類数が 5 で割り切れる二次体について*

東北大・理　佐藤 篤 (Atsushi SATO)

1 序

2 個のパラメータ a, b をもつ, 変数 X の 3 次式 $F(a, b\,; X)$ を

$$\begin{aligned} F(a, b\,; X) = 4X^3 + (a^2 + 6ab + b^2)X^2 + 2ab(10a^2 - 19ab - 9b^2)X \\ + ab(4a^4 - 40a^3b - 20a^2b^2 - 59ab^3 - 4b^4) \end{aligned}$$

により定める. このとき, 多くの $a, b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ に対し, 体 $\mathbb{Q}\big(\sqrt{F(a, b\,; \xi)}\big)$ の類数は 5 で割り切れることが知られている. より正確には, 3 個のパラメータ a, b, ξ をもつ, 変数 x の 5 次式 $\Lambda(a, b, \xi\,; x)$ を

$$\begin{aligned} \Lambda(a, b, \xi\,; x) = x^5 + 2abx^4 - ab(a^2 - 3ab - b^2)x^3 + 3a^2b^3(a + b)x^2 + a^3b^4(a + 3b)x + a^4b^6 \\ - \xi(x^4 + 2abx^3 + a^2b^2x^2) \end{aligned}$$

により定めるとき, 次が成り立つ:

定理 1.1 $a, b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ が次の条件をみたすとする:

(C1) $\Lambda(a, b, \xi\,; x)$ は $\mathbb{Q}$ 上既約;

(C2) $ab(a^2 + 11ab - b^2)$ の任意の素因子 p に対し,

$$\text{(1.1)} \qquad \begin{cases} \min\big\{\, \mathrm{ord}_p F(a, b\,; \xi),\, \mathrm{ord}_p F'(a, b\,; \xi) \,\big\} \le 0 & (p \neq 2 \text{ の場合}), \\ \mathrm{ord}_2\, \xi \le 0 & (p = 2 \text{ の場合}). \end{cases}$$

このとき, 体 $\mathbb{Q}\big(\sqrt{F(a, b\,; \xi)}\big)$ の類数は 5 で割り切れる.

本稿で考察するのは, 上の定理の逆に当たる次の問題である:

問題 1.2 類数が 5 で割り切れるような二次体は, 定理 1.1 の条件 (C1), (C2) をみたす $a, b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ によって $\mathbb{Q}\big(\sqrt{F(a, b\,; \xi)}\big)$ と表すことができるか?

---

*仙台数論及び組合せ論小研究集会 2006 (2007 年 1 月 29 日 – 30 日, 於 東北大学大学院情報科学研究科) 報告集

試しに数値実験をしてみると, 次のような結果が得られる:

例 1.3 判別式の絶対値が 10000 以下の二次体のうち, 類数が 5 で割り切れるものは, 実のものが 70 個, 虚のものが 617 個ある. これらのうち, 判別式が -9160 の虚二次体 $\mathbb{Q}\bigl(\sqrt{-2290}\,\bigr)$ を除く全ては, 定理 1.1 の条件 (C1), (C2) および

$$|a| \le 100, \qquad |b| \le 100, \qquad \bigl|(\xi \text{ の分子}) \cdot (\xi \text{ の分母})\bigr| \le 10000$$

をみたす $a, b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ を用いて $\mathbb{Q}\bigl(\sqrt{F(a,b\,;\xi)}\,\bigr)$ と表すことができる.

注意 1.4 (i) $ab = 0$ のとき $\Lambda(a,b,\xi\,;x) = x^5 - \xi x^4 = x^4(x-\xi)$ となるから, 条件 (C1) は $ab \neq 0$ を含む. また, $a, b \in \mathbb{Z}$ が $a^2 + 11ab - b^2 = 0$ をみたすのは $a = b = 0$ のときに限る.

(ii) $F(a,b\,;X)$ の判別式は $16ab(a^2 + 11ab - b^2)^5$.

(iii) $\Lambda(a,b,\xi\,;x)$ の判別式は $a^{14}b^{14}F(a,b\,;\xi)^2$.

(iv) $F(a,b\,;X)$, $\Lambda(a,b,\xi\,;x)$ は次をみたす:

$$F(ra, rb\,; r^2X) = r^6F(a,b\,;X), \qquad \Lambda(ra, rb, r^2\xi\,; r^2x) = r^{10}\Lambda(a,b,\xi\,;x).$$

従って a, b としては $a > 0$ (または $b > 0$) かつ $\gcd(a,b) = 1$ なるものだけを考えれば十分である.

本稿は “楕円曲線の同種写像を用いた代数体の類数の可除性の研究” の一例であり, 本田 [3], [4] における “3 で割り切れる” を “5 で割り切れる” で置き換えたものと言える. しかし, §5 で述べるように, まだ満足すべき結果が得られたとは言い難い. 中途半端な結論であるにも拘わらず講演の機会を与えてくれた主催者, ならびに筆者の手に余った D_5-多項式 (*cf.* §6) を “Brumer 化” してくれた陸名雄一氏に深く感謝したい. なお, 例 1.3 や §6 における数値計算には PARI/GP [9] を用いた.

記号と用語

- C_n で位数 n の巡回群を表し, D_n で位数 $2n$ の二面体群を表す:

$$C_n = \langle\, \sigma \;;\; \sigma^n = 1 \,\rangle, \qquad D_n = \langle\, \sigma, \tau \;;\; \sigma^n = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \,\rangle.$$

- K/k が体の Galois 拡大で $\mathrm{Gal}(K/k)$ が群 G に同型であるとき, K/k を G-拡大と呼ぶ.
- k を体とするとき, 多項式 $f(x) \in k[x]$ の k 上の最小分解体を $\mathrm{Spl}_k\bigl(f(x)\bigr)$ で表す. また, $\mathrm{Spl}_k\bigl(f(x)\bigr)/k$ が G-拡大であるとき, $f(x)$ は k 上の G-多項式であるという.
- K を有限次代数体とするとき, $\mathcal{O}_K$ で K の整数環を表す.

2　準備

本節を通して k を標数 0 の体とし, $l \in \mathbb{Z}, \geq 2$ とする.

2.1　二次体の類数の可除性と有理数体の二面体拡大

K を有限次代数体とするとき, K の類数が l で割り切れることと不分岐な C_l-拡大 L/K が存在することが同値であることは, 類体論から直ちにわかる. また, K が二次体で l が奇素数の場合には, 再び類体論 (および簡単な群論と体論) を用いると次が成り立つことが示せる:

命題 2.1 K を類数が奇素数 l で割り切れる二次体とし, L/K を不分岐な C_l-拡大とする. このとき $L/\mathbb{Q}$ は D_l-拡大である.

さて, l を奇素数とするとき, $D_l = \langle\, \sigma, \tau\ ;\ \sigma^l = \tau^2 = 1,\ \tau\sigma\tau^{-1} = \sigma^{-1} \,\rangle$ の自明でない部分群は $\langle\sigma\rangle \cong C_l$ と $\langle\, \tau\sigma^i \,\rangle \cong C_2$ $(i \in \mathbb{Z}/l\mathbb{Z})$ に限る. また, D_l の l 次対称群 S_l への埋め込みは共役の違いを除いて一意的で, その像は $l \equiv 1 \pmod 4$ (resp. $l \equiv 3 \pmod 4$) のとき l 次交代群 A_l に含まれる (resp. 含まれない). 従って:

命題 2.2 l を奇素数とし, L/k を D_l-拡大とする. このとき, L/k の自明でない中間体は, k 上 2 次のものが 1 個, k 上 l 次のものが l 個存在する. さらに, L/k の k 上 l 次の中間体 $M = k(\theta)$ をとり δ を θ の最小多項式の判別式とするとき, L は M の Galois 閉包で, $l \equiv 3 \pmod 4$ ならば L/k の k 上 2 次の (唯一の) 中間体は $k\big(\sqrt{\delta}\,\big)$ である. なお, $l \equiv 1 \pmod 4$ ならば $\sqrt{\delta} \in k$ となる.

系 2.3 命題 2.1 において, K は L に含まれる唯一の二次体である.

よって, もし仮に有理数体の D_l-拡大 L が全て求められて, しかも C_l-拡大 L/K (K は L に含まれる唯一の二次体) における分岐の様子を知ることが可能であるならば, 類数が l で割り切れる二次体は決定できることになる.

2.2　位数有限の有理点をもつ楕円曲線から生じる巡回拡大と二面体拡大

E を k 上定義された楕円曲線とし, E は位数 l の k-有理点 T をもつとする. このとき, k 上定義された楕円曲線 E^* と k 上定義された同種写像 $\lambda : E \to E^*$ で $\mathrm{Ker}\,\lambda = \langle T\rangle = \{\, [i]T\ ;\ i \in \mathbb{Z}/l\mathbb{Z} \,\}$ となるようなものが k-同型の違いを除いて一意的に存在する (E^* は $E/\langle T\rangle$ とも書かれる). $k(E^*)$ は $\mathrm{Aut}(k(E))$ の部分群 $\langle \tau_T^* \rangle \cong C_l$ の不変体と自然に同一視でき, 従って $k(E)/k(E^*)$ は C_l-拡大である.

さて, $\mathrm{Aut}(k(E))$ の部分群 $\langle [-1]^* \rangle \cong C_2$ の不変体 $k(E)_+$ は E 上の偶函数の全体に一致する. 同様に $\langle \tau_T^*, [-1]^* \rangle$ の不変体 $k(E^*)_+$ は E^* 上の偶函数の全体と同一視できる. また τ_T^* と $[-1]^*$ は

$$[-1]^* \notin \langle \tau_T^* \rangle, \qquad \tau_T^* \circ [-1]^* = [-1]^* \circ (\tau_T^*)^{-1}$$

をみたすことが容易にわかるから, $\langle \tau_T^*, [-1]^* \rangle$ は D_l に同型である. 従って $k(E)/k(E^*)_+$ は D_l-拡大で, $k(E)$ は l 次拡大 $k(E)_+/k(E^*)_+$ の Galois 閉包を与える.

続いて, $E^*/\langle [-1] \rangle \cong \mathbb{P}^1$ 上の k-有理点に関して拡大 $k(E)/k(E^*)/k(E^*)_+$ を特殊化することを考える. すなわち, E^* 上の点 Q で条件

$$\varphi(Q) \in k \cup \{\infty\} \qquad \forall \varphi \in k(E^*)_+ \tag{2.1}$$

をみたすものをとり,

$$K = k(Q), \qquad L = k\big(\lambda^{-1}(Q)\big) \tag{2.2}$$

と置く. このとき K/k は高々 2 次であり, L/K は $C_{l'}$-拡大 (l' は l の約数) である. さらに L/k は Galois 拡大であり, $[K:k] = 2$ かつ $[L:K] = l$ ならば $\mathrm{Gal}(L/k)$ は $\mathrm{Gal}\big(k(E)/k(E^*)_+\big) \cong D_l$ と自然に同一視できる.

なお, Weierstrass 方程式をとって

$$E : y^2 = f(x), \qquad E^* : Y^2 = F(X)$$

($f(x) \in k[x]$, $F(X) \in k[X]$ は共に重根をもたない 3 次式) とすると

$$k(E) = k(x,y), \qquad k(E^*) = k(X,Y), \qquad k(E)_+ = k(x), \qquad k(E^*)_+ = k(X).$$

従って, (2.1) は $X(Q) \in k \cup \{\infty\}$ と同値であり,

$$K = k\big(Y(Q)\big), \qquad L = k\big(x(P),\, y(P)\big)$$

(P は $\lambda^{-1}(Q)$ 内の任意の点) となっている.

3　定理 1.1 の証明の概略

本節では, §1 で定義した $F(a,b;X)$ や $\Lambda(a,b,\xi;x)$ の由来を説明し, 定理 1.1 の証明の概略を述べる. 詳しくは [12] (または [13]) を参照のこと.

$\mathbb{Q}$ 上定義された楕円曲線 E が位数 5 の $\mathbb{Q}$-有理点をもつとき, その方程式として

$$y^2 + (a+b)xy + ab^2 y = x^3 + abx^2 \qquad (a, b \in \mathbb{Z}, \neq 0) \tag{3.1}$$

なるものがとれて, $T = (0,0)$ が位数 5 の点を与える. $E^* = E/\langle T \rangle$ と $\lambda : E \to E^*$ を §2.2 のように定め, それらの具体的な形を Vélu [15] の公式を用いて計算すると, E^* は

$$\begin{aligned} Y^2 + (a+b)XY + ab^2 Y = X^3 + abX^2 + 5ab(a^2 - 2ab - b^2)X \\ + ab(a^4 - 10a^3 b - 5a^2 b^2 - 15ab^3 - b^4) \end{aligned} \tag{3.2}$$

により与えられ, λ は

$$X = \frac{x^5 + 2abx^4 - ab(a^2 - 3ab - b^2)x^3 + 3a^2b^3(a+b)x^2 + a^3b^4(a+3b)x + a^4b^6}{x^4 + 2abx^3 + a^2b^2x^2} \tag{3.3}$$

(Y の表示は省略) により与えられることがわかる. なお, (3.1) の判別式は $-a^5b^5(a^2+11ab-b^2)$ で, (3.2) の判別式は $-ab(a^2+11ab-b^2)^5$ である. また, (3.2) において $Y' = 2Y + (a+b)X + ab^2$ なる変数変換を行うと, E^* の方程式は $(Y')^2 = F(a,b;X)$ となる. さらに, (3.3) の分母を払って整理すると $\Lambda(a,b,X;x) = 0$ となる.

いま, 定理 1.1 の条件 (C1), (C2) をみたす $\xi \in \mathbb{Q}$ をとる. Q を $X(Q) = \xi$ (条件 (2.1) に相当) なる E^* 上の点とし,

$$K = \mathbb{Q}(Q) = \mathbb{Q}\big(\sqrt{F(a,b;\xi)}\,\big), \qquad L = \mathbb{Q}\big(\lambda^{-1}(Q)\big)$$

と置く (*cf.* (2.2)). このとき, 条件 (C1) より $L = \mathrm{Spl}_K\big(\Lambda(a,b,\xi;x)\big)$ で L/K は C_5-拡大になることがわかる. さらに, 条件 (C2) を用いると L/K において全ての有限素点は不分岐であることが示せるが, その鍵となるのは

補題 3.1 点 Q ならびに体 K, L は上の通りとし, $\mathfrak{p}$ を K の素イデアル, $\mathfrak{P}$ を L における $\mathfrak{p}$ の素因子とする. また, (3.2) を $\bmod \mathfrak{p}$ で還元して得られる $\mathcal{O}_K/\mathfrak{p}$ 上の曲線を $\widetilde{E^*}$ とし, (3.1) を $\bmod \mathfrak{P}$ で還元して得られる $\mathcal{O}_L/\mathfrak{P}$ 上の曲線を $\widetilde{E}$ とする. このとき, Q の $\widetilde{E^*}$ における像が非特異であるならば, $\lambda^{-1}(Q)$ 内の点で $\widetilde{E}$ における像が非特異であるようなものが存在する.

([12], 命題 5.4 の特別な場合) である. 一般に奇数次の Galois 拡大において無限素点は分岐しないから, L/K は不分岐な C_5-拡大となり, K の類数は 5 で割り切れる (従って $K \neq \mathbb{Q}$). なお, $L/\mathbb{Q}$ は D_5-拡大で, $L = \mathrm{Spl}_{\mathbb{Q}}\big(\Lambda(a,b,\xi;x)\big)$ でもある.

4 Brumer の 5 次式

標題の式とは, 2 個のパラメータ s,t をもつ, 変数 z の 5 次式

$$B(s,t;z) = z^5 + (s-3)z^4 + (-s+t+3)z^3 + (s^2-s-2t-1)z^2 + tz + s$$

のことである (文献により表記法に多少の違いがある). Armand Brumer が構成したとされるが, 未だに論文は出版されていない模様である. それにも拘わらず, 近藤 [6], [7] は Brumer の元々の構成意図とは無関係に $B(s,t;z)$ を研究し, 次を示した:

定理 4.1 (Kondo) s,t が $\mathbb{Q}$ 上代数的に独立であるとする. このとき:

(i) $B(s,t;z)$ は $\mathbb{Q}(s,t)$ 上の D_5-多項式である.

(ii) $\mathrm{Spl}_{\mathbb{Q}(s,t)}\big(B(s,t\,;z)\big)$ に含まれる $\mathbb{Q}(s,t)$ 上 2 次の (唯一の) 体は $\mathbb{Q}\big(s,t,\sqrt{\delta(s,t)}\,\big)$ である. ただし,

$$\delta(s,t) = -4t^3 + (s^2 - 30s + 1)t^2 + (24s^3 - 34s^2 - 14s)t - 4s^5 + 4s^4 + 40s^3 - 91s^2 + 4s.$$

注意 4.2 $B(s,t\,;z)$ の判別式は $s^2\delta(s,t)^2$.

近藤は, この他にも $s,t \in \mathbb{Q}$ と特殊化した場合に $\mathrm{Spl}_{\mathbb{Q}}\big(B(s,t\,;z)\big)$ における素イデアルの分解の様子を考察し, 二次体 $\mathbb{Q}\big(\sqrt{\delta(s,t)}\,\big)$ の類数が 5 で割り切れるための十分条件を得ている. それらの結果を基に, 佐瀬 [11] は, 岸・三宅 [5] と同様の手法を用いることによって, 類数が 5 で割り切れる二次体の族を構成した.

次の定理は, [8] によると Brumer が示したことになっているが ([8] には Brumer 自身による証明の概略も述べられている), 現在では橋本 [2] 等によって数通りの証明が与えられている:

定理 4.3 (Brumer ?) $B(s,t\,;z)$ は $\mathbb{Q}$ 上の生成的 D_5-多項式である. 特に, 標数 0 の体 k と D_5-拡大 L/k が任意に与えられたとき, $s,t \in k$ が存在して $L = \mathrm{Spl}_k\big(B(s,t\,;z)\big)$ となる.

注意 4.4 Brumer は, 上で述べた $B(s,t\,;z)$ の他に, ある 6 次式の族も構成しており, [6], [7] や [2] ではそれらも考察されている.

[8] の §2 と同様の計算により, §1 で定義した $\Lambda(a,b,\xi\,;x)$ と Brumer の 5 次式 $B(s,t\,;z)$ は

$$B(s,t\,;z) = \frac{z^5}{s^4}\,\Lambda\Big(-s, 1, -2s-t\,;\frac{s}{z}\Big)$$

なる関係で結ばれていることがわかる. 従って, D_5-拡大 $L/\mathbb{Q}$ が任意に与えられたとき, $s,t \in \mathbb{Q}$ で $L = \mathrm{Spl}_{\mathbb{Q}}\big(B(s,t\,;z)\big)$ なるものをとり, $a,b \in \mathbb{Z}$ $(b \neq 0)$ と $\xi \in \mathbb{Q}$ を

$$-s = \frac{a}{b}, \qquad -2s - t = \frac{\xi}{b^2} \tag{4.1}$$

により定めれば, 注意 1.4 の (iv) より

$$B(s,t\,;z) = \frac{z^5}{a^4b^6}\,\Lambda\Big(a, b, \xi\,;-\frac{ab}{z}\Big)$$

となることがわかるから $\mathrm{Spl}_{\mathbb{Q}}\big(B(s,t\,;z)\big) = \mathrm{Spl}_{\mathbb{Q}}\big(\Lambda(a,b,\xi\,;x)\big)$. すなわち:

系 4.5 任意の D_5-拡大 $L/\mathbb{Q}$ に対し, $a,b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ が存在して $L = \mathrm{Spl}_{\mathbb{Q}}\big(\Lambda(a,b,\xi\,;x)\big)$ となる.

5　現状と課題

結論を先に述べておくと, 冒頭に述べた問題 1.2 は, 現時点では肯定的にも否定的にも解決されていない. しかし, 筆者の感触では肯定的に解決される見込みが高いように思われる. 本節では, そのように考えるに至った根拠 (らしきもの) を述べる.

まず, 見通しをよくするため, 問題 1.2 を次の 2 つに切り分けることにする:

問題 5.1 類数が 5 で割り切れるような二次体は, $a, b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ によって $\mathbb{Q}\big(\sqrt{F(a,b\,;\xi)}\,\big)$ と表すことができるか?

問題 5.2 (問題 5.1 が肯定的に解決したとして) $a, b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ は定理 1.1 の条件 (C1), (C2) をみたすか?

5.1　問題 5.1 について

K を類数が 5 で割り切れるような二次体とする. このとき, §2.1 で述べたように, 不分岐な C_5-拡大 L/K が存在して $L/\mathbb{Q}$ は D_5-拡大となる. 従って, 系 4.5 より, $a, b \in \mathbb{Z}$ と $\xi \in \mathbb{Q}$ が存在して $L = \mathrm{Spl}_{\mathbb{Q}}\big(\Lambda(a,b,\xi\,;x)\big)$ となる. また, 明らかに $\Lambda(a,b,\xi\,;x)$ は $\mathbb{Q}$ 上既約である (D_5 は可約な 5 次式の Galois 群としては現れない).

上の a, b に対し, 楕円曲線 E, E^* と同種写像 $\lambda : E \to E^*$ を §3 のように定める. また, Q を $X(Q) = \xi$ なる E^* 上の点とし,

$$K' = \mathbb{Q}(Q) = \mathbb{Q}\big(\sqrt{F(a,b\,;\xi)}\,\big), \qquad L' = \mathbb{Q}\big(\lambda^{-1}(Q)\big)$$

と置く. このとき $[K' : \mathbb{Q}] \le 2$ で, $L' = \mathrm{Spl}_{K'}\big(\Lambda(a,b,\xi\,;x)\big)$ かつ $[L' : K'] = 5$. よって $L = L'$ となり, これより $K = K' = \mathbb{Q}\big(\sqrt{F(a,b\,;\xi)}\,\big)$ が従う.

以上で, 問題 5.1 は肯定的に解決されたことになる.

5.2　問題 5.2 について

上の a, b, ξ が条件 (C1) をみたすことは既に確認済みであるから, 残る問題は (C2) の正否である. すなわち, $ab(a^2 + 11ab - b^2)$ の或る素因子 p に対して条件 (1.1) が成り立っていないと仮定して, そこから矛盾が導ければよい.

いま, p をそのような素数とする. このとき, 補題 3.1 の逆に当たる

補題 5.3 記号や仮定は補題 3.1 と同じとするとき, Q の $\widetilde{E^*}$ における像が特異であるならば, $\lambda^{-1}(Q)$ 内の任意の点の $\widetilde{E}$ における像は特異である.

([14] の主結果の特別な場合) を用いると, $\Lambda(a,b,\xi\,;x)\in\mathbb{Z}_p[x]$ ならびに

$$\Lambda(a,b,\xi\,;x)\equiv(x-c)^5 \pmod{p}$$

が適当な $c\in\mathbb{Z}$ に対して成り立つことが示せる. 従って, $\Lambda(a,b,\xi\,;x)$ の根 θ をとり $M=\mathbb{Q}(\theta)$ と置くとき, $M/\mathbb{Q}$ において p は完全分岐することが期待される. 例えば, $\xi\in\mathbb{Z}$ かつ $p\nmid\big[\mathcal{O}_M:\mathbb{Z}[\theta]\big]$ ならば, p は M において $(p)=(p,\,\theta-c)^5$ と分解される (*cf.* [1], Theorem 4.8.13). p が 5 次拡大 $M/\mathbb{Q}$ で完全分岐するならば $L/\mathbb{Q}$ における p の分岐指数は 5 または 10 となる. 他方, L/K は不分岐であったから, $L/\mathbb{Q}$ における p の分岐指数は 1 または 2 でなければならない. よって $M/\mathbb{Q}$ において p が完全分岐するならば矛盾が得られることになる.

しかし, 次節で述べるように, 条件 (C2) は常に成り立つとは限らず, a,b や ξ の値を適切に取り直さないと話は上手く行かないようである.

6　判別式 -9160 の二次体について

例 1.3 における唯一の例外であった, 判別式が $-9160=-2^3\cdot5\cdot229$ の虚二次体 $K=\mathbb{Q}\big(\sqrt{-2290}\,\big)$ の類数は 20 で,

$$\begin{aligned}H(x)=x^5&-13303238324701431\,x^4+23882651240463868\,x^3\\&-32170459378391208\,x^2+197202371\,x-1\end{aligned}$$

と置くとき $L=\mathrm{Spl}_{\mathbb{Q}}\big(H(x)\big)$ は K の (唯一の) 不分岐 5 次巡回拡大を与える. $H(x)$ は $\mathbb{Q}$ 上の D_5-多項式であるから, $s,t\in\mathbb{Q}$ を適切に選べば $\mathrm{Spl}_{\mathbb{Q}}\big(H(x)\big)=\mathrm{Spl}_{\mathbb{Q}}\big(B(s,t\,;z)\big)$ となるようにできる. そのような s,t は陸名 [10] の "Brumer 化アルゴリズム" によって求めることができて, 例えば

$$s=\frac{5206442060539781884359}{14195747792364511859641285336 15},$$

$$t=\frac{13841372279687335890342508832120394576634133190546721562582368 53}{36918327586426094299917581839308907811074460582852778588617882 00}$$

と置くと $L=\mathrm{Spl}_{\mathbb{Q}}\big(B(s,t\,;z)\big)$ となる (これらの値は陸名氏本人に計算して戴いた). よって

$$a=-5206442060539781884359,\qquad b=14195747792364511859641285336 15,$$

$$\xi=2ab-b^2t=-\frac{13841372550491151740242171167472381908139336819420701706288410 93}{1832}$$

(*cf.* (4.1)) と置けば $L=\mathrm{Spl}_{\mathbb{Q}}\big(\Lambda(a,b,\xi\,;x)\big)$ で $K=\mathbb{Q}\big(\sqrt{F(a,b\,;\xi)}\,\big)$ となる. ところが, このように定めた a,b,ξ は条件 (C2) をみたさない. 実際, $p=3$ に対して条件 (1.1) は成り立っていない. つまり, 問題 5.2 の反例が得られたことになる.

上のように定めた a, b, ξ が (C2) をみたさない以上, パラメータの値を適切に取り直す必要があるのだが, この例の場合には ξ だけを次のように取り替えると上手く行く. すなわち, 上の a, b に対して楕円曲線 E^* を §3 のように定め, Q を $X(Q) = \xi$ なる E^* 上の点とする. このとき

$$\xi' = X\big([2]Q\big) = \frac{1}{4}\left(\frac{F'(a,b\,;\xi)^2}{4F(a,b\,;\xi)} - (a^2 + 6ab + b^2)\right) - 2\xi$$

と置けば, $L = \mathrm{Spl}_{\mathbb{Q}}\big(\Lambda(a,b,\xi'\,;x)\big)$ でもあり, 条件 (C1), (C2) (ξ を ξ' で置き換えたもの) も成立する. 因みに ξ' の分子は 252 桁で分母は 192 桁である.

参考文献

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math. **138**, Springer-Verlag, Berlin, 1993.

[2] K. Hashimoto, Generic families of quintic polynomials with dihedral Galois group of degree 5, 第 45 回代数学シンポジウム報告集, 2000, pp. 15–23.

[3] T. Honda, Isogenies, rational points and section points of group varieties, Japan J. Math. **30** (1960), 84–101.

[4] 本田 平, Abel 多様体と代数的整数論, 数学の歩み **8** (1961), 262–270.

[5] Y. Kishi and K. Miyake, Parametrization of the quadratic fields whose class numbers are divisible by three, J. Number Theory **80** (2000), 209–217.

[6] 近藤 武, ある 6 次式の族とそのガロワ群, 第 12 回代数的組合せ論シンポジウム報告集, 1996, pp. 165–176.

[7] 近藤 武, A. Brumer によって構成された 6 次式の族について, 第 2 回津田塾大学整数論シンポジウム報告集, 津田塾大学数学・計算機科学研究所報 **13**, 1997, pp. 27–36.

[8] O. Lecacheux, Constructions de polynômes génériques à groupe de Galois résoluble, Acta Arith. **86** (1998), 207–216.

[9] PARI/GP, version 2.3.1, Bordeaux, 2006, `http://pari.math.u-bordeaux.fr/`.

[10] 陸名 雄一, 生成的多項式の変換問題について, 第 1 回・第 2 回室蘭数論研究集会報告集, 2007, pp. 92–105.

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

[12] 佐藤 篤, Vélu の公式とその応用, 仙台数論小セミナー 2000 および仙台数論小研究集会 2000 報告集, 2001, pp. 1–24.

[13] A. Sato, On certain extensions of number fields obtained from elliptic curves with rational torsion points, preprint.

[14] A. Sato, On the reduction of certain isogenies of elliptic curves via the formulas by Vélu, preprint.

[15] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sc. Paris **273** (1971), 238–241.

980-8578 仙台市青葉区荒巻字青葉 6-3
東北大学大学院理学研究科数学専攻
E-mail atsushi@math.tohoku.ac.jp