素数次巡回拡大体の正規整基底 *

青木 美穂 (島根大学)

1　正規整基底とガウス周期

$K/\mathbb{Q}$ を有限次ガロア拡大とし, $\mathcal{O}_K$ を K の整数環, $n := [K : \mathbb{Q}]$, $G :=\mathrm{Gal}(K/\mathbb{Q})$ とおく. $a \in K$, $x = \sum_{\sigma\in G} n_\sigma\sigma \in K[G]$ に対し, $x.a := \sum_{\sigma\in G} n_\sigma\, \sigma(a)$ と定めると, K は $K[G]$ 加群である. 同様に O_K は $O_K[G]$ 加群である.

定義 1.1. ある $\xi\,(\in \mathcal{O}_K)$ に対し, $\{\sigma(\xi)\,|\,\sigma \in G\}$ が K の整基底 ($\mathcal{O}_K$ の $\mathbb{Z}$ 自由加群としての基底) であるとき, $\{\sigma(\xi)\,|\,\sigma \in G\}$ を K (または $K/\mathbb{Q}$) の正規整基底 (Normal Integral Basis, NIB)[1]という. このとき, $\mathbb{Z}[G]$ 加群としての同型 $\mathcal{O}_K \simeq \mathbb{Z}[G]$, $\xi \mapsto 1_G$ が成り立つ. ξ を K の正規整基底の生成元という.

補題 1.2. 有限次ガロア拡大 $K/\mathbb{Q}$ が NIB をもつと仮定し, ξ をその生成元とする. このとき,

$$\{x \in \mathcal{O}_K\,|\,K \text{ の NIB の生成元 }\} = \{u.\xi\,|\,u \in \mathbb{Z}[G]^\times\}$$

が成り立つ. また, $u.\xi = v.\xi$ $(u, v \in \mathbb{Z}[G]^\times)$ ならば $u = v$ が成り立つので K の NIB の生成元と $\mathbb{Z}[G]^\times$ の元は 1 対 1 に対応する.

素数位数巡回群 G に対し, $\mathbb{Z}[G]^\times$ の構造は次で与えられる.

補題 1.3. p を素数, G を位数 p の巡回群とすると, 次の群の同型が成り立つ.

$$\mathbb{Z}[G]^\times \simeq \begin{cases} \{u \in \mathbb{Z}[\zeta_p]^\times\,|\,u \equiv \pm 1 \pmod{(1-\zeta_p)}\} & (p \neq 2), \\ \{\pm 1\} \times \{\pm 1\} & (p = 2). \end{cases}$$

例題 1.4. p を素数, $G = \langle\sigma\rangle$ を位数 p の巡回群とする.[2]
(1) $p = 2$ のとき, $\mathbb{Z}[G]^\times = \{\pm 1_G, \pm\sigma\}$.
(2) $p = 3$ のとき, $\mathbb{Z}[G]^\times = \{\pm 1_G, \pm\sigma, \pm\sigma^2\}$.
(3) $p = 5$ のとき, $\mathbb{Z}[G]^\times = \{\pm\sigma^\ell(1 - \sigma^2 - \sigma^3)^k\,|\,\ell \in \mathbb{Z}/5\mathbb{Z},\, k \in \mathbb{Z}\}$ $(\simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z})$.

有理数体上のアーベル拡大体 K が NIB をもつための必要十分条件は, $K/\mathbb{Q}$ が馴分岐拡大であることである.

*本研究は橋本優さん (島根大学) との共同研究であり, JSPS 科研費 JP21K03181 の助成を受けています.
[1]一般の有限次ガロア拡大 L/K, $G :=\mathrm{Gal}(L/K)$ に対しても, $\mathcal{O}_L$ が $\mathcal{O}_K$ 自由加群であり, ある $\eta\,(\in \mathcal{O}_L)$ に対し $\{\sigma(\xi)\,|\,\sigma \in G\}$ が $\mathcal{O}_L$ の $\mathcal{O}_K$ 自由加群としての基底となるとき, $\{\sigma(\xi)\,|\,\sigma \in G\}$ を L/K の正規整基底という.
[2]一般に $p \geq 5$ のとき $\mathbb{Z}[G]^\times$ は無限群である.

定理 1.5 (Hilbert-Speiser)**.** 有限次アーベル拡大 $K/\mathbb{Q}$ に対し, 次の 3 条件は同値である.[3]

(i) $K/\mathbb{Q}$ は馴分岐拡大.

(ii) K の導手は平方因子をもたない.

(iii) $K/\mathbb{Q}$ は NIB をもつ.

特に導手 $\mathfrak{f}$ の円分体 $\mathbb{Q}(\zeta_\mathfrak{f})$ が NIB をもつための必要十分条件は $\mathfrak{f}$ が平方因子をもたないことであり, このとき $\{\sigma(\zeta_\mathfrak{f}) \mid \sigma \in G\}$ は $\mathbb{Q}(\zeta_\mathfrak{f})$ の NIB である. ここで正の整数 N に対し, ζ_N を 1 の原始 N 乗根とする. 一般の有限次馴分岐アーベル拡大 $K/\mathbb{Q}$ に対し, K の NIB の生成元は以下のガウス周期で与えられる ([20, Proposition 4.31]).

定義 1.6. 導手 $\mathfrak{f}$ の有限次アーベル拡大 $K/\mathbb{Q}$ に対し,

$$\eta := \mathrm{Tr}_{\mathbb{Q}(\zeta_\mathfrak{f})/K}(\zeta_\mathfrak{f})$$

とそのガロア共役を K のガウス周期という.

例題 1.7. 2 次体 $K = \mathbb{Q}(\sqrt{m})$ ($m\,(\neq 1, 0)$ は平方因子を含まない整数) の導手は,

$$\mathfrak{f} = \begin{cases} |m| & (m \equiv 1 \pmod 4), \\ 4|m| & (m \equiv 2, 3 \pmod 4) \end{cases}$$

であるので, K が NIB をもつための必要十分条件は, $m \equiv 1 \pmod 4$ である. またこのとき, $\mu(\mathfrak{f})(1+\sqrt{m})/2$, $\mu(\mathfrak{f})(1-\sqrt{m})/2$ (μ はメビウス関数) は K のガウス周期であり, NIB は $\{(1+\sqrt{m})/2, (1-\sqrt{m})/2\}$ と $\{-(1+\sqrt{m})/2, -(1-\sqrt{m})/2\}$ である (NIB の生成元は 4 個).

本稿では, 有限次馴分岐アーベル拡大 $K/\mathbb{Q}$ のすべての NIB を例題 1.7 のように, 導手に依存しない, K の定義多項式の根 ($K = \mathbb{Q}(\rho)$ と表したときの ρ の共役元) を用いて表すことについて考え, Shanks の 3 次巡回拡大体, Lehmer の 5 次巡回拡大体について得られた結果 ([13, 14]) について解説する.

2 Shanks の 3 次巡回拡大体

整数 n に対し定義される次の多項式を Shanks の多項式 ([23]) という.

$$f_n^{\mathrm{Sh}}(X) = X^3 - nX^2 - (n+3)X - 1$$

以下整数 n を固定し, ρ を $f_n^{\mathrm{Sh}}(X)$ の任意の根とし, $K^{\mathrm{Sh}} = \mathbb{Q}(\rho)$ とおく.[4] Shanks の 3 次巡回拡大体について, 以下のことが知られている.

(1) $f_n^{\mathrm{Sh}}(X)$ は $\mathbb{Q}$ 上既約.

[3] この定理の主張の (i) と (iii) の同値については「アーベル拡大」の仮定を外すと反例がある. Fröhlich [8] は馴分岐 quaternion field で NIB をもたない例を無限個構成している. 例えば $k = \mathbb{Q}(\sqrt{5}, \sqrt{21})$ の 2 次拡大体 $K = k(\sqrt{-3\sqrt{105}(\sqrt{5}-1)(\sqrt{21}-1)})$ は quaternion field (ガロア拡大で, ガロア群が位数 8 の四元数群と同型) であり判別式は $D_K = 3^6 \times 5^6 \times 7^6$ より $K/\mathbb{Q}$ は馴分岐拡大. 一方, $\mathrm{Gal}(K/\mathbb{Q})$ の 2 次元既約表現 ρ に対し, Artin root number $w(\rho)$ は -1 であることから $K/\mathbb{Q}$ は NIB をもたないことがわかる.

[4] この体は simplest cubic field と呼ばれている.

(2) $K^{\mathrm{Sh}}/\mathbb{Q}$ は3次巡回拡大であり, ガロア群の生成元は $\mathrm{Gal}(K^{\mathrm{Sh}}/\mathbb{Q}) = \langle\sigma\rangle$, $\sigma(\rho) = -1/(1+\rho)$ で与えられる. つまり $f_n^{\mathrm{Sh}}(X)$ の ρ 以外の根は $\rho' := -1/(1+\rho)$, $\rho'' := -1/(1+\rho')$ である.

(3) $\Delta_n := n^2+3n+9$ とおくと, $f_n^{\mathrm{Sh}}(X)$ の判別式は, $d(f_n^{\mathrm{Sh}}) = \Delta_n^2$ である.

(4) $\Delta_n = bc^3$ $(b, c \in \mathbb{Z}_{>0}, b$ は立方因子をもたない) とおくと, K^{Sh} の判別式 $D_{K^{\mathrm{Sh}}}$ と導手 $\mathfrak{f}_{K^{\mathrm{Sh}}}$ は次で与えられる (Δ_n が平方因子をもたないときは Cusick [4, Lemma 1], $n \not\equiv 3 \pmod 9$ のときは Washington [27, p372, Proposition 1], 一般の場合は Kashio-Sekigawa [16] 参照).

$$D_{K^{\mathrm{Sh}}} = \mathfrak{f}_{K^{\mathrm{Sh}}}^2, \quad \mathfrak{f}_{K^{\mathrm{Sh}}} = \gamma \prod_{\substack{p \mid b \\ p \neq 3}} p, \quad \gamma := \begin{cases} 1 & (\text{if } 3 \nmid n \text{ or } n \equiv 12 \pmod{27}), \\ 3^2 & (\text{otherwise}). \end{cases}$$

$\Delta_n = n^2+3n+9$ が素数 p のとき, K^{Sh} の導手は p であり, $f_n^{\mathrm{Sh}}(X)$ の任意の根 ρ に対し, $-\left(\frac{n}{3}\right)\left(\rho + \left(\left(\frac{n}{3}\right) - n\right)/3\right)$ は K^{Sh} のガウス周期であることが Lehmer [19] によって指摘されている (ここで, $\left(\frac{*}{*}\right)$ は平方剰余記号を表す). よってこのとき $\rho + \left(\left(\frac{n}{3}\right) - n\right)/3$ は NIB の生成元である. さらに, Δ_n が square-free のときも, $\rho + \left(\left(\frac{n}{3}\right) - n\right)/3$ が NIB の生成元であることが Lazarus [18], Châtelet [3] により示されている. 一般の馴分岐拡大 $K^{\mathrm{Sh}}/\mathbb{Q}$ に対する NIB の生成元は次に述べる定理で与えられる.

$K^{\mathrm{Sh}}/\mathbb{Q}$ のガロア群を $\mathrm{Gal}(K^{\mathrm{Sh}}/\mathbb{Q}) = \langle\sigma\rangle$, $\sigma(\rho) = -1/(1+\rho)$ とおき,

$$\Delta_n = n^2+3n+9 = A_n B_n = de^2c^3,$$

$A_n := n - 3\zeta^2$, $B_n := n - 3\zeta$ (ζ は 1 の原始 3 乗根), $d, e, c \in \mathbb{Z}$, d, e は square-free, $(d, e) = 1$ とおく.

定理 2.1 (Hashimoto-A [13])**.** $K^{\mathrm{Sh}}/\mathbb{Q}$ は馴分岐拡大とする ($\Leftrightarrow$ $3 \nmid n$ or $n \equiv 12 \pmod{27}$). a_0, a_1 を $ec = a_0^2 - a_0a_1 + a_1^2$, $a_0 + a_1\zeta \mid A_n$ in $\mathbb{Z}[\zeta]$ をみたす整数とする. さらに

$$\varepsilon\ (= \pm 1) := \begin{cases} \left(\frac{n(a_0+a_1)}{3}\right) & (3 \nmid n \text{ のとき}), \\ \left(\frac{a_0}{3}\right) & (n \equiv 12 \pmod{27} \text{ のとき}) \end{cases}$$

とおく. このとき,

$$\frac{1}{ec^2}\left((a_0 + a_1\sigma).\rho + \frac{\varepsilon ec^2 - n(a_0+a_1)}{3}\right)$$

は K^{Sh} の NIB の生成元である.

注意 2.2. Δ_n が square-free のとき, $3 \nmid n$, $e = c = 1$ より, $a_0 = 1, a_1 = 0$ と取れることから, 定理 2.1 より $\rho + \left(\left(\frac{n}{3}\right) - n\right)/3$ は K^{Sh} の NIB の生成元であることが分かる. これは前に述べた Lehmer, Lazarus, Châtelet の結果に一致する.

注意 2.3. 定理 2.1 の条件をみたす $a_0, a_1 \in \mathbb{Z}$ は以下のように見つけることができる. まず,

$$ec = 3^j p_1 \cdots p_k \ (p_1, \ldots, p_k \text{ は相異なるとは限らない素数}),$$
$$p_1 \equiv \cdots \equiv p_k \equiv 1 \pmod 3,$$
$$j = \begin{cases} 0 & (3 \nmid n \text{ のとき}), \\ 1 & (n \equiv 12 \pmod{27} \text{ のとき}) \end{cases}$$

とおける. 次に任意の $i \in \{1, \dots, k\}$ に対し, $\mathbb{Z}[\zeta]$ の素元 π_i, π_i' を次のように定める.

$$p_i = \pi_i \pi_i', \quad \pi_i | A_n, \quad \pi_i' | B_n.$$

このとき, 条件をみたす $a_0, a_1 \in \mathbb{Z}$ は $(1-\zeta)^j \pi_1 \cdots \pi_k = a_0 + a_1 \zeta$ で与えられる (A_n, B_n を共に含む $\mathbb{Z}[\zeta]$ の素イデアルは $(1-\zeta)$ のみであることに注意).

例題 2.4. (1) $3 \nmid n$ かつ Δ_n が square-free でない最小の正の整数 n は, $n = 235$ である. このとき, $\Delta_n = 331 \cdot 13^2$, $d = 331$, $e = 13$, $c = 1$ である. $ec = 13 = 3^2 - 3 \times (-1) + (-1)^2$ より $a_0 = 3$, $a_1 = -1$ ととれる. また $\varepsilon = -1$ であり, 定理 2.1 から,

$$\xi = \frac{1}{13}(3\rho - \rho' - 161) = -\frac{1}{13}(\rho^2 - 239\rho + 159)$$

は NIB の生成元である.[5]
(2) $n \equiv 12 \pmod{27}$ (このとき Δ_n は常に square-free ではない) をみたす最小の正の整数 n は, $n = 12$ である. このとき, $\Delta_n = 7 \cdot 3^3$, $d = 7$, $e = 1$, $c = 3$ である. $ec = 3 = 1^2 - 1 \times (-1) + (-1)^2$ より $a_0 = 1$, $a_1 = -1$ ととれる. また $\varepsilon = 1$ であり, 定理 2.1 から,

$$\xi = \frac{1}{9}(\rho - {\rho'}^2 + 3) = -\frac{1}{9}(\rho^2 - 14\rho - 5)$$

は NIB の生成元である.

補題 1.2 と例題 1.4 (2) より, K^{Sh} のすべての NIB の生成元は $\mathbb{Z}[G]^\times = \{\pm 1_G, \pm\sigma, \pm\sigma^2\}$ の元と 1 対 1 対応がある. よって, 次の系が得られる.

系 2.5. $\xi := \frac{1}{ec^2}\left((a_0 + a_1\sigma).\rho + (\varepsilon ec^2 - n(a_0 + a_1))/3\right)$ を定理 2.1 で得られる NIB の生成元とすると, K^{Sh} の NIB は, $\{\xi, \sigma(\xi), \sigma^2(\xi)\}$ と, $\{-\xi, -\sigma(\xi), -\sigma^2(\xi)\}$ の 2 組である (NIB の生成元は 6 個).

系 2.5 より, K^{Sh} に含まれる 3 つのガウス周期は, $\{\xi, \sigma(\xi), \sigma^2(\xi)\}$ または $\{-\xi, -\sigma(\xi), -\sigma^2(\xi)\}$ のいずれかである. K^{Sh} の導手を $\mathfrak{f}$ とし, $\eta := \mathrm{Tr}_{\mathbb{Q}(\zeta_\mathfrak{f})/K}(\zeta_\mathfrak{f})$ (ガウス周期) とおくと,

$$\mathrm{Tr}_{K^{\mathrm{Sh}}/\mathbb{Q}}(\eta) = \mathrm{Tr}_{K^{\mathrm{Sh}}/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta_\mathfrak{f})/K^{\mathrm{Sh}}}(\zeta_\mathfrak{f})) = \mathrm{Tr}_{\mathbb{Q}(\zeta_\mathfrak{f})/\mathbb{Q}}(\zeta_\mathfrak{f}) = \mu(\mathfrak{f})$$

である. 一方,

$$\mathrm{Tr}_{K^{\mathrm{Sh}}/\mathbb{Q}}(\mu(\mathfrak{f})\varepsilon\xi) = \frac{\mu(\mathfrak{f})\varepsilon}{ec^2}((a_0 + a_1)n + \varepsilon ec^2 - n(a_0 + a_1)) = \mu(\mathfrak{f})$$

であるから, K^{Sh} のガウス周期は $\mu(\mathfrak{f})\varepsilon\xi$ とその共役元であることが分かる.

系 2.6. K^{Sh} のガウス周期は, $\mu(\mathfrak{f})\varepsilon\xi$ とその共役元である.

例題 2.7. (1) $n = 235$ のとき, K^{Sh} の導手は $\mathfrak{f} = 13 \cdot 331$ である. 例題 2.4 (1) および 系 2.6 からガウス周期は, $-\xi = (\rho^2 - 239\rho + 159)/13$ とその共役元である.
(2) $n = 12$ のとき, K^{Sh} の導手は $\mathfrak{f} = 7$ である. 例題 2.4 (2) および系 2.6 からガウス周期は, $-\xi = (\rho^2 - 14\rho - 5)/9$ とその共役元である.

[5] $\rho' = -1/(1+\rho) = \rho^2 - (n+1)\rho - 2$, $\rho'' = -1/(1+\rho') = -\rho^2 + n\rho + (n+2)$ が成り立つ.

表 1: $K^{\mathrm{Sh}},\ 1 \le n \le 500,\ 3 \nmid n$ and Δ_n is not square-free

n	Δ_n	$\mathfrak{f}$	Gaussian period	minimal polynomial
235	$13^2 \cdot 331$	$13 \cdot 331$	$\frac{1}{13}(\rho^2 - 239\rho + 159)$	$X^3 - X^2 - 1434X + 15937$
250	$7^2 \cdot 1291$	$7 \cdot 1291$	$-\frac{1}{7}(\rho^2 - 253\rho + 79)$	$X^3 - X^2 - 3012X - 32801$
269	$13^2 \cdot 433$	$13 \cdot 433$	$\frac{1}{13}(\rho^2 - 266\rho - 446)$	$X^3 - X^2 - 1876X - 22933$
271	$7 \cdot 103^2$	$7 \cdot 103$	$\frac{1}{103}(9\rho^2 - 2450\rho - 616)$	$X^3 - X^2 - 240X - 1175$
286	$7^3 \cdot 241$	241	$-\frac{1}{49}(\rho^2 - 284\rho - 367)$	$X^3 + X^2 - 80X + 125$
299	$7^2 \cdot 19 \cdot 97$	$7 \cdot 19 \cdot 97$	$-\frac{1}{7}(\rho^2 - 302\rho + 100)$	$X^3 + X^2 - 4300X - 59249$
335	$7^2 \cdot 2311$	$7 \cdot 2311$	$-\frac{1}{7}(\rho^2 - 333\rho - 451)$	$X^3 - X^2 - 5392X + 85079$
356	$7 \cdot 19 \cdot 31^2$	$7 \cdot 19 \cdot 31$	$-\frac{1}{31}(6\rho^2 - 2137\rho - 1307)$	$X^3 + X^2 - 1374X - 18019$
374	$37^2 \cdot 103$	$37 \cdot 103$	$-\frac{1}{37}(3\rho^2 - 1118\rho - 1265)$	$X^3 - X^2 - 1270X + 4799$
397	$7^3 \cdot 463$	463	$\frac{1}{49}(\rho^2 - 400\rho + 114)$	$X^3 + X^2 - 154X + 343$
404	$7 \cdot 13^2 \cdot 139$	$7 \cdot 13 \cdot 139$	$\frac{1}{13}(\rho^2 - 408\rho + 263)$	$X^3 + X^2 - 4216X + 76831$
433	$7^2 \cdot 3853$	$7 \cdot 3853$	$\frac{1}{7}(\rho^2 - 431\rho - 577)$	$X^3 - X^2 - 8990X - 175811$
446	$7^2 \cdot 61 \cdot 67$	$7 \cdot 61 \cdot 67$	$-\frac{1}{7}(\rho^2 - 449\rho + 149)$	$X^3 + X^2 - 9536X - 194965$
482	$7^2 \cdot 13 \cdot 367$	$7 \cdot 13 \cdot 367$	$\frac{1}{7}(\rho^2 - 480\rho - 647)$	$X^3 + X^2 - 11132X - 249859$

3 E. Lehmer の 5 次巡回拡大体

整数 n に対し定義される次の多項式を Lehmer の多項式 ([19]) という.

$$f_n^{\mathrm{Leh}}(X) = X^5 + n^2X^4 - (2n^3 + 6n^2 + 10n + 10)X^3 + (n^4 + 5n^3 + 11n^2 + 15n + 5)X^2 + (n^3 + 4n^2 + 10n + 10)X + 1.$$

以下整数 n を固定し, ρ を $f_n^{\mathrm{Leh}}(X)$ の任意の根とし, $K^{\mathrm{Leh}} = \mathbb{Q}(\rho)$ とおく. Lehmer の 5 次巡回拡大体について, 以下のことが知られている.

(1) $f_n^{\mathrm{Leh}}(X)$ は $\mathbb{Q}$ 上既約.

(2) $K^{\mathrm{Leh}}/\mathbb{Q}$ は 5 次巡回拡大であり, ガロア群の生成元は $\mathrm{Gal}(K^{\mathrm{Leh}}/\mathbb{Q}) = \langle\sigma\rangle$, $\sigma(\rho) = (n + 2 + n\rho - \rho^2)/(1 + (n + 2)\rho)$ で与えられる.

(3) $\Delta_n := n^4 + 5n^3 + 15n^2 + 25n + 25$, $\delta_n := n^3 + 5n^2 + 10n + 7$ とおくと, $f_n^{\mathrm{Leh}}(X)$ の判別式は, $d(f_n^{\mathrm{Leh}}) = \delta_n^2\Delta_n^4$ である.

(4) K^{Leh} の判別式 $D_{K^{\mathrm{Leh}}}$ と導手 $\mathfrak{f}_{K^{\mathrm{Leh}}}$ は以下で与えられる ([15], [24, (1.3)] 参照).

$$D_{K^{\mathrm{Leh}}} = \mathfrak{f}_{K^{\mathrm{Leh}}}^4, \quad \mathfrak{f}_{K^{\mathrm{Leh}}} = 5^{\alpha} \prod_{\substack{p \mid \Delta_n,\, p \neq 5 \\ v_p(\Delta_n) \not\equiv 0 \pmod 5}} , \quad \alpha := \begin{cases} 0 & \text{if } 5 \nmid n, \\ 2 & \text{if } 5 \mid n \end{cases}$$

表 2: K^{Sh}, $1 \leq n \leq 500$ and $n \equiv 12 \pmod{27}$ (in this case, always Δ_n is not square-free)

n	Δ_n	$\mathfrak{f}$	Gaussian period	minimal polynomial
12	$3^3 \cdot 7$	7	$\frac{1}{9}(\rho^2 - 14\rho - 5)$	$X^3 + X^2 - 2X - 1$
39	$3^3 \cdot 61$	61	$\frac{1}{9}(\rho^2 - 41\rho - 5)$	$X^3 + X^2 - 20X - 9$
66	$3^3 \cdot 13^2$	13	$\frac{1}{117}(7\rho^2 - 464\rho - 317)$	$X^3 + X^2 - 4X + 1$
93	$3^3 \cdot 331$	331	$\frac{1}{9}(\rho^2 - 95\rho - 5)$	$X^3 + X^2 - 110X - 49$
120	$3^3 \cdot 547$	547	$\frac{1}{9}(\rho^2 - 122\rho - 5)$	$X^3 + X^2 - 182X - 81$
147	$3^3 \cdot 19 \cdot 43$	$19 \cdot 43$	$-\frac{1}{9}(\rho^2 - 149\rho - 5)$	$X^3 - X^2 - 272X + 121$
174	$3^3 \cdot 7 \cdot 163$	$7 \cdot 163$	$-\frac{1}{9}(\rho^2 - 176\rho - 5)$	$X^3 - X^2 - 380X + 169$
201	$3^3 \cdot 7^2 \cdot 31$	$7 \cdot 31$	$\frac{1}{63}(5\rho^2 - 1006\rho - 592)$	$X^3 - X^2 - 72X + 225$
228	$3^3 \cdot 1951$	1951	$\frac{1}{9}(3\rho^2 - 230\rho - 5)$	$X^3 + X^2 - 650X - 289$
255	$3^3 \cdot 2437$	2437	$\frac{1}{9}(\rho^2 - 257\rho - 5)$	$X^3 + X^2 - 812X - 361$
282	$3^3 \cdot 13 \cdot 229$	$13 \cdot 229$	$-\frac{1}{9}(\rho^2 - 284\rho - 5)$	$X^3 - X^2 - 992X + 441$
309	$3^3 \cdot 3571$	3571	$\frac{1}{9}(\rho^2 - 311\rho - 5)$	$X^3 + X^2 - 1190X - 529$
336	$3^3 \cdot 4219$	4219	$\frac{1}{9}(\rho^2 - 338\rho - 5)$	$X^3 + X^2 - 1406X - 625$
363	$3^3 \cdot 7 \cdot 19 \cdot 37$	$7 \cdot 19 \cdot 37$	$\frac{1}{9}(\rho^2 - 365\rho - 5)$	$X^3 + X^2 - 1640X - 729$
390	$3^3 \cdot 7 \cdot 811$	$7 \cdot 811$	$-\frac{1}{9}(\rho^2 - 392\rho - 5)$	$X^3 - X^2 - 1892X + 841$
417	$3^3 \cdot 13 \cdot 499$	$13 \cdot 499$	$-\frac{1}{9}(\rho^2 - 419\rho - 5)$	$X^3 - X^2 - 2162X + 961$
444	$3^3 \cdot 7351$	7351	$\frac{1}{9}(\rho^2 - 446\rho - 5)$	$X^3 + X^2 - 2450X - 1089$
471	$3^3 \cdot 8269$	8269	$\frac{1}{9}(\rho^2 - 473\rho - 5)$	$X^3 + X^2 - 2756X - 1225$
498	$3^3 \cdot 9241$	9241	$\frac{1}{9}(\rho^2 - 500\rho - 5)$	$X^3 + X^2 - 3080X - 1369$

$\Delta_n = n^4 + 5n^3 + 15n^2 + 25n + 25$ が素数 p のとき, K^{Leh} の導手は p であり, $f_n^{\mathrm{Leh}}(X)$ の任意の根 ρ に対し, $\left(\frac{n}{5}\right)\left(\rho + (n^2 - \left(\frac{n}{5}\right))/5\right)$ は K^{Leh} のガウス周期であることが Lehmer [19] によって指摘されている. よってこのとき $\rho + (n^2 - \left(\frac{n}{5}\right))/5$ は NIB の生成元である. さらに, Δ_n が square-free のときも, $\rho + (n^2 - \left(\frac{n}{5}\right))/5$ が NIB の生成元であることが Spearman-Williams [24] により示されている. 一般の馴分岐拡大 $K^{\mathrm{Leh}}/\mathbb{Q}$ に対する NIB の生成元は次に述べる定理で与えられる.

$K^{\mathrm{Leh}}/\mathbb{Q}$ のガロア群を $\mathrm{Gal}(K^{\mathrm{Leh}}/\mathbb{Q}) = \langle\sigma\rangle$, $\sigma(\rho) = (n + 2 + n\rho - \rho^2)/(1 + (n+2)\rho)$ とおき, $\rho^{(\ell)} := \sigma^\ell(\rho)$ $(\ell \in \mathbb{Z}/5\mathbb{Z})$ とおく. さらに,

$$\Delta_n = n^4 + 5n^3 + 15n^2 + 25n + 25 = A_n B_n C_n D_n = ab^2c^3d^4e^5,$$

$A_n = n + 2 + 2\zeta^4 + \zeta^2$, $B_n := n + 2 + 2\zeta^2 + \zeta$, $C_n := n + 2 + 2\zeta^3 + \zeta^4$, $D_n := n + 2 + 2\zeta + \zeta^3$ (ζ は 1 の原始 5 乗根), $a, b, c, d, e \in \mathbb{Z}$, a, b, c, d は square-free, a, b, c, d はどの 2 つも互いに素とおく.

定理 3.1 (Hashimoto-A [14]). $K^{\mathrm{Leh}}/\mathbb{Q}$ は馴分岐拡大とする ($\Leftrightarrow\ 5\nmid n$). $\alpha_0,\alpha_1,\alpha_3\in\mathbb{Z}[\zeta]$ を

$$\begin{aligned}
N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha_1)&=bc^2d^3e^3,\quad \alpha_1\,|\,A_n\ \text{ in }\mathbb{Z}[\zeta],\\
N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha_2)&=bcd^2e^2,\quad \alpha_2\,|\,B_n\ \text{ in }\mathbb{Z}[\zeta],\\
N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha_3)&=cde,\quad \alpha_3\,|\,C_n\ \text{ in }\mathbb{Z}[\zeta],\\
\alpha_1&\equiv\alpha_2\equiv\alpha_3\equiv 1\ (\mathrm{mod}\ (1-\zeta))
\end{aligned}$$

をみたす元とし, $\beta_0,\beta_1,\beta_2,\beta_3$ を $\alpha_1\alpha_2\alpha_3=\sum_{i=0}^{3}\beta_i\zeta^i$ をみたす整数とする. このとき,

$$\frac{1}{bc^2d^3e^4}\left((\sum_{i=0}^{3}\beta_i\sigma^i).\,\rho-\frac{\left(\frac{n}{5}\right)bc^2d^3e^4-n^2\sum_{i=0}^{3}\beta_i}{5}\right)$$

は K^{Leh} の NIB の生成元である.

注意 3.2. Δ_n が square-free のとき, $5\nmid n$, $b=c=d=e=1$ より, $\alpha_1=\alpha_2=\alpha_3=1$, $\beta_0=1$, $\beta_1=\beta_2=\beta_3=0$ と取れることから, 定理 3.1 より $\rho+\left(n^2-\left(\frac{n}{5}\right)\right)/5$ は K^{Leh} の NIB の生成元であることが分かる. これは前に述べた Spearman-Williams の結果に一致する.

注意 3.3. 定理 3.1 の条件をみたす $\alpha_1\in\mathbb{Z}[\zeta]$ は以下のように見つけることができる ($\alpha_2,\alpha_3\in\mathbb{Z}[\zeta]$ も同様). まず, $bc^2d^3e^3=p_1\cdots p_k$ ($p_1,\ldots,p_k$ は相異なるとは限らない素数), $p_1\equiv\cdots\equiv p_k\equiv 1\ (\mathrm{mod}\ 5)$ とおける. 次に任意の $i\in\{1,\ldots,k\}$ に対し, p_i を割る $\mathbb{Z}[\zeta]$ の素元で, A_n を割るものを π_i とおく. $\lambda:=\prod_{i=1}^{k}\pi_i$ とおき,

$$u:=\begin{cases}1 & (\lambda\equiv 1\ (\mathrm{mod}\ (1-\zeta))\ \text{のとき}),\\ -1 & (\lambda\equiv -1\ (\mathrm{mod}\ (1-\zeta))\ \text{のとき}),\\ \frac{1+\sqrt{5}}{2} & (\lambda\equiv 2\ (\mathrm{mod}\ (1-\zeta))\ \text{のとき}),\\ -\frac{1+\sqrt{5}}{2} & (\lambda\equiv -2\ (\mathrm{mod}\ (1-\zeta))\ \text{のとき})\end{cases}\qquad(\in\mathbb{Z}[\zeta]^{\times})$$

に対し, $\alpha_1:=u\lambda$ とすると, $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\alpha_1)=bc^2d^3e^3$, $\alpha_1\,|\,A_n$, $\alpha_1\equiv 1\ (\mathrm{mod}\ (1-\zeta))$ をみたす (A_n,B_n,C_nD_n のうち少なくとも 2 つを含む $\mathbb{Z}[\zeta]$ の素イデアルは $(1-\zeta)$ のみであり, $5\nmid n$ のときは $5\nmid\Delta_n$ が成り立つことから A_n,B_n,C_n,D_n はどの 2 つも互いに素である).

例題 3.4. $5\nmid n$ かつ Δ_n が square-free でない最小の正の整数 n は, $n=14$ である. このとき, $\Delta_n=11\cdot 71^2$, $a=11$, $b=71$, $c=d=e=1$ である. $bc^2d^3e^3=bcd^2e^2=71$ であり, 71 の $\mathbb{Z}[\zeta]$ における素元分解は, 次のようになる.

$$71=(2+\zeta+3\zeta^2)(2+3\zeta+\zeta^3)(1-2\zeta-\zeta^2+\zeta^3)(-3\zeta-\zeta^2-2\zeta^3)$$

$2+\zeta+3\zeta^2|A_n$, $2+3\zeta+\zeta^3|B_n$ であり, $2+\zeta+3\zeta^2\equiv 1\ (\mathrm{mod}\ (1-\zeta))$, $2+3\zeta+\zeta^3\equiv 1\ (\mathrm{mod}\ (1-\zeta))$ から, $\alpha_1=2+\zeta+3\zeta^2$, $\alpha_2=2+3\zeta+\zeta^3$ である. また $cde=1$ から $\alpha_3=1$ ととれる. $\alpha_1\alpha_2\alpha_2=6+7\zeta+8\zeta^2+10\zeta^3$ から $\beta_0=6$, $\beta_1=7$, $\beta_2=8$, $\beta_3=10$ ととれることが分かる. 定理 3.1 から,

$$\xi=\frac{1}{71}(6\rho+7\rho^{(1)}+8\rho^{(2)}+10\rho^{(3)}+1201)$$

は NIB の生成元である.

表 3 から, $1\le n\le 1000$, $5\nmid n$ かつ Δ_n が square-free でない n は 34 個あり, このうち $c\neq 1$ をみたすものは 4 個あることが分かる. $d\neq 1$ または $e\neq 1$ の例, および b,c,d,e のうち少なくとも 2 つが 1 ではない例は以下の通りである.

表 3: K^{Leh}, $1 \leq n \leq 1000$, $5 \nmid n$ and Δ_n is not square-free

n	Δ_n	$\mathfrak{f}$	a generator of NIB
14	$11 \cdot 71^2$	$11 \cdot 71$	$\frac{1}{71}(6\rho + 7\rho^{(1)} + 8\rho^{(2)} + 10\rho^{(3)} + 1201)$
44	$61 \cdot 41^3$	$41 \cdot 61$	$\frac{1}{41^2}(28\rho + 39\rho^{(1)} + 36\rho^{(2)} + 48\rho^{(3)} + 58131)$
69	$201511 \cdot 11^2$	$11 \cdot 201511$	$\frac{1}{11}(\rho - 3\rho^{(1)} - \rho^{(2)} - \rho^{(3)} - 3811)$
71	$7331 \cdot 61^2$	$61 \cdot 7331$	$\frac{1}{61}(-3\rho - 2\rho^{(2)} + 6\rho^{(3)} + 996)$
83	$11 \cdot 2141^2$	$11 \cdot 2141$	$\frac{1}{2141}(16\rho + 2\rho^{(1)} - 37\rho^{(2)} + 10\rho^{(3)} - 11972)$
86	$31 \cdot 15461 \cdot 11^2$	$11 \cdot 31 \cdot 15461$	$\frac{1}{11}(4\rho + 3\rho^{(1)} + 2\rho^{(2)} + 2\rho^{(3)} + 16269)$
98	$191 \cdot 4201 \cdot 11^2$	$11 \cdot 191 \cdot 4201$	$\frac{1}{11}(2\rho - 2\rho^{(2)} + \rho^{(3)} + 1923)$
207	$15545731 \cdot 11^2$	$11 \cdot 15545731$	$\frac{1}{11}(4\rho + 3\rho^{(1)} + 2\rho^{(2)} + 2\rho^{(3)} + 94270)$
219	$19450411 \cdot 11^2$	$11 \cdot 19450411$	$\frac{1}{11}(2\rho - 2\rho^{(2)} + \rho^{(3)} + 9590)$
226	$101 \cdot 19841 \cdot 11^3$	$11 \cdot 101 \cdot 19841$	$\frac{1}{11^2}(-2\rho - 9\rho^{(1)} - 6\rho^{(2)} - 12\rho^{(3)} - 296265)$
276	$61 \cdot 100801 \cdot 31^2$	$31 \cdot 61 \cdot 100801$	$\frac{1}{31}(\rho - 2\rho^{(1)} - 2\rho^{(2)} + 4\rho^{(3)} + 15229)$
311	$131 \cdot 461 \cdot 1301 \cdot 11^2$	$11 \cdot 131 \cdot 461 \cdot 1301$	$\frac{1}{11}(\rho - 3\rho^{(1)} - \rho^{(2)} - \rho^{(3)} - 77379)$
328	$97127081 \cdot 11^2$	$11 \cdot 97127081$	$\frac{1}{11}(4\rho + 3\rho^{(1)} + 2\rho^{(2)} + 2\rho^{(3)} + 236687)$
347	$121562411 \cdot 11^2$	$11 \cdot 121562411$	$\frac{1}{11}(2\rho + \rho^{(2)} - 2\rho^{(3)} + 24084)$
432	$291193681 \cdot 11^2$	$11 \cdot 291193681$	$\frac{1}{11}(\rho - 3\rho^{(1)} - \rho^{(2)} - \rho^{(3)} - 149297)$
449	$30877981 \cdot 11^3$	$11 \cdot 30877981$	$\frac{1}{11^2}(10\rho + 6\rho^{(1)} + 12\rho^{(2)} + 3\rho^{(3)} + 1249902)$
461	$377340791 \cdot 11^2$	$11 \cdot 377340791$	$\frac{1}{11}(2\rho - 2\rho^{(2)} + \rho^{(3)} + 42502)$
468	$400721701 \cdot 11^2$	$11 \cdot 400721701$	$\frac{1}{11}(2\rho + \rho^{(2)} - 2\rho^{(3)} + 43807)$
484	$131 \cdot 440431 \cdot 31^2$	$31 \cdot 131 \cdot 440431$	$\frac{1}{31}(-\rho + 3\rho^{(1)} - 3\rho^{(2)} - 3\rho^{(3)} - 187411)$
544	$41 \cdot 2243281 \cdot 31^2$	$31 \cdot 41 \cdot 2243281$	$\frac{1}{31}(6\rho + 3\rho^{(1)} + 2\rho^{(3)} + 651053)$
553	$779911631 \cdot 11^2$	$11 \cdot 779911631$	$\frac{1}{11}(\rho - 3\rho^{(1)} - \rho^{(2)} - \rho^{(3)} - 244645)$
582	$31 \cdot 71 \cdot 571 \cdot 761 \cdot 11^2$	$11 \cdot 31 \cdot 71 \cdot 571 \cdot 761$	$\frac{1}{11}(2\rho - 2\rho^{(2)} + \rho^{(3)} + 67747)$
589	$7151 \cdot 140281 \cdot 11^2$	$11 \cdot 7151 \cdot 140281$	$\frac{1}{11}(2\rho + \rho^{(2)} - 2\rho^{(3)} + 69382)$
613	$1091 \cdot 135781 \cdot 31^2$	$31 \cdot 1091 \cdot 135781$	$\frac{1}{31}(-6\rho - 4\rho^{(1)} - 6\rho^{(2)} - 3\rho^{(3)} - 1427916)$
674	$20411 \cdot 84181 \cdot 11^2$	$11 \cdot 20411 \cdot 84181$	$\frac{1}{11}(\rho - 3\rho^{(1)} - \rho^{(2)} - \rho^{(3)} - 363423)$
691	$1897892411 \cdot 11^2$	$11 \cdot 1897892411$	$\frac{1}{11}(4\rho + 3\rho^{(1)} + 2\rho^{(2)} + 2\rho^{(3)} + 1050456)$
703	$61 \cdot 101 \cdot 311 \cdot 1061 \cdot 11^2$	$11 \cdot 61 \cdot 101 \cdot 311 \cdot 1061$	$\frac{1}{11}(2\rho - 2\rho^{(2)} + \rho^{(3)} + 98844)$
726	$166407091 \cdot 41^2$	$41 \cdot 166407091$	$\frac{1}{41}(-2\rho - 6\rho^{(1)} - 4\rho^{(2)} - 7\rho^{(3)} - 2002897)$
812	$48491 \cdot 74551 \cdot 11^2$	$11 \cdot 48491 \cdot 74551$	$\frac{1}{11}(4\rho + 3\rho^{(1)} + 2\rho^{(2)} + 2\rho^{(3)} + 1450559)$
824	$61 \cdot 3271 \cdot 19211 \cdot 11^2$	$11 \cdot 61 \cdot 3271 \cdot 19211$	$\frac{1}{11}(2\rho - 2\rho^{(2)} + \rho^{(3)} + 135793)$
831	$41 \cdot 571 \cdot 169361 \cdot 11^2$	$11 \cdot 41 \cdot 571 \cdot 169361$	$\frac{1}{11}(2\rho + \rho^{(2)} - 2\rho^{(3)} + 138110)$
916	$31 \cdot 17155921 \cdot 11^3$	$11 \cdot 31 \cdot 17155921$	$\frac{1}{11^2}(4\rho - 6\rho^{(1)} - 3\rho^{(2)} + 6\rho^{(3)} + 167787)$
933	$101 \cdot 62337371 \cdot 11^2$	$11 \cdot 101 \cdot 62337371$	$\frac{1}{11}(4\rho + 3\rho^{(1)} + 2\rho^{(2)} + 2\rho^{(3)} + 1915078)$
952	$101 \cdot 811 \cdot 83311 \cdot 11^2$	$11 \cdot 101 \cdot 811 \cdot 83311$	$\frac{1}{11}(2\rho + \rho^{(2)} - 2\rho^{(3)} + 181263)$

例題 3.5. $d \neq 1$ をみたす最小の正の整数 n は, $n = 2888$ である. このとき, $\Delta_n = 11^4 \cdot$

4759595441 であり, K^{Leh} の導手は $\mathfrak{f} = 11 \cdot 4759595441$ である. 定理 3.1 から $(-16\rho - 6\rho^{(1)} - 26\rho^{(2)} - 41\rho^{(3)} - 148461417)/11^3$ は NIB の生成元である.

例題 3.6. $e \neq 1$ をみたす最小の正の整数 n は, $n = 7721$ である. このとき, $\Delta_n = 11^5 \cdot 26501 \cdot 833201$ であり, K^{Leh} の導手は $\mathfrak{f} = 26501 \cdot 833201$ である. 定理 3.1 から $(-10\rho + 6\rho^{(1)} - 35\rho^{(2)} - 20\rho^{(3)} - 703446252)/11^4$ は NIB の生成元である.

例題 3.7. b, c, d, e のうち少なくとも 2 つが 1 ではない最小の正の整数 n は, $n = 40846$ である. このとき, $\Delta_n = 11^4 \cdot 31^2 \cdot 197859618251$ であり, K^{Leh} の導手は $\mathfrak{f} = 11 \cdot 31 \cdot 197859618251$ である. 定理 3.1 から $(-211\rho - 96\rho^{(1)} - 158\rho^{(2)} - 14\rho^{(3)} - 159832317845)/(11^3 \cdot 31)$ は NIB の生成元である.

補題 1.2 と例題 1.4 (3) より, K^{Leh} のすべての NIB の生成元は $\mathbb{Z}[G]^\times = \{\pm\sigma^\ell(1 - \sigma^2 - \sigma^3)^k \,|\, \ell \in \mathbb{Z}/5\mathbb{Z},\, k \in \mathbb{Z}\}$ の元と 1 対 1 対応がある. よって, 次の系が得られる.

系 3.8. $\xi := \frac{1}{bc^2d^3e^4}\left((\sum_{i=0}^3 \beta_i\sigma^i).\,\rho - \left(\left(\frac{n}{5}\right) bc^2d^3e^4 - n^2\sum_{i=0}^3 \beta_i\right)/5\right)$ を定理 3.1 で得られる NIB の生成元とすると, K^{Leh} のすべての NIB の生成元は, $\{\pm\sigma^\ell(1 - \sigma^2 - \sigma^3)^k.\,\xi \,|\, \ell \in \mathbb{Z}/5\mathbb{Z},\, k \in \mathbb{Z}\}$ である. よって, NIB はある $k \in \mathbb{Z}$ に対して, $\{\sigma^\ell(1 - \sigma^2 - \sigma^3)^k.\,\xi \,|\, \ell \in \mathbb{Z}/5\mathbb{Z}\}$ または $\{-\sigma^\ell(1 - \sigma^2 - \sigma^3)^k.\,\xi \,|\, \ell \in \mathbb{Z}/5\mathbb{Z}\}$ で与えられる.

次にすべての NIB の生成元を $\mathbb{Q}(\sqrt{5})$ の基本単数または Lucas 数を用いて与える. 整数 k に対し, Fibonacci 数と Lucas 数を $F_0 = 0,\ F_1 = 1,\ F_k = F_{k-1} + F_{k-2},\ L_0 = 2,\ L_1 = 1,\ L_k = L_{k-1} + L_{k-2}$ で定める. また, $\lambda := \left((1 + \sqrt{5})/2\right)^2 = (3 + \sqrt{5})/2$ を $\mathbb{Q}(\sqrt{5})$ の基本単数の 2 乗, $\overline{\lambda} := (3 - \sqrt{5})/2$ を λ の共役元とする. 整数 k に対し, 数列 $a_k,\, b_k,\, c_k \in \mathbb{Z}$ を次のように定める.

$$\begin{aligned} a_k &:= \frac{1}{5}((-1)^k + 2(\lambda^k + \overline{\lambda}^k)) = \frac{1}{5}((-1)^k + 2L_{2k}), \\ b_k &:= \frac{1}{2}(a_k - a_{k-1}) = \frac{1}{5}((-1)^k + L_{2k-1}), \\ c_k &:= \frac{1}{2}(a_{k+1} - a_k) = \frac{1}{5}((-1)^{k+1} + L_{2k+1}). \end{aligned}$$

$f_n^{\mathrm{Leh}}(X)$ の根 ρ への $(1-\sigma^2-\sigma^3)^k$ $(k \in \mathbb{Z})$ の作用は, 数列 a_k, b_k, c_k を用いて, $(1-\sigma^2-\sigma^3)^k.\,\rho = (a_k + b_k(\sigma + \sigma^4) - c_k(\sigma^2 + \sigma^3)).\rho$ で与えられることから, 次の定理を得ることができる.

定理 3.9 (Hashimoto-A [14])**.** $K^{\mathrm{Leh}}/\mathbb{Q}$ は馴分岐拡大とする ($\Leftrightarrow\ 5 \nmid n$). $\beta_0,\, \beta_1,\, \beta_2,\, \beta_3 \in \mathbb{Z}$ を定理 3.1 の元とする. このとき, K^{Leh} のすべての NIB の生成元は次で与えられる.

$$\{x \,|\, K^{\mathrm{Leh}} \text{ の NIB の生成元 }\} = \{\pm\sigma^\ell.\,\xi_k \,|\, \ell \in \mathbb{Z}/5\mathbb{Z},\, k \in \mathbb{Z}\},$$

$$\xi_k := \frac{1}{bc^2d^3e^4}\left(\sum_{t=0}^4 \theta_t(k)\sigma^t.\,\rho - (-1)^k\frac{\left(\frac{n}{5}\right) bc^2d^3e^4 - n^2\sum_{i=0}^3 \beta_i}{5}\right).$$

ここで, $\theta_0(k), \ldots, \theta_4(k) \in \mathbb{Z}$ は次のように定める.

$$\begin{aligned} \theta_0(k) &:= a_k\beta_0 + b_k\beta_1 - c_k\beta_2 - c_k\beta_3, \\ \theta_1(k) &:= b_k\beta_0 + a_k\beta_1 + b_k\beta_2 - c_k\beta_3, \\ \theta_2(k) &:= -c_k\beta_0 + b_k\beta_1 + a_k\beta_2 + b_k\beta_3, \\ \theta_3(k) &:= -c_k\beta_0 - c_k\beta_1 + b_k\beta_2 + a_k\beta_3, \\ \theta_4(k) &:= b_k\beta_0 - c_k\beta_1 - c_k\beta_2 + b_k\beta_3. \end{aligned}$$

例題 3.10 (Davis-Eloff-Spearman-Williams [5, 7])**.** $n=-1$ のとき, $K^{\mathrm{Leh}}=\mathbb{Q}(\zeta_{11}+\zeta_{11}^{-1})$ のすべての NIB の生成元は次で与えられる.[6]

$$\{x \mid \mathbb{Q}(\zeta_{11}+\zeta_{11}^{-1}) \text{ の NIB の生成元 }\} = \{\pm\sigma^{\ell}.\,\xi_k \mid \ell \in \mathbb{Z}/5\mathbb{Z},\, k \in \mathbb{Z}\},$$
$$\xi_k := \frac{1}{10}(25F_{2k}+(-1)^k L_{2k}-2)+\frac{1}{2}(-5F_{2k}+(-1)^k L_{2k})\,\rho-4F_{2k}\,\rho^2+F_{2k}\,\rho^3+F_{2k}\,\rho^4.$$

例題 3.11. $n=14$ のとき, K^{Leh} のすべての NIB の生成元は次で与えられる.

$$\{x \mid K^{\mathrm{Leh}}\text{の NIB の生成元 }\} = \{\pm\sigma^{\ell}.\,\xi_k \mid \ell \in \mathbb{Z}/5\mathbb{Z},\, k \in \mathbb{Z}\},$$
$$\xi_k = (\theta_0(k)\rho+\theta_1(k)\rho^{(1)}+\theta_2(k)\rho^{(2)}+\theta_3(k)\rho^{(3)}+\theta_4(k)\rho^{(4)}+(-1)^k 1201)/71,$$
$$\theta_0(k)=\frac{31}{5}(-1)^k-L_{2k-1}-\frac{6}{5}L_{2k+1},$$
$$\theta_1(k)=\frac{31}{5}(-1)^k+\frac{4}{5}L_{2k+1},$$
$$\theta_2(k)=\frac{31}{5}(-1)^k+\frac{1}{5}L_{2k-1}+2L_{2k+1},$$
$$\theta_3(k)=\frac{31}{5}(-1)^k-\frac{12}{5}L_{2k-1}+\frac{7}{5}L_{2k+1},$$
$$\theta_4(k)=\frac{31}{5}(-1)^k+\frac{16}{5}L_{2k-1}-3L_{2k+1}.$$

$-5 \le k \le 5$ に対する ξ_k の具体的な値は以下の通りである.

k	ξ_k
-5	$(71+1451\rho-304\rho^{(1)}-959\rho^{(2)}+1856\rho^{(3)}-2044\rho^{(4)})/355$
-4	$(-71+554\rho-116\rho^{(1)}-366\rho^{(2)}+709\rho^{(3)}-11\rho^{(4)})/355$
-3	$(71+211\rho-44\rho^{(1)}-139\rho^{(2)}+271\rho^{(3)}-299\rho^{(4)})/355$
-2	$(-71+79\rho-16\rho^{(1)}-51\rho^{(2)}+104\rho^{(3)}-116\rho^{(4)})/355$
-1	$(71+26\rho-4\rho^{(1)}-14\rho^{(2)}+41\rho^{(3)}-49\rho^{(4)})/355$
0	$(-71-\rho+4\rho^{(1)}+9\rho^{(2)}+19\rho^{(3)}-31\rho^{(4)})/355$
1	$(71-29\rho+16\rho^{(1)}+41\rho^{(2)}+16\rho^{(3)}-44\rho^{(4)})/355$
2	$(-71-86\rho+44\rho^{(1)}+114\rho^{(2)}+29\rho^{(3)}-101\rho^{(4)})/355$
3	$(71-229\rho+116\rho^{(1)}+301\rho^{(2)}+71\rho^{(3)}-259\rho^{(4)})/355$
4	$(-71-601\rho+304\rho^{(1)}+789\rho^{(2)}+184\rho^{(3)}-676\rho^{(4)})/355$
5	$(71-1574\rho+796\rho^{(1)}+2066\rho^{(2)}+481\rho^{(3)}-1769\rho^{(4)})/355$

注意 3.12. Lehmer の 5 次巡回体 K^{Leh} の無限個の NIB の生成元のうち, どの元がガウス周期かは分かっていない.

4　定理 2.1, 定理 3.1 の証明の概略

定理 2.1, 定理 3.1 の証明は, Acciaro-Fieker [1] による素数次巡回拡大体の NIB を求めるアルゴリズムをパラメーター付きで適用することにより得られる. このアルゴリズムは大まかに述べると, 正規基底 (Normal Basis, NB) と整基底 (Integral Basis, IB) から正規整基底を求めるアルゴリズムである. $K^{\mathrm{Sh}}, K^{\mathrm{Leh}}$ の正規基底は $n \neq 0$ ならば, それぞれ $f_n^{\mathrm{Sh}}(X), f_n^{\mathrm{Leh}}(X)$ の

[6] $n=-1$ のとき, $f_n^{\mathrm{Leh}}(X)=X^5+X^4-4X^3-3X^2+3X+1$ は $\zeta_{11}+\zeta_{11}^{-1}$ の $\mathbb{Q}$ 上の最小多項式である.

根 ρ のすべての共役元で与えられる. 整基底については, K^{Sh} の場合, Δ_n が square-free ならば, $\{1, \rho, \rho^2\}$ が整基底となることが知られていた ([27]).[7] K^{Leh} の場合は, Δ_n が square-free ならば $\{1, \rho, \rho, \rho^2, \rho^3, *\}$ の形の整基底をもつこと ([9]), cube-free ならば $\{1, \rho, \rho, \rho^2, *, *\}$ の形の整基底をもつこと ([6]) が知られていた.[8] Acciaro-Fieker のアルゴリズムを用いるために, まず馴分岐拡大のときに K^{Sh}, K^{Leh} の整基底をパラメーター付きで与える. 正規基底と整基底から正規整基底を得るには, 次の Step1 $\sim$ Step4 を計算する (詳細は [13, 14] 参照).

$p = 3$ または 5, $\zeta := \zeta_p$, $K = K^{\mathrm{Sh}}$ または K^{Leh}, $G := \mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle$ とおき, ξ を求める NIB の生成元とする.

Step 1. NB の生成元 ρ に対し, $\ell\mathcal{O}_K \subset \mathbb{Z}[G].\rho$ をみたす整数 $\ell(\neq 0)$ を求める. このとき, $\mathcal{O}_K \subset \mathbb{Z}[G].(\rho/\ell)$ から $\xi = g.(\rho/\ell)$ をみたす $g \in \mathbb{Z}[G]$ が存在する. ξ を求めるためには g を求めればよい. ξ は NIB の生成元なので, $\mathcal{O}_K = \mathbb{Z}[G].\xi = g\mathbb{Z}[G].(\rho/\ell)$ である.

Step 2. $\{\alpha_1, \ldots, \alpha_p\}$ を $\mathcal{O}_K$ の IB とする. Step 1 より, 任意の $i \in \{1, \ldots, p\}$ に対し, $\alpha_i = g_i.(\rho/\ell)$ をみたす $g_i \in \mathbb{Z}[G]$ が存在するので, これを求める. このとき,

$$(g_1, \ldots, g_p) + \mathrm{Ann}_{\mathbb{Z}[G]}(\rho/\ell) = (g) + \mathrm{Ann}_{\mathbb{Z}[G]}(\rho/\ell)$$

が成り立つが, ρ/ℓ が NB の生成元であることから, $\mathrm{Ann}_{\mathbb{Z}[G]}(\rho/\ell) = 0$ となり, $(g_1, \ldots, g_p) = (g) =: \mathcal{I}$ を得る.

Step 3. 環の全射準同型写像 $\nu : \mathbb{Z}[G] \twoheadrightarrow \mathbb{Z}[\zeta]$, $\nu(\sigma) = \zeta$ に対し, $\nu(\mathcal{I}) = (\nu(g)) = (\nu(g_1), \ldots, \nu(g_p))$ が成り立つ. $\mathbb{Z}[\zeta]$ は単項イデアル整域なので, Step 2 で求めた $g_1, \ldots g_p \in \mathbb{Z}[G]$ に対し, イデアル $(\nu(g_1), \ldots, \nu(g_p))$ の生成元 $\gamma = \sum_{j=0}^{p-2} n_j\zeta^j \in \mathbb{Z}[\zeta]$ が求まる. このとき, ある $u \in \mathbb{Z}[\zeta]^\times$ に対し, $\nu(g) = u\gamma$ である. $u \equiv \pm 1 \pmod{(1-\zeta)}$ が示せ, ν から得られる補題 1.3 の同型から $\nu(v) = u^{-1}$ をみたす $v \in \mathbb{Z}[G]^\times$ が存在する.

Step 4. $\nu(vg) = \nu(v)\nu(g) = \gamma = \nu(\sum_{j=0}^{p-2} n_j\sigma^j)$ より, $vg - \sum_{j=0}^{p-2} n_j\sigma^j \in \mathrm{Ker}\,\nu = (1_G + \sigma + \sigma^2 + \sigma^3 + \sigma^4)$ から $(vg - \sum_{j=0}^{p-2} n_j\sigma^j).(\rho/\ell) = m\mathrm{Tr}_{K/\mathbb{Q}}(\rho/\ell)$ をみたす $m \in \mathbb{Z}$ が存在するので, これを求める. $v \in \mathbb{Z}[G]^\times$ より, NIB の生成元 $v.\xi$ が

$$v.\xi = (vg).(\rho/\ell) = \sum_{j=0}^{p-2} n_j\sigma^j.(\rho/\ell) + \frac{m}{l}\mathrm{Tr}_{K/\mathbb{Q}}(\rho)$$

として得られる.[9]

謝辞

このたび講演の機会を下さった世話人の先生方に, 心より感謝致します.

参考文献

[1] V. Acciaro and C. Fieker, Finding normal integral bases of cyclic number fields of prime degree, J. Symbolic Comput. **30** (2000), no. 2, 129–136.

[7] さらに K^{Sh} の導手 $\mathfrak{f}$ に対し, $\Delta_n/\mathfrak{f}$ が立方数のとき, K^{Sh} はべき整基底 (Power Integral Basis) をもつことが知られている ([10, 16]).

[8] 「*」は具体的に記述することができる. Gras の結果 [11] から, べき整基底をもつ K^{Leh} は $L_{-1} = L_{-2} = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ のみであることが分かる.

[9] K^{Sh} のとき $\mathrm{Tr}_{K/\mathbb{Q}}(\rho) = n$ であり, K^{Leh} のとき $\mathrm{Tr}_{K/\mathbb{Q}}(\rho) = -n^2$ である.

[2] A. A. Albert, A determination of the integers of all cubic fields, Ann. of Math. (2) **31** (1930), no. 4, 550–566.

[3] A. Châtelet, Arithmétique des corps abélians du troisième degré, Ann. Sci. École Norm. sup. (3) **63** (1946), 109–160.

[4] T. W. Cusick, Lower bounds for regulators, Number theory, 63–73, Lecture Notes in Math., 1068, Springer, Berlin, 1984.

[5] C. Davis, D. Eloff and B. K. Spearman, Normal integral bases of a cyclic quintic field, Fibonacci Quart. **55** (2017), no. 2, 152–156.

[6] D. Eloff, B. K. Spearman and K. S. Williams, Integral bases for an infinite family of cyclic quintic fields, Asian J. Math. **10** (2006), no. 4, 765–771.

[7] D. Eloff, B. K. Spearman and K. S. Williams, A number field with infinitely many normal integral bases, Fibonacci Quart. **45** (2007), no. 2, 151–154.

[8] A. Fröhlich, Artin root numbers and normal integral bases for quaternion fields, Invent. Math. **17** (1972), 143–166.

[9] I. Gaál and M. Pohst, Power integral bases in a parametric family of totally real cyclic quintics, Math. Comp. **66** (1997), no. 220, 1689–1696.

[10] M. N. Gras, Sur les corps cubiques cycliques dont l'anneau des entiers est monogène, Ann. Sci. Univ. Besancon Math. (3) 1973, no. 6, 26 pp.

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

[12] S. A. Hambleton and H. C. Williams, Cubic fields with geometry, CMS Books in Mathematics/Ouvrages de Mathematiques de la SMC, Springer, Cham, 2018.

[13] Y. Hashimoto and M. Aoki, Normal integral bases and Gaussian periods in the simplest cubic fields, to appear in Annales mathématiques du Québec.

[14] Y. Hashimoto and M. Aoki, Normal integral bases of Lehmer's cyclic quintic fields, preprint, 2022.

[15] S. Jeannin, Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer, J. Théor. Nombres Bordeaux **8** (1996), no. 1, 75–92.

[16] T. Kashio and R. Sekigawa, The characterization of cyclic cubic fields with power integral bases, Kodai Math. J. **44** (2021), no. 2, 290–306.

[17] 木田 雅成, Lehmer の 5 次多項式に関するいくつかの問題について, 計算機代数システムの進展, 64–76, COE Lecture note series, 35, 九州大学大学院数理学研究院, 2011.

[18] A. J. Lazarus, Gaussian periods and units in certain cyclic fields, Proc. Amer. Math. Soc. **115** (1992), no. 4, 961–968.

[19] E. Lehmer, Connection between Gaussian periods and cyclic units, Math. Comp. **50** (1988), no. 182, 535–541.

[20] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers. Third edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2004.

[21] 岡崎 龍太郎, Exposition of "The simplest cubic fields are non-isomorphic to each other", 177–198, 構成的ガロア逆問題と不変体の有理性問題, 第 27 回整数論サマースクール報告集, 2020.

[22] R. Schoof and L. C. Washington, Quintic polynomials and real cyclotomic fields with large class numbers, Math. Comp. **50** (1988), no. 182, 535–541.

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

[24] B. K. Spearman and K. S. Williams, Normal integral bases for Emma Lehmer's parametric family of cyclic quintics, J. Théor. Nombres Bordeaux **16** (2004), no. 1, 215–220.

[25] 角皆 宏, ガロア群の構成問題の明示解の活用～明示的な多項式があると出来ること～, 199–216, 構成的ガロア逆問題と不変体の有理性問題, 第 27 回整数論サマースクール報告集, 2020.

[26] G. Voronoi, Concerning algebraic integers derivable from a root of an equation of the third degree, Master's Thesis, St. Petersburg, 1894.

[27] L. C. Washington, Class numbers of the simplest cubic fields, Math. Comp. **48** (1987), no. 177, 371–384.