

本田・テイト理論と モジュラー曲線のレフシェッツ数

津嶋 貴弘 *

1 概要

本稿では最初に一般の形で本田・テイト理論の主定理を述べ、それを楕円曲線の場合に特化してより詳しく述べる。楕円曲線に対する本田・テイト理論に基づき、モジュラー曲線のレフシェッツ数を軌道積分を用いて表示する公式を紹介する。

2 本田・テイト理論について ([Ho], [Ta1], [Ta2])

2.1 主定理

任意の体 k 上のアーベル多様体の圏は、任意の k 上のアーベル多様体 A, B に対して $\mathrm{Hom}_k(A, B)$ が \mathbb{Z} 上有限生成自由加群となる加法圏である。この圏を少し修正した圏 $M(k)$ を定義する。対象を k 上のアーベル多様体とし、射を

$$\mathrm{Hom}_{M(k)}(A, B) = \mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$$

とおく。 $M(k)$ における同型射 $f: A \rightarrow B$ を k 上の同種 (isogeny) と呼ぶ。すると $M(k)$ の同型類を理解することは、アーベル多様体を k 上同種を除いて理解することになる。 $M(k)$ は半単純である。即ち、この圏の対象は単純な対象の有限個の積に $M(k)$ において同型である。アーベル多様体が単純であるとは、自明なもの以外の部分アーベル多様体を持たないことである。アーベル多様体の同種類を理解するためには以下の二つのことを理解すればよい。

* 千葉大学理学部 数学・情報数理学科 e-mail: tsushima@math.s.chiba-u.ac.jp

- 単純アーベル多様体の k 上同種類の集合。
- 各単純アーベル多様体 A の自己準同型環 $\text{End}_{M(k)}(A)$.

一般にアーベル多様体 A の自己準同型環 $\text{End}_{M(k)}(A)$ は \mathbb{Q} 上の半単純環になることが知られている。 $M(k)$ が半単純であることから、単純アーベル多様体 A の自己準同型環は斜体である。アーベル多様体 A が、互いに同種でない単純アーベル多様体 B_1, \dots, B_n の直積 $\prod_{i=1}^n B_i^{n_i}$ と同種とする。単純アーベル多様体 B_i を A の単純成分と呼ぶ。このとき、 $D_i = \text{End}_{M(k)}(B_i)$ とおけば次が成り立つ。

$$\text{End}_{M(k)}(A) \simeq \prod_{i=1}^n M_{n_i}(D_i). \quad (2.1)$$

これより、単純アーベル多様体 A の自己準同型環を理解すればよい。以下では、上述の二つの事柄を k が有限体の場合に理解する。これが本田・テイト理論の内容である。アーベル多様体の一般論については石塚氏の記事を見られたい。

k を標数 p , 位数 q の有限体とする。 k 上定義されたアーベル多様体 A を考えて、 $\pi_A \in \text{End}_k(A)$ を A の k 上フロベニウス自己準同型写像 (関数環の方で q 乗する写像) とする。 A を単純と仮定する。アーベル多様体の場合のヴェイユ予想により、 π_A は代数的整数であって全ての埋め込み $\iota: \mathbb{Q}(\pi_A) \hookrightarrow \mathbb{C}$ に対して、 $|\iota(\pi_A)| = q^{1/2}$ が成立する。このような性質を持つ代数的数を ヴェイユ q 数 (Weil q -number) と呼ぶ。二つのヴェイユ q 数 π_1, π_2 が \mathbb{Q} 上共役である とは、体の同型 $\iota: \mathbb{Q}(\pi_1) \simeq \mathbb{Q}(\pi_2)$ が存在して $\iota(\pi_1) = \pi_2$ となることである。

定理 2.1 (i) 対応 $A \mapsto \pi_A$ は k 上の単純アーベル多様体の k 上同種類の集合とヴェイユ q 数の \mathbb{Q} 上共役類の集合の間の一対一対応を誘導する。

(ii) A を k 上単純アーベル多様体とする。このとき、 \mathbb{Q} 代数

$$F = \mathbb{Q}(\pi_A) \subset D = \text{End}_{M(k)}(A)$$

を考える。

- D は F 上の中心斜体である。
- F の各実素点で D は分裂しない。
- F の p を割らない任意の有限素点で D は分裂する。
- v を p の上にある F の有限素点とすると、 D の v でのハッセ不変量が

次の公式で与えられる。

$$\text{inv}_v(D) \equiv \frac{v(\pi_A)}{v(q)} [F_v : \mathbb{Q}_p] \pmod{1}. \tag{2.2}$$

但し $v(\cdot)$ は、 F_v の素元で 1 となる正規化された離散付値とし、この等式は \mathbb{Q}/\mathbb{Z} での等式とする。

(e) 等式

$$2 \dim A = [D : F]^{1/2} [F : \mathbb{Q}] \tag{2.3}$$

が成り立つ。

注意 2.2 v を F の素点とする。 $|\cdot|_v$ を F_v 上の正規化ノルムとする。即ち、以下のように定義する。 F の有限素点 v に対して、 F_v の剰余体の位数を q_v と書く。 v が有限素点ならば $|x|_v = q_v^{-v(x)}$ ($x \in F_v$) とおく。 v が実素点ならば普通の絶対値とし、 v が複素素点ならば $|x|_v = |v(x)|^2$ とおく。定理 2.1(ii) より、全ての素点 v に対して

$$|\pi_A|_v = q^{-\text{inv}_v(D)}$$

が成立する。すると、積公式 $\prod_v |\pi_A|_v = 1$ は $\sum_v \text{inv}_v(D) \equiv 0 \pmod{1}$ を導く。[Ta1, (6), (7)] を参照。

定理 2.1(ii)(a) は系 2.4(1) で解説される。(b) は後述の系 2.7 から従う。定理 2.1(ii)(c) は後述の定理 2.3 から従う。(e) は系 2.4 で示される。(d) の公式 (2.2) の証明は、[MW, Theorem 2 in II] にある。本稿ではこれの証明は解説されない。[MW] は、本田・テイト理論のサーヴェイになっているので参照されたい。

2.2 A の唯一性と $\text{End}_{M(k)}(A)$ の構造

以下では定理 2.1(i) の単射性と定理 2.1(ii) を (d) を除いて解説する。

以下、 k は常に有限体と仮定しよう。 A を k 上のアーベル多様体とする。素数 $\ell \neq p$ を取る。 \mathbb{F} を k の代数閉包とする。 A の ℓ 進テイト加群を $T_\ell A$ と書く。 $V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ とおく。 $V_\ell A$ に $G = \text{Gal}(\mathbb{F}/k)$ が作用する。 $2 \dim A$ 次数の \mathbb{Z} 係数のモニック多項式 f_A で、全ての n について $|f_A(n)| = \deg(\pi_A - n)$ をみたすものが唯一つ存在する (cf. [Mi, Theorem 10.9])。 f_A を π_A の特性多項式という。 π_A の $V_\ell A$ 上の特性多項式は f_A と一致することが知られている (cf. [Mi, Proposition 10.20])。更に π_A の $V_\ell A$ への作用は半単純である。

A を単純と仮定する。 f_A は \mathbb{Q} 上既約モニック多項式 m_A の冪乗の形をしている。そこで $f_A = m_A^e$ とおく。 m_A は π_A の \mathbb{Q} 上最小多項式に他ならない。即ち $\deg \pi_A = [F : \mathbb{Q}]$ である。以上より、

$$2 \dim A = e[F : \mathbb{Q}] \quad (2.4)$$

という公式を得る。 π_A は \mathbb{Z} 係数のモニックな特性多項式の根であるから、 π_A は代数体 $F = \mathbb{Q}(\pi_A)$ の整数環 \mathcal{O}_F に含まれることが分かる。テイトは次を示した。この定理から派生したテイト予想については松本氏の記事を見られたい。

定理 2.3 このとき、任意の k 上のアーベル多様体 A, B に対して以下の自然な写像は同型を誘導する。

$$\mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_G(T_\ell A, T_\ell B).$$

この定理の証明の概略を見ておこう。その証明は、アーベル多様体 A についての次の自然な射

$$\alpha_\ell : \mathrm{End}_{M(k)}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \rightarrow \mathrm{End}_G(V_\ell A) \quad (2.5)$$

の全単射性に帰着される。単射性は k が有限であることに依拠しない一般の体上のアーベル多様体に対して成立する事実である ([Mi, Lemma 10.6] を参照)。全射性は以下の三ステップを経て示される。

- (1) 任意の正の整数 d と素数 ℓ に対して、 ℓ 冪同種 $B \rightarrow A$ が存在し、次数 d^2 の偏極を有するアーベル多様体 B の同型類の個数が有限個であることを示す。
- (2) ℓ が $F = \mathbb{Q}(\pi_A)$ で完全分解するならば、(2.5) が同型であることを示す ([Ta1, Proposition 2 in §2])。
- (3) (2.5) が単射であることと、ステップ (2) で少なくとも一つの素数 ℓ について同型 (2.5) が分かっていることから

$$\dim_{\mathbb{Q}_\ell} \mathrm{End}_G(V_\ell A)$$

が ℓ に依らないことが分かれば良い。

一つ目のステップで k が有限であることを使う。最後の主張における

「 $\dim_{\mathbb{Q}_\ell} \mathrm{End}_G(V_\ell A)$ が ℓ に依らないこと」

は次のようにして分かる。任意の \mathbb{Q} の拡大体 K に対して K 上多項式としての相異なる既約多項式への分解

$$f_A = \prod_P P^{a(P)}$$

を考えて、

$$r(f_A) = \sum_P a(P)^2 \deg P \tag{2.6}$$

とおく。これは拡大体 K の取り方によらないことが分かる。 π_A が $V_\ell A$ に半単純に作用し、 $\text{End}_G(V_\ell A)$ は $\text{End}_{\mathbb{Q}_\ell}(V_\ell A)$ における π_A の交換子であることから任意の素数 l について次が分かる。

$$\dim_{\mathbb{Q}_\ell} \text{End}_G(V_\ell A) = r(f_A). \tag{2.7}$$

以上全射性について述べたことの詳細は [Ta1, §2. The Proof] を参照。よって全ての素数 $l \neq p$ に対して、 α_ℓ は全単射であることが分かった。この定理 2.3 はアーベル多様体の場合のテイト予想と同値であることを注意しておく。

- 系 2.4** (1) 定理 2.1(ii) の記号の下で、 F は D の中心である。
 (2) 定理 2.1(ii)(c) が成り立つ。
 (3) 公式 (2.3) が成り立つ。

証明 (1) を示す。同型 (2.5) と [Ta1, Lemma 4] より、 $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ は $D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ の中心である。故に F は D の中心である。

(2) を示す。 l を p と異なる素数とする。

$$F_\ell := F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \prod_{v|\ell} F_v$$

となる。(2.5) より、 $F_\ell \otimes_F D \simeq \mathbb{Q}_\ell \otimes_{\mathbb{Q}} D$ は $\text{End}_{F_\ell}(V_\ell A)$ と同型である。後者は F_ℓ 上の行列環に他ならないから、題意が従う。

(3) を示す。 $f_A = m_A^e$ と書けることがわかっている。これと (2.6) より、

$$r(f_A) = e^2 \deg m_A = e^2 [F : \mathbb{Q}]$$

を得る。これと (2.5) の α_ℓ の全単射性と (2.7) により、

$$[D : \mathbb{Q}] = \dim_{\mathbb{Q}_\ell} \text{End}_G(V_\ell A) = r(f_A) = e^2 [F : \mathbb{Q}]$$

を得る。よって、 $e = [D : F]^{1/2}$ が分かる。これと (2.4) を合わせると題意を得る。□

定理 2.3 の帰結として以下が成立する。

定理 2.5 A, B を k 上のアーベル多様体とする。 f_A, f_B をそれぞれ A, B の k 上フロベニウス自己準同型の特性多項式とする。

(a) 以下は同値である。

- B は A の k 上定義された部分アーベル多様体に k 上同種である。
- ある ℓ について $V_\ell B$ から $V_\ell A$ への G 同変な単射がある。
- f_B は f_A を割り切る。

(b) 以下は同値である。

- A と B は k 上同種である。
- $f_A = f_B$.

証明 f_A, f_B はモニックだったから (a) から (b) が従う。(a) を示す。一般に k 上のアーベル多様体の射 $\varphi: B \rightarrow A$ に対して、 $\varphi_\ell: V_\ell B \rightarrow V_\ell A$ の核の \mathbb{Q}_ℓ 上線型空間としての次元は $\ker \varphi$ のスキームとしての次元の二倍に等しい。よって、 φ が有限になることと φ_ℓ が単射であることは同値になる。これより、一つ目から二つ目が分かる。逆を示す。 G 同変な単射 $u: V_\ell B \rightarrow V_\ell A$ が与えられているとする。すると、定理 2.3 によって、ある $\varphi \in \text{Hom}_{M(k)}(B, A)$ であって、 φ_ℓ は $\text{Hom}_G(V_\ell B, V_\ell A)$ において u に ℓ 進的にいくらでも近いものが取れる。 u に十分近く取っておけば、 φ は単射でかつ φ の適当な倍数は $\text{Hom}_k(B, A)$ に入るように取れる。先ほど述べたことと合わせると二つ目から一つ目がわかった。二つ目から三つ目は自明である。逆はフロベニウス自己準同型 π_A は $V_\ell A$ に半単純に作用することから従う。□

A を k 上の単純アーベル多様体とする。 $F = \mathbb{Q}(\pi_A)$ が実素点を持つと仮定する。このとき、 $\pi_A^2 = q$ だから $F = \mathbb{Q}$ であるか $F = \mathbb{Q}(\sqrt{q}) \neq \mathbb{Q}$ のいずれかが成立する。このとき、 A がどのようなようになるか以下の命題で分かる。これによれば、 F が実素点を持つことは滅多にないことが分かる。以下の主張に現れる超楕円曲線に関しては定義 2.16 において定義される。

命題 2.6 (1) A を単純とは限らない k 上のアーベル多様体とする。 $F = \mathbb{Q}(\pi_A) = \mathbb{Q}$ と仮定する。 D_p を p と ∞ のみで分岐する \mathbb{Q} 上の quaternion

algebra とする。このとき、同型 $D = \text{End}_{M(k)}(A) \simeq M_{\dim A}(D_p)$ が成り立つ。よって A は $\text{End}_{M(k)}(E) = D_p$ となるような超特異楕円曲線 E の $\dim A$ 個の直積と k 上同種である。特に A が単純ならば、そのような E と k 上同種である。

- (2) A を k 上の単純アーベル多様体とする。 $F = \mathbb{Q}(\sqrt{q}) \neq \mathbb{Q}$ と仮定する。このとき、 D は二つの実素点で分裂せず、 p で分裂する。また、 $\dim A = 2$ である。 k_2 を k の二次拡大体とすると、底変換 A_{k_2} は、 $\text{End}_{M(k_2)}(E) = D_p$ となるような超楕円曲線 E の二個の直積に同種となる。

証明 一つ目の主張を示す。 D が p の外で分裂することは定理 2.3 で分かる。唯一つの実素点で分裂すると仮定すると、ハッセ不変量の性質から p でも分裂してはならず $D \simeq M_{2 \dim A}(\mathbb{Q})$ となる。(2.1) より A はあるアーベル多様体の $2 \dim A$ 個の直積と同種でなければならない。次元を考えると、これは矛盾である。故に D は実素点で分岐し、ここでのハッセ不変量は $1/2$ である。よって D は p でも分岐してはならず、 p でのハッセ不変量は $1/2$ になる。故に $D \simeq M_{\dim A}(D_p)$ が分かる。よって (2.1) より題意を得る。

二つ目の主張を示す。 $F' = \mathbb{Q}(\pi_{A_{k_2}})$, $D' = \text{End}_{M(k_2)}(A)$ とおく。 $\pi_{A_{k_2}} = \pi_A^2 = q$ であるから $F' = \mathbb{Q}$ となる。

$$F' = \mathbb{Q} \subset F \subset D \subset D'.$$

D は D' における F の交換子であることからブラウアー群 $\text{Br}(F)$ において $D \sim D' \otimes_{F'} F$ が成立する。一つ目の主張を A_{k_2} に適用すれば D' は無限素点で分裂しないことが分かるので D もそうなることが分かる。ハッセ不変量を考えると D は p で分裂することが分かる。これより、 D は二つの実素点でのみ分岐する F 上の quaternion algebra である。よって、(2.3) より $\dim A = 2$ が分かる。更に A_{k_2} は、 $\text{End}_{M(k_2)}(E) = D_p$ となるような超楕円曲線 E の二個の直積に同種となることが一つ目の主張の証明の議論から分かる。以上述べたことについては [Ta1, Examples in p.97] と [Ta2, p.141] を参照。 \square

系 2.7 A を k 上の単純アーベル多様体とする。このとき、 $D = \text{End}_{M(k)}(A)$ は実素点で分岐する。

証明 上の命題 2.6 から直ちに従う。 \square

2.3 与えられたヴェイユ数からアーベル多様体を構成する

以下では、本田・テイト理論の定理 2.1(i) の全射性を示す。これは、[Ho] において示された。以下では、[Ta2] の議論に従う。 q を p の冪とする。本節の目標は、与えられたヴェイユ q 数 π に対して、そのフロベニウス自己準同型が π と \mathbb{Q} 上共役になるような k 上のアーベル多様体を構成することである。アーベル多様体は楕円曲線のように一つの定義方程式で定義されるわけではないので、具体的に定義方程式を構成してアーベル多様体を作ることは一般には不可能であろう。そのように考えてみると、この問題は非常に難しいと想像できる。虚数乗法論を使って数体上のアーベル多様体を構成し、その還元として欲しいアーベル多様体を作るというのがおおまかなアイデアである。欲しいアーベル多様体を作るために、志村・谷山公式を使う。虚数乗法論、志村・谷山公式については越川氏の記事を参照されたい。

以下、 π をヴェイユ q 数とする。 π が効果的であるとは、 \mathbb{F}_q 上の単純アーベル多様体 A が存在してそのフロベニウス自己準同型写像 π_A と π が \mathbb{Q} 上共役であることとする。

補題 2.8 N を 1 以上の整数とする。このとき、 π^N が効果的ならば π も効果的である。

証明 ヴェイユ q^N 数 π^N に対応する \mathbb{F}_{q^N} 上の単純アーベル多様体を A' と書く。ヴェイユ制限 $A = \text{Res}_{\mathbb{F}_{q^N}/\mathbb{F}_q}(A')$ を考えると、次が成立する。

$$f_A(T) = f_{A'}(T^N).$$

よって、 π は $f_A(T)$ の根である。 $M(\mathbb{F}_q)$ における単純アーベル多様体への分解

$$A \simeq \prod_{i=1}^n B_i^{n_i}$$

が成り立つとき、

$$f_A = \prod_{i=1}^n f_{B_i}^{n_i}$$

が成立することに注意する。 A の単純成分 B で f_B が π を根として持つものを考えれば、 π が効果的であることが分かる。□

$F = \mathbb{Q}(\pi)$ とおく。定理 2.1(ii) において、 π_A を π と取り替えて唯一つに定まる F 上の中心斜体を D と書く。総実体上の総虚二次拡大体を CM 体と呼ぶ。

補題 2.9 F を含む CM 体 L で次をみたすものが存在する。

- $[L : F] = [D : F]^{1/2}$
- D は L 上分裂する。

証明 まず、 F が総実のときを考える。 $L = F((-p)^{1/2})$ が題意を満たすことを確認する。仮定より $\pi^2 = q = p^r$ が成立する。 r が偶数ならば $F = \mathbb{Q}$ である。(2.2) より、 D は \mathbb{Q} 上の quaternion algebra である。これより題意の一つ目が分かる。 $D \otimes_F L$ が分裂することを確かめよう。 p の上にある L の素点は唯一つであり、無限素点と p の外の有限素点で D が分裂していることから直ちに従う。次に、 r が奇数であると仮定する。このとき、 $F = \mathbb{Q}(p^{1/2})$ である。 F の素イデアル $\mathfrak{p} = (p^{1/2})$ を考えると $(p) = \mathfrak{p}^2$ は F で分岐しており、(2.2) により $\text{inv}_{\mathfrak{p}}(D) \equiv 1 \equiv 0 \pmod{1}$ なので D は二つの実素点でのみ分岐する F 上の quaternion algebra である。このことから題意は直ちに従う。

F が総実でないときと仮定する。部分体 $F_0 = \mathbb{Q}(\pi + q\pi^{-1})$ は F の最大総実部分体である。更に F/F_0 は総虚二次拡大なので F は CM 体である。 $m = [D : F]^{1/2}$ とおく。 L_0 を F_0 の m 次の総実拡大体で、 p の上にある F_0 の任意の素点 v_0 における剰余次数が m になるものとする。即ち、 v'_0 を v_0 の上にある L_0 の任意の素点とすると、 $(L_0)_{v'_0}$ は $(F_0)_{v_0}$ 上の不分岐 m 次拡大になっている。 $L = L_0F$ とおくと L は CM 体であることが分かる。 $[L : F] = m$ は自明であろう。 $[D : F]^{1/2} = m$ であり、 p の上にある F の任意の素点 v とその上の L の素点 v' に対して $L_{v'}$ が F_v 上不分岐 m 次拡大体なので、 $D \otimes_{F_v} L_{v'}$ が分裂する。故に題意を得る。□

2.3.1 虚数乗法論

L を CM 体とする。 ρ を L の位数 2 の自己同型写像で、任意の埋め込み $L \hookrightarrow \mathbb{C}$ に対して複素共役と両立するものとする。 C を標数零の代数閉体とする。 Φ を $\text{Hom}(L, C)$ の部分集合で次をみたすものとする。

$$\Phi \sqcup \Phi\rho = \text{Hom}(L, C).$$

組 (L, Φ) を CM 型と呼ぶ。 C を C の部分環とする。 C 上のアーベルスキーム A が (L, Φ) 型であるとは、アーベル多様体 $A = \mathcal{A} \times_C C$ に対して埋め込み $L \hookrightarrow \text{End}_{M(C)}(A)$ が存在して、 A の接空間 t_A が L の表現として $\bigoplus_{\varphi \in \Phi} \varphi$ と同型であることとする。このようなアーベルスキーム \mathcal{A} を (L, Φ) 型のアーベルスキームと呼ぶ。

補題 2.10 C に含まれるある数体の整数環上定義された (L, Φ) 型のアーベルスキーム A が存在する。

証明のアイデア これは志村・谷山の虚数乗法論 ([ST]) の帰結である。簡単に証明の概略を解説する。複素トーラス $\mathbb{C}^\Phi / \Phi(\mathcal{O}_L)$ を考える。これに L を $\Phi(a)$ ($a \in L$) 倍で作用させる。 $L \otimes_{\mathbb{Q}} \mathbb{R}$ には非退化なリーマン形式 ($\alpha^\rho = -\alpha$ かつ $\text{Im } \alpha^\rho > 0$ なる $\alpha \in \mathcal{O}_L$ を取り $(a, b) \mapsto \text{Tr}_{L/\mathbb{Q}}(\alpha ab^\rho)$ ($(a, b) \in L$) と定める) が定義されるので、上の複素トーラスは代数的となりアーベル多様体とみなせる (リーマンの定理)。更にこれは数体上定義されることが示せる。更に Neron–Ogg–Shafarevich の判定法 (アーベル多様体が良い還元を持つこととテイト加群への作用が不分岐であることは同値) を用いると CM 乗法を持つ様なアーベル多様体は潜在的に良い還元を持つことが示せる (セール・テイトの定理)。このことから題意を得る。[Mi2, Proposition 10.5] も参照。□

以下では、 C を \mathbb{Q}_p の代数閉包とする。 w を p の上にある L の素点とする。 $\text{Hom}_{\mathbb{Q}_p}(L_w, C)$ を $\text{Hom}(L, C)$ の部分集合とみなし、 H_w と書く。 (L, Φ) を CM 型とする。更に $\Phi_w = \Phi \cap H_w$ とおく。このとき、次の分解が成り立つ。

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{w|p} L_w.$$

更に次が成立する。

$$\text{Hom}(L, C) = \bigcup_{w|p} H_w, \quad \Phi = \bigcup_{w|p} \Phi_w.$$

補題 2.11 志村・谷山公式 A を p 進体の整数環 \mathcal{O} 上定義された (L, Φ) 型のアーベルスキームとする。 k_0 を \mathcal{O} の剰余体とし、位数を q_0 と書く。 A_0 を \mathcal{A} の還元とする。このとき、 L のある元 π_0 が存在して、埋め込み $L \hookrightarrow \text{End}_{M(k_0)}(A_0)$ によるその

像が π_{A_0} と一致し、更に次が成り立つ。 p の上にある L の各素点 w に対して

$$\frac{w(\pi_0)}{w(q_0)} = \frac{|\Phi_w|}{|H_w|}. \tag{2.8}$$

2.3.2 全射性の証明

元の設定に戻り π, q, D, F は全て前節の通りとする。 L は補題 2.9 の条件をみたす CM 体とする。

主張 2.12 以下の等式が成り立つ様な Φ が取れる。 p の上にある L の各素点 w に対して

$$\frac{w(\pi)}{w(q)} = \frac{|\Phi_w|}{|H_w|}. \tag{2.9}$$

主張の証明 w を p の上にある L の素点とし、その下にある F の素点を v と書く。 $n_w = \frac{w(\pi)}{w(q)}|H_w|$ とおく。すると

$$n_w = \frac{w(\pi)}{w(q)}[L_w : \mathbb{Q}_p] = \frac{v(\pi)}{v(q)}[L_w : F_v][F_v : \mathbb{Q}_p] \equiv [L_w : F_v] \text{inv}_v(D) \pmod{1} \tag{2.10}$$

が成り立つ。一般に局所体の拡大 K'/K について $\text{Res}_{K'/K} : \text{Br}(K) \rightarrow \text{Br}(K')$ を $\otimes_K K'$ が引き起こす準同型とする。すると、次の図式は可換であることを思い出す。

$$\begin{array}{ccc} \text{Br}(K) & \xrightarrow{\text{Res}_{K'/K}} & \text{Br}(K') \\ \downarrow \text{inv}_K & & \downarrow \text{inv}_{K'} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[K':K]\times} & \mathbb{Q}/\mathbb{Z}. \end{array} \tag{2.11}$$

(2.10) と (2.11) と「 L で D が分裂すること」を思い出せば

$$n_w = \text{inv}_{L_w}(D \otimes_{F_v} L_w) \equiv 0 \pmod{1}$$

を得るので、 n_w は非負整数であることが分かる。 $\pi\pi^\rho = q$ であることから

$$n_w + n_{\rho w} = |H_w|$$

が分かる。自己同型写像 ρ は $\bigcup_w H_w$ において固定点を持たないことに注意すると、このような整数の組から位数が n_w である部分集合 $\Phi_w \subset H_w$ で $\Phi_w \sqcup \Phi_{\rho w} = H_w$ を満たすものが取れることは容易にチェックできる。故に合併 $\Phi = \bigcup_w \Phi_w$ は $\Phi \sqcup \Phi_\rho = H$ をみたす。□

主張 2.12 の Φ を考える。補題 2.10 により、 (L, Φ) 型のアーベルスキーム \mathcal{A} を取る。補題 2.11 のような $\pi_0 \in L$ を取る。すると (2.8) と主張 2.12 より、 p の上にある全ての L の素点 w に対して

$$\frac{w(\pi)}{w(q)} = \frac{w(\pi_0)}{w(q_0)}$$

が成り立つ。

命題 2.13 ある整数 N, N_0 が存在して $\pi^N = \pi_0^{N_0}$ が成り立つ。更に π は効果的である。

証明 π と π_0 を冪で取り替えることにより、 $q = q_0$ であると仮定してよい。よって p の上にある全ての L の素点 w に対して

$$w(\pi) = w(\pi_0)$$

が成り立つとしてよい。 π も π_0 も絶対値が p 冪であるから p の外の素点では π も π_0 も単元である。更にすべての無限素点で絶対値が等しいから、結局 π/π_0 は L の全ての素点で絶対値が 1 である。故に π/π_0 は 1 の冪根であることが分かる。よって必要ならば更に冪をとり、最初の主張を得る。 π_0 が効果的だから $\pi_0^{N_0}$ も効果的であり、 π^N が効果的と分かる。補題 2.8 より π が効果的であることがわかり二つ目の主張が従う。□

これより、全射性がわかった。

2.4 楕円曲線に対する本田・テイト理論

後で楕円曲線の場合が必要なのでこの場合に特化して定理 2.1 を述べる。その後で楕円曲線の超特異性・通常性の概念を思い出し、以下の定理との関係を述べる。本節の基本文献は [Si] や [W, Chapter 4] である。また本節執筆の上で [P] が非常に参考になった。

定理 2.14 k は前定理の通りとする。 E を k 上の楕円曲線とする。 π_E を E の k 上フロベニウス自己準同型とする。 f_E をその特性多項式とする。

(a) $D = \text{End}_{M(k)}(E)$ は $F = \mathbb{Q}(\pi_E)$ 上の中心斜体である。更に次が成立する。

$$[D : \mathbb{Q}] = 2 \text{ または } 4.$$

(b) 以下の条件は同値である。

- $[D : \mathbb{Q}] = 2$.
- f_E が重根を持たない。
- $D = F$.
- D は可換である。

(c) 以下の条件は同値である。

- $[D : \mathbb{Q}] = 4$.
- f_E が一次式の二乗になる。
- $F = \mathbb{Q}$.
- D は p と ∞ でのみ分岐する \mathbb{Q} 上の quaternion algebra に同型である。

証明 主張は定理 2.1 から従う。 □

補題 2.15 E を有限体 $k = \mathbb{F}_q$ 上の楕円曲線とする。

(1) 次が成り立つ。

$$f_E = f_E(X) = X^2 - a_q(E)X + q, \quad a_q(E) = q + 1 - |E(\mathbb{F}_q)|. \quad (2.12)$$

また、 $|a_q(E)| \leq 2\sqrt{q}$ が成立する。

(2) $F = \mathbb{Q}(\pi_E) \neq \mathbb{Q}$ ならば F は \mathbb{Q} 上の総虚二次拡大体である。

証明 1. これは楕円曲線の場合のヴェイユ予想の帰結である。証明については、例えば [Si, Theorem 2.3.1] を参照。

2. これは定理 2.14 と主張 1 の $|a_q(E)| \leq 2\sqrt{q}$ から従う。 □

定義 2.16 k の代数閉包を \mathbb{F} と書く。

(1) k 上の楕円曲線 E が通常であるとは、 $\text{End}_{M(\mathbb{F})}(E)$ が可換であることとする。

(2) k 上の楕円曲線 E が超特異であるとは、 E が通常でないこととする。

注意 2.17 (1) この定義は [W, Definition in §4.1] によった。この定義の同値な言い換えについては [Si, Theorem 3.1 in V.3] を参照。[Cl, p.127] の定義は間違えているので注意。

(2) k 上の楕円曲線 E に対して自然な単射がある。

$$\text{End}_{M(k)}(E) \hookrightarrow \text{End}_{M(\mathbb{F})}(E).$$

よって k 上の通常楕円曲線 E に対して $\text{End}_{M(k)}(E)$ は可換である。逆は必ずしも成り立たない。下記の例 2.21 に反例を挙げた。

次の同値性はよく知られている。

補題 2.18 E を k 上の楕円曲線とする。以下は同値である。

- E は超特異である。
- $a_q(E) \equiv 0 \pmod{p}$.

証明 例えば、[Si, p.150] の議論から従う。 □

楕円曲線 E が通常ならば定理 2.14 において (b) の場合になる。但し、(b) だからといって E が通常であるとは限らない。一方で、(c) の条件をみたすならば、楕円曲線 E は超特異になる。

補題 2.19 E を k 上の楕円曲線とする。

- (1) 以下の条件は同値である。
 - E は超特異である。
 - ある自然数 n が存在して $\pi_E^n \in \mathbb{Q}$ である。
- (2) 以下の条件は同値である。
 - E は通常である。
 - $D = F$ かつ F において p は分裂する。

この同値条件を満たすとき、 $(p) = \mathfrak{p}\mathfrak{p}'$ ($\mathfrak{p} \neq \mathfrak{p}'$) とおくと、 $v_{\mathfrak{p}}(\pi_E), v_{\mathfrak{p}'}(\pi_E)$ の内のいずれかは零になる。

証明 (1) を示す。一つ目から二つ目を示す。 E を超特異と仮定する。 k の有限次拡大 k_1 に対して、 E_{k_1} を E の k_1 への底変換とする。 $\overline{D} = \text{End}_{M(\mathbb{F})}(E)$ とおく。 k' を k の有限次拡大で、 $\text{End}_{M(k')}(E_{k'}) = \overline{D}$ をみたすものをとる。すると、 $r' = [k' : k]$ とおくと、 $\pi_{E_{k'}} = \pi_E^{r'}$ は \overline{D} の中心に入る。ところで [Si, Theorem 3.1 in V.3] より \overline{D} は \mathbb{Q} 上の quaternion algebra だから、 $\pi_E^{r'} \in \mathbb{Q}$ となる。二つ目から一つ目を示す。ある自然数 n が存在して $\pi_E^n \in \mathbb{Q}$ と仮定する。 k_n を k の n 次拡大体とする。すると、 $\mathbb{Q}(\pi_{E_{k_n}}) = \mathbb{Q}(\pi_E^n) = \mathbb{Q}$ だから $\text{End}_{M(k_n)}(E_{k_n})$ は定理 2.14(c) より、quaternion algebra である。すなわち、 E_{k_n} は超特異だから E も超特異である。

(2) を示す。一つ目から二つ目を示す。 E が通常なので定理 2.14(c) は有り得ない

から (b) となる。よって、 $D = F$ である。 E が通常であることと [Si, p.147 の下から七行目] より、埋め込み

$$F \hookrightarrow \text{End}_{\mathbb{Z}_p} \left(\varprojlim_m E[p^m](\mathbb{F}) \right) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}_p$$

が存在する。これと F が \mathbb{Q} 上の二次拡大体であることから、 p が分裂する。

逆を示す。仮定 $D = F$ と定理 2.14 より $F \neq \mathbb{Q}$ である。よって補題 2.15 より、

$$a_q(E) = \pi_E + \bar{\pi}_E, \quad \pi_E \bar{\pi}_E = q \tag{2.13}$$

が成立し、 F は \mathbb{Q} 上の総虚二次拡大である。 $(p) = \mathfrak{p}\mathfrak{p}'$ ($\mathfrak{p} \neq \mathfrak{p}'$) と書く。 $q = p^r$ として $(\pi_E) = \mathfrak{p}^m \mathfrak{p}'^n$, $(\bar{\pi}_E) = \mathfrak{p}'^n \mathfrak{p}^m$ ($m + n = r$) と書く。 m も n も正であると仮定して矛盾を導く。 π_E は p を割るので、 E の自己準同型 ϕ が存在して $\pi_E = [p] \circ \phi$ と書ける。 π_E は純非分離写像より、 $[p]$ もそうである。これより E は超特異になる (cf. [Si, Theorem 3.1 (a)(iii) in V.3])。主張 1 より、 $\pi_E^b \in \mathbb{Q}$ なる自然数 b が存在する。これより、 $\text{Nr}_{F/\mathbb{Q}}(\pi_E^b) = \pi_E^{2b}$ である。一方で、 $\text{Nr}_{F/\mathbb{Q}}(\pi_E) = q$ だから $\pi_E^{2b} = q^b$ を得る。よってこれの素イデアル分解を考えると

$$\mathfrak{p}^{2bm} \mathfrak{p}'^{2bn} = \mathfrak{p}^{br} \mathfrak{p}'^{br}$$

を得る。よって素イデアル分解の一意性より $m = n = r/2$ とならざるを得ない。よって、 $(\pi_E) = (\mathfrak{p}\mathfrak{p}')^{r/2}$ である。これと (2.2) により、 \mathfrak{p} における $D = F$ の局所ハッセ不変量が $1/2$ となり、これは矛盾である。よって、 m 或は n のいずれかは零でなくてはならない。必要なら順番を入れ替えて $(\pi_E) = \mathfrak{p}^r$, $(\bar{\pi}_E) = \mathfrak{p}'^r$ と書いてよい。すると、整数 $a_q(E) = \pi_E + \bar{\pi}_E$ は \mathfrak{p} でも \mathfrak{p}' でも割れないから p と素である。これと補題 2.18 から、 E は通常であることがわかった。

最後の主張は上の議論中で示されている。 □

系 2.20 E を k 上の楕円曲線とする。このとき、代数体 $F = \mathbb{Q}(\pi_E)$ の p の上にある素点 v で π_E の付値 $v(\pi_E)$ が正となるものが唯一つ存在する。

証明 p が分裂しないと仮定する。このとき、 p の上にある F の素点は一つしか存在しない。よって、 $\text{Nr}_{F/\mathbb{Q}}(\pi_E) = q$ より (π_E) はその唯一つの素イデアルの冪になる。よって、この場合の題意が従う。 p が分裂する場合は上の補題 2.19(2) の後半の主張より従う。 □

例 2.21 (i) 次のアフィン方程式を持つ \mathbb{F}_3 上の楕円曲線 E_1, E_2 を考える。

$$\begin{aligned} E_1: x^3 - x &= y^2, \\ E_2: x^3 - x &= y^2 - 1. \end{aligned}$$

$a_3(E_1) = 0, a_3(E_2) = -3$ が容易に確かめられ、補題 2.15(1) より

$$f_{E_1} = X^2 + 3, \quad f_{E_2} = X^2 + 3X + 3$$

となっている。 $3 \mid a_3(E_1), a_3(E_2)$ と補題 2.18 より、 E_1, E_2 は共に超特異である。 $\pi_{E_1}^2, \pi_{E_2}^6 \in \mathbb{Q}$ なので補題 2.19(1) を使っても E_1, E_2 が超特異であることが分かる。 $f_{E_1} \neq f_{E_2}$ と定理 2.5(b) より E_1 と E_2 は \mathbb{F}_3 上同種ではない。 $F_1 = \mathbb{Q}(\pi_{E_1}) = \mathbb{Q}(\sqrt{-3})$ である。 同じく $F_2 = \mathbb{Q}(\pi_{E_2}) = \mathbb{Q}(\sqrt{-3})$ である。 F_1 と F_2 は体として同型だが、 π_{E_1} と π_{E_2} は \mathbb{Q} 上共役でないことに注意する。 E_1, E_2 は共に定理 2.14 における (b) の場合をみたす超特異楕円曲線になる。 $\mathbb{Q}(\sqrt{-3})$ の整数環において $(\sqrt{-3})$ は素イデアルである。 素イデアル分解 $(3) = (\sqrt{-3})^2$, $(\pi_{E_1}) = (\pi_{E_2}) = (\sqrt{-3})$ が成り立つ。 これより、(3) は $F_1 = F_2$ で分岐している。

次にこの E_1, E_2 を \mathbb{F}_9 に底変換した場合を考えてみよう。

$$f_{(E_1)_{\mathbb{F}_9}} = (X + 3)^2, \quad f_{(E_2)_{\mathbb{F}_9}} = X^2 - 3X + 9$$

である。 これより、 $(E_1)_{\mathbb{F}_9}$ は定理 2.14 の (c) の場合になる。 このように底変換で自己準同型環が大きくなる様子が分かる。

$$\mathbb{Q}(\sqrt{-3}) = \text{End}_{M(\mathbb{F}_3)}(E_1) \subsetneq \text{End}_{M(\mathbb{F}_9)}(E_1) = D.$$

D は 3 と ∞ で分岐する \mathbb{Q} 上の quaternion algebra である。 一方で、 $(E_2)_{\mathbb{F}_9}$ は定理 2.14 の (b) の場合になる。 方程式 $x^3 = x - 1$ は \mathbb{F}_{3^3} に根を持つ。 その根を $\zeta \in \mathbb{F}_{3^3}$ を一つ固定する。

$$(E_1)_{\mathbb{F}_{3^3}} \rightarrow (E_2)_{\mathbb{F}_{3^3}}; (x, y) \mapsto (x + \zeta, y)$$

は同型となる。 このとき、フロベニウス特性多項式は共に $X^2 + 27$ になる。

(ii) $\zeta_3 \in \mathbb{F}_4$ を原始 3 乗根とする。 以下のアフィン方程式を持つ \mathbb{F}_4 上の楕円曲線 E を考える。

$$y^2 + y = \zeta_3 x^3.$$

このとき、 $|E(\mathbb{F}_4)| = 3$ が成立するので $f_E = X^2 - 2X + 4$ となる。よって、 $\pi_E = 1 \pm \sqrt{-3}$ であり、 $F = \mathbb{Q}(\sqrt{-3})$ である。 $2 \mid a_4(E)$ なので補題 2.18 より E は超特異である。整数環 \mathcal{O}_F は $\mathbb{Z}[\alpha]$ ($\alpha = (1 + \sqrt{-3})/2$) である。 $\alpha^2 - \alpha + 1 = 0$ をみたすので $\alpha, 1 - \alpha$ は単元である。(2) は \mathcal{O}_F の素イデアルであることが容易に確かめられる。よって $(\pi_E) = (2\alpha) = (2)$ は素イデアルである。まとめると、 E は 定理 2.14(b) の場合になるような超特異楕円曲線で、更に(2)が \mathcal{O}_F で素イデアルになる。

$E_{\mathbb{F}_2}$ は、同型を除いて唯一つの \mathbb{F}_2 上の超特異楕円曲線であることが知られている。

類似の \mathbb{F}_4 上の楕円曲線 $E' : y^2 + y = x^3$ を考える。 $f_{E'} = (X + 2)^2$ となる。 $F = \mathbb{Q}(\pi_{E'}) = \mathbb{Q}$ で定理 2.14(c) の場合をみたす。 E' は \mathbb{F}_2 上の同じ方程式で定義される楕円曲線の底変換になっている。この \mathbb{F}_2 上の楕円曲線を E_0 とかく。すると、 $f_{E_0} = X^2 + 2$ である。 $F_0 = \mathbb{Q}(\sqrt{-2})$ である。よって、定理 2.14(b) の場合になる。この場合は $(2) = (\sqrt{-2})^2$ と F_0 で分岐している。 \mathbb{F}_{2^6} は 1 の 9 乗根を含むので、 E_0 と E は \mathbb{F}_{2^6} 上で同型になる。

(iii) 次のアフィン方程式を持つ \mathbb{F}_5 上の楕円曲線 E を考える。

$$y^2 = x^3 + x.$$

すると、 $a_5(E) = 2$ が容易に確かめられる。 $F = \mathbb{Q}(i)$ である。このとき、 $\mathfrak{p} = (1 + 2i)$ 、 $\mathfrak{p}' = (1 - 2i)$ とおくと、これらは $\mathbb{Z}[i]$ の相異なる素イデアルになる。 $(5) = \mathfrak{p}\mathfrak{p}'$ となり、 $\mathbb{Z}[i]$ で (5) は分裂する。補題 2.19(2) より、 E は \mathbb{F}_5 上の通常楕円曲線である。補題 2.18 と $5 \nmid a_5(E)$ からこれも確かめられる。

本田・テイト理論を楕円曲線の場合に特化して、[Sch, Theorem 10.4] の形にまとめる。その前に簡単に楕円曲線の 1 次クリスタリニコホモロジーについてまとめる。 E を \mathbb{F}_q 上の楕円曲線とする。 $q = p^r$ と書く。 \mathbb{Q}_p の不分岐 r 次拡大体を \mathbb{Q}_q と書く。その整数環を \mathbb{Z}_q と書く。 $\sigma \in \text{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$ を p 乗フロベニウス自己同型写像の持ち上げとする。 E の 1 次クリスタリニコホモロジー $\Lambda_q = H_{\text{cris}}^1(E/\mathbb{Z}_q)$ は階数 2 の \mathbb{Z}_q 上自由加群である。更に σ -線型写像 F (i.e. $F(xv) = x^\sigma F(v)$ ($x \in \mathbb{Z}_q, v \in \Lambda_q$)) と σ^{-1} -線型写像 V を持ち、 $F \circ V = V \circ F = p$ をみたす。同型 $\Lambda_q \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \simeq \mathbb{Q}_q^2$ を一つ固定する。 F は σ 線型なので、ある $\delta \in \text{GL}_2(\mathbb{Q}_q)$ が存在して、 $F = \delta\sigma$ と書ける。

注意 2.22 A/k を g 次元アーベル多様体とする。

- (1) $\ell \neq p$ のとき、 $T_\ell A \simeq H^1(A_{\mathbb{F}}, \mathbb{Z}_\ell)^*$ が成り立つ。
- (2) 以下の関係式を満たす非可換環 $\mathfrak{D} = \mathbb{Z}_q[F, V]$ を考える。
 - $FV = VF = p$,
 - $F\alpha = \alpha^\sigma F, \alpha V = V\alpha^\sigma$ ($\alpha \in \mathbb{Z}_q$).

[MW, Theorem 4] 或は [D, Theorem in p.69] によれば次の反変圏同値が存在する。

$$D: \{ \text{階数が } p \text{ 冪の } k \text{ 上の可換有限群スキーム} \} \xrightarrow{\sim} \{ \text{長さ有限の } \mathfrak{D} \text{ 加群} \}.$$

有限群スキーム $A[p^n]$ を考える。 $D_n = D(A[p^n])$ とおく。包含写像 $A[p^n] \hookrightarrow A[p^{n+1}]$ に反変関手 D を施すと $D_{n+1} \rightarrow D_n$ という \mathfrak{D} 加群の射を得る。 $T_p A = \varprojlim_n D_n$ と定義し、これを A のデユドネ加群と呼ぶ。 $T_p A$ は \mathfrak{D} 加群であり、 \mathbb{Z}_q 上の階数 $2g$ の自由加群になる。このとき、 \mathfrak{D} 加群としての同型 $T_p A \simeq H_{\text{cris}}^1(A/\mathbb{Z}_q)$ が成立する。更に、次の自然な写像

$$\text{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\sim} \text{Hom}_{\mathfrak{D}}(T_p B, T_p A) \quad (2.14)$$

は同型であることが知られている (cf. [MW, Theorem 1 in II])。

定理 2.23 \mathbb{F}_q を標数 p の有限体とする。 $\ell \neq p$ とし、 $q = p^r$ と書く。

- (1) 任意の楕円曲線 E/\mathbb{F}_q に対して、 $H^1(E_{\mathbb{F}}, \mathbb{Q}_\ell)$ 上のフロベニウス作用は半単純である。その特性多項式 $f_E \in \mathbb{Z}[X]$ は ℓ によらない。更に、 F が $H_{\text{cris}}^1(E/\mathbb{Z}_q) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ に $\delta\sigma$ で作用しているとする、 $N\delta = \delta\sigma(\delta) \cdots \sigma^{r-1}(\delta)$ は半単純であって、その特性多項式は f_E に等しい。
- (2) $\gamma_E \in \text{GL}_2(\mathbb{Q})$ は半単純元で、その特性多項式が f_E であると仮定する。
 - (a) 以下の三条件をみたす $\text{GL}_2(\mathbb{Q})$ の半単純元 γ の共役類の集合 \mathfrak{S} を考える。
 - * γ の特性多項式が $X^2 - aX + q \in \mathbb{Z}[X]$ と書ける。
 - * γ の $\text{GL}_2(\mathbb{R})$ における像 γ_∞ が楕円的である (i.e. γ_∞ の最小多項式が \mathbb{R} 上既約であること。これより γ の特性多項式が重根を持たないとき、 $X^2 - aX + q$ の根は実数でない。)
 - * γ の根 π を取る。代数体 $\mathbb{Q}(\pi)$ の有限素点 v で $v(\pi) > 0$ なるものが唯一つ存在する。

このとき、対応 $E \mapsto \gamma_E$ は \mathbb{F}_q 上の楕円曲線の同種類の集合と \mathfrak{S} との間の一対一対応を与える。

(b) G_{γ_E} を γ_E の中心化群とする。次が成立する。

$$\begin{aligned} (\text{End}_{M(\mathbb{F}_q)}(E) \otimes \mathbb{Q}_\ell)^\times &\simeq G_{\gamma_E} \otimes \mathbb{Q}_\ell \quad (\ell \neq p), \\ (\text{End}_{M(\mathbb{F}_q)}(E) \otimes \mathbb{Q}_p)^\times &\simeq G_{\delta\sigma}(\mathbb{Q}_q) = \{y_p \in \text{GL}_2(\mathbb{Q}_q) \mid y_p^{-1} \delta y_p^\sigma = \delta\}. \end{aligned}$$

証明 (1) のクリスタリコホモロジーに関する主張以外はこれまで述べたことから従う。クリスタリコホモロジーに関する主張はクリスタリコホモロジーに関するレフシェッツ跡公式から従う。

主張 2 の (a) を示す。定理 2.5(b)、補題 2.15(1) と系 2.20 より、(a) の対応が well-defined であることが分かる。単射性は定理 2.5(b) より従う。全射性を考える。 $\gamma \in \mathfrak{S}$ を一つ取る。この特性多項式の根 π はヴェイユ q 数である。よって本田・テイト理論より、ある \mathbb{F}_q 上の単純アーベル多様体 A が存在して π_A と π が \mathbb{Q} 上共役になる。以下で $\dim A = 1$ を示す。 $F = \mathbb{Q}(\pi)$ とおく。仮定より、 $[F : \mathbb{Q}] \leq 2$ である。まず、 $F = \mathbb{Q}$ と仮定する。このとき、 r は偶数であり $\pi = \pm\sqrt{q} \in \mathbb{Q}$ が成り立つ。よって (2.2) により、斜体 $D = \text{End}_{M(k)}(A)$ の p におけるハッセ不変量は $1/2$ に等しい。よって、 $[D : \mathbb{Q}] = 4$ である。(2.3) より、 $\dim A = 1$ と分かる。

次に、 $[F : \mathbb{Q}] = 2$ と仮定する。このとき、 γ についての三つ目の条件より、 \mathfrak{p} を F の p の上にある素イデアルで、 $v_{\mathfrak{p}}(\pi) > 0$ なる唯一のものとする。 γ の条件より、 F は \mathbb{Q} の総虚二次拡大で $\pi\bar{\pi} = q$ が成り立つことを思い出す。このとき、 F における単項イデアル (p) と (π) の素イデアル分解について以下の三つの場合が有り得る。

- p が分裂の場合。 $(p) = \mathfrak{p}\mathfrak{p}'$ ($\mathfrak{p} \neq \mathfrak{p}'$), $(\pi) = \mathfrak{p}^r$, $(\bar{\pi}) = \mathfrak{p}'^r$
- p が分岐する場合。 $(p) = \mathfrak{p}^2$, $(\pi) = (\bar{\pi}) = \mathfrak{p}^r$,
- p が F で素イデアルの場合。 r が偶数であり、 $(p) = \mathfrak{p}$, $(\pi) = (\bar{\pi}) = \mathfrak{p}^{r/2}$.

いずれの場合にも容易に $\frac{v_{\mathfrak{p}}(\pi)}{v_{\mathfrak{p}}(q)} [F_{\mathfrak{p}} : \mathbb{Q}_p] = 1$ が確かめられるので、(2.2) より $\text{inv}_{\mathfrak{p}}(D) \equiv 0 \pmod{1}$ が示せる。 F は実素点がなく、 D は F 上分裂する斜体なので $D = F$ が分かる。故に (2.3) より、 $\dim A = 1$ が示せた。よって、 π は楕円曲線 A からくるヴェイユ q 数である。

主張 2 の (b) を示す。これは (2.5) と (2.14) から直ちに従う。 □

例 2.24 $q = 2^3$, $a = 2$ とする。 $X^2 - 2X + 8$ を特性多項式に持つ $\gamma \in \mathrm{GL}_2(\mathbb{Q})$ を考える。 $F = \mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{-7})$ であり、その整数環は $\mathbb{Z}[\alpha]$ ($\alpha = (1 + \sqrt{-7})/2$) である。 F は \mathbb{Q} 上の総虚二次拡大体である。 $\pi = 2\alpha$ は $X^2 - 2X + 8$ の根である。 $\mathfrak{p} = (\alpha)$, $\mathfrak{p}' = (\bar{\alpha})$ とおく。これらは $\mathbb{Z}[\alpha]$ の相異なる素イデアルである。 $\alpha\bar{\alpha} = 2$ が成り立つ。よって、以下の素イデアル分解が成り立つ。

$$(2) = \mathfrak{p}\mathfrak{p}', \quad (\pi) = (2\alpha) = \mathfrak{p}^2\mathfrak{p}'. \quad (2.15)$$

π はヴェイユ 8 数であるが、これは本田・テイト理論の意味で楕円曲線から来ないことを示す。もし仮にある \mathbb{F}_8 上の楕円曲線 E が存在して γ_E がこの γ と共役であると仮定する。定理 2.14, (2.15), 補題 2.19(2) より E は通常でなければならない。補題 2.18 より通常であれば $2 \nmid a_8(E) = a$ だが、 $a = 2$ なので矛盾である。

ところで γ は (a) における三つの条件の内最初の二つは満たす。よって、 γ は三つ目の条件をみたさないことが分かる。実際、これは (2.15) の二つ目の等式から見てとれる。

最後にヴェイユ 8 数 π に本田・テイト理論で対応するアーベル多様体 A の次元を求めてみる。 $D = \mathrm{End}_{M(\mathbb{F}_8)}(A)$ とおく。(2.2) と (2.15) により、 D の局所ハッセ不変量は以下ようになる。

$$\mathrm{inv}_{\mathfrak{p}}(D) \equiv \frac{2}{3}, \quad \mathrm{inv}_{\mathfrak{p}'}(D) \equiv \frac{1}{3} \pmod{1}.$$

これより、 $[D : \mathbb{Q}] = 9$ であり、(2.3) より $\dim A = 3$ になる。

注意 2.25 定理 2.23(a) の一つ目の条件に現れる $a \in \mathbb{Z}$ の動き得る範囲については [W, Theorem 4.1] に明示的に与えられている。[Sch, Theorem 10.4 (b)] では定理 2.23(2) の (a) における三つ目の条件が落ちているので注意が必要。

3 有理点の個数を勘定する ([Cl, §3], [Ko, §16], [Sch, §5])

この章の議論の高次元化、背景や更なる発展については、三枝氏の原稿「志村多様体のエタールコホモロジー」に詳述されているので、そちらを参照されたい。

3.1 ヘッケ対応と問題設定 ([Ko, §6])

ヘッケ対応について復習する。

p を素数とする。 \mathbb{A}_f^p を p の部分が自明な \mathbb{Q} の有限アデール環とする。 $\widehat{\mathbb{Z}}^p = \prod_{\ell \neq p} \mathbb{Z}_\ell$ を \mathbb{A}_f^p の整数環とする。 $\mathbb{A}_f^p = \widehat{\mathbb{Z}}^p \otimes_{\mathbb{Z}} \mathbb{Q}$ が成り立つ。 K^p を $\mathrm{GL}_2(\mathbb{A}_f^p)$ の開コンパクト部分群とする。後に K^p は

$$K(N) = \{g \in \mathrm{GL}_2(\widehat{\mathbb{Z}}^p) \mid g \equiv 1 \pmod{N}\}, \quad (p, N) = 1, \quad N \geq 3$$

ととる。 $\mathrm{GL}_2(\mathbb{Z}_p)K^p$ レベル構造を有するモジュラー曲線を Y_{K^p} と書くことにする。以下では Y_{K^p} が p で良い還元を持つので、還元して \mathbb{F}_p 上のスキームとみなす。 $g \in \mathrm{GL}_2(\mathbb{A}_f^p)$ を一つ固定する。これは次のヘッケ対応を誘導する。

$$Y_{K^p} \xleftarrow{a} Y_{K_g^p} \xrightarrow{b} Y_{K^p}. \tag{3.1}$$

但し、ここで $K_g^p = K^p \cap gK^p g^{-1}$ とおく。射 a は包含写像 $g^{-1}K_g^p g \subset K^p$ から誘導される被覆写像 $Y_{g^{-1}K_g^p g} \rightarrow Y_{K^p}$ と、同型 $K_g^p \xrightarrow{\sim} g^{-1}K_g^p g$; $h \mapsto g^{-1}hg$ が誘導する同型 $Y_{K_g^p} \xrightarrow{\sim} Y_{g^{-1}K_g^p g}$ の合成とする。射 b は単に包含写像 $K_g^p \subset K^p$ が誘導する被覆写像 $Y_{K_g^p} \rightarrow Y_{K^p}$ とする。このヘッケ対応 (3.1) を f と書く。

Y_{K^p} 上の p 乗フロベニウス自己準同型写像 Φ_p を考える。 $q = p^r$ に対して Φ_p^r を単に Φ_q と書く。「合成 $\Phi_q \circ f$ の固定点」を勘定する。この合成の意味を説明する。写像 Φ_q とヘッケ対応 f の合成は次のヘッケ対応になる。

$$Y_{K^p} \xleftarrow{a} Y_{K_g^p} \xrightarrow{c} Y_{K^p}.$$

但し、ここで c は合成 $\Phi_q \circ b$ である。合成 $\Phi_q \circ f$ の固定点とは、 $Y_{K_g^p}(\mathbb{F})$ の元であって a と c の像が一致するものこととする。

\mathbb{F} に含まれる有限体 k 上の楕円曲線 E に対して

$$H_1(E_{\mathbb{F}}, \widehat{\mathbb{Z}}^p) = \prod_{\ell \neq p} T_\ell E, \quad H_1(E_{\mathbb{F}}, \mathbb{A}_f^p) = H_1(E_{\mathbb{F}}, \widehat{\mathbb{Z}}^p) \otimes_{\mathbb{Z}} \mathbb{Q}$$

とおく。

K^p を $\mathrm{GL}_2(\mathbb{A}_f^p)$ の任意の開コンパクト部分群とする。以下ではモジュラー曲線 Y_{K^p} の \mathbb{F} 有理点は組 (E, η) の以下の意味の同種類とする。 E は \mathbb{F} 上の楕円曲線とし、 η はある同型 $\eta_0: (\mathbb{A}_f^p)^2 \xrightarrow{\sim} H_1(E_{\mathbb{F}}, \mathbb{A}_f^p)$ の K^p 軌道の集合 $\{\eta_0 \circ x \mid x \in K^p\}$ とする。二つの組 $(E, \eta), (E', \eta')$ が同種であるとは、ある p と素な同種 $f: E \rightarrow E'$ が存在して $\eta' = f \circ \eta$ となることとする。このような点の解釈の下で、ヘッケ作用素 $\Phi_q \circ f$ の固定点 $(E, \eta) \in Y_{K_g^p}(\mathbb{F})$ は E が \mathbb{F}_q 上の楕円曲線であり、 $\eta \circ g \equiv \pi_E \circ \eta \pmod{K^p}$ をみたすものことである (cf. [Ko, p.429 の最終段落])。

この固定点の個数を計算することが次の節の目標である。

l を p と異なる素数とする。 $\mathrm{GL}_2(\mathbb{A}_f^p)$ の連続 l 進表現 ξ を考える。これは Y_{K^p} 上のスムーズ l 進層 \mathcal{F}_{K^p} を誘導する。

3.2 レフシェッツ数

m を p と素な 3 以上の整数とする。

$$K^p = \left\{ g \in \mathrm{GL}_2(\widehat{\mathbb{Z}}^p) \mid g \equiv 1 \pmod{m} \right\}$$

とおく。この場合の Y_{K^p} はいわゆるフルレベル構造付きのモジュラー曲線 $Y(m)$ と一致する。このことを \mathbb{F} 有理点のところでも復習する。 $Y(m)$ の \mathbb{F} 有理点は \mathbb{F} 上の楕円曲線 E と同型 $\phi: (\mathbb{Z}/m)^2 \xrightarrow{\sim} E[m]$ の組の同型類 (E, ϕ) である。 ϕ を同型 $\tilde{\phi}: (\widehat{\mathbb{Z}}^p)^2 \xrightarrow{\sim} H_1(E_{\mathbb{F}}, \widehat{\mathbb{Z}}^p)$ に持ち上げて $\otimes_{\mathbb{Z}} \mathbb{Q}$ すると同型 $(\mathbb{A}_f^p)^2 \xrightarrow{\sim} H_1(E_{\mathbb{F}}, \mathbb{A}_f^p)$ を得る。これの K^p 軌道を考えれば、軌道は $\tilde{\phi}$ の取り方によらない。この軌道を η_ϕ と書くに対応 $(E, \phi) \mapsto (E, \eta_\phi)$ は全単射 $Y(m)(\mathbb{F}) \xrightarrow{\sim} Y_{K^p}(\mathbb{F})$ を誘導する。

E_0 を \mathbb{F}_q 上の楕円曲線とする。 \mathcal{F}_{K^p} を $\mathrm{GL}_2(\mathbb{A}_f^p)$ の有限次元表現 ξ に対応するスムーズ層と仮定する。 $g \in \mathrm{GL}_2(\mathbb{A}_f^p)$ とする。以下のレフシェッツ数を計算したい。

$$T(E_0, \xi, g) = \sum_x \mathrm{tr}(\Phi_q \circ f; \mathcal{F}_{K^p, \bar{x}}).$$

ここで、 x は Y_{K^p} の固定点 (E, η) に対応し E は E_0 に \mathbb{F}_q 上同種であるもの全体を走る。 \bar{x} は x の上の幾何学的点とする。この添字の集合を $\mathcal{M}_m(\mathbb{F}_q)(E_0)$ と書く。 $\mathbb{Z}_q = W(\mathbb{F}_q)$, $\mathbb{Q}_q = \mathbb{Z}_q \otimes_{\mathbb{Z}} \mathbb{Q}$ とおく。

$$H^p = H_1(E_{0, \mathbb{F}}, \mathbb{A}_f^p), \quad H_p = H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)^* \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$$

とおく。但し、 $H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)^*$ は \mathbb{Z}_q 加群としての $H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)$ の双対を表す。次のように $H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)^*$ 上の σ -線型自己準同型写像 F^* と σ^{-1} -線型自己準同型写像 V^* を定義する:

$$\begin{aligned} F^*: H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)^* &\rightarrow H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)^*; f \mapsto \sigma \circ f \circ V, \\ V^*: H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)^* &\rightarrow H_{\mathrm{cris}}^1(E_0/\mathbb{Z}_q)^*; f \mapsto \sigma^{-1} \circ f \circ F \end{aligned}$$

とおく。 $F^*V^* = V^*F^* = p$ が成り立つ。 $x \in \mathcal{M}_m(\mathbb{F}_q)(E_0)$ を任意に取る。 H^p の基底を取ると、 H^p の自己同型写像 $(\pi_{E_0})_*^{-1}$ に対応する元 $\boxed{\gamma \in \mathrm{GL}_2(\mathbb{A}_f^p)}$ を得る。 H_p

の基底を取ると H_p 上の等式 $F^* = \delta\sigma$ で特徴付けられる $\delta \in \text{GL}_2(\mathbb{Q}_q)$ が定まる。定理 2.23 (2) により、 E_0 から決まる γ_{E_0} を考え、 $\gamma_0 = \gamma_{E_0}^{-1} \in \text{GL}_2(\mathbb{Q})$ とおく。その $\text{GL}_2(\mathbb{A}_f^p)$, $\text{GL}_2(\mathbb{Q}_p)$ における像はそれぞれ γ , $N\delta$ と共役になる。同型 $(\mathbb{A}_f^p)^2 \simeq H^p$, $\mathbb{Q}_q^2 \simeq H_p$ を固定する。

補題 3.1 $\Gamma = (\text{End}_{M(k)}(E_0))^\times$, $K_p = \text{GL}_2(\mathbb{Z}_q)$ とおく。

$$Y^p = \{y \in \text{GL}_2(\mathbb{A}_f^p)/K_g^p \mid y^{-1}\gamma y \in K^p g^{-1}\},$$

$$Y_p = \left\{x \in \text{GL}_2(\mathbb{Q}_q)/K_p \mid x^{-1}\delta x^\sigma \in K_p \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} K_p \right\}$$

とおくとき、 $\mathcal{M}_m(\mathbb{F}_q)(E_0)$ は $\Gamma \setminus (Y^p \times Y_p)$ と自然に同一視される。

証明 well-defined 性:

$x = (E_x, \phi) \leftrightarrow (E_x, \eta_\phi) \in \mathcal{M}_m(\mathbb{F}_q)(E_0)$ を考える。軌道 η_ϕ の元 $\tilde{\phi}$ を一つとる。同種 $f: E_0 \rightarrow E_x$ を取る。 p の外をまず見る。次の可換図式で定まる $y^p \in \text{GL}_2(\mathbb{A}_f^p)$ を取る。

$$\begin{array}{ccc} (\mathbb{A}_f^p)^2 & \xrightarrow[\simeq]{\tilde{\phi}} & H_1(E_x, \mathbb{F}, \mathbb{A}_f^p) \\ \downarrow y^p & & \uparrow f_* \simeq \\ (\mathbb{A}_f^p)^2 & \xrightarrow[\simeq]{\text{fixed}} & H^p. \end{array}$$

すると $y^p K_g^p \in \text{GL}_2(\mathbb{A}_f^p)/K_g^p$ を得る。これは軌道の元 $\tilde{\phi}$ の取り方によらない。固定点の定義の $\eta_\phi \circ g \equiv \pi_E \circ \eta_\phi \pmod{K^p}$ を考える。これを翻訳すると $y^p K_g^p \in Y^p$ を得る。

次に Y_p の方を考える。次の状況を考える。

$$\mathbb{Q}_q^2 \simeq H_p \xrightarrow{f_*} H_{\text{cris}}^1(E_x/\mathbb{Z}_q)^* \otimes_{\mathbb{Z}_q} \mathbb{Q}_q. \tag{3.2}$$

最初の同型による H_p の格子 $H_{\text{cris}}^1(E_0/\mathbb{Z}_q)^*$ の \mathbb{Q}_q^2 における像を Λ と書く。二つの同型 (3.2) を通じた $H_{\text{cris}}^1(E_x/\mathbb{Z}_q)^*$ の \mathbb{Q}_q^2 における像は、ある元 $y_p K_p \in \text{GL}_2(\mathbb{Q}_q)/K_p$ が存在して $y_p \Lambda$ と書ける。この格子は F^* と V^* で安定であるため、 $F^* y_p \Lambda \subset y_p \Lambda$ かつ $V^* y_p \Lambda \subset y_p \Lambda$ が成立する。この条件は $F^* V^* = p$ を用いると結局

$$p y_p \Lambda \subset F^* y_p \Lambda \subset y_p \Lambda$$

と書ける。 $F^* = \delta\sigma$ と書いて、上の包含関係に y_p^{-1} をかけると

$$p\Lambda \subset y_p^{-1}\delta y_p^\sigma \Lambda \subset \Lambda \tag{3.3}$$

を得る。ヴェイユペアリングは H_p の \mathbb{Q}_q 上の二階外積と $\mathbb{Q}_q(1)$ の同型を導く。よって $v(\det(\delta)) = -1$ が分かる。 $v(\det(y_p^{-1}\delta y_p^\sigma)) = -1$ を得る。するとカルタン分解より

$$y_p^{-1}\delta y_p^\sigma \in K_p \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} K_p$$

と書ける。これより $y_p K_p \in Y_p$ を得る。逆に $y_p K_p \in Y_p$ とすれば (3.3) をみたく。

単射性を示す。 (E_x, η_x) と $(E_{x'}, \eta_{x'})$ が同じ像を持つとする。 $f_1: E_0 \rightarrow E_x$, $f_2: E_0 \rightarrow E_{x'}$ を同種とする。ここから作る $Y^p \times Y_p$ の元は E_0 の自己同種 h だけずれている。 $mh \in \text{End}(E_0)$ となる自然数 m をとり、 $h_0 = mh$ とおく。 f_1 と f_2 をそれぞれ $f_1 h_0$ と $f_2 m$ で置き換えれば $Y^p \times Y_p$ の元として一致しているとしてよい。 Y_p で一致しているから同種 $f = f_1 f_2^{-1}$ が p と素な同種であることを示せば十分である。これは Y_p の元として一致していることとデユドネ理論から従う。

次に全射性を考える。任意の $(y^p K_g^p, y_p K_p) \in Y^p \times Y_p$ を取る。スカラー倍で取り替えて $L := y^p(\widehat{\mathbb{Z}}^p)^2 \supset H_1(E_{0,\mathbb{F}}, \widehat{\mathbb{Z}}^p)$ かつ $\Lambda := y_p \mathbb{Z}_q^2 \supset H_{\text{cris}}^1(E_{0,\mathbb{F}}/\mathbb{Z}_q)^*$ と仮定してよい。すると、エタール被覆の理論とデユドネ理論から L と Λ に対応する E_0 の部分群 G^p と G_p が存在する。これを用いて $E = E_0/(G^p G_p)$ として楕円曲線を定める。 $f: E_0 \rightarrow E$ を標準射とする。可換図式

$$\begin{array}{ccc} (\widehat{\mathbb{Z}}^p)^2 & \xrightarrow{\phi} & L = H_1(E_{\mathbb{F}}, \widehat{\mathbb{Z}}^p) \\ \downarrow y^p & & \uparrow f_* \cup \\ (\mathbb{A}_f^p)^2 & \xrightarrow[\simeq]{\text{fixed}} & H^p \end{array}$$

により ϕ を定義する。同型 $\phi \otimes_{\mathbb{Z}} \mathbb{Q}$ の K_g^p 軌道を η とすれば $(E, \eta) \in \mathcal{M}_m(\mathbb{F}_q)(E_0)$ が欲しかったものになる。 □

γ は p.344 の通りとする。中心化部分群

$$\begin{aligned} G_\gamma(\mathbb{A}_f^p) &= \{y \in \text{GL}_2(\mathbb{A}_f^p) \mid y^{-1}\gamma y = \gamma\}, \\ G_{\delta\sigma}(\mathbb{Q}_p) &= \{x \in \text{GL}_2(\mathbb{Q}_q) \mid x^{-1}\delta x^\sigma = \delta\} \end{aligned}$$

を得る。 f^p を $K^p g^{-1} K^p$ の特性関数を K^p の体積で割った関数とする。 ϕ_q を

$$\mathrm{GL}_2(\mathbb{Z}_q) \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_q)$$

の特性関数を $\mathrm{GL}_2(\mathbb{Z}_q)$ の体積で割った関数とする。任意の $\mathrm{GL}_2(\mathbb{A}_f^p)$ 上のコンパクト台を持つスムーズな関数 f に対して軌道積分

$$O_\gamma(f) = \int_{G_\gamma(\mathbb{A}_f^p) \backslash \mathrm{GL}_2(\mathbb{A}_f^p)} f(y^{-1} \gamma y) dy$$

を考える。 $\mathrm{GL}_2(\mathbb{Q}_q)$ 上のコンパクト台を持つ任意のスムーズ関数 ϕ に対して twisted 軌道積分

$$TO_{\delta\sigma}(\phi) = \int_{G_{\delta\sigma}(\mathbb{Q}_p) \backslash \mathrm{GL}_2(\mathbb{Q}_q)} \phi(x^{-1} \delta x^\sigma) dx$$

も考える。

以下の定理は [Ko, (19.2)] にある。[Sch, Corollary 5.2] も参照されたい。 γ_0 は、p.345 の通りとする。

定理 3.2 次が成立する。

$$T(E_0, \xi, g) = \mathrm{vol}(\Gamma \backslash (\mathrm{End}(E_0) \otimes \mathbb{A}_f)^\times) O_\gamma(f^p) TO_{\delta\sigma}(\phi_q) \mathrm{tr} \xi(\gamma_0).$$

証明 補題 3.1 により $\mathcal{M}_m(\mathbb{F}_q)(E_0)$ は

$$\int_{\Gamma \backslash \mathrm{GL}_2(\mathbb{A}_f^p) \times \mathrm{GL}_2(\mathbb{Q}_q)} f^p(y^{-1} \gamma y) \phi_q(x^{-1} \delta x^\sigma) dy dx$$

と一致する。これは明らかに次に等しい。

$$\mathrm{vol}(\Gamma \backslash G_\gamma(\mathbb{A}_f^p) \times G_{\delta\sigma}(\mathbb{Q}_p)) O_\gamma(f^p) TO_{\delta\sigma}(\phi_q).$$

定理 2.23(b) より

$$\mathrm{vol}(\Gamma \backslash G_\gamma(\mathbb{A}_f^p) \times G_{\delta\sigma}(\mathbb{Q}_p)) = \mathrm{vol}(\Gamma \backslash (\mathrm{End}(E_0) \otimes \mathbb{A}_f)^\times)$$

が成り立つ。あとは $\mathrm{tr}(\Phi_q \circ f; \mathcal{F}_{K^p, \bar{x}})$ の計算である。これについては [Ko, p.433–434] に詳述されているので省略するが結果的には x によらず $\mathrm{tr} \xi(\gamma_0)$ に等しいことが分かる。□

■謝辞 清水氏と竹内氏から貴重なご意見を頂いた。また三枝氏と越川氏からも貴重なコメントを頂いた。各氏に感謝の意を表したい。本記事を作成するという機会を頂いたことに対して、サマースクールのオーガナイザーの方々に感謝したい。

参考文献

- [Cl] L. Clozel, *Nombre de points des variétés de Shimura sur un corps fini*, Séminaire Bourbaki (1992-1993) Exposé 766, 121–149.
- [D] M. Demazure, *Lectures on p -divisible groups*, LNM 302.
- [Ho] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.
- [Ko] R. E. Kottwitz, *Points on some Shimura varieties over finite fields*, J. Amer. Math. Soc., **5** (1992), 373–444.
- [Mi] J. S. Milne, *Abelian varieties*, in Course Notes in his homepage.
- [Mi2] J. S. Milne, *Introduction to Shimura varieties*, in Harmonic Analysis, the Trace Formula and Shimura Varieties, Clay Mathematics Proceedings, vol 4, AMS, 2005.
- [MW] J. S. Milne and W. C. Waterhouse, *Abelian varieties over finite fields*, Proc. Symp. Pure Math. **20** (1971), 53–64.
- [P] M. Papikian, *Honda-Tate theorem for elliptic curves*, in Expository Notes in his homepage.
- [Sch] P. Scholze, *The Langlands-Kottwitz method for the modular curve*, Int. Math. Res. Not. no. 15 (2011), 3368–3425.
- [Si] J. Silverman, *The arithmetic of elliptic curves*, GTM 106.
- [ST] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan, no. 6, 1961.
- [Ta1] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.
- [Ta2] J. Tate, *Classes d’isogénie des variétés abéliennes sur un corps fini (d’après T. Honda)*, Sémin. Bourbaki Nov. 1968, Exposé 352, 95–109.

- [W] W. C. Waterhouse, *Abelian varieties over finite fields*, Annales scientifiques de l'École Normale Supérieure **2** (1969), 521–560.