

低次数アーベル拡大の冪整基底について

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)

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. $\alpha \in \mathcal{O}_K$ が K の冪整基底を生成するとは, $n = [K : \mathbb{Q}]$ としたとき,

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

をみたすときをいう. 本講演ではガロア拡大を扱うため, 以下 $K/\mathbb{Q}$ はガロア拡大とし, そのガロア群 $G(K/\mathbb{Q})$ 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.

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

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.

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 の場合, 平方因子をもたない整数 d を用いて

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

であ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

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

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. 以下, 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, 上記の冪整基底をもつ. $p \geq 5$ の場合, 円分体の最大実部分体と一致するときを除いて, 冪整基底を持たないことが Gras によって証明された [Gr1]. 残る $p = 3$ の場合も, Gras が冪整基底をもつ必要十分条件を与え [Gr2], Dummit と Kisilevsky が冪整基底をもつ 3 次巡回拡大を無限個存在することを示した [DK].

著者は加塩氏との共同研究で, Gras の結果である, $\mathbb{Q}$ 上 3 次巡回拡大が冪整基底をもつ必要十分条件を整理し見通しを良くした [KS]. その後, その自然な一般化についていくつか結果を得た. 本講演ではそれらについて紹介したい.

2 3 次巡回拡大の冪整基底

この節では $\mathbb{Q}$ 上 3 次巡回拡大が冪整基底をもつ必要十分条件と冪整基底の生成元 $\gamma \in \mathcal{O}_K$ の明示的な表示を与える. 主定理を紹介する前に, 特別な 3 次巡回拡大である the simplest cubic field を定義する. 整数 t に対して, 多項式

$$f_t(x) := x^3 - tx^2 - (t+3)x - 1$$

の根を θ_t とおく. $f_t(x)$ の $\mathbb{Q}$ 上の分解体 $K_t = \mathbb{Q}(\theta_t)$ を the simplest cubic field という. K_t は基本単数が求まりやすいなどの数論的に“良い”特徴を持っており, Shanks によって定義された [Sh]. K_t のもつ性質のうち, 今回用いるものを以下に述べる.

- $K_t/\mathbb{Q}$ は 3 次巡回拡大である. ガロア群 $G = \text{Gal}(K_t/\mathbb{Q})$ の生成元を σ とおく.
- $K_t = K_{-t-3}$ が成り立つ. そのため以下 t は $t \geq -1$ とする.
- 根 θ_t は単数であり, 次を満たすように σ をとることができる.

$$\sigma(\theta_t) = \frac{-1}{1+\theta_t}, \quad \sigma^2(\theta_t) = -\frac{1+\theta_t}{\theta_t}, \quad 1+\theta_t+\theta_t\sigma(\theta_t)=0, \quad N_{K/\mathbb{Q}}(\theta_t)=1, \quad \text{Tr}_{K/\mathbb{Q}}(\theta_t)=t.$$

- $f_t(x)$ の判別式は Δ_t^2 ($\Delta_t := t^2 + 3t + 9$) である.
- 体 K の導手を c_K , 判別式を d_K とおくと,

$$c_{K_t} = \sqrt{d_{K_t}} \mid \Delta_t$$

が成り立つ ($c_{K_t} = \sqrt{d_{K_t}}$ は conductor - discriminant formula から従う).

この準備のもと, 3 次巡回拡大 $K/\mathbb{Q}$ が冪整基底をもつ必要十分条件が次のように与えられる.

定理 2.1 (Kashio and S.). $K/\mathbb{Q}$ を 3 次巡回拡大とする. このとき以下は同値である.

- K は冪整基底をもつ.
- 次を満たす $t \in \mathbb{Z}$ が存在する. $K = K_t$ かつ

$$\frac{\Delta_t}{c_K} \in \mathbb{N}^3 := \{n^3 \mid n \in \mathbb{N}\}.$$

- 次を満たす $t \in \mathbb{Z}$ が存在する. $K = K_t$ かつ

$$t \not\equiv 3, 21 \pmod{27} \text{ かつ } 3 \text{ 以外の任意の素数 } p \text{ に対して } v_p(\Delta_t) \not\equiv 2 \pmod{3}$$

また, 冪整基底を持つ場合, 整数 a で $a \equiv \frac{t}{3} \pmod{\sqrt[3]{\frac{\Delta_t}{c_K}}}$ をみたすものをとると,

$$\mathcal{O}_K = \mathbb{Z} \left[\frac{\theta_t - a}{\sqrt[3]{\frac{\Delta_t}{c_K}}} \right]$$

が成り立つ.

注意 2.2. $3 \mid \sqrt[3]{\frac{\Delta_t}{c_K}}$ ならば $3 \mid t$ が示せるため, $a \equiv \frac{t}{3} \pmod{\sqrt[3]{\frac{\Delta_t}{c_K}}}$ は意味を持つ.

岡崎氏や星氏によって, 異なる $-1 \leq t, t' \in \mathbb{Z}$ に対して $K_t = K_{t'}$ となるのは

$$K_{-1} = K_5 = K_{12} = K_{1259}, \quad K_0 = K_3 = K_{54} (= \mathbb{Q}(\zeta_9 + \zeta_9^{-1})), \quad K_1 = K_{66}, \quad K_2 = K_{2389}$$

のみであることが証明されている [Ho]. また, K_{-1}, K_0, K_1, K_2 は定理 2.1 より冪整基底を持つことが直接計算によって確かめられる. よって定理 2.1 から次の系が得られる.

系 2.3. $K/\mathbb{Q}$ を 3 次巡回拡大とする. K が冪整基底を持つならば, K は the simplest cubic field である. すなわち, $K = K_t$ となる整数 $t \geq -1$ が存在する. さらに以下は同値である.

- (i) the simplest cubic field K_t は冪整基底をもつ.
- (ii) $t \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ または $\frac{\Delta_t}{c_{K_t}} \in \mathbb{N}^3$.
- (iii) $t \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$ または

$$t \not\equiv 3, 21 \pmod{27} \text{ かつ } 3 \text{ 以外の任意の素数 } p \text{ に対して } v_p(\Delta_t) \not\equiv 2 \pmod{3}.$$

注意 2.4. 定理 2.1-(ii) は Gras によっても与えられている [Gr2]. 著者は, 定理 2.1-(iii), 系 2.3-(iii) を得た. これにより Δ_t の計算のみで K_t が冪整基底を持つか調べることができる.

以下, 定理 2.1 証明の一部の概要を述べる. まず次が示せる.

補題 2.5. $K/\mathbb{Q}$ を 3 次巡回拡大とする. $\mathfrak{C}_K$ を $N_{K/\mathbb{Q}}(\mathfrak{C}_K) = c_K$ をみたす K の整イデアルとする. K が冪整基底をもつならば, 次が成り立つ.

- $\mathfrak{C}_K$ は単項イデアルである.
- K は the simplest cubic field.

しかし, この逆は成り立たない. 実際 $t = 101471$ のとき, $\mathfrak{C}_{K_t}$ は単項イデアルだが, K_t は冪整基底をもたない. 逆が成り立つにはどのような条件が必要か考える. まずいくつか記号を準備する. K の分数イデアル全体がなす群を I_K , 単項イデアル全体がなす群を P_K とおく. さらに, I_K^G, P_K^G を次で定義する.

$$I_K^G := \{\mathfrak{A} \in I_K \mid \sigma(\mathfrak{A}) = \mathfrak{A}\}, \quad P_K^G := I_K^G \cap P_K.$$

K の単数群 $\mathcal{O}_K^\times$ を係数とする 1 次のガロアコホモロジーを $H_1(G, \mathcal{O}_K^\times)$ で表す. 補題 2.5 の逆について考えるうえで, $H_1(G, \mathcal{O}_K^\times)$ や商群 $P_K^G/P_{\mathbb{Q}}$ が重要な役割を担う.

補題 2.6. K が the simplest cubic field かつ $\mathfrak{C}_K$ が単項イデアルとする. $\mathfrak{C}_K$ の生成元を β , すなわち $\mathfrak{C}_K = (\beta)$ としたとき, 以下は同値である.

- (a) K が冪整基底をもつ.
- (b) 次を満たす $t \in \mathbb{Z}$ が存在する. $K = K_t$ かつ $[\beta^{\sigma-1}] = [\theta_t] \in H^1(G, \mathcal{O}_K^\times)$.
- (c) 次を満たす $t \in \mathbb{Z}$ が存在する. $K = K_t$ かつ $\overline{\mathfrak{C}_K} = \overline{(\theta_t - \theta_t^\sigma)} \in P_K^G/P_{\mathbb{Q}}$.
- (d) 次を満たす $t \in \mathbb{Z}$ が存在する. $K = K_t$ かつ $\frac{\Delta_t}{c_K} \in \mathbb{N}^3$.

補題 2.5, 2.6 から定理 2.1-[(i) $\Leftrightarrow$ (ii)] が導かれる. 定理 2.1 の残りの証明やこの節で述べた系や補題の証明については [KS] を参照されたい.

3 具体例

実際に定理 2.1, 系 2.3 を使って $t = 4, 39, 41, 286$ のときの K_t が冪整基底をもつか調べる.

- $t = 4$ の場合, $t \not\equiv 3, 21 \pmod{27}$, $\Delta_t = 37^1$ より冪整基底をもつ. 生成元については, $c_K \mid \Delta_t$ から $c_K = 37$ がわかるため $\mathcal{O}_{K_t} = \mathbb{Z}[\theta_t]$.
- $t = 39$ の場合, $t \not\equiv 3, 21 \pmod{27}$, $\Delta_t = 3^3 61^1$ より冪整基底をもつ. 生成元については, 実際に導手 c_{K_t} を計算すると $\frac{\Delta_t}{c_K} = 3^3$. よって $\mathcal{O}_{K_t} = \mathbb{Z}[\frac{\theta_t - 13}{3}]$.
- $t = 41$ の場合, $\Delta_t = 7^2 37^1$ すなわち $v_7(\Delta_t) = 2$ より冪整基底をもたない.
- $t = 286$ の場合, $t \equiv 16 \not\equiv 3, 21 \pmod{27}$, $\Delta_t = 7^3 241^1$ より冪整基底をもつ. 生成元については, 実際に計算すると $\frac{\Delta_t}{c_K} = 7^3$. よって $\mathcal{O}_{K_t} = \mathbb{Z}[\frac{\theta_t - 2}{7}](\frac{286}{3} \equiv 2 \pmod{7})$.

その他の例については [KS] を参照されたい. c_K , Δ_t の値の表や冪整基底をもたない K_t の表など載せている.

参考文献

- [Cu] Cusick, T. W., Lower bounds for regulators, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), *Lecture Notes in Math.*, **1068** (1984) 63–73.
- [DK] Dummit, D. S., Kisilevsky, H., Indices in cyclic cubic fields, *Number theory and algebra* (1977), 29–42. Academic Press, New York.
- [Gr1] Gras, M. N., Non monogénéité de l’anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$, *J. Number Theory* **23** (1986), no. 3, 347–353.
- [Gr2] Gras, M. N., Sur les corps cubiques cycliques dont l’anneau des entiers est monogène, *Ann. Sci. Univ. Besançon Math.*, (3), Fasc. 6 (1973).
- [KS] Kashio, T., Sekigawa, S., On the monogeneity of the rings of integers of cyclic cubic fields, preprint, arXiv:1912.03103.
- [Ho] Hoshi, A., On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields, *J. Number Theory* **131** (2011), no. 11, 2135–2150.
- [Se] Sekigawa, R., Relative power integral bases in certain ray class fields of an imaginary quadratic number field, preprint.
- [Sh] Shanks, D., The simplest cubic fields, *Math. Comp.* **28** (1974), 1137–1152.
- [Yo] Yokoi, H., On the class number of a relatively cyclic number field, *Nagoya Math. J.* **29** (1967), 31–44.