実円分体上の素数次巡回拡大の相対冪整基底について

東京理科大学大学院 理工学研究科 数学専攻
関川隆太郎 (Ryutaro SEKIGAWA)

概要

代数体 K の整数環 $\mathcal{O}_K$ が $\mathbb{Z}$ 上 1 元生成であるかという冪整基底問題は古くから続く未解決問題である. 代数拡大 K/k においても, 同様に相対冪整基底問題が考えられている. 本講演では, 陸名の巡回生成多項式が与える素数次巡回拡大が相対冪整基底をもつための十分条件と, 条件を満たす体が無限個存在することなどを紹介する.

1 導入

有理数体 $\mathbb{Q}$ の有限次拡大体 K を代数体という. $\alpha \in K$ がある整数係数モニック多項式の根となるとき, $\alpha \in K$ は代数的整数であるという. K に属する代数的整数全体の集合を K の整数環といい, $\mathcal{O}_K$ で表す. K が冪整基底をもつとは, $\mathcal{O}_K$ が整数環 $\mathbb{Z}$ 上一元生成されるとき, すなわち, ある $\alpha \in \mathcal{O}_K$ で

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \{x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} \mid x_i \in \mathbb{Z}\} \quad (n := [K : \mathbb{Q}])$$

を満たすものが存在するときのことをいう. このとき, K は monogenic であるなどともいわれる. 代数拡大 K/k に関しても同様にして, ある $\alpha \in \mathcal{O}_K$ で $\mathcal{O}_K = \mathcal{O}_k[\alpha]$ を満たすものが存在するとき, K/k は (相対) 冪整基底をもつという. 与えられた代数体が (相対) 冪整基底をもつかどうか特徴付ける問題は古くから研究されている.

簡単のため, $K/\mathbb{Q}$ をガロア拡大とし, そのガロア群 を G で表す. K の判別式を d_K で表すと, $\alpha \in \mathcal{O}_K$ が冪整基底を生成することと, 以下が成り立つことは同値である.

$$\pm d_K = d_K(\alpha) := \mathrm{N}_{K/\mathbb{Q}}\left(\prod_{\sigma \in G\setminus\{id\}} (\alpha - \alpha^\sigma)\right). \tag{1.1}$$

代数拡大 K/k については, k のイデアルとしての等式となることに注意が必要だが, 同様のことが成り立つ. 冪整基底に関する研究の多くはこの方程式が糸口となっている.

今回, 単数群やその Galois コホモロジーなどを用いた代数的な手法による進展があったので紹介したい. 具体的には, 陸名の巡回生成多項式が与える素数次巡回拡大が相対冪整基底をもつための十分条件と, 条件を満たす体が無限個存在することなどを紹介する.

2　先行研究

良く知られた具体例と先行研究を紹介する. 例えば, 2 次体 K は平方因子をもたない整数 d で

$$K = \mathbb{Q}(\sqrt{d}), \qquad \mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & (d \equiv 1 \bmod 4), \\ \mathbb{Z}[\sqrt{d}] & (d \equiv 2, 3 \bmod 4) \end{cases}$$

と表せることは良く知られている. また, ζ_m を 1 の原始 m 乗根とすると, 円分体 $\mathbb{Q}(\zeta_m)$ やその最大実部分体 $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ に関しては

$$\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m], \qquad \mathcal{O}_{\mathbb{Q}(\zeta_m+\zeta_m^{-1})} = \mathbb{Z}[\zeta_m + \zeta_m^{-1}].$$

他にも様々な代数体に関して冪整基底の研究がされてきた. 特に $\mathbb{Q}$ 上の素数 p 次アーベル拡大（すなわち巡回拡大）に関する結果をいくつか紹介する. $p = 2$ の場合, 上記通り常に冪整基底をもつ. $p \geq 5$ の場合, 円分体の最大実部分体と一致するときを除いて, 冪整基底をもたないことが Gras によって証明された [6]. 残る $p = 3$ の場合については, Archinard [1] や Gras [3, 4, 5] による研究などがある. 冪整基底をもつ場合ともたない場合があり, その必要十分条件は明らかになっている [3, Théorème 2]. また, Dummit と Kisilevsky は 3 次巡回拡大で冪整基底をもつ体ともたない体のどちらも無限個存在することを示した [2].

講演者と加塩朋和氏（東京理科大学）は, $p = 3$ のときについて研究し, 単数群やその Galois コホモロジー, Shanks の巡回 3 次式を用いて, 冪整基底をもつための必要十分条件の別証明を与え, 整理した [7]. この結果をもとに, 講演者は, 陸名の巡回生成多項式によって定義される素数次巡回拡大の相対冪整基底に関する結果を得た.

3　陸名の巡回生成多項式

l を奇素数, $\zeta_l = e^{\frac{2\pi i}{l}}$, $k = \mathbb{Q}(\zeta_l + \zeta_l^{-1})$ とする. 多項式 $p(X), q(X) \in k[X]$ と $F_u(X) \in k(u)[X]$ を次で定義する.

$$\begin{aligned} p(X) &= \frac{\zeta_l^{-1}(X - \zeta_l)^l - \zeta_l(X - \zeta_l^{-1})^l}{\zeta_l^{-1} - \zeta_l}, \\ q(X) &= \frac{(X - \zeta_l)^l - (X - \zeta_l^{-1})^l}{\zeta_l^{-1} - \zeta_l}, \\ F_u(X) &= p(X) - uq(X). \end{aligned}$$

$F_u(X)$ は陸名の巡回生成多項式という. 今回, $\Omega_s(X) := F_{\frac{s}{l}}(X) \in k(s)[X]$ を考える.

注意 3.1. $F_u(X)$ は陸名によって定義された巡回拡大を生成する generic 多項式であり, より一般の場合で定義されている. 詳細については [9] を, $\Omega_s(X)$ については [8] を参照されたい.

以下 $s \in \mathcal{O}_k$, $\omega := \zeta_l + \zeta_l^{-1}$ とし, $\Omega_s(X)$ の根を θ_s, k 上の最小分解体を K_s で表す. K_s/k に関して, 以下が成り立つ.

- K_s/k は l 次巡回拡大である. そのガロア群の生成元を σ とおく.
- 根 θ_s は K_s の単数であり以下を満たす. ただし $\nu_j := \frac{\zeta^j-\zeta^{-j}}{\zeta-\zeta^{-1}} \in k$ とおき, 必要があれば σ を取りかえる.

$$\mathrm{N}_{K_s/k}(\theta_s)=1, \quad \mathrm{Tr}_{K_s/k}(\theta_s)=s, \quad \sigma^j(\theta_s)=\frac{\nu_{j+1}\theta_s-\nu_j}{\nu_j\theta_s-\nu_{j-1}} \quad (j\in\{0,1,\dots,l-1\}).$$

- Δ_s を $s^2-l\omega s+l^2\in k$ で生成される k の単項イデアルとする. Δ_s^{l-1} は $\Omega_s(X)$ の判別式と等しい. すなわち,

$$\Delta_s^{l-1}=\left(\mathrm{N}_{K_s/k}\left(\prod_{\sigma\neq id}(\theta_s-\sigma(\theta_s))\right)\right).$$

- K_s/k の導手を $\mathfrak{c}_{K_s/k}$, 判別式を $\mathfrak{d}_{K_s/k}$ とすると, 次が成り立つ.

$$\mathfrak{c}_{K_s/k}^{l-1}=\mathfrak{d}_{K_s/k}\mid\Delta_s^{l-1}.$$

例 3.2. $l=3,5$ の場合, $\Omega_s(X)$ は以下のようになる.

(i) $l=3$, $(\omega=\zeta_3+\zeta_3^{-1}=-1,)$

$$\Omega_s(X)=X^3-sX^2-(s+3)X-1.$$

(ii) $l=5$, $\omega=\zeta_5+\zeta_5^{-1}$,

$$\Omega_s(X)=X^5-sX^4+2(\omega s-5)X^3+2\omega(s+5)X^2-(s-5\omega)X-1.$$

$l=3$ のときの $\Omega_s(X)$ は Shanks の巡回 3 次式と一致することがわかる.

4 主結果

$k=\mathbb{Q}(\zeta_l+\zeta_l^{-1})$, $s\in O_k$ とし, θ_s を $\Omega_s(X)$ の根, K_s を k 上 $\Omega_s(X)$ の最小分解体とする. 講演者は, l 次巡回拡大 K_s/k の相対冪整基底について, K_s/k の導手 $\mathfrak{c}_{K_s/k}$ と k の整イデアル $\Delta_s=\left(s^2-l(\zeta_l+\zeta_l^{-1})s+l^2\right)$ を用いた以下の結果を得た.

定理 4.1. 整イデアル $\Delta_s\mathfrak{c}_{K_s/k}^{-1}$ が k のある単項イデアルの l 乗と等しいならば, K_s/k は相対冪整基底をもつ. このとき, ある $b\in\mathcal{O}_k$ で $\Delta_s\mathfrak{c}_{K_s/k}^{-1}=(b)^l$ と表せ, 以下が成り立つ.

$$\mathcal{O}_{K_s}=\mathcal{O}_k\left[\frac{\theta_s-a}{b}\right].$$

ただし, a は $a\equiv sl^{-1} \bmod (b)$ を満たす任意の $\mathcal{O}_k$ の元とする.

注意 4.2. $l=3$ のとき, 定理 4.1 の $\Delta_s\mathfrak{c}_{K_s/k}^{-1}$ に関する条件は必要十分条件となる [7].

§3 で紹介した K_s/k に関する事実と (1.1), Newton 多角形を用いることで証明できる. Newton 多角形を考える際, 以下の補題が重要となる.

補題 4.3. l 以下の正の整数 m と相異なる $n_1, \ldots, n_m \in \{0, 1, \ldots, l-1\}$ をとる. このとき, $\mathrm{Tr}_{K_s/k}(\sigma^{n_1}(\theta_s) \cdots \sigma^{n_m}(\theta_s))$ の値は m にしかよらない.

定理 4.1 から次の系を得る.

系 4.4. 整イデアル Δ_s が素イデアルの 2 乗で割れないならば, $\mathcal{O}_{K_s} = \mathcal{O}_k[\theta_s]$.

系 4.4 と新谷の基本領域, 下の体が $k = \mathbb{Q}(\zeta_l + \zeta_l^{-1})$ であることなどを用いて, 以下を証明した.

定理 4.5. l を 5 以上の素数とする. $\mathcal{O}_{K_s} = \mathcal{O}_k[\theta_s]$ を満たす体 $K_s (s \in \mathcal{O}_k)$ は無限個存在する.

注意 4.6. 5 以上の素数 l に関して, $\mathbb{Q}$ 上 l 次巡回拡大で冪整基底をもつものは 0 個もしくは 1 個である [6]. しかし, $\mathbb{Q}(\zeta_l + \zeta_l^{-1})$ 上 l 次巡回拡大で冪整基底をもつものは無限個存在することが, 定理 4.5 からわかる.

参考文献

[1] G. Archinard, Extensions cubiques cycliques de Q dont l'anneau des entiers est monogène, Enseign. Math. (2). **20** (1974), 179–203.

[2] D. S. Dummit and H. Kisilevsky, Indices in cyclic cubic fields, Number theory and algebra (1977), 29–42.

[3] M. N. Gras, Sur les corps cubiques cycliques dont l'anneau des entiers estmonogène, Ann. Sci. Univ. Besançon Math. (3), No. 6 (1973), 26 pp.

[4] M. N. Gras, Sur les corps cubiques cycliques dont l'anneau des entiers estmonogène, C. R. Acad. Sci. Paris Sér. A **278** (1974), 59–62.

[5] M. N. Gras, Lien entre le groupe des unités et la monogèneité des corps cubiques cycliques, Séminaire de Théorie des Nombres Besançon, Année 1975-76.

[6] M. N. Gras, Non monogènéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geqq 5$, J. Number Theory **23** (1986), no. 3, 347–353.

[7] T. Kashio and R. Sekigawa, The characterization of cyclic cubic fields with power integral bases (arXiv:1912.03103), to appear in Kodai Math. J.

[8] T. Komatsu, Arithmetic of Rikuna's generic cyclic polynomial and generalization of Kummer theory, Manuscripta Math. 114 (2004), 265-279.

[9] Y. Rikuna, On simple families of cyclic polynomials, Proc. Amer. Math. Soc. **130** (2002), 2215-2218.

[10] R. Sekigawa, Rikuna's generic cyclic polynomial and the monogenity, preprint.

[11] R. Sekigawa, Relative power integral bases in certain ray class fields of an imaginary quadratic number field, preprint.

[12] D. Shanks, The simplest cubic fields, Math. Comp. **28** (1974), 1137–1152.