楕円曲線を通じた
Brumer と Lecacheux の 5 次多項式族の研究

小柴将和

新潟大学大学院自然科学研究科博士前期課程
数理物質科学専攻

概要

群 G に対して G 生成的多項式とは基礎体を含むような体上の G-拡大 (ガロア群として G を持つような体) すべてをパラメーターの特殊化によって実現する多項式である. 生成的多項式が与えられたとき次のような問題が考えられる「生成的多項式の異なる変数の特殊化は, いつ同型な分解体を与えるか」(同型問題), また,「同型な分解体を与える変数の組が無限に存在するか」(無限族の構成). その問題に対して, Brumer [Bru](1995 年) により構成された D_5 生成的多項式（以降 Brumer 多項式と呼ぶ）については, 付随する楕円曲線の有理点を用いた木田, 陸名, 佐藤 [KRS](2010 年) の研究結果がある.

筆者は木田, 陸名, 佐藤 [KRS] による研究結果を参考に, Lecacheux によって構成された F_{20} 生成的多項式 (以後 Lecacheux 多項式と呼ぶ) についても同様の結果が得られるかについてフリーの計算ソフトウェア [Sage] を用いて計算を行い考察した. その結果, 楕円曲線の 2 倍写像を用いることで Lecacheux 多項式の最小分解体が同型であるパラメーターの組を構成ができた. 本論文ではその構成についての解説を目標にしている.

第 1 章では, 楕円曲線について, 必要な基本事項についてまとめた. 証明とより詳しい内容に関しては, Silverman による楕円曲線の教科書である [Sil] を参照.

第 2 章では, 2.1 節, 2.2 節については [佐藤] に基づき, 1 章で定義した同種写像を具体的に構成する Vélu の公式について証明を与えた. さらに同種写像により与えられる体の拡大について定義し, そのガロア群について考察を行った. 2.3 節では Vélu の公式について [Sage] 上での実装と具体的な楕円曲線の計算例をみる.

第 3 章では, 3.1 節, 3.2 節については Lecacheux の論文 [Lec](1998 年) に基づき楕円曲線の同種写像を用いた Brumer 多項式と Lecacheux 多項式の構成法を紹介する. 3.3 節では Brumer 多項式と Lecacheux 多項式に関する同型問題について星, 三宅の結果 [HM](2010 年) を紹介する. 3.4 節では付随する楕円曲線を定義し, その有理点により特殊化された Lecacheux 多項式の最小分解体について具体例を計算していく. 3.5 節では Lecacheux 多項式の最小分解体が同型となるパラメーターの組を楕円曲線の 2 倍写像を用いて構成し, 同型を与えていることを証明する.

謝辞

主指導教官である星明考先生には, 学部をあわせて 3 年間の研究室でのセミナー, また本学位論文をまとめるにあたり, 多大なるご指導を賜り深く感謝いたします. 星研究室の金井和貴先輩, 長谷川寿人先輩, 同期の小川紘平君にはセミナーを進める中や, 議論を通じて多くのことを学ばせていただきました. 小島研究室の長峰孝典先輩には折りに触れ, 多くの助言を頂きました. また, 父母には学部, 修士を通じて多くの面で支えていただきました. ここに感謝の意を表します.

目次

1　楕円曲線

この章では, 楕円曲線についての Silverman による標準的な教科者である [Sil] の第 1 章から第 3 章にある楕円曲線, モーデル・ヴェイユ群, 同種写像を定義とそれらに関する命題を復習する.

以下 K を体とする.

定義　種数 1 の非特異曲線 E, 点 $O \in E$ の組 (E, O) を**楕円曲線 (Elliptic curve)** と呼ぶ. E が K 上定義されていて, $O \in E(K)$ であるとき, E は K 上定義されるといい, E/K と表す.

命題 1.1 [Sil, III, 3.1.] E を K 上定義された楕円曲線とする.

1. 次をみたす $x, y \in K(E)$ が存在する. 写像

$$\phi : E \longrightarrow \mathbb{P}^2,\ \phi = [x, y, 1]$$

   は E/K から曲線 $C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ $(a_i \in K)$ (この形の方程式を**ワイエルシュトラス方程式**と呼ぶ) への同型写像でかつ $\phi(O) = [0, 1, 0]$ を満たす. x, y を E に対する**ワイエルシュトラス座標**と呼ぶ.
2. 1. での意味で E に対して得られた任意の二つのワイエルシュトラス方程式は, 次の線形変換により移る.

$$X = u^2X' + r,\ Y = u^3Y' + su^2X' + t\ (u \in K^\times, r, s, t \in K).$$

3. 逆に任意のワイエルシュトラス方程式により与えられるような非特異曲線は K 上定義され, $O = [0, 1, 0]$ (無限遠点) との組であるような楕円曲線である.

前の命題により任意の楕円曲線はワイエルシュトラス方程式により与えられる平面曲線と同型ということが分かった. 以降, **楕円曲線といった場合はワイエルシュトラス方程式により定義される平面曲線のこととする**.

定義　$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ $(a_i \in K)$ 上の点 $P = (x_1,\ y_1),\ Q = (x_2,\ y_2)$ に対して, 次のように演算を定義する：

- $-P = (x_1,\ -y_1 - a_1x_1 - a_3)$,
- $P + Q = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_3,\ -(\lambda + a_1)x_3 - \nu - a_3)$.

また, $\lambda,\ \nu$ は以下のように定める：

- $x_1 = x_2$ のとき, $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$, $\nu = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$,
- $x_1 \neq x_2$ のとき, $\lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$, $\nu = \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$.

さらに, 整数倍を $nP = P + P + \cdots + P$ (n 個の和) で定義する.

この演算は実際に図で考えてみるとよい. 任意の楕円曲線と直線は必ず 3 点で交わり, これらを $P,\ Q,\ R$ とすれば $P + Q + R = O$ が成り立つ.

上で定めた加法によって, $E(\overline{K})$ はアーベル群を成す (このとき無限遠点 O が単位元となる). この加法は有理点に関して閉じており, E 上の K 有理点全体もアーベル群をなす.

定義　E を K 上の楕円曲線とするとき, E 上の K 有理点全体を $E(K)$ と書き**モーデル・ヴェイユ群 (Mordell–Weil group)** と呼ぶ.

定理 1.2 (Mordell–Weil [Sil, VIII. 6.7.])　$E(K)$ は有限生成アーベル群である. すなわち

$$E(K) \simeq \mathbb{Z}^{\oplus r} \oplus G$$

ただし G は有限群である. G は $E(K)$ のねじれ部分なので, $E(K)_{\mathrm{tors}}$ と書くことにする.

$K = \mathbb{Q}$ のときの $E(K)$ のねじれ部分の構造は Mazur により完全に決定されている.

定理 1.3 (Mazur [Sil, VIII. 7.5.])　$E(\mathbb{Q})_{\mathrm{tors}}$ は次のいずれかと同型である：
$\mathbb{Z}/m\mathbb{Z}$,　ただし　$1 \leq m \leq 12,\ m \neq 11$,
$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$,　ただし　$1 \leq m \leq 4$.

楕円曲線はねじれ部分群の構造により, 次の表にあるような楕円曲線と同型であることが Kubert [Kub] によって示されている.

1. $\{0\} : y^2 = x^3 + ax^2 + bx + c\ ;\ \Delta(a,b,c) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0.$
2. $\mathbb{Z}/2\mathbb{Z} : y^2 = x(x^2 + ax + b)\ ;\ \Delta(a,b) = a^2b^2 - 4b^3 \neq 0.$
3. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : y^2 = x(x+r)(x+s)\ ,\ r \neq 0, s \neq 0.$
4. $\mathbb{Z}/3\mathbb{Z} : y^2 + a_1xy + a_3y = x^3\ ;\ \Delta(a_1,a_3) = a_1^3a_3^3 - 27a_3^4 \neq 0.$

これ以降は $E(b,c) := y^2 + (1-c)xy - by = x^3 - by^2\ ,\ \Delta(b,c) := (1-c)^4b^3 - 8(1-c)^2b^4 - (1-c)^3b^3 + 36(1-c)b^4 + 16b^5 - 27b^4$ として b, c の関係式を決める事で得られる.

5. $\mathbb{Z}/4\mathbb{Z} : E(b,c)\ ,\ c = 0\ ,\ \Delta(b,c) = b^4(1-16b) \neq 0.$
6. $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : E(b,c)\ ,\ b = v^2 - 1/16, v \neq 0, \pm 1/4, c = 0.$
7. $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : E(b,c)\ ,\ b = (2d-1)(d-1), c = (2d-1)(d-1)/d,$
   $d = (1-c)(8(1-c)+2)/(8(1-c)-1), d(d-1)(2d-1)(8d^2-8d+1) \neq 0.$
8. $\mathbb{Z}/8\mathbb{Z} : E(b,c)\ ,\ b = (2d-1)(d-1), c = (2d-1)(d-1)/d, \Delta(b,c) \neq 0.$
9. $\mathbb{Z}/6\mathbb{Z} : E(b,c)\ ,\ b = c + c^2, \Delta(b,c) = c^6(c+1)^3(9c+1) \neq 0.$
10. $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} : E(b,c)\ ,\ b = t + t^2, c = (8+2t)/((1-t)^2 - 9),$
    $\Delta(b,c) = t^6(t+1)^3(9t+1) \neq 0.$
11. $\mathbb{Z}/12\mathbb{Z} : E(b,c)\ ,\ b = cd, c = fd - f, d = m + \tau, f = m/(1-\tau),$
    $(m = 3\tau - 3\tau^3 - 1)/(\tau - 1), \Delta(b,c) \neq 0.$
12. $\mathbb{Z}/9\mathbb{Z} : E(b,c)\ ,\ b = cd, c = fd - f, d = f(f-1) + 1, \Delta(b,c) \neq 0.$
13. $\mathbb{Z}/5\mathbb{Z} : E(b,c)\ ,\ b = c, \Delta(b,c) = b^5(b^2 - 11b - 1) \neq 0.$
14. $\mathbb{Z}/10\mathbb{Z} : E(b,c)\ ,\ b = cd, c = fd - f, d = f^2(f - (f-1)^2), f \neq (f-1)^2, \Delta(b,c) \neq 0.$
15. $\mathbb{Z}/7\mathbb{Z} : E(b,c)\ ,\ b = d^3 - d^2, c = d^2 - d, \Delta(b,c) = d^7(d-1)^7(d^3 - 8d^2 + 5d + 1) \neq 0.$

注意 $E(b,c)$ は**テイト正規型 (Tate normal form)** と呼ばれ $(0,0)$ をねじれ部分群の生成元としてもっている.

続いて, 2 つの楕円曲線 $E_1,\ E_2$ が与えられたとき, 同型を少し弱めた同種という概念を定義する. 後の定理 1.5 で見るように, 同種写像は $E_1,\ E_2$ のモーデル・ヴェイユ群の準同

型写像になっている.

定義 E_1, E_2 は楕円曲線であるとする. 有理写像 $\phi : E_1 \longrightarrow E_2$ で $\phi(O) = O$ を満たすものを**同種写像 (Isogeny)** という.
$\phi(E_1) \neq O$ であるような同種写像 $\phi : E_1 \longrightarrow E_2$ が存在するとき, E_1, E_2 は**同種 (Isogenous)** という

例 1.4 $m \in \mathbb{Z}$ に対して,

$$[m] : E \longrightarrow E; P \longmapsto [m]P \quad (m \text{ 倍写像})$$

は同種写像である.

同種写像に関して次のことが成り立つ.

定理 1.5 [Sil, III, 4.8.] $\phi : E_1 \longrightarrow E_2$ を同種写像としたとき次が成り立つ.

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

系 1.6 [Sil, III, 4.9.] $\phi : E_1 \longrightarrow E_2$ を零写像でない同種写像としたとき, $\mathrm{Ker}\ \phi = \phi^{-1}(O)$ は有限群になる.

また, E の関数体 $K(E)$ と同種写像について次のような命題が成り立つ.

定理 1.7 [Sil, III, 4.10.] $\phi : E_1 \longrightarrow E_2$ を零写像でない同種写像とする.

1. すべての $Q \in E_2$ について, $\#\phi^{-1}(Q) = \deg_s \phi$. さらにすべての $P \in E_1$ に対して, $\mathrm{e}_\phi(P) = \deg_i \phi$.
   ただし, ここで $\mathrm{e}_\phi(P)$ は写像 ϕ の点 P における分岐次数である.
2. 写像
   $$\mathrm{Ker}\ \phi \longrightarrow \mathrm{Aut}(K(E_1)/\phi^* K(E_2)); T \longmapsto \tau_T^*$$
   は同型である. ここで τ_T^* は T による平行移動の写像である (つまり

$f \in K(E_1),\ P \in E_1$ に対して $\tau_T^*(f)(P) = f(P+T)$ で定まる写像).

3. ϕ が分離的であると仮定すると, ϕ は不分岐であり, $\#\mathrm{Ker}\ \phi = \deg\ \phi$ かつ $K(E_1)$ は $\phi^* K(E_2)$ 上ガロア拡大である.

命題 1.8 [Sil, III, 4.12.] E を楕円曲線, Φ を E の有限部分群とすると, 楕円曲線 E^* と $\mathrm{Ker}\ \phi = \Phi$ を満たすような同種写像 $\phi : E \longrightarrow E^*$ が同型を除いて一意に存在する.

2 Vélu の公式

1 章の命題 1.8 は, 楕円曲線 E とその有限部分群 Φ が与えられたとき, 同種である楕円曲線 E^* と同種写像 $\phi : E \longrightarrow E^*$ が同型を除いて一意的に定まることを主張しているが, その証明は構成的ではない (証明については [Sil, III, 4.12.] を参照). この章では, E と Φ が与えられた時に, E^* と ϕ の具体的な構成を与える Vélu の公式 [Vél] について佐藤 [佐藤] に基づき証明を与える. その後, フリーの計算ソフトウェア Sage [Sage] 上で Vélu の公式の計算例を紹介する.

2.1 Vélu の公式の証明

体 k 上定義された楕円曲線を次で定義する:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\ (a_i \in k).$$

元 $g^x,\ g^y \in k(E)$ をそれぞれ次のように定める:

$$g^x = 3x^2 + 2a_2x + a_4 - a_1y,\ g^y = -2y - a_1x - a_3.$$

また, E 上の点 $Q \neq O$ に対して $x(Q)$, $y(Q)$, $g^x(Q)$, $g^y(Q)$ をそれぞれ x_Q, y_Q, g^x_Q, g^y_Q と略すことにする.

$$t_Q := \begin{cases} g^x_Q & Q \in E[2] \text{ のとき} \\ 2g^x_Q - a_1 g^y_Q & \text{それ以外の場合} \end{cases}, \quad u_Q := (g^y_Q)^2.$$

注意 楕円曲線の逆元の取り方から,

$$x_{-Q} = x_Q,\ y_{-Q} = g^y_Q + y_Q,\ g^x_{-Q} = g^x_Q - a_1 g^x_Q,\ g^y_{-Q} = -g^y_Q.$$

従って,

$$t_{-Q} = t_Q,\ u_{-Q} = u_Q$$

であることに注意する.

$S \subset \Phi$ を $(\Phi - \{O\})/\{\pm 1\}$ の完全代表系とする.

$$t := \sum_{T \in S} t_T,\ \omega := \sum_{T \in S} (u_T + x_T t_T).$$

上の注意より t, $\omega \in k$ は S の取り方によらない.

ここで,

$$A_1 := a_1,\ A_2 := a_2,\ A_3 := a_3,\ A_4 := a_4 - 5t,\ A_6 := a_6 - (a_1^2 + 4a_2)t - 7\omega$$

とする.

定理 2.1 (Vélu の公式 [Vél]) 楕円曲線 E とその有限部分群 Φ について, $E^* := E/\Phi$ と $\mathrm{Ker}\ \phi = \Phi$ を満たす同種写像 $\phi : E \longrightarrow E^*$ はそれぞれ次で与えられる:

$$E^* : Y^2 + A_1 XY + A_3 Y = X^3 + A_2 X^2 + A_4 X + A_6,$$

$$X = x + \sum_{T \in S} \left(\frac{t_T}{x - x_T} + \frac{u_T}{(x - x_T)^2} \right),$$

$$Y = y - \sum_{T \in S} \left(u_T \frac{2y + a_1 x + a_3}{(x - x_T)^3} + t_T \frac{a_1(x - x_T) + y - y_T}{(x - x_T)^2} + \frac{a_1 u_T - g^x_T g^y_T}{(x - x_T)^2} \right).$$

証明　E のワイエルシュトラス方程式を与えることと, 次の条件を満たす $x,\ y \in k(E)$ を与えることは同値である.

条件

$$\mathrm{ord}_O(x) = -2,\ \mathrm{ord}_O(y) = -3,\ \frac{y^2}{x^3}(O) = 1;$$
$$\mathrm{ord}_Q(x) \geq 0,\ \mathrm{ord}_Q(y) \geq 0 \quad \text{if } Q \in E(\overline{k}) - \{O\}.$$

$z = -\frac{x}{y}$ とすると, $\mathrm{ord}_O(z) = 1$ より, $x,\ y$ を z により, 点 O の近傍でローラン展開する ([Sil, IV] 参照).

$$x = z^{-2} - \alpha_1 z^{-1} - \alpha_2 - \alpha_3 z - -\alpha_4 z^2 - \alpha_5 z^3 - \alpha_5 z^4 - \cdots,$$
$$y = -\frac{x}{z} = -z^{-3} + \alpha_1 z^{-2} + \alpha_2 z^{-1} + \alpha_3 + \alpha_4 z + \alpha_5 z^2 + \cdots.$$

これを E に代入して係数比較をすると,

$$\begin{aligned}
&\alpha_1 = a_1, \quad \alpha_2 = a_2, \quad \alpha_3 = a_3,\\
&\alpha_4 = a_1 a_2 + a_4,\\
&\alpha_5 = a_2 a_3 + a_1^2 a_3 + a_1 a_4,\\
&\alpha_6 = a_1^2 a_4 + a_1^3 a_3 + a_2 a_4 + 2a_1 a_2 a_3 + a_3^2 + a_6.
\end{aligned}$$

よって a_i を α_i によって表すことができる. 以上の議論を E^* に対して用いる. E^* のワイエルシュルトラス方程式を得ることと, 次の条件を満たすような $X,\ Y \in \overline{k}(E)^{\Phi} \bigcap k(E)$ を構成することは同値である.

条件

$$\mathrm{ord}_O(X) = -2,\ \mathrm{ord}_O(Y) = -3,\ \frac{Y^2}{X^3}(O) = 1;$$
$$\mathrm{ord}_Q(X) \geq 0,\ \mathrm{ord}_Q(Y) \geq 0 \quad \text{if } Q \in E(\overline{k}) - \Phi.$$

E^* を X, Y により得られる楕円曲線とすると $\mathrm{ord}_Q(X) \geq 0,\ \mathrm{ord}_Q(Y) \geq 0$ $(Q \in \Phi)$ であることから, $\phi : E \longrightarrow E^*; x \mapsto X,\ y \mapsto Y$ は同種写像で $\mathrm{Ker}\ \phi \subset \Phi$ なことが分かる. 一方で ϕ により引き起こされる関数体の準同型写像 $\phi^* : k(E^*) \longrightarrow k(E)$ の像 $\phi^*(k(E^*))$

について $[k(E):\phi^*(k(E^*))] = \#\mathrm{Ker}\ \phi$, また, X, Y の取り方より, $\phi^*(k(E^*)) \subset k(E)^\Phi$. 以上より $\#\Phi \geq \#\mathrm{Ker}\ \phi$ である. したがって, $\mathrm{Ker}\ \phi = \Phi$ なので E^* が求めたい楕円曲線であることが分かった.

あとは, 上の条件を満たす X, Y を具体的に構成し, E でしたように X の $Z = -\frac{X}{Y}$ による点 O の近傍でのローラン展開について計算をすれば E^* の係数がわかる.

実際, X, $Y \in k(E)$ を次のように取ればよい,

$$X := x + \sum_{T \in \Phi - \{O\}} (x \circ \tau_T - x_T),$$
$$Y := y + \sum_{T \in \Phi - \{O\}} (y \circ \tau_T - y_T).$$

ここで, τ_T は T についての平行移動 (すなわち, $\tau_T(P) = P + T$ である写像) とする. X, Y が条件を満たすことは明らか. これを前の注意で述べた $x_{-Q} = x_Q$, $y_{-Q} = g_Q^y + y_Q$, $g_{-Q} = g_Q^x - a_1 g_Q^y$, $g_{-Q}^y = -g_Q$ の関係式と, 和の公式から次の変形が得られる:

$$x \circ \tau_Q - x_Q = \frac{g_Q^x}{x - x_Q} + \frac{g_Q^y (y - y_Q)}{(x - x_Q)^2},$$
$$y \circ \tau_Q - y_Q = -\frac{a_1 g_Q^x}{x - x_Q} - \frac{(g_Q^x + a_1 g_Q^y)(y - y_Q)}{(x - x_Q)^2} - \frac{g_Q^y (y - y_Q)}{(x - x_Q)^3}.$$

上の関係式を用いれば, X, Y について主張の形が得られる.

主張の X, Y の式の x, y に z でのローラン展開したものを代入すると

$$X = z^{-2} - \alpha_1 z^{-1} - \alpha_2 - \alpha_3 z - (\alpha_4 - t) z^2 - (\alpha_5 - \alpha_1 t) z^3 - (\alpha_6 - \alpha_1^2 t - \alpha_2 t - \omega) z^4 - \cdots,$$
$$Y = -z^{-3} + \alpha_1 z^{-2} + \alpha_2 z^{-1} + \alpha_3 + (\alpha_4 + t) z + \alpha_5 z^2 + (\alpha_6 + \alpha_2 t + 3\omega) z^3 + \cdots.$$

したがって,

$$Z = -\frac{X}{Y} = z + 2tz^5 + 3\alpha_1 t z^6 + (4\alpha_1^2 t + 4\alpha_2 t + 3\omega) z^7 + \cdots.$$

以上が, べき級数の計算によりわかる. これを逆に解いて,

$$z = Z - 2tZ^5 - 3\alpha_1 t Z^6 - (4\alpha_1^2 t + 4\alpha_2 t + 3\omega) Z^7 + \cdots.$$

よって

$$\begin{aligned} X =& Z^{-2} - \alpha_1 Z^{-1} - \alpha_2 - \alpha_3 Z \\ & - (\alpha_4 - 5t)Z^2 - (\alpha_5 - 5\alpha_1 t)Z^3 - (\alpha_6 - 6\alpha_1^2 t - 9\alpha_2 t - 7\omega)Z^4 - \cdots . \end{aligned}$$

これと, E^* について X を Z でローラン展開したものとの係数を比較して,

$$\alpha_1 = \mathrm{A}_1,\ \alpha_2 = \mathrm{A}_2,\ \alpha_3 = \mathrm{A}_3,\ \alpha_4 - 5t = \mathrm{A}_1\mathrm{A}_3 + \mathrm{A}_4,$$
$$\alpha_6 - 6\alpha_1^2 t - 9\alpha_2 t - 7\omega = \mathrm{A}_1^2\mathrm{A}_4 + \mathrm{A}_1^3\mathrm{A}_3 + \mathrm{A}_2\mathrm{A}_4 + 2\mathrm{A}_1\mathrm{A}_2\mathrm{A}_3 + \mathrm{A}_3^2 + \mathrm{A}_6.$$

これを解くことにより, E^* の係数が求めらて, 主張の形になる. □

注意 E 上の不変微分

$$\omega(x, y) = \frac{dx}{-g^y} = \frac{dy}{g^x}$$

と, $G^X := 3X^2 + 2\mathrm{A}_2 X + \mathrm{A}_4 - \mathrm{A}_1 Y,\ G^Y := -2Y - \mathrm{A}_1 X - \mathrm{A}_3$ としたときの E^* 上の不変微分

$$\omega(X, Y) = \frac{dX}{-G^Y} = \frac{dY}{G^X}$$

は一致する ([Sil, IV] 参照).

このことから, 次が成り立つ.

$$G^x = mg^x + n(g^y)^2,\ G^y = mg^y.$$

ここで,

$$m = 1 - \sum_{T \in S} \left(\frac{t_T}{(x - x_T)^2} + \frac{2u_T}{(x - x_T)^3} \right),$$
$$n = \sum_{T \in S} \left(\frac{t_T}{(x - x_T)^3} + \frac{3u_T}{(x - x_T)^4} \right).$$

2.2 同種写像から生じる体の拡大

k は標数が 2 ではない体, l を素数, E を k 上定義された楕円曲線とする. Φ は $E(\overline{k})$ の有限な部分群で $\mathrm{Gal}(\overline{k}/k)$-不変かつ $\#\Phi = l$ であることを仮定する. このとき, 命題 1.8 より定まる楕円曲線を E^*, 同種写像を ϕ とする.

E^* の点 P ($[2]P \neq O$) を k に添加した体と, 同種写像 ϕ による引き戻しの点を k に添加した体をそれぞれ次のように定義する:

$$K := k(P) = k(X_P,\ Y_P),\ K' := k(\phi^{-1}(P)) = k(x_Q,\ y_Q; Q \in \phi^{-1}(P)).$$

ここで X_P, Y_P は点 $P \in E^*(\overline{k})$ の x 座標と y 座標を表す. 同様に x_Q, y_Q は点 $Q \in E(\overline{k})$ の x 座標と y 座標を表す. ϕ は k 上定義されているので $K \subset K'$ が成り立つ.

以下, 点 $Q \in E(\overline{k})$ に対して $g^x(Q),\ g^y(Q),\ m(Q)$ を $g^x_Q,\ g^y_Q,\ m_Q$. 点 $P \in E^*(\overline{k})$ に対して $G^x(P),\ G^y(P)$ を $G^x_P,\ G^y_P$ と略記する.

$$K = k(X_P,\ G^Y_P),\ K' = k(x_Q,\ g^y_Q; Q \in \phi^{-1}(P))$$

と表すことができる.

任意の $Q \in \lambda^{-1}(P)$ に対し,

$$G^Y_P = m_Q g^y_Q.$$

$[2]P \neq O$ (すなわち, $G^Y_P \neq O$) より,

$$m_Q \neq 0,\ g^y_Q = m_Q^{-1} G^Y_P \in k(x_Q, G^Y_P).$$

したがって,

$$K' = K(x_Q; Q \in \phi^{-1}(P)).$$

同種写像の x 座標の有理関数について,

$$\begin{aligned} X &= x + \sum_{T \in S} \left(\frac{t_T}{x - x_T} + \frac{u_T}{(x - x_T)^2} \right) \\ &= x + \sum_{T \in S} \left(\frac{t_T (x - x_T) + u_T}{(x - x_T)^2} \right) \\ &= \frac{I(x)}{J(x)}. \end{aligned}$$

ここで,

$$\begin{aligned} I(x) &:= x \prod_{T \in S} (x - x_T)^2 + \cdots \\ &= x^l - \left(\sum_{T \in \Phi - \{O\}} (x_T) \right) x^{l-1} + \cdots, \\ J(x) &:= \prod_{T \in \Phi - \{O\}} (x - x_T) = x^{l-1} - \left(\sum x_T \right) x^{l-2} + \cdots \end{aligned}$$

という形に書き直せる.

$[k(x) : k(X)] = [k(E) : k(E^*)] = l$ であることから $I(x)$ と $J(x)$ は互いに素なことがわかる.

今, $P \in E^*(\overline{k})$ は $[2]P \neq O$ であるような点がある. 任意の $Q \in \phi^{-1}(P)$ について, ϕ が同種写像なことから, $Q \neq O$ ならば $J(x_Q) \neq 0$ であり,

$$I(x_Q) - X_P J(x_Q) = 0$$

が成り立つ.

$[2]P \neq O$ より,

$$\#\{x_Q; Q \in \phi^{-1}(P)\} = \#\phi^{-1}(P) = l.$$

したがって,

$$I(x) - X_P J(x) = \prod_{Q \in \phi^{-1}(P)} (x - x_Q)$$

であるから, K' は $I(x) - X_P J(x)$ の K 上最小分解体となる.

今後, E^* の方程式を

$$E^* : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \ (A_i \in k)$$

により表し, $\Phi = \langle T_0 \rangle$ $(T_0 \in E(k))$ として議論をする.

E^* の両辺を 4 倍して左辺を Y について平方完成する:

$$(2Y + A_1X + A_3)^2 = 4X^3 + (A_1^2 + 4A2)X^2 + 2(A_1A_3 + 2A_4)X + A_3^2 + 4A_6.$$

右辺を $F(X)$ とおくと

$$(G^Y)^2 = F(X)$$

と変形できる.

$X_P = \xi \in k$ であるような $P \in E^*(\overline{k}) - O$ に対して, $K_\xi = k(\sqrt{F(\xi)})$ とすると, K_ξ は $k(P)$ に一致する.

また, 各 $\xi \in k$ に対し, k 係数の l 次式 $\Lambda_\xi(x)$ を

$$\Lambda_\xi(x) = I(x) - \xi J(x)$$

により定める.

以下, $F(\xi) \neq 0$ かつ $\Lambda_\xi(x)$ が k 上既約を満たす $X_P = \xi \in k$ である $P \in E^*(\overline{k}) - O$ をひとつ固定して, $K = k(P)$ $(= K_\xi)$, $K' = k(\phi^{-1}(P))$ とおく.

定理 2.2 K'/K は l 次巡回拡大.

証明 K' は K 上 $\Lambda_\xi(x)$ の最小分解体であることから, K'/K はガロア拡大である. この証明には次の写像が群に関して単射準同型であることを示せば十分である:

$$\iota : \mathrm{Gal}(K'/K) \longrightarrow \Phi, \ \sigma \longmapsto Q^\sigma - Q \ (\text{ここで } Q \text{ は } \phi^{-1}(P) \text{ の任意の点である. })$$

写像 ι が単射準同型ならば, $\#\Phi = l$ である仮定により $\mathrm{Im}\ \iota$ $(= \mathrm{Gal}(K'/K))$ は $\{O\}$ ま

たは Φ に一致する. しかし, $\Lambda_\xi(x)$ が K 上既約であるという仮定から $\mathrm{Im}\ \iota \neq \{O\}$. したがって, $\mathrm{Gal}(K'/K)$ は位数 l の巡回群である.

よって写像 ι が単射群準同型を示す.

$\phi^{-1}(P)$ 内の任意の点 Q の x 座標は Λ_ξ の解である. y 座標は x 座標により決まるので群 $\mathrm{Gal}(K'/K)$ は $\phi^{-1}(P)$ に推移的に作用する. このことから, 写像 ι は点 Q の取り方によらないことと写像の単射性が導かれる.

準同型性は, $Q^\sigma - Q \in \Phi \subset E(k)$ であり, $k \subset K$ なことを用いて,

$$\begin{aligned} Q^{\sigma\tau} - Q &= (Q^\sigma - Q)^\tau + Q^\tau - Q \\ &= (Q^\sigma - Q) + (Q^\tau - Q) \end{aligned}$$

であるので成り立つ. □

以上により, K'/K は l 次の巡回拡大となる.

2.3 計算機における Vélu の公式の実装と計算例

この節では, Vélu の公式を計算ソフトウェア Sage [Sage] 上に実装するプログラム例を紹介する. 実際の計算は Sage のクラウドサービスである Cocalc を利用して計算している.

まず, 楕円曲線 $y^2 + (1-t)xy - ty = x^3 - tx^2$ とその 5 等分点 $\langle(0,0)\rangle$ に対して, Vélu の公式を用いて, 同種写像とその値域となる楕円曲線を求めてみる.

まず楕円曲線を定義する.

```
sage :  K.⟨t⟩ =FractionField(PolynomialRing(QQ,'t'));
sage :  Et=EllipticCurve([1-t,-t,-t,0,0]);
sage :  P=Et(0,0);
```

Vélu の公式により楕円曲線 E_t の位数 5 のねじれ部分群 $\langle P\rangle$ により決まる同種写像とそ

の値域となる楕円曲線を求めるには上に続けて次のように入力すればよい.

```
sage : a=Et.a_invariants();
sage : a1=a[0];a2=a[1];a3=a[2];a4=a[3];a6=a[4];
sage : F.⟨x,y⟩=FractionField(PolynomialRing(K,'x,y'));
sage : gx(x,y)=3*x^2+2*a2*x+a4-a1*y;
sage : gy(x,y)=-2*y-a1*x-a3;
sage : T=0;W=0;
sage : X=x;Y=y;
sage : for i in range(1,3) :
 ... :      t=2*gx((i*P)[0],(i*P)[1])-a1*gy((i*P)[0],(i*P)[1]);
 ... :      u=(gy((i*P)[0],(i*P)[1]))^2;
 ... :      X=X+t/(x-(i*P)[0])+(gy((i*P)[0],(i*P)[1]))^2/(x-(i*P)[0])^2;
 ... :      Y=Y-(u*(2*y+a1*x+a3)/(x-(i*P)[0])^3+t*(a1*(x-(i*P)[0])+y
      -(i*P)[1])/(x-(i*P)[0])^2+(a1*u-gx((i*P)[0],(i*P)[1])*
      gy((i*P)[0],(i*P)[1]))/(x-(i*P)[0])^2);
 ... :      T=T+t;
 ... :      W=W+(u+(i*P)[0]*t);
```

これにより求めたい同種写像は, 次で得られる.

```
sage : X;
       (t - 1)*t/x + x + ((t - 1)*t - 2*t^2 + t)^2/(t - x)^2 - (2*(t - 1)
       *t^2 + ((t - 1)*t - 2*t^2 + t)*(t - 1) + 2*t^2)/(t - x) + t^2/x^2
sage : Y;
       ((t - 1)*x - y)*(t - 1)*t/x^2 + (t - 1)*t^2/x^2 + y - ((t - 1)*t
        - 2*t^2 + t)^2*((t - 1)*x + t - 2*y)/(t - x)^3 - (2*(t - 1)*t^2
        + ((t - 1)*t - 2*t^2 + t)*(t - 1) + 2*t^2)*((t - x)*(t - 1) - t^2
       + y)/(t - x)^2 + ((t - 1)*x + t - 2*y)*t^2/x^3 + (((t - 1)*t - 2*t^2
        + t)^2*(t - 1) + ((t - 1)*t^2 + t^2)*((t - 1)*t - 2*t^2 + t))/(t - x)^2
```

x 座標について整理をすると, $X = N(x)/D(x)$

ここで,

$$N(x) = x^5 - 2tx^4 + 3t^2(1-t)x^2 + t^3(t-3)x + t^4,\ D(x) = (t-x)^3x^3$$

である.

また, 求めた同種写像の値域となる楕円曲線は,

```
sage : EllipticCurve([a1,a2,a3,a4-5*T,a6-(a1^2+4*a2)*T-7*W]);
      Elliptic Curve defined by y^2 + (-t+1)*x*y + (-t)*y = x^3 + (-t)*x^2
      + (-10*(t-1)*t^2-5*((t-1)*t-2*t^2+t)*(t-1)-5*(t-1)*t-10*t^2)*x +
      (-7*((t-1)*t-2*t^2+t)^2-(2*(t-1)*t^2+((t-1)*t-2*t^2+t)*(t-1)
      +(t-1)*t+2*t^2)*(t^2-6*t+1)-7*(2*(t-1)*t^2+((t-1)*t-2*t^2
      +t)*(t-1)+2*t^2)*t-7*t^2) over Symbolic Ring
```

によって与えられる.

例 2.3 ($\sharp\Phi = 3$) 楕円曲線 $E : y^2 + a_1xy + a_3y = x^3 (a_1, a_2 \in k,\ \ b(a^2 - 27b) \neq 0)$ について, E は $\Phi = \langle(0,0)\rangle$ を $E(k)$ の位数 3 のねじれ部分群にもつ. Vélu の公式を適用すると, 同種写像 $\lambda : E \longrightarrow E^*$ の x 座標 (y 座標は省略する) と, 楕円曲線 E^* は次で与えられる :

$$E^* : Y^2 + a_1XY + a_2Y = X^3 - 5a_1a_2X - a_1^3a_2 - 7a_2^2,$$

$$X = \frac{x^3 + a_1a_2x + a_2^2}{x^2}.$$

例 2.4 ($\sharp\Phi = 7$) 楕円曲線 $E : y^2 + (1 + d - d^2)xy + d^2(d-1)y = x^3 + d^2(d-1)x^2 (d \in k,\ \ d(1-d)(d^3 - 8d^2 + 5d + 1) \neq 0)$ について, E は $\Phi = \langle(0,0)\rangle$ を $E(k)$ の位数 7 のねじれ部分群にもつ. Vélu の公式を適用すると, 同種写像 $\lambda : E \longrightarrow E^*$ の x 座標 (y 座標は省略する) と, 楕円曲線 E^* は次で与えられる :

$$E^* : Y^2 + (1+d-d^2)XY + d^2(d-1)Y$$
$$= X^3 + d^2(d-1)X^2 - 5d(d-1)(d^2-d+1)(d^3+2d^2-5d+1)X$$
$$- d(d-1)(d^9+9d^8-37d^7+70d^6-132d^5+211d^4-182d^3+76d^2-18d+1),$$

$$X = \frac{N(x)}{D(x)}.$$

ここで

$$N(x) = x^7 + 2d(1-d^2)x^6 + d(d-1)(d^5+2d^4-3d^3+5d^2-7d+1)x^5$$
$$- d^3(d-1)^2(6d^4-9d^3+12d^2-13d-1)x^4 + d^4(d-1)^3(d^5+d^4+4d^3-8d^2-7d-1)x^3$$
$$- (d+1)(d-1)^4d^6(3d^2-5d-3)x^2 + 168(d-1)^5d^8(d^2-3d-3)x + (d-1)^6d^{10},$$

$$D(x) = x^2(x-d^2+d)^2(x-d^3+d^2)^2.$$

5 等分点をもつ $\mathbb{Q}$ 上の楕円曲線をひとつ決めて Vélu の公式により同種写像を求め, その x 座標から得られる 5 次方程式を $\Lambda_X(x) = N(x) - XD(x)$ とする. ここで $X \in \mathbb{Q}$ として $\Lambda_X(x)$ が既約のときの最小分解体について, 数値計算の例を見ていく.

例 2.5 ($E : y^2+y = x^3-x^2-10x-20$) 楕円曲線 E の Mordell–Weil 群は $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z}$ であり, 生成元は $P = (5,5)$ である.
Vélu の公式から同種写像とその値域となる楕円曲線 E^* を求めると :

$$E^* : y^2 + y = x^3 - x^2 - 7820x - 263580,$$

$$X = \frac{x^5 - 42x^4 + 2163x^3 - 30420x^2 + 170498x - 324599}{x^4 - 42x^3 + 601x^2 - 3360x + 6400}.$$

x についての 5 次方程式

$$f_X(x) = x^5 - (42+X)x^4 + (2163+42X)x^3 - (30420+601X)x^2 \\ + (170498+3360X)x - 324599 - 6400X$$

の X に $\mathbb{Q}$ の値を代入した多項式の $\mathbb{Q}$ 上の最小分解体を Sage を用いて計算する．
$X = 1$ ($f_1(x) = x^5 - 43x^4 + 2205x^3 - 31021x^2 + 173858x - 330999$) として f_1 の最小分解体 K を計算しその体の $\mathbb{Q}$ 上の拡大次数を求める．

```
sage : R.⟨x⟩=PolynomialRing(QQ)
sage : f = x^5 - 43*x^4 + 2205*x^3 - 31021*x^2 + 173858*x - 330999
sage : K = f.splitting_field('a')
sage : K.absolute_degree()
       10
```

ガロア理論より $\mathbb{Q}$ 上既約な 5 次多項式の最小分解体 K のガロア群 $\mathrm{Gal}(K/\mathbb{Q})$ は 5 次対称群の可移部分群になる．ここで $\mathbb{Q}$ 上拡大次数が 10 であることから $\mathrm{Gal}(K/\mathbb{Q}) \simeq D_5$ がわかる．同じように X に値を代入してガロア群を考える．$X \in \mathbb{Z}$ として $-500 \leq X \leq 500$ の範囲では f_X の最小分解体はすべて $\mathbb{Q}$ 上 D_5 拡大を与えている．

3 Brumer 多項式と Lecacheux 多項式について

2 章では, 特殊化 (パラメーターに値を代入) することで, 一般に最小分解体が $\mathbb{Q}$ 上 D_5 拡大になる多項式が得られた．この章では特殊化により $\mathbb{Q}$ 上すべての D_5 拡大を与えるような多項式が存在し, それが同種写像の x 座標により得られることを紹介していく．この章の同種写像による Brumer 多項式 (3.1 節) と Lecacheux 多項式 (3.2 節) の構成は Lecacheux の論文 [Lec] に基づいている．

3.1 Brumer 多項式の構成

まず, 体 k 上生成的な多項式を次のように定義する.

定義 任意の体 k を基礎体として固定し, G を有限群とする. 基礎体上の m 個の独立変数 $t = (t_1, t_2, \ldots, t_m)$ を取り, $k(t)$ を k 上の m 変数有理関数体とする. 多項式 $F(t_1, t_2, \ldots, t_m; X) \in k(t)[X]$ は以下の条件 (1), (2) を満たすとき, k **上** G **生成的多項式**という :

(1) 多項式 $F(t_1, t_2, \ldots, t_m; X)$ の $k(t)$ 上のガロア群は G と同型であり,

(2) 各無限体 $M \supset k$ とその G-拡大 L/M に対して, L が $F(a; X)$ の M 上の最小分解体になるような $a = (a_1, a_2, \ldots, a_m) \in M^m$ が必ず存在する.

注意 Kemper の定理 [Kem] により, 任意の部分群 $H \subset G$ に対して, M 上すべての H-ガロア拡大は $F(t; X)$ の変数の特殊化 $t \mapsto a$ によって得られることが知られている.

次に, 1 章で紹介していたテイト正規型について, 5 等分点をもつ任意のワイエルシュトラス方程式の形をした楕円曲線がテイト正規型に書き直せることを証明し, テイト正規型の同種写像を考えることによって, k 上生成的な D_5 多項式が得られることを見る.

E を 5 等分点をもつ k 上の楕円曲線として, A を $E[5](k)$ の生成元とする. A の n 倍を $A_n := [n]A$ と表すことにする.
このとき, 次のような関数をとることができる.

$$\begin{aligned} {}^{\exists!}X \in k(E) \text{ s.t. } X(A_1) = X(A_4) &= 1, \\ X(A_2) = X(A_3) &= \infty, \\ X(A_0) &= 0. \end{aligned}$$

すぐにわかるように, 因子は次のようになっている.

$$\mathrm{div}(X) = 2A_0 - A_2 - A_3,\ \mathrm{div}(X - 1) = A_1 + A_4 - A_2 - A_3.$$

また, A による平行移動から定まる関数体 $k(E)$ の同型写像を ϕ とする. すなわち, 任意の点 $M \in E$ と $f \in k(E)$ に関して, $\phi(f)(M) = f(M+A)$ である. ϕ による X の像を $X_i := \phi^i(X)$ と定義しておく.
簡単な計算から, X_i $(0 \leq i \leq 4)$ の因子について次が得られる :

$$\mathrm{div}(X_i) = 2A_{5-i} - A_{2-i} - A_{3-i}, \quad \mathrm{div}(X_i - 1) = A_{1-i} + A_{4-i} - A_{2-i} - A_{3-i}.$$

X_i の因子の等式から $X_i X_{i+2} = k'(1 - X_{i+1})$ $(k' \in k^\times)$ という関係式を得られる. ここで ϕ が位数 5 であることから $k' = 1$ となる.
$\prod_{i=0}^{4} X_i$ は $\mathrm{div}\left(\prod_{i=0}^{4} X_i\right) = 0$ より定数関数であるから $-t := \prod_{i=0}^{4} X_i$ とおく.
$Y := X_1$ として $\phi(Y) = \frac{1-Y}{X}$ であることより

$$\begin{aligned} -t = \prod_{i=0}^{4} X_i &= X_0 X_1 X_2 X_3 X_4 \\ &= X\left(1 - \frac{1-Y}{X}\right)\frac{Y - 1 + \frac{1-Y}{X}}{X}, \\ -tXY &= (X - 1 + Y)(Y-1)(X-1). \end{aligned}$$

ここで, $X = t/x, \quad Y = 1 - tx/y$ とする. この x, y の因子を計算すると, $\mathrm{div}(x) = \mathrm{div}(t/X) = A_2 + A_3 - 2A_0$, $\mathrm{div}(x) = \mathrm{div}(-tx/(Y-1)) = A_1 + 2A_3 - 3A_0$ なことから, ワイエルシュトラス座標になっていることがわかり, 上の式に代入し整理すれば,

$$E_t : y^2 + (1-t)xy - ty = x^3 - tx^2$$

となり, 目標としていたテイト正規型に変形することができた. このとき 5 等分点は $A = (t, 0)$, $2A = (0, 0)$, $3A = (0, t)$, $4A = (t, t^2)$ となっている. $E'_t = E_t/\langle A \rangle$ を求める,

$$X = 2\prod_{i=0}^{4} \phi^i(x-2) = 2\frac{(x-2)(x^2+2tx-1)(2x^2-2tx-2x+t)}{x(x-1)^2},$$

$$\begin{aligned} Y &= 4\prod_{i=0}^{4}\phi^i(x-y) \\ &= 4\,\frac{(tx^2+(2x-1)(x-1)^2)((x+1)t-x^2(x-1))R(x,y)}{x^2(x-1)^3}. \end{aligned}$$

ここで $R(x,y)=tx+(x-1)(x+2(y-1))$.

これは次数 5 の同種写像になっており, E'_t は次のようになっている :

$$\begin{aligned} E'_t : Y^2 &= X^3+25(1+t^2)X^2 \\ &\quad +(208+76t+252t^2-76t^3+208t^4)X+4(1+t^2)(-3t+4)^2(4t+3)^2. \end{aligned}$$

同種写像の x 座標を整理すれば, x についての 5 次方程式が得られ, 次のようになっている:

$$\begin{aligned} x^5+(t-3)x^4+\left(1-\frac{1}{4}X-2t^2-\frac{7}{2}t\right)x^3 \\ +\left(4t+3+5t^2+\frac{1}{2}X\right)x^2+\left(-2t^2-2-\frac{1}{4}X-\frac{5}{2}t\right)x+t. \end{aligned}$$

$s:=-2t^2-2-\frac{1}{4}X-\frac{5}{2}t$ として整理しなおすと,

$$x^5+(t-3)x^4+(s-t+3)x^3+(t^2-t-2s-1)x^2+sx+t.$$

この 5 次多項式は Brumer 多項式と呼ばれ, k 上 D_5 生成多項式であることが知られている. 生成性の証明については, Jensen, Ledet, Yui の書いた生成的多項式の教科書である [JLY] を参照してほしい.

注意 Brumer 多項式は最初 Brumer [Bru] により構成された. その後, 橋本 [Has] により別解釈による再構成と, 生成性の再証明が与えられており, 橋本と角皆 [HT] によりさらに別の幾何学的構成が与えられている.

3.2 Lecacheux 多項式の構成

Lecacheux [Lec] は Brumer 多項式での同種写像の考察をさらに進め, 次で見るような F_{20} 生成的多項式を構成している.

次のような楕円曲線 E_p について考える.

$$E_p : y^2 - \frac{d}{4}(x^2+1) = \frac{1}{2}L(x)L'(x).$$

ここで, $d = p^2+4, L(x) = x^2 - px - 1$. $L'(x)$ は $L(x)$ の x についての微分である.
$t, -1/t$ を L の根として, s を次で定義する.

$$s^2 := \frac{d}{4}(t^2+1) = \frac{d^{3/2}}{4}t$$

このとき, $\mathbb{Q}(s)/\mathbb{Q}(p)$ は 4 次の巡回拡大になり, $\mathrm{Gal}(\mathbb{Q}(s)/\mathbb{Q}(p)) = \langle\lambda\rangle$, λ は $s \mapsto -s/t$ という作用である.

また, E_p は位数 5 の点 $A = (t, s)$ を持ち $\langle A\rangle$ は $\mathrm{Gal}(\mathbb{Q}(s)/\mathbb{Q}(p))$-不変である. それは, E_p が x 座標に対して対称になっており, 点 (t, s) における E_p の接線が E_p と $(-1/t, -s/t)$ と交わること, 点 $(-1/t, -s/t)$ における E_p の接線が E_p と $(t, -s)$ と交わることから確認できる.

続いて, E_p の $\langle A\rangle$ に対する同種写像の x 座標についてみていく. ϕ を A による平行移動で定まる $k(E_p)$ の同型写像とする. すなわち $f \in k(E_p)$, $M \in E_p$ に対して $\phi(f)(M) = f(M+A)$ である. このとき,

$$\sum_{i=0}^{4}\phi^i(x) = x + 2p + d^2\frac{px+2}{L^2} + d\frac{x(p+2)+(p^2-p+6)}{L}$$

となり, $rd + 5p/2 = \sum_{i=0}^{4}\phi^i(x)$ として $l = L/d$ とおくと次の関係式が得られる.

$$l^5 + \left(-r^2d + 2p + \frac{17}{4}\right)l^4 + \left(3rd + p^2 + \frac{13}{2}p + 5\right)l^3 + \left(rd + \frac{11}{2}p - 8\right)l^2 + (p-6)l - 1.$$

これがそのまま F_{20} の生成的多項式いる．生成性については Brumer 多項式と同じく [JLY] を参照してほしい．この多項式を Lecacheux 多項式と呼ぶ.

定理 3.1 (Lecacheux [Lec, Theorem 3.1.]) 標数が 0 の体 k について, 次の多項式は, k 上 F_{20} 生成的多項式である:

$$x^5+\left(-r^2d+2p+\frac{17}{4}\right)x^4+\left(3rd+p^2+\frac{13}{2}p+5\right)x^3+\left(rd+\frac{11}{2}p-8\right)x^2+(p-6)x-1.$$

3.3 多重分解多項式による体の同型の判定

一般の生成的多項式について, 体 $M \supset k$ 上の任意の H-拡大 ($H \subset G$) が k-生成的多項式の変数の特殊化によって得られるという事実から次の問題が自然に生じる：

生成的多項式の部分体問題. $F(t;X)$ を G に対する k k-生成的多項式とする．無限体 $M \supset k$ と $a, b \in M^m$ に対して, 最小分解体 $\mathrm{Spl}_M F(b;X)$ が最小分解体 $\mathrm{Spl}_M F(a;X)$ の部分体となるための必要十分条件を与えよ.

固定した有限群 G に対し, 体 M 上のガロア拡大を考察する場合には, 次の部分体問題の特別な場合を考えれば十分である：

生成的多項式の同型問題. 無限体 $M \supset k$ と $a, b \in M^m$ に対して, $\mathrm{Spl}_M F(a;X)$ と $\mathrm{Spl}_M F(b;X)$ が M 上同型となるための必要十分条件を与えよ.

この同型問題について, D_5, F_{20} については星と三宅 [HM] により, 多重分解多項式を因数分解したときの型を見ることにより, 判定をできることが証明されている．$a, b \in M^m$ と値が与えられたときに, どのようにして判定するのか結果だけを紹介する.

k は標数が 2 でない体とする．Brumer 多項式を

$$f_{s,t}^{D_5}(X) = X^5 + (t-3)X^4 + (s-t+3)X^3 + (t^2-t-2s-1)X^2 + sX + t$$

としておき, $F^1_{\mathbf{s},\mathbf{s}'}(X), F^2_{\mathbf{s},\mathbf{s}'}(X)$ を次で定義する.

$$F^1_{\mathbf{s},\mathbf{s}'}(X) := (G^1_{\mathbf{s},\mathbf{s}'}(X))^2 - \frac{d^2 d'^2}{4}(G^2_{\mathbf{s},\mathbf{s}'}(X))^2 \in k(s,t,s',t')[X],$$
$$F^2_{\mathbf{s},\mathbf{s}'}(X) := F^1_{(\frac{s+5t}{t^2},-\frac{1}{t}),(s',t')}(X).$$

ここで,

$$G^1_{\mathbf{s},\mathbf{s}'}(X) = X^5 - (t-3)(t'-3)X^4 + c_3X^3 + \frac{c_2}{2}X^2 + \frac{c_1}{2}X + \frac{c_0}{2},$$
$$G^2_{\mathbf{s},\mathbf{s}'}(X) = X^2 + (t+t'-1)X + s - t + s' - t' + tt' + 2.$$

$c_3,\ c_2,\ c_1,\ c_0 \in k(s,t,s',t')$ は次で与えられる:

$$\begin{aligned}
c_3 =&[2s - 21t + 3t^2 - 2ts' + t^2s' - t^2t'] + 31 - 3ss' + 5tt',\\
c_2 =&[-20s + 112t + 8st - 32t^2 + 2t^3 + 5ts' - 13sts' - 12t^2s' + 4t^3s' - 15stt' + 14t^2t'\\
&+ 2t^3t' + 8t^2s't' - 2t^3t'^2] - 102 + 27ss' - 119tt' - sts't' + 6t^2t'^2,\\
c_1 =&[32s + 2s^2 - 128t - 26st + 60t^2 + 4st^2 - 8t^3 - 6s^2s' - 7ts' + 38sts' + 9t^2s'\\
&- 5st^2s' - 12t^3s' + 2t^4s' - 20ts'^2 - 8sts'^2 + 6t^2s'^2 + 2t^3s'^2 + 2stt' - 77t^2t'\\
&+ 3st^2t' + 8t^3t' - 29t^2s't' + st^2s't' + 18t^3s't' - 2st^2t'^2 + 10t^3t'^2]\\
&+ 80 - 37ss' + 145tt' - 45sts't' + 24t^2t'^2 - 8t^3t'^3,\\
c_0 =&[-16s - 2s^2 + 56t + 24st + 2s^2t - 38t^2 - 8st^2 + 8t^3 + 5s^2s' - 2ts' - 38sts'\\
&- 7s^2ts' + 5t^2s' + 13st^2s' + 8t^3s' + 2st^3s' - 4t^4s' - 21ts'^2 - 11sts'^2 - 2t^2s'^2\\
&+ 2st^2s'^2 + 4t^3s'^2 - 104stt' - 33s^2tt' + 105t^2t' + 35st^2t' + 4t^3t' + 16st^3t' - 2t^5t'\\
&- s^2ts't' + 36t^2s't' - 14st^2s't' - 6t^3s't' + 6t^4s't'8t^2s'^2t' - 37st^2t'^2 + 22t^3t'^2\\
&+ 8t^4t'^2 + 8t^3s't'^2 - 2t^4t'^3] - 24 + 14ss' - 8s^2s'^2 - 224tt' + sts't' - 101t^2t'^2\\
&- st^2s't'^2 - 8t^3t'^3.
\end{aligned}$$

省略のため, $a \in k(s,t,s',t')$ に対して $[a] := a + \iota(a)$ としている. ι は $\iota(s,t,s't') = (s',t',s,t)$ によって定義されるものとする.

ここで,

$$d^2 = s^2 - 4s^3 + 4t - 14st - 30s^2t - 91t^2 - 34st^2 + s^2t^2 + 40t^3 + 24st^3 + 4t^4 - 4t^5,\quad d'^2 = \iota(d)^2.$$

定理 3.2 (星, 三宅 [HM, Theorem 7.13.]) 標数が 2 ではない体 k 上 $f_{s,t}^{D_5}$ を, $\mathbf{a} = (a_1, a_2), \mathbf{a}' = (a_1', a_2') \in M^2$ で特殊化したときの最小分解体のガロア群をそれぞれ G_{a}, $G_{\mathrm{a}'}$ として $G_{\mathrm{a}} \geq G_{\mathrm{a}'} \geq C_5$ を仮定する.

$f_{s,t}^{D_5}(X)$ の $\mathbf{a} = (a_1, a_2), \mathbf{a}' = (a_1', a_2') \in M^2$ による特殊化で得られる体の共通部分の様子は $F_{\mathbf{a},\mathbf{a}'}^1, F_{\mathbf{a},\mathbf{a}'}^2$ の M 上での因数分解の型により次の表のように分類される:

$G_{\mathbf{a}}$	$G_{\mathbf{a}}'$	$G_{\mathbf{a},\mathbf{a}'}$		$F_{\mathbf{a},\mathbf{a}'}^1$	$F_{\mathbf{a},\mathbf{a}'}^2$
D_5	D_5	$D_5 \times D_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
		$(C_5 \times C_5) \rtimes C_2$	$[L_{\mathbf{a}} \cap L_{\mathbf{a}'} : M] = 2$	5^2	5^2
		D_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5, 2^2, 1$	5^2
		D_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	5^2	$5, 2^2, 1$
	C_5	$D_5 \times C_5$	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
C_5	C_5	$C_5 \times C_5$	$L_{\mathbf{a}} \neq L_{\mathbf{a}'}$	5^2	5^2
		C_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$5, 1^5$	5^2
		C_5	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	5^2	$5, 1^5$

注意 $G_{\mathbf{a}'} = C_2$ であるときは次のようになる:

$G_{\mathbf{a}}$	$G_{\mathbf{a}'}$	$G_{\mathbf{a},\mathbf{a}'}$		$F_{\mathbf{a}}^1$	$F_{\mathbf{a}'}^2$
D_5	C_2	D_{10}	$L_{\mathbf{a}} \not\supset L_{\mathbf{a}'}$	10	10
		D_5	$L_{\mathbf{a}} \supset L_{\mathbf{a}'}$	5^2	5^2
C_5		C_{10}	$L_{\mathbf{a}} \cap L_{\mathbf{a}'} = M$	10	10
C_2		$C_2 \times C_2$	$L_{\mathbf{a}} \neq L_{\mathbf{a}'}$	$4^2, 2$	$4^2, 2$
		C_2	$L_{\mathbf{a}} = L_{\mathbf{a}'}$	$2^4, 1^2$	$2^4, 1^2$

星と三宅の論文 [HM] では, Brumer 多項式の結果を用いることによって, Lecacheux 多項式に対する同型問題を解決している. その手法を紹介する.

まず標数が 2 でないことを仮定する, Lecacheux 多項式を

$$g_{p,r}^{F_{20}}(X) := X^5 + \left(r^2(p^2+4) - 2p - \frac{17}{4}\right)X^4 + \left((p^2+4)(3r+1) + \frac{13}{2}p + 1\right)X^3 - \left(r(p^2+4)X^2 + \frac{11}{2}p - 8\right) + (p-6)X + 1 \in k(p,r)[X]$$

とすると, Brumer 多項式 $f_{s,t}^{D_5}$ を次の変数変換によって, Lecacheux 多項式 $g_{p,r}^{F_{20}}$ に変換できる :

$$s = -\frac{1}{4}(5p + 8r + 2p^2r + (2pr+5)\sqrt{p^2+4}), \quad t = \frac{1}{2}(p + \sqrt{p^2+4}).$$

このとき, 同型問題としては, M 上の 2 次拡大体 $M(\sqrt{p^2+4}) = M(\sqrt{p'^2+4})$ であるような p, p' に対して考えれば十分である. $M(\sqrt{p^2+4})$ 上で上の変数変換と D_5 に関する結果を適用することにより, F_{20} の同型問題が解決される.

3.4 Lecacheux 多項式の同型の判定

D_5 生成多項式, F_{20} 生成的多項式についての同型問題について, 同型な体がどのくらい存在するかということが問題になる.
この問題に対し, ある楕円曲線の有理点によって特殊化された Brumer 多項式については, 木田, 陸名, 佐藤 [KRS] により先行研究がなされている. この節では最初に, その結果の紹介する. その後, Lecacheux 多項式についても同様に楕円曲線の有理点による特殊化を行い, 考察をする.

まずは, 木田, 陸名, 佐藤 [KRS] の結果について紹介するための準備を行う. $d(s,t)$ を次のように定める.

$$d(s,t) := -4s^3 + (t^2 - 30t + 1)s^2 + 2t(3t+1)(4t-7)s - t(4t^4 - 4t^3 - 40t^2 + 91t - 4)$$

それぞれ変数 s, t に対して, Brumer 多項式 $f_{s,t}^{D_5}$ の判別式は $t^2 d(s,t)^2$ である.
このとき, 最小分解体 $\mathrm{Spl}_{\mathbb{Q}(s,t)}(f_{s,t}^{D_5})$ はただひとつの 2 次体を部分体としてもち, それは

$k_{s,t} = \mathbb{Q}(s,t)(\sqrt{d(s,t)})$ である.
与えられた $s,t \in \mathbb{Q}$ による $f_{s,t}^{D_5}$ の最小分解体に対して $f_{\alpha,\beta}^{D_5}$ の最小分解体が同型であれば, その部分体の 2 次体は一致する. したがって, 次の等号を考える :

$$du^2 = d(\alpha, \beta)$$

ここで $d = d(s,t) \in \mathbb{Q}, u$ はある 0 でない有理数としている. さらに,

$$\beta = t,\ (x,y) := (-4d\alpha, 4d^2u),$$

として次の $\mathbb{Q}$ 上定義された楕円曲線が得られる :

$$E_{s,t} : y^2 = x^3 + d(t^2 - 30t + 1)x^2 - 8d^2t(3t+1)(4t-7)x - 16d^3t(4t^4 - 4t^3 - 40t^2 + 91t - 4).$$

楕円曲線 $E_{s,t}$ は次数 5 の同種写像 ϕ を持ちその像の楕円曲線 $E_{s,t}^*$ は次のようになる :

$$\begin{aligned} E_{s,t}^* : y^2 =& x^3 + d(t^2 - 30t + 1)x^2 - 8d^2(26t^4 - 310t^3 + 327t^2 + 315t + 26)x \\ &+ 16d^3(68t^6 - 1120t^5 + 3804t^4 + 1760t^3 + 6929t^2 + 1380t + 68). \end{aligned}$$

また,

$$\phi^* : E_{s,t}^* \to E_{s,t}$$

を ϕ の双対同種写像とする. このとき, アーベル群 $E_{s,t}(\mathbb{Q})/\phi(E_{s,t}^*(\mathbb{Q}))$ は弱 Mordell-Weil 定理から有限になることがわかる.
任意の有理点 $P = (x(P), y(P)) \in E_{s,t}(Q)$ に対して,

$$f_P^{D_5}(X) := f_{\frac{x(P)}{-4d},t}(X)$$

とする.

定理 3.3 (木田, 陸名, 佐藤 [KRS, Theorem 2.1.]) 上の記号のもとで次が成り立つ:

1. 有理点 $P \in E_{s,t}(\mathbb{Q})$ に対して,

Brumer 多項式 $f_P^{D_5}$ が $\mathbb{Q}$ 上可約 $\iff$ $P \in \phi^*(E^*_{s,t}(\mathbb{Q}))$.

2. 有限集合

$$\{E_{s,t}(\mathbb{Q})/\phi^*(E^*_{s,t}) \text{ の位数 } 5 \text{ である部分群 }\},$$

$$\{\mathrm{Spl}_{\mathbb{Q}}(f_P^{D_5}(X)) | P \in E_{s,t}(\mathbb{Q}) \setminus \phi(E^*_{s,t}(\mathbb{Q}))\}$$

の間には $E_{s,t}(Q) \ni P \mapsto f_P^{D_5}$ によって引き起こされる写像により全単射が存在する.

この結果を参考にして, Lecacheux 多項式 $g_{p,r}^{F_{20}}$ でも同様のことが起こるのかについて考察する.

まずは Lecacheux 多項式 $g_{p,r}^{F_{20}}$ に付随する楕円曲線を定義する.

最小分解体 $\mathrm{Spl}_M(g_{p,r}^{F_{20}}(X))$ はただひとつの M 上 4 次巡回拡大を含み, どのような体であるかは星と三宅の論文 [HM] により特定されている.

命題 3.4 (星, 三宅 [HM, Lemma 7.4. (1)])

$$W_{p,r} := 16(p^2+4)r^3 + 4(p^2+4)r^2 - 4(19p+41)r - 16p - 199,$$

$$d^2 = \delta'_{p,r} = W_{p,r}((p^4+5p^2+4) + p(p^2+3)\sqrt{p^2+4})/8$$

とおくと, $G_{p,r} = F_{20}$ であるような $(p,r) \in M^2$ に対して $\mathrm{Spl}_M(g_{p,r}^{F_{20}}(X))$ の M 上巡回 4 次の部分体は $M(d)$ で与えられる.

ここで, 与えられた $(p,r) \in \mathbb{Q}$ に対して, $W = W_{p,r} \in \mathbb{Q}$ とし, $g_{\alpha,\beta}^{F_{20}}$ として, 次の等式を考える :

$$Wu^2 = W_{\alpha,\beta}.$$

$$\alpha = p, \quad (x,y) := (4(p^2+4)W\beta, 2(p^2+4)W^2u)$$

とすれば, 次の $\mathbb{Q}$ 上定義された楕円曲線 $E_{p,r}$ が得られる:

$$E_{p,r} : y^2 = x^3 + (p^2+4)Wx^2 - 4(19p+41)W^2x - 4(p^2+4)^2(16p+199)W^3.$$

任意の有理点 $P=(x(P),y(P))\in E_{p,r}$ について,

$$g_P^{F_{20}}(X):=g_{p,\frac{x(P)}{4(p^2+4)W}}(X)$$

とする. 付随する楕円曲線 $E_{p,r}$ の有理点 P によって特殊化された $g_P^{F_{20}}$ について具体例を見ていく.

例 3.5 $(p=1,r=0)$ $W_{1,0}=-215$ であり, 次の等式を考える:

$$W_{1,0}u^2=W_{1,\beta}.$$

すなわち,

$$-215u^2=16\cdot 5\beta^3+4\cdot 5\beta^2-4\cdot 60\beta-215.$$

両辺に $\dfrac{-4\cdot 43^3}{5}$ を掛けて, $(x,y)=(-4\cdot 43\beta,2\cdot 43^2u)$ とおけば, 次のような楕円曲線が得られる:

$$E:y^2=x^3-43x^2-88752x+13675204.$$

この楕円曲線 E について, Sage を用いてモーデル・ヴェイユ群 $E(\mathbb{Q})$ のランクが 1 を確認でき, 生成元は $(0,3698)$ である.

Lecacheux 多項式 $g_{p,r}^{F_{20}}$ の楕円曲線 E の有理点 Q による特殊化を次で定義する:

$$g_Q^{F_{20}}:=g_{p,\frac{x(Q)}{-4\cdot 43}}^{F_{20}}.$$

$P=(0,3698)$ とおいたとき, $\mathrm{Spl}_{\mathbb{Q}}(g_P^{F_{20}})$ と $\mathrm{Spl}_{\mathbb{Q}}(g_{[2]P}^{F_{20}})$ の同型を前節で紹介した星と三宅の論文 [HM] の手法により判定する. 今, $P=(0,3698)$, $[2]P=(187,-1514)$ であるので, $(p,r)=(1,0)$, $(1,-187/172)$ の組の同型を判定する.

次の変数変換をして, D_5 の結果 (定理 3.2) を用いる:

$$s=-\frac{1}{4}(5p+8r+2p^2r+(2pr+5)\sqrt{p^2+4}),\quad t=\frac{1}{2}(p+\sqrt{p^2+4}).$$

上の変数変換により

$$(p,r)=(1,0)\longmapsto(s,t)=\left(-\frac{5}{4}(1+\sqrt{5}),\frac{1}{2}(1+\sqrt{5})\right),$$

$$(1,-187/172)\longmapsto\left(-\frac{1}{344}(-505+243\sqrt{5}),\frac{1}{2}(1+\sqrt{5})\right)$$

と移る．$\mathbf{a}=\left(-\frac{5}{4}(1+\sqrt{5}),\frac{1}{2}(1+\sqrt{5})\right)$, $\mathbf{a}'=\left(-\frac{1}{344}(-505+243\sqrt{5}),\frac{1}{2}(1+\sqrt{5})\right)$ とおく．

$F^1_{\mathbf{a},\mathbf{a}'}$, $F^2_{\mathbf{a},\mathbf{a}'}$ を計算する:

$$\begin{aligned}F^1_{\mathbf{a},\mathbf{a}'}&=x^{10}+(-15+5\sqrt{5})x^9+\frac{1}{344}(43995-26415\sqrt{5})x^8\\&+\frac{1}{344}(-323525+160370\sqrt{5})x^7+\frac{1}{236672}(1064275175-420155525\sqrt{5})x^6\\&+\frac{1}{236672}(-3086484025+1226945025\sqrt{5})x^5\\&+\frac{1}{20353792}(436559269000+-262070607125\sqrt{5})x^4\\&+\frac{1}{10176896}(-450882725500+127780533375\sqrt{5})x^3\\&+\frac{1}{3500852224}(123052909610000-57038110305125\sqrt{5})x^2\\&+\frac{1}{7001704448}(308379014350625+278214699158125\sqrt{5})x\\&+\frac{1}{28006817792}(4208317720616875+1718103239765625\sqrt{5}),\end{aligned}$$

$$\begin{aligned}F^2_{\mathbf{a},\mathbf{a}'}&=x^{10}-10x^9+\frac{1}{172}(14415-1870\sqrt{5})x^8\\&+\frac{1}{344}(-150975+37400\sqrt{5})x^7+\frac{1}{118336}(251502475-86739950\sqrt{5})x^6\\&+\frac{1}{118336}(-938262450+381877375\sqrt{5})x^5\\&+\frac{1}{20353792}(506821312250-221445470125\sqrt{5})x^4\\&+\frac{1}{10176896}(-593604895125+265599466000\sqrt{5})x^3\end{aligned}$$

$$+\frac{1}{7001704448}(691389470305625-311955319344625\sqrt{5})x^2$$
$$+\frac{1}{7001704448}(-669494991459375+305127753789375\sqrt{5})x$$
$$+\frac{1}{28006817792}(1034660258696875-469097289134375\sqrt{5}).$$

それぞれ, $\mathbb{Q}(\sqrt{5})$ 上で因数分解すると, $F^1_{\mathbf{a},\mathbf{a}'}$ は (5^2) 型, $F^2_{\mathbf{a},\mathbf{a}'}$ は $(1,2^2,5)$ 型に分解する. 実際に $F^2_{\mathbf{a},\mathbf{a}'}$ は $\left(x+\frac{1}{2}\sqrt{p^2+4}\right)$ を一次因子として持つ定理 3.2 より $\mathrm{Spl}_{\mathbb{Q}}(g_P^{F_{20}})$ と $\mathrm{Spl}_{\mathbb{Q}}(g_{[2]P}^{F_{20}})$ は同型である.

同様にして $\mathrm{Spl}_{\mathbb{Q}}(g_P^{F_{20}})$ と楕円曲線 E の有理点 P の n 倍 $(1\leq n\leq 10)$ により得られる拡大 $\mathrm{Spl}_{\mathbb{Q}}(g_{[n]P}^{F_{20}})$ の同型を判定すると, $n=5,10$ を除いてすべて同型になっている.

$n=5,10$ のときは, $\mathrm{Spl}_{\mathbb{Q}}(g_{[n]P}^{F_{20}})$ は $\mathbb{Q}$ 上 4 次体 $\mathbb{Q}\left(\sqrt{-5\cdot 43(5+2\sqrt{5})}\right)$ に一致している.

ここで, E は $\mathbb{Q}(\sqrt{43})$ 上で 5 等分点を持つ. 実際, $\Phi=\langle(258,344\sqrt{43})\rangle$ とすると

$$\Phi=\{(258,344\sqrt{43}),\ (-86,688\sqrt{43}),\ (-86,-688\sqrt{43}),\ (258,-344\sqrt{43}),\ O\}.$$

E, Φ に対して定まる同種写像を ϕ, その値域を E^* とする. このとき,

$$E^*: y^2=x^3-43x^2-384592x-1080341116.$$

Sage でモーデル・ヴェイユ群 $E^*(\mathbb{Q})$ はランク 1 で生成元は $(83248/9,23892778/27)$ を確認できる. $Q=(83248/9,23892778/27)$, ϕ の双対同種写像を ϕ^* とすると,

$$\phi^*(Q)=[-5]P.$$

したがって,

$$[5]P,\ [10]P\in\phi^*(E^*(\mathbb{Q})).$$

3.5　楕円曲線の 2 倍写像を用いた Lecacheux 多項式の同型族の構成

3.3 節のことを踏まえて, 有理点の 2 倍写像を用いて, Lecacheux 多項式について無限族を与えるパラメータを与える.

命題 3.6 (主結果) $\psi(p,r) = a(p,r)/(4dW)$ とする.
ここで

$$\begin{aligned} d :=& p^2+4, \\ a(p,r) :=& 16d^2r^4 + 8d(19p+41)r^2 + 4(32p^3+398p^2+128p+159)r \\ &+ 16p^3+560p^2+1622p+2477, \\ W :=& 16dr^3 + 4dr^2 - 4(19p+41)r - (16p+199). \end{aligned}$$

このとき, Lecacheux 多項式を (p,r) で特殊化したものと $(p,\psi(p,r))$ 特殊化したものは $\mathbb{Q}(p,r)$ 上同じ分解体を与える:

$$\mathrm{Spl}_{\mathbb{Q}(p,r)}(g_{p,r}^{F_{20}}) \equiv \mathrm{Spl}_{\mathbb{Q}(p,r)}(g_{p,\psi(p,r)}^{F_{20}}).$$

証明　上のパラメータの組に対して, 星と三宅 [HM] の手法を用いて計算すると $F^2_{(p,r),(p,\psi(p,r))}$ が常に $\left(x + \dfrac{1+2r}{2}\sqrt{p^2+4} + \dfrac{p-1}{2}\right)$ を持つので上の命題が成り立っている.

これは Sage で次のように入力すれば確認できる.

まず, 付随する楕円曲線を定義して 2 倍公式を求める.

```
sage :K.<p,r>=FractionField(PolynomialRing(QQ,'p,r'));
sage :d=p^2+4;
sage :W=16*d*r^3+4*d*r^2-4*(19*p+41)*r-(16*p+199);
sage :E=EllipticCurve([0,d*W,0,-4*d*(19*p+41)*W^2,-4*(16*p+199)*d^2*W^3]);
sage :b=E.b_invariants()
sage :b2=b[0]; b4=b[1]; b6=b[2]; b8=b[3];
```

```
sage :x=4*d*W*r;
sage :N=x^4-b4*x^2-2*b6*x-b8;
sage :D=4*x^3+b2*x^2+2*b4*x+b6;
sage :f=N/D;f
      16*p^4*r^4 + 128*p^2*r^4 + 152*p^3*r^2 + 128*p^3*r + 328*p^2*r^2
      + 256*r^4 + 16*p^3 + 1592*p^2*r + 608*p*r^2 + 560*p^2 + 512*p*r
      + 1312*r^2 + 1622*p + 6368*r + 2477
```

多重分解多項式 $F^2_{\mathbf{s},\mathbf{s}'}$ を定義する.

```
sage :R.<x>=PolynomialRing(QQ)
sage :s,t,ss,tt=var('s,t,ss,tt')
sage :s=(s1+5*t1)/t1^2; ss=s2; t=-1/t1; tt=t2
sage :c3=(2*s - 21*t + 3*t^2 - 2*t*ss + t^2*ss - t^2*tt) + (2*ss - 21*tt
       + 3*tt^2 - 2*tt*s + tt^2*s - tt^2*t) + 31 - 3*s*ss + 5*t*tt;
sage :c2=(-20*s + 112*t + 8*s*t - 32*t^2 + 2*t^3 + 5*t*ss - 13*s*t*ss
       - 12*t^2*ss + 4*t^3*ss - 15*s*t*tt + 14*t^2*tt + 2*t^3*tt
       + 8*t^2*ss*tt - 2*t^3*tt^2) + (-20*ss + 112*tt + 8*ss*tt - 32*tt^2
       + 2*tt^3 + 5*tt*s - 13*ss*tt*s - 12*tt^2*s + 4*tt^3*s - 15*ss*tt*t
       + 14*tt^2*t + 2*tt^3*t + 8*tt^2*s*t - 2*tt^3*t^2)-102 + 27*s*ss
       - 119*t*tt - s*t*ss*tt + 6*t^2*tt^2;
sage :c1=(32*s + 2*s^2 - 128*t - 26*s*t + 60*t^2 + 4*s*t^2 - 8*t^3
       - 6*s^2*ss - 7*t*ss + 38*s*t*ss + 9*t^2*ss - 5*s*t^2*ss - 12*t^3*ss
       + 2*t^4*ss - 20*t*ss^2 - 8*s*t*ss^2 + 6*t^2*ss^2
       + 2*t^3*ss^2 + 2*s*t*tt - 77*t^2*tt + 3*s*t^2*tt + 8*t^3*tt
       - 29*t^2*ss*tt + s*t^2*ss*tt + 18*t^3*ss*tt - 2*s*t^2*tt^2
       + 10*t^3*tt^2) + (32*ss + 2*ss^2 - 128*tt - 26*ss*tt + 60*tt^2
       + 4*ss*tt^2 - 8*tt^3 - 6*ss^2*s - 7*tt*s + 38*ss*tt*s + 9*tt^2*s
       - 5*ss*tt^2*s - 12*tt^3*s + 2*tt^4*s - 20*tt*s^2 - 8*ss*tt*s^2
       + 6*tt^2*s^2 + 2*tt^3*s^2 + 2*ss*tt*t - 77*tt^2*t + 3*ss*tt^2*t
```

```
       + 8*tt^3*t - 29*tt^2*s*t + ss*tt^2*s*t + 18*tt^3*s*t - 2*ss*tt^2*t^2
       + 10*tt^3*t^2) + 80 - 37*s*ss + 145*t*tt - 45*s*t*ss*tt + 24*t^2*tt^2
       - 8*t^3*tt^3;
sage :c0=(- 16*s - 2*s^2 + 56*t + 24*s*t + 2*s^2*t - 38*t^2 - 8*s*t^2
       + 8*t^3 + 5*s^2*ss - 2*t*ss - 38*s*t*ss - 7*s^2*t*ss + 5*t^2*ss
       + 13*s*t^2*ss + 8*t^3*ss + 2*s*t^3*ss - 4*t^4*ss - 21*t*ss^2
       - 11*s*t*ss^2 - 2*t^2*ss^2 + 2*s*t^2*ss^2 + 4*t^3*ss^2 - 104*s*t*tt
       - 33*s^2*t*tt + 105*t^2*tt + 35*s*t^2*tt + 4*t^3*tt + 16*s*t^3*tt
       - 6*t^4*tt - 2*t^5*tt - s^2*t*ss*tt + 36*t^2*ss*tt - 14*s*t^2*ss*tt
       - 6*t^3*ss*tt + 6*t^4*ss*tt + 8*t^2*ss^2*tt - 37*s*t^2*tt^2
       + 22*t^3*tt^2 - 2*s*t^3*tt^2 + 8*t^4*tt^2 + 8*t^3*ss*tt^2 - 2*t^4*tt^3)
       + (- 16*ss - 2*ss^2 + 56*tt + 24*ss*tt + 2*ss^2*tt - 38*tt^2
       - 8*ss*tt^2 + 8*tt^3 + 5*ss^2*s - 2*tt*s - 38*ss*tt*s - 7*ss^2*tt*s
       + 5*tt^2*s + 13*ss*tt^2*s + 8*tt^3*s + 2*ss*tt^3*s - 4*tt^4*s
       - 21*tt*s^2 - 11*ss*tt*s^2 - 2*tt^2*s^2 + 2*ss*tt^2*s^2 + 4*tt^3*s^2
       - 104*ss*tt*t - 33*ss^2*tt*t + 105*tt^2*t + 35*ss*tt^2*t + 4*tt^3*t
       + 16*ss*tt^3*t - 6*tt^4*t - 2*tt^5*t - ss^2*tt*s*t + 36*tt^2*s*t
       - 14*ss*tt^2*s*t - 6*tt^3*s*t + 6*tt^4*s*t + 8*tt^2*s^2*t
       - 37*ss*tt^2*t^2 + 22*tt^3*t^2 - 2*ss*tt^3*t^2 + 8*tt^4*t^2
       + 8*tt^3*s*t^2 - 2*tt^4*t^3) - 24 + 14*s*ss - 8*s^2*ss^2 - 224*t*tt
       + s*t*ss*tt - 101*t^2*tt^2 - s*t^2*ss*tt^2 - 8*t^3*tt^3;
sage :G1=x^5-(t-3)*(tt-3)*x^4+c3*x^3+c2/2*x^2+c1/2*x+c0/2;
sage :G2=x^2+(t+tt-1)*x+s-t+ss-tt+t*tt+2;
sage :d1=s^2 - 4*s^3 + 4*t - 14*s*t - 30*s^2*t - 91*t^2 - 34*s*t^2
       + s^2*t^2 + 40*t^3 + 24*s*t^3 + 4*t^4 - 4*t^5;
sage :d2=ss^2 - 4*ss^3 + 4*tt - 14*ss*tt - 30*ss^2*tt - 91*tt^2
       - 34*ss*tt^2 + ss^2*tt^2 + 40*tt^3 + 24*ss*tt^3 + 4*tt^4 - 4*tt^5;
sage :f2=G1^2-d1*d2/4*G2^2;
```

$F^2_{(p,r),(p,\psi(p,r))}$ に $-\left(\dfrac{1+2r}{2}\sqrt{p^2+4}+\dfrac{p-1}{2}\right)$ を代入したものを計算してみる.

```
sage :R.<t>=PolynomialRing(K);
sage :L.<a>=K.extension(t^2-d);
sage :RR.<x>=PolynomialRing(L);
sage :s1=-(5*p+8*r+2*p^2*r+(2*p*r+5)*a)/4;
sage :t1=(p+a)/2:
sage :s2=-(5*p+8*f/(4*d*W)+2*p^2*f/(4*d*W)+(2*p*f/(4*d*W)+5)*a)/4;
sage :t2=(p+a)/2;
sage :f2(-((1+2*r)/2*a+1/2*p-1/2))
      0
```

よって, $F^2_{(p,r),(p,\psi(p,r))}$ が $\left(x+\dfrac{1+2r}{2}\sqrt{p^2+4}+\dfrac{p-1}{2}\right)$ を因子として持つことを確認できる. すなわち, 定理 3.2 により最小分解体 $\mathrm{Spl}_{\mathbb{Q}(p,r)}(g^{F_{20}}_{p,r})$ と $\mathrm{Spl}_{\mathbb{Q}(p,r)}(g^{F_{20}}_{p,\psi(p,r)})$ は $\mathbb{Q}(p,r)$ 上同型である. □

今後は, 木田, 陸名, 佐藤 [KRS] の結果の Lecacheux 多項式の場合での証明をつけること. また現在, 楕円曲線を決めるパラメータ p を固定しているが, 異なる場合についてどうなるのかということを研究したいと思っている.

参考文献

[佐藤] 佐藤 篤，Vélu の公式とその応用．以下より入手可能．
http://staff.miyakyo-u.ac.jp/˜taya/sendaiNT/2000/sato.pdf

[Bru] A. Brumer, *The rank of $J_0(N)$*, Astérisque No. 228 (1995), 41–68.

[Has] K. Hashimoto, *On Brumer's family of RM-curves of genus two*, Tohoku Math. J. (2) **52** (2000), 475–488.

[HT] K. Hashimoto, H. Tsunogai, *Generic polynomials over* $\mathbf{Q}$ *with two parameters for the transitive groups of degree five*, Proc. Japan. Acad. Ser. A **79** (2003), 142–145.

[HM] A. Hoshi, K. Miyake, *On the field intersection problem of solvable quintic generic polynomials*, Int. J. Number Theory **6** (2010), 1047–1081.

[JLY] C. Jensen, A. Ledet, N. Yui, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, Cambridge, 2002.

[Kem] G. Kemper, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139–141.

[KRS] M. Kida, Y. Rikuna, A. Sato, *Classifying Brumer's quintic polynomials by weak Mordell–Weil groups*, Int. J. Number Theory **6** (2010), 691–704.

[Kub] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), 193–237.

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

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Second Edition, Graduate Texts in Mathematics 106, Springer-Verlag, Dordrecht, 2009.

[Sage] W. A. Stein et al., *Sage Mathematics Software*, Version 8.4, The Sage Development Team, 2009, http://www.sagemath.org.

[Vél] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.