Genus one fibrations on norm-trace surfaces

高妻 倫太郎 (大分高専)

1 Introduction

代数体上定義された位数 3 の有理点を持つ楕円曲線を, 代数体の 3 次巡回拡大によって特徴づけることが目的である.

位数 3 の有理点を持つ楕円曲線は, 付随する 3-isogeny から定義される Galois cohomology の完全列を見ることによって, 基礎体上の 3 次巡回拡大と関連していることが Descent via isogeny の理論から見て取れる (§2 で述べる). これは, Mordell や Weil の時代に本質的にはすでに知られていた事実である. 本稿ではこの関連性について更なる考察を行い, 位数 3 の有理点を持つ楕円曲線に特有と思われる結果を報告する.

主な記号

F : 代数体
E/F : F 上定義された位数 3 の有理点を持つ楕円曲線
$\phi : E \to \widehat{E}$: 位数 3 の有理点から構成される F 上定義された 3-isogeny ($\widehat{E}$ は E の双対)
$\widehat{\phi} : \widehat{E} \to E$: ϕ の dual isogeny ($\widehat{\phi} \circ \phi = [3]_E$, $\phi \circ \widehat{\phi} = [3]_{\widehat{E}}$, ただし $[3]$ は 3 倍写像)
K/F : 3 次巡回拡大

主結果は, 楕円曲線 E/F の Descent via 3-isogeny に現れる主等質空間 (代数的閉体 $\overline{F}$ 上 E と正則同型な F 上定義された種数 1 曲線) の族が, 3 次巡回拡大に付随する norm と trace により定義される代数曲面の fibration になっている, という事実である. この結果の中核は次の特徴づけにある (§4-5 を参照. K/F は固定しておく):

$$\left\{\begin{array}{l}\text{性質「}{}^{\exists}P \in \widehat{E}(F) \text{ s.t. } F\big(\phi^{-1}(P)\big) = K\text{」}\\ \text{を満たし, 位数 3 の有理点を持つ楕円曲線}\\ E/F \text{ の同型類全体の集合}\end{array}\right\} = \left\{\begin{array}{l}\text{3 次巡回拡大 } K/F \text{ に付随する norm}\\ \text{多様体の平面切断から生ずる楕円曲}\\ \text{線の同型類全体の集合}\end{array}\right\}.$$

この事実自体が特定の楕円曲線に対する特有の視点を与えており, とくに, 右辺に属する楕円曲線の Weierstrass form の中に 3 次巡回拡大 K/F の norm と trace が現れることが発端となって, 表題にある genus one fibration へ導かれる (§4-5).

§2 では, 主結果を具体的に述べるために必要な理論の導入を行い, §3, §4-5 において, それぞれ主結果とそれに至った経緯を説明および証明する. 最後に, 応用例を §6 とする.

2 Descent via 3-isogeny

Descent via 3-isogeny とは, 3-isogeny ϕ および $\widehat{\phi}$ から作られる短完全列の Galois cohomology をとることにより次の連結準同型写像 δ, $\widehat{\delta}$ を得て, その像となる有限群を評価する一種のアル

ゴリズムである:

$$\begin{aligned}
\widehat{\delta} : \frac{E(F)}{\widehat{\phi}(\widehat{E}(F))} &\hookrightarrow H^1(F,\, \widehat{E}[\widehat{\phi}]),\\
\delta : \frac{\widehat{E}(F)}{\phi(E(F))} &\hookrightarrow H^1(F,\, E[\phi]) = \mathrm{Hom}(G_F,\, C_3)\\
&\longrightarrow \{K/F : \text{Galois extension } \mathrm{Gal}(K/F) \subset C_3\};\\
P &\longmapsto F\big(\phi^{-1}(P)\big)/F.
\end{aligned} \tag{1}$$

ここで, $E[\phi] = \mathrm{Ker}\phi$, $\widehat{E}[\widehat{\phi}] = \mathrm{Ker}\widehat{\phi}$, $G_F = \mathrm{Gal}(\overline{F}/F)$, $C_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

δ と $\widehat{\delta}$ の像が計算できれば, 次の公式から E/F の Mordell-Weil 群の階数を得る:

$$\mathrm{rank}_{\mathbb{Z}} E(F) = \dim_{\mathbb{F}_3} \frac{E(F)}{\widehat{\phi}\big(\widehat{E}(F)\big)} + \dim_{\mathbb{F}_3} \frac{\widehat{E}(F)}{\phi\big(E(F)\big)} - \mu. \tag{2}$$

ここで,

$$\mu = \begin{cases} 2 & (\zeta_3 \in F \text{ のとき}),\\ 1 & (\zeta_3 \notin F \text{ のとき}). \end{cases}$$

上記に現れる Galois cohomology 群は, E/F の主等質空間の正則同型類の各々を有限群 $E[\phi]$ (resp. $\widehat{E}[\widehat{\phi}]$) に関する同値関係で細分した群

$$H^1(F,\, E[\phi]) \simeq \left\{ \text{同型類}\{C/F,\, \theta\} \;\middle|\; \begin{array}{l} C/F \text{ は } E/F \text{ の主等質空間},\\ \theta : C \to E \text{ は } \overline{F} \text{ 上定義された正則同型写像で}\\ \theta^{\sigma} \circ \theta^{-1} \in E[\phi] \ \big({}^{\forall}\sigma \in \mathrm{Gal}(\overline{F}/F)\big) \text{ を満たす} \end{array} \right\}$$

と解釈される $\big(\text{resp. } H^1(F,\, \widehat{E}[\widehat{\phi}])$ についても同様$\big)$. 本質は次の同値にある:

$$\text{主等質空間 } C/F \text{ について } C(F) \neq \emptyset \iff \{C/F,\, \theta\} \text{ が連結準同型の像に含まれる}. \tag{3}$$

したがって Mordell-Weil 群の階数を決定するためには, 主等質空間 C/F 上の有理点の有無を調べればよい (主等質空間自体は具体的なモデルをとることが可能). この考え方が Descent via 3-isogeny の理論である.

3 Norm-trace 曲面

基礎体を固定して考えるとき, その 3 次巡回拡大体の族は affine 直線 $\mathbb{A}^1$ によりパラメトライズされることはよく知られている. したがって, 前節 (1) に現れる集合

$$\{K/F : \text{Galois extension } \mathrm{Gal}(K/F) \subset C_3\} = \{K/F : 3 \text{ 次巡回拡大}\} \cup \{F\}$$

は $\mathbb{A}^1$ でパラメトライズされる. このことから, (1) における Galois cohomology 群 $H^1(F,\, E[\phi])$ は, 大雑把に言って, $\mathbb{A}^1$ でパラメトライズされた (楕円曲線 E/F の $E[\phi]$ に付随する) 主等質空間の同型類の集合 (以下では $\{C_t/F,\, \theta\}$ を略して $\{C_t/F\}$ と書く)

$$\big\{\{C_t/F\} \;\big|\; t \in \mathbb{A}^1(F)\big\}$$

と同一視される．主等質空間の同型類 $\{C_t/F\}$ が群 $H^1(F,\, E[\phi])$ の単位元になるような $t \in \mathbb{A}^1(F)$ 全体の集合を U とおくと (この同型類は (1) の自明な元 F に対応する), 同値性 (3) から, とくに次の同値が成り立つ:

$$C_t(F) \neq \emptyset \text{ となるような } t \in \mathbb{A}^1(F) \setminus U \text{ が存在する} \iff \dim_{\mathbb{F}_3} \frac{\widehat{E}(F)}{\phi\big(E(F)\big)} > 0$$

(右辺は §2 の階数公式に現れる)．ここで, 曲線族 $\{C_t\}_{t\in\mathbb{A}^1}$ をある曲面 S の $\mathbb{A}^1$ 上の fibration $\pi : S \to \mathbb{A}^1$ とみなせることに着目すると, 次のように言い換えることができる:

$$S \text{ の部分多様体 } S_0 := \pi^{-1}\big(\mathbb{A}^1(F) \setminus U\big) \text{ に対して } S_0(F) \neq \emptyset \iff \dim_{\mathbb{F}_3} \frac{\widehat{E}(F)}{\phi\big(E(F)\big)} > 0. \quad (4)$$

$S \setminus S_0$ は, t が U 上を動いたときの fibre C_t の和 $\pi^{-1}(U)$ である．証明は §5 で述べるが, 位数 3 の有理点を持つ一般の楕円曲線に関し, 次が示される．

Lemma 3.1. $E(F)[\phi] = \langle T\rangle$, $\widehat{E}(F)[\widehat{\phi}] = \langle \widehat{T}\rangle$ に対して ($\widehat{T} = \mathcal{O}$ の場合も許す),

$$T = 3^r T',\ \widehat{T} = 3^{\widehat{r}}\widehat{T}'$$

(ただし, r, $\widehat{r}$ は非負整数, $T' \in E(F)$, $\widehat{T}' \in \widehat{E}(F)$ は 3 等分不可能, $\widehat{T} = \mathcal{O}$ の場合には $\widehat{T}' = \mathcal{O}$) と既約化しておく．このとき条件「$T' \notin \widehat{\phi}\big(\widehat{E}(F)\big)$ かつ $\widehat{T}' \in \phi\big(E(F)\big)$」は

$$\dim_{\mathbb{F}_3} \frac{\widehat{E}(F)}{\phi\big(E(F)\big)} > 0 \implies \operatorname{rank}_{\mathbb{Z}} E(F) > 0$$

が一般に成立するための必要十分条件である．

上の条件「…」は具体的に計算判定可能であり, 性質 (4) と合わせて次が言える:

$$\text{条件「}T' \notin \widehat{\phi}\big(\widehat{E}(F)\big) \text{ かつ } \widehat{T}' \in \phi\big(E(F)\big)\text{」の下, } S_0(F) \neq \emptyset \implies \operatorname{rank}_{\mathbb{Z}} E(F) > 0. \quad (5)$$

このとき, 楕円曲線 E/F の階数が 0 か正かを判定する上で, 次のような考えが挙げられる:

> 曲線族が与えられたとき, 各々の曲線上で有理点の有無を判定するよりも, それらを束ねた曲面上で判定する方が見通しがよい場合もあるのではないか？

そのように考える理由は次である:

> ある曲面 S から affine 直線 $\mathbb{A}^1$ への fibration $\pi : S \to \mathbb{A}^1$ に関して, 各 fibre において Hasse の原理は一般に成り立たないが S 上では成り立つ, という場合がある．このような場合, S 上の有理点の存在を有限回のステップで判定することができる (具体例としては, S が 3 次巡回拡大体の norm で定義される多様体, π を適当な fibration とすれば, fibre は種数 1 曲線であり, norm 多様体 S 上では Hasse の原理が成立する)．

Colliot-Thélène, Skorobogatov, Swinnerton-Dyer は論文 [1] および [2] において, genus one fibration を持つ曲面に対して Hasse の原理が成り立つための十分条件を, 代数多様体の Brauer 群 (および類体論) を用いた Brauer-Manin obstruction と呼ばれる手法を用いて調べている．論文中に明記はされていないが, おそらく上の考えも想定範囲内にあったのではないかと感じられる．

次に, 主結果を述べるためにいくつか準備を行う．

Shanks 型 C_3 生成的多項式

$$g(x;t) = x^3 + tx^2 - (t+3)x + 1 \in F(t)[x].$$

$g(x;t) = 0$ の $F(t)$ 上の最小分解体を K_t, 3 つの根をそれぞれ α_1, α_2, α_3 とおく. このとき, $\mathrm{Tr}_{K_t/F(t)}(\alpha_i) = -t$, $\mathrm{N}_{K_t/F(t)}(\alpha_i) = -1$ $(i = 1, 2, 3)$, $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = -(t+3)$. また,

$$U := \left\{ \frac{s^3 - 3s + 1}{s - s^2} \;\middle|\; s \in F \right\}$$

とおくと, $t \in U \Leftrightarrow K_t = F$.

位数 3 の有理点を持つ楕円曲線

位数 3 の有理点を点 $(0, 0)$ に平行移動して整理することにより, 次の Weierstrass form に変形可能:

$$E_{A,B} : y^2 + Axy + By = x^3 \ \big(A,\, B \in F \text{ s.t. } \Delta := (A^3 - 27B)B^3 \neq 0\big).$$

Norm-trace 曲面

A, $B \in F$ に対して, 2 つの方程式

$$\mathrm{Tr}_{K_t/F(t)}(x + y\alpha_1 + z\alpha_2) = Aw,\ \mathrm{N}_{K_t/F(t)}(x + y\alpha_1 + z\alpha_2) = -Bw^3 \tag{6}$$

により定義される $\mathbb{P}^3 \times_F \mathbb{A}^1$ 内の曲面を, 本稿では norm-trace 曲面と呼び, $S_{A,B}$ で表すことにする. このとき $([x, y, z, w], t) \in \mathbb{P}^3 \times_F \mathbb{A}^1$ と考える. 具体的に計算すると次の式になる (x を消去して 1 つの定義方程式に纏めることによって $\mathbb{P}^2 \times_F \mathbb{A}^1$ 内の曲面としている):

$$\begin{aligned} S_{A,B} : {} & (A^3 + 27B)w^3 - 3Aw(9 + 3t + t^2)(y^2 - yz + z^2) \\ & - (9 + 3t + t^2)\big((3 + 2t)y^3 - 3(-3 + t)y^2z - 3(6 + t)yz^2 + (3 + 2t)z^3\big) = 0. \end{aligned}$$

以上の準備の下, 次が成り立つ.

Theorem 3.2. 楕円曲線 $E_{A,B}/F$ に対して, norm-trace 曲面 $S_{A,B}/F$ は性質 (4), (5) を持つ. また, fibration $\pi : S_{A,B} \to \mathbb{A}^1; ([x, y, z, w], t) \mapsto t$ について, 次が成り立つ:

$$\begin{aligned} &{}^{\forall}\{C/F\} \in H^1(F, E_{A,B}[\phi]) \text{ に対し}, {}^{\exists}t \in \mathbb{A}^1(F) \text{ s.t. } C \simeq \pi_t, \\ &{}^{\forall}t \in \mathbb{A}^1(F) \text{ に対し}, {}^{\exists}\{C/F\} \in H^1(F, E_{A,B}[\phi]) \text{ s.t. } C \simeq \pi_t. \end{aligned}$$

ここで π_t は fibre $\pi^{-1}(t)$ を表す. とくに次が成立.

$$\begin{aligned} \{K/F\} \in \mathrm{Im}\,\delta \ (K \neq F) &\iff {}^{\exists}\alpha \in K \text{ s.t. } \mathrm{Tr}_{K/F}(\alpha) = A,\ \mathrm{N}_{K/F}(\alpha) = -B \\ &\iff E_{A,B}(F) \simeq \{\alpha \in K_t \mid \mathrm{Tr}_{K_t/F}(\alpha) = A,\ \mathrm{N}_{K_t/F}(\alpha) = -B\}. \end{aligned}$$

この定理は, 本稿冒頭の目的にあるように, 位数 3 の有理点を持つ楕円曲線と 3 次巡回拡大体の関連性を具体的に記述している. 定義方程式 (6) の形から, 位数 3 の有理点を持つ楕円曲線に関係する問題を 3 次巡回拡大体の言葉で書き表すことができる (具体例は §6 参照). また, 前頁で触れた「$S_{A,B}$ に対して Hasse の原理が成り立つための条件」, 「$S_{A,B}$ および各 fibre π_t のそれぞれに対する Hasse の原理の関係」等の考察については今後の課題である.

上の定理の証明自体は容易になされるが, この形に辿り着くまでの過程にいくつかの結果を含んでいるので, その流れを報告することを次節以降の目的としたい.

4 Norm-trace 曲面が現れた背景

一般に, 主等質空間 C/F (のモデル) は cocycle 類 $\{\xi\} \in H^1(F,\, E[\phi])$ が具体的に与えられれば計算できるが, 仮にそれらを束ねて適当な fibration $\{C_t/F\}_{t\in\mathbb{A}^1}$ を構成しても norm-trace 曲面は現れない. 本節ではどのようにして norm-trace 曲面が現れたのか, その背景を説明する.

$\mathcal{X}$ を 3 次巡回拡大 $K_t/F(t)$ の norm から定義される, $\mathbb{P}^3$ 内の射影曲面 (以下 norm 多様体と呼ぶ)

$$\mathrm{N}_{K_t/F(t)}(x + y\alpha_1 + z\alpha_2) = w^3$$

とする. ここで (簡単のため) α_1, α_2 は Shanks 型生成的多項式の根の 2 つとする (実際のところ, 以下の議論は基底 $\{1,\, \alpha_1,\, \alpha_2\}$ の選び方に依存しない). $\mathcal{X}$ は $\mathbb{P}^2$ と K_t 上双有理同値な, $F(t)$ 上定義された特異曲面である. 次に

$$\mathcal{E}(\mathcal{X}) := \left\{ \begin{array}{l} \mathcal{X} \text{ の平面 } h \in \check{\mathbb{P}}^3\big(F(t)\big) \text{ による切断から生じる楕円曲線 } \mathcal{X}_h/F(t) \\ \text{の同型類全体の集合 (平面 } h \text{ を動かす)} \end{array} \right\}$$

とし, $\mathcal{E}_{K_t/F(t)}$ を次の 2 条件 (P) を満たす楕円曲線 $E/F(t)$ の同型類全体の集合とする:

(P1) E は $F(t)$ 上定義された位数 3 の有理点 T を持つ.

(P2) $F(t)\big(\phi^{-1}(P)\big) = K_t$ を満たす有理点 $P \in \widehat{E}\big(F(t)\big) \setminus \{\mathcal{O}\}$ が存在する. (ここで, $\phi : E \to \widehat{E} := E/\langle T\rangle$.)

このとき, norm-trace 曲面 $S_{A,\,B}$ は以下を証明する段階を経て現れた. ここで, i)–iv) については特殊化 $t \in F$ を行った場合においても成立する.

i) $\mathcal{E}(\mathcal{X}) \subset \mathcal{E}_{K_t/F(t)}$.

ii) 3 次曲線 $\mathcal{X}_h$ の Weierstrass form の計算.
$\left(\begin{array}{l} \text{結果: } y^2 + \mathrm{Tr}_{K_t/F(t)}(\gamma_h)xy - \mathrm{N}_{K_t/F(t)}(\gamma_h)y = x^3 \ (^{\exists}\gamma_h \in K_t^*), \text{ ここで} \\ \text{平面 } h \text{ を } \check{\mathbb{P}}^3\big(F(t)\big) \text{ の中で走らせると, } \gamma_h \text{ は } K_t^* \text{ の中をくまなく動く.} \end{array} \right)$

iii) $\mathcal{E}(\mathcal{X}) \supset \mathcal{E}_{K_t/F(t)}$ (i.e. $\mathcal{E}(\mathcal{X}) = \mathcal{E}_{K_t/F(t)}$).

iv) 有理点 $P \in \mathcal{X}_{w\neq 0}\big(F(t)\big)$ および P を通る平面 $h \in \check{\mathbb{P}}^3\big(F(t)\big)$ を固定したとき, 集合 $\mathcal{H}_{h,P} := \{P \text{ を通る平面 } h' \in \check{\mathbb{P}}^3\big(F(t)\big) \mid \mathcal{X}_h \text{ と } \mathcal{X}_{h'} \text{ は } F(t) \text{ 上正則同型 } \}$ の特徴づけ. (結果: $\zeta_3 \notin F$ ならば, $\mathcal{H}_{h,P}$ と $\mathcal{X}_h\big(F(t)\big)$ は集合として 1 対 1 対応である.)

v) 位数 3 の有理点を持つ任意の楕円曲線 $E_{A,\,B}$ に対して

$$\{K/F\} \in \mathrm{Im}\,\delta \iff {}^{\exists}\alpha \in K \text{ s.t. } \mathrm{Tr}_{K/F}(\alpha) = A,\ \mathrm{N}_{K/F}(\alpha) = -B.$$

i) と ii) は論文 [6], iii) と iv) は論文 [5] で証明. v) は (1) における連結準同型 δ の定義を踏まえ, ii) と iii) (の証明) から即座に示される.

v) の結果から, 3 次巡回拡大 K/F を自由に動かす (すなわち生成的多項式のパラメータ t を自由に動かす) と fibration を持つ曲面が出来上がり, それが $S_{A,\,B}$ の定義方程式 (6) になる. とくに, iv) と v) の結果は次のようにまとめることができる.

vi) fibration $\pi : S_{A,\,B} \to \mathbb{A}^1;\, ([x,\, y,\, z,\, w],\, t) \mapsto t$ について

$$\left\{ \begin{array}{l} \text{fibre } \pi_t \text{ は } F \text{ 上定義された種数 1 曲線で, } E_{A,\,B} \text{ と } \overline{F} \text{ 上正則同型.} \\ \pi_t(F) \neq \emptyset \iff \{K_t/F\} \in \mathrm{Im}\,\delta. \end{array} \right.$$

この結果は, Theorem 3.2 の特別な場合として解釈できる. (つまり, $H^1(F, E_{A,B}[\phi])$ を, その部分群 $\operatorname{Im}\delta$ に制限すると得られる.)

次の節では, i), ii), iii), iv) および, vi) を拡張した Theorem 3.2 の説明および証明について述べる.

5 証明

$\mathrm{Gal}\big(K_t/F(t)\big) = \langle\sigma\rangle$ とおく.

5.1 i) の証明

Lemma 5.1. $\mathcal{E}_{K_t/F(t)}$ の定義における 2 条件 (P) は次の条件 (P′) と同値である.

(P′) $\mathrm{Tr}_{K_t/F(t)}(Q) = 3Q$ を満たす有理点 $Q \in E(K_t) \setminus \{Q^\sigma, Q^{\sigma^2}\}$ が存在する.

Proof. まず, (P) ならば (P′) を示す. (P2) より, $Q \in \phi^{-1}(P)$ に対して $Q^\sigma \neq Q$ かつ $\phi(Q^\sigma - Q) = P^\sigma - P = \mathcal{O}$ となるので, $Q^\sigma - Q \in E[\phi] \setminus \{\mathcal{O}\}$ である. ここで (P1) より $E[\phi] = \langle T\rangle \subset E\big(F(t)\big)$ なので, 有理点 $Q^\sigma - Q$ は $\mathrm{Gal}\big(K_t/F(t)\big)$-不変, つまり $(Q^\sigma - Q)^\sigma = Q^\sigma - Q$ となる. この等式から (P′) を得る.

次に, (P′) ならば (P) を示す. $T := Q^\sigma - Q$ とおくと, $3T = (3Q)^\sigma - 3Q = \mathcal{O}$ より, $T \in E[3]$. さらに $\mathrm{Tr}_{K_t/F(t)}(Q) = 3Q\,(= 3Q^\sigma = 3Q^{\sigma^2})$ より, $Q^{\sigma^2} - Q^\sigma = Q^\sigma - Q$. これはすなわち $T^\sigma = T$ を意味する. よって, T は $F(t)$ 上定義された位数 3 の有理点である. これより (P1) が従う. $\phi : E \to \widehat{E} = E/\langle T\rangle$ とすると, $\phi(T) = \phi(Q)^\sigma - \phi(Q) = \mathcal{O}$ となるので, $\phi(Q) \in \widehat{E}\big(F(t)\big)$. $P := \phi(Q)$ とおけばこれは (P2) を満たす. □

Proposition 5.2. D を次の方程式で K_t 上定義される, norm 多様体 $\mathcal{X}$ の因子とする:

$$w = 0,\ x + y\alpha_1 + z\alpha_2 = 0.$$

このとき任意の楕円曲線 $\{\mathcal{X}_h/F(t)\} \in \mathcal{E}(\mathcal{X})$ に対して, $Q := D \cap h$ とおくと, $Q \in \mathcal{X}_h$ は条件 (P′) を満たす.

Proof. 今, 平面 h は $F(t)$ 上定義されているから, $Q = D \cap h$ は K_t 上定義された $\mathcal{X}_h (= \mathcal{X} \cap h)$ の有理点である. また, D の定義方程式より, Q, Q^σ, $Q^{\sigma^2} \in \mathcal{X}_h(K_t)$ は互いに異なる有理点となる. $\mathcal{X}$ の定義方程式を使って有理点 Q, Q^σ, Q^{σ^2} における局所環の uniformizer をそれぞれ計算することにより, 次がわかる:

$$\mathrm{div}\frac{x + y\alpha_1 + z\alpha_2}{w} = 3(Q) - \{(Q) + (Q^\sigma) + (Q^{\sigma^2})\}.$$

さらに, $\mathcal{X}_h$ と $\mathrm{Cl}^0(\mathcal{X}_h)$ は $F(t)$ 上で同型なので, $\mathrm{Tr}_{K_t/F(t)}(Q) = 3Q$ を得る. □

したがって, Lemma 5.1, 5.2 より, i) $\mathcal{E}(\mathcal{X}) \subset \mathcal{E}_{K_t/F(t)}$ が得られた.

Remark 5.3. 事実として Lemma 5.1, Proposition 5.2 は特殊化 $t \in F$ を行っても成立する. (その際 Q^σ などについてはまず t を不定元とし $K_t/F(t)$ の Galois 群を Q に作用させておいた上で, 特殊化 $t \in F$ を行うものと解釈する. 特殊化しても Q, Q^σ, Q^{σ^2} は互いに異なる有理点となることを注意しておく.) 証明の詳細はここでは省略する.

i) は, 平面切断から得られる楕円曲線 $\mathcal{X}_h/F$ が 2 条件 (P) を性質として持つことを主張している. とくに, 特殊化 $t \in F$ を行うと後者の条件 (P2) は次のように言い換えることができる.

K_t/F が 3 次巡回拡大のとき

$(\dim_{\mathbb{F}_3} \mathrm{Im}\,\delta =) \dim_{\mathbb{F}_3} \dfrac{\widehat{E}(F)}{\phi\big(E(F)\big)} > 0$. (公式 (2) に見られるように左辺は楕円曲線の階数に関係する不変量である.)

$K_t = F$ のとき

$E(F) \setminus E(F)[\phi] \neq \emptyset$, すなわち, E/F は位数 3 の有理点の他に非自明な有理点を持つ.

Remark 5.4. $\mathcal{X}$ 上の特異因子は D, D^σ, D^{σ^2} の 3 つである. Proposition 5.2 は, 条件 (P′) あるいは (P) を満たす有理点が norm 多様体の特異因子の平面切断から生ずることを意味している.

5.2 ii) の証明

3 次曲線の定義方程式が与えられたとき, 具体的に有理点が少なくともひとつ求められればそれを基点として Weierstrass form に変形することができる. まず任意の 3 次巡回拡大 $K_t/F(t)$ に対して, それに付随する norm 多様体 $\mathcal{X}$ は有理点 $O := [1,\, 0,\, 0,\, 1]$ を持つことに着目する. 次の補題は, 任意の同型類 $\{\mathcal{X}_h/F(t)\} \in \mathcal{E}(\mathcal{X})$ の中から, O を有理点として持つ楕円曲線 $\mathcal{X}_{h_0}/F(t)$ を選ぶことができるということを主張する. (論文 [6] で既に証明されていることだが, 証明に使われることを後で再利用するので書いておく.)

Lemma 5.5. 任意の $\{\mathcal{X}_h/F(t)\} \in \mathcal{E}(\mathcal{X})$ に対して

$$^{\exists} h_0 \in \check{\mathbb{P}}^3\big(F(t)\big) \text{ s.t. } \mathcal{X}_h \text{ と } \mathcal{X}_{h_0} \text{ は } F(t) \text{ 上正則同型かつ } O \in \mathcal{X}_{h_0}\big(F(t)\big).$$

Proof. norm 多様体の affine 部分 $\mathcal{X}_{w\neq 0} := \mathcal{X} \cap \{w \neq 0\}$ は O を単位元とする線形代数群である. よって, 任意の点 $P \in \mathcal{X}_{w\neq 0}(\overline{F(t)})$ による左移動 $\mathcal{X}_{w\neq 0}(\overline{F(t)}) \to \mathcal{X}_{w\neq 0}(\overline{F(t)}); Q \mapsto P \cdot Q$ は, 付随する正則表現 ρ を引き起こし, その具体的な像は次のようになる:

$$\begin{aligned} \rho : \mathcal{X}_{w\neq 0}(\overline{F(t)}) &\longrightarrow \mathrm{PGL}_3(\overline{F(t)}); \\ [x,\, y,\, z,\, 1] &\longmapsto \begin{pmatrix} x & 2y - z & -y + (t+2)z & 0 \\ y & x - (t+1)y & z & 0 \\ z & -y + z & x + y - tz & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

表現 ρ により, 代数群 $\mathcal{X}_{w\neq 0}$ は集合 $\mathcal{X}(\overline{F(t)})$ へ線形に作用する:

$$\begin{aligned} \mathcal{X}_{w\neq 0}(\overline{F(t)}) \times \mathcal{X}(\overline{F(t)}) &\longrightarrow \mathcal{X}(\overline{F(t)}); \\ (P,\, [x,\, y,\, z,\, w]) &\longmapsto [x,\, y,\, z,\, w] \cdot \rho(P). \end{aligned}$$

以下 ρ を使って題意を示す. $\mathcal{X}_h/F$ は楕円曲線であるから, $F(t)$ 上定義されたある有理点 P を持つ. このとき $\mathcal{X}/F(t)$ の定義方程式より, $P \in \mathcal{X}_{w\neq 0}\big(F(t)\big)$ である. 線形代数群 $\mathcal{X}_{w\neq 0}\big(F(t)\big)$

における P の逆元 P^{-1} をとり, $\rho(P^{-1})$ を考えるとこれは $\mathrm{PGL}_4\big(F(t)\big)$ の元なので, $h_0 := \rho(P^{-1})(h) \in \check{\mathbb{P}}^3\big(F(t)\big)$ であり, さらに定義より $\rho(P^{-1})(\mathcal{X}) = \mathcal{X}$. 以上より, 写像

$$\rho(P^{-1}) : \mathcal{X}_h \longrightarrow \mathcal{X}_{h_0}$$

は $F(t)$ 上定義された正則同型. また, $O = P^{-1} \cdot P \in h_0$ なので $O \in \mathcal{X}_{h_0}\big(F(t)\big)$ も言える. □

上の補題により, O を有理点として持つ楕円曲線 $\mathcal{X}_h/F(t)$ のみを考えればよいことがわかる. $O \in h$ を満たす平面 $h \in \check{\mathbb{P}}^3\big(F(t)\big)$ の定義方程式は

$$a(x-w) + by + cz = 0,\ [a,\, b,\, c,\, -a] \in \check{\mathbb{P}}^3\big(F(t)\big)$$

と書ける. 以下, このような平面のみを取り扱うこととする.

Proposition 5.6. 楕円曲線 $\mathcal{X}_h/F$ の Weierstrass form は次で与えられる:

$$\mathcal{X}_h : y^2 + \mathrm{Tr}_{K_t/F(t)}(\gamma_h)xy - \mathrm{N}_{K_t/F(t)}(\gamma_h)y = x^3.$$

ここで,

$$\gamma_h := \begin{vmatrix} 1 & \alpha_1 & \alpha_2 \\ 1 & \alpha_1^\sigma & \alpha_2^\sigma \\ a & b & c \end{vmatrix} \in K_t^*,\ h : a(x-w) + by + cz = 0,\, [a,\, b,\, c,\, -a] \in \check{\mathbb{P}}^3\big(F(t)\big).$$

Proof. 3 次巡回拡大の生成的多項式 (ここでは §3 の Shanks 型) を用いて, たとえば Cassels の本 [4] にあるような方法で計算することができる. この際, 有理点 $O \in \mathcal{X}_h\big(F(t)\big)$ を基点に用いるというところが要点となる. 主張の形に計算・整理するのは長々として結構面倒である. 詳しくは, 論文 [6] を参照のこと. □

Remark 5.7. γ_h を展開すると, ある $\beta \in K_t$ が存在して

$$\gamma_h = a + b\beta + c\beta^\sigma,\ F(t)(\beta) = K_t$$

と書ける. これより, 任意の $\alpha \in K_t^*$ に対して

$$^\exists h \in \check{\mathbb{P}}^3\big(F(t)\big) \text{ s.t. } \gamma_h = \alpha$$

となる. これは, 任意の $\alpha \in K_t^*$ に対して

$$y^2 + \mathrm{Tr}_{K_t/F(t)}(\alpha)xy - \mathrm{N}_{K_t/F(t)}(\alpha)y = x^3$$

で定義される曲線 E_α が, norm 多様体の平面切断から生ずることを意味している. とくに E_α が楕円曲線となる場合 (非特異の場合) に制限すると

$$\mathcal{E}(\mathcal{X}) = \{\text{ 楕円曲線 } E_\alpha \text{ の同型類 } \mid \alpha \in K_t^*\}$$

が成り立つ.

5.3 iii) の証明

任意の $\{E/F(t)\} \in \mathcal{E}_{K_t/F(t)}$ に対して, 楕円曲線 $E/F(t)$ は条件 (P1) を満たすので次の形の Weierstrass form を持つ:

$$y^2 + Axy + By = x^3 \ \big(A,\, B \in F(t)\big).$$

$\{E/F(t)\} \in \mathcal{E}(\mathcal{X})$ を示すには, 次を満たす $h = [a,\, b,\, c,\, -a] \in \check{\mathbb{P}}^3\big(F(t)\big)$ の存在を言えば十分である:

$$\mathrm{Tr}_{K_t/F(t)}(\gamma_h) = A,\ \mathrm{N}_{K_t/F(t)}(\gamma_h) = -B.$$

以下, 条件 (P2) を使ってこのような $a,\, b,\, c \in F(t)$ を具体的に構成する.

まず, 論文 [5, III-§3] より, 3-isogeny $\phi : E \to \widehat{E} = E/\langle(0,\, 0)\rangle$ は

$$(x,\, y) \ \longmapsto \ \left(\frac{x^3 + B(Ax+b)}{x^2},\, \frac{x^3(y+4B) - B(Ax+B)^2 + By(y-B)}{x^3}\right)$$

と表すことができ, $\widehat{E}$ の Weierstrass form は

$$y^2 + Axy - 9By = x^3 - (A^3 + 27B)B$$

で与えられる. すると, 条件 (P2) は次の条件と同等である:

$$\begin{aligned}&{}^{\exists}P = (u,\, v) \in \widehat{E}\big(F(t)\big) \text{ s.t.}\\ &\quad\begin{cases}\dfrac{x^3 + B(Ax+B)}{x^2} = u,\ \dfrac{x^3(y+4B) - B(Ax+B)^2 + By(y-B)}{x^3} = v\\ \text{の根 } x,\, y \text{ は } F(t) \text{ 上 } K_t \text{ を生成する } \big(\text{i.e. } F(t)(x,\, y) = F(t)(x) = K_t\big).\end{cases}\end{aligned}$$

そこで α を根 x のひとつとする. このとき $F(t)(\alpha) = K_t$ である. (もし $x \in F(t)$ とすると, y の最小多項式の次数が 2 となり, $F(t)(x,\, y) = K_t$ とならないので矛盾.) 多少面倒な計算を経て, 根 x のうち, α と異なる根

$$\frac{2A^2B + u(-3B+v)}{Au - 9B + 2v} + \frac{A^3B + 27B^2 - 10Bv + v^2 + Au(-4B+v)}{B(Au - 9B + 2v)}\alpha + \frac{3AB - u^2}{B(Au - 9B + 2v)}\alpha^2$$

を見つけることができる. ここで, この根が α^σ と等しくなるように $\mathrm{Gal}\big(K_t/F(t)\big)$ の生成元 σ を選ぶ. そして $\{1,\, \alpha,\, \alpha^2\}$ を K_t の $F(t)$-基底とする (これらは具体的な計算を行うためにする). このとき

$$a = \frac{A}{B(Au - 9B + 2v)},\ b = -\frac{3}{Au - 9B + 2v},\ c = -\frac{u}{Au - 9B + 2v}$$

とすると

$$\mathrm{Tr}_{K_t/F(t)}(\gamma_h) = A,\ \gamma_h = B/\alpha$$

が成り立つことを具体的な計算により示すことができる. したがって, α の最小多項式の定数項 $-\mathrm{N}_{K_t/F(t)}(\alpha) = B^2$ から $\mathrm{N}_{K_t/F(t)}(\gamma_h) = -B$ がわかり, それゆえ E と $\mathcal{X}_h$ の Weierstrass form が一致するので, $\{E/F(t)\} \in \mathcal{E}(\mathcal{X})$ を得る.

5.4 iv) の証明

平面 $h,\ h' \in \check{\mathbb{P}}^3\big(F(t)\big)$ (ただしこれらは $O\,(=[1,\,0,\,0,\,1])$ を通るものとする) に対し, Proposition 5.6 により, 楕円曲線 $\mathcal{X}_h/F(t)$ および $\mathcal{X}_{h'}/F(t)$ の Weierstrass form はそれぞれ次の形になる:

$$y^2 + \mathrm{Tr}_{K_t/F(t)}(\gamma_h)xy - \mathrm{N}_{K_t/F(t)}(\gamma_h)y = x^3,$$
$$y^2 + \mathrm{Tr}_{K_t/F(t)}(\gamma_{h'})xy - \mathrm{N}_{K_t/F(t)}(\gamma_{h'})y = x^3.$$

このとき平面 h を固定すると式の形から

$$\begin{matrix}{}^{\exists}h' \in \check{\mathbb{P}}^3\big(F(t)\big), \\ {}^{\exists}k \in F(t)^*\end{matrix} \ \text{s.t.}\ \begin{cases}\mathrm{Tr}_{K_t/F(t)}(\gamma_{h'}) = \mathrm{Tr}_{K_t/F(t)}(\gamma_h)k, \\ \mathrm{N}_{K_t/F(t)}(\gamma_{h'}) = \mathrm{N}_{K_t/F(t)}(\gamma_h)k^3\end{cases} \Longrightarrow \mathcal{X}_h \text{ と } \mathcal{X}_{h'} \text{ は } F(t) \text{ 上正則同型}$$

が成り立つ. 以下では, この命題の十分条件を満たすような平面 $h' \in \check{\mathbb{P}}^3\big(F(t)\big)$ の集合が Mordell-Weil 群 $\mathcal{X}_h\big(F(t)\big)$ と 1 対 1 対応であることを示し, さらに $\zeta_3 \notin F$ を仮定すると逆が成立することを証明する.

ここでは, 平面を動かして考えるので, $h = [a,\,b,\,c,\,-a] \in \check{\mathbb{P}}^3\big(F(t)\big)$ に対して, 便宜上次のようにおく:

$$\mathrm{T}(a,\,b,\,c) := \mathrm{Tr}_{K_t/F(t)}(\gamma_h),\ \mathrm{N}(a,\,b,\,c) := \mathrm{N}_{K_t/F(t)}(\gamma_h).$$

これらは $F(t)$ 上定義された不定元 $a,\,b,\,c$ に関する多項式とみなせる.

また, 写像 ρ を次のようにして集合 $\mathcal{X}(\overline{F(t)})$ 上に拡張しておく (これはもはや準同型でない):

$$\begin{aligned}\tilde{\rho} : \mathcal{X}(\overline{F(t)}) &\longrightarrow \mathrm{PGL}_4(\overline{F(t)}); \\ [x,\,y,\,z,\,w] &\longmapsto \begin{pmatrix} x & 2y-z & -y+(t+2)z & 0 \\ y & x-(t+1)y & z & 0 \\ z & -y+z & x+y-tz & 0 \\ 0 & 0 & 0 & w \end{pmatrix}.\end{aligned}$$

Lemma 5.8. 任意の有理点 $P \in \mathcal{X}(\overline{F(t)})$, $[a,\,b,\,c,\,d] \in \mathbb{P}^3\big(F(t)\big)$ に対して, $[a',\,b',\,c',\,d'] := [a,\,b,\,c,\,d]\cdot\tilde{\rho}(P)$ とおく. このとき次の等式が成り立つ:

$$\mathrm{N}(a',\,b',\,c')d^3 = \mathrm{N}(a,\,b,\,c){d'}^3.$$

また, 任意の平面 $h = [a,\,b,\,c,-a] \in \check{\mathbb{P}}^3\big(F(t)\big)$, 有理点 $P \in \mathcal{X}_h(\overline{F(t)})$ および元 $d \in F(t)$ に対して $[a',\,b',\,c',\,d'] := [a,\,b,\,c,\,d]\cdot\tilde{\rho}(P)$ とおくと次の等式が成り立つ:

$$\mathrm{T}(a',\,b',\,c')d = \mathrm{T}(a,\,b,\,c)d'.$$

Proof. 写像 $\tilde{\rho}$ に対する $[x,\,y,\,z,\,w]$ の像として現れる行列を $\tilde{M}(x,\,y,\,z,\,w)$ とし, さらに

$$f(x,\,y,\,z,\,w) := \mathrm{N}_{K_t/F(t)}(x + y\alpha_1 + z\alpha_2) \in F(t)[x,\,y,\,z,\,w]$$

とおく. すると $(a',\,b',\,c',\,d') := (a,\,b,\,c,\,d)\cdot\tilde{M}(x,\,y,\,z,\,w)$ に対し, 不定元 $a,\,b,\,c,\,x,\,y,\,z$ の多項式として

$$\mathrm{N}(a',\,b',\,c') = \mathrm{N}(a,\,b,\,c)f(x,\,y,\,z,\,w)$$

となることが容易に計算される (生成的多項式を用いる). ここで $P=[x,\,y,\,z,\,w]\in\mathcal{X}$ とすると, $\mathcal{X}$ の定義方程式から $f(P)=w^3$ であり, 今 $d'=dw$ なので,

$$\mathrm{N}(a',\,b',\,c')d^3=\mathrm{N}(a,\,b,\,c)f(P)d^3=\mathrm{N}(a,\,b,\,c)(dw)^3=\mathrm{N}(a,\,b,\,c)d'^3.$$

したがって最初の主張が証明された.

また後半の主張については, $P=[x,\,y,\,z,\,w]\in\mathcal{X}$ とし, $[a',\,b',\,c',\,d']:=[a,\,b,\,c,\,d]\cdot\tilde{\rho}(P)$ を計算すると

$$^{\exists}k\in\overline{F(t)}^{*}\ \text{s.t.}\ \begin{cases}a'k=ax+by+cz,\\ d'k=dw\end{cases}$$

となる. さらに $h=[a,\,b,\,c,-a]$, $P\in\mathcal{X}_h$ のときには, $a'k=ax+by+cz=aw$, $d'k=dw$ より $a'd=ad'$ なので,

$$\mathrm{T}(a',\,b',\,c')d=-a'(t^2+3t+9)d=-a(t^2+3t+9)d'=\mathrm{T}(a,\,b,\,c)d'.$$

(最初と最後の等式は具体的な計算により得られる. 詳細は省略する.) □

Remark 5.9. 上の補題より, とくに $a,\,b,\,c$に関する多項式 $\mathrm{N}(a,\,b,\,c)$ は線形代数群 $\mathcal{X}_{w\neq0}/F(t)$ の不変式であることがわかる (群作用は Lemma 5.5 の証明における正則表現 ρ により与えるものとする). すなわち, 正則表現 ρ の像として現れる行列の第 4 行と第 4 列を除いた成分により作られる 3 次正方行列を $M(x,\,y,\,z)$ とすると次が成り立つ:

$$\mathrm{N}\big((a,\,b,\,c)\cdot M(x,\,y,\,z)\big)=\mathrm{N}(a,\,b,\,c),\ ^{\forall}P=[x,\,y,\,z,\,1]\in\mathcal{X}_{w\neq0}.$$

Proposition 5.10. 任意の平面 $h=[a,\,b,\,c,\,-a]\in\check{\mathbb{P}}^3(\overline{F(t)})$ に対して, $\mathcal{C}_h$ を次の方程式で定義される 3 次射影曲線とする:

$$\mathrm{T}(x,\,y,\,z)=\mathrm{T}(a,\,b,\,c)w,\ \mathrm{N}(x,\,y,\,z)=\mathrm{N}(a,\,b,\,c)w^3,\ \big([x,\,y,\,z,\,w]\in\mathbb{P}^3\big).$$

このとき, 3 次曲線 $\mathcal{C}_h/F(t,\,h)$ は楕円曲線 $\mathcal{X}_h/F(t,\,h)$ と $F(t,\,h)$ 上で正則同型.

Proof. Lemma 5.8 より次の正則写像が定義される:

$$\begin{aligned}\xi:\mathcal{X}_h\ &\longrightarrow\ \mathcal{C}_h;\\ P=[x,\,y,\,z,\,w]\ &\longmapsto\ [a,\,b,\,c,\,1]\cdot\tilde{\rho}(P).\end{aligned}$$

さらに次の写像は ξ の逆写像である:

$$\begin{aligned}\eta:\mathcal{C}_h\ &\longrightarrow\ \mathcal{X}_h;\\ [a',\,b',\,c',\,d']\ &\longmapsto\ [x,\,y,\,z,\,w].\end{aligned}$$

ここで

$$
\begin{aligned}
x &= -\frac{t^2+3t+9}{\mathrm{N}(a,\,b,\,c)}\Big((2t+3)a^2a' - b^2(a'+ta'+b') + bc\big((t^2+t-1)a' + 2c' + t(b'+c')\big)\\
&\qquad + c^2\big((t-1)a' + b' + c'\big) - a\big(b(t^2a' + 2b' + t(3a'+b') + c') + c(3ta' + b' + 2c')\big)\Big),\\
y &= -\frac{t^2+3t+9}{\mathrm{N}(a,\,b,\,c)}\Big(- b^2a' + c^2(a'-b') + bc(ta'+c') + a^2\big((t+2)b' + c'\big)\\
&\qquad - a\big(b((t+2)a' - b') + c(a' + tb' + c')\big)\Big),\\
z &= -\frac{t^2+3t+9}{\mathrm{N}(a,\,b,\,c)}\Big(c^2a' + bc\big((t+2)a' + b'\big) - b^2c' + a^2(b' + 2c')\\
&\qquad - a\big(c(2a' + b' + c') + b(a' + c' + tc')\big)\Big),\\
w &= d'.
\end{aligned}
$$

事実として, $[x,\,y,\,z,\,w]$ は連立 1 次方程式 $[a',\,b',\,c',\,d'] = [a,\,b,\,c,\,1]\cdot\tilde{\rho}\big([x,\,y,\,z,\,w]\big)$ の唯一の解なので, η は正則写像である. 構成の仕方から ξ および η は双有理写像であるので証了. □

以下で, iv) の証明を行う. まず Lemma 5.5 より, $P = O \in \mathcal{X}_h\big(F(t)\big)$ としても一般性は失われない. P を通る任意の平面 $h = [a,\,b,\,c,\,-a] \in \check{\mathbb{P}}^3\big(F(t)\big)$ に対して, Proposition 5.10 より, 写像

$$
\begin{aligned}
\mathcal{C}_{h,\,w\neq 0} &\longrightarrow \mathcal{H}_{h,O};\\
[a',\,b',\,c',\,1] &\longmapsto [a',\,b',\,c',\,-a']
\end{aligned}
$$

は単射. 以下, これが全射であることを示す. 任意の平面 $h' = [a',\,b',\,c',\,-a'] \in \mathcal{H}_{h,O}$ に対して $F(t)$ 上定義された正則同型

$$\iota : \mathcal{X}_h \longrightarrow \mathcal{X}_{h'}$$

が存在する. ここで $\iota(O) = O$ を満たすと仮定してよい (必要であれば適当な有理点で移動すればよい). ι はとくに群同型写像である. 次に楕円曲線 $\mathcal{X}_h$, $\mathcal{X}_{h'}$ の Weierstrass form への変形のうち, 単位元を固定するような変形をそれぞれ $\vartheta : \mathcal{X}_h \xrightarrow{\sim} \mathcal{W}(\mathcal{X}_h)$, $\vartheta' : \mathcal{X}_{h'} \xrightarrow{\sim} \mathcal{W}(\mathcal{X}_{h'})$ とおく. ここで Proposition 5.6 より

$$
\begin{aligned}
\mathcal{W}(\mathcal{X}_h) &: y^2 + \mathrm{T}(a,\,b,\,c)xy - \mathrm{N}(a,\,b,\,c)y = x^3,\\
\mathcal{W}(\mathcal{X}_{h'}) &: y^2 + \mathrm{T}(a',\,b',\,c')xy - \mathrm{N}(a',\,b',\,c')y = x^3
\end{aligned}
$$

である. すると合成写像

$$\vartheta' \circ \iota \circ \vartheta^{-1} : \mathcal{W}(\mathcal{X}_h) \longrightarrow \mathcal{W}(\mathcal{X}_{h'})$$

は F 上定義された群同型写像である (なぜならば, この写像は単位元を単位元にうつす). これは Weierstrass form を保つ群同型写像となるので, 具体的に次の形で書ける ([7, III-§1]):

$$(x,\,y) \longmapsto (u^2x + r,\,u^3y + u^2sx + q).$$

ここで $u,\,r,\,s,\,q \in F(t)$, $u \neq 0$ である. このとき, $\mathcal{W}(\mathcal{X}_h)$ の位数 3 の有理点 $(0,\,0)$, $\big(0,\,\mathrm{N}(a,\,b,\,c)\big)$ をうつすと

$$
\begin{aligned}
(0,\,0) &\longmapsto (r,\,q),\\
\big(0,\,\mathrm{N}(a,\,b,\,c)\big) &\longmapsto \big(r,\,u^3\mathrm{N}(a,\,b,\,c) + q\big)
\end{aligned}
$$

となる. 今 $\zeta_3 \notin F$ なので, Weil pairing の性質より $\mathcal{W}(\mathcal{X}_{h'})\big(F(t)\big)[3] = \langle (0,\,0) \rangle$. したがって, 点 $(0,\,0)$ の像は $(0,\,0)$, $\big(0,\,\mathrm{N}(a',\,b',\,c')\big) = -(0,\,0)$ のいずれかであるから, 同型写像 $\vartheta' \circ \iota \circ \vartheta^{-1}$ を適当に ± 1 倍して $(r,\,q) = (0,\,0)$ となるようにできる. このとき $s = 0$ が成り立ち ([7, III-§1]), 結局

$$\mathrm{T}(a',\,b',\,c') = u\mathrm{T}(a,\,b,\,c),\ \mathrm{N}(a',\,b',\,c') = u^3\mathrm{N}(a,\,b,\,c)$$

であることがわかる. これはすなわち $[a',\,b',\,c',\,u] \in \mathcal{C}_{h,\,w\neq 0}$ を意味する.

5.5 Lemma 3.1 と Theorem 3.2 の証明

Proof of Lemma 3.1. $E(F)[\phi] = \langle T \rangle$, $T = 3^r T'$ (T' は 3 等分不可能) に対して

$$T' \in \widehat{\phi}\big(\widehat{E}(F)\big) \iff {}^{\exists}T'' \in \widehat{E}(F) \text{ s.t. } \begin{cases} \widehat{\phi}(T'') = T', \\ T'' \notin \phi\big(E(F)\big) \end{cases} \implies \dim_{\mathbb{F}_3} \frac{\widehat{\mathrm{E}}(\mathrm{F})}{\phi\big(\mathrm{E}(\mathrm{F})\big)} > 0,$$

$$T' \notin \widehat{\phi}\big(\widehat{E}(F)\big) \implies \dim_{\mathbb{F}_3} \frac{E(F)}{\widehat{\phi}\big(\widehat{E}(F)\big)} > 0.$$

$\widehat{E}(F)[\widehat{\phi}]$ についても同様な主張が言える. ここで条件「$T' \notin \widehat{\phi}\big(\widehat{E}(F)\big)$ かつ $\widehat{T}' \in \phi\big(E(F)\big)$」を仮定すれば

$$\zeta_3 \in F \implies \dim_{\mathbb{F}_3} \frac{E(F)}{\widehat{\phi}\big(\widehat{E}(F)\big)} > 1,$$

$$\zeta_3 \notin F \implies \dim_{\mathbb{F}_3} \frac{E(F)}{\widehat{\phi}\big(\widehat{E}(F)\big)} > 0$$

となる. よって階数公式 (2) より

$$\dim_{\mathbb{F}_3} \frac{\widehat{E}(F)}{\phi\big(E(F)\big)} > 0 \implies \mathrm{rank}_{\mathbb{Z}} E(F) > 0$$

がわかる. □

Proof of Theorem 3.2. まず $A,\,B \in F$ に対し, 次の方程式で定義される 3 次射影曲線を $C_{A,\,B}$ とおく:

$$x + y + z = Aw,\ xyz = Bw^3.$$

z を消去して $xy(Aw - x - y) = Bw^3$. 変換 $(x,\,y) = \left(\frac{y'}{B},\,w',\,-\frac{x'}{B}\right)$ を施すと $y'^2 + Ax'y' + By' = x'^3$, すなわち楕円曲線 $E_{A,\,B}$ と F 上双正則同型である. このとき任意の $t \in \mathbb{A}^1(F)$ に対して, 次の K_t 上の双正則写像が存在する:

$$\begin{aligned} \theta_t : \pi_t &\longrightarrow C_{A,\,B}; \\ [x,\,y,\,z,\,w] &\longmapsto [x,\,y,\,z,\,w] \cdot M_t. \end{aligned}$$

ここで

$$M_t := \begin{pmatrix} 1 & 1 & 1 & 0 \\ \alpha_1 & \alpha_2 & \alpha_3 & 0 \\ \alpha_2 & \alpha_3 & \alpha_1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

具体的な計算により, cocycle $\{\sigma \mapsto \theta_t^{\sigma}\theta_t^{-1}\}$ は $H^1(F,\, E_{A,\,B}[\phi])$ の元で, 連結準同型 (1) を介して $\{K_t/F\}$ にうつることがわかる. 任意の $\{K_t/F\}$ に対し, 上のようにして対応する cocycle を構成できるので, $H^1(F,\, E[\phi])$ の元は $\{\pi_t/F\}_{t\in\mathbb{A}^1(F)}$ の同値類からなることが言える. また, 以上より, 性質 (4), (5), および定理の後半の主張も容易に従う. □

6 Knight's problem

$$n = (a+b+c)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right)\ (a,\, b,\, c \in \mathbb{Q}) \tag{7}$$

の形に書くことができる整数 n はどのような整数か？

この問題に対して, 任意に整数 $n \in \mathbb{Z}$ が与えられたとき, n を上の形に書くことができるかどうかの判定法について考える. $n \notin \{0,\, 1,\, 9,\, 10\}$ のとき, Bremner, Guy, Nowakowski は次の対応により, 問題が楕円曲線の問題に書き換えられることに着目した (論文 [3]):

$$\{[a,\, b,\, c] \in \mathbb{P}^2(\mathbb{Q}) \mid (a,\, b,\, c) \text{ は等式 (7) を満たす}\} \overset{\theta}{\longleftrightarrow} E_n(\mathbb{Q}) \setminus E_n(\mathbb{Q})[6]\,;$$

$$[a,\, b,\, c] \longmapsto \left(-\frac{(a+c)(b+c)}{c^2},\, \frac{a(a+c)(b+c)^2}{bc^3}\right),$$

$$\left[-\frac{(x+1)y}{x^2+y},\, -\frac{x(x+1)}{x-y},\, 1\right] \longmapsto (x,\, y).$$

ここで E_n は Weierstrass form

$$E_n : y^2 + (n-3)xy + (n-1)y = x^3 \ \left(\Delta = n^2(n-1)^3(n-9) \neq 0\right)$$

で $\mathbb{Q}$ 上定義される, 位数 3 の有理点を持つ楕円曲線である.

楕円曲線 $E_n : y^2 + (n-3)xy + (n-1)y = x^3$ について, $n \notin \{0,\, 1,\, 9,\, 10\}$ のとき, 次が成立.

- $\mathrm{rank}E_n(\mathbb{Q}) = 0$ ならば, n は (7) の形に書くことができない.
- $\mathrm{rank}E_n(\mathbb{Q}) > 0$ ならば, n は (7) の形に書くことが可能.

Proposition 6.1. $\widehat{E_n}(\mathbb{Q})[3] = \{\mathcal{O}\}$ と仮定する. このとき次が成り立つ:

$$\begin{array}{l}{}^{\exists}3 \text{ 次巡回体 } K/\mathbb{Q}, \\ {}^{\exists}\alpha \in K\end{array} \text{ s.t. } \begin{cases}\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = n-3, \\ \mathrm{N}_{K/\mathbb{Q}}(\alpha) = n-1\end{cases} \implies \text{整数 } n \text{ を (7) の形に書くことが可能.}$$

Proof. $\widehat{E_n}(\mathbb{Q})[3] = \{\mathcal{O}\}$ より, Lemma 3.1 の条件「…」が満たされる. すなわち, $\widehat{T}' = \mathcal{O} \in \phi\big(E(\mathbb{Q})\big)$ かつ $T' \notin \widehat{\phi}\big(\widehat{E}(\mathbb{Q})\big)$ が成り立つ (後者はそうでないと仮定すると $\widehat{E_n}(\mathbb{Q})[3]$ が非自明な有理点を持ってしまい, 矛盾). このとき

$${}^{\exists}t \in \mathbb{A}^1(\mathbb{Q}) \setminus U \text{ s.t. } \pi_t(\mathbb{Q}) \neq \emptyset \iff S_0(\mathbb{Q}) \neq \emptyset \implies \mathrm{rank}E_n(\mathbb{Q}) > 0$$

となることから主張が示される. □

謝辞

末筆となりましたが, 講演の機会を与えてくださいました金子昌信先生, 権寧魯先生, 岸康弘先生に感謝致します.

参考文献

[1] J.-L. Colliot-Thélène and P Swinnerton-Dyer, Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties, J. Reine Angew. Math. **453** (1994), 49–112.

[2] J.-L. Colliot-Thélène, A. N. Skorobogatov and P. Swinnerton-Dyer, Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, Invent. Math. **134** (1998), 579–650.

[3] A. Bremner, R. K. Guy and R. J. Nowakowski, Which integers are representable as the product of the sum of three integers with the sum of their reciprocals?, Math. Comput. **61** (1993), 117–130.

[4] J. W. S. Cassels, Lectures on Elliptic Curves, London Math. Soc. Stud. Texts, 24, Cambridge Univ. Press, 1991.

[5] R. Kozuma, A Study on Elliptic Curves Related with Cyclic Cubic Extensions and Their Generalizations, Kyushu Univ. Doctral Thesis.

[6] R. Kozuma, Elliptic curves related to cyclic cubic extensions, Int. J. Number Theory **5** (2009), 591–623.

[7] J. H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., 106, Springer-Verlag, 1986.