楕円曲線の等分体のイデアル類群について

慶應義塾大学大学院理工学研究科 基礎理工学専攻
臺信 直人 (Naoto Dainobu)

Abstract

有理数体 $\mathbb{Q}$ 上の楕円曲線 E に対し, その等分体と呼ばれる代数体 K が定まり, これは一般に $\mathbb{Q}$ 上の非 abel 拡大となる. 本稿では, E の等分体 K のイデアル類群の Galois 加群構造について, 筆者が最近得た結果を紹介する.

1 背景

以下, 有理数体 $\mathbb{Q}$ の有限次拡大を代数体と呼ぶ. 代数体 K に対し, その**イデアル類群**と呼ばれる有限群 $\mathrm{Cl}(K)$ が定まる. 一応, その定義を紹介しておく.

定義 1.1. K を代数体とする. $I(K)$ を K の 0 でない分数イデアルのなす群, $P(K)$ を K の 0 でない単項分数イデアルのなす $I(K)$ の部分群とする. このとき, K のイデアル類群 $\mathrm{Cl}(K)$ を,

$$\mathrm{Cl}(K) := I(K)/P(K)$$

で定義する.

代数体のイデアル類群は整数論において大変重要な研究対象である. その研究の歴史は, Kummer による Fermat 予想の解決に向けた 19 世紀の仕事に始まる. 現代でもイデアル類群は, 乗法群 $\mathbb{G}_m$ に関する岩澤理論や同変玉河数予想などの整数論のとてもホットな話題において, その主要な登場人物として盛んに研究されている.

代数体 K が例えば $\mathbb{Q}$ 上の Galois 拡大であるとすると, Galois 群 $\mathrm{Gal}(K/\mathbb{Q})$ が $\mathrm{Cl}(K)$ に自然に作用する. このような状況において, $\mathrm{Cl}(K)$ を単なる群としてではなく, Galois 群 $\mathrm{Gal}(K/\mathbb{Q})$ の作用込みで調べる, つまり $\mathrm{Gal}(K/\mathbb{Q})$ 加群として調べるということがよくなされる. 1.1 節の後半で述べるように, $K/\mathbb{Q}$ が abel 拡大 ($\mathrm{Gal}(K/\mathbb{Q})$ が abel 群) の場合には, $\mathrm{Cl}(K)$ の $\mathrm{Gal}(K/\mathbb{Q})$ 加群構造については多くのことが知られている. 一方で, K が $\mathbb{Q}$ 上の非 abel 拡大 ($\mathrm{Gal}(K/\mathbb{Q})$ が非 abel 群) の場合には, $\mathrm{Cl}(K)$ の $\mathrm{Gal}(K/\mathbb{Q})$ 加群構造については, まだまだわからないことが多い状況である.

本稿では, $\mathbb{Q}$ 上の楕円曲線に対して定まる**等分体**と呼ばれる $\mathbb{Q}$ の非 abel 拡大を考察の対象とし, そのイデアル類群の Galois 加群構造について筆者が得た結果について紹介する. 結果の位置づけを簡単に述べると, まず $\mathbb{Q}$ 上の円分体に関する **Herbrand-Ribet の定理** (定理 1.4) という有名な結果がある. Herbrand-Ribet の定理について, その楕円曲線の等分体における類似を考察した **Prasad-Shekhar の定理** (定理 1.9) を部分的に精密化したものが, 筆者の結果 (定理 2.3, 系 2.4) である.

1.1 円分体のイデアル類群

まずは $\mathbb{Q}$ 上の abel 拡大の典型例である円分体のイデアル類群について, 前述の Herbrand-Ribet の定理を含め, どのようなことが調べられてきたかを解説する.

p を奇素数とし, μ_p を複素数体 $\mathbb{C}$ の中の 1 の p 乗根のなす群とする. Kummer は, Fermat 予想の解決に向けた研究の中で, $\mathbb{Q}$ に μ_p を添加した円の p 分体 $\mathbb{Q}(\mu_p)$ のイデアル類群 $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ を考察するに至った. 以下, A_p を $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ の p-Sylow 部分群とする. 次の定理は Kummer の判定法と呼ばれる結果である.

定理 1.2 (Kummer)**.**

$$\exists k \in 2\mathbb{Z}_{>0} \ \text{ s.t } \ p \text{ が } \zeta(1-k) \text{ の分子を割る } \iff A_p \neq 0.$$

ここで $\zeta(s)$ は Riemann の ζ-関数であり, 解析接続して $\mathbb{C}$ 上の有理型関数と見ている. また, $\zeta(1-k)$ の値は有理数であることが知られている.

注意 1.3. 一見, 全然関係がないように見える ζ-関数の値とイデアル類群 $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ とが, 定理 1.2 のように結びついていることはとても神秘的に感じられる. しかし, 話が逸れないように注意しておくと, 筆者の結果を含め, 1.2 節以降で紹介するイデアル類群に関する結果では, 残念ながら定理 1.2 に見られるような ζ-関数や, いわゆる L 関数とイデアル類群との結びつきは (まだ) 確認できない. この節では ζ-関数と $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ の結びつきよりも, $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ そのものについて何が調べられてきたか (定理 1.2, 1.4 の主張の右側) に注意して読んでいただきたい.

後に Herbrand [3] と Ribet [8] により, Kummer の結果の精密化が証明されている. 彼らは $\mathrm{Cl}(\mathbb{Q}(\mu_p))$ を単なる群ではなく, この章の始めに述べたように Galois 群 $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ が作用する群, つまり $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ 加群として扱った. 彼らは A_p を $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ 加群として

$$A_p = \bigoplus_{k=0}^{p-2} A_p^{\omega_{\mathrm{cyc}}^k} \tag{1.1}$$

のように分解して考察した. ここで, $\omega_{\mathrm{cyc}} : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to \mathbb{Z}_p^\times$ は mod p 円分指標で, $A_p^{\omega_{\mathrm{cyc}}^k}$ は $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ が $\omega_{\mathrm{cyc}}^k(\sigma)$ 倍で作用するような A_p の部分空間である. ざっくりいうと, (1.1) では A_p を $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ の作用に関する幾つかの固有空間に細分化したのである. このとき, Herbrand と Ribet は次を得た.

定理 1.4 (Herbrand-Ribet)**.** k を $2 \leqslant k \leqslant p-3$ を満たす偶数とする. このとき

$$p \text{ が } \zeta(1-k) \text{ の分子を割る } \iff A_p^{\omega_{\mathrm{cyc}}^{1-k}} \neq 0.$$

これは定理 1.2 の精密化になっている. 注目していただきたいのは, Kummer は A_p 全体の非自明性を考察しているのに対し, Herbrand と Ribet は A_p を Galois 群の作用に関して分解して, その分解における幾つかの成分の非自明性を考察している点である.

現在では, Mazur と Wiles による岩澤主予想の帰結として $A_p^{\omega_{\mathrm{cyc}}^{1-k}}$ の位数も明らかにできる. また, 円分体に限らず一般の $\mathbb{Q}$ 上の abel 拡大のイデアル類群についても, 幾つかの仮定の下に岩澤主予想から同様のことを明らかにできる.

1.2　楕円曲線の等分体のイデアル類群

最近, Prasad [6] によって $\mathbb{Q}$ 上の楕円曲線の等分体において, Herbrand-Ribet の定理の非 abel 類似が考察されている.

まず楕円曲線に関する用語を簡単にまとめる. ($\mathbb{Q}$ 上の) 楕円曲線とは, 基本的には $y^2 = x^3 + ax + b$ $(a, b \in \mathbb{Q})$ の形で定義される代数曲線 E のことである. ただし, 定義方程式の右辺には重根がないものとする. E 上の $\bar{\mathbb{Q}}$ 値点全体の集合

$$E(\bar{\mathbb{Q}}) := \{(X, Y) \in \bar{\mathbb{Q}}^2 \mid \ Y^2 = X^3 + aX + b\}$$

を考える. ここで, $\mathbb{Q}$ の代数閉包 $\bar{\mathbb{Q}}$ $(\subset \mathbb{C})$ を一つ取って固定している. 楕円曲線の顕著な性質として, $E(\bar{\mathbb{Q}})$ と無限遠点と呼ばれる点 $\mathcal{O}$ を合わせた集合に abel 群の構造が入ることが知られている.

定義 1.5 (E の等分点)**.** 非負整数 N に対して, $E(\bar{\mathbb{Q}})$ と $\mathcal{O}$ のなす abel 群の N ねじれ元全体のなす部分群を $E[N]$ と書き, E **の** N **等分点**と呼ぶ.

楕円曲線 E と非負整数 N に対し, 次のような代数体を定義することができる.

定義 1.6 (E の等分体)**.** E を $\mathbb{Q}$ 上の楕円曲線とする. このとき E **の** N**-等分体** $\mathbb{Q}(E[N])$ を,

$$\mathbb{Q}(E[N]) := \mathbb{Q}(\{X, Y \mid (X, Y) \in E[N]\})$$

で定める.

注意 1.7. $E[N]$ には $\mathbb{Q}$ の絶対 Galois 群 $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ が作用しており, $\mathbb{Q}(E[N])$ は $\mathbb{Q}$ 上の Galois 拡大である. 一般に $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$ は $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ の部分群で, 非 abel 群である.

p を再び奇素数とする. Prasad は [6] で, E の p 等分体 $\mathbb{Q}(E[p])$ のイデアル類群 $\mathrm{Cl}(\mathbb{Q}(E[p]))$ を $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群として扱い, 非 abel 拡大 $\mathbb{Q}(E[p])/\mathbb{Q}$ における定理 1.4 の類似を考察した. 以下, $A(E)_p$ を $\mathrm{Cl}(\mathbb{Q}(E[p]))$ の p-Sylow 部分群, $A(E)_p^{\mathrm{ss}}$ を $A(E)_p$ の $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})]$ 加群としての**半単純化**とする. ここで半単純化 $A(E)_p^{\mathrm{ss}}$ は, だいたい $A(E)_p$ の $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群としての既約分解のようなものだと思ってよい. つまり $A(E)_p^{\mathrm{ss}}$ は,

$$A(E)_p^{\mathrm{ss}} = \bigoplus_M M^{\oplus r_M} \tag{1.2}$$

のように $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群としての直和分解で表される. ただし, 上の直和の M は $\mathbb{F}_p$ 上の既約 $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群を全て走り, 非負整数 r_M は $A(E)_p^{\mathrm{ss}}$ における M 成分の重複度を表している.

この状況で, Prasad は次の問を提起した.

問 1.8. M を $\mathbb{F}_p$ 上の既約 $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群とする. (1.2) の分解において, いつ $r_M \neq 0$ となるか?

この問は勿論定理 1.4 に触発されたものである. [7] で Prasad と Shekhar は, $E[p]$ が既約 $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群である状況で, $M = E[p]$ の場合の問 1.8 に E の Selmer 群を用いて部分的回答を与えた.

定理 1.9 (Prasad-Shekhar)**.** E に関して, 次の条件を仮定する.

(1) E は p で良還元を持つ.

(2) $a_p(E) \equiv 1 \pmod{p}$ であり, E が $\mathbb{Q}_p$ の拡大体上で虚数乗法を持たなければ, $E[p]$ は $G_{\mathbb{Q}}$ の表現として p で暴分岐する. ここで, $a_p(E) := (p+1) - \#E(\mathbb{F}_p)$ である.

(3) 任意の素数 ℓ で, E の ℓ での玉河数が p と素である.

(4) $E[p]$ は $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群として既約である.

このとき $\dim_{\mathbb{F}_p}(\mathrm{Sel}(G_{\mathbb{Q}}, E[p])) \geqslant 2$ であれば,

$$E[p] \subset A(E)_p^{\mathrm{ss}},$$

つまり $r_{E[p]} \neq 0$ が成立する. ここに, $\mathrm{Sel}(G_{\mathbb{Q}}, E[p])$ は E の p-Selmer 群である.

注意 1.10. Birch と Swinnerton-Dyer による予想 (BSD 予想) を仮定すると, この結果を楕円曲線 E の L 関数 $L(E,s)$ を用いて書き換えることができる. $L^*(E,1)$ を $L(E,s)$ の $s=1$ における Taylor 展開の先頭係数とする. このとき定理 1.9 から, 定理 1.9 の仮定と BSD 予想の下で,

$$p \text{ が } L^*(E,1)^{alg} \text{ の分子を割る} \Rightarrow E[p] \subset A(E)_p^{\mathrm{ss}}$$

という, 非 abel 拡大 $\mathbb{Q}(E[p])/\mathbb{Q}$ における定理 1.4 の類似と見れる主張が得られる. ここに, $L^*(E,1)^{alg}$ は $L^*(E,1)$ の有理数部分である.

次の章で述べる筆者の主結果は, この定理 1.9 の部分的精密化を与える. 後に両者の関係性を述べるために, ここで定理 1.9 の証明について簡単に述べる. 以下, E の p 等分体 $\mathbb{Q}(E[p])$ を単に K と書くことにする.

定理 1.9 の帰結 $E[p] \subset A(E)_p^{\mathrm{ss}}$ のためには, 群コホモロジー $H^1(G_{\mathbb{Q}}, E[p])$ の**全素点不分岐な類**の成す部分群 $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p])$ の非自明性が十分である. 一応 $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p])$ の定義を紹介しておく. 素数 ℓ に対し, ℓ での惰性群を I_ℓ とかく. I_ℓ は $G_{\mathbb{Q}}$ の部分群であり, $H^1(G_{\mathbb{Q}}, E[p])$ の元を I_ℓ に制限する写像

$$\mathrm{Res}_\ell : H^1(G_{\mathbb{Q}}, E[p]) \to H^1(I_\ell, E[p])$$

を考えることができる.

定義 1.11.

$$H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p]) := \bigcap_{\ell:\text{素数}} \mathrm{Ker}(\mathrm{Res}_\ell)$$

と定め, この群 $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p])$ の元を $H^1(G_{\mathbb{Q}}, E[p])$ の全素点不分岐な類と呼ぶ.

この $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p])$ はイデアル類群 $\mathrm{Cl}(K)$ と密接に関係している. コホモロジー類を $G_{\mathbb{Q}}$ から $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ に制限する写像

$$\mathrm{Res} : H^1(G_{\mathbb{Q}}, E[p]) \to \mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Gal}(\bar{\mathbb{Q}}/K), E[p])$$

による $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p])$ の像を考えると,

$$\begin{aligned} H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p]) &\xrightarrow{\mathrm{Res}} \mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Gal}(K^{\mathrm{ur}}/K), E[p]) \ (\subset \mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Gal}(\bar{\mathbb{Q}}/K), E[p])) \\ &\xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathrm{Cl}(K), E[p]) \end{aligned} \tag{1.3}$$

となる. ここに, K^{ur} は K の最大不分岐 abel 拡大であり, 2 行目は類体論による同型 $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \mathrm{Cl}(K)$ を用いた. (1.3) の Hom の集合に非自明な射 f があれば, $E[p]$ の既約性から f は全射になる. この全射 f の存在から, $E[p] \subset A(E)_p^{\mathrm{ss}}$ が帰結される. ここで, 定理 1.9 の仮定 (4) の下で Res は単射である. 故に,

$$H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p]) \neq 0 \Rightarrow E[p] \subset A(E)_p^{\mathrm{ss}} \tag{1.4}$$

が従う.

[7] での定理 1.9 の証明の流れは, E の Selmer 群 $\mathrm{Sel}(G_{\mathbb{Q}}, E[p])$ $(\subset H^1(G_{\mathbb{Q}}, E[p]))$ の次元が十分大きければ (今の場合 2 以上ならば), Selmer 群の中に非自明な $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p])$ の元が存在することを示し, (1.4) から定理の帰結を得るというものである.

2 主結果

この章で筆者の主結果を紹介する. まず, 問 1.8 の次の精密化を考える.

問 2.1. M を $\mathbb{F}_p$ 上の既約 $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群とする. (1.2) の分解において, r_M の値はいくつか?

筆者の主結果の一つ (系 2.4) は, $E[p]$ が既約な $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ 加群である状況で, $M = E[p]$ の場合の問 2.1 に部分的な回答を与えるものである.

2.1 全素点不分岐な有理点

まず, 主結果を述べるために重要な概念を導入する.

素数 ℓ に対し, $\mathbb{Q}_\ell$ を ℓ 進体, $\mathbb{Q}_\ell^{\mathrm{ur}}$ を $\mathbb{Q}_\ell$ の最大不分岐拡大とする. $\mathbb{Q}_\ell$ は局所体と呼ばれる体の最も基本的な例の一つだが, ここでは単に包含 $\mathbb{Q} \subset \mathbb{Q}_\ell \subset \mathbb{Q}_\ell^{\mathrm{ur}}$ があることをおさえていただければ良い. 以下, 体 F を $\mathbb{Q}$, $\mathbb{Q}_\ell$, または $\mathbb{Q}_\ell^{\mathrm{ur}}$ のいずれかとして,

$$E(F) := \{(X, Y) \in F^2 \mid (X, Y) \text{ は } E \text{ 上の点 }\}$$

と定め E の F-有理点と呼ぶ. $E(F)$ は $E(\bar{\mathbb{Q}})$ と同様に, 無限遠点 $\mathcal{O}$ と合わせて abel 群となる.

定義 2.2. n を正の整数とし, $E(\mathbb{Q})$ の部分群 $E(\mathbb{Q})_{\mathrm{ur},p^n}$ を

$$E(\mathbb{Q})_{\mathrm{ur},p^n} := \mathrm{Ker}\left(E(\mathbb{Q}) \xrightarrow{\prod_\ell \iota_\ell} \prod_{\ell:\text{素数}} \frac{E(\mathbb{Q}_\ell^{\mathrm{ur}})}{p^n E(\mathbb{Q}_\ell^{\mathrm{ur}})} \right)$$

で定める. ただし上の写像 $\iota_\ell : E(\mathbb{Q}) \to E(\mathbb{Q}_\ell^{\mathrm{ur}})/p^n E(\mathbb{Q}_\ell^{\mathrm{ur}})$ は, 包含写像 $E(\mathbb{Q}) \to E(\mathbb{Q}_\ell^{\mathrm{ur}})$ と mod p^n 写像 $E(\mathbb{Q}_\ell^{\mathrm{ur}}) \to E(\mathbb{Q}_\ell^{\mathrm{ur}})/p^n E(\mathbb{Q}_\ell^{\mathrm{ur}})$ の合成である. また, 非負整数 $r_{\mathrm{ur},p^n}(E)$ を

$$r_{\mathrm{ur},p^n}(E) := \mathrm{length}_{\mathbb{Z}_p}(E(\mathbb{Q})_{\mathrm{ur},p^n}/p^n E(\mathbb{Q}))$$

で定める.

この $E(\mathbb{Q})_{\mathrm{ur},p^n}$ の元を E の全素点不分岐な有理点と呼ぶことにする．$E(\mathbb{Q})_{\mathrm{ur},p^n}$ は $E(\mathbb{Q})$ の元であって, 任意の素数 ℓ で局所的に $E(\mathbb{Q}_\ell^{\mathrm{ur}})$ の元と見たときに, その p^n 倍元となるような点のなす群である．非負整数 $r_{\mathrm{ur},p^n}(E)$ は, 全ての素数で局所的に p^n 倍点となる点の群 $E(\mathbb{Q})_{\mathrm{ur},p^n}$ と, $E(\mathbb{Q})$ の p^n 倍点のなす群 $p^nE(\mathbb{Q})$ の間の差を測る量である．

全素点不分岐な有理点の群 $E(\mathbb{Q})_{\mathrm{ur},p^n}$ の最も大事な性質は, その元から $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p^n])$ の元を作れるということである．ここで, 前の節では $n=1$ の場合にしか $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p])$ の定義を紹介していないが, 一般の正の整数 n に対しても $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p^n])$ は同様に定義される．Kummer 写像

$$\kappa_n : E(\mathbb{Q})/p^nE(\mathbb{Q}) \hookrightarrow H^1(G_{\mathbb{Q}}, E[p^n])$$

という, E の $\mathbb{Q}$-有理点に $H^1(G_{\mathbb{Q}}, E[p^n])$ の類を対応させる写像がある．この κ_n に関して, $E(\mathbb{Q})_{\mathrm{ur},p^n}$ の定義から直ちに

$$\kappa_n(E(\mathbb{Q})_{\mathrm{ur},p^n}/p^nE(\mathbb{Q})) \subset H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p^n]) \tag{2.1}$$

が成立する．

筆者の主結果の一つである定理 2.3 では, E の p^n 等分体 $K_n := \mathbb{Q}(E[p^n])$ のイデアル類群 $\mathrm{Cl}(K_n)$ を考察する．一般の正の整数 n についても (1.3) と同様に,

$$H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p^n]) \to \mathrm{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\mathrm{Cl}(K_n), E[p^n])$$

という, 比較的緩い条件 (定理 2.3 の (Inj)) の下で単射になる写像が存在する．包含 (2.1) を考慮すると, $\mathrm{Cl}(K_n)$ を調べる上で $E(\mathbb{Q})_{\mathrm{ur},p^n}$ が重要になりそうな雰囲気がしてくる．

2.2 主結果

以下, E の p^n 等分体 $\mathbb{Q}(E[p^n])$ を前節の最後と同様に K_n とかく．特に $n=1$ のときは, 単に K_1 を K とかく．次が本稿における筆者の一つ目の主結果である．

定理 2.3 (D)**.** 次の 3 つの条件を仮定する．

(Add) $p=3$ ならば, E は 3 以外の素数で悪還元かつ潜在的良還元をもたない．

(Mult) 素数 ℓ に対し, $v_\ell(j(E)) < 0$ ならば, $p \nmid v_\ell(j(E))$ である．ここで v_ℓ は ℓ 進付値で, $j(E)$ は E の j 不変量である．

(Inj) $H^1(\mathrm{Gal}(K_n/\mathbb{Q}), E[p^n]) = 0$.

このとき, 次が成立する．

(A) $E(\mathbb{Q})_{\mathrm{ur},p^n} = \mathrm{Ker}\left(E(\mathbb{Q}) \to E(\mathbb{Q}_p^{\mathrm{ur}})/p^nE(\mathbb{Q}_p^{\mathrm{ur}})\right)$.

(B) $\mathrm{length}_{\mathbb{Z}_p}\left(\mathrm{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\mathrm{Cl}(K_n), E[p^n])\right) \geqslant r_{\mathrm{ur},p^n}(E)$.

主張 (A) は, 素数全てにわたる条件で定義されていた $E(\mathbb{Q})_{\mathrm{ur},p^n}$ が, 定理 2.3 の条件 ((Add) と (Mult)) の下では, 固定した p での条件だけから決まるということを述べている．また主張 (B) によって, $r_{\mathrm{ur},p^n}(E)$ から $\mathrm{Cl}(K_n)$ の大きさを把握することができる．

$n=1$ で $E[p]$ が既約な状況では, 定理 2.3 は $M = E[p]$ の場合の問 2.1 に部分的な回答を与えることができる．

系 2.4 (D)**.** $n=1$ とする. 定理 2.3 の条件 (Add), (j-inv), (Inj) と, $E[p]$ の $\mathrm{Gal}(K/\mathbb{Q})$ 加群としての既約性を仮定する. このとき,

$$E[p]^{\oplus r_{\mathrm{ur},p}(E)} \subset A(E)_p^{\mathrm{ss}}$$

が成立する.

つまり系 2.4 の仮定の下では, $A(E)_p$ の半単純化 (1.2) における $E[p]$ 成分の重複度 $r_{E[p]}$ の下界として, $r_{\mathrm{ur},p}(E)$ をとることができる. $r_{\mathrm{ur},p}(E)>1$ なる状況であれば, 系 2.4 は定理 1.9 よりも $A(E)_p^{\mathrm{ss}}$ の $E[p]$ 成分について精密なことが帰結できることになる.

注意 2.5. [4, Theorem 1, Theorem 2] において, 定理 2.3 の仮定 (Inj) が成立しない例が調べられている. この結果から $p\geqslant 13$ であれば, 任意の n と E に対して仮定 (Inj) は成立することがわかる. (Add) と (Mult) もそこまで強い仮定ではない. (大雑把なことを言ってしまうと, p が十分大きければ満たされる仮定である.)

定理 2.3 のポイントは二点あると考えている. 一つは, 勿論 $E(\mathbb{Q})_{\mathrm{ur},p^n}$ の導入である. $n=1$ の場合の定理 1.9 の帰結 $E[p]\subset A(E)_p^{\mathrm{ss}}$ には, (1.4) で述べた通り $H^1_{\mathrm{ur}}(G_{\mathbb{Q}},E[p])\neq 0$ が十分であった. これに対し, Prasad と Shekhar は定理 1.9 の証明で, Selmer 群の次元が十分大きければ $H^1_{\mathrm{ur}}(G_{\mathbb{Q}},E[p])$ に非自明な元が存在することを示しただけで, 具体的に $H^1_{\mathrm{ur}}(G_{\mathbb{Q}},E[p])$ の類を構成したわけではない. 一方, 定理 2.3 では Kummer 写像を通して $H^1_{\mathrm{ur}}(G_{\mathbb{Q}},E[p])$ の類を作る具体的な点の集合 $E(\mathbb{Q})_{\mathrm{ur},p^n}$ を導入した. このことは, 定理 1.9 の帰結の精密化のみならず, いくつかの場合に定理の適応範囲の改良も可能にしている. (例 2.8, 注意 2.9 参照).

二つ目のポイントは主張 (A) において, 比較的緩い条件 (Add), (Mult) の下で, $E(\mathbb{Q})_{\mathrm{ur},p^n}$ の考察を素数 p における $E(\mathbb{Q})$ の考察へ帰着させている点である. これは後に紹介するように, 具体的な状況で定理 2.3 や系 2.4 を適用するときに, $r_{\mathrm{ur},p}(E)$ を計算するのに重要となる.

2.3 系 2.4 の適用方法, 適用例

本稿の最後に, 系 2.4 の適用方法とその適用例を紹介する. 系 2.4 を用いて, $A(E)_p^{\mathrm{ss}}$ の $E[p]$ 成分を考察するには, $r_{\mathrm{ur},p}(E)=\dim_{\mathbb{F}_p}(E(\mathbb{Q})_{\mathrm{ur},p}/pE(\mathbb{Q}))$ の計算が重要である. 定理 2.3 の主張 (A) によると, 仮定 (Add), (Mult) の下では

$$E(\mathbb{Q})_{\mathrm{ur},p}=\mathrm{Ker}(E(\mathbb{Q})\to E(\mathbb{Q}_p^{\mathrm{ur}})/pE(\mathbb{Q}_p^{\mathrm{ur}}))$$

となるのであった.

ここで点 $P\in E(\mathbb{Q})$ について, いつ $P\in\mathrm{Ker}(E(\mathbb{Q})\to E(\mathbb{Q}_p)/pE(\mathbb{Q}_p))$ となるかを考える. このとき, 特に $P\in E(\mathbb{Q})_{\mathrm{ur},p}$ である.

補題 2.6. E の定義方程式が p で minimal であるとする. E に付随する形式群を $\hat{E}$ で表し, $\hat{E}$ の対数を $\log_{\hat{E}}$ とかく. $E_1(\mathbb{Q}_p)$ で法 p 還元 $E(\mathbb{Q}_p)\xrightarrow{\mathrm{mod}\ p}E(\mathbb{F}_p)$ の核を表すものとする. このとき, 群の同型

$$E_1(\mathbb{Q}_p)\xrightarrow{\sim}p\mathbb{Z}_p\quad (X,Y)\mapsto\log_{\hat{E}}(-X/Y)$$

が存在する.

証明は [9, Chapter VII, Proposition 2.2] 参照. 対数 $\log_{\hat{E}}$ については説明しないが,

$$\log_{\hat{E}}(-X/Y) \in p^2\mathbb{Z}_p \iff -X/Y \in p^2\mathbb{Z}_p$$

が成立する [9, Chapter VII, Theorem 6.4 (b)]. 故に, この補題から点 $P(X,Y)$ が $E_1(\mathbb{Q}_p)$ に属していれば, 単に $-X/Y$ の値を求め, その値 (の分子) が p^2 で割れていれば, $P \in pE_1(\mathbb{Q}_p) \subset pE(\mathbb{Q}_p)$ がわかる. 点 $P(X,Y)$ が $E_1(\mathbb{Q}_p)$ に属しているかどうかも簡単に判定でき, 実際 $v_p(X) < 0$ であれば良い. ここで v_p は p 進付値であり, $x \in \mathbb{Q}$ を $x = p^k \cdot \frac{c}{d}$ $(k \in \mathbb{Z},\ p \nmid c, d)$ と表したとき, $v_p(x) = k$ である.

まとめると, 次が得られたことになる.

命題 2.7. 定理 2.3 の仮定 (Add), (Mult) が満たされていて, E の定義方程式が p で minimal であるとする. $P(X,Y) \in E(\mathbb{Q})$ について,

$$v_p(X) < 0 \text{ かつ } v_p(X/Y) \geqslant 2 \Rightarrow P \in E(\mathbb{Q})_{\mathrm{ur},p}.$$

このことを用いて得られる例を二つ紹介する.

例 2.8. E を方程式 $y^2 = x^3 - 432x + 15120$ で定義される楕円曲線とする. $p = 13$ として, 系 2.4 を E に適用することで

$$E[13] \subset A(E)^{\mathrm{ss}}_{13} \tag{2.2}$$

が証明できる.

系 2.4 の仮定が満たされることをまず確認する. E はデータベース [5] において 43.a1 とラベリングされている楕円曲線である. [5] によると, $j(E) = 2^{12} \cdot 43^{-1}$ で定理 2.3 の仮定 (j-inv) は満たされている. 注意 2.5 から, 仮定 (Inj) も満たされている. $E[13]$ の既約性も, [5] でチェックできる.

[5] によると, 群 $E(\mathbb{Q})$ は $S := (0,0)$ によって生成され, $\mathbb{Z}$ と同型であることがわかる. 特に $S \notin 13E(\mathbb{Q})$ である. 点 S の 19 倍を計算すると,

$$19S = \left(\frac{-2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 59 \cdot 61 \cdot 107}{\mathbf{13}^6 \cdot 37^2}, \frac{3^4 \cdot 11^2 \cdot 17 \cdot 59^2 \cdot 173 \cdot 211}{\mathbf{13}^9 \cdot 37^3} \right).$$

となる. 故に点 $19S$ は命題 2.7 の点 P の条件を満たしており, $19S \in E(\mathbb{Q})_{\mathrm{ur},13}$ である (E の定義方程式が 13 で minimal であることもチェックできる). $19S \notin 13E(\mathbb{Q})$ であるから, $19S$ の $E(\mathbb{Q})_{\mathrm{ur},13}/13E(\mathbb{Q})$ のにおける像は非自明である. よって $r_{\mathrm{ur},13}(E) > 0$ であり, 系 2.4 から包含 (2.2) が得られる.

注意 2.9. [5] によると, BSD 予想のもとではあるが E の Tate-Shafarevich 群は自明であることがわかり, $\dim_{\mathbb{F}_{13}}(\mathrm{Sel}(G_{\mathbb{Q}}, E[13])) = 1$ である. この場合, 定理 1.9 は使えないことに注意する. この例のように, 定理 2.3 で $E(\mathbb{Q})_{\mathrm{ur},p}$ を具体的に調べることによって, $\dim_{\mathbb{F}_p}(\mathrm{Sel}(G_{\mathbb{Q}}, E[p])) \leqslant 1$ であっても (2.1) から $H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, E[p]) \neq 0$ であることがわかり, (1.4) から包含 $E[p] \subset A(E)^{\mathrm{ss}}_p$ が得られる場合がある.

例 2.10. E を方程式 $y^2 = x^3 - 2401x + 1$ で定義される楕円曲線とする. $p = 7$ として, 系 2.4 を E に適用することで

$$E[7]^{\oplus 3} \subset A(E)^{\mathrm{ss}}_7 \tag{2.3}$$

が証明できる.

注意 2.11. 上の E は, [2] で扱われた二つのパラメーター $m, n \in \mathbb{Z}$ で定まる楕円曲線の族を, $m = 49$, $n = 1$ に特殊化したものである. E には $S := (0, 1)$, $T := (-49, 1)$, $U := (-1, 49)$ という $\mathbb{Q}$-有理点があることがわかるが, これらが $\mathbb{Z}$ 上一次独立であり, $E(\mathbb{Q})$ の基底に延長できることが [2, Theorem 1.1 (2)] で証明されている. 特に, $S, T, U \notin 7E(\mathbb{Q})$ がわかる.

系 2.4 の仮定が満たされることをまず確認する. $j(E) = 2^8 \cdot 3^3 \cdot 7^{12}/1069 \cdot 51791533$ より, 定理 2.3 の仮定 (j-inv) は満たされている. [4, Theorem 1.1] より, (Inj) も満たされていることがわかる. SageMath を用いた計算によって, $E[7]$ が既約 $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$-加群であることも確かめられる.

注意 2.11 の点 $S, T, U \in E(\mathbb{Q})$ について,

$$3S = \left(\frac{-2^3 \cdot 79 \cdot 199 \cdot 367 \cdot 2399}{\mathbf{7}^{16}}, \frac{37 \cdot 4691 \cdot 19523423 \cdot 169609859}{\mathbf{7}^{24}} \right),$$

$$3T = \left(\frac{5^2 \cdot 13 \cdot 53 \cdot 181 \cdot 1777 \cdot 73483}{2^2 \cdot \mathbf{7}^4 \cdot 67^2 \cdot 439}, \frac{29 \cdot 31 \cdot 6151 \cdot 12992635846499}{2^3 \cdot \mathbf{7}^6 \cdot 67^3 \cdot 439^3} \right),$$

$$2U = \left(\frac{3^2 \cdot 139 \cdot 1153}{\mathbf{7}^4}, \frac{5 \cdot 345311039}{\mathbf{7}^6} \right)$$

が計算でき, 3 点 $3S, 3T, 2U$ は全て命題 2.7 の点 P の条件を満たしている (E の定義方程式が 7 で minimal であることもチェックできる). 故に, $3S, 3T, 2U \in E(\mathbb{Q})_{\mathrm{ur},7}$ である. 注意 2.11 で述べたことから, $3S, 3T, 2U$ の $E(\mathbb{Q})_{\mathrm{ur},7}/7E(\mathbb{Q})$ における像はそれぞれ非自明で, かつそれらは $\mathbb{F}_7$ 上一次独立であることがわかる. よって $r_{\mathrm{ur},7}(E) \geqslant 3$ であることがわかり, 系 2.4 から包含 (2.3) が得られる.

References

[1] N. Dainobu, On ideal class groups of division fields of elliptic curves and everywhere unramifed rational points, in preparation.

[2] Y. Fujita and T. Nara, The Mordell-Weil bases for the elliptic curve of the form $y^2 = x^3 - m^2x + n^2$, Publ. Math. **92** (2018), 79-99.

[3] J. Herbrand, Sur les classes des corps circulaires, Journal de Mathématiques Pures et Appliquées **11** (1932), 417-441.

[4] T. Lawson, C. Wuthrich, Vanishing of some Galois cohomology groups for elliptic curves. In D. Loeffler, S. L. Zerbes (Eds.), Elliptic curves, modular forms and Iwasawa theory: in honour of John H. Coates' 70th birthday, Cambridge, UK, March 2015, Springer (2016).

[5] The LMFDB Collaboration, The L-functions and modular forms database, 2022. (https://www.lmfdb.org/)

[6] D. Prasad, A proposal for non-abelian Herbrand-Ribet, preprint

[7] D. Prasad, and S. Shekhar, Relating the Tate-Shafarevich group of an elliptic curve with the class group, Pacific Journal of Mathematics **312** (1) (2021), 203-218.

[8] K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, Invent. math. **34** (1976), 151-162.

[9] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts inMathematics, **106**. Springer-Verlag, New York (1986).