λ不変量が3である岩澤加群の同型類を決定する新しい不変量について

村上 和明 (慶應義塾大学)

1 はじめに

p を奇素数, $\Lambda = \mathbb{Z}_p[[T]]$ を p 進整数環 $\mathbb{Z}_p$ 上の一変数冪級数環とする. Λ が作用する加群の構造の研究は岩澤理論において重要である. 環 Λ の性質より, Λ-加群の構造は擬同型類まで分類することができる. 本稿はいくつかの条件のもとで λ 不変量が 3 である Λ-加群の同型類を決定する不変量について考える. また, 得られた結果を楕円曲線の岩澤理論へ応用する.

まず, 以下の問題を考えたい.

問題 1. 有限生成ねじれ Λ-加群について, その特性イデアルよりも詳しい情報は得られるか?

有限生成ねじれ Λ-加群 M に対して, その特性イデアル $\mathrm{char}(M)$ は M の Λ-加群としての構造を知るうえで最も重要な不変量である. 岩澤理論では代数体に付随する岩澤加群の特性イデアルは, p 進 L 関数の代数的な側面と考えることができる.

この他に, 高次 Fitting イデアルも Λ-加群として構造を知るうえで重要な不変量である. Λ-加群 M の高次 Fitting イデアルは M の有限表示から定義される行列の小行列式たちで生成されるイデアルである (正確な定義は後で述べる). 特に, $\mathbb{Z}_p$-自由な Λ-加群の 0 次 Fitting イデアルはその特性イデアルであることを注意しておく. 一般に, Λ-加群 M の高次 Fitting イデアルは M の擬同型類を決定することが知られているが, M の同型類を決定することはできない ([7], Remark 9.4). それゆえ, M の同型類を知るためには M のより詳細な情報が必要となる.

この様な問題に関して, distinguished 多項式 $f(T)$ を一つ固定して次の集合を考える:

$$\mathcal{M}_{f(T)} = \left\{ [M]_{\mathbb{Q}_p} \;\middle|\; \begin{array}{l} M \text{ は有限生成ねじれ } \Lambda\text{-加群}, \\ \mathrm{char}(M) = (f(T)),\ M \text{ は自由 } \mathbb{Z}_p\text{-加群} \end{array} \right\}.$$

ここで, $[M]_{\mathbb{Q}_p}$ は M の Λ-加群としての同型類を表す (M の Λ-同型類を $[M]_{\mathbb{Q}_p}$ や $[M]$ で表す). $\mathcal{M}_{f(T)}$ は $f(T)$ が重根を持たないときに限り有限集合になる ([15], Thoerem 2). $\deg f(T) = 1$ の場合は, $\mathcal{M}_{f(T)} = \{[\Lambda/(f(T))]\}$ である. $\deg f(T) = 2$ の場合は, 隅田氏と小池氏の研究により $\mathcal{M}_{f(T)}$ が決定されている ([4], [15]). 栗原氏は高次 Fitting イデアルを用いて $\mathcal{M}_{f(T)}$ を決定している ([6], Corollary 9.3). また, 隅田氏と小池氏の研究手法により, $\deg f(T) = 3$ と $\deg f(T) = 4$ の場合も $\mathcal{M}_{f(T)}$ が決定されている ([10], [11]).

本稿は

$$f(T) = (T-\alpha)(T-\beta)(T-\gamma)$$

と仮定する. ここで α, β, γ は相異なる $p\mathbb{Z}_p$ の元である. $\mathcal{E}(\alpha, \beta, \gamma) = \Lambda/(T-\alpha) \oplus \Lambda/(T-\beta) \oplus \Lambda/(T-\gamma)$ とおく. Λ-加群の構造定理により, Λ-加群 M で $[M] \in \mathcal{M}_{f(T)}$ を満たすもの

を $\mathcal{E}(\alpha,\beta,\gamma)$ の Λ-部分加群とみなすことができる．さらに，各同型類 $\mathfrak{C} \in \mathcal{M}_{f(T)}$ に対して，$\mathcal{E}(\alpha,\beta,\gamma)$ の部分加群

$$M(m,n,x) := \langle (1,1,1), (0,p^m,x), (0,0,p^n) \rangle_{\mathbb{Z}_p}$$

で $[M(m,n,x)] = \mathfrak{C}$ を満たすものが取れる (次節で詳しく述べる)．ここで $\langle * \rangle_{\mathbb{Z}_p}$ は $*$ で生成される $\mathbb{Z}_p$-部分加群を表し，m と n は非負整数，x は $\mathbb{Z}_p$ の元である．m と n は同型類 $[M(m,n,x)]$ で決まる不変量である ([10], Corollary 4.2)．

M を有限生成ねじれ Λ-加群とし，$[M] = [M(m,n,x)]$ を満たとする．このとき，

$$s(M) = m + n$$

と定義する．$s(M)$ は α,β,γ の順番に依存しないことが証明できる (命題 2.3)．

本稿の最初の主定理は M の Λ-同型類がその 1 次 Fitting イデアルと不変量 $s(M)$ で決定されることである:

定理 1.1. $[M]_{\mathbb{Q}_p}, [M']_{\mathbb{Q}_p} \in \mathcal{M}_{f(T)}$ とする．このとき，以下のことは同値である．

(i) $M \cong M'$.

(ii) $s(M) = s(M')$, $\mathrm{Fitt}_{1,\Lambda}(M) = \mathrm{Fitt}_{1,\Lambda}(M')$, ここで $\mathrm{Fitt}_{1,\Lambda}(M)$ と $\mathrm{Fitt}_{1,\Lambda}(M')$ は M, M' の 1 次 Fitting イデアルである．

上述の定理はより一般に有限次拡大 $K/\mathbb{Q}$ に対して，$f(T)$ が K 上の分離的な distinguished 多項式であれば成立することを注意しておく．次に，定理 1.1 の岩澤理論への応用として以下の問題を考えたい．

問題 2. 有限生成ねじれ Λ-加群 M に対して，$s(M)$ の数論的な意味は何か?

この問題に関して，楕円曲線に付随する Selmer 群を考える．$K/\mathbb{Q}$ を有限次拡大，E を $\mathbb{Q}$ 上の楕円曲線とする．奇素数 p を固定し，E は p で good ordinary reduction を持つと仮定する．自然数 $n \geq 0$ に対して，$\mathbb{Q}_n$ を $\mathbb{Q}_\infty$ の $\mathbb{Q}$ 上 p^n 次である唯一の中間体とする．$E[p^\infty]$ を E の p 冪等分点とする．E に対する K 上の p-Selmer 群を $\mathrm{Sel}_p(E,K)$ で表し，その Pontrjagin 双対を $X_p(E,K)$ と書く．

さらに，無限次拡大における Selmer 群を

$$\mathrm{Sel}_p(E,\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}_p(E,\mathbb{Q}_n)$$

で定義する．但し，順極限はコホモロジー群における制限写像でとる．また，$\mathrm{Sel}_p(E,\mathbb{Q}_\infty)$ の Pontrjagin 双対を $X_p(E,\mathbb{Q}_\infty)$ と表すことにする．このとき，$X_p(E,\mathbb{Q}_\infty)$ は有限生成ねじれ $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$-加群になることが知られている．$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ の位相的生成元を一つ固定して得られる環同型 $\Lambda = \mathbb{Z}_p[[T]] \cong \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$ により，$X_p(E,\mathbb{Q}_\infty)$ は有限生成 Λ-加群になることがわかる．本稿では $X_p(E,\mathbb{Q}_\infty)$ の Λ-加群としての同型類をいくつかの条件のもとで決定したい．以下のことを仮定する．p は玉河数を割らない．$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の $T_p(E)$ への作用は全射的である．$(E,\mathbb{Q}_\infty/\mathbb{Q})$ の μ 不変量は 0 で，p は anomalous でないとする．ここで $\overline{\mathbb{Q}}$ は $\mathbb{Q}$ の代数的閉包，$T_p(E)$ は E の Tate 加群である．これらの条件を $(\sharp)$ と書くことにする．ord_p を正規化された p 進付値とする．$[X_p(E,\mathbb{Q}_\infty)] \in \mathcal{M}_{f(T)}$ とするとき，以下の定理により $s(X_p(E,\mathbb{Q}_\infty))$ と $X_p(E,\mathbb{Q}_\infty)$ の同型類を決定することができる．

定理 1.2. E を $\mathbb{Q}$ 上の楕円曲線とする. Ш$(E/\mathbb{Q})$ の p-成分は有限で E は条件 (♯) を満たすとする. ここで, Ш$(E/\mathbb{Q})$ は E の $\mathbb{Q}$ 上の Tate-Shafarevich 群である. さらに, $[X_p(E,\mathbb{Q}_\infty)] \in \mathcal{M}_{f(T)}$, $f(T) = T(T-\beta)(T-\gamma) \in \mathbb{Z}_p[T]$ は分離的な distinguished 多項式であるとする. このとき,

$$\begin{aligned} X_p(E,\mathbb{Q}_\infty) &\cong M\left(\frac{1}{3}s, \frac{2}{3}s, \frac{\gamma}{\beta}p^{\frac{1}{3}s}\right) \\ &= \left\langle (1,1,1), (0, p^{\frac{1}{3}s}, \frac{\gamma}{\beta}p^{\frac{1}{3}s}), (0,0,p^{\frac{2}{3}s}) \right\rangle_{\mathbb{Z}_p} \\ &\subset \Lambda/(T) \oplus \Lambda/(T-\beta) \oplus \Lambda/(T-\gamma). \end{aligned}$$

但し, $s = s(X_p(E,\mathbb{Q}_\infty)) = 3\left(\mathrm{ord}_p(\beta) - \frac{1}{2}\mathrm{ord}_p(\#Ш(E/\mathbb{Q}))\right)$.

3 節で上述の定理の証明を与える. 証明のポイントは楕円曲線 E が条件 (♯) が満たすとき, $X_p(E,\mathbb{Q}_\infty)$ の行列表示を skew-Hermitian になるよう選ぶことができるという点である ([6], [9]). 行列が skew-Hermitian であることは定義 3.1 で述べる.

最後に, 補足として $f(T)$ が 2 次式に場合についての結果を述べる.

$$f(T) = (T-\alpha)(T-\beta)$$

とおく. 但し, α と β は相異なる $p\mathbb{Z}_p$ の元である. 先ほどと同様に楕円曲線 E は (♯) を満たすと仮定する. Mazur-Rubin ([9], Proposition 9.2.1) と小池氏 ([4], Theorem 2.1) の結果を合わせることで次を示すことができる.

定理 1.3. E を $\mathbb{Q}$ 上の楕円曲線とする. Ш$(E/\mathbb{Q})$ の p-成分は有限で E は条件 (♯) を満たすとする. さらに, $[X_p(E,\mathbb{Q}_\infty)] \in \mathcal{M}_{f(T)}$, $f(T) = (T-\alpha)(T-\beta) \in \mathbb{Z}_p[T]$ は分離的な distinguished 多項式であるとする. このとき,

$$X_p(E,\mathbb{Q}_\infty) \cong \Lambda/(T-\alpha) \oplus \Lambda/(T-\beta).$$

2 準備

p を奇素数, K を p 進体 $\mathbb{Q}_p$ 上の有限次拡大体, $\mathcal{O}_K$ を K の整数環とする. また, π を K の素元, ord_K を K の正規化された付値とし, $\Lambda_K := \mathcal{O}_K[[T]]$ と表すことにする. Λ_K-加群の構造定理 (cf. [17], Chapter 13) により, Λ_K-準同型写像

$$\varphi : M \longrightarrow (\bigoplus_i \Lambda_K/(\pi^{m_i})) \oplus (\bigoplus_j \Lambda_K/(f_j(T)^{n_j}))$$

で kernel と cokernel が有限になるものが存在する. ここで, m_i, n_j は非負整数, $f_j(T) \in \mathcal{O}_K[T]$ は既約な distinguished 多項式である. M の特性イデアルを

$$\mathrm{char}(M) = (\prod_i \pi^{m_i} \prod_j f_j(T)^{n_j})$$

と定義する.

前節と同様に固定された distinguished 多項式 $f(T)$ に対して, 特性イデアルが $f(T)$ で生成される有限生成ねじれ Λ_K-加群の集合 $\mathcal{M}_{f(T)}^K$ を導入する:

$$\mathcal{M}_{f(T)}^K = \left\{ [M]_K \;\middle|\; \begin{array}{l} M \text{ は有限生成ねじれ } \Lambda_K\text{-加群}, \\ \mathrm{char}(M) = (f(T)),\ M \text{ は自由 } \mathcal{O}_K\text{-加群} \end{array} \right\}.$$

ここで $[M]_K$ は M の Λ_K-同型類を表すことにする. 前節で述べたとおり, 本稿では

$$f(T) = (T-\alpha)(T-\beta)(T-\gamma) \tag{1}$$

の場合を考える. ここで α, β, γ は相異なる $\pi\mathcal{O}_K$ の元である. Λ-加群の標準的な表示の仕方を述べたい. $[M]_K \in \mathcal{M}_{f(T)}^K$ とする. M は非自明な有限 Λ_K-部分加群を持たないので, 単射な Λ_K-準同型写像

$$\varphi(\alpha,\beta,\gamma) : M \hookrightarrow \Lambda_K/(T-\alpha) \oplus \Lambda_K/(T-\beta) \oplus \Lambda_K/(T-\gamma) =: \mathcal{E}(\alpha,\beta,\gamma)$$

で cokernel が有限になるものが存在する. 右辺を $\mathcal{E}(\alpha,\beta,\gamma)$ と表すことにする. 上述より, 各 $\mathcal{M}_{f(T)}^K$ の類は $\mathcal{E}(\alpha,\beta,\gamma)$ の Λ_K-部分加群として表すことができる.

$\mathcal{E}(\alpha,\beta,\gamma)$ の部分加群の表示を以下のように固定しよう. まず標準的な同型写像 $\Lambda_K/(T-\alpha) \cong \mathcal{O}_K$ $(f(T) \longmapsto f(\alpha))$ を用いて, 同型写像

$$\iota(\alpha,\beta,\gamma) : \mathcal{E}(\alpha,\beta,\gamma) = \Lambda_K/(T-\alpha) \oplus \Lambda_K/(T-\beta) \oplus \Lambda_K/(T-\gamma) \longrightarrow \mathcal{O}_K^{\oplus 3}$$

を $(f_1(T), f_2(T), f_3(T)) \longmapsto (f_1(\alpha), f_2(\beta), f_3(\gamma))$ で定義する. $\iota(\alpha,\beta,\gamma)$ によって, $\mathcal{E}(\alpha,\beta,\gamma)$ と $\mathcal{O}_K^{\oplus 3}$ を同一視することにする. 従って, $\mathcal{E}(\alpha,\beta,\gamma)$ の元は $(a_1,a_2,a_3) \in \mathcal{O}_K^{\oplus 3}$ の形で表せる. M の $\mathbb{Z}_p$-ランクは 3 であるので, M を

$$M = \langle (a_1,a_2,a_3), (b_1,b_2,b_3), (c_1,c_2,c_3) \rangle_{\mathcal{O}_K} \subset \mathcal{E}(\alpha,\beta,\gamma)$$

と表すことができる. ここで $\langle * \rangle_{\mathcal{O}_K}$ は $*$ で生成される $\mathcal{O}_K$-部分加群を表す. さらに, T の作用はこの表示により

$$T(a_1,a_2,a_3) = (\alpha a_1, \beta a_2, \gamma a_3)$$

となる. また, $M(m,n,x)$ を

$$M(m,n,x) := \langle (1,1,1), (0,\pi^m,x), (0,0,\pi^n) \rangle_{\mathcal{O}_K} \subset \mathcal{E}(\alpha,\beta,\gamma)$$

と定義する. 次の命題により, $\mathcal{M}_{f(T)}^K$ の元は $(*)$ を満たす三つ組で表すことができる.

命題 2.1 (Proposition 3.3, [10])**.** $f(T) \in \mathcal{O}_K[T]$ を (1) と同じ distinguished 多項式とする. このとき

$$\mathcal{M}_{f(T)}^K = \{ [M(m,n,x)]_K \mid m,n,x \text{ は } (*) \text{ を満たす } \},$$

$$(*) \begin{cases} \text{(A) } 0 \le m \le \mathrm{ord}_K(\beta-\alpha), \\ \text{(B) } 0 \le n \le \mathrm{ord}_K(\gamma-\beta) + \mathrm{ord}_K(x), \\ \text{(C) } n \le \mathrm{ord}_K\{(\gamma-\alpha) - (\beta-\alpha)\pi^{-m}x\}. \end{cases}$$

次に本稿の 1 節に述べた不変量と高次 Fitting イデアルを定義する.

定義 2.2. $[M]_K \in \mathcal{M}^K_{f(T)}$ とする. $[M]_K = [M(m,n,x)]_K$ であるとき,

$$s(M) = m + n$$

と定義する.

$s(M)$ について以下のことが成り立つ. 証明は [12] を参照せよ.

命題 2.3. (1) $s(M)$ は三つ組 (m,n,x) の取り方に依らない.
(2) $s(M)$ は Λ_K-準同型写像 $\varphi(\alpha,\beta,\gamma)$ と α,β,γ の順番の取り方に依らない.

次に, 高次 Fitting イデアルの定義を述べる. 可換環 R と有限表示を持つ R-加群 M に対して, 次の完全列

$$R^m \xrightarrow{f} R^n \to M \to 0$$

を考える. ここで, m と n は正の整数である. $0 \leq i < n$ を満たす整数 i に対して, M の i 次 Fitting イデアルは f に対応する行列の全ての $(n-i)\times(n-i)$ 次小行列式で生成される R のイデアルである. M の i 次 Fitting イデアルを $\mathrm{Fitt}_{i,R}(M)$ と書くことにする. この定義は完全列の取り方に依らないことを注意しておく ([13]).

本稿の最初の主定理は $[M] \in \mathcal{M}_{f(T)}$ を満たす M の同型類は不変量 $s(M)$ と $\mathrm{Fitt}_{1,\Lambda}(M)$ で決まるというものである. 証明は [12] を参照せよ.

定理 2.4. $[M]_K, [M']_K \in \mathcal{M}^K_{f(T)}$ とする. このとき以下のことは同値である.
(i) $M \cong M'$.
(ii) $s(M) = s(M')$, $\mathrm{Fitt}_{1,\Lambda_K}(M) = \mathrm{Fitt}_{1,\Lambda_K}(M')$.

3 定理 1.2 の証明

E を $\mathbb{Q}$ 上の楕円曲線とする. 奇素数 p を固定し, E は p で良い還元を持つと仮定する. 有限次拡大 $K/\mathbb{Q}$ に対して, E の K 上の p-Selmer 群を

$$\mathrm{Sel}_p(E,K) = \ker\left(H^1(K, E[p^\infty]) \to \prod_v \frac{H^1(K_v, E[p^\infty])}{E(K_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p}\right)$$

と定義する. ここで, $E[p^\infty]$ は E の p 冪等分点, v は K の全ての素点を走り, $E(K_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ を Kummer 準同型の像と同一視する.

$\mathbb{Q}_\infty/\mathbb{Q}$ を $\mathbb{Q}$ の円分 $\mathbb{Z}_p$-拡大. $n \geq 0$ に対して, $\mathbb{Q}_n$ を $\mathbb{Q}$ 上の拡大次数が p^n となる唯一の中間体を表すとする. 円分 $\mathbb{Z}_p$-拡大 $\mathbb{Q}_\infty/\mathbb{Q}$ に対して, その Selmer 群を

$$\mathrm{Sel}_p(E,\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}_p(E,\mathbb{Q}_n)$$

で定義する. ここで, 順極限はコホモロジー群における制限写像でとる. また, その Pontrjagin 双対を

$$X_p(E,\mathbb{Q}_\infty) = \mathrm{Hom}(\mathrm{Sel}_p(E,\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

と定義する. このとき, $X_p(E,\mathbb{Q}_\infty)$ は有限生成ねじれ $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$-加群になることが知られている ([5]). $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ の位相的生成元を一つ固定して得られる環同型 $\Lambda = \mathbb{Z}_p[[T]] \cong$

$\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]]$ により, $X_p(E,\mathbb{Q}_\infty)$ は有限生成 Λ-加群になることがわかる ([5]). 岩澤主予想により, その特性イデアルは p 進 L 関数で生成される:

$$\mathrm{char}(X_p(E,\mathbb{Q}_\infty)) = (L_p(E,T)).$$

ここで, $L_p(E,T)$ は楕円曲線 E に付随する p 進 L 関数である.

$\overline{\mathbb{Q}}$ を $\mathbb{Q}$ の代数的閉包, $T_p(E)$ を E の Tate 加群とする. 以下の 4 つの条件を仮定する.

$$(\sharp)\begin{cases}(1)\ E \text{ は } p \text{ で good ordinary reduction を持つ.}\\ (2)\ p \text{ は玉河数を割らない.}\\ (3)\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \text{ の } T_p(E) \text{ への作用は全射的である.}\\ (4)\ p\text{anomalous でない, つまり } \#E(\mathbf{F}_p) \not\equiv 0 \mod p.\end{cases}$$

K を $\mathbb{Q}_p$ の有限次拡大体とする. $\iota : \Lambda_K \longrightarrow \Lambda_K$ を K の標準的な involution, つまり

$$\iota(1+T) = (1+T)^{-1}$$

を満たす同型写像とする.

定義 3.1. 行列 $A = (a_{ij})_{ij} \in \mathrm{M}_n(\Lambda_K)$ が skew-Hermitian であるとは, A の成分が $a_{ij} = -\iota(a_{ji})$ を満たすことと定義する. 行列 $A = (a_{ij})_{ij}$ に対して, 行列 $(\iota(a_{ji}))_{ij}$ を A^* で表す.

楕円曲線 E は条件 $(\sharp)$ を満たすとし, $(E,\mathbb{Q}_\infty/\mathbb{Q})$ における μ 不変量は 0 と仮定する. 以下の定理は主定理 1.2 の証明に必要である.

定理 3.2 ([8], Lemma 10.3, [9], Theorem 7.5)**.** p を奇素数, E を $\mathbb{Q}$ 上の楕円曲線とする. E が条件 $(\sharp)$ を満たすと仮定するとき, $X_p(E,\mathbb{Q}_\infty)$ に対応する行列が skew-Hermitian になるように選ぶことができる.

以下のような場合を考えよう:

$$\mathrm{char}(X_p(E,\mathbb{Q}_\infty)) = ((T-\alpha)(T-\beta)(T-\gamma)).$$

以下を準備する.

補題 3.3. p を奇素数, E を $\mathbb{Q}$ 上の楕円曲線とする. E は条件 $(\sharp)$ を満たし, $\mathrm{char}(X_p(E,\mathbb{Q}_\infty)) = ((T-\alpha)(T-\beta)(T-\gamma))$, $\mathrm{ord}_K(\gamma) \le \mathrm{ord}_K(\beta) \le \mathrm{ord}_K(\alpha)$ であるとする. ここで, α,β,γ は $p\mathbb{Z}_p$ の相異なる元である. このとき,

$$\alpha = 0, \quad \gamma = -\frac{\beta}{1+\beta}$$

である.

証明. ([2], Theorem 1.14) より,

$$((T-\alpha)(T-\beta)(T-\gamma)) = (\iota((T-\alpha)(T-\beta)(T-\gamma)))$$

を得る. 右辺は

$$\left(\frac{1}{1+T} - (\alpha+1)\right)\left(\frac{1}{1+T} - (\beta+1)\right)\left(\frac{1}{1+T} - (\gamma+1)\right).$$

従って

$$\alpha = -\frac{\alpha}{1+\alpha}, \quad \alpha = -\frac{\beta}{1+\beta} \quad \text{または} \quad \alpha = -\frac{\gamma}{1+\gamma}.$$

まず$\alpha = -\dfrac{\beta}{1+\beta}$と仮定する. このとき, $\beta = -\dfrac{\alpha}{1+\alpha}$ または$\beta = -\dfrac{\gamma}{1+\gamma}$ である. $\beta = -\dfrac{\alpha}{1+\alpha}$ の場合は$\gamma = -\dfrac{\gamma}{1+\gamma}$ である. それゆえ $\gamma = 0$ または$\gamma = 2$ である. p は奇素数なので $\gamma = 0$ であることがわかる. $\mathrm{ord}_K(\gamma) \leq \mathrm{ord}_K(\beta) \leq \mathrm{ord}_K(\alpha)$ より, $\alpha = \beta = \gamma = 0$ である. これは仮定に矛盾する. $\beta = -\dfrac{\gamma}{1+\gamma}$ の場合は, $\alpha = \gamma$ である. さらに $\gamma = -\dfrac{\alpha}{1+\alpha}$ であるので $\alpha = \beta = \gamma = 0$ である. これも仮定に矛盾する. 次に $\alpha = -\dfrac{\gamma}{1+\gamma}$ と仮定する. 上述と同じ手法で, $\alpha = \beta = \gamma = 0$ となる. これも仮定に矛盾する. 従って $\alpha = -\dfrac{\alpha}{1+\alpha}$ であることがわかる. α は単数ではないので, $\alpha = 0$ である. また, α, β, γ は相異なるため, $\gamma = -\dfrac{\beta}{1+\beta}$ である. □

補題 3.4. $A \in \mathrm{M}_n(\Lambda_K)$ とする. ある行列 $P \in \mathrm{GL}_n(\Lambda_K)$ と $Q \in \mathrm{GL}_n(\Lambda_K)$ が存在して PAQ が skew-Hermitian になると仮定する. このとき, ある行列 $Y \in \mathrm{GL}_n(\Lambda_K)$ が存在して YA が skew-Hermitian になる.

証明. $B = PAQ$ とおく. このとき $B^* = -B$ である. $B^* = Q^*A^*P^*$ であるため,

$$(Q^*)^{-1}PAQ(P^*)^{-1} = -A^*$$

である. $Y = (P^*Q^{-1})^*$ とおく. このとき $YA(Y^*)^{-1} = -A^*$. であるので,$-YA = (YA)^*$ が成り立つ. □

定理 3.5. $f(T) = T(T-\beta)(T-\gamma) \in \mathcal{O}_K[T]$ を分離的な distinguished 多項式とする. $[M]_K \in \mathcal{M}^K_{f(T)}$, $\gamma = -\dfrac{\beta}{1+\beta}$ とする. また, M のある基底に関する行列表示が skew-Hermitian であると仮定する. このとき,

$$\begin{aligned} M &\cong M\left(\frac{1}{3}s(M), \frac{2}{3}s(M), \frac{\gamma}{\beta}\pi^{\frac{1}{3}s(M)}\right) \\ &= \left\langle (1,1,1), (0, \pi^{\frac{1}{3}s(M)}, \frac{\gamma}{\beta}\pi^{\frac{1}{3}s(M)}), (0,0,\pi^{\frac{2}{3}s(M)}) \right\rangle_{\mathcal{O}_K} \\ &\subset \Lambda_K/(T) \oplus \Lambda_K/(T-\beta) \oplus \Lambda_K/(T-\gamma), \end{aligned}$$

但し, $\mathrm{s}(M)$ は定義 2.2 で定義した値である.

証明. 命題 2.1 より三つ組 (m,n,x) で $M \cong M(m,n,x)$ を満たすものが存在する. Auslander-Buchsbaum の完全列により, 完全列

$$0 \to \Lambda_K \otimes_{\mathcal{O}_K} M \xrightarrow{\Phi} \Lambda_K \otimes_{\mathcal{O}_K} M \xrightarrow{\Psi} M \to 0$$

が存在する. ここで Φ と Ψ は $a \in \Lambda_K$ と $m \in M$ に対して以下で定義される:

$$\begin{aligned} \Phi(a \otimes m) &= Ta \otimes m - a \otimes Tm, \\ \Psi(a \otimes m) &= am, \end{aligned}$$

$(1,1,1),(0,\pi^m,x),(0,0,\pi^n)$ を M の基底として取ると, それらに対する行列表示は

$$\begin{pmatrix} T & 0 & 0 \\ \beta\pi^{-m} & T-\beta & 0 \\ -(\gamma-\beta\pi^{-m}x)\pi^{-n} & (\gamma-\beta)x\pi^{-n} & T-\gamma \end{pmatrix}$$

と同値である. まず $m>0$ を仮定する. T による剰余を考えることで,

$$A \equiv \begin{pmatrix} 0 & 0 & 0 \\ \beta\pi^{-m} & -\beta & 0 \\ -(\gamma-\beta\pi^{-m}x)\pi^{-n} & (\gamma-\beta)x\pi^{-n} & -\gamma \end{pmatrix} \mod T$$

が成り立つ. 補題 3.4 より, 行列 $Y=(a_{ij}(T))_{ij}\in \mathrm{GL}_3(\Lambda_K)$ が存在して YA が skew-Hermitian になる. $a_{ij}(T)=\sum_{k=0}^{\infty} a_{ij}^{(k)}T^k$ $(a_{ij}^{(k)}\in\mathcal{O}_K)$ とおく. このとき

$$\begin{aligned} YA &\equiv \begin{pmatrix} a_{11}^{(0)} & a_{12}^{(0)} & a_{13}^{(0)} \\ a_{21}^{(0)} & a_{22}^{(0)} & a_{23}^{(0)} \\ a_{31}^{(0)} & a_{32}^{(0)} & a_{33}^{(0)} \end{pmatrix} A \mod T \\ &\equiv \begin{pmatrix} a_{12}^{(0)}\beta\pi^{-m}-a_{13}^{(0)}(\gamma-\beta\pi^{-m}x)\pi^{-n} & a_{13}^{(0)}(\gamma-\beta)x\pi^{-n}-a_{12}^{(0)}\beta & -a_{13}^{(0)}\gamma \\ a_{22}^{(0)}\beta\pi^{-m}-a_{23}^{(0)}(\gamma-\beta\pi^{-m}x)\pi^{-n} & a_{23}^{(0)}(\gamma-\beta)x\pi^{-n}-a_{22}^{(0)}\beta & -a_{23}^{(0)}\gamma \\ a_{32}^{(0)}\beta\pi^{-m}-a_{33}^{(0)}(\gamma-\beta\pi^{-m}x)\pi^{-n} & a_{33}^{(0)}(\gamma-\beta)x\pi^{-n}-a_{32}^{(0)}\beta & -a_{33}^{(0)}\gamma \end{pmatrix} \mod T \end{aligned}$$

となる. YA は skew-Hermitian であることにより,

$$a_{12}^{(0)}\beta\pi^{-m}-a_{13}^{(0)}(\gamma-\beta\pi^{-m}x)\pi^{-n}=0, \tag{2}$$
$$-a_{22}^{(0)}\beta+a_{23}^{(0)}(\gamma-\beta)x\pi^{-n}=0, \tag{3}$$
$$a_{33}^{(0)}\gamma=0, \tag{4}$$
$$a_{32}^{(0)}\beta\pi^{-m}-a_{33}^{(0)}(\gamma-\beta\pi^{-m}x)\pi^{-n}=a_{13}^{(0)}\gamma, \tag{5}$$
$$a_{22}^{(0)}\beta\pi^{-m}-a_{23}^{(0)}(\gamma-\beta\pi^{-m}x)\pi^{-n}=a_{12}^{(0)}\beta-a_{13}^{(0)}(\gamma-\beta)x\pi^{-n}, \tag{6}$$
$$-a_{32}^{(0)}\beta+a_{33}^{(0)}(\gamma-\beta)x\pi^{-n}=a_{23}^{(0)}\gamma \tag{7}$$

を得る. (4) により, $a_{33}^{(0)}=0$ がわかる. $m>0$ と (5) を用いて, $a_{32}^{(0)}\equiv 0 \mod p$ を得る. また, (7) から, $a_{23}^{(0)}\equiv 0 \mod p$ である. Y は可逆なので, $\det(Y)\not\equiv 0 \mod p$ である. ここで $\det(Y)$ は Y の行列式である. それゆえ $a_{13}^{(0)}, a_{22}^{(0)}\in\mathbb{Z}_p^{\times}$. (2) から

$$x=\frac{\gamma}{\beta}\pi^m-\frac{a_{12}^{(0)}}{a_{13}^{(0)}}\pi^n$$

であることが従うので $x=\dfrac{\gamma}{\beta}\pi^m$ であると仮定してよい. 従って (2) から $a_{12}^{(0)}=0$. (6) と $x=\dfrac{\gamma}{\beta}\pi^m$ を用いて,

$$a_{22}^{(0)}\beta\pi^{-m}=-a_{13}^{(0)}(\gamma-\beta)x\pi^{-n}$$

がわかる. $a_{13}^{(0)}, a_{22}^{(0)} \in \mathbb{Z}_p^\times$ より $\mathrm{ord}_K(\beta) - m = \mathrm{ord}_K(\beta-\gamma) + \mathrm{ord}_K(x) - n$ であることもわかる. これにより $n = 2m$ である. $s(M)$ の定義より, $s(M) = m + n = 3m$ を得る. 従って $m = \frac{1}{3}s(M), n = \frac{2}{3}s(M)$ である. それゆえ

$$M \cong M\left(\frac{1}{3}s(M), \frac{2}{3}s(M), \frac{\gamma}{\beta}\pi^{\frac{1}{3}s(M)}\right).$$

次に $m = 0$ を仮定する. $m > 0$ と同様な議論より, (2), (3), (4), (5), (6), (7) が成り立つ. (4) より, $a_{33}^{(0)} = 0$ である. (5) と (7) を用いて, $a_{23}^{(0)} = -a_{13}^{(0)}$ と $a_{32}^{(0)} = \frac{\gamma}{\beta}a_{13}^{(0)}$ を得る. Y は可逆であるので, $\det(Y) \not\equiv 0 \bmod p$ である. $a_{13}^{(0)} \equiv 0 \bmod p$ を仮定すると, $\det(Y) \equiv 0 \bmod p$ となる. 従って $a_{13}^{(0)} \in \mathbb{Z}_p^\times$ である. これにより $a_{23}^{(0)}, a_{32}^{(0)} \in \mathbb{Z}_p^\times$ もわかる. (2) より

$$x = \frac{\gamma}{\beta} - \frac{a_{12}^{(0)}}{a_{13}^{(0)}}\pi^n$$

であることもわかる. それゆえ $x = \frac{\gamma}{\beta}$ であると仮定してよい. (2) より $a_{12}^{(0)} = 0$ である. (6) と $x = \frac{\gamma}{\beta}$ より,

$$a_{22}^{(0)}\beta = -a_{13}^{(0)}(\gamma - \beta)x\pi^{-n}$$

となる. $a_{13}^{(0)} \in \mathbb{Z}_p^\times$ より $\mathrm{ord}_K(a_{22}^{(0)}) + \mathrm{ord}_K(\beta) = \mathrm{ord}_K(\beta-\gamma) + \mathrm{ord}_K(x) - n$ である. $a_{22}^{(0)} \in \mathcal{O}_K$ から, $n = \mathrm{ord}_K(x) = 0$ を得る. それゆえ $s(M) = 0$ であるので

$$M \cong M(0,0,0).$$

□

M を Λ-加群とする. $\xi \in \Lambda$ に対して, 写像 $\Pi_\xi = \Pi_\xi^M : M \longrightarrow M$ を $\Pi_\xi(y) = \xi y$ によって定義する. 以下, 定理 1.2 の証明をする.

定理 1.2 の証明. 前半部分は定理 3.5 からわかる. それゆえ $X_p(E, \mathbb{Q}_\infty) \cong M\left(\frac{1}{3}s, \frac{2}{3}s, \frac{\gamma}{\beta}\pi^{\frac{1}{3}}\right)$. ここで $s = s(X_p(E, \mathbb{Q}_\infty))$ である. 後半部分を示す. 仮定より $X_p(E, \mathbb{Q}) \cong X_p(E, \mathbb{Q}_\infty) \otimes_\Lambda \Lambda/(T)$ であることを注意しておく. 写像 $\Pi_T^X : X \longrightarrow X$ について考える. 定理 3.5 の証明と同様に, X の行列表示から

$$A = \begin{pmatrix} 0 & 0 & 0 \\ \beta p^{-\frac{1}{3}s} & \beta & 0 \\ 0 & (\gamma-\beta)\frac{\gamma}{\beta}p^{-\frac{1}{3}s} & \gamma \end{pmatrix}$$

を得る. 行列の基本変形により, A は

$$\begin{pmatrix} 0 & 0 & 0 \\ p^{\mathrm{ord}_p(\beta)-\frac{1}{3}s} & 0 & 0 \\ 0 & p^{\mathrm{ord}_p(\beta)-\frac{1}{3}s} & 0 \end{pmatrix}$$

と同値である. これにより

$$X_p(E, \mathbb{Q}_\infty)/TX_p(E, \mathbb{Q}_\infty) \cong \mathbb{Z}_p/p^{\mathrm{ord}_p(\beta)-\frac{1}{3}s}\mathbb{Z}_p \oplus \mathbb{Z}_p/p^{\mathrm{ord}_p(\beta)-\frac{1}{3}s}\mathbb{Z}_p \oplus \mathbb{Z}_p$$

であることがわかる. $\mathrm{Tor}_{\mathbb{Z}_p}(\mathrm{Sel}_p(E/\mathbb{Q}))$ は $Ш(E,\mathbb{Q})$ の p 成分の位数と一致するので

$$2\left(\mathrm{ord}_p(\beta)-\frac{1}{3}s\right)=\mathrm{ord}_p(\#Ш(E,\mathbb{Q}))$$

であることもわかる. 従って,

$$s=3\left(\mathrm{ord}_p(\beta)-\frac{1}{2}\mathrm{ord}_p(\#Ш(E,\mathbb{Q}))\right).$$

□

4 数値例

この節の記号はこれまでと同じ意味で用いることにする. E は条件 (♮) を満たし, $(E,\mathbb{Q}_\infty/\mathbb{Q})$ の λ 不変量が 3 である場合において, SAGE を用いて $X_p(E,\mathbb{Q}_\infty)$ の同型類を決定する例を与える. まず次の二つの命題を紹介する.

命題 4.1 ([10], Proposition 5.1)**.** distinguished 多項式 $f(T)\in\mathbb{Z}_p[T]$ に対して, K を $f(T)$ の $\mathbb{Q}_p$ 上の最小分解体とする. このとき自然な写像

$$\Psi:\mathcal{M}_{f(T)}^{\mathbb{Q}_p}\longrightarrow\mathcal{M}_{f(T)}^{K}\qquad([M]\longmapsto[M\otimes_\Lambda\Lambda_K]_K)$$

は単射である.

命題 4.1 を用いて次の命題を示すことができる. 証明については ([12]) を参照せよ.

命題 4.2. $[X_p(E,\mathbb{Q}_\infty)]\in\mathcal{M}_{f(T)}$ と仮定する. $Ш(E/\mathbb{Q})$ の p 成分は有限で,

$$\mathrm{ord}_p\left(\left.\frac{L_p(E,T)}{T}\right|_{T=0}\right)=1$$

が成り立つとする. ここで $L_p(E,T)$ は E に付随する p 進 L 関数である. このとき,

$$X_p(E,\mathbb{Q}_\infty)\cong\Lambda/(L_p(E,T))$$

である.

例 1. E を Cremona の表 ([1]) にある楕円曲線 37A とする. 極小 Weierstrass model は $y^2+y=x^3-x$ である. $p=13$ とする. Pollack の表 ([14], tables of Iwasawa invariants) により, $(E,\mathbb{Q}_\infty/\mathbb{Q})$ の μ 不変量は 0 で, λ 不変量は 3 である. SAGE により, E は条件 (♮) を満たすことが確認できる. さらに, SAGE により

$$\begin{aligned}L_{13}(E,T)\equiv{}&(13+2\cdot13^2+4\cdot13^3)T+(5\cdot13+4\cdot13^2+4\cdot13^3)T^2\\&+(6+7\cdot13^2+13^3)T^3\bmod(13,T)^4\end{aligned}$$

と計算できる. 従って命題 4.2 より, $[X_p(E,\mathbb{Q}_\infty)]=[\Lambda/(T(g(T)))]$ がわかる.

例 2. E を Cremona の表にある楕円曲線 430C とする [1]. 極小 Weierstrass model は $y^2+xy=x^3+4x+16$ である. $p=13$ とする. SAGE により, E は条件 (♮) を満たすことが確認できる. さらに, SAGE により

$$L_{13}(E,T) \equiv (10\cdot 13^2+2\cdot 13^3)T+(12\cdot 13^2+5\cdot 13^3)T^2+(10+11\cdot 13^2)T^3 \bmod (5,T)^4$$

と計算できる. 補題 3.3 と p 進 Weierstrass の準備定理 ([17], Theorem 7.3) により, $g(T)\in\mathbb{Z}_{13}[[T]]$ と $g(T)\in\mathbb{Z}_{13}[[T]]^\times$ が存在して

$$L_{13}(E,T)=Tg(T)U(T)$$

となる. ここで $g(T)\equiv T^2+1521T+169 \mod (13,T)^3$ である. 従って $g(T)$ は可約多項式である. $g(T)=(T-\beta)(T-\gamma)$ とく. $\beta,\gamma\in p\mathbb{Z}_p$ であることに注意する. このとき, $\mathrm{ord}_K(\beta)=\mathrm{ord}_K(\gamma)=1$ である. 補題 3.3 から, $\mathrm{ord}_K(\beta-\gamma)=1$ である. 定理 1.2 より,

$$\begin{aligned} X_p(E,\mathbb{Q}_\infty) &\cong M\left(\frac{1}{3}s,\frac{2}{3}s,\frac{\gamma}{\beta}p^{\frac{1}{3}s}\right) \\ &= \left\langle (1,1,1),(0,p^{\frac{1}{3}s},\frac{\gamma}{\beta}p^{\frac{1}{3}s}),(0,0,p^{\frac{2}{3}s})\right\rangle_{\mathbb{Z}_p} \\ &\subset \Lambda/(T)\oplus\Lambda/(T-\beta)\oplus\Lambda/(T-\gamma) \end{aligned}$$

を得る. ここで $s=s(X_p(E,\mathbb{Q}_\infty))=3(\mathrm{ord}_p(\beta)-\mathrm{ord}_p(\#Ш(E/\mathbb{Q})))$. 再び SAGE を用いて, $Ш(E/\mathbb{Q})=1$ であることがわかる. それゆえ $s=3$ である. 従って $[X_p(E,\mathbb{Q}_\infty)]=[\Lambda/(L_p(E,T))]$.

参考文献

[1] J. E. Cremona, Algorithms for modular elliptic curves, Cambridge University Press, Cambridge, 1992.

[2] R. Greenberg, Iwasawa theory for elliptic curves, In: Arithmetic theory of elliptic curves (Cetraro, 1997), 51–144, Lecture Notes in Math., 1716, Springer, Berlin, 1999.

[3] K. Iwasawa, On Γ-extensions of algebraic number fields, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[4] M. Koike, On the isomorphism classes of Iwasawa modules associated to imaginary quadratic fields with $\lambda=2$, J. Math. Sci. Univ. Tokyo **6** (1999), 371–396.

[5] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Cohomologies p-adiques et applications arithmetiques, III, Asterisque **295** (2004), 117–290.

[6] M. Kurihara, Iwasawa theory and Fitting ideals, J. Reine Angew. Math. **561** (2003), 39–86.

[7] M. Kurihara, Refined Iwasawa theory and Kolyvagin systems of Gauss sum type, Proc. Lond. Math. Soc. **104** (2012), 728–769.

[8] M. Kurihara, Refined Iwasawa theory for p-adic representations and the structure of Selmer groups, Munster J. Math. **7** (2014), 149–223.

[9] B. Mazur and K. Rubin, Organizing the arithmetic of elliptic curves, Adv. Math. **198** (2005), 504–546.

[10] K. Murakami, On the isomorphism classes of Iwasawa modules with $\lambda = 3$ and $\mu = 0$, Osaka J. Math. **51** (2014), 829–865.

[11] K. Murakami, Isomorphism classes of modules over Iwasawa algebra with $\lambda = 4$, Tokyo J. Math. **37** (2016), 101–132.

[12] K. Murakami, On a new invariant determining the isomorphism classes of Λ-modules, preprint.

[13] D. G. Northcott, Finite free resolutions, Cambridge University Press, Cambridge-New York, 1976.

[14] R. Pollack, `http://math.bu.edu/people/rpollack/`.

[15] H. Sumida, Greenberg's conjecture and the Iwasawa polynomial, J. Math. Soc. Japan **49** (1997), 689–711.

[16] H. Sumida, Isomorphism classes and adjoints of certain Iwasawa modules, Abh. Math. Sem. Univ. Hamburg **70** (2000), 113–117.

[17] L. C. Washington, Introduction to cyclotomic fields. Second edition, Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.