イデアル類群の漸近挙動と楕円曲線の精 Selmer 群の岩澤加群について

群馬大学・共同教育学部　大下達也
Tatsuya Ohshita
Cooperative Faculty of Education,
Gunma University

1　序

「代数体の拡大塔に沿ったイデアル類群の漸近的挙動」に関する研究は，岩澤健吉氏による代数体の $\mathbb{Z}_p$ 拡大に関する岩澤の類数公式 ([6]) という著しい結果を端緒の 1 つとする，岩澤理論における古典的かつ重要な領域の 1 つである．

本稿では，RIMS 共同研究 (公開型)「代数的整数論とその周辺」2021 での筆者の講演に基づいて，楕円曲線の素数冪ねじれ点から定まる代数体の非可換な拡大塔に沿ったイデアル類群（の商）の漸近挙動と楕円曲線の精 Selmer 群の定める（円分）岩澤加群の関係に関する平之内俊郎氏との共同研究 [4] で得られた結果について概説する．詳細については，プレプリント [4] を参照して頂きたい．

まず，本稿で扱う設定を簡単に述べておきたい．本稿全体を通して，E を有理数体 $\mathbb{Q}$ 上の楕円曲線とし，E が良い還元を持つような奇素数 p を固定する．各正の整数 N に対して，有理数体の代数閉包の乗法群 $\overline{\mathbb{Q}}^\times$ における 1 の N 乗根全体のなす部分群を $\mu_N := \mu_N(\overline{\mathbb{Q}})$ と表し，$E(\overline{\mathbb{Q}})$ の N ねじれ点全体のなす部分群を $E[N]$ と表す．各非負整数 n に対して，$K_n := \mathbb{Q}(\mu_{p^n})$ と書き，楕円曲線 E から定まる法 p^n Galois 表現

$$\rho_n^E \colon G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]) = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

の核で固定される $\overline{\mathbb{Q}}$ の最大の部分体を K_n^E と書く．（すなわち，K_n^E は有理数体に $E[p^n]$ の全ての点の座標を添加した体である．）楕円曲線の Weil 対

$$E[p^n] \times E[p^n] \longrightarrow \mu_{p^n}$$

が Galois 群 $G_{\mathbb{Q}}$ の作用を保つことから，$K_n \subseteq K_n^E$ が成り立つことに注意する．

以下では，代数体 F の整数環を $\mathcal{O}_F$ と書く．また，Dedekind 整域 $\mathcal{O}$ のイデアル類群を $\mathrm{Cl}(\mathcal{O})$ と書く．

本稿 (および [4]) の主定理は，体の拡大塔 $\{K_n^E\}_{n>0}$ に沿ったイデアル類群（の商）の漸近挙動に関する結果である．本稿の主結果の概要を述べる前に，楕円曲線 E の Mordell–Weil 群と類数を関係づける先行研究を紹介したい．2 つの実数列 $\{a_n\}_{n>0}$, $\{b_n\}_{n>0}$ が

$$\liminf_{n\to\infty}(a_n - b_n) > -\infty$$

を満たすとき，$a_n \succ b_n$ と書く．西来路文朗氏，山内卓也氏による先行研究 ([13], [14]) および平之内俊郎氏による先行研究 ([3]) により，組 (E,p) に関するいくつかの条件の下で，Mordell–Weil 群の階数 $r := \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ を用いた，$\mathrm{Cl}(\mathcal{O}_{K_n^E}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ の位数の漸近的な下界を与える次の不等式が得られている:

$$\mathrm{ord}_p(\#\,\mathrm{Cl}(\mathcal{O}_{K_n^E}) \otimes_{\mathbb{Z}} \mathbb{Z}_p) \succ 2(r-1)n. \tag{1.1}$$

ただし，ord_p は $\mathrm{ord}_p(p) = 1$ となるよう正規化された加法的 p 進付値である．

注意 1.1. ここでは詳細には立ち入らないが，筆者の論文 [9] では，Galois 表現の Selmer 群の言葉を用いて再定式化することで，[13], [14], [3] の結果を「p 進 Galois 表現から定まる代数体の拡大塔に沿ったイデアル類群の位数の p 進付値の漸近的下界の構成」という形に一般化している．特に，[9] の結果をアーベル多様体に付随する p 進 Galois 表現に適用することで，不等式 (1.1) を E がアーベル多様体である場合に拡張することが出来る．尚，筆者の研究 [9] とは独立に，J. Garnek 氏による研究 ([2]) でも不等式 (1.1) の E がアーベル多様体の場合への拡張が得られている．

正確な説明は後回しにして，本稿 (および [4]) の主結果の概要を述べよう．プレプリント [4] では，各正の整数 n に対して，「法 p^n Galois 表現

$$\rho_n^E|_{G_{K_n}} : G_{K_n} := \mathrm{Gal}(K_n^E/K_n) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]) = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$$

で切り取られる $\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])$ の商[*1]」A_n^E を定義して，$n \to \infty$ としたときの A_n^E の漸近的挙動を精 Selmer 群 $\mathrm{Sel}_p(K_n, E[p^n])$ を用いて記述した．本稿および [4] の主結果の大雑把な主張は以下の通りである．

[*1] A_n^E の定義については後述の定義 3.2 を参照せよ．尚，定義 3.2 を見ればわかる通り，(一般的な状況では，少なくとも定義の上では) A_n^E は「$\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])$ の商」ではないが，注意 3.4 で後述する通り，本稿で扱う状況に限れば，自然な写像 $\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]) \longrightarrow A_n^E$ が全射になるので A_n^E を $\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])$ の（従って $\mathrm{Cl}(\mathcal{O}_{K_n^E})$ の）商と見なせる．

定理 1.2 (正確な主張は定理 3.2 参照)**.** 組 (E,p) がある条件を満たすとき，核と余核の位数が有界な $\mathbb{Z}_p$ 加群の準同型の列

$$\left\{ r_n \colon \mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2} \xrightarrow{G_{K_n}\ \text{同変}} (A_n^E)^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(A_n^E, E[p^n]) \right\}_{n>0}$$

が存在する．

2 つの実数列 $\{a_n\}_{n>0}$, $\{b_n\}_{n>0}$ が $a_n \succ b_n$ かつ $b_n \succ a_n$ を満たすとき，

$$a_n \sim b_n$$

と書くことにする．円分 $\mathbb{Z}_p$ 拡大に関する楕円曲線の精 Selmer 群のコントロール定理と定理 3.2 を合わせることで，「岩澤の類数公式」型の次のような A_n^E の位数に関する漸近公式が得られる．

系 1.3 (正確な主張は系 6.3 参照)**.** 組 (E,p) がある条件を満たすとき，

$$\mathrm{ord}_p(\#A_n^E) \sim 2\Big(\mu(X_\infty)p^n + \lambda(X_\infty)n\Big)$$

が成り立つ．ここで，$\mu(X_\infty)$ および $\lambda(X_\infty)$ はそれぞれ，精 Selmer 群の Pontrjagin 双対で定まる岩澤加群

$$X_\infty := \mathrm{Hom}_{\mathbb{Z}_p}\left(\varinjlim_n \mathrm{Sel}_p(K_n, E[p^\infty]), \mathbb{Q}_p/\mathbb{Z}_p\right)$$

の岩澤 μ 不変量，岩澤 λ 不変量である．

注意 1.4. 系 1.3 の右辺に現れる $\mu(X_\infty)$ および $\lambda(X_\infty)$ は，楕円曲線の岩澤主予想の下では，Beilinson–加藤元を用いて記述できる（詳細については後述の系 7.2 を参照）．

注意 1.5. $r := \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ とおくと，$\lambda(X_\infty) \geq r-1$ が成り立つ．従って，系 1.3 から不等式 (1.1) が従うので，系 1.3 の主張は不等式 (1.1) の精密化と見なせる．

本稿の構成について述べる．まず，第 2 節で精 Selmer 群の定義を述べ，第 3 節で本稿および [4] の主定理（定理 1.2 の正確な主張）を述べる．第 4 節で，本稿の主定理から従う A_n^E の $\mathbb{Z}_p$ 加群構造の漸近挙動に関する結果を紹介し，第 5 節で第 4 節の結果の証明の概略を説明する．第 6 節では，拡大 $K_\infty/\mathbb{Q}$ に関する楕円曲線の岩澤理論の観点から得られる結果（系 1.3 の正確な主張）を述べ，類数の漸近挙動に関する先行研究との比較を行う．第 7 節では，第 6 節で述べた結果に関する楕円曲線の岩澤主予想の観点からの補足を行う．

2　精 Selmer 群

F を代数体とし，$n \in \mathbb{Z}_{>0} \cup \{\infty\}$ とする．精 Selmer 群 $\mathrm{Sel}_p(F, E[p^n])$ の定義を思い出そう．F の各有限素点 v に対して，短完全列

$$0 \longrightarrow E[p^n] \xrightarrow{\subseteq} E(\overline{F}_v) \xrightarrow{\times p^n} E(\overline{F}_v) \longrightarrow 0.$$

から誘導される写像

$$E(F_v) = H^0(F_v, E(\overline{F}_v)) \longrightarrow H^1(F_v, E[p^n])$$

の像を $H^1_{\mathrm{cl}}(F_v, E[p^n])$ と書く．古典的な Selmer 群 $\mathrm{Sel}(F, E[p^n])$ は

$$\mathrm{Sel}(F, E[p^n]) := \mathrm{Ker}\left(H^1(F, E[p^n]) \longrightarrow \prod_{v:\ \text{有限素点}} \frac{H^1(F_v, E[p^n])}{H^1_{\mathrm{cl}}(F_v, E[p^n])} \right)$$

で定まる $H^1(F, E[p^n])$ の部分群であった．精 Selmer 群 $\mathrm{Sel}_p(F, E[p^n])$ の定義は次の通りである:

$$\mathrm{Sel}_p(F, E[p^n]) := \mathrm{Ker}\left(\mathrm{Sel}(F, E[p^n]) \longrightarrow \prod_{v|p} H^1(F_v, E[p^n]) \right).$$

3　主定理

本節では, 本稿の主結果 (定理 1.2) の主張を正確に述べる．まず, いくつか記号を用意しよう．第 1 節と同様, 各非負整数 m に対して, $K_m := \mathbb{Q}(\mu_{p^m})$ と定義する．更に, $K_\infty := \mathbb{Q}(\mu_{p^\infty}) = \bigcup_{m \geq 0} K_m$ と定める．$m_2 > m_1$ を満たす $m_1, m_2 \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ に対して, $\mathcal{G}_{m_2,m_1} := \mathrm{Gal}(K_{m_2}/K_{m_1})$ とおき, $\Delta := \mathcal{G}_{1,0} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ と書く．p は奇素数であるので, 任意の $m \geq 1$ に対して, $\mathcal{G}_{m,0} = \Delta \times \mathcal{G}_{m,1}$ が成り立つ．この直積分解により, $\mathbb{Z}_p[\Delta]$ を $\mathbb{Z}_p[\mathcal{G}_{m,0}]$ の部分環と見なす．Δ の指標のなす群 $\widehat{\Delta} := \mathrm{Hom}(\Delta, \mathbb{Z}_p^\times)$ を考える．各指標 $\chi \in \widehat{\Delta}$ に対して, $\mathbb{Z}_p$ 代数としては $\mathbb{Z}_p$ と同型で, Δ が χ を通して作用するような $\mathbb{Z}_p[\Delta]$ 代数を $\mathbb{Z}_p(\chi)$ と書き, M が $\mathbb{Z}_p[\Delta]$ 加群であるとき $M_\chi := M \otimes_{\mathbb{Z}_p[\Delta]} \mathbb{Z}_p(\chi)$ と定める．群 Δ の位数 $p-1$ は p と互いに素であるので, $M = \bigoplus_{\chi \in \widehat{\Delta}} M_\chi$ が成り立つ．各非負整数 m, n に対して,

$$R_{m,n} := \mathbb{Z}/p^n\mathbb{Z}[\mathcal{G}_{m,0}] = \mathbb{Z}_p/p^n\mathbb{Z}_p[\mathrm{Gal}(K_m/\mathbb{Q})],$$

と定めて, $R_n := R_{n,n}$ とおく．R_n 加群 A_n^E を次で定める．

定義 3.1. $E[p^n]^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(E[p^n], \mathbb{Z}/p^n\mathbb{Z})$ への $G_{\mathbb{Q}}$ の右作用

$$(\rho_n^E)^\vee \colon \mathrm{Gal}(K_n^E/\mathbb{Q})^{\mathrm{op}} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p^n]^\vee) = \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z}) \tag{3.1}$$

を考える．$\mathbb{Z}/p^n\mathbb{Z}$ 係数の 2 次正方行列全体のなす環を $M_2(\mathbb{Z}/p^n\mathbb{Z})$ とおく．群準同型 (3.1) から誘導される環準同型

$$\mathbb{Z}/p^n\mathbb{Z}[\mathrm{Gal}(K_n^E/\mathbb{Q})]^{\mathrm{op}} \longrightarrow M_2(\mathbb{Z}/p^n\mathbb{Z})$$

も $(\rho_n^E)^\vee$ という記号で表すことにする．このとき，$(\rho_n^E)^\vee$ により $M_2(\mathbb{Z}/p^n\mathbb{Z})$ に右 $\mathbb{Z}[\mathrm{Gal}(K_n^E/K_n)]$ 加群の構造を入れて，

$$A_n^E := M_2(\mathbb{Z}/p^n\mathbb{Z}) \otimes_{\mathbb{Z}[\mathrm{Gal}(K_n^E/K_n)]} \mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]) \tag{3.2}$$

と定める．A_n^E への $\mathbb{Z}_p$ 線形な $\sigma \in G_{\mathbb{Q}}$ の作用が次で定まる: $A \in M_2(\mathbb{Z}/p^n\mathbb{Z})$ とし，$[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p])$ とするとき，

$$\sigma(A \otimes [\mathfrak{a}]) := A(\rho_n^E)^\vee(\sigma^{-1}) \otimes [\sigma\mathfrak{a}].$$

G_{K_n} の任意の元は A_n^E に自明に作用するので，A_n^E は自然に R_n 加群と見なせる．

以上の準備の下で，本稿および [4] の主結果の主張を述べよう．

定理 3.2 ([4, Theorem 1.1, Theorem 5.16])**.** E を $\mathbb{Q}$ 上の楕円曲線とし，p を E が良い還元を持つような奇素数とする．組 (E, p) が次の 3 つの条件 (C1), (C2), (C3) を満たすと仮定する．

(C1) Galois 表現

$$\rho_1^E \colon G_{K_\infty} := \mathrm{Gal}(\overline{\mathbb{Q}}/K_\infty) \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

は $\mathbb{F}_p$ 上絶対既約である．

(C2) n を正の整数とし，v を K_n^E の有限素点とする．$K_{n,v}^E$ 上の楕円曲線 $E_{K_{n,v}^E}$ が潜在的乗法還元を持つとき，$E(K_{n,v})[p] = 0$ が成り立つ．

(C3) もし E が虚数乗法を持つのであれば，$\overline{\mathbb{Q}}$ 上で定義される E の自己準同型全体のなす環 $\mathrm{End}(E)$ はある虚二次体の整数環である．

このとき，ある正の整数 B が存在して，次が成り立つ:

「任意の正の整数 n に対して，ある R_n 加群の準同型

$$r_n : \mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2} \longrightarrow (A_n^E)^\vee$$

が存在して，$\#\operatorname{Ker} r_n < B$ かつ $\#\operatorname{Coker} r_n < B$ が成り立つ．」

注意 3.3 ((C1) と (C2) についての補足)**.** ここでは，定理 3.2 の条件 (C1), (C2) に関する補足を述べる．

(1) 次の条件 $(\mathrm{C1})_{\mathrm{str}}$ が成り立つとき，(C1) は成り立つ ([4, Proposition 3.1]):

$(\mathrm{C1})_{\mathrm{str}}$ Galois 表現

$$\rho^E = \rho^{E,p} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

は全射である．

E が虚数乗法を持たないときは，Serre の “open image theorem” ([15]) により，有限個を除くすべての素数 p で ρ^E は全射になる．一方，E が虚数乗法を持つ場合は，ρ^E は決して全射にならない．

(2) $\mathbb{Q}$ 上の任意の楕円曲線 E と E が良い還元を持つような任意の奇素数 p に対して，適切に E の二次ひねり $E'/\mathbb{Q}$ をとると (E', p) が条件 (C2) を満たす ([4, Proposition 3.2] 参照)．

注意 3.4. (E, p) が条件 (C1) を満たしているとき，法 p Galois 表現

$$\rho_1^E|_{G_{K_\infty}} \colon G_{K_\infty} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(E[p]) = \mathrm{GL}_2(\mathbb{F}_p)$$

から誘導される環準同型 $\mathbb{Z}_p[G_{K_\infty}] \longrightarrow M_2(\mathbb{F}_p)$ は全射である．従って，有限生成 $\mathbb{Z}_p$ 加群に関する中山の補題より，条件 (C1) の下では，(3.1) から誘導される自然な写像

$$(\rho_n^E)^\vee \colon \mathbb{Z}_p[G_{K_n}]^{\mathrm{op}} \longrightarrow M_2(\mathbb{Z}/p^n\mathbb{Z})$$

が全射になり，これにより自然な写像

$$\mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]) \longrightarrow (M_2(\mathbb{Z}/p^n\mathbb{Z}), (\rho_n^E)^\vee) \otimes_{\mathbb{Z}[\mathrm{Gal}(K_n^E/K_n)]} \mathrm{Cl}(\mathcal{O}_{K_n^E}[1/p]) = A_n^E$$

も全射になる．特に，条件 (C1) の下では，A_n^E はイデアル類群 $\mathrm{Cl}(\mathcal{O}_{K_n^E})$ の剰余群と見なせる．

注意 3.5. 詳細には立ち入らないが，D. Prasad 氏と S. Shekhar は論文 [11] で

$$\mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_1^E/\mathbb{Q})]}(\mathrm{Cl}(\mathcal{O}_{K_1^E}) \otimes_{\mathbb{Z}} \mathbb{F}_p, E[p]) \tag{3.3}$$

と $\mathrm{Sel}_p(\mathbb{Q}, E[p])$ の関係について研究している．組 (E, p) が $E(\mathbb{Q}_p)[p] = \{0\}$ を満たすときは，本稿で定義した A_1^E の自明指標 $\mathbf{1}$ $(\in \widehat{\Delta})$ 成分の Pontrjagin 双対 $(A_{1,\mathbf{1}}^E)^\vee$ は，(3.3) を 2 つ直和した $\mathbb{F}_p$ 上のベクトル空間と同型になる[*2]．

[*2] この事実は以下の議論により確認できる．右 $\mathbb{F}_p[\mathrm{Gal}(K_1^E/\mathbb{Q})]$ 加群の同型 $(M_2(\mathbb{F}_p), (\rho_1^E)^\vee) \simeq$

4　主定理の証明の概要

本節では，前節で紹介した本稿および [4] の主定理，すなわち定理 3.2 の証明の概要を簡単に述べる．各 $n \in \mathbb{Z}_{>0}$ に対して，Galois コホモロジーの制限写像

$$\mathrm{res}_n \colon H^1(K_n, E[p^n]) \longrightarrow H^0(K_n, H^1(K_n^E, E[p^n]))$$

から R_n 加群の準同型

$$\mathrm{res}_n^{\mathrm{Sel}} \colon \mathrm{Sel}_p(K_n, E[p^n]) \longrightarrow H^0(K_n, \mathrm{Sel}_p(K_n^E, E[p^n]))$$

が誘導される．定理 3.2 は次の (A), (B) を示すことで証明できる．

(A) 組 (E, p) が条件 (C1), (C2), (C3) を満たすとき，ある正の整数 B_1 が存在して，任意の正の整数 n に対して，$\#\operatorname{Ker}\mathrm{res}_n < B_1$ かつ $\#\operatorname{Coker}\mathrm{res}_n < B_1$ が成り立つ．

(B) 組 (E, p) が条件 (C2) を満たすとき，ある正の整数 B_2 が存在して，次が成り立つ:

「任意の正の整数 n に対して，ある R_n 加群の準同型

$$s_n \colon H^0(K_n, \mathrm{Sel}_p(K_n^E, E[p^n]))^{\oplus 2} \longrightarrow (A_n^E)^\vee$$

が存在して，$\#\operatorname{Ker} s_n < B_2$ かつ $\#\operatorname{Coker} s_n < B_2$ が成り立つ．」

(A) の証明について

大域体および局所体の Galois コホモロジーの計算を通して，写像 $\mathrm{res}_n^{\mathrm{Sel}}$ の核と余核の位数を抑えることで (A) を示す．まず，Galois コホモロジーの膨張・制限

$(E[p]^\vee)^{\oplus 2}$ により，$\mathbb{F}_p$ 上のベクトル空間の同型

$$(A_1^E)^\vee \simeq \mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_1^E/\mathbb{Q})]}(\mathrm{Cl}(\mathcal{O}_{K_1^E}[1/p]) \otimes_{\mathbb{Z}} \mathbb{F}_p, E[p])^{\oplus 2}$$

を得る．p の上にある $\mathcal{O}_{K_1^E}$ の素イデアル $\mathfrak{p}$ を 1 つとり，$\mathfrak{p}$ における $\mathrm{Gal}(K_1^E/\mathbb{Q})$ の分解群 $D_{\mathfrak{p}}$ を考える．$D_{\mathfrak{p}}$ の $[\mathfrak{p}] \otimes 1 \in \mathrm{Cl}(\mathcal{O}_{K_1^E}) \otimes_{\mathbb{Z}} \mathbb{F}_p$ への作用（自明）と，$D_{\mathfrak{p}}$ の $E[p]$ への作用を比較することで，次の自然な同型を得る:

$$\begin{aligned}&\mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_1^E/\mathbb{Q})]}(\mathrm{Cl}(\mathcal{O}_{K_1^E}[1/p]) \otimes_{\mathbb{Z}} \mathbb{F}_p, E[p]) \\ &\xrightarrow{\simeq} \mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_1^E/\mathbb{Q})]}(\mathrm{Cl}(\mathcal{O}_{K_1^E}) \otimes_{\mathbb{Z}} \mathbb{F}_p, E[p]).\end{aligned}$$

よって所望の同型 $(A_n^E)^\vee \simeq \mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(K_1^E/\mathbb{Q})]}(\mathrm{Cl}(\mathcal{O}_{K_1^E}) \otimes_{\mathbb{Z}} \mathbb{F}_p, E[p])^{\oplus 2}$ を得る．

(inflation-restriction) 完全列と大域体の Galois コホモロジーに関する次の命題から，制限写像 res_n の核と余核の有界性が従う．

命題 4.1 ([4, Proposition 5.1])**.** 組 (E,p) が条件 (C1) および (C3) を満たすとき，各 $i \in \{1,2\}$ に対して，$\{\#H^i(K_n^E/K_n, E[p^n])\}_{n\geq 0}$ は有界である．

制限写像 res_n の核の有界性から，$\mathrm{res}_n^{\mathrm{Sel}}$ の核の有界性が従う．更に，制限写像 res_n の余核の有界性と局所体の Galois コホモロジーに関する次の補題から，$\mathrm{res}_n^{\mathrm{Sel}}$ の余核の有界性が従う．

補題 4.2 ([4, Proposition 5.11])**.** 「任意の $m \in \mathbb{Z}_{\geq 0}$ に対して，E_{K_m} は ℓ の上にある K_m のある素点で悪い還元を持つ」という条件を満たす素数 ℓ 全体の集合を Σ_0^0 とおく．各正の整数 n および K_n の各素点 v に対して，次の写像を考える:

$$\mathrm{res}_{n,v}^{\mathrm{loc}} \colon H^1(K_{n,v}, E[p^n]) \longrightarrow H^0\left(K_n, \prod_{w|v} H^1(K_{n,w}^E, E[p^n])\right),$$

$$\mathrm{res}_{n,v}^{f} \colon H_f^1(K_{n,v}, E[p^n]) \longrightarrow H^0\left(K_n, \prod_{w|v} H_f^1(K_{n,w}^E, E[p^n])\right)$$

E が p で良い還元を持ち，組 (E,p) が条件 (C2) を満たすとき，次が成り立つ．

(1) 任意の $\ell \in \Sigma_0^0$ に対して，$\{\#\operatorname{Ker}(\mathrm{res}_{n,v}^{\mathrm{loc}}) \mid n \geq 0, v \mid \ell\}$ は有界である．
(2) $\{\#\operatorname{Ker}(\mathrm{res}_{n,v}^{\mathrm{loc}}) \mid n \geq 0, v \mid p\}$ は有界である．
(3) 任意の $\ell \in \Sigma_0^0$ に対して，$\{\#\operatorname{Coker}(\mathrm{res}_{n,v}^{f}) \mid n \geq 0, v \mid \ell\}$ は有界である．

補題 4.2 (1), (3) の証明では，E が素点 v が潜在的に良い還元を持つか，潜在的に乗法還元を持つかで場合分けして考える．条件 (C2) は，潜在的に乗法還元を持つような素点 v での $\operatorname{Ker}(\mathrm{res}_{n,v}^{\mathrm{loc}})$ および $\#\operatorname{Coker}(\mathrm{res}_{n,v}^{f})$ の位数の有界性を保証するために課された条件である．補題 4.2(2) の証明では，E が p で通常還元を持つか，超特異還元を持つかで場合分けして考える．通常還元を持つ場合は今井の定理 [6] を用い，超特異還元を持つ場合は $E[p]$ への $G_{\mathbb{Q}_p}$ の惰性群 $I_{\mathbb{Q}_p}$ の作用の表示を用いることで，$\mathrm{res}_{n,v}^{\mathrm{loc}}$ の位数の有界性を示す．

(B) の証明について

各正の整数 n に対して，

$$S_n^E := \operatorname{Hom}_{\mathbb{Z}_p}(\operatorname{Cl}(\mathcal{O}_{K_n^E}[1/p]) \otimes_{\mathbb{Z}} \mathbb{Z}_p, E[p^n])$$

と定める．このとき，右 $\mathbb{Z}_p[\mathrm{Gal}(K_n^E/K_n)]$ 加群の同型

$$(M_2(\mathbb{Z}/p^n\mathbb{Z}), (\rho_n^E)^\vee) \simeq (E[p^n]^\vee)^{\oplus 2}$$

により，R_n 加群の同型 $H^0(K_n, S_n^E)^{\oplus 2} \simeq (A_n^E)^\vee$ が得られる．$G_{K_n^E}$ は $E[p^n]$ に自明に作用するので，類体論より，S_n^E は自然に「不分岐局所条件 H^1_{ur}」に関する精 Selmer 群，すなわち，自然な写像

$$H^1(K_n^E, E[p^n]) \longrightarrow \prod_{v \nmid p\infty} H^1(K_{n,v}^{E,\mathrm{ur}}, E[p^n]) \times \prod_{w|p} H^1(K_{n,w}^{E,\mathrm{ur}}, E[p^n])$$

の核と同型である．拡大塔 $K_\infty/\mathbb{Q}$ に沿って考えるとき，条件 (C2) の下では，「$\mathrm{Sel}_p(K_n^E, E[p^n])$ を定める局所条件 H^1_{cl} $(= H^1_f$, Bloch–Kato の局所条件 [1]) と S_n^E を定める局所条件 H^1_{ur} のずれ」が有界であることを示すことが出来る ([4, §5.3]). これにより，(B) が得られる．

5 A_n^E の群構造の漸近挙動

本節では，定理 3.2 を用いて $\mathbb{Z}_p$ 加群 A_n^E の構造の漸近的挙動を記述しよう．まず，PID 上の有限生成加群の構造定理から定まる不変量を導入する．

定義 5.1. M を有限生成ねじれ $\mathbb{Z}_p$ 加群とする．このとき，構造定理より，ある正の整数の有限減少列 $\{e_j\}_{j=1}^s \subseteq \mathbb{Z}_{>0}$ が（ただ 1 つ）存在して，$\mathbb{Z}_p$ 加群の同型

$$M \simeq \bigoplus_{j=1}^{s} \mathbb{Z}_p/p^{e_j}\mathbb{Z}_p$$

が成り立つ．各非負整数 i に対して，次のように定める:

$$\Phi_i(M) := \begin{cases} \displaystyle\sum_{j=i+1}^{s} e_j & (0 \le i < s), \\ 0 & (i \ge s). \end{cases}$$

注意 5.2. $\{\Phi_i(M)\}_{i\ge 0}$ の定義より，次が成り立つ．

(1) $\{\Phi_i(M)\}_{i\ge 0}$ は非負整数の減少列である．
(2) $\Phi_0(M) = \mathrm{ord}_p(\#M)$ が成り立つ．
(3) 数列 $\{\Phi_i(M)\}_{i\ge 0}$ から数列 $\{e_j\}_{j=1}^s \subseteq \mathbb{Z}_{>0}$ が復元できるので，数列 $\{\Phi_i(M)\}_{i\ge 0}$ から $\mathbb{Z}_p$ 加群 M の同型類が決定できる．

注意 5.3. 本稿では詳細に立ち入らないが，[4] では $\mathbb{Z}_p$ 加群 M の高次 Fitting イデアルを用いて $\{\Phi_i(M)\}_{i\geq 0}$ を定義している ([4, Definition 2.6] 参照).

不変量 $\Phi_i(M)$ は次のような性質を持つ.

補題 5.4 ([4, Lemma 2.8] 参照)**.** 有限生成ねじれ $\mathbb{Z}_p$ 加群の間の準同型の列

$$\{f_n \colon M_n \longrightarrow M'_n\}_{n>0}$$

を考える．$\{\#\operatorname{Ker} f_n\}_{n>0}$ と $\{\#\operatorname{Coker} f_n\}_{n>0}$ がともに有界であるとき，任意の $i \in \mathbb{Z}_{\geq 0}$ に対して，$\Phi_i(M_n) \sim \Phi_i(M'_n)$ が成り立つ.

指標 $\chi \in \widehat{\Delta}$ を任意にとる．このとき，$\mathbb{Z}_p$ 加群としての（標準的でない）同型

$$(A^E_{n,\chi^{-1}})^\vee = \operatorname{Hom}_{\mathbb{Z}_p}(A^E_{n,\chi^{-1}}, \mathbb{Z}/p^n\mathbb{Z}) \simeq A^E_{n,\chi}$$

が存在するので，任意の $i \in \mathbb{Z}_{\geq 0}$ に対して，$\Phi_i(A^E_{n,\chi}) = \Phi_i((A^E_{n,\chi^{-1}})^\vee)$ が成り立つ．同様に，$\Phi_i(A^E_n) = \Phi_i((A^E_n)^\vee)$ も成り立つ．従って，定理 3.2 と補題 5.4 より，次の系を得る.

系 5.5. E を $\mathbb{Q}$ 上の楕円曲線とし，p を E が良い還元を持つような素数とする．組 (E,p) が条件 (C1), (C2), (C3) を満たすとする．$i \in \mathbb{Z}_{\geq 0}$ を任意の非負整数とする．このとき，

$$\Phi_i(A^E_n) = \Phi_i((A^E_n)^\vee) \sim \Phi_i\left(\operatorname{Sel}_p(K_n, E[p^n])^{\oplus 2}\right)$$

が成り立ち，更に任意の指標 $\chi \in \widehat{\Delta}$ に対して

$$\Phi_i(A^E_{n,\chi}) = \Phi_i((A^E_{n,\chi^{-1}})^\vee) \sim \Phi_i\left(\operatorname{Sel}_p(K_n, E[p^n])^{\oplus 2}_{\chi^{-1}}\right),$$

が成り立つ.

6 「岩澤の類数公式」型の漸近公式

ここでは，定理 3.2 から従う A^E_n の位数に関する「岩澤の類数公式」型の漸近公式を紹介する.

まず，岩澤理論に関連する記号をいくつか用意しよう．各 $m \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ に対して，$K_m := \mathbb{Q}(\mu_{p^m})$ とおき，$m_2 > m_1$ を満たす $m_1, m_2 \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ に対して，$\mathcal{G}_{m_2,m2_1} := \operatorname{Gal}(K_{m_2}/K_{m_1})$ と定めていたことを思い出そう．以下では，

$$\Gamma := \mathcal{G}_{\infty,1} = \operatorname{Gal}(K_\infty/K_1)$$

と書く．このとき，標準的でない同型 $\Gamma \simeq \mathbb{Z}_p$ が存在する．以下では，位相的生成元 $\gamma \in \Gamma$ を 1 つ固定する．

完備群環 $\Lambda := \mathbb{Z}_p[\![\Gamma]\!] := \varprojlim \mathbb{Z}_p[\mathcal{G}_{m,1}]$ を考える．位相的生成元 $\gamma \in \Gamma$ のとり方に応じて，標準的でない位相 $\mathbb{Z}_p$ 代数の同型写像

$$\Lambda \xrightarrow{\simeq} \mathbb{Z}_p[\![T]\!]; \gamma \longmapsto 1+T$$

が定まる．（従って，Λ は UFD である．）正の整数 $m, n \in \mathbb{Z}_{>0}$ に対して，

$$\Lambda_{m,n} := \mathbb{Z}/p^n\mathbb{Z}[\mathcal{G}_{m,1}] \simeq \Lambda/(p^n, \gamma^{p^{m-1}} - 1),$$

と定め，$\Lambda_n := \Lambda_{n,n}$ とおく．直積分解 $\mathcal{G}_{m,0} = \Delta \times \mathcal{G}_{m,1}$ により，$R_{m,n} = \Lambda_{m,n}[\Delta]$ が成り立つことに注意する．

精 Selmer 群に関連する記号を導入しよう．各 $m, n \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$ に対して，

$$X_{m,n} := \mathrm{Sel}_p(K_m, E[p^n])^\vee := \mathrm{Hom}_{\mathbb{Z}_p}\left(\mathrm{Sel}_p(K_m, E[p^n]), \mathbb{Q}_p/\mathbb{Z}_p\right),$$

と定めて，$X_n := X_{n,n}$ と書く．（ここで，$m = \infty$ の場合は

$$\mathrm{Sel}_p(K_\infty, E[p^\infty]) := \varinjlim_m \mathrm{Sel}_p(K_m, E[p^\infty]).$$

と定義する．）各 $\chi \in \widehat{\Delta}$ に対して，$X_{\infty,\chi}$ は有限生成ねじれ Λ 加群であることが知られている ([7]). 従って，$X_{\infty,\chi}$ や X_∞ に対して，次で復習する特性イデアルや岩澤不変量を考えることが出来る．

定義 6.1 (特性イデアル，岩澤不変量)**.** M を有限生成ねじれ Λ 加群とする．このとき，M の特性イデアル $\mathrm{char}_\Lambda(M)$ を次で定義する:

$$\mathrm{char}_\Lambda(M) := \prod_{\mathfrak{p}} \mathfrak{p}^{\ell_{\mathfrak{p}}(M_{\mathfrak{p}})},$$

ここで，右辺の $\mathfrak{p}$ は Λ の高さ 1 のイデアル全体を動き，$\ell_{\mathfrak{p}}(M_{\mathfrak{p}})$ は $\Lambda_{\mathfrak{p}}$ 加群 $M_{\mathfrak{p}}$ の長さを表す．Λ は UFD なので，Λ の高さ 1 のイデアルは単項イデアルであり，従って特性イデアル $\mathrm{char}_\Lambda(M)$ は Λ の単項イデアルである．更に，p 進 Weierstrass の準備定理より，次を満たす非単数根 (distinguished) 多項式 $f(T) \in \mathbb{Z}_p[T]$ がただ 1 つ存在する:

$$\mathrm{char}_\Lambda(M) = p^{\ell_{p\Lambda}(M_{p\Lambda})} f(\gamma - 1)\Lambda.$$

非負整数 $\mu(M) := \ell_{p\Lambda}(M_{p\Lambda})$ を M の岩澤 μ 不変量と呼ぶ．また，$f(T)$ の次数を $\lambda(M)$ と書き，M の岩澤 λ 不変量と呼ぶ.

注意 6.2. M が有限生成ねじれ Λ 加群であるとき,

$$\Phi_0(M \otimes_\Lambda \Lambda_n) = \mathrm{ord}_p\left(\#(M \otimes_\Lambda \Lambda_n)\right) \sim \mu(M)p^n + \lambda(M)n$$

が成り立つ.

以下, $\chi \in \widehat{\Delta}$ を任意にとる. このとき, 円分 $\mathbb{Z}_p$ 拡大に沿った精 Selmer 群のコントロール定理より,

$$\Phi_0(X_{\infty,\chi} \otimes_\Lambda \Lambda_n) \sim \Phi_0(X_{n,\chi}) \sim \Phi_0\left(\mathrm{Sel}_p(K_n, E[p^n])^{\oplus 2}_{\chi^{-1}}\right) \tag{6.1}$$

が成り立つ (例えば [12, Proposition 7.4.4] 参照). $X_{\infty,\chi}$ は有限生成ねじれ Λ であるので, 岩澤不変量を用いることで,

$$\Phi_0(X_{\infty,\chi} \otimes_\Lambda \Lambda_n) \sim \mu(X_{\infty,\chi})p^n + \lambda(X_{\infty,\chi})n$$

を得る. 従って, $i = 0$ の場合の系 5.5 の主張から, 次が得られる.

系 6.3. E を $\mathbb{Q}$ 上の楕円曲線とし, p を E が良い還元を持つような素数とする. 組 (E, p) が条件 (C1), (C2), (C3) を満たすとする. $i \in \mathbb{Z}_{\geq 0}$ を任意の非負整数とする. このとき,

$$\Phi_0(A^E_n) \sim 2\left(\mu(X_\infty)p^n + \lambda(X_\infty)n\right)$$

であり, 更に任意の $\chi \in \widehat{\Delta}$ に対して,

$$\Phi_0(A^E_{n,\chi}) \sim 2\left(\mu(X_{\infty,\chi})p^n + \lambda(X_{\infty,\chi})n\right)$$

が成り立つ.

系 6.3 とイデアル類群の漸近挙動に関する先行研究を比較しよう. 任意の代数体 L に対して

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_p(L, E[p^\infty]) \geq \mathrm{rank}_{\mathbb{Z}} E(L) - [L : \mathbb{Q}]$$

が成り立つことに注意する. (実際, これは精 Selmer 群 $\mathrm{Sel}_p(L, E[p^\infty])$ は $\mathbb{Z}_p$ 加群準同型

$$E(L) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow E(L \otimes_{\mathbb{Q}} \mathbb{Q}_p) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = \prod_{v|p} E(L_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p,$$

の核を含んでいることと,

$$\mathrm{corank}_{\mathbb{Z}_p}\left(\prod_{v|p} E(L_v) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p\right) = \sum_{v|p} [L_v : \mathbb{Q}_p] = [L : \mathbb{Q}]$$

であることから従う．詳細については，例えば，[9, §4.1] の議論を参照せよ．）この不等式と精 Selmer 群に関するコントロール定理と合わせると，任意の $m \in \mathbb{Z}_{\geq 0}$ に対して

$$\lambda(X_\infty) \geq \operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_p(K_m, E[p^\infty]) \geq \operatorname{rank}_{\mathbb{Z}} E(K_m) - \varphi(p^m)$$

が成り立つことが分かる．ここで，φ は Euler 関数を表す．従って，系 6.3 より次が得られる．

系 6.4. E を $\mathbb{Q}$ 上の楕円曲線とし，p を E が良い還元を持つような素数とする．組 (E, p) が条件 (C1), (C2), (C3) を満たすとする．$m, n \in \mathbb{Z}_{\geq 0}$ を非負整数とし，$r_m := \operatorname{rank}_{\mathbb{Z}} E(K_m)$ とおく．このとき，m を固定して $n \to \infty$ とすると

$$\operatorname{ord}_p\left(\#\mathrm{Cl}(\mathcal{O}_{K_n^E})\right) \geq \Phi_0\left(A_n^E\right) \succ 2(r_m - \varphi(p^m))n$$

が成り立つ．

注意 6.5. $m = 0$ のときの系 6.4 の主張は，西来路–山内両氏，平之内氏らの先行研究 ([13], [14], [3]) で得られた漸近的な不等式 (1.1) と一致する．また，$m \geq 0$ のときの系 6.4 の主張は筆者の論文 [9] の主結果を Galois 群 G_{K_m} の p 進表現 $T_p(E) = \varprojlim_n E[p^n]$ に適用して得られる漸近的な不等式と一致する．従って，本稿および [4] の主結果，特に本稿の定理 3.2 系 6.3 は次の意味で先行研究の精密化になっている:

- 系 6.3 からイデアル類群 $\mathrm{Cl}(\mathcal{O}_{K_n^E})$ の商 A_n^E の位数の漸近的挙動を（下界を与えるだけでなく）決定することが出来る．
- 定理 3.2 は A_n^E の位数だけでなく，R_n 加群としての構造（特に $\mathbb{Z}_p$ 加群としての構造）も記述している．

本節の最後に，具体例を 1 つ挙げておこう．

例 6.6. E を方程式 $y^2 + y = x^3 - 7x + 6$, で定義される $\mathbb{Q}$ 上の楕円曲線 (LMFDB label 5077.a1, Cremona ラベル 5077a1) とし，$p := 7$ とする．このとき，次が成り立つことが知られている ([8]):

(i) E は虚数乗法を持たず，(E, p) は条件 $(\mathrm{C1})_{\mathrm{str}}$ を満たす．
(ii) E の導手は 5077（素数）であり，E は 5077 において非分裂乗法還元を持つ．
(iii) Mordell–Weil 群 $E(\mathbb{Q})$ の階数は 3 である．
(iv) 円分 $\mathbb{Z}_7$ 拡大 $\mathbb{Q}_\infty/\mathbb{Q}$ に沿った古典的な Selmer 群の Pontrjagin 双対の定める岩澤加群 $\widetilde{X} := \mathrm{Sel}(\mathbb{Q}_\infty, E[7^\infty])^\vee$ に対して，$\mu(\widetilde{X}) = 0$ および $\lambda(\widetilde{X}) = 3$ が成り立つ．

性質 (iii) および (iv) より $\mathrm{char}_\Lambda(\widetilde{X}) = (\gamma-1)^3\Lambda$ が成り立つ．これにより，更に $\mathrm{char}_\Lambda(X_{\infty,\mathbf{1}}) = (\gamma-1)^2\Lambda$ も成り立つ (例えば, [17, VI.10] 参照)．従って, $\mu(X_{\infty,\mathbf{1}}) = 0$ および $\lambda(X_{\infty,\mathbf{1}}) = 2$ が成り立つ．また，E の性質 (ii) および $p \equiv 3 \bmod 4$ であること，$-p$ が法 5077 で平方剰余であることを用いて，組 $(E, 7)$ が (C2) も満たしていることも示せる ([4, Proposition 3.6, Example 3.7])．従って，$\Phi_0(A^E_{n,\mathbf{1}}) \sim 2n$ が成り立つ．

7　岩澤主予想と漸近公式

楕円曲線の岩澤主予想の下で，X_∞ の特性イデアルは（従って $\mu(X_\infty)$ と $\lambda(X_\infty)$ は）Beilinson–加藤元の Euler 系を用いて記述される．

楕円曲線の岩澤主予想には様々な同値な言い換えがあるが，ここでは，本稿の内容と直接関係している，Beilinson–加藤元を用いた楕円曲線の岩澤主予想の定式化を思い出そう．各非負整数 $q \in \mathbb{Z}_{\geq 0}$ に対して，

$$\mathbf{H}^q = \mathbf{H}^q(T_p(E)) := \varprojlim_m H^1\left(K_m, T_p(E)\right)$$

と定める．ここでは定義の詳細には触れないが，加藤和也氏は論文 [7] で Beilinson–加藤元の Euler 系を構成し，Beilinson–加藤元のなす $\mathbf{H}^1$ の部分 Λ 加群 Z を定義した．（Λ 加群 Z の定義については，f_E を楕円曲線 E に付随する重さ 2 の尖点形式とし，f_E に付随する p 進 Galois 表現

$$T = T_p(E) \subseteq V_{\mathbb{Q}_p}(f_E) := T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

を考えたうえで，[7, Theorem 12.6] を参照せよ．）$\chi \in \widehat{\Delta}$ とする．次の等式が成り立つだろうという予想が，(E, p, χ) の岩澤主予想である:

$$\mathrm{char}_\Lambda(\mathbf{H}^2_\chi) = \mathrm{char}_\Lambda(\mathbf{H}^1_\chi/Z_\chi). \tag{7.1}$$

([7, Theorem 12.6] を踏まえて [7, Conjecture 12.10] を参照せよ.) 今，E は p で良い還元を持つので，等式 (7.1) の左辺に関して，

$$\mathrm{char}_\Lambda(X_{\infty,\chi}) = \mathrm{char}_\Lambda(\mathbf{H}^2_\chi)$$

が成り立つ．実際，これは次から従う．

- Poitou–Tate 完全列の極限を取ることで，X_∞ は $\Lambda[\Delta]$ 加群

$$\mathbf{H}^2(T_p(E))_0 := \mathrm{Ker}\left(\mathbf{H}^2 \longrightarrow \mathbf{H}^2_{\mathrm{loc}} := \varprojlim_m H^1(\mathbb{Q}_p(\mu_{p^m}), T_p(E))\right)$$

と同型であることが分かる．（例えば [10, Proposition 3.17] を参照せよ．）

- E は p で良い還元を持つので，Galois コホモロジーの局所双対定理と，今井の定理 [5] より，$\mathbf{H}^2_{\mathrm{loc}}$ の位数は有限であり，従って $\mathbf{H}^2(T_p(E))$ における $\mathbf{H}^2(T_p(E))_0$ の指数は有限である．

加藤氏は Euler 系の理論を用いることで，条件 $(\mathrm{C1})_{\mathrm{str}}$ の下で成り立つ次の条件 $(*)$ の下で，任意の $\chi \in \widehat{\Delta}$ に対して等式 (7.1) の片側

$$\mathrm{char}_\Lambda(\mathbf{H}^2_{0,\chi}) \supseteq \mathrm{char}_\Lambda(\mathbf{H}^1_\chi/Z_\chi) \tag{7.2}$$

が成り立つことを証明した:

$(*)$ Galois 表現

$$\rho^E|_{G_{K_\infty}} : G_{K_\infty} \longrightarrow \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

の像は $\mathrm{SL}_2(\mathbb{Z}_p)$ を含む．

([7, Theorem 13.4] を参照せよ．その際に，条件 $(\mathrm{C1})_{\mathrm{str}}$ から [7, Theorem 13.4] の条件 (3) が従うことに注意せよ.) 従って，系 6.3 から次が得られる．

系 7.1. E を奇素数 p で良い還元を持つ $\mathbb{Q}$ 上の楕円曲線とする．

(1) 組 (E,p) が条件 $(\mathrm{C1})_{\mathrm{str}}$ および (C2) を満たすとき，次が成り立つ:

$$\Phi_0(A^E_n) \prec 2\bigg(\mu(\mathbf{H}^1/Z)p^n + \lambda(\mathbf{H}^1/Z)n\bigg).$$

(2) 組 (E,p) が条件 (C1), (C2), (C3) を満たすとする．$\chi_0 \in \widehat{\Delta}$ とする．(E,p,χ_0) に関する岩澤主予想が成り立つとき，次が成り立つ:

$$\Phi_0(A^E_{n,\chi_0}) \sim 2\bigg(\mu(\mathbf{H}^1_{\chi_0}/Z_{\chi_0})p^n + \lambda(\mathbf{H}^1_{\chi_0}/Z_{\chi_0})n\bigg).$$

特に，任意の $\chi \in \widehat{\Delta}$ に対して (E,p,χ) に関する岩澤主予想が成り立つとき，

$$\Phi_0(A^E_n) \sim 2\bigg(\mu(\mathbf{H}^1/Z)p^n + \lambda(\mathbf{H}^1/Z)n\bigg)$$

が成り立つ．

Δ の自明指標を $\mathbf{1} \in \widehat{\Delta}$ と書く．C. Skinner 氏と E. Urban 氏は論文 [16] において，以下の条件の下で，加藤氏によって得られた (7.2) と逆向きの包含関係を示すことで，$(E,p,\mathbf{1})$ に関する岩澤主予想を証明した ([16, Theorem 3.33]):

- 組 (E,p) は条件 $(\mathrm{C1})_{\mathrm{str}}$ を満たす.
- 楕円曲線 E は p で良い通常還元を持つ.
- E が乗法還元を持つような素数 ℓ_0 が存在する.

これらの条件は，E が至る所半安定還元を持ち，$p \geq 11$ であり，E が p で良い通常還元を持つときは満たされている ([16, Theorem 3.34] 参照)．従って，次の系を得る．

系 7.2. E を至る所半安定還元を持つ $\mathbb{Q}$ 上の楕円曲線とする．p を 11 以上の素数とし，E は p で良い通常還元を持つと仮定する．(E,p) が条件 (C2) を満たすとき，

$$\Phi_0(A^E_{n,\mathbf{1}}) \sim 2\Big(\mu(\mathbf{H}^1_{\mathbf{1}}/Z_{\mathbf{1}})p^n + \lambda(\mathbf{H}^1_{\mathbf{1}}/Z_{\mathbf{1}})n\Big)$$

が成立する.

謝辞

RIMS 共同研究 (公開型)「代数的整数論とその周辺」2021 での講演と本稿の執筆の機会を下さったプログラム委員の小林真一氏，加塩朋和氏，星明考氏と，本稿執筆にあたり大変有意義なご助言を賜りました平之内俊郎氏にこの場を借りて感謝の意を申し上げます．本研究は JSPS 科研費 18H05233, 20K14295, 21K18577 の助成を受けています.

参考文献

[1] Bloch, S. and Kato, K., *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, 333–400, Progr. Math. **86**, Birkhüser Boston, Boston, MA, 1990.

[2] Garnek, J., *On class numbers of division fields of abelian varieties*, J. Théor. Nombres Bordeaux, **31** (2019), no. 1, 227–242.

[3] Hiranouchi, T., *Local torsion primes and the class numbers associated to an elliptic curve over* $\mathbb{Q}$, Hiroshima Math. J. **49** (2019), no. 1, 117–128.

[4] Hiranouchi, T. and Ohshita, T., *Asymptotic behavior of class groups and cyclotomic Iwasawa theory of elliptic curves*, preprint (2022), arXiv:2203.16039.

[5] Imai, H., *A remark on the rational points of abelian varieties with values in cyclotomic* $\mathbb{Z}_p$*-extensions*, Proc. Japan Acad. **51** (1975), 12–16.

[6] Iwasawa, K., *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.

[7] Kato, K., *p-adic Hodge theory and values of zeta functions of modular forms*, no. 295, 2004, Cohomologies p-adiques et applications arithmétiques. III, pp. ix, 117–290.

[8] The LMFDB Collaboration, *The L-functions and modular forms database*, Elliptic curve with LMFDB label `5077.a1` (Cremona label `5077a1`), `https://www.lmfdb.org/EllipticCurve/Q/5077/a/1`, [Online; accessed 21 March 2022].

[9] Ohshita, T., *Asymptotic lower bound of class numbers along a Galois representation*, J. Number Theory **211** (2020), 95–112.

[10] ———, *On higher Fitting ideals of certain Iwasawa modules associated with Galois representations and Euler systems*, Kyoto J. Math. **61** (2021), no. 1, 1–95.

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

[12] Rubin, K., *Euler systems*, Hermann Weyl lectures, Ann. of Math. Studies, vol. **147**, Princeton Univ. Press (2000).

[13] Sairaiji, F. and Yamauchi, T., *On the class numbers of the fields of the p^n-torsion points of certain elliptic curves over $\mathbb{Q}$*, J. Number Theory **156** (2015), 277–289.

[14] ———, *On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$*, J. Théor. Nombres Bordeaux **30** (2018), no. 3, 893–915.

[15] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (4) (1972), 259–331.

[16] Skinner, C. and Urban, E., *The Iwasawa Main Conjectures for* GL_2, Invent. Math. **195** (2014), 1–277.

[17] Wuthrich, C, *The fine Selmer group and height pairings*, Ph.D. thesis, University of Cambridge, UK, 2004.