類数が5の倍数である虚二次体の新たな族について

Kwang-Seob Kim (Chosun University)　岸 康弘 (愛知教育大学)

概 要

本稿では $5D_s = F_{10s+5}$ (F_n は n 番目のフィボナッチ数) を満たす D_s に対し, 虚二次体 $\mathbb{Q}(\sqrt{-D_s})$ を考察する. 先行研究 [6] では, $s \not\equiv 0 \pmod{20}$ のとき, $\mathbb{Q}(\sqrt{-D_s})$ の類数が 5 で割り切れることが示された. 本論文では議論を精緻化することでこの制限を取り除き, 任意の正整数 s に対して $\mathbb{Q}(\sqrt{-D_s})$ の類数が 5 で割り切れることを証明する. 証明は, 5 次多項式の構成, フィボナッチ数とリュカ数の性質, および佐瀬による分岐判定基準を組み合わせ, 次数 10 の二面体拡大内に不分岐な C_5-拡大を実現することで与えられる.

1　序文

二次体の類数の可除性は数論における古典的テーマである. 任意の整数 $n > 1$ に対し, 類数が n で割り切れる虚二次体は無限に存在することが知られている (Ankeny–Chowla [1], 山本 [13], Murty [8, 9], Soundararajan [11], etc.). しかしながら, 具体的な無限族を与えることは容易ではない. $n = 5$ の場合に関しては, 佐瀬 [10] による 5 次多項式と分岐制御の方法, Byeon [3] による実二次体の場合の議論, さらにフィボナッチ・リュカ数を用いた岸 [7], 青木-岸 [2] などの構成がある.

Jin–Kim による先行論文 [6] では,

$$D_s = \frac{F_{10s+5}}{5}$$

とおき, 虚二次体 $\mathbb{Q}(\sqrt{-D_s})$ の類数が $s \not\equiv 0 \pmod{20}$ のとき 5 で割り切れることを示した. その証明の要点は, 二次部分体が $\mathbb{Q}(\sqrt{-D_s})$ となる D_5-拡大を与えるような 5 次多項式を構成し, この拡大が $\mathbb{Q}(\sqrt{-D_s})$ 上不分岐な C_5-拡大であることを確かめることにあった.

本稿の目的は, 先の制限 $s \not\equiv 0 \pmod{20}$ を取り除いた次の定理を示すことである.

定理 1.1. 任意の正整数 s に対し, 5 次多項式

$$g_s(X) := X^5 - 10X^3 - 20X^2 + 5(20F_{10s+5}^2 - 3)\,X + 40F_{10s+5}^2(1 + (-1)^{s+1}L_{10s+5}) - 4$$

は $\mathbb{Q}$ 上既約であり, その分解体は $\mathbb{Q}(\sqrt{-D_s})$ 上の不分岐な C_5-拡大を与える. 従って, $\mathbb{Q}(\sqrt{-D_s})$ の類数は 5 で割り切れる.

先行論文 [6] においては, $s \equiv 0 \pmod{20}$ の場合に $g_s(X)$ の既約判定のための素数が与えられていなかったことに対し, 環類体や惰性次数の議論とフィボナッチ・リュカ数の追加的性質を組み合わせることによりそのような素数を見つけたことが, 証明の鍵となる. 不分岐性については, [6] と同様となる佐瀬の分岐制御の方法を用いる.

論文の構成は次の通りである. 第 2 節では二面体拡大の構成と Sase の判定法を復習する. 第 3 節ではフィボナッチ数とリュカ数の必要事項を整理する. 第 4 節では $\mathbb{Z}[\sqrt{-125}]$ の環類体の性質を調べる. 第 5 節では主定理 (定理 1.1) に証明を与える.

2　二面体拡大の構成と Sase の判定法

2.1　二面体拡大を与える 5 次多項式

非負整数 s に対し, 整数係数の 5 次多項式 $G_s(X)$, $g_s(X)$ を

$$G_s(X) := X^5 - 10X^3 - 20X^2 + 5(20F_{2s+1}^2 - 3)\,X + 40F_{2s+1}^2(1 + (-1)^s L_{2s+1}) - 4,$$
$$g_s(X) := X^5 - 10X^3 - 20X^2 + 5(20F_{10s+5}^2 - 3)\,X + 40F_{10s+5}^2(1 + (-1)^{s+1} L_{10s+5}) - 4$$

で定める. これらは, [5, Example 3.3] の手法で作られた多項式であり, 先行研究により次のことが示されている.

命題 2.1 ([7, Theorem 1])**.** $G_s(X)$ が $\mathbb{Q}$ 上既約ならば, その分解体は $\mathbb{Q}$ 上 D_5-拡大であり, 二次体 $\mathbb{Q}(\sqrt{-F_{2s+1}})$ を含む.

命題 2.2 ([6, Proposition 2.1, §4])**.** $g_s(X)$ が $\mathbb{Q}$ 上既約ならば, その分解体は $\mathbb{Q}$ 上 D_5-拡大であり, 二次体 $\mathbb{Q}(\sqrt{-D_s})$ を含む.

2.2　佐瀬による素数の分岐判定基準

佐瀬は, 多項式

$$\varphi(X) = X^p + \sum_{j=0}^{p-2} a_j X^j \quad (a_j \in \mathbb{Z})$$

の根で定まる p 次体において素数が完全分岐するための判定法を与えた.

命題 2.3 (Sase の判定法, [10, Proposition 2])**.** $p \neq 2$, q を素数とする. また, 上記多項式 $\varphi(X) \in \mathbb{Z}[X]$ が $\mathbb{Q}$ 上既約とし, $v_q(a_j) < p - j$ を満たす j $(0 \leq j \leq p-2)$ が少なくとも一つあるとする. さらに, θ を φ の根とする.
(1) $q \neq p$ のとき, q が $\mathbb{Q}(\theta)/\mathbb{Q}$ で完全分岐することと,

$$0 < \frac{v_q(a_0)}{p} \leq \frac{v_q(a_j)}{p-j} \quad \text{for every } j,\ 1 \leq j \leq p-2$$

が成り立つことは同値である.
(2) $q = p$ が $\mathbb{Q}(\theta)/\mathbb{Q}$ で完全分岐することと, (S-i) または (S-ii) のいずれかが成り立つことは同値である.

(S-i) $0 < \dfrac{v_p(a_0)}{p} \leq \dfrac{v_p(a_j)}{p-j}$ for every $j,\ 1 \leq j \leq p-2$.

(S-ii) (S-ii-1) $v_p(a_0) = 0$.
(S-ii-2) $v_p(a_j) > 0$ for every $j,\ 1 \leq j \leq p-2$.
(S-ii-3) $\dfrac{v_p(\varphi(-a_0))}{p} \leq \dfrac{v_p(\varphi^{(j)}(-a_0))}{p-j}$ for every $j,\ 1 \leq j \leq p-1$.
(S-ii-4) $v_p(\varphi^{(j)}(-a_0)) < p - j$ for some $j,\ 0 \leq j \leq p-1$.

3　フィボナッチ数とリュカ数の性質

3.1　基本性質

ここでは, フィボナッチ数 F_n とリュカ数 L_n の基本的な性質を述べる. まず初めに, 定義及び一般項を再掲する:

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n, \quad L_0 = 2,\ L_1 = 1,\ L_{n+2} = L_{n+1} + L_n,$$
$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n), \quad L_n = \alpha^n + \beta^n. \tag{3.1}$$

但し, $\alpha = (1+\sqrt{5})/2,\ \beta = (1-\sqrt{5})/2$.

命題 3.1. 任意の整数 m, n について

$$F_{n+m} + (-1)^m F_{n-m} = F_n L_m, \quad L_{n+m} + (-1)^m L_{n-m} = L_n L_m.$$

命題 3.2. 整数 m, n に対し,

$$L_m \mid L_n \iff {}^{\exists}k \in \mathbb{Z} \ \text{ s.t. } \ n = (2k-1)m.$$

特に, 命題 3.1 により, 任意の $t \in \mathbb{Z}$ に対して

$$F_{200t+5} + F_5 = F_{100t+5} L_{100t}, \quad L_{200t+5} + L_5 = L_{100t+5} L_{100t} \tag{3.2}$$

が成り立つことがわかる.

3.2　リュカ数の特殊な素因子

補題 3.3. $n = p_1 \cdots p_k$ (p_i は素数) とし, 各 p_i が $p_i = x_i^2 + 5y_i^2$ $(x_i, y_i \neq 0)$ の形で表せたとする. このとき, n も $n = x^2 + 5y^2$ の形で表せる. また, すべての i で $5 \mid y_i$ ならば $5 \mid y$ となる.

Proof. 恒等式 $(a^2 + Db^2)(c^2 + Dd^2) = (ac + Dbd)^2 + D(ad - bc)^2$ から前半は直ちに従う. 後半は $\mathbb{Q}(\sqrt{-5})$ における分解と虚部比較による. □

命題 3.4. 任意の $u > 0$ に対し, $L_{2^u 5}$ は $p \equiv 1, 9 \pmod{20}$ を満たし, かつ $p = x^2 + 125y^2$ の形で表せない素因子 p を持つ.

Proof. $L^*_{2^u 5} := L_{2^u 5}/L_{2^u}$ とおく. (3.1) を用いて直接計算することにより, 等式

$$L^*_{2^u 5} = (5F_{2^u}^2 + 1)^2 + 5F_{2^u}^2 = (5F_{2^u}^2 - 1)^2 + (5F_{2^u})^2 \tag{3.3}$$

を得る. p を $L^*_{2^u 5}$ の素因子とすると,

$$(5F_{2^u}^2 + 1)^2 \equiv -5F_{2^u}^2 \pmod{p}, \quad (5F_{2^u}^2 - 1)^2 \equiv -(5F_{2^u})^2 \pmod{p}$$

となることから, -5, -1 がともに mod p で平方剰余となり, $p \equiv 1, 9 \pmod{20}$ を導く. また $F_{2^u} \not\equiv 0 \pmod{5}$ と補題 3.3 より, $L^*_{2^u 5}$ の素因子のうち少なくとも一つは $x^2 + 125y^2$ の形にならないことがわかる. □

注意 3.5. $u = 0$ では (3.3) は成り立たない.

系 3.6. 任意の $t > 0$ に対し, L_{100t} は $p \equiv 1, 9 \pmod{20}$ を満たし, かつ $p = x^2 + 125y^2$ の形で表せない素因子 p を持つ.

Proof. $100t = 2^u 5v$ (v は奇数) とすると, 命題 3.2 から $L_{2^u 5} \mid L_{100t}$. よって, 命題 3.4 より系 3.6 を得る. □

4 $\mathbb{Z}[\sqrt{-125}]$ の環類体

4.1 ある二面体多項式と分解体

s を $s \equiv 0 \pmod{20}$ を満たす正の整数とし, $s = 20t$ $(t \in \mathbb{Z})$ と表す. また, p を L_{100t} の素因子とする. (3.2) より $F_{200t+5} \equiv -F_5 \pmod{p}$, $L_{200t+5} \equiv -L_5 \pmod{p}$ となることから

$$g_{20t}(X) \equiv X^5 - 10X^3 - 20X^2 + 2485X + 11996 \pmod{p}$$

を得る. ここで,

$$h(X) := X^5 - 10X^3 - 20X^2 + 2485X + 11996$$

とおくと, $h(X)$ は $\mathbb{Q}$ 上既約であることが確かめられる. そこで, $h(X)$ の分解体を L と書く. また, $K = \mathbb{Q}(\sqrt{-5})$ とおく.

命題 4.1. $L/\mathbb{Q}$ は D_5-拡大で, 唯一の二次部分体は K である. さらに L/K は 5 の外で不分岐な C_5-拡大であり, 5 の上の素イデアルは完全分岐する.

Proof. $h(X) = G_2(X)$ であることから命題 2.1 を適用する. Sase の判定法 (命題 2.3) により, 5 以外は完全分岐せず 5 が完全分岐することが確認できる. □

4.2 $\mathbb{Z}[\sqrt{-125}]$ の環類体

K の極大整環 $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ の判別式は $d_K = -20$ で, K の類数は $h_K = 2$ となる. また, 導手 5 の整環 $\mathcal{O} = \mathbb{Z}[\sqrt{-125}] = \mathbb{Z} + 5\sqrt{-5}\,\mathbb{Z}$ の判別式は -500 で, 類数は類数公式 (例えば [4, p. 146]) により $h(\mathcal{O}) = 10$ となることがわかる. $\mathcal{O}$ の環類体 M は $[M : K] = 10$ で, K の Hilbert 類体 $\mathbb{Q}(\sqrt{-5}, \sqrt{-4})$ を中間体として含み, さらに, K 上の導手が $(5) \cdot \infty$ を割る $\mathbb{Q}$ 上の D_5-拡大をすべて含む ([12, p. 75]). よって, 命題 4.1 から $L \subset M$ が従う.

ここで, 素数 $p \neq 5$ が M で完全分解するための必要十分条件を与える.

命題 4.2. $p \neq 5$ が M で完全分解することと, $p = x^2 + 125y^2$ $(x, y \in \mathbb{Z})$ の形で表せることは同値である.

Proof. [4, Theorem 9.4] を参照. □

4.3 素数の選択と惰性次数による既約性

補題 4.3. $p \equiv 1, 9 \pmod{20}$ を満たし, かつ $p = x^2 + 125y^2$ の形で表せない素数 p に対し, $h(X)$ は mod p で既約である.

Proof. p は $p \equiv 1, 9 \pmod{20}$ を満たすことから $\mathbb{Q}(\sqrt{-5})$ と $\mathbb{Q}(\sqrt{-4})$ の双方で分解し, 従って $\mathbb{Q}(\sqrt{-5}, \sqrt{-4})$ で完全分解する. もし p が $L/\mathbb{Q}$ で完全分解すれば $M/\mathbb{Q}$ でも完全分解するが, これは命題 4.2 に反する. よって $L/\mathbb{Q}$ における p の惰性次数は 5 となり, 従って $h(X)$ は mod p で既約である. □

5　主定理の証明

$s \not\equiv 0 \pmod{20}$ のとき, それぞれ $s \equiv 1, 2, 3, 6, 7, 8 \pmod{10}$ ならば mod 151 で, $s \equiv 4, 9 \pmod{10}$ ならば mod 101 で, $s \equiv 5 \pmod{20}$ ならば mod 401 で, $s \equiv 15 \pmod{20}$ ならば mod 41 で $g_s(X)$ は既約となる ([6, Proposition 4.2]). また, $s \equiv 0 \pmod{20}$ のときは, $s = 20t$ ($t \in \mathbb{Z}$) と表すと, 系 3.6 の素数 p に対して $g_s(X) \equiv h(X) \pmod{p}$ となり, 補題 4.3 より $h(X)$ は mod p で既約となる. 従って, 任意の正整数 s に対して $g_s(X)$ は $\mathbb{Q}$ 上既約である.

命題 2.2 により $g_s(X)$ の分解体は $\mathbb{Q}$ 上 D_5-拡大で $\mathbb{Q}(\sqrt{-D_s})$ を含む. そこで, Sase の判定法 (命題 2.3) を適用すると, 5 以外は完全分岐せず, さらに 5 も完全分岐しないことが確認できる. よって $\mathbb{Q}(\sqrt{-D_s})$ 上不分岐な C_5-拡大が得られる.

以上により, 主定理が示された.

注意 5.1. $s = 0$ では $\mathbb{Q}(\sqrt{-D_0}) = \mathbb{Q}(i)$ で類数は 1 となる.

参考文献

[1] N. Ankeny and S. Chowla, On the divisibility of the class numbers of quadratic fields, Pacific J. Math. **5** (1955), 321–324.

[2] M. Aoki and Y. Kishi, An infinite family of pairs of imaginary quadratic fields with both class numbers divisible by five, J. Number Theory **176** (2017), 333–343.

[3] D. Byeon, Real quadratic fields with class number divisible by 5 or 7, Manuscripta Math. **120** (2006), 211–215.

[4] D. A. Cox, Primes of the form $x^2 + ny^2$, John Wiley & Sons, New York etc., 1989.

[5] M. Imaoka and Y. Kishi, On dihedral extensions and Frobenius extensions, In: Galois theory and modular forms, 195–220, Dev. Math., 11, Kluwer Acad. Publ., Boston, MA, 2004.

[6] S. Jin and K.-S. Kim, A new family of imaginary quadratic fields with class number divisible by 5, Ramanujan J. **66** (2025), Paper No. 53,

[7] Y. Kishi, A new family of imaginary quadratic fields whose class number is divisible by five, J. Number Theory **128** (2008), 2450–2458.

[8] M. R. Murty, The ABC conjecture and exponents of class groups of quadratic fields, In: Number theory, 85–95, Contemp. Math., 210, American Mathematical Society, Providence, RI, 1998.

[9] M. R. Murty, Exponents of class groups of quadratic fields, In: Topics in Number Theory (Univ. Park, PA, 1997), 229–239, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999.

[10] M. Sase, On a family of quadratic fields whose class numbers are divisible by five, Proc. Japan Acad. Ser. A Math. Sci. **74** (1998), 120–123.

[11] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. Lond. Math. Soc. **61** (2000), 681–690.

[12] P. Stevenhagen, Ray class groups and governing fields, Publ. Math. Fac. Sci. Besançon, Théor. Nombres 1988/89, No. 1, 1989.

[13] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57–76.