岩澤理論の楕円曲線の数論への応用

松野 一夫 (東京都立大学)

本稿では, 楕円曲線の数論における重要な未解決問題である Birch, Swinnerton-Dyer 予想に関してこれまでに得られている結果と (拡張, 一般化された) 岩澤理論との関連を, Coates-Wiles や Rubin の結果を中心に概説する. その他の関連する結果に関しては §4 で簡単に触れる. なお, 本稿を通じての参考文献として [deS], [Rub5], [Gre2] を挙げておく.

1 楕円曲線と Birch, Swinnerton-Dyer 予想

1.1 楕円曲線

F を体とする.

定義 1.1. F 上で定義された種数 1 の非特異代数曲線 E で, F-有理点の集合 $E(F)$ が空集合でないようなものを (F 上の) 楕円曲線と呼ぶ.

楕円曲線は次の形の model を持つ.

命題 1.2. F 上の任意の楕円曲線 E は

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

という方程式で定義される射影平面上の非特異曲線と同型になる. 逆に, この形の方程式で定まる射影曲線で非特異なものは楕円曲線となる.

注. (1) の斉次化

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

は $(X:Y:Z) = (0:1:0)$ という解を常に持つので, (1) で定義される射影曲線は必ず (無限遠に) F-有理点を持つ.

(1) は楕円曲線 E の Weierstrass 方程式と呼ばれ, (1) で定義される射影平面上の曲線を E の Weierstrass model と呼ぶ. 与えられた楕円曲線に対する Weierstrass model の取り方は一意的ではなく, F の標数が 2 でないならば $a_1 = a_3 = 0$ であるような model が取れる. (標数が 3 でもなければ更に $a_2 = 0$ ともできる.) (1) で定義される曲線 E が非特異となるのは, 係数 $a_1, \cdots, a_6$ から定まる E の判別式 Δ_E (定義は [Sil1, Chap. III] などを参照) が 0 でないときと書ける. $a_1 = a_3 = 0$ の時には右辺の x の 3 次式が重根を持たないことと同値である.

以下, E を F 上の楕円曲線とする. 種数 g の代数曲線に対してヤコビ多様体と呼ばれる g 次元のアーベル多様体が定まるが (八森氏の稿参照), 楕円曲線は種数が 1 なのでそのヤコビ多様体は 1 次元, つまり再び曲線になる.

命題 1.3. E とそのヤコビ多様体 $\mathrm{Jac}(E)$ は F 上で同型である. 特に E は F 上のアーベル多様体であり, F の任意の拡大体 F' に対し, $E(F')$ にはアーベル群の構造が入る.

(1) で定義された楕円曲線では, 無限遠にある有理点を単位元とし,

$$P_1+P_2+P_3=0 \iff 3\text{ 点 }P_1,P_2,P_3\text{ が同一直線上にある}$$

となるように群演算が定められる.

例. $F=\mathbb{C}$ のとき, ある格子 $L\subset\mathbb{C}$ が存在して $\mathbb{C}/L\cong E(\mathbb{C})$ となる.

例. F が有限体なら $E(F)$ は有限アーベル群, $E(\overline{F})$ は torsion アーベル群.

定義 1.4. E 上の n 倍写像を $[n]$ と書き, $E[n]:=\mathrm{Ker}([n])\subset E(\overline{F})$ と表す. $E_{\mathrm{tors}}:=\bigcup_n E[n]$ と書く. 更に $E(F)[n]=E[n]\cap E(F)$, $E(F)_{\mathrm{tors}}=E_{\mathrm{tors}}\cap E(F)$ といった記号も用いる.

命題 1.5. p を素数, $i\geq 1$ とする. そのとき

$$E[p^i]\cong\begin{cases}\mathbb{Z}/p^i\mathbb{Z}\oplus\mathbb{Z}/p^i\mathbb{Z} & \mathrm{ch}(F)\neq p\\ \mathbb{Z}/p^i\mathbb{Z}\text{ または }\{0\} & \mathrm{ch}(F)=p.\end{cases}$$

特に F の標数が 0 のとき $E_{\mathrm{tors}}\cong\mathbb{Q}/\mathbb{Z}\oplus\mathbb{Q}/\mathbb{Z}$.

注. F が標数 p の有限体のとき, $E[p]\cong\mathbb{Z}/p\mathbb{Z}$ となるものを ordinary, そうでないものを supersingular な楕円曲線と呼ぶ.

代数体上の楕円曲線の有理点に関しては, 次の有名な Mordell-Weil の定理がある.

定理 1.6 (Mordell-Weil の定理). F が有限次代数体のとき, $E(F)$ は有限生成アーベル群.

具体的に E が与えられたときに, $E(F)$ の torsion 部分を求めることは難しくないが, 自由部分の rank や生成元を求めるのは大変で, (確実に決定できる) アルゴリズムも今のところない. Birch, Swinnerton-Dyer 予想はその rank に関する予想である.

1.2 楕円曲線の L 関数

E を $\mathbb{Q}$ 上の楕円曲線とする. E の整数係数の Weierstrass model の中で判別式が最小のものを E の (global) minimal Weierstrass model と呼ぶ ([Sil1, Chap.VIII] 参照).

定義 1.7. p を素数とする. E の minimal Weierstrass model を modulo p して得られる $\mathbb{F}_p$ 上の曲線 $\widetilde{E}_p$ が再び非特異となるとき, E は p で good reduction を持つと言う. そうでない (bad reduction を持つ) とき, 特異点の種類によって (split または non-split) multiplicative reduction, additive reduction を持つと言う ([Sil1, Chap.III, VII] 参照).

定義 1.8. 次の Euler 積で定義される Dirichlet 級数 $L(E,s)$ を楕円曲線 E の (Hasse-Weil の) L 関数と呼ぶ:

$$L(E,s) = \prod_{p:\text{good}} (1 - a_p p^{-s} + p^{1-2s})^{-1} \times \prod_{p:\text{bad}} (1 - a_p p^{-s})^{-1}.$$

ただし素数 p に対し $a_p \in \mathbb{Z}$ は以下のように定める:

$$a_p := \begin{cases} 1 + p - \#\widetilde{E}_p(\mathbb{F}_p) & E \text{ は } p \text{ で good reduction,} \\ 1 & E \text{ は } p \text{ で split multiplicative reduction,} \\ -1 & E \text{ は } p \text{ で non-split multiplicative reduction,} \\ 0 & E \text{ は } p \text{ で additive reduction.} \end{cases}$$

次の Hasse の定理により, Dirichlet 級数 $L(E,s)$ は $\mathrm{Re}(s) > \frac{3}{2}$ で絶対収束し, その範囲で正則関数となることがわかる.

定理 1.9 (Hasse). 任意の p に対し $|a_p| < 2\sqrt{p}$ が成り立つ.

更に次が予想されていた.

予想 1.10. $L(E,s)$ は $\mathbb{C}$ 全体に正則に解析接続される. 更に

$$\Lambda(E,s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$$

と置くとき, 関数等式

$$\Lambda(E,s) = w_E \Lambda(E, 2-s) \quad (w_E = \pm 1)$$

が成り立つ. ただし N_E は E の conductor (定義は [Sil2, Chap.IV] など参照).

重さ 2 の cuspform に付随する L 関数は $\mathbb{C}$ 全体に解析接続され, 上の形の関数等式を満たすので, 予想 1.10 は最終的に [BCDT] で解決された谷山志村予想から従う.

予想 1.11 (谷山志村予想). $\mathbb{Q}$ 上の任意の楕円曲線 E は modular である. すなわち $L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ と書くとき, $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ は重さ 2, level N_E の cuspform となる.

定理 1.12 (Wiles,$\cdots$,[BCDT]). 予想 1.11 は正しい. 従って予想 1.10 も正しい.

1.3 Birch, Swinnerton-Dyer 予想

Birch, Swinnerton-Dyer 予想とは代数体上の楕円曲線から, Mordell-Weil 群のように算術的, 代数的に定義される対象と, Hasse-Weil L 関数のように解析的に定義される対象という, 全く異なる世界に属するものの間に実は密接な関係があるであろうという予想である. ここでは有理数体上の楕円曲線の場合のみを見る.

予想 1.13 (Birch, Swinnerton-Dyer 予想). E を $\mathbb{Q}$ 上の楕円曲線とする.

(i) $E(\mathbb{Q})$ の rank は $L(E,s)$ の $s=1$ での零点の位数と等しい. すなわち

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L(E,s).$$

(ii) $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ とするとき, 次の等式が成り立つ.

$$\frac{\lim_{s\to 1}(s-1)^{-r} L(E,s)}{\Omega_E} = \frac{\#Ш(E/\mathbb{Q}) R(E/\mathbb{Q}) \prod_l c_l}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}.$$

ただし, 上式に表れている量は以下の通り. (詳細は [Sil1] 等を参照のこと.)

- $\Omega_E = \int_{E(\mathbb{R})} |\omega_E|$ ($\omega_E = \frac{dx}{2y+a_1x+a_3}$: E の不変微分形式).
- $Ш(E/\mathbb{Q})$: $E/\mathbb{Q}$ の Tate-Shafarevich 群 (§3.3, 予想 3.5 参照).
- $R(E/\mathbb{Q}) = \det(\langle P_i, P_j \rangle)$: $E(\mathbb{Q})$ の regulator ($\{P_1, \cdots, P_r\}$: $E(\mathbb{Q})$ の自由部分の生成元, $\langle\ ,\ \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ は height pairing).
- $c_l = [E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)]$ ($E_0(\mathbb{Q}_l)$ は mod l 写像による非特異点たちの逆像).

この予想は Birch と Swinnerton-Dyer によって, 実例計算などを基に予想されたものである ([BSD]).

1.4 虚数乗法を持つ楕円曲線

F を標数 0 の体, E を F 上の楕円曲線とする. そのとき E の F 上の自己準同型環 (E から E への F-isogeny のなす環) $\mathrm{End}_F(E)$ は必ず (定数倍写像として) $\mathbb{Z}$ を含むが, $\mathbb{Z}$ より真に大きくなる場合, $\mathrm{End}_F(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ は虚 2 次体になることが知られている. 即ち,

命題 1.14. $\mathrm{End}_F(E)$ は $\mathbb{Z}$ かまたはある虚 2 次体の order $\mathcal{O}$ と同型.

定義 1.15. $\mathrm{End}_F(E) \cong \mathcal{O} \neq \mathbb{Z}$ のとき, 楕円曲線 E は F 上で $\mathcal{O}$ に虚数乗法 (complex multiplication, CM) を持つという. $\overline{F}$ 上で CM を持つとき, 単に E は CM を持つという言い方もする.

例. 虚 2 次体の order $\mathcal{O}$ は $\mathbb{C}$ 内の格子と思えるが, その格子が定める $\mathbb{C}$ 上の楕円曲線 E は $\mathcal{O}$ に虚数乗法を持つ. 実際, 任意の $\alpha \in \mathcal{O}$ に対し $\alpha\mathcal{O} \subset \mathcal{O}$ であるから, $\mathbb{C}$ での α 倍写像は $\mathbb{C}/\mathcal{O} \cong E(\mathbb{C})$ の自己準同型を与える.

例. Weierstrass 方程式 $y^2 = x^3 + Ax$ および $y^2 = x^3 + B$ ($A, B \in F$) で定義される楕円曲線は, それぞれ ($F(\sqrt{-1})$ および $F(\sqrt{-3})$ 上で) $\mathbb{Z}[\sqrt{-1}]$ および $\mathbb{Z}[\frac{-1+\sqrt{-3}}{2}]$ に *CM* を持つ.

以下, $\mathcal{O}_K$ を虚 2 次体 K の整数環とし, E は代数体 F 上の楕円曲線で $\mathrm{End}_F(E) \cong \mathcal{O}_K$ を満たすものとする. $\mathrm{End}_F(E)$ と $\mathcal{O}_K$ の間の同型を次のように正規化しておく.

定義 1.16. 任意の $\alpha \in \mathcal{O}_K$ に対して $[\alpha] \in \mathrm{End}_F(E)$ を $[\alpha]^* \omega_E = \alpha\omega_E$ となるものとして定める. ただし ω_E は E の不変微分形式.

定義 1.17. $\alpha \in \mathcal{O}_K$ に対し, $[\alpha] : E(\overline{F}) \to E(\overline{F})$ の kernel を $E[\alpha]$ と書く. また, $\mathcal{O}_K$ のイデアル $\mathfrak{a}$ に対し $E[\mathfrak{a}] := \bigcap_{\alpha\in\mathfrak{a}} E[\alpha]$ と置く. 更に

$$E[\alpha^\infty] := \bigcup_i E[\alpha^i], \quad E[\mathfrak{a}^\infty] := \bigcup_i E[\mathfrak{a}^i]$$

といった記号も使う.

注. 単項イデアル $\mathfrak{a} = \alpha\mathcal{O}_K$ に対しては $E[\mathfrak{a}] = E[\alpha]$ となる. 更に任意のイデアル $\mathfrak{a}$ に対し $\mathfrak{a}^k = \alpha\mathcal{O}_K$ となる k を取ると $E[\mathfrak{a}^\infty] = E[\alpha^\infty]$ となる.

虚数乗法論等より得られる結果で後に必要になるものをまとめておく. 定義等の詳細や証明については [deS], [Rub5], [Sil2, Chap.II] などを見よ.

定義 1.18. 虚 2 次体 K の $\mathfrak{m}$ を法とする ray class field を $K(\mathfrak{m})$ と書き, Hilbert 類体 $K(1)$ を H と書く. $K(\mathfrak{m}^\infty) = \bigcup_i K(\mathfrak{m}^i)$ といった記号も使う. $(\mathfrak{a},\mathfrak{m}) = 1$ なるイデアル $\mathfrak{a}$ に対して $(\mathfrak{a}, K(\mathfrak{m})/K) \in \mathrm{Gal}(K(\mathfrak{m})/K)$ を一般に $\sigma_\mathfrak{a}$ と書く.

CM 楕円曲線 E/F に更に次の条件を仮定する:

(G) $F(E_{\mathrm{tors}})$ は K のアーベル拡大.

このとき F も K のアーベル拡大だが, その conductor を $\mathfrak{f}_{F/K}$ とする. また, $\psi_{E/F} : \mathbb{A}_F^\times/F^\times \to \mathbb{C}^\times$ を E に付随する Hecke 指標 ([Rub5, §5], [Sil2, Chap.II,§9] 参照) とするとき, (G) の下では infinity type が $(1,0)$ の Hecke 指標 $\varphi : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ で, $\psi_{E/F} = \varphi \circ N_{F/K}$ となるものが存在する ($N_{F/K}$ は norm, [deS, II.1.4] 参照). φ の conductor を $\mathfrak{f}_\varphi$ とし, $\mathfrak{f} = \mathrm{lcm}(\mathfrak{f}_{F/K}, \mathfrak{f}_\varphi)$ と置く.

命題 1.19. $\mathfrak{a}$ を $\mathcal{O}_K$ のイデアルとするとき, 次が成り立つ.

(i) E の j 不変量を j_E と書くとき $K(j_E) = H = K(1)$. 特に $F \supset H$.

(ii) $\mathcal{O}_K$ 加群として $E[\mathfrak{a}] \cong \mathcal{O}_K/\mathfrak{a}$. 特に $\mathrm{Gal}(F(E[\mathfrak{a}])/F) \subset (\mathcal{O}_K/\mathfrak{a})^\times$.

(iii) $\mathfrak{f}|\mathfrak{a}$ ならば $K(\mathfrak{a}) = F(E[\mathfrak{a}])$.

(iv) $\mathfrak{q}$ を $\mathfrak{a}$ と素な F の素イデアルとする. そのとき E が $\mathfrak{q}$ で good reduction を持つことと $\mathfrak{q}$ が $F(E[\mathfrak{a}^\infty])/F$ で不分岐であることが同値.

2 虚 2 次体のアーベル拡大の岩澤主予想

この節では K を虚 2 次体, $\mathcal{O}_K$ をその整数環とし, p は 5 以上の素数とする. 更に p の上にある K の素イデアル $\mathfrak{p}$ を一つ固定し, その複素共役を $\mathfrak{p}^*$ と書く. (p が $K/\mathbb{Q}$ で分解しなければ $\mathfrak{p} = \mathfrak{p}^*$.)

2.1 虚 2 次体の $\mathbb{Z}_p$ 拡大

虚 2 次体では Leopoldt 予想が明らかに成立するので, K の全ての $\mathbb{Z}_p$ 拡大の合成体は K の $\mathbb{Z}_p^2$ 拡大になることがわかる.

定義 2.1. K の唯一の $\mathbb{Z}_p^2$ 拡大体を $K_\infty^{(2)}$ と書く. ($\mathrm{Gal}(K_\infty^{(2)}/K) \cong \mathbb{Z}_p^2$.)

これより特に, K には無限個の $\mathbb{Z}_p$ 拡大が $K_\infty^{(2)}$ の部分体として存在している. その中のいくつかの代表的な $\mathbb{Z}_p$ 拡大にも記号をつけておくことにする.

$\mathrm{Gal}(K/\mathbb{Q})$ の生成元 σ は $\mathrm{Gal}(K_\infty^{(2)}/K)$ に共役で作用する. そのとき, σ がそれぞれ ± 1 倍で作用するような $\mathrm{Gal}(K_\infty^{(2)}/K)$ の部分群を $\Gamma^\pm$ と書く. $p \neq 2$ としているので $\mathrm{Gal}(K_\infty^{(2)}/K) \cong \Gamma^+ \oplus \Gamma^-$ と直和分解される.

定義 2.2. $K_\infty^{(2)}$ の Γ^- による固定体を K_∞^+ と, Γ^+ による固定体を K_∞^- と書く. K_∞^+/K を円分 $\mathbb{Z}_p$ 拡大 (cyclotomic $\mathbb{Z}_p$-extension), K_∞^-/K を反円分 $\mathbb{Z}_p$ 拡大 (anticyclotomic $\mathbb{Z}_p$-extension) と呼ぶ.

定義により $\mathrm{Gal}(K_\infty^+/K) \cong \Gamma^+$, $\mathrm{Gal}(K_\infty^-/K) \cong \Gamma^-$ は $\mathbb{Z}_p$ と同型で, K_∞^+, K_∞^- はともに K の $\mathbb{Z}_p$ 拡大である. K_∞^+ は $\mathbb{Q}$ の唯一の $\mathbb{Z}_p$ 拡大 (円分 $\mathbb{Z}_p$ 拡大) と K の合成体となり, K_∞^- は $\mathbb{Q}$ 上 Galois な K の $\mathbb{Z}_p$ 拡大でその Galois 群が非可換 (dihedral) となる唯一のものと特徴付けられる.

次に $\mathfrak{p} \neq \mathfrak{p}^*$, つまり p は $K/\mathbb{Q}$ で分解すると仮定する. そのとき類体論から, $\mathfrak{p}$ および $\mathfrak{p}^*$ が不分岐であるような K の $\mathbb{Z}_p$ 拡大がそれぞれ一つ存在することがわかる. (不分岐な $\mathbb{Z}_p$ 拡大は存在しないので, もう一方の p 上の素点は必ず分岐する.)

定義 2.3. $\mathfrak{p} \neq \mathfrak{p}^*$ のとき, K の $\mathbb{Z}_p$ 拡大で $\mathfrak{p}$ のみ分岐するものを $K_\infty^{(\mathfrak{p})}$ と, $\mathfrak{p}^*$ のみ分岐するものを $K_\infty^{(\mathfrak{p}^*)}$ と書く. $\mathfrak{p} = \mathfrak{p}^*$ のときには便宜的に $K_\infty^{(\mathfrak{p})} = K_\infty^{(\mathfrak{p}^*)} = K_\infty^{(2)}$ とする.

注. 上に挙げた記号たちは本稿の中だけでのもので, 一般的なものではない.

これらの $\mathbb{Z}_p$, $\mathbb{Z}_p^2$ 拡大は K に CM を持つ楕円曲線の p 冪分点から作られる拡大と関係する (命題 1.19 参照).

命題 2.4. E/F を $\mathrm{End}_F(E) \cong \mathcal{O}_K$ なる楕円曲線で, p の上にある全ての素点で good reduction を持つようなものとする. そのとき, $F(E[p^\infty]) = K_\infty^{(2)} \cdot F(E[p])$, $F(E[\mathfrak{p}^\infty]) = K_\infty^{(\mathfrak{p})} \cdot F(E[\mathfrak{p}])$ となる.

2.2 楕円単数

アーベル体上の岩澤理論において, 1 の冪根から作られる円単数が重要な役割を果たしていたように, 虚 2 次体のアーベル拡大でも CM 楕円曲線の等分点から作られる楕円単数が重要な役割を果たす. ここでは楕円単数の定義を簡単に復習する. 詳しくは [deS, Chap.II, III], [Rob], [Rub2, §12], [Rub5, §7] などを参照.

$\mathcal{O}_K$ に CM を持つ $H = K(1)$ 上の楕円曲線 E で仮定 (G) を満たすものを一つ取っておく (必ず存在する).

定義 2.5. 6 と素な $\mathcal{O}_K$ のイデアル $\mathfrak{a}$ に対し, E 上の関数 $\Theta_{E,\mathfrak{a}}$ を

$$\Theta_{E,\mathfrak{a}}(Q) = \alpha^{-12}\Delta_E^{N\mathfrak{a}-1} \prod_{P\in E[\mathfrak{a}]-\{0\}} (x(Q)-x(P))^{-6}$$

と定める. ただし, $\alpha \in \mathcal{O}_H$ は単項イデアル $\mathfrak{a}\mathcal{O}_H$ の生成元, $N\mathfrak{a}$ は $\mathcal{O}_K/\mathfrak{a}$ の位数. Δ_E は E の判別式で, x は E 上の点の x 座標を表す.

注. $\Theta_{E,\mathfrak{a}}$ は E の ($\mathbb{C}$ 上の) Weierstrass model の取り方によらない. [deS] の記号では $\Theta(z;L,\mathfrak{a})$, [Rub3] の記号では $\Theta_0(z,\mathfrak{a})^{12}$ となる.

定理 2.6 ([deS, Chap.II] 参照). $\mathfrak{b}$ を $\mathfrak{a}$ と素な $\mathcal{O}_K$ のイデアルとし, $Q \in E[\mathfrak{b}]$ を $\mathfrak{b}$ の任意の真の divisor $\mathfrak{b}'$ に対しては $Q \notin E[\mathfrak{b}']$ となる点とする. そのとき次が成り立つ.

(i) $\Theta_{E,\mathfrak{a}}(Q) \in K(\mathfrak{b})$.

(ii) $\mathfrak{b}$ が素イデアルの冪でなければ $\Theta_{E,\mathfrak{a}}(Q)$ は単数になる. $\mathfrak{b}$ が素イデアル $\mathfrak{q}$ の冪のときは $\mathfrak{q}$ 以外の素点に関して単数.

(iii) 任意の $\mathfrak{b}$ と素な $\mathfrak{c} = c\mathcal{O}_K$ に対し, $\Theta_{E,\mathfrak{a}}(Q)^{\sigma_\mathfrak{c}} = \Theta_{E,\mathfrak{a}}([c]Q)$.

(iv) $\mathfrak{b} = \mathfrak{lc}$, $\mathfrak{l} = \ell\mathcal{O}_K$ は素イデアルとする. そのとき $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{c})^\times$ が単射ならば

$$N_{K(\mathfrak{b})/K(\mathfrak{c})}\Theta_{E,\mathfrak{a}}(Q) = \begin{cases} \Theta_{E,\mathfrak{a}}([\ell]Q)^{1-\sigma_\mathfrak{l}^{-1}} & \mathfrak{l}\nmid\mathfrak{c} \text{ のとき}, \\ \Theta_{E,\mathfrak{a}}([\ell]Q) & \mathfrak{l}|\mathfrak{c} \text{ のとき} \end{cases}$$

が成り立つ.

証明の概略. (i) は命題 1.19 (iii) より. (ii) は $\mathfrak{q}$ を $\mathcal{O}_K$ の素イデアルとするとき, $\mathfrak{b}$ が $\mathfrak{q}$ の冪でなければ $\mathrm{ord}_\mathfrak{q}(\Theta_{E,\mathfrak{a}}(Q)) = 0$ であることを見れば良い. E の Weierstrass model で整数係数かつ $\mathrm{ord}_\mathfrak{q}(\Delta_E) = 0$ なるものが取れる. そのとき, $R \in E_{\mathrm{tors}}$ に対して $\mathrm{ord}_\mathfrak{q}(x(R)) < 0$ と $R \in E[\mathfrak{q}^\infty]$ は同値となることを用いて, $\mathrm{ord}_\mathfrak{q}(x(Q)-x(P)) = \min(\mathrm{ord}_\mathfrak{q}(x(Q)), \mathrm{ord}_\mathfrak{q}(x(P))) \le 0$ が言える. これが実際に負になるのは $\mathfrak{b}$ が $\mathfrak{q}$ の冪のときか, $P \in E[\mathfrak{q}^\infty] \cap E[\mathfrak{a}]$ のとき. 後者はそのような P を動かすことで $\mathrm{ord}_\mathfrak{q}(\alpha^{-12})$ とキャンセルする. (iii) は $E[\mathfrak{b}]$ への Galois 作用より, (iv) は (iii) と *distribution relation* ([deS, II.2.3]) より. □

この定理により, 関数 $\Theta_{E,\mathfrak{a}}$ を用いて K のアーベル拡大体上の単数が得られた. このように作られる単数を楕円単数と呼ぶ.

定義 2.7. F を K のアーベル拡大とするとき, 楕円単数たちで生成される群

$$C'(F) := \langle N_{FK(\mathfrak{b})/F}(\Theta_{E,\mathfrak{a}}(Q))^{\sigma-1} \mid \mathfrak{a},\mathfrak{b},Q \text{ は上のもの}, \sigma \in \mathrm{Gal}(F/K)\rangle$$

と F に含まれる 1 の冪根の群 $\mu_\infty(F)$ の積

$$C(F) := \mu_\infty(F)C'(F)$$

は F の単数群の $\mathbb{Z}[\mathrm{Gal}(F/K)]$-submodule となる. この $C(F)$ を F の楕円単数群と呼ぶ.

更に, 円単数と同様に楕円単数からも Euler 系が作られ, 岩澤主予想の証明や p 進 L 関数の構成に使われる.

F を K のアーベル拡大で $F \supset K(1)$ かつ $p \nmid [F:K]$ なるものとする. 6 と素な $\mathcal{O}_K$ の素イデアル $\mathfrak{a}$ と p の冪 M を取る. $\mathfrak{a}$ と素な素イデアル $\mathfrak{l}$ で F/K で完全分解かつ $N\mathfrak{l} \equiv 1 \pmod{M}$ となるようなものに対し, $FK(\mathfrak{l})$ に含まれる F の M 次巡回拡大で, $\mathfrak{l}$ 上の素点のみ分岐 (それらは完全分岐) するような拡大を $F(\mathfrak{l})$ と表す. $\mathfrak{n}$ を上の条件を満たす相異なる素イデアル $\mathfrak{l}$ の積とし, $F(\mathfrak{n})$ は $F(\mathfrak{l})$ たちの合成体とする.

定義 2.8 (楕円単数の Euler 系, [Rub3, §1]). $\mathfrak{b}$ を $\mathfrak{a}$ と素なイデアルで $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{b})^\times$ が単射になるようなものとする. そのとき, 上のような $\mathfrak{n}$ で $\mathfrak{a}\mathfrak{b}$ と素なものに対し

$$\alpha(\mathfrak{n}) := N_{FK(\mathfrak{b}\mathfrak{n})/F(\mathfrak{n})}\big(\Theta_{E,\mathfrak{a}}(Q_\mathfrak{n})\big) \in F(\mathfrak{n})$$

と定める. ただし $Q_\mathfrak{n}$ は $E[\mathfrak{b}\mathfrak{n}]$ の生成元で, $\mathfrak{n} = \mathfrak{l}\mathfrak{n}'$ のとき自然な写像 $E[\mathfrak{b}\mathfrak{n}] \twoheadrightarrow E[\mathfrak{b}\mathfrak{n}']$ による像が $Q_{\mathfrak{n}'}$ となるようなもの.

定理 2.6 (ii) より, $\mathfrak{n} \neq \mathcal{O}_K$ なら $\alpha(\mathfrak{n})$ は $F(\mathfrak{n})$ の単数となり, 同 (iv) より Euler 系の norm property が確かめられる.

2.3 岩澤主予想

F を K の有限次アーベル拡大で $p \nmid [F:K]$ を満たすものとし, K_∞ で $\mathrm{Gal}(K_\infty/K)$ が $\mathbb{Z}_p^r$ ($r = 1$ または 2) と同型になるような K の Galois 拡大を表す. 更に $F_\infty = FK_\infty$ とし,

$$\Delta = \mathrm{Gal}(F/K),\ \ \Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathrm{Gal}(F_\infty/F) \cong \mathbb{Z}_p^r,\ \ G = \mathrm{Gal}(F_\infty/K) \cong \Delta \times \Gamma$$

と置く. そのとき完備群環 $\Lambda := \mathbb{Z}_p[\![\Gamma]\!]$ は $\mathbb{Z}_p$ 係数の r 変数形式的冪級数環と同型となる. Δ の指標 $\chi : \Delta \to \overline{\mathbb{Q}_p}^\times$ に対し, $\mathbb{Z}_p$ に χ の像を添加した環を $\mathbb{Z}_p[\chi]$ と書き, $\Lambda_\chi := \mathbb{Z}_p[\chi][\![\Gamma]\!]$ とする.

定義 2.9. $X(F_\infty)$ (resp. $\mathfrak{X}_\mathfrak{p}(F_\infty)$) を F_∞ の不分岐 (resp. $\mathfrak{p}$ の外不分岐) 最大アーベル p 拡大の Galois 群とする.

定義 2.10. F_∞/F の中間体 F' で $[F':F] < \infty$ なるものに対し, $\mathfrak{p}$ の上にある全ての素イデアル v に対する主単数群 $U(F'_v)$ の直積を $U_\mathfrak{p}(F') = \prod_{v|\mathfrak{p}} U(F'_v)$ とする. また F' の単数群 $\mathcal{O}_{F'}^\times$ および楕円単数群 $C(F')$ と $U_\mathfrak{p}(F')$ との ($\prod_{v|\mathfrak{p}} F'^\times_v$ における) 共通部分の閉包をそれぞれ $E_\mathfrak{p}(F'), C_\mathfrak{p}(F')$ と書く. それらのノルムに関する逆極限をそれぞれ

$$U_\mathfrak{p}(F_\infty) := \varprojlim_{F'} U_\mathfrak{p}(F'),\quad E_\mathfrak{p}(F_\infty) := \varprojlim_{F'} E_\mathfrak{p}(F'),\quad C_\mathfrak{p}(F_\infty) := \varprojlim_{F'} C_\mathfrak{p}(F')$$

と置く.

これら $X(F_\infty), \mathfrak{X}_\mathfrak{p}(F_\infty), U_\mathfrak{p}(F_\infty), E_\mathfrak{p}(F_\infty), C_\mathfrak{p}(F_\infty)$ はアーベル体のときと同様に, 全て有限生成 Λ 加群とみなせる. 更に類体論から

$$1 \to E_\mathfrak{p}(F_\infty)/C_\mathfrak{p}(F_\infty) \to U_\mathfrak{p}(F_\infty)/C_\mathfrak{p}(F_\infty) \to \mathfrak{X}_\mathfrak{p}(F_\infty) \to X(F_\infty) \to 1 \tag{2}$$

という Λ 加群の完全列が得られる.

命題 2.11. $X(F_\infty)$ と $E_\mathfrak{p}(F_\infty)/C_\mathfrak{p}(F_\infty)$ は Λ-torsion である. $\mathfrak{X}_\mathfrak{p}(F_\infty)$ と $U_\mathfrak{p}(F_\infty)/C_\mathfrak{p}(F_\infty)$ は $\mathfrak{p} \neq \mathfrak{p}^*$ のとき Λ-torsion.

これらの torsion Λ 加群の特性イデアルの関係を予想するのが今の場合の岩澤主予想である. ($\Gamma \cong \mathbb{Z}_p^2$ の場合にも, pseudo-null Λ 加群を適切に定義することにより, 構造定理や elementary module, 特性イデアル等が考えられる. 伊藤氏の稿の Appendix 参照.) torsion Λ 加群 M の特性イデアルを $\mathrm{char}_\Lambda(M)$ と表す ($\mathrm{char}_{\Lambda_\chi}(M^\chi)$ も同様).

予想 2.12 (岩澤主予想). χ を Δ の指標とするとき, 次が成り立つ.

(i) $\mathrm{char}_{\Lambda_\chi}(X(F_\infty)^\chi) = \mathrm{char}_{\Lambda_\chi}(E_\mathfrak{p}(F_\infty)^\chi/C_\mathfrak{p}(F_\infty)^\chi)$.

(ii) $\mathfrak{p} \neq \mathfrak{p}^*$ のとき $\mathrm{char}_{\Lambda_\chi}(\mathfrak{X}_\mathfrak{p}(F_\infty)^\chi) = \mathrm{char}_{\Lambda_\chi}(U_\mathfrak{p}(F_\infty)^\chi/C_\mathfrak{p}(F_\infty)^\chi)$.

この予想は $\mathfrak{p} \neq \mathfrak{p}^*$ で $K_\infty = K_\infty^{(\mathfrak{p})}$ のとき「1 変数主予想 (one-variable main conjecture)」と呼ばれ, $K_\infty = K_\infty^{(2)}$ のとき「2 変数主予想 (two-variable main conjecture)」と呼ばれる. また (i) と (ii) はそれぞれ, 尾崎氏の稿での有理数体上の場合の岩澤主予想の定式化 (III) と (II) に対応するものである. $\mathfrak{p} \neq \mathfrak{p}^*$ のときには完全列 (2) により, 2 つの定式化 (i) と (ii) は同値となる.

アーベル体での岩澤主予想は Mazur と Wiles によって解決された後, Thaine, Kolyvagin の仕事を受けて, Rubin が円単数の Euler 系を利用した別証明を与えた. Rubin はその直後に, 虚 2 次体のアーベル拡大とその上の楕円単数に同じ方法を適用し, 次を証明した.

定理 2.13 (Rubin [Rub3], [Rub4]). $\mathfrak{p} \neq \mathfrak{p}^*$ または Δ の指標 χ の $\mathfrak{p}$ の分解群への制限が自明でなければ予想 2.12 は正しい, つまり $\mathrm{char}_{\Lambda_\chi}(X(F_\infty)^\chi) = \mathrm{char}_{\Lambda_\chi}(E_\mathfrak{p}(F_\infty)^\chi/C_\mathfrak{p}(F_\infty)^\chi)$ が成り立つ.

注. [Rub3] では $F \supset K(1)$ という仮定がつけられており, 特に ($p \nmid [F:K]$ なので) K の類数が p で割れる場合は除外されていたことになる. その仮定を外す方法は [Rub4] にまとめられている. ($p \nmid [F:K]$ という仮定はそのまま.)

この定理はアーベル体の場合と同様に, 楕円単数の Euler 系を用いて $\mathrm{char}_{\Lambda_\chi}(X(F_\infty)^\chi)$ が $\mathrm{char}_{\Lambda_\chi}(E_\mathfrak{p}(F_\infty)^\chi/C_\mathfrak{p}(F_\infty)^\chi)$ を含むことを示し, 解析的類数公式などを用いてそれを等号にするという方針で証明される. アーベル体の場合の Ferrero-Washington の結果 (田谷氏の稿) に対応する μ 不変量に関する結果 (Gillard, Schneps) や, $\mathbb{Z}_p$ 拡大と $\mathbb{Z}_p^2$ 拡大を行き来するような議論も用いられる. 詳細は [Rub3] やアーベル体の場合の青木氏の講演を参照して頂きたい.

2.4 p 進 L 関数

$\mathfrak{p} \neq \mathfrak{p}^*$ とする. アーベル体の場合に円単数と Kubota-Leopoldt の p 進 L 関数が結びついていた (都地氏の稿) ように, 楕円単数と p 進 L 関数も結びつけることができ, 主予想もそれを使って定式化することができる. ここでは 2 変数 p 進 L 関数に関する結果のみを簡単に述べる. 詳しくは [CW2], [Katz], [Yag], [deS] などを参照.

$\mathbb{C}_p$ で $\overline{\mathbb{Q}_p}$ の完備化を, $\widehat{\mathbb{Z}_p^{\mathrm{ur}}}$ で $\mathbb{Q}_p$ の最大不分岐拡大の完備化の整数環を表す. $\mathfrak{f}$ を p と素な $\mathcal{O}_K$ のイデアルとする. conductor が $\mathfrak{f}p^\infty$ を割る Hecke 指標 $\varepsilon : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ に対して p 進 Galois 指標 $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K) \to \mathbb{C}_p^\times$ を定めることができるが ([deS, II.1.1] 参照), それも同じ ε で表す. (ただし infinity type が $(k,0)$ の指標が $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$ からの指標と対応するように, $\overline{\mathbb{Q}}$ の $\mathbb{C}_p$ への埋め込みを取る.) Galois 指標 ε は自然に準同型 $\mathbb{Z}_p[\![\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)]\!] \to \mathbb{C}_p$ などを導くがそれも ε と書く.

定理 2.14 ([deS, II.4.16]). 次の条件を満たす $\mathcal{L}_{\mathfrak{p},\mathfrak{f}} \in \widehat{\mathbb{Z}_p^{\mathrm{ur}}}[\![\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)]\!]$ が存在する: conductor が $\mathfrak{f}p^\infty$ を割り, infinity type (k,j) が $0 \le j < -k$ であるような任意の Hecke 指標 ε に対し,

$$\Omega_p^{k-j}\varepsilon(\mathcal{L}_{\mathfrak{p},\mathfrak{f}}) = \Omega^{k-j}\Big(\frac{2\pi}{\sqrt{d_K}}\Big)^j G(\varepsilon^{-1})\Big(1-\frac{\varepsilon^{-1}(\mathfrak{p})}{p}\Big)L_{\infty,\mathfrak{f}\mathfrak{p}^*}(\varepsilon,0)$$

が成り立つ. ただし, $L_{\infty,\mathfrak{f}\mathfrak{p}^*}(\varepsilon,s)$ は ε の L 関数 $L(\varepsilon,s)$ から $\mathfrak{f}\mathfrak{p}^*$ の Euler 因子を除き, 適切な Γ 因子を掛けたもの ([deS, II.1.1]), $(\Omega,\Omega_p) \in \mathbb{C}\times\mathbb{C}_p$ は複素周期と p 進周期の組 ([deS, II.4.4]). $-d_K$ は K の基本判別式であり, $G(\varepsilon^{-1})$ は "Gauss 和" ([deS, II.4.14]).

F を $p \nmid [F:K]$ なる K のアーベル拡大で, conductor の p と素な部分が $\mathfrak{f}$ となるもの, χ を $\Delta = \mathrm{Gal}(F/K)$ の指標とする. $\mathbb{Z}_p[\mathrm{Gal}(K(\mathfrak{f}p)/K)] \to \mathbb{Z}_p[\Delta] \xrightarrow{\chi} \mathbb{Z}_p[\chi]$ が誘導する射 $\widehat{\mathbb{Z}_p^{\mathrm{ur}}}[\![\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)]\!] \to \widehat{\mathbb{Z}_p^{\mathrm{ur}}}[\chi][\![\Gamma]\!]$ を $\widetilde{\chi}$ と書く. $F_\infty = FK_\infty^{(2)}$, $\Gamma = \mathrm{Gal}(F_\infty/F)$ とする.

定理 2.15 (Yager [Yag], de Shalit [deS]). $\mathrm{char}_{\Lambda_\chi}(U_{\mathfrak{p}}(F_\infty)^\chi/C_{\mathfrak{p}}(F_\infty)^\chi)\widehat{\mathbb{Z}_p^{\mathrm{ur}}}[\chi][\![\Gamma]\!]$ は $\mathcal{L}_{\mathfrak{p}}^\chi := \widetilde{\chi}(\mathcal{L}_{\mathfrak{p},\mathfrak{f}})$ により生成される.

これにより定理 2.13 は次のように書き換えられる.

系 2.16. 定理 2.13 の条件を満たす χ に対し, $\mathrm{char}_{\Lambda_\chi}(\mathfrak{X}_{\mathfrak{p}}(F_\infty)^\chi)\widehat{\mathbb{Z}_p^{\mathrm{ur}}}[\chi][\![\Gamma]\!] = (\mathcal{L}_{\mathfrak{p}}^\chi)$.

2.5 反円分主予想について

Rubin は円単数や楕円単数の Euler 系を使った岩澤主予想の証明を与えたが, アーベル体の場合には Mazur-Wiles による保型形式を利用し, 円単数の Euler 系は使わない証明があった. (そもそもそちらが先だった.) その方法は肥田理論を使う形になって, Wiles による一般の総実体上のアーベル拡大での主予想の証明にも使われたのであった. (栗原氏の稿を参照.)

虚 2 次体上の場合も, 反円分 $\mathbb{Z}_p$ 拡大 K_∞^-/K に関する岩澤主予想については, Euler 系の議論を使わない証明法が Tilouine により与えられている ([Til], [MaTi]). 更に, その方法は一般の CM 体 (総実体の虚 2 次拡大) にも適用することができ, その場合にも反円分的拡大の主予想がいくつかの仮定の下で解決されたようである ([HiTi], [Hid] 参照). その場合には円単数, 楕円単数のような Euler 系は見つかっておらず, 主予想は p 進 L 関数を用いた定式化が用いられる.

3 主予想の応用

この節では拡張された岩澤理論, 特に虚 2 次体の岩澤主予想が (CM を持つ) 楕円曲線の数論, 特に Birch, Swinnerton-Dyer 予想とどのように関連するかを見る.

3.1 Selmer 群と Tate-Shafarevich 群

まず楕円曲線の Selmer 群と Tate-Shafarevich 群の定義を見る. ここでは F を任意の (有限次と限らない) 代数体とし, E を F 上定義された楕円曲線とする. E は虚数乗法を持つとは仮定しないが, $\mathcal{O}$ を $\mathbb{Z}$ または虚 2 次体の整数環とし, $\mathrm{End}_F(E) \cong \mathcal{O}$ とする. また $[\,] : \mathcal{O} \xrightarrow{\sim} \mathrm{End}_F(E)$ を定義 1.16 の同型とする.

Selmer 群は楕円曲線とその上の自己準同型 (もしくは一般に 2 つの楕円曲線の間の isogeny) に付随して定義される.

定義 3.1. $\alpha \in \mathcal{O}$ に対し, E/F の α-Selmer 群 $\mathrm{Sel}_\alpha(E/F)$ を

$$\mathrm{Sel}_\alpha(E/F) := \left(H^1(F, E[\alpha]) \longrightarrow \prod_v H^1(F_v, E[\alpha]) / \big(E(F_v)/[\alpha]E(F_v)\big)\right)$$

と定める. ただし v は F の全ての素点を走り, F_v は F の v に関する完備化を表す.

上の定義で $E(F_v)/[\alpha]E(F_v)$ は $\mathrm{Gal}(\overline{F_v}/F_v)$ 加群としての完全列

$$0 \longrightarrow E[\alpha] \longrightarrow E(\overline{F_v}) \xrightarrow{[\alpha]} E(\overline{F_v}) \longrightarrow 0$$

の cohomology を取ることで得られる完全列

$$0 \longrightarrow E(F_v)/[\alpha]E(F_v) \longrightarrow H^1(F_v, E[\alpha]) \longrightarrow H^1(F_v, E(\overline{F_v}))[\alpha] \longrightarrow 0$$

により $H^1(F_v, E[\alpha])$ の部分群とみなしている. 同様に $E(F)/[\alpha]E(F)$ を $H^1(F, E[\alpha])$ の部分群とみなすことができるが, そのとき $E(F)/[\alpha]E(F) \subset \mathrm{Sel}_\alpha(E/F)$ であることは容易にわかる. その商を $Ш(E/F)[\alpha]$ と書くことにする.

$\alpha, \beta \in \mathcal{O}$ とすると $E[\alpha] \subset E[\alpha\beta]$ なので, 自然な写像 $H^1(F, E[\alpha]) \to H^1(F, E[\alpha\beta])$ が誘導される. そのとき $\mathrm{Sel}_\alpha(E/F)$ の像は $\mathrm{Sel}_{\alpha\beta}(E/F)$ に含まれ, $Ш(E/F)[\alpha] \to Ш(E/F)[\alpha\beta]$ は単射となる.

定義 3.2. $\alpha \in \mathcal{O}$ に対し,

$$\mathrm{Sel}_{\alpha^\infty}(E/F) := \varinjlim_i \mathrm{Sel}_{\alpha^i}(E/F) \qquad Ш(E/F)[\alpha^\infty] := \bigcup_i Ш(E/F)[\alpha^i]$$

$$\mathrm{Sel}(E/F) := \varinjlim_n \mathrm{Sel}_n(E/F) \qquad Ш(E/F) := \bigcup_n Ш(E/F)[n]$$

と定める. $Ш(E/F)$ を楕円曲線 E の F 上の Tate-Shafarevich 群と呼ぶ.

注. Tate-Shafarevich 群の持つ意味については [Sil1, Chap.X] などを見よ.

定義 3.3. イデアル $\mathfrak{a} \subset \mathcal{O}$ に対し, $\mathfrak{a}^k = \alpha\mathcal{O}$ となる $k \in \mathbb{N}$, $\alpha \in \mathcal{O}$ を取って

$$\mathrm{Sel}_{\mathfrak{a}^\infty}(E/F) := \mathrm{Sel}_{\alpha^\infty}(E/F), \quad Ш(E/F)[\mathfrak{a}^\infty] := Ш(E/F)[\alpha^\infty]$$

と書く. (k, α の取り方によらない.)

定義より明らかなように

$$0 \longrightarrow E(F) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(E/F) \longrightarrow Ш(E/F)[p^\infty] \longrightarrow 0$$

などといった完全列が存在する. また, $\varinjlim_i H^1(F, E[\alpha^i])$ は自然に $H^1(F, E[\alpha^\infty])$ と一致するので, $\mathrm{Sel}_{\alpha^\infty}(E/F)$ をその部分群と見なすことが出来る.

Selmer 群の大きさに関しては, 次が知られている ([Sil1, Chap.X] など参照).

命題 3.4. F が有限次代数体のとき, 任意の $\alpha \in \mathcal{O}$ に対して $\mathrm{Sel}_\alpha(E/F)$ は有限アーベル群. p が素数ならば $\mathrm{Sel}_{p^\infty}(E/F)$ の Pontryagin dual は $\mathbb{Z}_p$ 上有限生成.

また, Tate-Shafarevich 群に関しては次が予想されている.

予想 3.5. F が有限次代数体のとき $Ш(E/F)$ は有限アーベル群.

強い形の Birch, Swinnerton-Dyer 予想 (予想 1.13(ii)) は, E の L 関数の $s = 1$ での Taylor 展開の leading term が $Ш(E/\mathbb{Q})$ の位数などの量を使って書けるという予想であるが, 予想 3.5 は $F = \mathbb{Q}$ の場合でも一般には解決されていない.

3.2 楕円曲線の岩澤理論

岩澤理論では, 代数体のイデアル類群が $\mathbb{Z}_p$ 拡大と呼ばれる代数体の拡大でどのように変化するかや, その変化と p 進 L 関数との関係などが研究の対象であったが, イデアル類群だけでなく, より一般の数論的対象を問題とする岩澤理論の一般化が存在する (詳しくは八森氏の稿). その出発点となったのが, Mazur による楕円曲線に対する一般化である (1970 年頃). Mazur はイデアル類群の代わりに楕円曲線や高次元のアーベル多様体の Selmer 群を考え, その $\mathbb{Z}_p$ 拡大での振る舞いを考察し, L 関数との関連などの予想や問題を提案した. ここでは, その Mazur に始まる楕円曲線の岩澤理論に関する結果や予想の一部を簡単に述べる. 詳しくは [Maz1], [Man], [Kur1], [Gre2] などを見よ.

F を有限次代数体, E を F 上の楕円曲線とする. ここでは簡単のため E は素数 p の上にある全ての素点で good reduction を持つと仮定する. F_∞/F を $\mathbb{Z}_p$ 拡大とするとき, E の Selmer 群 $\mathrm{Sel}_{p^\infty}(E/F_\infty)$ には Galois 群 $\Gamma = \mathrm{Gal}(F_\infty/F)$ が自然に作用する. その作用は ($\mathrm{Sel}_{p^\infty}(E/F_\infty)$ を離散アーベル群と思って) 連続であるので, Pontryagin dual

$$\mathfrak{X}_p(E/F_\infty) := \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

は compact Λ 加群とみなせる. ただし Λ は完備群環 $\mathbb{Z}_p[\![\Gamma]\!]$. 中山の補題を使って $\mathfrak{X}_p(E/F_\infty)$ が Λ 上有限生成であることが確かめられる. そのときまず問題になるのが $\mathfrak{X}_p(E/F_\infty)$ はいつ torsion Λ 加群となるかであるが, 次の結果が知られている.

命題 3.6. E が F_∞/F で分岐する F のある素点で supersingular reduction を持つならば, $\mathfrak{X}_p(E/F_\infty)$ は Λ-torsion ではない.

以下では次の条件を仮定する.

(Ord) E は p の上にある F の全ての素点で good ordinary reduction を持つ.

この条件の下でも $\mathfrak{X}_p(E/F_\infty)$ は必ずしも Λ-torsion であるとは限らないが (定理 3.17, 定理 4.4 参照), 少なくとも次は予想されている.

予想 3.7 (Mazur). F_∞/F が円分 $\mathbb{Z}_p$ 拡大であれば, (Ord) の下で $\mathfrak{X}_p(E/F_\infty)$ は Λ-torsion となる.

(Ord) の下ではイデアル類群のときと同様に, $\mathbb{Z}_p$ 拡大 F_∞/F での Selmer 群の振る舞いと $\mathfrak{X}_p(E/F_\infty)$ の Λ 加群としての構造が密接に関係している. それを示す次の定理は, Mazur の control theorem と呼ばれる.

定理 3.8 (Mazur). (Ord) の下, 自然な制限写像

$$\mathrm{Sel}_{p^\infty}(E/F_n) \longrightarrow \mathrm{Sel}_{p^\infty}(E/F_\infty)^{\Gamma_n}$$

の kernel, cokernel はともに有限であり, それらの位数は有界. ただし, F_n は F_∞/F の n-th layer, $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$.

証明方針. Selmer 群の定義から, 大域および局所 cohomology 群の制限写像での kernel や cokernel がわかれば良い. 問題になるのは p 上の局所 cohomology 群の kernel で, そこは楕円曲線に付随する形式群の universal norm を調べるなどして求められる. 詳細は [Gre2], [Gre3] 等参照. □

これにより, $\mathfrak{X}_p(E/F_\infty)$ の Λ-torsion 性に関する一つの十分条件や, 岩澤類数公式 (藤井氏の稿) の類似が得られる.

系 3.9. $\mathrm{Sel}_{p^\infty}(E/F)$ は有限, つまり $E(F)$ と $Ш(E/F)[p^\infty]$ はともに有限であるとする. そのとき, (Ord) の下, 任意の $\mathbb{Z}_p$ 拡大 F_∞/F で $\mathfrak{X}_p(E/F_\infty)$ は Λ-torsion.

系 3.10. 任意の n で $Ш(E/F_n)[p^\infty]$ は有限であると仮定する. そのとき (Ord) の下で次が成り立つ.

(i) $E(F_\infty)$ は有限生成アーベル群 $\iff$ $\mathfrak{X}_p(E/F_\infty)$ は Λ-torsion かつ $E(F_\infty)[p^\infty]$ は有限.

(ii) (i) の条件が成立するとき, ある $\nu \in \mathbb{Z}$ が存在して,

$$\#Ш(E/F_n)[p^\infty] = p^{\lambda n + \mu p^n + \nu} \quad (n : \text{十分大})$$

が成立する. ただし $\lambda = \lambda(\mathfrak{X}_p(E/F_\infty)) - \mathrm{rank}_{\mathbb{Z}} E(F_\infty)$, $\mu = \mu(\mathfrak{X}_p(E/F_\infty))$.

注. 定理 3.8 の kernel, cokernel の位数は十分大きな n で一定になる.

更に Mazur は $\mathfrak{X}_p(E/F_\infty)$ が Λ-torsion になるとき, その特性イデアルの生成元は楕円曲線の L 関数の特殊値の p 進的な振る舞い (p 進 L 関数) と関係するであろうという, 岩澤主予想の一般化も提案した. $F=\mathbb{Q}$ の場合には p 進 L 関数が次のように構成されている.

定理 3.11 ([MaSw], [MTT]). (Ord) を満たす $\mathbb{Q}$ 上の楕円曲線 E に対し, 次のような $\mathcal{L}_{E,p}\in\Lambda\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ が存在する: 位数 p^n の $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ の任意の指標 ϕ に対し

$$\phi(\mathcal{L}_{E,p})=\begin{cases}(1-\alpha^{-1})^2\frac{L(E,1)}{\Omega_E} & n=0\text{ のとき},\\ \alpha^{-n-1}p^{n+1}G(\overline{\phi})^{-1}\frac{L(E,\overline{\phi},1)}{\Omega_E} & n\geq 1\text{ のとき}\end{cases}$$

が成り立つ. ただし, $\alpha\in\mathbb{Z}_p^\times$ は x^2-a_px+p の根で p 進単数の方. $L(E,\overline{\phi},s)$ は E の L 関数を Dirichlet 指標 $\overline{\phi}$ でひねったもの. $G(\overline{\phi})$ は Gauss 和で, Ω_E は予想 1.13 のもの.

予想 3.12 (楕円曲線の岩澤主予想). $\mathcal{L}_{E,p}$ は Λ に含まれ, torsion Λ 加群 $\mathfrak{X}_p(E/\mathbb{Q}_\infty)$ の特性イデアル $\mathrm{char}_\Lambda(\mathfrak{X}_p(E/\mathbb{Q}_\infty))$ を生成する.

最後に, $E/\mathbb{Q}$ が p で supersingular reduction を持つ場合に触れておく. その場合には Selmer 群の Pontryagin dual は Λ-torsion とならず (命題 3.6), p 進 L 関数も構成されてはいるが $\Lambda\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ に含まれないので, 主予想を予想 3.12 の形では定式化できない. しかし最近, p 進 L 関数をうまく分解することにより Λ の元が取り出せることを Pollack が示し ([Pol]), それに対応するような dual が Λ-torsion である Selmer 群の部分加群も小林によって構成された ([Kob]). [Kob] では, それらの間に予想 3.12 のような関係が成り立つとして, 主予想が定式化されている. 系 3.10 に対応する, Tate-Shafarevich 群の位数の振る舞いに関しては [Kur1] を見よ (ordinary の場合とは大きく異なる).

3.3 CM 楕円曲線の場合

E を $\mathbb{Q}$ 上の楕円曲線で, 虚 2 次体 K に対し $\mathrm{End}_K(E)\cong\mathcal{O}_K$ となるようなものとする. ($j_E\in\mathbb{Q}$ なので命題 1.19 (i) より K の類数は 1 となる.) このような CM 楕円曲線の場合には, $\mathbb{Z}_p$ 拡大 K_∞/K 上での Selmer 群の dual $\mathfrak{X}_p(E/K_\infty)$ の Λ 加群としての構造を, Rubin の定理 2.13 を使って調べることが出来る.

$p\geq 5$ とし, E は p で *good ordinary reduction* を持つとする. そのとき p は $\mathcal{O}_K$ で $p\mathcal{O}_K=\mathfrak{p}\mathfrak{p}^*$ ($\mathfrak{p}\neq\mathfrak{p}^*$) と分解することがわかる. $F=K(E[p])$, $F_\infty^{(2)}=K(E[p^\infty])$ と置くと, 命題 2.4 により $F_\infty^{(2)}=FK_\infty^{(2)}$ となる. $\mathrm{Gal}(\overline{K}/F_\infty^{(2)})$ は $E[\mathfrak{p}^\infty]$ に自明に作用するので $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty^{(2)})$ は $\mathrm{Hom}(\mathrm{Gal}(\overline{K}/F_\infty^{(2)}),E[\mathfrak{p}^\infty])$ の部分群とみなせるが, 更に次がわかる.

命題 3.13. $\mathrm{Gal}(F_\infty^{(2)}/F)\cong\mathrm{Gal}(K_\infty^{(2)}/K)\cong\mathbb{Z}_p^2$ の作用も込めた canonical な同型

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty^{(2)})\cong\mathrm{Hom}(\mathfrak{X}_{\mathfrak{p}}(F_\infty^{(2)}),E[\mathfrak{p}^\infty]),\quad \mathrm{Sel}_{\mathfrak{p}^\infty}(E/K_\infty^{(2)})\cong\mathrm{Hom}(\mathfrak{X}_{\mathfrak{p}}(F_\infty^{(2)})^{\chi_{\mathfrak{p}}},E[\mathfrak{p}^\infty])$$

が存在する. ただし $\chi_{\mathfrak{p}}$ は $\mathrm{Gal}(F/K)$ の $E[\mathfrak{p}]$ への作用により定まる指標, $\mathfrak{X}_{\mathfrak{p}}(F_\infty^{(2)})$ は $F_\infty^{(2)}$ 上の $\mathfrak{p}$ の外不分岐最大アーベル p 拡大の Galois 群.

略証. $F(E[\mathfrak{p}^\infty])/F$ では $\mathfrak{p}$ しか分岐しないので, 命題 1.19(iv) より E は F の全ての素点で good reduction を持つ. それにより $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty^{(2)}) \subset \mathrm{Hom}(\mathfrak{X}_\mathfrak{p}(F_\infty^{(2)}), E[\mathfrak{p}^\infty])$ がわかる. 一方, v を $F_\infty^{(2)}$ の $\mathfrak{p}$ 上の素点とするとき $H^1(F_{\infty,v}^{(2)}, E(\overline{K_\mathfrak{p}}))[\mathfrak{p}^\infty] = 0$ が Tate local duality と極限操作で得られ, 逆向きの包含関係が示せる. (詳細は [Per2, Chap.II], [Rub1, §2] 参照.) また $\mathrm{Gal}(F/K) \subset (\mathcal{O}/p\mathcal{O})^\times$ であるから $p \nmid [F:K]$ となるので, $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/K_\infty^{(2)}) \cong \mathrm{Sel}_{\mathfrak{p}^\infty}(E/F_\infty^{(2)})^{\mathrm{Gal}(F/K)}$ となり, 後者の同型も得られる. □

この命題により, 虚 2 次体の岩澤主予想 (定理 2.13) は以下のように言い換えられる. $\Gamma^{(2)} = \mathrm{Gal}(K_\infty^{(2)}/K)$, $\Lambda^{(2)} = \mathbb{Z}_p[\![\Gamma^{(2)}]\!]$ と置き, $\kappa_{E,\mathfrak{p}} : \Gamma^{(2)} \to 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ を $\Gamma^{(2)}$ の $E[\mathfrak{p}^\infty]$ への作用により定まる指標とする.

定理 3.14 (Rubin). $\mathrm{Sel}_{\mathfrak{p}^\infty}(E/K_\infty^{(2)})$ の Pontryagin dual を $\mathfrak{X}_\mathfrak{p}(E/K_\infty^{(2)})$ と書くとき,

$$\mathrm{char}_{\Lambda^{(2)}}(\mathfrak{X}_\mathfrak{p}(E/K_\infty^{(2)})) = \mathrm{char}_{\Lambda^{(2)}}\big((U_\mathfrak{p}(F_\infty)/C_\mathfrak{p}(F_\infty))^{\chi_\mathfrak{p}} \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{\mathbb{Z}_p}(E[\mathfrak{p}^\infty], \mathbb{Q}_p/\mathbb{Z}_p)\big).$$

特に $\mathfrak{X}_\mathfrak{p}(E/K_\infty^{(2)})$ は $\Lambda^{(2)}$-torsion であり $\mathrm{char}_{\Lambda^{(2)}}(\mathfrak{X}_\mathfrak{p}(E/K_\infty^{(2)}))\widehat{\mathbb{Z}_p^{\mathrm{ur}}}[\![\Gamma^{(2)}]\!] = (\iota_\mathfrak{p}(\mathcal{L}_\mathfrak{p}^{\chi_\mathfrak{p}}))$. ただし $\iota_\mathfrak{p}$ は $\gamma \mapsto \kappa_{E,\mathfrak{p}}(\gamma)\gamma$ なる変数変換.

$\mathfrak{p}^*$ に対しても同様の結果が得られるが, $\mathfrak{p} \neq \mathfrak{p}^*$ のときには

$$\mathfrak{X}_p(E/K_\infty^{(2)}) \cong \mathfrak{X}_\mathfrak{p}(E/K_\infty^{(2)}) \oplus \mathfrak{X}_{\mathfrak{p}^*}(E/K_\infty^{(2)})$$

となるので, $\mathfrak{X}_p(E/K_\infty^{(2)})$ も $\Lambda^{(2)}$-torsion で特性イデアルは $\mathcal{L}_E^{(2)} := \iota_\mathfrak{p}(\mathcal{L}_\mathfrak{p}^{\chi_\mathfrak{p}})\iota_{\mathfrak{p}^*}(\mathcal{L}_{\mathfrak{p}^*}^{\chi_{\mathfrak{p}^*}})$ により生成される. この結果を特殊化することで, $\mathbb{Z}_p$ 拡大 K_∞/K 上の Selmer 群の構造や (p 進) L 関数との関係が調べられる. $\Gamma = \mathrm{Gal}(K_\infty/K)$, $\Lambda = \mathbb{Z}_p[\![\Gamma]\!]$ とし, $\mathrm{sp} : \Lambda^{(2)} \to \Lambda$ を自然な射 $\Gamma^{(2)} \to \Gamma$ が導く準同型とする.

系 3.15. $K_\infty \neq K_\infty^{(\mathfrak{p})}, K_\infty^{(\mathfrak{p}^*)}$ のとき $\mathrm{char}_\Lambda(\mathfrak{X}_p(E/K_\infty))$ は $\mathrm{sp}(\mathcal{L}_E^{(2)})$ により生成される. 特に $\mathfrak{X}_p(E/K_\infty)$ が Λ-torsion となるのは $\mathrm{sp}(\mathcal{L}_E^{(2)}) \neq 0$ のとき.

注. $K_\infty = K_\infty^{(\mathfrak{p})}$ のときには, 命題 3.13 や定理 3.14 が $K_\infty^{(\mathfrak{p})}$ 上で成り立つので, $\mathfrak{X}_\mathfrak{p}(E/K_\infty^{(\mathfrak{p})})$ は Λ-torsion であり, その特性イデアルは 1 変数 p 進 L 関数と関係する.

理由. 仮定の下, 制限射 $\mathrm{Sel}_{p^\infty}(E/K_\infty) \to \mathrm{Sel}_{p^\infty}(E/K_\infty^{(2)})^{\mathrm{Gal}(K_\infty^{(2)}/K_\infty)}$ は同型であり ([Per2, Lem.9, Prop.12]), $\mathfrak{X}_p(E/K_\infty^{(2)})$ は自明でない pseudo-null $\Lambda^{(2)}$ 部分加群を持たない ([Rub3, Thm.5.3, Lem.11.14]). [Rub3, Lem.6.2] を参照. □

$K_\infty = K_\infty^+$, つまり K_∞/K が円分 $\mathbb{Z}_p$ 拡大の場合にこの議論を適用すると, §3.2 の予想が CM 楕円曲線の時に正しいことが示される.

定理 3.16 ([Rub3, §12]). 上の状況の下で予想 3.7, 3.12 は正しい. つまり $\mathfrak{X}_p(E/\mathbb{Q}_\infty)$ は $\mathbb{Z}_p[\![\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]\!]$-torsion であり, その特性イデアルは $\mathcal{L}_{E,p}$ により生成される.

証明方針. p は K で分解していることより, $\mathfrak{X}_p(E/\mathbb{Q}_\infty)$ と $\mathfrak{X}_\mathfrak{p}(E/K_\infty^+)$ が Λ 加群として同型であることがわかる. $\mathfrak{X}_\mathfrak{p}(E/K_\infty^+)$ の特性イデアルは $\mathrm{sp}(\iota_\mathfrak{p}(\mathcal{L}_\mathfrak{p}^{\chi_\mathfrak{p}}))$ で生成されるが, それは $\mathcal{L}_{E,p}$ と単数倍のずれを除いて一致することが定理 2.14 の式より確かめられる. $\mathcal{L}_{E,p} \neq 0$ なので ([Roh]), 主張を得る. □

一方, 反円分 $\mathbb{Z}_p$ 拡大 K_∞^-/K の場合には, $\mathfrak{X}_p(E/K_\infty^-)$ は Λ-torsion とは限らない.

定理 3.17 (Greenberg, [Gre1]). 予想 1.10 にある関数等式の符号 w_E が -1 のとき, $\mathfrak{X}_p(E/K_\infty^-)$ は Λ-torsion ではない.

理由. 関数等式から $\mathrm{Gal}(K_\infty^-/K)$ の有限位数指標 ρ に対して $L(E,\rho,1)=0$ となる. □

この反円分 $\mathbb{Z}_p$ 拡大の場合でも, [AgHo] などでは $\mathfrak{X}_p(E/K_\infty^-)$ の torsion 部分と p 進 L 関数との関係が考察されている.

最後に E が p で good supersingular reduction を持つ場合について. この場合には全ての $\mathbb{Z}_p$ 拡大 K_∞/K で $\mathfrak{X}_p(E/K_\infty)$ は Λ-torsion ではない (命題 3.6, CM のときは p が $K/\mathbb{Q}$ で不分解で $\mathfrak{X}_\mathfrak{p}(F_\infty^{(2)})$ が $\Lambda^{(2)}$-torsion とならないことからも従う) が, 円分 $\mathbb{Z}_p$ 拡大に対しては, 小林の Selmer 群の dual が Λ-torsion になり, その特性イデアルが Pollack の p 進 L 関数で生成されると予想されていた. [PoRu] では定理 2.13 からその予想が従うことが示されている.

3.4 Birch, Swinnerton-Dyer 予想への応用

引き続き E は $\mathbb{Q}$ 上の楕円曲線で $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ が (類数 1 の) 虚 2 次体 K の整数環と同型になるようなものとする. この設定の下で, Coates と Wiles は次を示した.

定理 3.18 (Coates-Wiles [CW1]). $E(\mathbb{Q})$ が無限群であれば $L(E,1)=0$.

対偶を取ると $L(E,1)\neq 0$ ならば $E(\mathbb{Q})$ は有限 ($\mathrm{rank}_\mathbb{Z}E(\mathbb{Q})=0$) となり, その場合に Birch, Swinnerton-Dyer 予想 (予想 1.13(i)) が正しいということになる. この結果は Birch, Swinnerton-Dyer 予想に対する初めての理論的な結果であるが, [CW1] の Introduction には, この結果が岩澤理論的な考え方 (spirit of Iwasawa) に基づいて証明されると書かれており, 岩澤理論の立場からも重要な結果であった. 実際その証明には, 楕円単数と L 関数との関係など, 後の Rubin の結果 (定理 2.13) の証明とも関係する道具や手法が広く用いられている. ここでは逆に, 定理 2.13 の方から定理 3.18 やその拡張がどのように導かれるかを見る.

E が good ordinary reduction を持つような素数 $p\geq 5$ を一つ取る (必ず存在する). そのとき, control theorem (定理 3.8) により $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\Gamma$ が有限であることと $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ が有限であること, つまり $E(\mathbb{Q})$ と $Ш(E/\mathbb{Q})[p^\infty]$ がともに有限になることは同値である. 一般に torsion Λ 加群に対し, 構造定理から次がわかる.

補題 3.19. M を有限生成 torsion Λ 加群, $f\in\Lambda$ を $\mathrm{char}_\Lambda(M)$ の生成元とする.

(i) $\varphi_0:\Lambda\to\mathbb{Z}_p$ を augmentation map とし, M_Γ で M の Γ-coinvariant を表す. そのとき $\varphi_0(f)\neq 0 \iff M_\Gamma$ は有限.

(ii) $\varphi_0(f)\neq 0$ のとき $\#(M_\Gamma)\sim\varphi_0(f)$. ($\sim$ は p 進付値が等しいという意味.)

注. Λ と $\mathbb{Z}_p[\![T]\!]$ を同一視するとき, $M_\Gamma\cong M/TM$, $\varphi_0(f)=f(0)$ である.

定理 3.16 により, $\mathfrak{X}_p(E/\mathbb{Q}_\infty)$ の特性イデアルは $E/\mathbb{Q}$ の p 進 L 関数 $\mathcal{L}_{E,p}$ で生成される. $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\Gamma$ は $\mathfrak{X}_p(E/\mathbb{Q}_\infty)_\Gamma$ の Pontryagin dual であるから, $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ が有限となるのはちょうど $\varphi_0(\mathcal{L}_{E,p}) \neq 0$ となるときである. 更に $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ と $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\Gamma$ の位数のずれも正確に調べることで次がわかる.

系 3.20 (Rubin). E が p で good ordinary reduction を持つとする.

(i) $L(E,1) \neq 0$ ならば $E(\mathbb{Q})$ と $Ш(E/\mathbb{Q})[p^\infty]$ はともに有限であり,

$$\frac{L(E,1)}{\Omega_E} \sim \frac{\#Ш(E/\mathbb{Q})[p^\infty]\prod_l c_l}{(\#E(\mathbb{Q})[p^\infty])^2} \tag{3}$$

が成り立つ. ただし, c_l は予想 1.13 のもの.

(ii) $L(E,1) = 0$ ならば $E(\mathbb{Q})$ か $Ш(E/\mathbb{Q})[p^\infty]$ のいずれかは無限.

略証. $\mathcal{L}_{E,p}$ の定義により $\varphi_0(\mathcal{L}_{E,p}) = (1-\alpha^{-1})^2\frac{L(E,1)}{\Omega_E}$. $(1-\alpha^{-1}) \sim \#\widetilde{E}_p(\mathbb{F}_p)$ より $\alpha \neq 1$ なので, 上の説明により (i) の有限性と (ii) が従う. (i) の後半は, 定理 3.8 の証明を詳しく見ることで,

$$\#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \sim \frac{\#(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\Gamma)(\#E(\mathbb{Q})[p^\infty])^2}{(\#\widetilde{E}_p(\mathbb{F}_p))^2\prod_l c_l}$$

となることより ([Gre2, §4] 参照). □

注. [Rub3] では $\mathbb{Q}_\infty/\mathbb{Q}$ ではなく $\mathbb{Z}_p$ 拡大 $K_\infty^{(p)}/K$ を利用して証明している.

系 3.20 の (i) の最初の主張が Coates-Wiles による定理 3.18 であるが, 岩澤主予想を認めると $L(E,1) \neq 0$ のときに $Ш(E/\mathbb{Q})[p^\infty]$ の有限性と強い形の Birch, Swinnerton-Dyer 予想 (予想 1.13 (ii)) の p 部分まで示すことができるのである. (その場合の $Ш(E/\mathbb{Q})[p^\infty]$ の有限性は, Rubin が主予想の証明より前に Thaine の結果を拡張して示していた. [Rub2]) また, $Ш(E/\mathbb{Q})$ はいつでも有限であろうと予想されているので (予想 3.5), 系 3.20 の (ii) は定理 3.18 の逆にあたる結果である. これは $w_E = -1$ の場合には, 主予想の証明より前に Greenberg [Gre1] によって示されていた (定理 3.17 と定理 3.8 から従う.)

もし式 (3) を全ての p で示すことができれば, CM を持つ楕円曲線 E に対して $L(E,1) \neq 0$ の下で $Ш(E/\mathbb{Q})$ の有限性と Birch, Swinnerton-Dyer 予想が確かめられたことになるのだが, 系 3.20 では E が p で good ordinary reduction を持つと仮定していたので, 密度 $\frac{1}{2}$ の素数 p に対してしか示すことができない. しかし Rubin は E が p で good ordinary reduction を持たない場合にも, 上の系と同様の結果を証明している ([Rub3, Thm.11.18], [PoRu] 参照). それにより, $p = 2$ などを除くほとんど全ての素数で (3) がわかる. 更にある種の楕円曲線の族に対しては, 有限個の例外の素数の部分を別に処理することで $Ш(E/\mathbb{Q})$ の有限性と強い形の Birch, Swinnerton-Dyer 予想が成り立つことも確かめられている.

3.5 p 進 Birch, Swinnerton-Dyer 予想との関連

系 3.20 で $L(E,1) \neq 0$ の場合に Birch, Swinnerton-Dyer 予想の p 部分が主予想から導かれることを見たが, もともと主予想は p 進 L 関数と Selmer 群の関係を与えるものな

ので, p 進の Birch, Swinnerton-Dyer 予想というものを考える方が自然で, より強い結果が得られる.

まず E を $\mathbb{Q}$ 上の (CM とは限らない) 楕円曲線で, $p \geq 5$ で good ordinary reduction を持つようなものとする. $\kappa : \Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)) \to 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ を 1 の p 冪根への作用により得られる指標 (円分指標) とする.

定義 3.21. $\mathbb{Z}_p$ 上の関数 $L_p(E,s)$ を $L_p(E,s) := \kappa^{s-1}(\mathcal{L}_{E,p})$ と定める. ただし $\mathcal{L}_{E,p} \in \Lambda$ は定理 3.11 のもの.

この p 進 L 関数 $L_p(E,s)$ に対して, Birch, Swinnerton-Dyer 予想と同様の予想が成り立つであろうというのが, 次の p 進 Birch, Swinnerton-Dyer 予想である.

予想 3.22 (p 進 Birch, Swinnerton-Dyer 予想). (i) $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \mathrm{ord}_{s=1} L_p(E,s)$.

(ii) $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q})$ とするとき, 次の等式が成り立つ:

$$\lim_{s\to 1}(s-1)^{-r} L_p(E,s) \sim \frac{\#Ш(E/\mathbb{Q})[p^\infty] R_p(E/\mathbb{Q}) (\#\widetilde{E}_p(\mathbb{F}_p))^2 \prod_l c_l}{(\#E(\mathbb{Q})[p^\infty])^2}.$$

ただし, $R_p(E/\mathbb{Q})$ は (円分 $\mathbb{Z}_p$ 拡大に対応する) p 進 height pairing $\langle\ ,\ \rangle_{E,p} : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{Q}_p$ から, $R(E/\mathbb{Q})$ と同様に定義される p-adic regulator ([Sch] 等参照).

注. 予想の (i) を認めると (ii) の式の左辺は 0 ではないので, (ii) は特に $R_p(E/\mathbb{Q}) \neq 0$ も含んでいるのであるが, 一般にはそれもまだわかっていない.

注. E が p で split multiplicative reduction を持つ場合には, $L_p(E,s)$ は $s=1$ に「自明な零点」を持つので, 予想を修正する必要がある. [MTT] 参照.

定理 3.16 と定理 3.8 により, 次は容易にわかる.

命題 3.23. $E/\mathbb{Q}$ が CM のとき

$$\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \leq \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) + \mathrm{corank}_{\mathbb{Z}_p} Ш(E/\mathbb{Q})[p^\infty] \leq \mathrm{ord}_{s=1} L_p(E,s) \tag{4}$$

が成り立つ. ただし $\mathrm{corank}_{\mathbb{Z}_p}$ は Pontryagin dual の $\mathbb{Z}_p$-rank を表す.

実際, 式 (4) の左側の不等式は自明であり (等号成立は $Ш(E/\mathbb{Q})[p^\infty]$ が有限のとき), 右側の不等式は中央の項が定理 3.8 により $\mathfrak{X}_p(E/\mathbb{Q}_\infty)_\Gamma$ の $\mathbb{Z}_p$-rank に等しいことと, Λ 加群の構造定理から従う. 注意すべきことは, torsion Λ 加群 M の特性イデアルがわかっていても, それだけでは M_Γ の $\mathbb{Z}_p$-rank は上から評価することしかできないということである. (例えば γ を Γ の位相的生成元とするとき, $\Lambda/(\gamma-1)^2\Lambda$ と $(\Lambda/(\gamma-1)\Lambda)^{\oplus 2}$ の特性イデアルは等しいが, それらの Γ-coinvariant の $\mathbb{Z}_p$-rank は 1 および 2 と異なる.) 今の場合も, 定理 3.16 によって $\mathfrak{X}_p(E/\mathbb{Q}_\infty)$ の特性イデアルはわかっているが, (4) の右側の不等式を等式にするには Λ 加群としての構造がもう少しわかる必要がある. p 進 height pairing $\langle\ ,\ \rangle_{E,p}$ の非退化性を仮定すれば, より強い結果を得られる ([Sch], [Per1] 参照).

定理 3.24. E は CM, $Ш(E/\mathbb{Q})[p^\infty]$ は有限であり, $\langle\ ,\ \rangle_{E,p}$ は非退化であると仮定する. そのとき (4) は全て等式であり, 予想 3.22 の主張が成り立つ.

4 その他の結果

これまで, CM を持つ楕円曲線の Birch, Swinnerton-Dyer 予想と虚 2 次体上の岩澤主予想との関係を見てきたが, CM を持たない楕円曲線についても岩澤理論的な手法による結果がいくつか知られている.

4.1 Kolyvagin の結果

Euler 系の理論は Kolyvagin により考え出されたのであるが, その基となったのは Heegner 点と呼ばれる (modular な) 楕円曲線の有理点の族を使った, Mordell-Weil 群や Tate-Shafarevich 群の有限性に関する結果 ([Kol1]) であった.

$E/\mathbb{Q}$ を conductor N の楕円曲線とすると, (E は modular なので) modular 曲線 $X_0(N)$ から E への全射 φ が存在する. 一方, 楕円曲線とその位数 N の巡回部分群の組は $X_0(N)$ 上に有理点を定めるが, N の素因子が全て分解するような虚 2 次体 K の整数環 (または一般の order) に CM を持つような楕円曲線を考えると, それは K の Hilbert 類体 (またはあるアーベル拡大) 上の有理点を定める. (N が $\mathfrak{N}\overline{\mathfrak{N}}$ と分解するとき, $\mathfrak{N}$ 分点全体が位数 N の巡回部分群となる. 命題 1.19 (ii) を見よ.) $\varphi : X_0(N) \to E$ によるそれらの点の像たちを Heegner 点と呼ぶ. その Heegner 点は Euler 系をなしており, それを使って Kolyvagin は次を示した ([Kol2], [Gro] 参照).

定理 4.1 (Kolyvagin). $\mathrm{ord}_{s=1}L(E,s) \leq 1$ ならば予想 1.13 の (i) は正しい. またそのとき $Ш(E/\mathbb{Q})$ は有限.

注. L 関数の値などを使った $Ш(E/\mathbb{Q})$ の位数の上からの評価もある.

ただし実際にこの定理を示すためには Euler 系の議論の他に, 楕円曲線の (虚 2 次体上の) L 関数の導関数の特殊値と Heegner 点の height との関係を与える Gross-Zagier の公式 ([GrZa]) や, うまい虚 2 次体の存在を保証するための L 関数の特殊値に関する結果も使われる.

4.2 non-CM 楕円曲線の岩澤主予想

§3 では CM 楕円曲線の場合に, 虚 2 次体の岩澤主予想 (定理 2.13) から ordinary な楕円曲線の主予想 (予想 3.12) が従い, それから Coates-Wiles による Birch, Swinnerton-Dyer 予想に関する結果 (定理 3.18) や p 進 Birch, Swinnerton-Dyer 予想に関する結果が得られることを見た. しかし, §3 での議論や結果には CM でない場合にも適用できるものも多く, 例えば予想 3.12 が正しければ, 系 3.20 や命題 3.23 などは CM でない楕円曲線に対してもそのまま成り立つ. 予想 3.12 は今のところまだ完全な解決には至っていないが, 加藤は modular 曲線の K 群に元を作り, それから楕円曲線の cohomology 群に Euler 系を作ることで, 次の結果を示した.

定理 4.2 (加藤, [Kato]). $E/\mathbb{Q}$ は non-CM 楕円曲線で素数 p で good ordinary reduction を持つとする. そのとき $\mathfrak{X}_p(E/\mathbb{Q}_\infty)$ は Λ-torsion であり, その特性イデアルは $p^i\mathcal{L}_{E,p}$ を

含む (i はある非負整数).

予想 3.12 は $\mathrm{char}_\Lambda(\mathfrak{X}_p(E/\mathbb{Q}_\infty))$ とイデアル $(\mathcal{L}_{E,p})$ が等しいというものなので, そのうちの「一方の包含関係」がほぼ示されていることになる. この結果だけでも, §3 の議論で系 3.20(i) の有限性や命題 3.23 などを示すことが出来る.

「逆向きの包含関係」についても最近, Skinner, Urban らにより研究が進んでいるようである.

4.3 Heegner 点に関する Mazur の予想

E を $\mathbb{Q}$ 上の conductor N の楕円曲線とし, K を基本判別式が N と素であるような虚 2 次体とする. (仮定より $\mathrm{End}_{\overline{\mathbb{Q}}}(E)\otimes_{\mathbb{Z}}\mathbb{Q}\neq K$ となり, §3.3 の状況とは異なる.) N を K で分解する素数からなる因子 N^+ と K で惰性する素数からなる因子 N^- の積に分解する. p は N を割らない素数とする.

E が p で good ordinary reduction を持つとき, 加藤の定理により円分 $\mathbb{Z}_p$ 拡大 K_∞^+ 上での E の Selmer 群の Pontryagin dual $\mathfrak{X}_p(E/K_\infty^+)$ は Λ-torsion となるが, 反円分 $\mathbb{Z}_p$ 拡大 K_∞^- 上では必ずしも Λ-torsion ではなく, その Λ-rank は N の素因子の K での分解の様子と関係すると予想されている.

予想 4.3 ([Maz2, §18] 参照). E は p で good ordinary reduction を持つとし, N^- は square-free とする. N^- の素因子の個数を t と置くとき,

$$\mathrm{rank}_\Lambda(\mathfrak{X}_p(E/K_\infty^-))=\begin{cases}0 & t \text{ は奇数},\\ 1 & t \text{ は偶数}.\end{cases}$$

更に $N^-=1$ のとき, つまり N の素因子が全て K で分解するときには (Heegner hypothesis と呼ばれる), $\mathfrak{X}_p(E/K_\infty^-)$ の Λ-rank 1 は Heegner 点から来ると予想されている. §4.1 で述べたように $N^-=1$ のとき, K のアーベル拡大体上に E の有理点の系列 (Heegner 点) が作られるが, それを使って K_∞^-/K の中間体 K_n^- 上の有理点の norm 系列 $\{P_n\in E(K_n^-)\}$ が得られる ([Cor, Intro] 参照). この P_n は十分大きな n に対しては位数無限となるであろうというのが, (高次 Heegner 点に関する) Mazur の予想である ([Maz2, §19]). この予想は Vatsal と Cornut によって最近解決された.

定理 4.4 (Cornut [Cor], Vatsal [Vat2]). $P_n\notin E(K_n^-)_{\mathrm{tors}}$ となる $n\geq 0$ が存在する.

系 4.5 ([Maz2], [Ber]). $N^-=1$ のとき $E(K_\infty^-)\otimes_{\mathbb{Z}}\mathbb{Q}_p/\mathbb{Z}_p$ の Pontryagin dual は Λ-rank 1 であり, 予想 4.3 も正しい.

定理 4.4 は Nekovář による Birch, Swinnerton-Dyer 予想での偶奇性に関する次の結果 (parity 予想) の証明にも使われている.

定理 4.6 (Nekovář, [Nek]). E が p で good ordinary reduction を持つとき

$$\mathrm{ord}_{s=1}L(E,s)\equiv \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}))\pmod 2$$

である. 特に $Ш(E/\mathbb{Q})[p^\infty]$ が有限ならば $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})$ と $\mathrm{ord}_{s=1}L(E,s)$ の偶奇は等しい.

$\mathfrak{X}_p(E/K_\infty^-)$ が Λ-torsion となる場合の, 特性イデアルと p 進 L 関数の関係や岩澤 μ 不変量などに関しては [BeDa], [MaRu], [Vat1] 等を見よ.

参考文献

[AgHo] A. Agboola and B. Howard, *Anticyclotomic Iwasawa theory of CM elliptic curves*, preprint, 2003.

[Ber] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions*, Compos. Math. **99** (1995), 153–182.

[BeDa] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, to appear in Annals of Math.

[BSD] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. reine angew. Math. **218** (1965), 79–108.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[LNM] J. Coates, R. Greenberg, K. A. Ribet, and K. Rubin, "Arithmetic Theory of Elliptic Curves", Lecture Notes in Math., vol. 1716, Springer-Verlag, 1999.

[CW1] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. math. **39** (1977), 223-251.

[CW2] J. Coates and A. Wiles, *On p-adic L-functions and elliptic units*, J. Aust. Math. Soc., Ser. A **26** (1978), 1-25.

[Cor] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. math. **148** (2002), 495–523.

[deS] E. de Shalit, "Iwasawa Theory of Elliptic Curves with Complex Multiplication", Perspectives in Math., vol. 3, Academic Press, 1987.

[Gre1] R. Greenberg, *On the Birch and Swinnerton-Dyer conjecture*, Invent. math. **72** (1983), 241–265.

[Gre2] R. Greenberg, *Iwasawa theory for elliptic curves*, in [LNM], pp. 51–144.

[Gre3] R. Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compos. Math. **136** (2003), 255–297.

[Gro] B. H. Gross, *Kolyvagin's work on modular elliptic curves* in "L-functions and arithmetic (Durham, 1989)", LMS Lecture Notes, vol. 153, Cambridge University Press, 1991, pp. 235–256.

[GrZa] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. math. **84** (1986), 225–320.

[Hid] H. Hida, *Anticyclotomic main conjectures*, preprint, 2003.

[HiTi] H. Hida and J. Tilouine, *On the anticyclotomic main conjecture for CM fields*, Invent. math. **117** (1994), 89–147.

[Kato] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, to appear.

[Katz] N. Katz, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. **104** (1976), 459–571.

[Kob] S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. math. **152** (2003), 1–36.

[Kol1] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $Ш(E,\mathbf{Q})$ for a subclass of Weil curves*, Math. USSR Izv. **32** (1989), 523–541.

[Kol2] V. A. Kolyvagin, *Euler systems*, in "The Grothendieck Festschrift, Vol. II", Birkhäuser, 1990, pp. 435–483.

[Kur1] 栗原 将人, 岩澤理論の一般化についての概説, 京大数理研講究録, **925** (1995), 53–65.

[Kur2] M. Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*, Invent. math. **149** (2002), 195–224.

[Man] Ju. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), 7–78.

[Maz1] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. math. **18** (1972), 183–266.

[Maz2] B. Mazur, *Modular curves and arithmetic*, in Proceedings of the ICM, Warszawa 1983, vol. 1, pp. 185–211.

[MaRu] B. Mazur and K. Rubin, *Elliptic curves and class field theory*, in Proceedings of the ICM, Beijing 2002, vol. II, pp. 185–195.

[MaSw] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. math. **25** (1974), 1–61.

[MTT] B. Mazur, J. Tate and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. math. **84** (1986), 1–48.

[MaTi] B. Mazur et J. Tilouine, *Représentations galoisiennes, différentielles de Kähler et "conjecture principales"*, Inst. Hautes Études Sci. Publ. Math. **71** (1990), 65–103.

[Nek] J. Nekovář, *On the parity of ranks of Selmer groups II*, C. R. Acad. Sci. Paris, Ser. I, **332** (2001), 99–104.

[Per1] B. Perrin-Riou, *Descente infinie et hauteur p-adique sur les courbes elliptiques à multiplication complexe*, Invent. math. **70** (1983), 369–398.

[Per2] B. Perrin-Riou, *Arithmétique des courbes elliptiques et théorie d'Iwasawa*, Mém. Soc. Math. France (N.S.) **17** (1984), 1–130.

[Pol] R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), 523–558.

[PoRu] R. Pollack and K. Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, preprint, 2003.

[Rob] G. Robert, *Unités elliptiques*, Bull. Soc. Math. France, Mémoir **36** (1973).

[Roh] D. E. Rohrlich, *On L-function of elliptic curves and cyclotomic towers*, Invent. math. **75** (1984), 409–423.

[Rub1] K. Rubin, *Elliptic curves and $\mathbb{Z}_p$-extensions*, Compos. Math. **56** (1985), 237–250.

[Rub2] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. math. **89** (1987), 527–560.

[Rub3] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. math. **103** (1991), 25–68.

[Rub4] K. Rubin, *More "main conjectures" for imaginary quadratic fields*, in "Elliptic Curves and Related Topics", CRM Proc. and Lecture Notes, vol. 4, AMS, 1994, pp. 23–28.

[Rub5] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, in [LNM], pp. 167–234.

[Sch] P. Schneider, *p-adic height pairings. II*, Invent. math. **79** (1985), 329–374.

[Sil1] J. H. Silverman, "The arithmetic of Elliptic Curves", Grad. Texts in Math., vol. 106, Springer-Verlag, 1986.

[Sil2] J. H. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves", Grad. Texts in Math., vol. 151, Springer-Verlag, 1994.

[Til] J. Tilouine, *Sur la conjecture principale anticyclotomique*, Duke Math. J. **59** (1989), 629–673.

[Vat1] V. Vatsal, *Uniform distribution of Heegner points*, Invent. math. **148** (2002), 1–46.

[Vat2] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), 219–261.

[Yag] R. Yager, *On two variable p-adic L-functions*, Ann. of Math. **115** (1982), 411–449.

東京都立大学大学院理学研究科数学専攻
〒 192-0397 東京都八王子市南大沢 1-1
matsuno@comp.metro-u.ac.jp