3.3　n を 3 以上の整数とし, その素因数分解を $n = 2^e p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ とし, $n' = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ とおく．

(1)　$e = 0$ のとき,

$$\mathrm{tr}_{n,2} \simeq_{\mathbb{Z}_2} \Big(\bigoplus_{\mathbf{i}^{(r)} \in I^{(r)}} \langle (-1)^{\sum_{m=1}^r i_m} n \prod_{m=1}^r p_m^{i_m} \rangle \Big) \oplus \big((\varphi(n) - 2^r)/2 \times H \big).$$

(2)　$e \geq 2$ のとき,

$$\mathrm{tr}_{n,2} \simeq_{\mathbb{Z}_2} \begin{cases} \langle 2^{e-1} \rangle \big(\langle 1 \rangle \oplus \langle -1 \rangle \oplus (2^{e-2} - 1) \times H \big), & n' = 1, \\ \langle 2^{e-1} \rangle \big(Z_n \oplus \langle -1 \rangle Z_n \oplus (\varphi(n) - 2^{r+1})/2 \times H \big), & n' > 1. \end{cases}$$

ここで,

$$Z_n = \bigoplus_{\mathbf{i}^{(r)} \in I^{(r)}} \langle (-1)^{\sum_{m=1}^r i_m} n' \prod_{m=1}^r p_m^{i_m} \rangle.$$

4　Main results for certain trinomial extensions

$P_n(x) := x^n + nklx^s + l$ を以下の性質 (P.1), (P.2), (P.3) を満たす trinomial とする;

(P.1)　$1 \leq s < n$ かつ $\gcd(n, s) = 1$.
(P.2)　$k, l \in \mathbb{Z}$ かつ n の素因数は l の素因数でもある．
(P.3)　l と $d := 1 + (-1)^{n-1}(n-s)^{n-s}k^n(ls)^s$ は平方因子を持たない．

また, $n(s) := 2s + 1$ とおき, s' を次のように定義する;

$$s' := \begin{cases} s & n(s) \leq n, \\ n - s & n(s) > n. \end{cases}$$

ここで, $s' \geq 2$ ならば, ユークリッドの互除法から

$$r_0 = n,\ r_1 = s',$$
$$r_{m-1} = q_{m-1}r_m + r_{m+1}\ (0 < r_{m+1} < r_m,\ 1 \leq m \leq \omega),\ r_\omega = q_\omega r_{\omega+1}\ (r_{\omega+1} = 1)$$

を満たす正整数 q_m と r_m が取れる．$s' = 1$ のときは, $q_0 = n - 1$, $r_2 = 1$ とおくこととする．

Theorem 4.1　n を上記の条件を満たす任意の整数とし, n が奇数ならば,

$$a_0 = \begin{cases} s\{-(n-s)k\}^{q_0-1}kl & n(s) \leq n, \\ s'\{-(n-s')kl\}^{q_0-1}k & n(s) > n, \end{cases} \quad b_0 = \begin{cases} (n-s)k & n(s) \leq n, \\ (n-s')kl & n(s) > n, \end{cases}$$
$$a_m = (-a_{m-1})^{q_m} b_{m-1},\ \ b_m = a_{m-1}\ (1 \leq m \leq \omega - 1),$$
$$d_0 = \begin{cases} a_0 & s' = 1, \\ -a_{\omega-2}b_{\omega-2} & s' \geq 2,\ r_{\omega-1} = r_\omega + 1,\ r_\omega : \text{odd}, \\ a_{\omega-1} & \text{それ以外} \end{cases}$$

とおく. このとき,

$$\mathrm{tr}_{P_n} \simeq_{\mathbb{Z}} \langle n\rangle \oplus \langle -nl\rangle\big(X_0 \oplus n_0 \times H\big).$$

ここで,

$$X_0 = \begin{cases} \left\langle \begin{bmatrix} d_0 & 1 \\ 1 & (1-d)/d_0 \end{bmatrix} \right\rangle & n : \text{odd}, \\ \langle d\rangle & n : \text{even}, \end{cases} \quad n_0 = \begin{cases} (n-3)/2 & n : \text{odd}, \\ (n-2)/2 & n : \text{even}. \end{cases}$$

次に, tr_{P_n} を $\mathbb{Z}_p$ まで係数拡大して得られる $\mathrm{tr}_{P_n,p}$ の標準形に関する結果を述べる. 以下, 任意の $r \in \mathbb{Z}_p$ に対し, $v_p(r)$ で r の p 進付値を表すものとする. また, 多項式 $f(x) \in \mathbb{Q}[x]$ に対し, $d(f)$ で f の判別式を表すものとする.

Theorem 4.2 p を奇素数とし, $n = p^{\varepsilon_n} n_p$, $d = p^{\varepsilon_d} d_p$, $l = p^{\varepsilon_l} l_p$ $(\varepsilon_n = v_p(n), \varepsilon_d = v_p(d), \varepsilon_l = v_p(l))$ と表す.

(1) $p \nmid l$ かつ $p \nmid d$ のとき,

$$\mathrm{tr}_{P_n,p} \simeq_{\mathbb{Z}_p} (n-1) \times \langle 1\rangle \oplus \langle u_{d(P_n),p}\rangle.$$

(2) $p \nmid l$ かつ $p \mid d$ のとき,

$$\mathrm{tr}_{P_n,p} \simeq_{\mathbb{Z}_p} \langle p\rangle\langle u_{d'_0,p}\rangle \oplus \big((n-2) \times \langle 1\rangle \oplus \langle u_{d'_1,p}\rangle\big).$$

ここで,

$$d'_0 = \begin{cases} nd_p l/d_0 & n : \text{odd}, \\ -nd_p l & n : \text{even}, \end{cases} \quad d'_1 = \begin{cases} (-1)^{(n-1)/2} n^{n-1} d_0 l^{n-2} & n : \text{odd}, \\ (-1)^{(n-2)/2} n^{n-1} l^{n-2} & n : \text{even}. \end{cases}$$

(3) $p \mid l$ のとき,

$$\mathrm{tr}_{P_n,p} \simeq_{\mathbb{Z}_p} \langle p^{\varepsilon_n}\rangle\langle u_{n_p,p}\rangle \oplus \langle p^{\varepsilon_n+1}\rangle\big((n-2) \times \langle 1\rangle \oplus \langle u_{d'_2,p}\rangle\big).$$

ここで,

$$d'_2 = \begin{cases} (-1)^{(n-1)/2} n_p^{n-1} d l_p^{n-1} & n : \text{odd}, \\ (-1)^{n/2} n_p^{n-1} d l_p^{n-1} & n : \text{even}. \end{cases}$$

Theorem 4.3 $n = 2^{\varepsilon_n} n_2$, $l = 2^{\varepsilon_l} l_2$ $(\varepsilon_n = v_2(n), \varepsilon_l = v_2(l))$ とおく.

(1) $2 \nmid n$ のとき,

$$\mathrm{tr}_{P_n,2} \simeq_{\mathbb{Z}_2} \begin{cases} \langle u_{n,2}\rangle \oplus G \oplus (n-3)/2 \times H & 2 \nmid kl,\ n = 3 \text{ or } 2 \nmid kl,\ s' = 2, \\ \langle u_{n,2}\rangle \oplus \langle 2^{\varepsilon_l}\rangle\big((n-1)/2 \times H\big) & \text{それ以外}. \end{cases}$$

(2) $2 \mid n$ のとき,

$$\mathrm{tr}_{P_n,2} \simeq_{\mathbb{Z}_2} \langle 2^{\varepsilon_n}\rangle\langle u_{n_2,2}\rangle \oplus \langle 2^{\varepsilon_n+1}\rangle\big(\langle u_{-n_2 dl_2,2}\rangle \oplus (n-2)/2 \times H\big).$$

参考文献

[1] P. E. Conner; R. Perlis. A survey of trace forms of algebraic number fields. Series in Pure Mathematics, 2. World Scientific Publishing Co., Singapore, 1984.

[2] M. G. Krein; M. A. Naimark. The method of symmetric and Hermitian forms in the theory of the separation of the roots of algebraic equations. Linear and Multilinear Algebra 10 (1981), no. 4, 265-308.

[3] J. Milnor; D. Husemoller. Symmetric bilinear forms. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73. Springer-Verlag, New York-Heidelberg, 1973.

[4] S. Otake. Orthogonal decompositions of integral trace forms of cyclotomic fields and their canonical forms over the ring of p-adic integers. J. Number Theory 134 (2014), 258-279.

[5] S. Otake. A Bezoutian approach to orthogonal decompositions of trace forms or integral trace forms of some classical polynomials. Linear Algebra Appl. 471 (2015), 291-319.

[6] T. Takagi, *daisuugakukougi kaiteishimban*. (Japanese) Kyouritsushuppan (1965).

[7] O. Taussky. The discriminant matrices of an algebraic number field. J. London Math. Soc. 43 (1968), 152-154.

[8] J. P. Serre. L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$. Comment. Math. Helv. 59 (1984), no. 4, 651-676.