Coates-Wiles の定理
～ Rubin の Lecture Note の翻訳 ～

野本慶一郎

目次

この pdf では Coates-Wiles の定理という楕円曲線論における大定理の証明を解説した Rubin の Lecture Note [4] を翻訳していくことにする．しかしその pdf は行間も多く読みづらい部分が多々あるので, 修論として綺麗にまとめられている pdf [1] を主に参考にしながらまとめることにする．また, 楕円曲線の一般論をつらつらと書いていっても抽象的でよく分からないと思うので, 全て楕円曲線

$$E_1 : y^2 = x^3 - x$$

で統一して例を挙げたいと思う．ただし E_1 の定義体は適切に base change する．(適切な例が作れない場合は適宜楕円曲線を変更する．) また, 他の楕円曲線でも遊んでみたい人のために, Magma [2] のコードを例として載せる．それをお試し用のサイトの

http://magma.maths.usyd.edu.au/calc/

に打ち込んで遊んでみてほしい．楕円曲線 $E_1/\mathbb{Q} : y^2 = x^3 - x$ を定義するには

```
> E:=EllipticCurve([-1,0]);
> E;
Elliptic Curve defined by y^2 = x^3 - x over Rational Field
```

とすればよい．ただし各行の初めにある「>」は, 本物の Magma でコードを打ち込むときに勝手に現れるものなので, お試し用サイトで打ち込む場合は無視して $E := \cdots$ と書き始めればよい．一般の Weierstrass 方程式

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

で $\mathbb{Q}$ 上の楕円曲線を定義するには EllipticCurve($[a_1, a_2, a_3, a_4, a_6]$) と書く．上の $E_1/\mathbb{Q}$ の例は, $y^2 = x^3 + ax + b$ という形で定義されるので, 省略系の EllipticCurve([a, b]) と書くことができる．

1 Complex Multiplication

特に断りがない限り以下の記号と記法を固定する．

- $F \subset \mathbb{C}$; 部分体.
- E/F; 楕円曲線.
- E が虚二次体の order $\iota(\mathrm{End}_F(E)) = \mathcal{O}$ により虚数乗法をもつ場合, $K := \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}$. (cf. Proposition 1.1)
- $K \subset F$.
- $\mathfrak{a} \leq \mathcal{O}_K; \mathcal{O}_K$ の整イデアル.
- $\mathfrak{a} \leq K$; K の分数イデアル .
- $\mathfrak{a} \lhd \mathcal{O}_K$; 6 と互いに素な非自明な整イデアル.
- $E[\mathfrak{a}] := \cap_{\alpha\in\mathfrak{a}} E[\alpha]$.
- $E[\mathfrak{p}^\infty] := \cup_{n\geq 1} E[\mathfrak{p}^n]$ ($\mathfrak{p} \leq \mathcal{O}_K$; 素イデアル).

ここでの目標としては (i) 虚数乗法をもつ楕円曲線に対して Hecke 指標を構成すること, (ii) 等分点を添加した体のガロア群 $G(K(E[\mathfrak{a}])/K)$ の性質を調べること, である．上に現れた準同型 ι は以下の命題のものである．

Proposition 1.1: [4, p. 3, Definition 1.7]

$\mathcal{D}$ で E/F の正則微分形式のなす 1 次元ベクトル空間を表すものとする．このときアーベル群としての準同型

$$\iota = \iota_F : \mathrm{End}_F(E) \to \mathrm{End}_F(\mathcal{D}(E/F)) \simeq F; \phi \mapsto [\omega_E \mapsto \phi^*\omega_E] \mapsto \alpha_\phi$$

が存在する．ただし $\omega_E = fdx$ は $\mathcal{D}(E/F)$ の基底であり, $\phi^*(fdx) := (f \circ \phi)d(x \circ \phi)$ である．また, $\alpha_\phi \in \mathbb{C}$ は $\phi^*\omega_E = \alpha_\phi\omega_E$ を満たす定数である．$\mathrm{Ker}\,\iota$ は非分離な自己準同型のなすイデアルであり, $\mathrm{ch}(F) = 0$ ならば ι_F は単射である．

楕円曲線 E/F が虚数乗法 (Complex Multiplication) をもつというのは $\iota(\mathrm{End}_F(E))$ が $\mathbb{Z}$ よりも真に大きくなること, 特に今 $F \subset \mathbb{C}$ と仮定しているので $\iota(\mathrm{End}_F(E))$ は虚二次体の order にしかなり得ない．従って以降は楕円曲線 E/F の自己準同型環は, ある虚二次体の order$\mathcal{O}$ が存在して $\iota(\mathrm{End}_F(E)) = \mathcal{O}$ を満たし, その虚二次体を $K := \mathbb{Q} \otimes \mathcal{O}$ とする．

与えられた楕円曲線が CM をもつかどうかは, 以下のように確かめられる.

```
E:=EllipticCurve([-1,0]);
> HasComplexMultiplication(E);
true -4
```

返り値の -4 というのは, 虚二次体の判別式を返してくれる. すなわちこの場合は $K = \mathbb{Q}(\sqrt{-1})$ の order により虚数乗法をもつということが分かる.

以下の命題は, 楕円曲線 E の自己準同型が定義される体を見るには ι の像を見ればよいということを主張している.

Lemma 1.2: [4, p. 3, Lemma 1.8]

$L \supset F$ を体, $\phi \in \mathrm{End}_L(E)$ とする. このとき $\iota_L(\phi) \in F$ ならば $\phi \in \mathrm{End}_F(E)$.

Proof. $\phi \in \mathrm{End}_L(E)$ を一つ取る. このとき任意の $\sigma \in \mathrm{Aut}_F(\bar{L})$ に対して $\phi^\sigma = \phi$ を示せばよい. 特に Proposition 1.1 より $\iota_L(\phi^\sigma) = \iota(\phi)$ を示せば ι の単射性より ok. さらに仮定 $\iota_L(\phi) \in F$ より $\iota_L(\phi) = \sigma(\iota_L(\phi))$ であるから, $\iota_L(\phi^\sigma) = \sigma(\iota_L(\phi))$ を示せばよい. これは定義に従って考えることで分かる.

> $\mathrm{End}_F(\mathcal{D}(E/F))$ の基底を $\omega = f dx$ と表す. このとき $\iota_L(\phi) = a_\phi$ と書ける. ただし a_ϕ は $\phi^*\omega = a_\phi \omega$ を満たす定数である. 従って $a_{\phi^\sigma} = \sigma(a_\phi)$ を示せばよい. さらに $a_\phi \in F$ なので $a_{\phi^\sigma} = a_\phi$ を示せばよい. 定義から
>
> $$(\phi^*\omega)^\sigma = a_\phi \omega^\sigma, \quad (\phi^\sigma)^*\omega^\sigma = a_{\phi^\sigma}\omega^\sigma$$
>
> が成り立つので, $(\phi^*\omega)^\sigma = (\phi^\sigma)^*\omega^\sigma$ を示せばよい. これらを書き下すと
>
> $$\begin{aligned}(\phi^*\omega)^\sigma &= (\phi^* f dx)^\sigma = (f \circ \phi \; d(x \circ \phi))^\sigma = (f \circ \phi)^\sigma \; d(x \circ \phi)^\sigma = f^\sigma \circ \phi^\sigma \; d(x^\sigma \circ \phi^\sigma) \\ (\phi^\sigma)^*\omega^\sigma &= (\phi^\sigma)^* f^\sigma dx^\sigma = f^\sigma \circ \phi^\sigma \; d(x^\sigma \circ \phi^\sigma)\end{aligned}$$
>
> となって確かに等しいことが分かる.

□

Proposition 1.3: [4, p. 15, Propositoin 5.3]

ある F 上定義された同種 $\phi : E \to E'$ が存在する. ここで E'/F は maximal order $\mathcal{O}_K$ により虚数乗法をもつ楕円曲線である.

Proof. まず order $\mathcal{O}$ を, あるイデアル $\mathfrak{c} = c\mathcal{O}_K$ を用いて $\mathcal{O} = \mathbb{Z} + \mathfrak{c} = \mathbb{Z} + c\mathcal{O}_K$ と表しておく. このとき

Proposition 1.4: [5, Remark 4.13.2, p. 74]

K を体, E/K を楕円曲線, $\Phi \leq E$ を有限部分群で $G(\bar{K}/K)$ 不変なもの, すなわち任意の $P \in \Phi, \sigma \in G(\bar{K}/K)$ に対して $\sigma(P) \in \Phi$ を満たすとする. このとき

$$^\exists E'/K; \text{楕円曲線}, \quad ^\exists \phi : E \to E'; \text{同種}/K \;\text{ such that }\; \mathrm{Ker}\,\phi = \Phi$$

が成り立つ.

を用いて E' を構成する. まず $E[\mathfrak{c}]$ が $G(\bar{F}/F)$ 不変を示す. 任意の $P \in E[\mathfrak{c}]$ と任意の $\sigma \in G(\bar{F}/F)$ を取る. このとき $c \in \mathfrak{c}$ に対して $c(P^\sigma) = O$ を示せばよい. $c \in \mathrm{End}_F(E)$ は $\iota(\mathrm{End}_F(E)) = \mathcal{O}$ の元と同一視しているから $c^\sigma = c$ である. 従って

$$c(P^\sigma) = c^\sigma(P^\sigma) = (cP)^\sigma = O^\sigma = O$$

となって ok. また, 準同型定理から $E/E[\mathfrak{c}] \simeq E'$ が成り立つ.

あとは $\mathrm{End}_F(E') \simeq \mathcal{O}_K$ を示せばよい. 特に全射 $\phi : E \to E'$ から単射 $\mathrm{End}_F(E') \to \mathrm{End}_F(E) \simeq \mathcal{O} \subset \mathcal{O}_K$ が誘導されるので, 単射 $\mathcal{O}_K \hookrightarrow \mathrm{End}_F(E')$ が存在することを示せばよい. さらに Lemma 1.2 より, 任意の $\alpha \in \mathcal{O}_K$ に対して $\alpha \in \mathrm{End}_{\mathbb{C}}(E')$ を示せばよい. 格子 L を用いて同型 $E(\mathbb{C}) \simeq \mathbb{C}/L$ を固定する. このとき $E'(\mathbb{C}) \simeq \mathbb{C}/L'$ が成り立つ. ただし

同型 $E/E[\mathfrak{c}] \simeq E'$ から

$$L' = \{z \in \mathbb{C} \mid z\mathfrak{c} \subset L\}$$

と書けることに注意する．$\mathrm{End}_{\mathbb{C}}(E') \simeq \{z \in \mathbb{C} \mid zL' \subset L'\}$ であるから，$\alpha L' \subset L'$ を示せばよい．つまり任意の $w \in L'$ に対し $\alpha w \in L'$，すなわち $(\alpha w)\mathfrak{c} \subset L$ を示せばよい．そしてそれは

$$(\alpha w)\mathfrak{c} = w(\alpha \mathfrak{c}) \in L \quad (\because w \in L')$$

より ok. □

E/F は虚二次体の order $\mathcal{O}$ により虚数乗法をもつと仮定しているが，Proposition 1.3 より E を E' に置き換えることで，maximal order，すなわち整数環 $\mathcal{O}_K$ により虚数乗法をもつと"仮定してよい"．ただし，E と E' はいわゆる"isogenous (同種)"なだけであり，同型より少し弱い．isogenous な楕円曲線は bad な素点が一致する，特にコンダクターと呼ばれる reductuion の様子を表す不変量が等しいなどの特徴があるが，全ての性質が等しくなるわけではない．実際，周期と呼ばれる値は楕円曲線の model に依存するので値が異なる．従って $\mathcal{O}_K$ により虚数乗法をもつとするのか，一般の $\mathcal{O}$ により虚数乗法をもつとするのか，適切に選択しなければならないことに注意をしておく．

Proposition 1.5: [4, p. 16, Proposition 5.4]

$0 \neq \mathfrak{a} \leq \mathcal{O}_K$ とする．このとき $\mathcal{O}_K$ 加群としての同型 $E[\mathfrak{a}] \simeq \mathcal{O}_K/\mathfrak{a}$ が成り立つ．

Proof. 群同型

$$\xi : E(\mathbb{C}) \simeq \mathbb{C}/L$$

を固定する．E には，同一視 $\mathcal{O}_K \simeq \mathrm{End}_F(E)$ を用いて $\mathcal{O}_K$ 加群の構造が入り，$\mathbb{C}/L$ にも $\mathcal{O}_K$ の元を掛けるという作用により $\mathcal{O}_K$ 加群の構造が入る．このとき ξ は $\mathcal{O}_K$ 同型であることを注意しておく．このとき自然に $\xi|_{E[\mathfrak{a}]} : E[\mathfrak{a}] \simeq \mathfrak{a}^{-1}L/L$ が成り立つ．

> 感覚的には両辺とも $\mathfrak{a}$ 倍して消える元の集合という形で分かる．実際には $\xi|_{E[\mathfrak{a}]}$ の像が $\mathfrak{a}^{-1}L/L$ であることを示せばよい．$z \in \mathrm{Im}(\xi|_{E[\mathfrak{a}]})$ を任意に取る．このとき ${}^{\exists}P \in E[\mathfrak{a}]$ such that $\xi|_{E[\mathfrak{a}]}(P) = z$ が成り立つ．従って $\alpha \in \mathfrak{a}$ に対して
>
> $$\alpha z = \alpha \xi|_{E[\mathfrak{a}]}(P) = \xi|_{E[\mathfrak{a}]}(\alpha P) = \xi|_{E[\mathfrak{a}]}(0) = 0$$
>
> であるから $\alpha z \in L$，すなわち $z \in \mathfrak{a}^{-1}L/L$ が成り立つ．逆の包含も同様にして分かる．

□

Corollary 1.6: [4, p. 16, Corollary 5.6]

$0 \neq \mathfrak{a} \leq \mathcal{O}_K$ とすると，作用 $G(\bar{F}/F) \curvearrowright E[\mathfrak{a}]$ は単射

$$G(F(E[\mathfrak{a}])/F) \hookrightarrow (\mathcal{O}_K/\mathfrak{a})^{\times}$$

を誘導する．特に $F(E[\mathfrak{a}])/F$ はアーベル拡大である．

Proof. Proposition 1.5 より

$$\mathrm{Aut}_{\mathcal{O}_K}(E[\mathfrak{a}]) \simeq \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{O}_K/\mathfrak{a}) = (\mathcal{O}_K/\mathfrak{a})^{\times}$$

であるから，単射 $G(F(E[\mathfrak{a}])/F) \hookrightarrow \mathrm{Aut}_{\mathcal{O}_K}(E[\mathfrak{a}])$ が存在することを言えばよい．写像

$$\varphi : G(F(E[\mathfrak{a}])/F) \to \mathrm{Aut}_{\mathcal{O}_K}(E[\mathfrak{a}])$$

を，$\varphi(\sigma) :=$ "$P \mapsto \sigma(P)$" と定める．well-defined と単射性をチェックする．

(well-defined) $\varphi(\sigma)(P)=\sigma(P)\in E[\mathfrak{a}]$ であること，$P\mapsto\sigma(P)$ の逆写像は $P\mapsto\sigma^{-1}(P)$ で与えられることから，$\varphi(\sigma)$ が $\mathcal{O}_K$ 加群としての準同型であることのみ示せばよい．任意の $\beta\in\mathcal{O}_K$，任意の $\sigma\in G(\bar{F}/F)$ に対して

$$\begin{aligned}\varphi(\sigma)(\beta P)&=\sigma(\beta P)\\&=\sigma(\beta)\sigma(P)\\&=\beta(\sigma P)\ (\because \beta\in\mathrm{End}_F(E),\text{すなわち }F\text{ 上定義されている})\\&=\beta\varphi(\sigma)(P)\end{aligned}$$

となるから ok.

(単射) $\varphi(\sigma)=\mathrm{id}$，すなわち任意の $P\in E[\mathfrak{a}]$ に対し $\sigma(P)=P$ と仮定する．このとき σ は $F(E[\mathfrak{a}])$ を固定するので $\sigma=\mathrm{id}\ \text{in}\ G(F(E[\mathfrak{a}])/F)$ である．ok. □

Example 1.7

$F=\mathbb{Q},K=\mathbb{Q}(i),E_1/F:y^2=x^3-x,\mathfrak{a}=4$ に対して本当に $G(F(E_1[\mathfrak{a}])/F)$ がアーベル群なのか調べてみる．それには $E_1[4]$ を求める必要があるが，Magma の DivisionPoints(O, 4) コマンドは，E の定義体上の 4 分点しか計算してくれない，すなわち今の場合 $E_1(\mathbb{Q})[4]$ しか計算してくれない．なので一度 $\mathbb{C}$ に base change した上で 4 分点を調べる．

```
> C<i>:=ComplexField();
> E:=EllipticCurve([-1,0]);
> E:=BaseChange(E,C);
> O:=E![0,1,0];
> DivisionPoints(O,4);
[ (0.000000000000000000000000000000 : 1.00000000000000000000000000000 :
0.000000000000000000000000000000), (-2.41421356237309504880168872421 :
3.41421356237309504880168872421*i : 1.00000000000000000000000000000),
(-1.00000000000000000000000000000 : 0.000000000000000000000000000000 :
1.00000000000000000000000000000), (-0.414213562373095048801688724210 :
0.585786437626904951198311275790 : 1.00000000000000000000000000000),
(0.000000000000000000000000000000 : 0.000000000000000000000000000000 :
1.00000000000000000000000000000), (0.414213562373095048801688724210 :
0.585786437626904951198311275790*i : 1.00000000000000000000000000000),
(1.00000000000000000000000000000 : 0.000000000000000000000000000000 :
1.00000000000000000000000000000), (2.41421356237309504880168872421 :
3.41421356237309504880168872421 : 1.00000000000000000000000000000),
(-1.00000000000000000000000000000*i : -1.00000000000000000000000000000 -
1.00000000000000000000000000000*i : 1.00000000000000000000000000000),
(-1.00000000000000000000000000000*i : 1.00000000000000000000000000000 +
1.00000000000000000000000000000*i : 1.00000000000000000000000000000),
(1.00000000000000000000000000000*i : -1.00000000000000000000000000000 +
1.00000000000000000000000000000*i : 1.00000000000000000000000000000),
(1.00000000000000000000000000000*i : 1.00000000000000000000000000000 -
1.00000000000000000000000000000*i : 1.00000000000000000000000000000) ]
```

すると 12 個の点から成るリストが出てくる．順番に見ていくと，$[0:1:0],[-1-\sqrt{2}:(2+\sqrt{2})i:1],\cdots$ という感じであろうか．つまり $\mathbb{Q}(E_1[4])=\mathbb{Q}(i,\sqrt{2})$ である．確かに $G(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ はアーベル群である．

Corollary 1.8: [4, p. 16, Corollary 5.6]

作用 $G(\bar{F}/F)\curvearrowright E[\mathfrak{a}^\infty]$ は単射

$$G(F(E[\mathfrak{a}^\infty])/F)\hookrightarrow\left(\varprojlim_n\mathcal{O}_K/\mathfrak{a}^n\right)^\times$$

を誘導する．特に全ての素数 p について

$$G(F(E[p^\infty])/F)\hookrightarrow(\mathcal{O}_K\otimes\mathbb{Z}_p)^\times.$$

Proof. Corollary 1.6 より, 任意の $n \geq 1$ について単射 $i_n : G(F(E[\mathfrak{a}^n])/F) \hookrightarrow (\mathcal{O}_K/\mathfrak{a}^n)^\times$ が存在する．また,

$$G(F(E[\mathfrak{a}^\infty])/F) = G(F(\cup_n E[\mathfrak{a}^n])/F) \simeq G(F(\varinjlim_n E[\mathfrak{a}^n])/F) \simeq \varprojlim_n G(F(E[\mathfrak{a}^n])/F)$$

であることから, 単射

$$f : \varprojlim_n G(F(E[\mathfrak{a}^n])/F) \to \left(\varprojlim_n \mathcal{O}_K/\mathfrak{a}^n\right)^\times$$

を構成すればよい．そして, $f((\varphi_n)_n) := (i_n(\varphi_n))_n$ と定義する．

(well-defined) $(i_n(\varphi_n))_n$ が単元であることを示せばよい．i_n の定義から $i_n(\varphi_n) \in (\mathcal{O}_K/\mathfrak{a}^n)^\times$ なので, ある $\alpha_n \in \mathcal{O}_K/\mathfrak{a}^n$ が存在して $i_n(\varphi_n)\alpha_n = 1$ が成り立つ．このときすぐ分かるように $(\alpha_n)_n \in \varprojlim_n \mathcal{O}_K/\mathfrak{a}^n$ であり，これは $(i_n(\varphi_n))_n$ の逆元である．ok.

(単射) 全ての n について $i_n(\varphi_n) = 1$ であるとすると, i_n は単射であったから $\varphi_n = 1$ である．従って $(\varphi_n)_n = 1$ となって ok.

最後の主張を示すには, $\varprojlim_n \mathcal{O}_K/\mathfrak{p}^n \simeq \mathcal{O}_K \otimes \mathbb{Z}_p$ を示せばよい.

$$\mathcal{O}_K \otimes \mathbb{Z}_p \simeq \mathcal{O}_K \otimes (\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}) \simeq \varprojlim_n (\mathcal{O}_K \otimes \mathbb{Z}/p^n\mathbb{Z}) \simeq \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n$$

より ok. ただし二つ目の同型は, $\mathcal{O}_K$ が有限生成 $\mathbb{Z}$ 加群よりテンソルと射影極限が交換可能, という事実から従う． □

Theorem 1.9: [4, p. 16, Theorem 5.7]

ℓ を素数, $F/\mathbb{Q}_\ell$ を有限次拡大とする．このとき以下が成り立つ.

- E; potentially good reduction.
- $\mathfrak{p} \leq \mathcal{O}_K$ が $(\mathfrak{p}, \ell) = 1$ を満たし, $n \in \mathbb{N}$ が $1 + \mathfrak{p}^n\mathcal{O}_{K.\mathfrak{p}}$ が torsion free とする．このとき $E/F(E[\mathfrak{p}^n])$ は $\mathfrak{p}$ を割らない素点で good reduction.

Proof. 証明には"Criterion of Néron-Ogg-Shafarevich"を用いる．(1) と (2) はほとんど同様の証明であるので, 少し簡単な (1) のみ証明の流れを述べる．Criterion of Néron-Ogg-Shafarevich とは, 素点 v に対する惰性群 $I_v \subset G(\bar{F}/F)$ の Tate 加群 $T_\ell(E)$ への作用が自明ならば E は v で good reduction という判定法である．これを少し一般化して, F として $F(E[p])$ とする．また, 特に $I_v = 0$ しかないことを示す.

Corollary 1.8 を用いることで

$$G(F(E[p^\infty])/F(E[p])) \hookrightarrow 1 + p\mathcal{O} \simeq \mathcal{O}_p \simeq \mathbb{Z}_p^2$$

が成り立つ．ガロア群は Krull 位相に関してコンパクト．従って $\mathbb{Z}_p^2$ の中でもコンパクトなので閉部分群である．$\mathbb{Z}_p^2$ の閉部分群は 0 か $\mathbb{Z}_p$ か $\mathbb{Z}_p^2$ に同型であることを考えると

$$G(F(E[p^\infty])/F(E[p])) \simeq \mathbb{Z}_p^d \quad (d = 1, 2)$$

が成り立つ．このとき連続全射

$$\mathcal{O}_{F(E[p])}^\times \twoheadrightarrow I$$

が存在するが, $\mathcal{O}_{F(E[p])}^\times \simeq (\text{finite}) \times \mathbb{Z}_\ell^r$ という形をしていること, $I \simeq \mathbb{Z}_p^i$ $(i \leq d)$ という形をしていることから $I = 0$ しかない．という流れ. □

$x = (x_\mathfrak{p})_\mathfrak{p} \in \mathbb{A}_K^\times$ に対して K の分数イデアルを

$$\mathfrak{I}(x) := \prod_{\mathfrak{p} \in M_K^0} \mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})}$$

と定義する．つまり有限素点部分を適切に束ねたものである．ただしイデール群 $\mathbb{A}_K^\times$ の定義からこれは有限積となることに注意する．このとき $\mathfrak{a} \leq K$ に対して $x\mathfrak{a} := \mathfrak{I}(x)\mathfrak{a}$ と定義する．また, ここからは楕円曲線 E/F は maximal order $\mathcal{O}_K$ ではなく, 一般の order $\mathcal{O}$ により虚数乗法をもつと仮定する.

Theorem 1.10: [3, p. 35, Theorem 2.4.4]

$\mathfrak{a} \leq K$ を, 同型 $\xi : \mathbb{C}/\mathfrak{a} \to E(\mathbb{C})$ を満たすものとして固定する. $\sigma \in \mathrm{Aut}_K(\mathbb{C})$ とし, $\sigma|_{K^{ab}} = [x, K^{ab}/K]$ となるような $x \in \mathbb{A}_K^\times$ を一つ固定する. このとき以下の図式を可換にするような同型 $\xi' : \mathbb{C}/x^{-1}\mathfrak{a} \to E^\sigma(\mathbb{C})$ が唯一存在する.

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "x^{-1}"'] & E(\mathbb{C}) \arrow[d, "\sigma"] \\ K/x^{-1}\mathfrak{a} \arrow[r, "\xi'"] & E^\sigma(\mathbb{C}) \end{tikzcd}$$

Corollary 1.11: [4, p. 18, Corollary 5.12]

H を K のヒルベルト類体, すなわち最大不分岐アーベル拡大とする. このとき以下が成り立つ.

- $K(j(E)) = H \subset F$.
- $j(E) \in \mathcal{O}_H$.

Proof. (1) Theorem 1.10 の記法を用いる. $\sigma \in \mathrm{Aut}_K(\mathbb{C})$ に対して σ が $j(E)$ を固定することと H を固定することが同値であればよい. 特にある $x \in \mathbb{A}_K^\times$ に対して $\sigma = [x, K^{ab}/K]$ のときを示せば十分である.

$$\begin{aligned} j(E) = j(E)^\sigma &\iff j(E) \simeq j(E^\sigma) \quad (\because j(E) \text{ は有理式で書ける}) \\ &\iff E \simeq E^\sigma \quad (\because \text{よく知られた事実}) \\ &\iff \mathbb{C}/\mathfrak{a} \simeq \mathbb{C}/x^{-1}\mathfrak{a} \quad (\because \text{Theorem1.10}) \\ &\overset{(!)}{\iff} {}^\exists\lambda \in K^\times \ \text{such that} \ x^{-1}\mathfrak{a} = \lambda\mathfrak{a} \quad (\because \mathbb{C}/L \simeq \mathbb{C}/L' \text{ならば格子は定数倍}) \\ &\iff x \in K^\times \left(\prod_{\mathfrak{p} \in M_K^0} \mathcal{O}_\mathfrak{p}^\times \prod_{\mathfrak{p} \in M_K^\infty} K_\mathfrak{p}^\times \right) \quad (\because x^{-1}\mathfrak{a} \text{ は } \mathfrak{a} \text{ の定数倍}) \\ &\iff [x, H/K] = 1 \quad (\because \text{大域類体論のイデール ver.}) \\ &\iff \sigma \text{は } H \text{ を固定} \end{aligned}$$

となり ok.

▌ 4 つ目の同値において, 本来 $\lambda \in \mathbb{C}^\times$ である. このとき $\lambda\mathfrak{a} = \mathfrak{I}(x)^{-1}\mathfrak{a} \leq K$ であるから, $\lambda \in K^\times$ でなければならない.

(2) H の任意の素点 $\mathfrak{p}$ に対して, $E/\mathcal{O}_{H,\mathfrak{p}}$ が potentially good reduction であることと $j(E) \in \mathcal{O}_{H,\mathfrak{p}}$ であることは同値である. ([5, VII, 5.4]) また, Theorem 1.9 より $E/\mathcal{O}_{H,\mathfrak{p}}$ は potentially good reduction であるから $j(E) \in \mathcal{O}_{H,\mathfrak{p}}$ が分かる. これは全ての H の素点で成り立つから $j(E) \in \prod_{\mathfrak{p} \in M_H^0} \mathcal{O}_{H,\mathfrak{p}} \cap H = \mathcal{O}_H$ である. □

Example 1.12

$F = \mathbb{Q}(i)$ に対して $E_1/K : y^2 = x^3 - x$ とする. このとき $K = F = \mathbb{Q}(i)$ であった. 以下で j 不変量と Hilbert 類体を計算すると $j(E) = 1728, H = K$ となることが分かる. 確かに $K(1728) = K = H$ となっている.

```
> P<x>:=PolynomialRing(Integers());
> K:=NumberField(x^2+1);
> H:=HilbertClassField(K);
> E:=EllipticCurve([-1,0]);
> j:=jInvariant(E);
> j;
1728
> H;
Number Field with defining polynomial x^2 + 1 over the Rational Field
```

Corollary 1.13: [4, p. 19, Corollary 5.13]

K のヒルベルト類体を H とする．このとき以下が成り立つ．

$$^{\exists}E'/H; \text{楕円曲線 such that } \mathcal{O}_K \text{により虚数乗法をもち}, \mathbb{C} \text{ 上の同型 } E \simeq E' \text{が成り立つ}.$$

Proof. まず $\mathcal{O}$ は格子だから $\mathbb{C}/\mathcal{O}$ は楕円曲線, すなわち $E'''(\mathbb{C}) \simeq \mathbb{C}/\mathcal{O}$ なる楕円曲線 $E'''/\mathbb{C}$ が存在する．このとき

$$\mathrm{End}_{\mathbb{C}}(E''') \simeq \{\alpha \in \mathbb{C} \mid \alpha\mathcal{O} \subset \mathcal{O}\} = \mathcal{O}$$

が成り立つ．また, Corollary 1.11 より $j(E''') \in H$ であって, [5, III, Proposition 1.4] より

$$^{\exists}E''/H; \text{楕円曲線 such that } j(E'') = j(E''')(\in H)$$

が成り立つ．よって $E'' \simeq_{\mathbb{C}} E'''$ より $\mathrm{End}_{\mathbb{C}}(E'') \simeq \mathrm{End}_{\mathbb{C}}(E''') \simeq \mathcal{O}$ を得る．あとは $\mathrm{End}_H(E'') = \mathcal{O}$ であれば, Proposition 1.3 を用いることで $\mathcal{O}_K$ により虚数乗法をもつ H 上の楕円曲線 E' が得られる．従って $\mathrm{End}_H(E'') = \mathrm{End}_{\mathbb{C}}(E'')$ を示す．それには Lemma 1.2 より $\iota(\phi) \in H$ を示せばよい．($\phi \in \mathrm{End}_{\mathbb{C}}(E'')$) 単射 $\iota : \mathrm{End}_{\mathbb{C}}(E'') \to \mathbb{C}$ に対して Corollary 1.11 より $\iota(\mathrm{End}_{\mathbb{C}}(E'')) = \mathcal{O} \subset K \subset K(j(E'')) = H$ となり ok. □

Proposition 1.14: [3, p. 34, Proposition 2.4.1]

$\mathfrak{a} \leq K$ とする．このとき同型

$$K/\mathfrak{a} \simeq \oplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}$$

が成り立つ．ここで和は全ての $\mathcal{O}_K$ の有限素点を渡り, $\mathfrak{a}_{\mathfrak{p}} := \mathfrak{a}\mathcal{O}_{\mathfrak{p}}$ である．

Proof. [6, Lemma 8.1(c)] 参照. □

$x \in \mathbb{A}_K^{\times}$ に対して等式 $\mathfrak{I}(x)_{\mathfrak{p}} := \mathfrak{I}(x)\mathcal{O}_{\mathfrak{p}} = x_{\mathfrak{p}}\mathcal{O}_{\mathfrak{p}}$ より,

$$(x\mathfrak{a})_{\mathfrak{p}} = \mathfrak{I}(x)\mathfrak{a}\mathcal{O}_{\mathfrak{p}} = x_{\mathfrak{p}}\mathfrak{a}\mathcal{O}_{\mathfrak{p}} = x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}$$

が成り立つので, Proposition 1.14 より同型

$$K/x\mathfrak{a} \simeq \oplus_{\mathfrak{p}} K_{\mathfrak{p}}/x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}}$$

を得る．このとき $K/\mathfrak{a}$ における x 倍写像を, 各 $\mathfrak{p}$ 成分での $x_{\mathfrak{p}}$ 倍写像, すなわち以下の図式が可換となることと定義する．

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[r, "x"] \arrow[d, "\simeq"] & K/x\mathfrak{a} \arrow[d, "\simeq"] \\
\oplus_{\mathfrak{p}} K_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \arrow[r] & \oplus_{\mathfrak{p}} K_{\mathfrak{p}}/x_{\mathfrak{p}}\mathfrak{a}_{\mathfrak{p}} \\
(t_{\mathfrak{p}})_{\mathfrak{p}} \arrow[r, mapsto] & (x_{\mathfrak{p}}t_{\mathfrak{p}})_{\mathfrak{p}}
\end{tikzcd}$$

Lemma 1.15: [3, p. 40, Lemma 2.5.5]

$\mathfrak{b} \leq \mathcal{O}, \mathfrak{a} \leq K$ とする．$x \in \mathbb{A}_K^{\times}$ は, K の全ての有限素点で $\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}}) = 0$ を満たすと仮定する．このとき写像

$$\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \to \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}; \alpha \mapsto x\alpha$$

が恒等写像であることと, $\mathfrak{b}$ を割る全ての素点 $\mathfrak{p}$ に対して $x_{\mathfrak{p}} \equiv 1 \bmod \mathfrak{b}_{\mathfrak{p}}$ であることは同値である．

Proof. Proposition 1.14 の同型を $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ に制限することにより, 可換図式

$$\begin{tikzcd}
\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\cdot x"] \arrow[d, "\simeq"] & \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \arrow[d, "\simeq"] \\
\oplus_{\mathfrak{p}} \mathfrak{b}_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \arrow[r, "(\cdot x_{\mathfrak{p}})_{\mathfrak{p}}"] & \oplus_{\mathfrak{p}} \mathfrak{b}_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}}
\end{tikzcd}$$

を得る．ただし下の写像が well-defined であることはチェックしなければならない．$[y_\mathfrak{p}]=[z_\mathfrak{p}]\in\mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}\simeq\mathfrak{a}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$ を取り，$[x_\mathfrak{p}y_\mathfrak{p}]=[x_\mathfrak{p}z_\mathfrak{p}]\in\mathfrak{a}_\mathfrak{p}/\mathfrak{b}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$ を示す．まず $y_\mathfrak{p},z_\mathfrak{p}$ の取り方から $y_\mathfrak{p}-z_\mathfrak{p}\in\mathfrak{b}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$ が成り立っている．$\mathrm{ord}_\mathfrak{p}(x_\mathfrak{p})=0$ より $x_\mathfrak{p}\in\mathcal{O}_\mathfrak{p}^\times$ であることから $x_\mathfrak{p}$ 倍写像は $\mathfrak{b}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$ において全単射である．以上より $x_\mathfrak{p}y_\mathfrak{p}-x_\mathfrak{p}z_\mathfrak{p}\in\mathfrak{b}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$，すなわち $[x_\mathfrak{p}y_\mathfrak{p}]=[x_\mathfrak{p}z_\mathfrak{p}]$ を得る．

さて，$\mathfrak{b}$ を割る全ての素点 $\mathfrak{p}$ に対して同値

$$x_\mathfrak{p}-1\in\mathfrak{b}_\mathfrak{p}\iff\mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}(x_\mathfrak{p}-1)\in\mathfrak{a}_\mathfrak{p}\iff{}^\forall t_\mathfrak{p}\in\mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p},\ t_\mathfrak{p}(x_\mathfrak{p}-1)\in\mathfrak{a}_\mathfrak{p}\iff{}^\forall t_\mathfrak{p}\in\mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p},t_\mathfrak{p}x_\mathfrak{p}=t_\mathfrak{p}\text{ in }\mathfrak{b}_\mathfrak{p}^{-1}\mathfrak{a}_\mathfrak{p}/\mathfrak{a}_\mathfrak{p}$$

が成り立つので，$x_\mathfrak{p}\equiv1\bmod\mathfrak{b}_\mathfrak{p}$ ならば全ての $\mathfrak{b}$ を割る素点 $\mathfrak{p}$ で $x_\mathfrak{p}$ 倍写像が恒等写像になり，可換図式から x 倍写像が恒等写像になる．逆も同様に分かる．□

Proposition 1.16: [3, p. 36, Proposition 2.5.1]

以下を満たすような準同型

$$\alpha_{E/F}:\mathbb{A}_F^\times\to K^\times$$

が存在する．$x\in\mathbb{A}_F^\times,y:=N_{F/K}(x)\in\mathbb{A}_K^\times$ に対して $\alpha=\alpha_{E/F}(x)\in K^\times$ は以下を満たす唯一の元である．

- $\alpha\mathcal{O}_K=\mathfrak{I}(y)$．
- $\mathfrak{a}\le K$ と同型 $\xi:\mathbb{C}/\mathfrak{a}\simeq E(\mathbb{C})$ に対して以下の可換図式が成り立つ．

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "\alpha y^{-1}"] & E(F^{ab}) \arrow[d, "{[x,F]}"] \\ K/\mathfrak{a} \arrow[r, "\xi"] & E(F^{ab}) \end{tikzcd}$$

Proof. $[x,F]$ を $\mathrm{Aut}(\mathbb{C}/F)$ に延長させたものの一つを σ，さらに $y:=N_{F/K}(x)\in\mathbb{A}_K^\times$ とする．このとき相互写像の性質から $\sigma|_{K^{ab}}=[y,K]$ が成り立つので Theorem 1.10 が適用でき，同型 $\xi':\mathbb{C}/y^{-1}\mathfrak{a}\simeq E^\sigma(\mathbb{C})$ と可換図式

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "y^{-1}"] & E(\mathbb{C}) \arrow[d, "\sigma"] \\ K/y^{-1}\mathfrak{a} \arrow[r, "\xi'"] & E(\mathbb{C}) \end{tikzcd}$$

が成り立つ．ただし E は F 上定義されているので $E^\sigma=E$ であることに注意する．従って

$$\mathbb{C}/y^{-1}\mathfrak{a}\xrightarrow{\xi'}E(\mathbb{C})\xrightarrow{\xi^{-1}}\mathbb{C}/\mathfrak{a}$$

は同型であり，$\xi^{-1}\circ\xi'=(\alpha\text{倍})$ となるような $\alpha\in\mathbb{C}^\times$ が存在し，さらに $\alpha\mathfrak{a}=\mathfrak{I}(y)\mathfrak{a}$ を満たす．従って $\alpha\mathcal{O}_K=\mathfrak{I}(y)$ が成り立ち，$\mathfrak{I}(y)\le K$ であるから $\alpha\in K$ である．これで前半が示された．

後半を示す．$\xi^{-1}\circ\xi'=(\alpha\text{倍})$ に右から y^{-1} 倍写像を，左から ξ を作用させると $\xi'\circ(y^{-1}\text{倍})=\xi\circ(\alpha y^{-1}\text{倍})$ を得る．これは目的の可換図式が成り立つことを表している．ただし ξ,ξ' の値域が $E(F^{ab})$ となっていること，σ と $[x,F]$ が等しいことはこれから示す．任意の $z=\alpha/\beta+\mathfrak{a}\in K/\mathfrak{a}$ に対して $\beta z\in\mathcal{O}_K/\mathfrak{a}$ であるから，$\xi(\beta z)\in E[\mathfrak{a}]$ である．従って Corollary 1.6 より

$$\xi(z)=\frac{1}{\beta}\xi(\beta z)\in\frac{1}{\beta}E[\mathfrak{a}]\subset E[\mathfrak{a}\mathfrak{b}]\subset E(F^{ab})$$

を得る．以上より $\xi(K/\mathfrak{a})\subset E(F^{ab})$ が分かる．さらに相互写像の性質から $\sigma|_{F^{ab}}=[x,F]$ であるからこれも ok.

α の一意性と $\alpha_{E/F}$ が準同型であることを示す．可換図式を満たす α' がもう一つ存在すると仮定する．このとき $(\alpha y^{-1}\text{倍})=(\alpha' y^{-1}\text{倍})$，すなわち $(\alpha y^{-1}\text{倍})\circ(y\alpha'^{-1}\text{倍})=\mathrm{id}$ が成り立ち，任意の $t\in K/\mathfrak{a}$ に対して

$$t=(\alpha y^{-1}\text{倍})\circ(y\alpha'^{-1}\text{倍})(t)=\alpha\alpha'^{-1}t$$

が成り立つ．従って $(1-\alpha\alpha'^{-1})t=0$，すなわち $(1-\alpha\alpha'^{-1})K\subset\mathfrak{a}$ が成り立つ．これが起こり得るのは $\alpha=\alpha'$ のときのみである．一意性が示された．準同型を示すには一意性から $\alpha(x_1)\alpha(x_2)$ が $\alpha(x_1x_2)$ の性質を満たすことを示せばよい．特に非

自明な可換図式の性質だけ見ることにする.

$$\begin{aligned}\xi\circ(\alpha(x_1)\alpha(x_2)(y_1y_2)^{-1}\text{倍}) &= \xi\circ(\alpha(x_1)y_1^{-1}\text{倍})\circ(\alpha(x_2)y_2^{-1}\text{倍})\\ &= [x_1,F]\circ\xi\circ(\alpha(x_2)y_2^{-1}\text{倍}) \quad (\because \alpha(x_1)\text{ の可換図式})\\ &= [x_1,F]\circ[x_2,F]\circ\xi \quad (\because \alpha(x_2)\text{ の可換図式})\\ &= [x_1x_2,F]\circ\xi \quad (\because \text{相互写像の準同型性})\end{aligned}$$

これは $\alpha(x_1)\alpha(x_2)$ が $\alpha(x_1x_2)$ の可換図式を満たすことを意味している. ok.

最後に α が $\mathfrak{a}$ と同型 ξ の取り方に依らないことを示す. $\mathfrak{a}'$ と同型 $\xi':\mathbb{C}/\mathfrak{a}'\simeq E(\mathbb{C})$ を別に取る. このとき $\xi^{-1}\circ\xi':\mathbb{C}/\mathfrak{a}'\simeq\mathbb{C}/\mathfrak{a}$ は同型だから, ある $\gamma\in\mathbb{C}^\times$ が存在して $\xi^{-1}\circ\xi'=(\gamma\text{倍})$ と $\mathfrak{a}'\gamma=\mathfrak{a}$ が成り立ち, 従って $\xi'(z)=\xi(\gamma z)$ が成り立つ. よって任意の $z\in K/\mathfrak{a}'$ に対して

$$[x,F](\xi'(z))=[x,F](\xi(\gamma z))=\xi(\alpha y^{-1}\gamma z)=\xi'(\alpha y^{-1}z)$$

が成り立つので ok. □

Theorem 1.17: [3, p. 38, Theorem 2.5.3]

Proposition 1.16 の記法の下, 以下の写像

$$\psi:\mathbb{A}_F^\times\to\mathbb{C}^\times; x\mapsto\alpha_{E/F}(x)N_{F/K}(x^{-1})_\infty$$

は Hecke 指標, すなわち $\psi(F^\times)=1$ を満たす連続準同型である.

Proof. $\mathfrak{a}\le K$ と同型 $\xi:\mathbb{C}/\mathfrak{a}\to E(\mathbb{C})$ を固定する.

(ψ: 準同型) $\alpha_{E/F}$ が準同型であることは既に Proposition 1.16 で示したので $N_{F/K}(\cdot)_\infty$ が準同型であることを示せばよい. $N_{F/K}:\mathbb{A}_F^\times\to\mathbb{A}_K^\times$ は準同型であって, その無限素点 part を取り出す写像も準同型であって, さらに $x\mapsto x^{-1}$ も準同型であることから, これら 3 つの写像の合成も準同型である. ok.

($\psi(F^\times)=1$) $\beta\in F, x_\beta=(\beta,\beta,\dots)\in\mathbb{A}_F^\times$ に対して $\psi(x_\beta)=1$, すなわち $\alpha_{E/F}(x_\beta)=N_{F/K}(x_\beta)_\infty$ を示せばよい. これを $\alpha_{E/F}(x_\beta)=N_{F/K}(\beta)=N_{F/K}(x_\beta)_\infty$ と, 2 ステップに分けて示す. まず大域類体論の相互写像の定義から $[x_\beta,F]=\mathrm{id}$ であって, 従って Proposition 1.16 の可換図式より $\alpha=\alpha_{E/F}(x_\beta)\in K^\times$ は「$\alpha N_{F/K}(x_\beta)^{-1}$ 倍写像は $K/\mathfrak{a}$ における恒等写像」かつ「$\alpha\mathcal{O}_K=N_{F/K}((x_\beta))\mathcal{O}_K=N_{F/K}(\beta)\mathcal{O}_K$」を満たす唯一の元である. そしてそれは $\alpha=N_{F/K}(\beta)$ に他ならない. 次に, イデール群のノルムの定義から

$$\left(N_{F/K}(x_\beta)\right)_\infty=\prod_{w|\infty}N_{F_w/K_\infty}(\beta)=\prod_{w\in M_L^\infty}N_{\mathbb{C}/\mathbb{C}}\beta^w=N_{F/K}(\beta)$$

となるので ok.

(ψ: 連続) $\mathbb{A}_F^\times,\mathbb{C}^\times$ は位相群なので, ある一点での連続性のみ示せばよい. さらにノルム写像, $x\mapsto x^{-1}$, 無限素点 part を取り出す写像は全て連続であるから $\alpha_{E/F}$ の一点での連続性のみ示せばよい. さらに $\alpha_{E/F}^{-1}(\{1\})=U$ となる閉部分群 $U\le\mathbb{A}_F^\times$ を見つければよい. 位相群において開ならば閉なので, $\alpha_{E/F}(U)=1$ となる開部分群 U を見つければよい.

$m\ge 3$ として相互写像 $[\cdot,F]$ による $G(F^{ab}/F(E[m]))$ の逆像を B_m とおく. まずガロア群は open であり, 相互写像は連続なので B_m は open である. さて

$$\begin{aligned}W_m &:= \left\{s\in\mathbb{A}_K^\times \mid {}^\forall\mathfrak{p}, s_\mathfrak{p}\in\mathcal{O}_\mathfrak{p}^\times,\ s_\mathfrak{p}\in 1+m\mathcal{O}_\mathfrak{p}\right\}\\ U_m &:= B_m\cap\left\{x\in\mathbb{A}_F^\times \mid N_{F/K}(x)\in W_m\right\}\end{aligned}$$

とおく. イデール群の位相の定義から W_m は open であり, $U_m=B_m\cap N_{F/K}^{-1}(W_m)$ よりこれも open. (明らかに $(1,1,\dots,)\in U_m$ なので $U\neq\varnothing$ である.) U_m の定義から $x\in U_m$ ならば $y:=N_{F/K}(x)\in W_m$ であり, $[x,F]|_{E[m]}=\mathrm{id}$ である. これを Proposition 1.16 において $\xi\mapsto\xi|_{m^{-1}\mathfrak{a}/\mathfrak{a}}$ として適用すると, 可換図式

$$\begin{tikzcd} m^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "\alpha y^{-1}"] & E[m] \arrow[d, "\mathrm{id}"] \\ m^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] & E[m] \end{tikzcd}$$

を得る. $y \in W_m$ であるから, Lemma 1.15 より y^{-1} は ($m^{-1}\mathfrak{a}/\mathfrak{a}$ 上の) 恒等写像であり, 従って全ての $t \in m^{-1}\mathfrak{a}/\mathfrak{a}$ に対して

$$\xi(t) = \xi(\alpha s^{-1}t) = \xi(\alpha t) \longrightarrow {}^{\forall}t \in m^{-1}\mathfrak{a},\ t - \alpha t \in \mathfrak{a} \longrightarrow m^{-1}\mathfrak{a}(1-\alpha) \subset \mathfrak{a}$$

が成り立つ. これが起こり得るのは $\alpha \equiv 1 \bmod m\mathcal{O}_K$ のときのみである. ここで, Proposition 1.16 と $y \in W_m$ であるということから $\alpha\mathcal{O} = \mathfrak{I}(y) = \mathcal{O}$ が成り立たなければならない. 従って $\alpha \in \mathcal{O}_K^{\times}$ かつ $m|(\alpha-1)$ が成り立つ. 特に $N_{K/\mathbb{Q}}(m)|N_{K/\mathbb{Q}}(\alpha-1)$ が成り立つ. Dirichlet の単数定理と $\alpha \in \mathcal{O}_K^{\times}$ より

$$\alpha \in \left\{\pm 1, \pm i, \pm\omega, \pm\omega^2\right\}$$

でなければならないが, 簡単な計算により $N_{K/\mathbb{Q}}(\alpha-1) < 9$ であることが分かる. m は 3 以上の自然数を任意に取ることができるので, $N_{K/\mathbb{Q}}(m)|N_{K/\mathbb{Q}}(\alpha-1)$ が成り立つためには $\alpha = 1$ でなければならない. ok. □

Definition 1.18: [3, p. 40, Definition 2.5.6]

Hecke 指標 ψ のコンダクターが $\mathfrak{f}$ であるとは, 以下の条件を満たす任意の finite idele $x = (x_{\mathfrak{P}}) \in \mathbb{A}_F^{\times}$ に対して $\psi(x) = 1$ であるような最大のイデアル $\mathfrak{f} \leq \mathcal{O}_F$ のことである.

$$\begin{cases} x_{\mathfrak{P}} \in \mathcal{O}_{F,\mathfrak{P}}^{\times} & (\mathfrak{P} \leq \mathcal{O}_F : \text{素イデアル}) \\ x_{\mathfrak{P}} \in 1 + \mathfrak{f}\mathcal{O}_{F,\mathfrak{P}} & (\mathfrak{P}|\mathfrak{f}) \end{cases}$$

Definition 1.19: [3, p. 40, Definition 2.5.7]

Hecke 指標 $\psi : \mathbb{A}_F^{\times}/F^{\times} \to \mathbb{C}^{\times}$ のコンダクターを $\mathfrak{f}$ とする. このとき $\mathfrak{f}$ と互いに素な F の分数イデアル群 $I_F(\mathfrak{f})$ の指標を

$$I_F(\mathfrak{f}) \to \mathbb{C}^{\times}; \mathfrak{P} \mapsto \psi(1, \ldots, \pi, 1, \ldots,)$$

と定義する. ここで $\mathfrak{P}$ は素イデアルであり, $\pi \in \mathcal{O}_{F,\mathfrak{P}}$ は uniformizer である. これを $\mathfrak{f}$ と互いに素なイデアル全体に乗法的に延長したものも改めて ψ と書く.

Example 1.20

Magma で Hecke 指標 (Grossencharacter) を定義することはできる. ただし定義域は $\mathbb{A}_F^{\times}/F^{\times}$ ではなく, 同型な $I_F(\mathfrak{f})/P_{F,1}(\mathfrak{f})$ という群になっている.

```
> E:=EllipticCurve([-1,0]);
> G:=Grossencharacter(E);
> G;
Grossencharacter G of type [[ 1, 0 ]] for Hecke-Dirichlet pair (1,$.1^3) with
modulus of norm 8 over Quadratic Field with defining polynomial x^2 + 1 over the
Rational Field
```

Hecke 指標 G は type $(1,0)$, すなわち $G((\alpha)) = u\alpha^i\bar{\alpha}^j$ $(u \in \mathcal{O}_K^{\times})$ と表したときに $(i,j) = (1,0)$ である. さらにモジュラス $\mathfrak{f}$ のノルムは 8, すなわち $(1+i)^4\mathcal{O}_K$ であることが分かる.

Example 1.21

Hecke 指標のコンダクターも Magma で計算することができる.

```
> E:=EllipticCurve([-1,0]);
> G:=Grossencharacter(E);
> Conductor(G);
Ideal
Two element generators:
    8
    2*$.2 - 2
[]
```

「\$.2」というのは未だ定義されてない記号を表している．ここでは虚数単位 i である．この場合は $\mathfrak{f}=(8,2i-2)=(2i-2)$ である．

Proposition 1.22: [3, p. 41, Proposition 2.5.9]

$\mathfrak{P}\leq F$ を素イデアルとする．このとき以下が成り立つ．

$$\psi(\mathcal{O}_{F,\mathfrak{P}}^{\times})=1 \iff E/F : \text{good reduction at } \mathfrak{P}$$

Proof. Néron-Ogg-Shafarevich を用いるので証明は省略する． □

Corollary 1.23: [3, p. 41, Corollary 2.5.10]

$\mathfrak{f}$ を Hecke 指標 $\psi_{E/F}$ のコンダクターとする．素イデアル $\mathfrak{P}\leq\mathcal{O}_F$ が $\mathfrak{P}\not|\mathfrak{f}$ を満たすならば E/F は $\mathfrak{P}$ で good reduction である．

Proof. Propositon 1.22 より，$x=(1,\dots,1,u_{\mathfrak{P}},1,\dots)\in\mathbb{A}_F^{\times}$ $(u_{\mathfrak{P}}\in\mathcal{O}_{F,\mathfrak{P}}^{\times})$ に対して $\psi(x)=1$ を示せばよい．コンダクターの定義から $x\in\mathfrak{f}$ であるので $\psi(x)=1$ である．ok. □

Proposition 1.24: [3, p. 41, Proposirion 2.5.11]

$\mathfrak{f}$ を Hecke 指標 $\psi_{E/F}$ のコンダクター，F の素イデアル $\mathfrak{P}$ は $(\mathfrak{P},\mathfrak{f})=1$ を満たすとする．このとき同種 $\widetilde{[\psi(\mathfrak{P})]}$ は Frobenius 準同型

$$\varphi_q:\tilde{E}\to\tilde{E};(x,y)\mapsto(x^q,y^q)$$

に一致する．ただし $q=N_{F/\mathbb{Q}}(\mathfrak{P})$ である．

Proof. $x=(1,\dots,1,\pi,1,\dots)\in\mathbb{A}_F^{\times}$ を取る．ただし $\pi\in\mathcal{O}_{F,\mathfrak{P}}$ を uniformizer とする．$N_{F/K}(x)_\infty=1$ なので $\psi(\mathfrak{P})=\alpha_{F/K}(x)=:\alpha$ である．Propositin 1.16 より $\alpha\mathcal{O}_K=\mathfrak{I}(N_{F/K}(x))=N_{F/K}(\mathfrak{P})$ であるので $\alpha\in\mathcal{O}_K\simeq\mathrm{End}_F(E)$ である．あとは $\widetilde{[\psi(\mathfrak{P})]}=\varphi_q$，すなわち $\widetilde{[\alpha]}=\varphi_q$ を示せばよい．核が有限でない同種は零写像しかないことを考えると $\mathrm{Ker}(\widetilde{[\alpha]}-\varphi_q)$ が任意に大きくできることを示せばよい．特に mild な仮定を満たす $m\in\mathbb{Z}$ に対して $E[m]\subset\mathrm{Ker}(\widetilde{[\alpha]}-\varphi_q)$ を示し，また，上手く体 L を取ることで $E(L)[m]\hookrightarrow\tilde{E}(k_L)$ と出来るので，そのような体 L を上手く取り $\tilde{E}(k_L)\subset\mathrm{Ker}(\widetilde{[\alpha]}-\varphi_q)$ を示せばよい．

m を $\mathfrak{P}$ と互いに素な整数，$P\in E[m]$ とする．Theorem 1.17 の証明で用いた可換図式と，Lemma 1.15 の証明で用いた図式を用いることで，可換図式

$$\begin{tikzcd}
\oplus_{\mathfrak{p}}(m)_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \arrow[r, "\simeq"] \arrow[d, "\alpha N_{F/K}(x)_{\mathfrak{p}}^{-1}"] & (m)^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "\alpha N_{F/K}(x)^{-1}"] & E[m] \arrow[d, "{[x,F]}"] \\
\oplus_{\mathfrak{p}}(m)_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \arrow[r, "\simeq"] & (m)^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] & E[m]
\end{tikzcd}$$

を得る．ただし $\mathfrak{p}\leq\mathcal{O}_K$ は $\mathfrak{P}\leq\mathcal{O}_F$ の下にある素イデアルを渡る．ここで，可換図式の左上から左下の写像の $N_{F/K}(x)_{\mathfrak{p}}^{-1}$ は，$(m,\mathfrak{P})=1$ より恒等写像でなければならない．従って α 倍だけが残り，真ん中上から真ん中下の写像も α 倍写像になる．以上より可換図式の右の四角形から

$$[\alpha]P=[x,F]P$$

を得る．大域類体論の相互写像の定義から，不分岐拡大 $F(E[m])/F$ の自己準同型 $[x,F]$ の reduction(すなわち対応する剰余体における準同型) は $\mathfrak{P}$-Frobenius に等しい．従って

$$\widetilde{[\alpha]}\tilde{P}=\widetilde{[\alpha]P}=\widetilde{[x,F]P}=\varphi_q(\tilde{P})$$

を得る．ここで，reduction は $\mathfrak{P}$ の上にある $F(E[m])$ の素点で行っている．Corollary 1.23 より E は $\mathfrak{P}$ で，さらにその上に

ある $F(E[m])$ の素点でも good reduction となるので

$$E[m] \hookrightarrow \tilde{E}(k_{F(E[m])}) \hookrightarrow \mathrm{Ker}(\widetilde{[\alpha]} - \varphi_q)$$

を得る．ok. $\square$

Proposition 1.25: [3, p. 47, Proposition 2.6.5]

$\mathfrak{O} \leq \mathcal{O}_F$ を有限素点とする．このとき以下の条件を満たす楕円曲線 E'/F が存在する．

1. $E \simeq_{\bar{F}} E'$.
2. E' は $\mathfrak{O}$ で good reduction.

Proof. Proposition 1.22 より，$\psi_{E'}(\mathcal{O}_{F,\mathfrak{O}}^\times) = 1$ を満たす楕円曲線 E' で $\bar{F}$ 上 E と同型なものを構成すればよい．E に付随する Hecke 指標 ψ_E を用いて，指標

$$\chi : \mathbb{A}_F^\times / F^\times \longrightarrow \mathcal{O}_{F,\mathfrak{O}}^\times \xrightarrow{\psi_E} \mathcal{O}_K^\times$$

を考える．ただし最初の写像は $\mathfrak{O}$ 成分への射影である．また，$\psi_E(\mathcal{O}_{F,\mathfrak{O}}^\times) \subset \mathcal{O}_K^\times$ であることは Proposition 1.16 より従う．

> $x \in \mathcal{O}_{F,\mathfrak{O}}^\times, y := N_{F/K}(x) \in \mathcal{O}_{K,\mathfrak{o}}^\times$ とする．ただし $\mathfrak{o}$ は $\mathfrak{O}$ の下にある K の素イデアルである．このとき $\psi_E(x) = \alpha_{E/F}(x) N_{F/K}(x^{-1})_\infty$ であって当然 y^{-1} の無限素点部分は 1 なので $\psi_E(x) = \alpha_{E/F}(x)$ である．また，$\alpha_{E/F}(x)$ は Proposition 1.16 より $\alpha_{E/F}(x)\mathcal{O}_K = \mathfrak{I}(y)$ を満たすが，$v_{\mathfrak{o}}(y) = 0$ なので $\mathfrak{I}(y) = \mathcal{O}_K$ である．従って $\alpha_{E/F}(x) \in \mathcal{O}_K^\times$.

大域類体論アデール ver. の相互写像 $(\ ,F) : \mathbb{A}_F^\times/F^\times \twoheadrightarrow G(F^{ab}/F)$ を用いて準同型 $\bar{\chi}$ を以下のように定義する．

$$\bar{\chi} : G(\bar{F}/F) \xrightarrow{\mathrm{res}} G(F^{ab}/F) \longrightarrow \mathbb{A}_F^\times/F^\times \longrightarrow \mathcal{O}_{F,\mathfrak{O}}^\times \xrightarrow{\psi_E} \mathcal{O}_K^\times$$

ただし二つ目の写像は $\sigma \in G(F^{ab}/F)$ に対して，$(\ ,F)$ による σ の引き戻しの一つ $x \in \mathbb{A}_F^\times/F^\times$ を対応させる写像とする．

> 上の写像を用いた準同型 $G(F^{ab}/F) \to \mathbb{A}_F^\times/F^\times \to \mathcal{O}_{F,\mathcal{O}}^\times$ が well-defined であることを示す．$(x,F) = (y,F)$ ならば $x_{\mathfrak{O}} = y_{\mathfrak{O}}$ を示せばよい．特に準同型性から $(x,F) = \mathrm{id}$ ならば $x_{\mathfrak{O}} = 1$ を示せばよい．大域類体論と局所類体論の相互写像の整合性から，可換図式
>
> $$\begin{tikzcd} F_{\mathfrak{O}}^\times \arrow[r, hook, "(\ ,F_{\mathfrak{O}})"] \arrow[d] & G(F_{\mathfrak{O}}^{ab}/F_{\mathfrak{O}}) \arrow[d, hook] \\ \mathbb{A}_F^\times/F^\times \arrow[r, "(\ ,F)"] & G(F^{ab}/F) \end{tikzcd} \qquad \begin{tikzcd} x_{\mathfrak{O}} \arrow[r, mapsto] \arrow[d, mapsto] & (x_{\mathfrak{O}}, F_{\mathfrak{O}}) \arrow[d, mapsto] \\ x \arrow[r, mapsto] & (x,F) \end{tikzcd}$$
>
> が成り立っていた．よって $(x,F) = \mathrm{id}$ であること，上と右の写像が単射であることから $x_{\mathfrak{O}} = 1$ でなければならない．

目標は楕円曲線 E'/F を構成して $\chi(\cdot)^{-1}\psi_E = \psi_{E'}$ を示すことである．そうすれば $\psi_{E'}(\mathcal{O}_{F,\mathfrak{O}}^\times) = \chi(\mathcal{O}_{F,\mathfrak{O}}^\times)^{-1}\psi_E(\mathcal{O}_{F,\mathfrak{O}}^\times) = 1$ となって ok. ($\mathcal{O}_{F,\mathfrak{O}}^\times$ において $\psi_E = \chi$ であることに注意)

目標を示す前に準備をする．$\omega := \#\mathcal{O}_K^\times$ とする．このとき $\mathcal{O}_K^\times = \mu_\omega$ であって，

$$\mathrm{Hom}(G(\bar{F}/F), \mathcal{O}_K^\times) = H^1(G(\bar{F}/F), \mu_\omega) \simeq F^\times/(F^\times)^\omega$$

が成り立つ．

> 最初の等式は作用 $G(\bar{F}/F) \curvearrowright \mathcal{O}_K^\times; \sigma \cdot x := x^\sigma$ が自明であることから従う．二つ目の同型はアーベル群の完全列
>
> $$1 \longrightarrow \mu_\omega \longrightarrow \bar{F}^\times \xrightarrow{\omega 乗} \bar{F}^\times \longrightarrow 1$$
>
> に対してコホモロジー長完全列を取って
>
> $$1 \longrightarrow \mu_\omega(F) \longrightarrow F^\times \xrightarrow{\omega 乗} F^\times \xrightarrow{\delta} H^1(G(\bar{F}/F), \mu_\omega) \longrightarrow H^1(G(\bar{F}/F), \bar{F}^\times) \longrightarrow \cdots$$

を得るが, Hilbert 90 より $H^1(G(\bar{F}/F), \bar{F}^\times) = 1$ なので上の完全列は

$$1 \longrightarrow \mu_\omega(F) \longrightarrow F^\times \xrightarrow{\omega乗} F^\times \xrightarrow{\delta} H^1(G(F^{ab}/F), \mu_\omega) \longrightarrow 1$$

となって,

$$H^1(G(F^{ab}/F), \mu_\omega) = \operatorname{Im}\delta \simeq F^\times/\operatorname{Ker}\delta = F^\times/\operatorname{Im}\omega乗 = F^\times/(F^\times)^\omega$$

となることより従う.

よって今構成した準同型 $\bar{\chi} \in \operatorname{Hom}(G(\bar{F}/F), \mathcal{O}_K^\times)$ に対して $\bar{\chi}^\omega = \mathrm{id}$ in $H^1(G(\bar{F}/F), \mu_\omega)$ である. よってある $d \in \mu_\omega$ が存在して $\bar{\chi}(\sigma)^\omega = d^\sigma/d \quad ({}^\forall\sigma \in G(\bar{F}/F))$ と書ける. 言い換えれば, ある $d \in F^\times$ が存在して, 全ての $\sigma \in G(\bar{F}/F)$ に対して

$$\tilde{\chi}(\sigma) = (d^{1/\omega})^\sigma/d^{1/\omega}$$

が成り立つ. 今楕円曲線は代数体上定義されているとしているので, model を上手く取って $E : y^2 = x^3 + ax + b \ (a, b \in F)$ という式で表されるとしてよい. このとき (ω に依存した) 楕円曲線 E' を

$$E' = \begin{cases} y^2 = x^3 + d^2ax + d^3b & (\omega = 2) \\ y^2 = x^3 + dax & (\omega = 4) \\ y^2 = x^3 + db & (\omega = 6) \end{cases}$$

とすると, $F(d^{1/\omega})$ 上の同型写像 $\phi : E \to E'$ が以下で与えられる.

$$\phi : (x, y) \mapsto \begin{cases} (dx, d^{3/2}y) & (\omega = 2) \\ (d^{1/2}x, d^{3/4}y) & (\omega = 4) \\ (d^{1/3}x, d^{1/2}y) & (\omega = 6) \end{cases}$$

任意の $\sigma \in G(\bar{F}/F)$ に対して $\bar{\chi}(\sigma) \in \mathcal{O}_K^\times$ なので, $[\bar{\chi}(\sigma)] \in \operatorname{End}(E)$ は同型写像である. さらに同型 ϕ を通して E' の同型写像でもある. 実際には $[\bar{\chi}(\sigma)](x, y) = (\bar{\chi}(\sigma)^2x, \bar{\chi}(\sigma)^3y)$ という同型写像になっている. (cf. [5, p. 104, Corollary 10.2]) この表現から簡単に

$$[\bar{\chi}(\sigma)^{-1}] \circ \phi \circ \sigma(P) = \sigma \circ \phi(P) \quad ({}^\forall P \in E)$$

となることが分かる.

他は同様なので $\omega = 2$ の場合のみ計算する.

$$\begin{aligned} [\bar{\chi}(\sigma)^{-1}] \circ \phi \circ \sigma(x, y) &= [\bar{\chi}(\sigma)^{-1}] \circ \phi(x^\sigma.y^\sigma) = [\bar{\chi}(\sigma)^{-1}](dx^\sigma, d^{3/2}y^\sigma) = (\bar{\chi}(\sigma)^{-2}dx^\sigma, \bar{\chi}(\sigma)^{-3}d^{3/2}y^\sigma) \\ &= (d(d^{-1})^\sigma dx^\sigma, d^{3/2}(d^{-3/2})^\sigma d^{3/2}y^\sigma) = (dx^\sigma, -d^{3/2}y^\sigma) \\ \sigma \circ \phi(x, y) &= \sigma(dx, d^{3/2}y) = (d^\sigma x^\sigma, (d^{3/2})^\sigma y^\sigma) = (dx^\sigma, -d^{3/2}y^\sigma) \end{aligned}$$

あとは $\chi^{-1}\psi_{E/F} = \psi_{E'/F}$ であることを見ればよい. $\psi_{E/F}(x) = \alpha_{E/F}(x)N_{F/K}(x^{-1})_\infty$ であったから $\chi(x)^{-1}\alpha_{E/F}(x)N_{F/K}(x^{-1})_\infty = \alpha_{E'/F}(x)N_{F/K}(x^{-1})_\infty$ を, すなわち $\chi(x)^{-1}\alpha_{E/F}(x) = \alpha_{E'/F}(x)$ を示せばよい. 特に α の一意性から, $\chi(\cdot)^{-1}\alpha_{E/F}$ が $\alpha_{E'/F}$ の二つの性質を満たすことを示せばよい. まず一つ目の条件を見る. 任意の $x \in \mathbb{A}_F^\times/F^\times, y := N_{F/K}(x) \in \mathbb{A}_K^\times/K^\times$ に対して, $\chi(x)^{-1}\alpha_{E/F}(x)\mathcal{O}_K = \mathfrak{I}(y)$ が成り立つことを確認すればよい. $\chi(x)^{-1} \in \mathcal{O}_K^\times$ で生成されるイデアルは 1 なので $\alpha_{E'/F}(x)\mathcal{O}_K = \mathfrak{I}(y)$ が成り立つことを見ればよいが, これは $\alpha_{E'/F}$ の性質そのものである. 二つ目の条件を見る. ある $\mathfrak{b} \leq K$ と同型 $\xi : \mathbb{C}/\mathfrak{b} \simeq E'(\mathbb{C})$ が存在して以下のような可換図式が成り立てばよい.

$$\begin{tikzcd} K/\mathfrak{b} \arrow[r, "\xi"] \arrow[d, "\chi(x)^{-1}\alpha_{E/F}(x)y"'] & E'(F^{ab}) \arrow[d, "{[x,F]}"] \\ K/\mathfrak{b} \arrow[r, "\xi"] & E'(F^{ab}) \end{tikzcd}$$

実際, 同型 $\xi' : \mathbb{C}/\mathfrak{a} \simeq E(\mathbb{C})$ に対して

$$\begin{tikzcd}
K/\mathfrak{a} \arrow[r, "\xi'"] \arrow[d, "\alpha_{E/F}(x)y"'] & E(F^{ab}) \arrow[r, "\phi"] \arrow[d, "{[x,F]}"'] & E'(F^{ab}) \arrow[dd, "\sigma:=[x,F]"'] \\
K/\mathfrak{a} \arrow[r, "\xi'"] \arrow[d, "\chi(x)^{-1}"'] & E(F^{ab}) \arrow[d, "\phi"'] & \\
K/\mathfrak{a} \arrow[r] & E'(F^{ab}) \arrow[r, "{[\bar{\chi}(\sigma)^{-1}]}"] & E'(F^{ab})
\end{tikzcd}$$

という図式が成り立ち, 左上の四角形は $\alpha_{E/F}$ の性質から可換, 右の四角形は上で示したことから可換である. 左下の図式について, 下の写像を $\phi \circ \xi' \circ (\chi(x)$ 倍) と定めれば可換となって ok. □

Remark 1.26

Proposition 1.25 の証明において $\psi_{E'} = \chi^{-1}\psi_E$ という等式を示していた. 楕円曲線 E と E' はいわゆる"ツイスト"の関係, すなわち射

$$E : y^2 = x^3 + x \to E' : y^2 = x^3 + dx; (x, y) \mapsto (d^{1/2}x, d^{3/4}y) \quad (d \in \mathbb{Z})$$

は $\mathbb{Q}$ 上同型ではないが, $\mathbb{Q}(d^{1/4})$ 上の同型である. このとき $K = \mathbb{Q}(i)$ に対して $\chi \in H^1(G(\bar{K}/K), \mathrm{Aut}(E))$ が以下のように定まる.

$$\chi(\sigma) := [(d^{1/4})^\sigma / d^{1/4}]$$

このとき χ は準同型 $\mathbb{A}_K^\times \to \mathbb{C}^\times$ を誘導し, $\psi_{E'} = \chi^{-1}\psi_E$ が成り立つことを示していた.

要するにツイストされた楕円曲線の Hecke 指標は, ツイストする前の楕円曲線の Hecke 指標を用いて explicit に書けるということである. さらに ψ_E はツイストする前の楕円曲線の Hecke 指標で $d \in \mathbb{Z}$ に依存しないので, 代わりに χ に d の情報が全て詰まっている. このようにツイストされた楕円曲線の Hecke 指標は特定のパラメータに依存した指標と依存しない指標に分解することができる. (筆者の第一論文はこの手法と p 進 L 関数の理論を用いて $L(\psi_{E_d/\mathbb{Q}}, 1) = L(\chi\psi_{E_1/\mathbb{Q}}, 1)$ の計算を Hecke L 関数のある特殊値 $L(\psi_{E_1/\mathbb{Q}}^{2k-1}, k)$ の計算に帰着させた.)

最後に, このツイストされた楕円曲線の Hecke 指標をツイストする前の楕円曲線の Hecke 指標を用いて記述する方法は, Silverman Advanced の演習問題 [6, p.183, Exercise 2.25] に載っている. (上の命題の証明により, その演習問題は解けたことになる.)

Corollary 1.27: [3, p. 42, Corollary 2.6.1]

E/K を $\mathcal{O}_K$ により虚数乗法をもつ楕円曲線, すなわち $F = K$ とする. ψ を E/K に付随する Hecke 指標, $\mathfrak{f}$ をそのコンダクターとする. このとき以下が成り立つ.

1. reduction map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f})^\times$ は単射である.
2. E は K の全ての有限素点で good reduction とはならない.

Proof. (1) $1 \neq u \in \mathcal{O}_K^\times$ に対して $u \not\equiv 1 \bmod \mathfrak{f}$ を示せばよい. $x \in \mathbb{A}_K^\times$ を, 無限素点部分が 1, 全ての有限素点部分が u であるものとする. コンダクターの定義から $\psi(x) = u \neq 1$ を示せば $u \not\equiv 1 \bmod \mathfrak{f}$ が導かれる. $\psi(x)$ の定義から

$$\begin{aligned}
\psi(x) &= \psi(u)^{-1}\psi(x) \quad (\because \psi(K^\times) = 1) \\
&= \psi(u^{-1}x) \quad (\because \psi : \text{準同型}) \\
&= \alpha_{E/K}(u^{-1}x) N_{K/K}(ux^{-1})_\infty \quad (\because \text{Theorem 1.17}) \\
&= \alpha_{E/K}(u^{-1}x) u \quad (\because x \text{ の取り方})
\end{aligned}$$

となる. 従ってあとは $\alpha_{E/K}(u^{-1}x) = 1$ を示せばよい. $u^{-1}x = (u^{-1}, 1, 1, \dots)$ であることから $[u^{-1}x, K] = 1$ である. このとき Proposition 1.16 の可換図式から $\alpha_{E/K}(u^{-1}x)$ 倍写像は $K/\mathfrak{a}$ 上で恒等写像となって ok.

大域類体論の同型定理より, (有限とは限らない)K の任意の素点 $\mathfrak{p}$ に対して

$$\begin{tikzcd} K_{\mathfrak{p}}^{\times} \arrow[r, "{[\ ,K_{\mathfrak{p}}]}"] \arrow[d, "*"] & G(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}}) \arrow[d, hook] \\ \mathbb{A}_K^{\times}/K^{\times} \arrow[r, "{[\ ,K]}"] & G(K^{ab}/K) \end{tikzcd}$$

が可換図式となる連続準同型 $[\ ,K] : \mathbb{A}_K^{\times}/K^{\times} \to G(K^{ab}/K)$ が存在する．ここで $* : K_{\mathfrak{p}}^{\times} \hookrightarrow \mathbb{A}_K^{\times} \twoheadrightarrow \mathbb{A}_K^{\times}/K^{\times}$ で, $[\ ,K_{\mathfrak{p}}]$ は局所類体論の相互写像である．K を虚二次体, $\mathfrak{p} = \infty$ とすると

$$\begin{tikzcd} \mathbb{C}^{\times} \arrow[r, "{[\ ,K_{\mathfrak{p}}]}"] \arrow[d, "*"] & \{1\} \arrow[d, hook] \\ \mathbb{A}_K^{\times}/K^{\times} \arrow[r, "{[\ ,K]}"] & G(K^{ab}/K) \end{tikzcd} \qquad \begin{tikzcd} u^{-1} \arrow[r, mapsto] \arrow[d, mapsto] & 1 \arrow[d, mapsto] \\ (u^{-1}, 1, \ldots) \arrow[r, mapsto] & {[u^{-1}x, K]} \end{tikzcd}$$

となり $[u^{-1}x, K] = 1$ を得る．また, $\alpha := \alpha_{E/K}(u^{-1}x) = 1$ となることを示す．可換図式から, 任意の $x \in K/\mathfrak{a}$ に対して

$$[u^{-1}x, K] \circ \xi(x) = \xi(\alpha x)$$

が成り立っているが, $[u^{-1}x, K] = 1$ であるから $\xi(x) = \xi(\alpha x)$, すなわち $(\alpha - 1)\xi(x) = 0$ が成り立つ．x は任意なので $\alpha = 1$ でなければならない．

(2) E/K は全ての有限素点 $\mathfrak{p}$ で good reduction であると仮定して矛盾を導く．以下のようなイデールの列 $(a_i)_{i \in \mathbb{N}} \subset \mathbb{A}_K^{\times}$ を考える．

$$a_1 = (1, u, 1, 1, \ldots,), \quad a_2 = (1, u, u, 1, 1, \ldots), \quad a_3 = (1, u, u, u, 1, 1, \ldots), \ldots$$

この点列は明らかに (1) で取った $x \in \mathbb{A}_K^{\times}$ に収束する．今仮定から Propositon 1.22 より $\psi(a_i) = 1$ $({}^{\forall}i)$ でなければならない．ψ は連続準同型であったからその収束先に対しても $\psi(x) = 1$ となる．これは (1) の証明中に示したことに矛盾． □

Corollary 1.28: [3, p. 43, Corollary 2.6.2]

E/K を楕円曲線, $\mathfrak{p} \leq \mathcal{O}_K$ を有限素点とする．reduction map $\mathcal{O}_K^{\times} \to (\mathcal{O}_K/\mathfrak{p})^{\times}$ が全射ではないと仮定する．このとき $E[\mathfrak{p}] \not\subset E(K)$ が成り立つ．

Proof. 対偶を示す．すなわち $E[\mathfrak{p}] \subset E(K)$ と仮定して reduction map $\mathcal{O}_K^{\times} \to (\mathcal{O}_K/\mathfrak{p})^{\times}$ が全射であることを示す．任意に $z \in (\mathcal{O}_K/\mathfrak{p})^{\times}$ を一つ取る．このとき $\alpha \bmod \mathfrak{p} = z$ となる $\alpha \in \mathcal{O}_K^{\times}$ を見つければよい．まず $u \in \mathcal{O}_{\mathfrak{p}}^{\times}$ で $u \bmod \mathfrak{p}\mathcal{O}_{\mathfrak{p}} = z$ となるものをとる．このような u が取れるのは Hensel の補題による．また, $x \in \mathbb{A}_K^{\times}$ を, $\mathfrak{p}$ 成分のみ u で他は 1 というイデールとする．Proposition 1.16(2), (1) を用いると, $[x, K]|_{E[\mathfrak{p}]}$ の $E[\mathfrak{p}]$ への作用は, $K/\mathfrak{p}$ において $\alpha(x)x^{-1}$ 倍写像になる．しかし仮定より $[x, K]|_{E[\mathfrak{p}]} = \mathrm{id}$ であるから, $\alpha(x)x^{-1}$ 倍写像は恒等写像である．Lemma 1.15 より $(\alpha(x)x^{-1})_{\mathfrak{p}} \equiv 1 \bmod \mathfrak{p}$ が成り立つ．従って

$$\alpha(x) \equiv x_{\mathfrak{p}} \equiv u \equiv z \bmod \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$$

を得る． $\alpha(x), z \in \mathcal{O}_K$ であるからこの合同式は $\mathrm{mod} \mathfrak{p}$ で成り立たなければならない． よって目的の条件を満たす $\alpha(x) \in \mathcal{O}_K^{\times}$ が取れた． □

Theorem 1.29: [3, p. 44, Theorem 2.6.4]

E/K を楕円曲線, ψ を E/K に付随する Hecke 指標, $\mathfrak{f}$ をそのコンダクターとする．また, $\mathfrak{b} \leq \mathcal{O}_K$ を $(\mathfrak{b}, \mathfrak{f}) = 1$ となるイデアル, $\mathfrak{p} \leq \mathcal{O}_K$ を $\mathfrak{p} \nmid \mathfrak{f}$ を満たす素イデアルとする．このとき以下が成り立つ．

1. $E[\mathfrak{b}\mathfrak{f}] \subset E(K(\mathfrak{b}\mathfrak{f}))$.
2. Corollary 1.8 の単射 $G(K(E[\mathfrak{b}])/K) \to (\mathcal{O}/\mathfrak{b})^{\times}$ は同型.
3. $\mathfrak{c}|\mathfrak{b}$ ならば自然な写像 $G(K(\mathfrak{b}\mathfrak{f})/K(\mathfrak{c}\mathfrak{f})) \to G(K(E[\mathfrak{b}])/K(E[\mathfrak{c}]))$ は同型.
4. 拡大 $K(E[\mathfrak{p}^n\mathfrak{b}])/K(E[\mathfrak{b}])$ は $\mathfrak{p}$ の上にある素点について総分岐.

5. reduction map $\mathcal{O}_K^\times \to (\mathcal{O}/\mathfrak{b})^\times$ が単射ならば $K(E[\mathfrak{p}^n\mathfrak{b}])/K(E[\mathfrak{b}])$ は $\mathfrak{p}$-外不分岐.

Proof. 類体論をゴリゴリに使う割に証明長すぎるので省略. □

1.1 The L-series Attached to a CM Elliptic Curve

よく私は「CM 楕円曲線の L 関数は Hecke L 関数である」と言う. ここではその事実を (いくつかの事実を認め) 証明することにする. 楕円曲線の L 関数は有理点の個数から定まる L 関数であり, 非常に計算が難しい. 実際例えば $\mathbb{C}$ 全体に解析接続されるかは未解決問題である. しかし Hecke L 関数の解析接続問題が完了していることから CM 楕円曲線の L 関数は $\mathbb{C}$ 全体に解析接続される. さらに Wiles の結果から $\mathbb{Q}$ 上の楕円曲線の L 関数は保型 L 関数に等しく, それもまた解析接続の問題は解決している. 話が逸れてしまったが, とりあえず「CM 楕円曲線の L 関数は Hecke L 関数である」を示していこう.

まずは楕円曲線の L 関数の定義を復習する. $F/\mathbb{Q}$ を代数体, E/F を楕円曲線とする. F の有限素点 $\mathfrak{P}$ に対して

$$\mathbb{F}_{\mathfrak{P}} := \mathcal{O}_F/\mathfrak{P}, \quad q_{\mathfrak{P}} := N_{F/\mathbb{Q}}\mathfrak{P} = \#\mathbb{F}_{\mathfrak{P}}, \quad a_{\mathfrak{P}} := q_{\mathfrak{P}} + 1 - \#\tilde{E}(\mathbb{F}_{\mathfrak{P}})$$

とする. このとき楕円曲線 E/F の $\mathfrak{P}$ での局所 L 関数を以下のように定義する.

$$L_{\mathfrak{P}}(E/L, T) = \begin{cases} 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2 & (\text{good reduction at } \mathfrak{P}) \\ 1 - T & (\text{split multiplicative reduction at } \mathfrak{P}) \\ 1 + T & (\text{non-split multiplicative reduction at } \mathfrak{P}) \\ 1 & (\text{additive reduction at } \mathfrak{P}) \end{cases}$$

Definition 1.30: [6, p. 172, Definition]

楕円曲線 E/F の Hasse-Weil L 関数を Euler 積

$$L(E/F, s) := \prod_{\mathfrak{P}} \frac{1}{L_{\mathfrak{P}}(E/F, q_{\mathfrak{P}}^{-s})} = \prod_{\text{good}} \frac{1}{1 - a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s} + q_{\mathfrak{P}}^{1-2s}} \prod_{\text{split}} \frac{1}{1 - q_{\mathfrak{P}}^{-s}} \prod_{\text{non-split}} \frac{1}{1 + q_{\mathfrak{P}}^{-s}}$$

によって定義する. ここで積は F の全ての有限素点 $\mathfrak{P}$ を渡る.

Hasse の不等式 $|a_{\mathfrak{P}}| \le 2\sqrt{q_{\mathfrak{P}}}$ を用いることで L 関数は $\mathrm{Re}(s) > 3/2$ において収束することが示せる.

> 複素解析より, $\prod_n a_n \quad ({}^\forall n, a_n \neq 0)$ が収束するためには $\sum_n \log(a_n)$ が収束することが必要十分であった.
>
> $$\begin{aligned} \sum_{\mathfrak{P}} \log \frac{1}{1 - a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s} + q_{\mathfrak{P}}^{1-2s}} &= -\sum_{\mathfrak{P}} \log(1 - (a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s} - q_{\mathfrak{P}}^{1-2s})) \\ &= \sum_{\mathfrak{P}} \sum_{n=1}^{\infty} (a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s} - q_{\mathfrak{P}}^{1-2s})^n \frac{1}{n} \\ &\overset{(!)}{=} \sum_{n=1}^{\infty} \sum_{\mathfrak{P}} (a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s} - q_{\mathfrak{P}}^{1-2s})^n \frac{1}{n} \\ &= \sum_{\mathfrak{P}} (a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s} + q_{\mathfrak{P}}^{1-2s}) + (\text{higher term}) \\ &= \sum_{\mathfrak{P}} a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s} + (\text{higher term}) \end{aligned}$$
>
> より $\sum_{\mathfrak{P}} a_{\mathfrak{P}}q_{\mathfrak{P}}^{-s}$ の絶対収束性をチェックすればよい. (!) の部分の等号, すなわち和の順序の入れ替えは, 絶対収束性をチェックすれば正当化される.
>
> $$\sum_{\mathfrak{P}} \left| \frac{a_{\mathfrak{P}}}{q_{\mathfrak{P}}^s} \right| \le \sum_{\mathfrak{P}} \frac{2q_{\mathfrak{P}}^{1/2}}{q_{\mathfrak{P}}^{\mathrm{Re}(s)}} = 2\sum_{\mathfrak{P}} \frac{1}{q_{\mathfrak{P}}^{\mathrm{Re}(s)-1/2}} < 2\sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^{\mathrm{Re}(s)-1/2}}$$
>
> 上のように評価され, 最右辺の Dedekind ζ 関数は $\mathrm{Re}(s) - 1/2 > 1$ で収束することから主張を得る.

Conjecture 1.31: [6, p. 173, Conjecture 10.2]

F を代数体, E/F を楕円曲線とする. L 関数 $L(E/F, s)$ は $\mathbb{C}$ 全体に解析接続され, s と $2-s$ での値について関数等式を満たす.

最初に述べたように, 上の Conjecture は CM 楕円曲線と $\mathbb{Q}$ 上の楕円曲線については解決している.

Definition 1.32: [6, p. 173, Definition]

Hecke 指標 (Grössencharacter) $\psi : \mathbb{A}_L^\times \to \mathbb{C}^\times$ に付随する Hecke L 関数を, Euler 積

$$L(\psi, s) := \prod_{\mathfrak{P}} \frac{1}{1-\psi(\mathfrak{P})q_{\mathfrak{P}}^{-s}}$$

によって定義する. ここで $\mathfrak{P}$ は L の全ての有限素点を渡る. また, $1-\psi(\mathfrak{P})T$ を $\mathfrak{P}$ での局所 L 関数ということにする.

Theorem 1.33: [6, p. 173, Theorem 10.3]

Grössencharacter ψ に付随する Hecke L 関数 $L(\psi, s)$ は $\mathbb{C}$ 全体に解析接続される. さらにある $N = N(\psi) \in \mathbb{R}$ が存在して, $L(\psi, s)$ と $L(\bar{\psi}, N-s)$ の間に関数等式が成り立つ.

さて, CM 楕円曲線の L 関数が Hecke L 関数であることを示すに一つ命題を証明する.

Proposition 1.34: [6, p. 124, Proposition 4.4]

F を代数体, $\mathfrak{P} \leq \mathcal{O}_F$ を極大イデアル, $E_1/F, E_2/F$ を $\mathfrak{P}$ で good reduction な楕円曲線, $\tilde{E}_1, \tilde{E}_2$ をそれぞれ mod $\mathfrak{P}$ での reduction とする. このとき自然な写像

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\tilde{E}_1, \tilde{E}_2); \phi \mapsto \tilde{\phi}$$

は単射である. さらに次数の保存, すなわち $\deg\phi = \deg\tilde{\phi}$ が成り立つ.

Proof. まず単射性を示す. 同種 $\phi : E_1 \to E_2$ を, $\tilde{\phi} = [0]$ を満たすものとする. [5, p. 192, Proposition 3.1] より, $\mathfrak{P}$ と互いに素な任意の整数 m に対して単射 $\iota : E_2(L)[m] \hookrightarrow \tilde{E}_2(\mathbb{F}_{\mathfrak{P}})$ が存在する. ここで, $T \in E_1(L)[m]$ に対して仮定より

$$\widetilde{\phi(T)} = \tilde{\phi}(\tilde{T}) = \tilde{O}$$

である. これは, $\phi(T) \in E_2(L)[m]$ の ι の像が潰れていることを意味している. ι の単射性から $\phi(T) = O$ でなければならない. 以上より $E_1(L)[m] \subset \mathrm{Ker}\,\phi$ がわかった. m は任意に大きく取れるので $\mathrm{Ker}\,\phi$ は任意に大きくならなければならないが, 非自明な同種の核は有限なので, $\phi = 0$ となるしかない.

次に次数の等式を示す. $\mathfrak{P}$ と互いに素な素数 ℓ を一つ取る. 任意の $x, y \in T_\ell(E_1)$ に対して Weil pairing $e_{E_1} : T_\ell(E_1) \times T_\ell(E_1) \to T_\ell(\mu)$ は

$$\begin{aligned} e_{E_1}(x,y)^{\deg\phi} &= e_{E_1}([\deg\phi]x, y) \quad (\because \text{Weil pairing の線形性}) \\ &= e_{E_1}((\hat{\phi}\circ\phi)x, y) \quad (\because \text{双対同種の性質}) \\ &= e_{E_2}(\phi(x), \phi(y)) \quad (\because \text{Weil pairing の compatibility}) \end{aligned} \tag{1}$$

と計算できたことを思い出す. 同様に $\tilde{E}_1$ 上でも

$$e_{\tilde{E}_1}(\tilde{x}, \tilde{y})^{\deg\tilde{\phi}} = e_{\tilde{E}_2}(\tilde{\phi}\tilde{x}, \tilde{\phi}\tilde{y}) \tag{2}$$

が成り立つ. ここで, [5, p. 192, Proposition 3.1(b)] より $E[\ell^n] \simeq \tilde{E}[\ell^n]$ $({}^\forall n)$ が成り立ち, 従って $T_\ell(E) \simeq T_\ell(\tilde{E})$ が成り立つ.

> 例えば Corollary 1.8 より楕円曲線の等分点を付け加えた体は有限次拡大である. 従って $F' := F(E[\ell^n])$ とすれば F'/F は有限次拡大であり, $\#E(F')[\ell^n] = \ell^{2n}$ である. 故に $E(F')[\ell^n] = E[\ell^n]$ である. [5, p. 192, Proposition 3.1(b)] を用いると単射
>
> $$E[\ell^n] = E(F')[\ell^n] \hookrightarrow \tilde{E}(\mathbb{F}_{\mathfrak{P}'})[\ell^n] \subset \tilde{E}[\ell^n]$$

が得られるが, $\#\tilde{E}[\ell^n] = \ell^{2n}$ であるので上の写像は同型である.

そして Weil pairing の定義に戻ることにより

$$^{\forall}x, y \in T_\ell(E), \quad \widetilde{e_E(x,y)} = e_{\tilde{E}}(\tilde{x}, \tilde{y}) \tag{3}$$

が分かる. 以上より

$$\begin{aligned}
e_{\tilde{E}_1}(\tilde{x}, \tilde{y})^{\deg\phi} &= \widetilde{e_{E_1}(x,y)}^{\deg\phi} \quad (\because (3)) \\
&= e_{E_2}\widetilde{(\phi(x), \phi(y))} \ (\because (1)) \\
&= e_{\tilde{E}_2}(\widetilde{\phi(x)}, \widetilde{\phi(y)}) \ (\because (3)) \\
&= e_{\tilde{E}_2}(\tilde{\phi}\tilde{x}, \tilde{\phi}\tilde{y}) \\
&= e_{\tilde{E}_1}(\tilde{x}, \tilde{y})^{\deg\tilde{\phi}} \ (\because (2))
\end{aligned}$$

を得る. Weil pairing の非退化性より $\deg\phi = \deg\tilde{\phi}$ が成り立たなければならない. □

以下が CM 楕円曲線の L 関数と Hecke L 関数を結ぶ重要な主張である. 実際に Hecke 指標の値を計算するのにも必要な公式であるので, 主張を覚えておくと便利だろう.

Corollary 1.35: [6, p. 175, Corollary 10.4.1]

1. $q_{\mathfrak{P}} = N_{F/\mathbb{Q}}\mathfrak{P} = N_{K/\mathbb{Q}}(\psi_{E/F}(\mathfrak{P}))$.
2. $\#\tilde{E}(\mathbb{F}_{\mathfrak{P}}) = N_{F/\mathbb{Q}}\mathfrak{P} + 1 - \psi_{E/F}(\mathfrak{P}) - \overline{\psi_{E/F}(\mathfrak{P})}$.
3. $a_{\mathfrak{P}} = \psi_{E/F}(\mathfrak{P}) + \overline{\psi_{E/F}(\mathfrak{P})}$.

Proof. (1)

$$\begin{aligned}
N_{F/\mathbb{Q}}\mathfrak{P} &= \deg\phi_{\mathfrak{P}} \quad (\because [5, \text{p. } 25, \text{Proposition } 2.11]) \\
&= \deg[\widetilde{\psi_{E/F}(\mathfrak{P})}] \quad (\because \text{Proposition } 1.24) \\
&= \deg[\psi_{E/F}(\mathfrak{P})] \quad (\because \text{Proposition } 1.34) \\
&= N_{K/\mathbb{Q}}(\psi_{E/F}(\mathfrak{P})) \quad (\because [6, \text{p. } 104, \text{Corollary } 1.5])
\end{aligned}$$

となって ok. ただし最後の等式は証明していないが, $\deg[m] = m^2 = |N_{K/\mathbb{Q}}(m)|$ の類似である. ここから何となく理解できるだろう.

(2) まず容易に分かるように $\phi : \tilde{E}(\mathbb{F}_{\mathfrak{P}}) \to \mathrm{Ker}(1 - \phi_{\mathfrak{P}}); \tilde{P} \mapsto \tilde{P}$ は全単射である. 従って

$$\begin{aligned}
\#\tilde{E}(\mathbb{F}_{\mathfrak{P}}) &= \#\mathrm{Ker}(1 - \phi_{\mathfrak{P}}) \\
&= \deg(1 - \phi_{\mathfrak{P}}) \quad (\because [5, \text{p. } 79, \text{Corollary } 5.5], [5, \text{p. } 72, \text{Theorem } 4.10(\text{c})]) \\
&= \deg[1 - \widetilde{\psi_{E/F}(\mathfrak{P})}] \quad (\because \text{Proposition } 1.24) \\
&= \deg[1 - \psi_{E/F}(\mathfrak{P})] \quad (\because \text{Proposition } 1.34) \\
&= N_{K/\mathbb{Q}}(1 - \psi_{E/F}(\mathfrak{P})) \quad (\because [6, \text{p. } 104, \text{Corollary } 1.5]) \\
&= (1 - \psi_{E/F}(\mathfrak{P}))(1 - \overline{\psi_{E/F}(\mathfrak{P})}) \quad (\because \text{ノルムの定義}) \\
&= 1 - \psi_{E/F}(\mathfrak{P}) - \overline{\psi_{E/F}(\mathfrak{P})} + N_{F/\mathbb{Q}}(\mathfrak{P}) \quad (\because (1))
\end{aligned}$$

となって ok.

(3) $a_{\mathfrak{P}}$ の定義と (1) と (2) より

$$\begin{aligned}
a_{\mathfrak{P}} &:= q_{\mathfrak{P}} + 1 - \#\tilde{E}(\mathbb{F}_{\mathfrak{P}}) \\
&= N_{F/\mathbb{Q}}(\mathfrak{P}) + 1 - \left(1 - \psi_{E/F}(\mathfrak{P}) - \overline{\psi_{E/F}(\mathfrak{P})} + N_{F/\mathbb{Q}}(\mathfrak{P})\right) \\
&= \psi_{E/F}(\mathfrak{P}) + \overline{\psi_{E/F}(\mathfrak{P})}
\end{aligned}$$

となって ok. □

以上で CM 楕円曲線の L 関数が Hecke L 関数であることの証明の準備が整った.

Theorem 1.36: [6, p. 176, Theorem 10.5]

E/F を楕円曲線で, K の整数環 $\mathcal{O}_K$ により虚数乗法をもつと仮定する. このとき以下が成り立つ.

1. $K \subset F$ のとき, $\psi_{E/F}$ を楕円曲線 E/F に付随する Hecke 指標とする. このとき
$$L(E/F, s) = L(\psi_{E/F}, s)L(\overline{\psi_{E/F}}, s).$$
2. $K \not\subset F$ のとき, $F' := FK$ とおく. $\psi_{E/F'}$ を E/F' に付随する楕円曲線とする. このとき
$$L(E/F, s) = L(\psi_{E/F'}, s).$$

Proof. (2) は演習問題に投げられていて, 割と step が多いので省略する. (1) を示す. Hasse-Weil L 関数側から全ての有限素点に対する局所 L 関数を計算する. Theorem 1.9 より E/L は potentially good reduction であり, 従って [5, p. 198, Proposition 5.4(b)] より E/L が multiplicative reduction となる有限素点は存在しない. よって

$$L_{\mathfrak{P}}(E/F, T) = \begin{cases} 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2 & (\text{good reduction at } \mathfrak{P}) \\ 1 & (\text{bad reduction at } \mathfrak{P}) \end{cases}$$

が分かる.

次に Hecke L 関数側から全ての有限素点に対する局所 L 関数を計算する. $\mathfrak{P}$ が bad reduction ならば Corollary 1.23 より $\mathfrak{P}|\mathfrak{f}_\psi$ が成り立つ. ここで $\mathfrak{f}_\psi$ は $\psi_{E/F}$ のコンダクターである. よって $\psi_{E/F}(\mathfrak{P}) = \overline{\psi_{E/F}(\mathfrak{P})} = 0$ である. 従って

$$L_{\mathfrak{P}}(\psi_{E/F}, s) = 1 - \psi_{E/F}(\mathfrak{P})T\big|_{\psi_{E/F}(\mathfrak{P})=0} = 1$$

である. $\mathfrak{P}$ が good reduction ならば Corollary 1.35 より

$$\begin{aligned} L_{\mathfrak{P}}(\psi_{E/F}, s)L_{\mathfrak{P}}(\overline{\psi_{E/F}}, s) &= \{1 - \psi_{E/F}(\mathfrak{P})T\}\left\{1 - \overline{\psi_{E/F}(\mathfrak{P})}T\right\} \\ &= 1 - (\psi_{E/F}(\mathfrak{P}) + \overline{\psi_{E/F}(\mathfrak{P})})T + (N_{K/\mathbb{Q}}\psi_{E/F}(\mathfrak{P}))T^2 \\ &= 1 - a_{\mathfrak{P}}T + q_{\mathfrak{P}}T^2 \end{aligned}$$

となって確かに全ての L の有限素点で局所 L 関数が一致している. □

Example 1.37: [6, p. 186, Exercise 2.33, 2.34]

$D \in \mathbb{Z}$ を 0 でない整数, $E/\mathbb{Q} : y^2 = x^3 - Dx$ を楕円曲線, p を $p \nmid 2D$ を素数とする. (E が bad reduction となる素点は 2 の上にある素点と D の上にある素点であることが分かっているから, $p \nmid 2D$ という仮定は L 関数に影響を与えない) このとき $L(E/\mathbb{Q}, s)$ を Hecke L 関数で表してみる. $E/\mathbb{Q}$ は $K = \mathbb{Q}(i)$ の整数環により虚数乗法をもつから, Theorem 1.36 により, それは付随する Hecke 指標 $\psi = \psi_{E/K}$ を用いて $L(\psi, s)$ と表せる. 従ってあとは ψ の explicit な表示を求めればよい. そのためには Corolalry 1.35 より有理点の個数を求めればよい.

まともに計算しようと思うとなかなか大変なので, [6, p. 185, Exercise 2.33] を見ると,

$$\#\tilde{E}(\mathbb{F}_\mathfrak{p}) = \begin{cases} p + 1 - \overline{\left(\dfrac{D}{\pi}\right)_4}\pi - \left(\dfrac{D}{\pi}\right)_4\bar{\pi} & (p \equiv 1 \bmod 4) \\ p + 1 \end{cases}$$

である. ただし $p \equiv 1 \bmod 4$ のとき $\mathfrak{p} = (\pi)$ は p の上にある K の素イデアルで $\pi \equiv 1 \bmod 2 + 2i$ と正規化したものである. 従って Corollary 1.35(3) より

$$\psi(\mathfrak{p}) = \begin{cases} \overline{\left(\dfrac{D}{\pi}\right)_4}\pi \text{ or } \left(\dfrac{D}{\pi}\right)_4\bar{\pi} & (p \equiv 1 \bmod 4) \\ -p \text{ or } p & (p \equiv 3 \bmod 4) \end{cases}$$

のいずれかを得る. $[\psi(\mathfrak{p})]$ が p-Frobenius になること用いると explicit な Hecke 指標は

$$\psi : \mathbb{A}_K^\times \to \mathbb{C}^\times; \mathfrak{p} \mapsto \overline{\left(\frac{D}{\pi}\right)_4}\pi \quad (\pi \equiv 1 \bmod 2 + 2i)$$

と書け, L 関数は

$$
\begin{aligned}
L(E/\mathbb{Q}, s) &= \prod_{\mathfrak{p} \nmid 2D} \frac{1}{1 - \overline{\left(\frac{D}{\pi}\right)_4} \pi N_{K/\mathbb{Q}} \mathfrak{p}^{-s}} \quad (\pi \equiv 1 \bmod 2+2i) \\
&= \sum_{\mathfrak{a}} \frac{\varepsilon(\mathfrak{a})\alpha}{N_{K/\mathbb{Q}} \mathfrak{a}^s} \quad (\mathfrak{a} = (\alpha),\ \alpha \equiv 1 \bmod 2+2i)
\end{aligned}
$$

と書ける. ただし

$$
\varepsilon(\mathfrak{a}) = \varepsilon((\alpha)) = \overline{\left(\frac{D}{\alpha}\right)_4}
$$

である.

2 Elliptic Units

虚二次体 K の整数環により虚数乗法をもつ楕円曲線 E の楕円単数 (elliptic units) とはノルムと compatible な, ある関係式をもつ K のあるアーベル拡大の unit である. この整合性によって Euler system が構成される.

このセクションでは K は類数 1 の虚二次体, $E/\mathbb{C}$ を $\mathcal{O}_K$ により虚数乗法をもつ楕円曲線とする.

2.1 The rational functions $\Theta_{E,\mathfrak{a}}$ and $\Lambda_{E,\mathfrak{a}}$

Definition 2.1

楕円曲線 E の model を一つ固定し, $\Delta(E)$ をその model により定まる判別式, さらに整イデアル $\mathfrak{a} = (\gamma) \leq \mathcal{O}_K$ を一つ固定する. このとき

$$\Theta_{E,\mathfrak{a}} = \gamma^{-12}\Delta(E)^{N\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}]-O} (x - x(P))^{-6}$$

と定義する.

イデアル $\mathfrak{a}$ の生成元 γ の取り方には $\mathcal{O}_K^\times$ の曖昧さがある. しかし K は虚二次体であるから任意の $\mathcal{O}_K^\times$ の元の位数は 12 を割り切る. 従って $\Theta_{E,\mathfrak{a}}$ の定義は生成元 γ の取り方に依らない.

Proposition 2.2

関数 $\Theta_{E,\mathfrak{a}}$ は以下を満たす.

1. 楕円曲線 E の model に依らない.
2. $E'/\mathbb{C}$ が $\phi : E \to E'$ により同型ならば $\Theta_{E,\mathfrak{a}} = \Theta_{E',\mathfrak{a}} \circ \phi$.
3. $F \subset \mathbb{C}$ が部分体で楕円曲線 E が F 上定義されているならば, $\Theta_{E,\mathfrak{a}} \in K(E)_F$.

ただし $K(E)_F$ は F 上 定義された E の有理関数体である.

Proof. (1) x, y を楕円曲線 E の座標関数とする. このとき楕円曲線の $\mathbb{C}$ 上の同型類は変数変換

$$x' = u^2x + r, \quad y' = u^3y + sx + t \quad (u \in \mathbb{C}^\times, r, s, t \in \mathbb{C})$$

で与えられ, $\Delta(E') = u^{12}\Delta(E)$ が成り立つのであった. このとき $\Theta_{E,\mathfrak{a}} = \Theta_{E',\mathfrak{a}}$ を示せばよい. 定義に従って計算すれば

$$\begin{aligned}
\Theta_{E',\mathfrak{a}} &= \gamma^{-12}\Delta(E')^{N\mathfrak{a}-1} \prod_{P \in E'[\mathfrak{a}]-O} (x' - x'(P))^{-6} \\
&= \gamma^{-12}u^{12(N\mathfrak{a}-1)}\Delta(E)^{N\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}]-O} \left(u^2x - u^2x(P)\right)^{-6} \\
&= \gamma^{-12}u^{12(N\mathfrak{a}-1)}\Delta(E)^{N\mathfrak{a}-1}u^{-12(N\mathfrak{a}-1)} \prod_{P \in E[\mathfrak{a}]-O} (x - x(P))^{-6} \\
&= \gamma^{-12}\Delta(E)^{N\mathfrak{a}-1} \prod_{P \in E[\mathfrak{a}]-O} (x - x(P))^{-6} \\
&= \Theta_{E,\mathfrak{a}}
\end{aligned}$$

となって ok.

(2) $\phi(x, y) = (u^2x + r, u^3y + sx + t)$ の形をしているから (1) の計算と全く同様になる.

(3) 任意の $\sigma \in G(\bar{F}/F)$ に対して $\Theta_{E,\mathfrak{a}}^\sigma = \Theta_{E,\mathfrak{a}}$ を示せばよい. $\gamma \in \mathcal{O}_K^\times$ であること, 仮定 E/F より $\Delta(E) \in F$ であるこ

とより

$$\begin{aligned}\Theta_{E,\mathfrak{a}}^{\sigma} &= (\gamma^{\sigma})^{-12}(\Delta(E)^{\sigma})^{N\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]-O}(x^{\sigma}-x(P)^{\sigma})^{-6}\\ &= \gamma^{-12}\Delta(E)^{N\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]-O}(x-x(P^{\sigma}))^{-6}\\ &= \gamma^{-12}\Delta(E)^{N\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]-O}(x-x(P))^{-6}\\ &= \Theta_{E,\mathfrak{a}}\end{aligned}$$

となって ok. 最後の等式は $E[\mathfrak{a}]\to E[\mathfrak{a}]; P\mapsto P^{\sigma}$ が全単射であることから従う. □

Proposition 2.3

$\mathfrak{b}\leq\mathcal{O}_K$ を $(\mathfrak{b},\mathfrak{a})=1$ を満たす非自明なイデアル, $Q\in E[\mathfrak{b}]$ とする. このとき $\Theta_{E,\mathfrak{a}}\in K(\mathfrak{b})$ が成り立つ.

Proof. 今 K の類数は 1 と仮定していること, 不分岐類体論より Hilbert 類体とイデアル類群が同型であることから K の Hilbert 類体は K そのものである. よって Corollary 1.13 より $\mathcal{O}_K$ により虚数乗法をもつ楕円曲線 E'/K で, $\mathbb{C}$ 上 E と同型なものが存在する. Proposition 2.2 (2) より関数 $\Theta_{E,\mathfrak{a}}$ は E の同型類に依らないから, 初めから E は K 上定義されているとしてよい. さらに Proposition 2.2 (3) より $\Theta_{E,\mathfrak{a}}$ は K 上定義されることに注意する.

まず $U_{\mathfrak{b}}:=\{x\in\mathbb{A}_K^{\times}\mid {}^{\forall}\mathfrak{p},\ x_{\mathfrak{p}}\in 1+\mathfrak{b}\mathcal{O}_{\mathfrak{p}}\}$ とおく. このとき $x\in U_{\mathfrak{b}}$ ならば $\Theta_{E,\mathfrak{a}}(Q)$ が $[x,K]$ により固定されることを見ればよい. ただし $\Theta_{E,\mathfrak{a}}(Q)\in K^{ab}$ であることを注意しておく. これは例えば Theorem 1.29 (2) 等から従う.

> $G(K^{ab}/K(\mathfrak{b}))=[U_K^{\mathfrak{b}},K]$ を示せばよい. まず $C_K:=\mathbb{A}_K^{\times}/K^{\times}$ をイデール群, $\mathfrak{m}$ を K のモジュラスとする. さらに
>
> $$U_K^{\mathfrak{m}(\mathfrak{p})}=\begin{cases}\mathcal{O}_{\mathfrak{p}}^{\times} & (\mathfrak{p}\nmid\infty,\mathfrak{m}(\mathfrak{p})=0)\\ 1+\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}\mathcal{O}_{\mathfrak{p}} & (\mathfrak{p}\nmid\infty,\mathfrak{m}(\mathfrak{p})>0)\\ K_{\mathfrak{p}}^{\times} & (\mathfrak{p}|\infty,\mathfrak{m}(\mathfrak{p})=0)\\ \mathbb{R}_{>0}^{\times} & (\mathfrak{p}:\mathrm{real},\mathfrak{m}(\mathfrak{p})>0)\end{cases}$$
>
> とし, $U_K^{\mathfrak{m}}=\prod_{\mathfrak{p}\in M_K}U_K^{\mathfrak{m}(\mathfrak{p})}$ とおく. このとき同型定理から, 有限次アーベル拡大 L/K に対し $[\ ,L/K]:C_K/N_{L/K}C_L\simeq G(L/K)$ が成り立つが, 特に存在定理から $N_{L/K}C_L=U_K^{\mathfrak{m}}$ となるような L が一意的に存在し, モジュラス $\mathfrak{m}$ の ray class field というのであった. すなわち ray class field $K(\mathfrak{b})$ とは
>
> $$[\ ,K(\mathfrak{b})/K]:C_K/U_K^{\mathfrak{b}}=G(K(\mathfrak{b})/K)$$
>
> を満たす唯一の K の有限次アーベル拡大である. よって以下を得る.
>
> $$\begin{aligned}G(K^{ab}/K(\mathfrak{b}))&=\mathrm{Ker}\left(G(K^{ab}/K)\to G(K(\mathfrak{b})/K)\right)\\ &=[\ ,K]\left(\mathrm{Ker}\left(C_K\to G(K(\mathfrak{b})/K)\right)\right)\\ &=[\ ,K]\left(\mathrm{Ker}\left(C_K\to C_K/U_K^{\mathfrak{b}}\right)\right)\\ &=[\ ,K](U_K^{\mathfrak{b}})\\ &=[U_K^{\mathfrak{b}},K]\end{aligned}$$

まず $\Theta_{E,\mathfrak{a}}$ は K 上定義されているとしているので $\Theta_{E,\mathfrak{a}}(Q)^{[x,K]}=\Theta_{E,\mathfrak{a}}^{[x,K]}(Q)^{[x,K]}=\Theta_{E,\mathfrak{a}}(Q^{[x,K]})$ である. Proposition 1.16 より $Q\in E[\mathfrak{b}]$ への $[x,K]$ の作用は $\alpha(x)x^{-1}$ 倍 $(\alpha(x)\in\mathcal{O}_K^{\times})$ という作用になる. 今 $x\in U^{\mathfrak{b}}$ だから Lemma 1.15 より x 倍の作用は自明となる. 従って $[\alpha(x)]$ が同型写像になることに注意すれば

$$\Theta_{E,\mathfrak{a}}(Q^{[x,K]})=\Theta_{E,\mathfrak{a}}([\alpha(x)]Q)=\Theta_{E,\mathfrak{a}}(Q)$$

となって ok. □

Theorem 2.4: Weierstrass の準備定理の系

$\mathcal{O}$ を完備なネーター局所環, $\mathfrak{p}$ を唯一の極大イデアルとする. $g(X)=\sum_{i\geq 0} a_i X^i \in \mathcal{O}[[X]]$ が

$$a_0 \equiv \cdots \equiv a_{n-1} \equiv 0 \bmod \mathfrak{p}, \quad a_n \not\equiv 0 \bmod \mathfrak{p}$$

を満たすならば, $g(X)=u(X)g_0(X)$ となる $u(X)\in\mathcal{O}[[X]]^\times$ と n 次有徴多項式 $g_0(X)\in\mathcal{O}[X]$ が一意的に存在する. ここで $g_0(X)\in\mathcal{O}[X]$ が n 次有徴多項式であるとは

$$g_0(X)=b_0+b_1X+\cdots+b_{n-1}X^{n-1}+X^n, \quad (b_0\equiv\cdots\equiv b_{n-1}\equiv 0 \bmod \mathfrak{p})$$

を満たすことをいう.

Lemma 2.5

K を局所体, $\mathfrak{p}=(\pi)$ を K の整数環 $\mathcal{O}$ の素イデアル, $f(X)\in\mathcal{O}[X]$ を $\mathfrak{p}$ に関する Eisenstein 多項式で $f(X)\equiv \pi \bmod \deg 2$ を満たすとする. また $f(X)$ の根の一つを α とし, $L:=K(\alpha)$ とおく. v を K の加法付値で $v(\pi)=1$ を満たすものとして, L まで延長しそれもまた v と書く. このとき

$$v(\alpha)=\frac{1}{\deg f}$$

が成り立つ.

Proof. $\mathfrak{P}$ を $\mathfrak{p}$ の上にある L の素イデアルとする. K の正規化加法付値を v_K と書くと, 例えば雪江代数 3 の命題 3.3.20 より L の正規化付値 v_L は

$$[L:K]v_L(x)=v_K(N_{L/K}(x)) \quad ({}^\forall x\in L)$$

を満たすように延長される. 上の式において $x=\alpha$ とすると, $f(X)\equiv\pi \bmod \deg 2$ より $N_{L/K}(\alpha)=\pi$ なので

$$[L:K]v_L(\alpha)=v_K(\pi)=1$$

を得る. f は $\mathcal{O}$ 上既約だから $[L:K]=\deg f$ である. 主張はここから従う. □

Proposition 2.6: de Shalit ノート Proposition 1.35 (special case)

$k/\mathbb{Q}_p$ を有限次拡大, ν を k 上の正規化付値, $\mathcal{O}$ を k の付値環, $\wp$ を $\mathcal{O}$ の極大イデアル, k^{ur} の k の最大不分岐拡大, φ を $G(k^{ur}/k)$ の Frobenius かつ位相的生成元とする. また, $\wp$ の uniformizer $\pi\in\mathcal{O}$ に対して

$$\mathcal{F}_\pi=\left\{f\in\mathcal{O}[[X]] \mid f\equiv \pi X \bmod \deg 2, f\equiv X^{N\mathfrak{p}} \bmod \mathfrak{p}\right\}$$

とおく. このとき $f=\pi X+\cdots\in\mathcal{F}_\pi$ と $a\in\mathcal{O}$ に対し

$$^{\exists!}[a](X)\in \mathrm{End}_{\mathcal{O}}(F_f) \ \text{ such that } \begin{cases}[a](X)\equiv aX \bmod \deg 2\\ f\circ[a]=[a]\circ f\end{cases}$$

が成り立つ. ここで F_f は f の Lubin-Tate 形式群である. さらに

$$\Phi:\mathcal{O}\to\mathrm{End}_{\mathcal{O}}(F_f); a\mapsto[a](X)$$

は群同型であり $[a]=f$ が成り立つ.

Lemma 2.7

E/K を楕円曲線, $\mathfrak{p}=(\pi)$ を E/K が good reduction となる K の素イデアル, $\hat{E}/\mathcal{O}_\mathfrak{p}$ を $E/K_\mathfrak{p}$ に付随する形式群とする. このとき

$$[\pi^n](X)\equiv X^{N\mathfrak{p}^n} \bmod \mathfrak{p}\mathcal{O}_\mathfrak{p}[[X]]$$

が成り立つ.

Proof. $f = \pi X + \cdots \in \mathcal{F}_\pi$ とおく．このとき Proposition 2.6 よりある条件を満たす $[\pi](X) \in \mathrm{End}_{\mathcal{O}_\mathfrak{p}}(\hat{E})$ が存在し，さらに $f = [\pi]$ である．n で主張が成り立っているとする．このとき $[\pi^{n+1}](X) = [\pi]([\pi^n](X)) \equiv [\pi](X^{N\mathfrak{p}^n}) = f(X^{N\mathfrak{p}^n}) \equiv (X^{N\mathfrak{p}^n})^{N\mathfrak{p}} = X^{N\mathfrak{p}^{n+1}}$ であるから $n+1$ のときも成り立つ．よって $n = 1$ のときだけ示せばよい．

一般に，$\phi \in \mathrm{End}_K(E)$ に対し，ある $\phi(X) \in \mathrm{End}_{\mathcal{O}_\mathfrak{p}}(\hat{E})$ が存在して

$$\phi(x(X), y(X)) = (x(\phi(X)), y(\phi(X)))$$

が成り立つ．

> よく分からん．省略．

この事実において $\phi \mapsto [\pi] \in \mathrm{End}_K(E)$ として用いると

$$\begin{aligned}(x([\pi](X)), y([\pi](X))) &= [\pi](x(X), y(X)) \equiv \varphi_{N\mathfrak{p}}(x(X), y(X)) \quad (\because \text{Proposition 1.24}) \\ &= (x(X)^{N\mathfrak{p}}, y(X)^{N\mathfrak{p}}) \equiv (x(X^{N\mathfrak{p}}), y(X^{N\mathfrak{p}}))\end{aligned}$$

ただし全て $\mathrm{mod}\,\mathfrak{p}\mathcal{O}_\mathfrak{p}((X))$ で考えている．よって

$$[\pi](X) = -\frac{x([\pi](X))}{y([\pi](X))} \equiv -\frac{x(X^{N\mathfrak{p}})}{y(X^{N\mathfrak{p}})} = X^{N\mathfrak{p}}$$

となって ok. □

Lemma 2.8

E は K 上定義されているとし，K の素点 $\mathfrak{p} = (\pi)$ で good reduction であるとする．E の $\mathfrak{p}$ での minimal model を固定する．また，$\mathfrak{b}, \mathfrak{c}$ を $\mathcal{O}_K$ の非自明なイデアルで $(\mathfrak{b}, \mathfrak{c}) = 1$ とする．$P \in E[\mathfrak{b}], Q \in E[\mathfrak{c}]$ を位数がそれぞれちょうど $\mathfrak{b}, \mathfrak{c}$ であると仮定する．最後に K の正規化加法付値 $v = v_\mathfrak{p}$，すなわち $v(\mathfrak{p}) = 1$ を満たすものを $\bar{K}$ まで延長しておく．このとき以下が成り立つ．

1. $\mathfrak{b} = \mathfrak{p}^n$ ならば $v(x(P)) = -2/(N\mathfrak{p}^n - N\mathfrak{p}^{n-1})$.
2. $\mathfrak{b}$ が $\mathfrak{p}$ ベキでないならば，$v(x(P)) \geq 0$.
3. $\mathfrak{p} \nmid \mathfrak{b}\mathfrak{c}$ ならば $v(x(P) - x(Q)) = 0$.

Proof. (1) $F = K(E[\mathfrak{p}^n])$ として，$\mathfrak{p}$ の上にある F の素点 $\mathfrak{P}$ を一つ固定する．ψ を E/K に付随する Hecke 指標とすると $\psi(\mathfrak{p}) \in \mathbb{C}^\times$ は $\psi(\mathfrak{p})\mathcal{O}_K = \mathfrak{I}(\mathfrak{p}) = \mathfrak{p}$ を満たす．つまり $\psi(\mathfrak{p})$ は $\mathcal{O}_K$ の素元であり，$\pi := \psi(\mathfrak{p})$ は $\mathfrak{p}$ の生成元の一つである．Proposition 1.24 より $\widetilde{[\pi]} = \varphi_{N\mathfrak{p}}$，すなわち $[\pi] \in \mathrm{End}_{\mathcal{O}_K}(E)$ の $\mathfrak{p}$ による reduction は $\tilde{E}(k)$ における $N\mathfrak{p}$-Frobenius であった．(k は $K_\mathfrak{p}$ の剰余体) これより $E[\mathfrak{p}^n] \subset E_1(F_\mathfrak{P})$ が分かる．

> 任意に $P \in E[\mathfrak{p}^n]$ を取ると $[\pi^n]P = O$ である．したがって $\mathfrak{P}$ による reduction を考えると
>
> $$\tilde{P} = \tilde{P}^{N\mathfrak{P}^n} = \varphi^n_{N_\mathfrak{P}}(\tilde{P}) = \widetilde{[\pi^n]}\tilde{P} = \widetilde{[\pi^n]P} = \tilde{O}$$
>
> が成り立つ．以上より $P \in E_1(F_\mathfrak{P})$ を得る．

[4, p. 10, Corollary 3.13] より

$$E_1(F_\mathfrak{P}) \to \hat{E}(\mathfrak{P}); (x, y) \mapsto -\frac{x}{y}$$

は同型となる．以上より $E[\mathfrak{p}^n] \subset E_1(F_\mathfrak{P}) \simeq \hat{E}(\mathfrak{P}); (x, y) \mapsto -x/y$ を得る．さらに [4, p. 7, Lemma 3.5] より

$$E_1(F_\mathfrak{P}) = \{(x, y) \in E(F_\mathfrak{P}) \mid v(x) < 0\} = \{(x, y) \in E(F_\mathfrak{P}) \mid v(y) < 0\}$$

であること，さらに $(x, y) \in E_1(F_\mathfrak{P})$ ならば $3v(x) = 2v(y) < 0$ であることが分かっている．これらの事実から，$P \in E[\mathfrak{p}^n]$ に対して

$$-\frac{1}{2}v(x(P)) = v(x(P)) - \frac{3}{2}v(x(P)) = v(x(P)) - v(y(P)) = v\left(\frac{x(P)}{y(P)}\right) = v\left(-\frac{x(P)}{y(P)}\right)$$

を得る．よってあとは形式群の言葉で $z(P)=-x(P)/y(P)$ を調べればよい．

Proposition 2.6 において $k=K_{\mathfrak{p}}, f=f_0=\pi X+\cdots\in F_\pi$ とすると

$$
{}^{\exists!}[\pi](X)\in \mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(\hat{E})\ \text{ such that }\begin{cases}[\pi](X)\equiv \pi X \bmod \deg 2\\ f_0\circ[\pi]=[\pi]\circ f_0\end{cases}
$$

が成り立つ．さらに単射

$$
\mathrm{End}_K(E)\xrightarrow{\iota}\mathcal{O}_K\hookrightarrow\mathcal{O}_{\mathfrak{p}}\xrightarrow{\Phi}\mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(\hat{E});[\pi]\mapsto\pi\mapsto\pi\mapsto[\pi](X)
$$

も成り立つ．冪級数

$$
f(X)=\frac{[\pi^n](X)}{[\pi^{n-1}](X)}\in\mathcal{O}_{\mathfrak{p}}[[X]]
$$

を考える． このとき Lemma 2.7 より $f(X)\equiv X^{N\mathfrak{p}^n-N\mathfrak{p}^{n-1}} \bmod \mathfrak{p}$ が成り立つので，$f(X)$ は Weierstrass の準備定理の系の仮定を満たし，ある $u(X)\in\mathcal{O}_{\mathfrak{p}}[[X]]^\times$ と $N\mathfrak{p}^n-N\mathfrak{p}^{n-1}$ 次有徴多項式 $e(X)\in\mathcal{O}_{\mathfrak{p}}[X]$ が一意的に存在して $f(X)=u(X)e(X)$ が成り立つ．ただし $[\pi^n](X)\equiv\pi^n \bmod \deg 2$ なので $f(X)\equiv\pi \bmod \deg 2$ となり $e(X)$ は特に Eisenstein 多項式である．今，$P\in E[\mathfrak{p}^n]$ はちょうど位数 $\mathfrak{p}^n$ と仮定をしているから，$[\pi^n]P=O$ かつ $[\pi^{n-1}](P)\neq O$ であり，したがって $[\pi^n](X)|_{X=z(P)}=0$ かつ $[\pi^{n-1}](X)|_{X=z(P)}\neq 0$ である．以上より $z=z(P)=-x(P)/y(P)$ に対して $f(z)=0$ である．故に $u(z)\neq 0$ なので $e(z)=0$ が成り立つ．よって Lemma 2.5 より

$$
v(z)=\frac{1}{N\mathfrak{p}^n-N\mathfrak{p}^{n-1}}
$$

を得る．

(2) $P\in E(F)$ となるように有限次拡大 F/K を取っておく．$\mathfrak{P}$ を $\mathfrak{p}$ の上にある F の素点とする．E/K が $\mathfrak{p}$ で good reduction であることから E/F も $\mathfrak{P}$ で good reduction であることに注意する．

$$
E_1(F_{\mathfrak{P}})=\{(x,y)\in E(F_{\mathfrak{P}})\mid v(x)<0\}=\{(x,y)\in E(F_{\mathfrak{P}})\mid v(y)<0\}
$$

であったことから $v(x(P))\geq 0$ を示すためには $P\notin E_1(F_{\mathfrak{P}})$ を示せばよい．$P\in E_1(F_{\mathfrak{P}})$ と仮定して矛盾を導く．同型 $E_1(F_{\mathfrak{P}})\simeq\hat{E}(\mathfrak{P})$ より，$z:=-x(P)/y(P)$ の位数は $N\mathfrak{P}$ べきではない．しかし [5, Proposition 3.2] より任意の $\hat{E}(\mathfrak{P})$ の点の位数は $N\mathfrak{P}$ べき (または ∞) なので矛盾．

(3) $P,Q\in E(F)$ となるように有限次拡大 F/K を取っておく．$\mathfrak{P}$ を $\mathfrak{p}$ の上にある F の素点とする．$\mathfrak{b},\mathfrak{c}$ は $\mathfrak{p}$ べきでないので，(2) より $v(x(P)),v(x(Q))\geq 0$ が成り立つ．よって

$$
v(x(P)-x(Q))\geq\min\{v(x(P)),v(x(Q))\}\geq 0
$$

となる．背理法で示す．$v(x(P)-x(Q))>0$ と仮定する．このとき

$$
\begin{aligned}
v(x(P)-x(Q))>0 &\iff x(P)\equiv x(Q) \bmod \mathfrak{p}\\
&\iff x(\tilde{P})=x(\tilde{Q})\\
&\iff \tilde{P}=\pm\tilde{Q}\\
&\iff \widetilde{P\pm Q}=\tilde{O}\\
&\iff P\pm Q\in E_1(F_{\mathfrak{P}})
\end{aligned}
$$

が成り立つ．(2) の証明と同様の議論で $P\pm Q\notin E_1(F_{\mathfrak{P}})$ であるから矛盾． □

Theorem 2.9

E/K を楕円曲線，$\mathfrak{b}\leq\mathcal{O}_K$ を $\mathfrak{a}$ と互いに素な非自明なイデアルとする．$Q\in E[\mathfrak{b}]$ を位数がちょうど $\mathfrak{b}$ となる点とする．このとき以下が成り立つ．

1. $\mathfrak{b}$ が $\mathfrak{p}$ べきでないならば，$\Theta_{E,\mathfrak{a}}(Q)\in K(\mathfrak{b})$ は global unit，すなわち $K(\mathfrak{b})$ の任意の有限素点 $\mathfrak{P}$ に対して $v_{\mathfrak{P}}\Theta_{E,\mathfrak{a}}(Q)=0$.
2. $\mathfrak{b}$ がある K の素点 $\mathfrak{p}$ のべきならば，$\Theta_{E,\mathfrak{a}}(Q)\in K(\mathfrak{b})$ は $\mathfrak{p}$ の上にない $K(\mathfrak{b})$ の素点 $\mathfrak{P}$ について local unit，すな

わちそのような $\mathfrak{P}$ について $v_{\mathfrak{P}}\Theta_{E,\mathfrak{a}}(Q)=0$.

Proof. (1) $\mathfrak{b}$ は $\mathfrak{q}$ べきでないとする．$\Theta_{E,\mathfrak{a}}$ は E の $\mathbb{C}$ 上同型類に依らなかったので, Proposition 1.25 より E/K は初めから $\mathfrak{q}$ で good reduction であると仮定してよい．よって $\Delta(E)$ と $\mathfrak{q}$ は互いに素, すなわち $v_{\mathfrak{q}}(\Delta(E))=0$ である．$n=v_{\mathfrak{q}}(\gamma)$ とおく．このとき

$$\begin{aligned} v_{\mathfrak{q}}\Theta_{E,\mathfrak{a}}(Q) &= -12v_{\mathfrak{q}}(\gamma)+(N\mathfrak{a}-1)v_{\mathfrak{q}}(\Delta(E))-6\sum_{P\in E[\mathfrak{a}]-O} v_{\mathfrak{q}}\left(x(Q)-x(P)\right) \\ &= -12n-6\sum_{P\in E[\mathfrak{q}^n]-O} v_{\mathfrak{q}}\left(x(Q)-x(P)\right)-6\sum_{P\in E[\mathfrak{a}]-E[\mathfrak{q}^n]} v_{\mathfrak{q}}\left(x(Q)-x(P)\right) \end{aligned}$$

と計算できる．P の位数がちょうど $\mathfrak{q}^m$ $(m>0)$ ならば Lemma 2.8 (1), (2) より

$$v_{\mathfrak{q}}\left(x(Q)-x(P)\right)=\min\left\{v_{\mathfrak{q}}(x(Q)),v_{\mathfrak{q}}(x(P))\right\}=v_{\mathfrak{q}}(x(P))=\frac{-2}{N\mathfrak{q}^m-N\mathfrak{q}^{m-1}} \tag{4}$$

となる．P の位数が $\mathfrak{q}$ べきでないならば Lemma 2.8 (3) より $v_{\mathfrak{q}}(x(Q)-x(P))=0$ である．以上より

$$\begin{aligned} v_{\mathfrak{q}}\Theta_{E,\mathfrak{a}}(Q) &= -12n-6\sum_{m=1}^{n}\left(\sum_{P\in E[\mathfrak{q}^m]-E[\mathfrak{q}^{m-1}]}\frac{-2}{N\mathfrak{q}^m-N\mathfrak{q}^{m-1}}\right) \\ &= -12n-6\sum_{m=1}^{n}\left(N\mathfrak{q}^m-N\mathfrak{q}^{m-1}\right)\frac{-2}{N\mathfrak{q}^m-N\mathfrak{q}^{m-1}} \\ &= -12n-6\cdot(-2n) \\ &= 0 \end{aligned}$$

を得る．

(2) $\mathfrak{b}$ が $\mathfrak{q}$ べきならば (4) の式は一般に成り立つとは限らない．何故ならば $v_{\mathfrak{q}}(x(Q))\geq 0$ とは限らないために (4) の最初の等号が成り立つとは限らないからである．他の計算は同様にできるため, 主張はこれらの事実から従う． $\square$

Definition 2.10

E/K を楕円曲線, ψ を付随する Hecke 指標, $\mathfrak{f}$ をそのコンダクターとする．$S\in E[\mathfrak{f}]$ を $\mathcal{O}_K$ 加群としての生成元とする．このとき

$$\Lambda_{E,\mathfrak{a}}=\prod_{\sigma\in G(K(\mathfrak{f})/K)}\Theta_{E,\mathfrak{a}}\circ\tau_{S^\sigma}$$

と定義する．ただし $\tau_{S^\sigma}:E\to E$ は S^σ 平行移動写像である．

Proposition 2.11

E/K を楕円曲線, ψ を付随する Hecke 指標, $\mathfrak{f}$ をそのコンダクターとする．

1. 有理関数 $\Lambda_{E,\mathfrak{a}}$ は K 上定義される．
2. $\boldsymbol{\tau}\leq\mathcal{O}_K$ を $\mathfrak{f}$ と互いに素な非自明なイデアル, $Q\in E[\boldsymbol{\tau}]$ を位数がちょうど $\boldsymbol{\tau}$ である点とする． このとき $\Lambda_{E,\mathfrak{a}}(Q)\in K(E[\boldsymbol{\tau}])$ は global unit である．

Proof. (1) 任意の $\sigma'\in\mathrm{Aut}(\mathbb{C}/K)$ に対して $\Lambda^{\sigma}_{E,\mathfrak{a}}=\Lambda_{E,\mathfrak{a}}$ を示せばよい．$\Theta_{E,\mathfrak{a}}$ は K 上定義されることに気を付けると

$$\begin{aligned} \Lambda^{\sigma'}_{E,\mathfrak{a}}(X) &= \prod_{\sigma\in G(K(\mathfrak{f})/K)}\left(\Theta_{E,\mathfrak{a}}\circ\tau_{S^\sigma}\right)^{\sigma'}(X) \\ &= \prod_{\sigma\in G(K(\mathfrak{f})/K)}\Theta^{\sigma'}_{E,\mathfrak{a}}\circ\tau^{\sigma'}_{S^\sigma}(X) \\ &= \prod_{\sigma\in G(K(\mathfrak{f})/K)}\Theta_{E,\mathfrak{a}}(X+S^{\sigma\sigma'}) \\ &= \prod_{\sigma\in G(K(\mathfrak{f})/K)}\Theta_{E,\mathfrak{a}}(X+S^{\sigma}) \\ &= \Lambda_{E,\mathfrak{a}}(X) \end{aligned}$$

となって ok.

(2) まず $\Lambda_{E,\mathfrak{a}}(Q) \in K(E[\boldsymbol{\tau}])$ であることは, $\Theta_{E,\mathfrak{a}}$ は K 上の有理関数であること, $S^\sigma \in E[\boldsymbol{\tau}]$ であることから従う. global unit であることを示すには, 各因子 $\Theta_{E,\mathfrak{a}} \circ \tau_{S^\sigma}(Q)$ が global unit であることを示せば十分である. $\Theta_{E,\mathfrak{a}} \circ \tau_{S^\sigma}(Q) = \Theta_{E,\mathfrak{a}}(Q+S^\sigma)$ に対して $Q+S^\sigma$ は位数がちょうど $\boldsymbol{\tau}\mathfrak{f}$ である. よって $\Theta_{E,\mathfrak{a}} \circ \tau_{S^\sigma}(Q) \in K(\boldsymbol{\tau}\mathfrak{f})$ であり, $\boldsymbol{\tau}\mathfrak{f}$ は $\mathfrak{p}$ べきでないので Theorem 2.9 よりこれは global unit である.

□

2.2 The distribution relation

Lemma 2.12

関数 $\Theta_{E,\mathfrak{a}}$ は以下を因子にもつ有理関数である.

$$12N\mathfrak{a}(O) - 12 \sum_{P \in E[\mathfrak{a}]} (P).$$

Proof. まず楕円曲線 $E/\mathbb{C}$ の座標関数 x を用いた関数 $x - x(P)$ は有理関数であるので, $\Theta_{E,\mathfrak{a}}$ が有理関数であることは明らかである. 座標関数 x は無限遠点で 2 位の極であったことを思い出すと関数 $x - x(P)$ の因子は $(P) + (-P) - 2(O)$ となる. したがって $\Theta_{E,\mathfrak{a}}$ の因子は

$$\begin{aligned}
\mathrm{div}(\Theta_{E,\mathfrak{a}}) &= -6 \sum_{P \in E[\mathfrak{a}]-O} \{(P) + (-P) - 2(O)\} \\
&= 12 \sum_{P \in E[\mathfrak{a}]-O} (O) - 6 \sum_{P \in E[\mathfrak{a}]-O} (P) - 6 \sum_{P \in E[\mathfrak{a}]-O} (-P) \\
&= 12(N\mathfrak{a} - 1)(O) - 12 \sum_{P \in E[\mathfrak{a}]-O} (P) \\
&= 12N\mathfrak{a}(O) - 12 \sum_{P \in E[\mathfrak{a}]} (P)
\end{aligned}$$

と計算できる. □

Theorem 2.13

E/K を楕円曲線, $\mathfrak{a} \leq \mathcal{O}_K$ を 6 と互いに素なイデアル, $\mathfrak{b} \leq \mathcal{O}_K$ を $(\mathfrak{a}, \mathfrak{b}) = 1$ である非自明なイデアルとする. $\mathfrak{b}$ の $\mathcal{O}_K$ 加群としての生成元を β とする. このとき任意の $X \in E(\mathbb{C})$ に対して

$$\prod_{R \in E[\mathfrak{b}]} \Theta_{E,\mathfrak{a}}(X+R) = \Theta_{E,\mathfrak{a}}(\beta X)$$

が成り立つ.

Proof. Lemma 2.12 を用いることで両辺の因子が等しいことが分かる．実際,

$$\begin{aligned}
\operatorname{div}\left(\prod_{R\in E[\mathfrak{b}]}\Theta_{E,\mathfrak{a}}(X+R)\right) &= \sum_{R\in E[\mathfrak{b}]}\operatorname{div}(\Theta_{E,\mathfrak{a}}\circ\tau_R(X)) \\
&= \sum_{R\in E[\mathfrak{b}]}\operatorname{div}(\tau_R^*\Theta_{E,\mathfrak{a}}(X)) \\
&= \sum_{R\in E[\mathfrak{b}]}\tau_R^*\operatorname{div}(\Theta_{E,\mathfrak{a}}(X)) \\
&= \sum_{R\in E[\mathfrak{b}]}\tau_R^*\left(12N\mathfrak{a}(O)-12\sum_{P\in E[\mathfrak{a}]}(P)\right) \\
&= \sum_{R\in E[\mathfrak{b}]}\left(12N\mathfrak{a}(-R)-12\sum_{P\in E[\mathfrak{a}]}(P-R)\right) \\
&= 12N\mathfrak{a}\sum_{R\in E[\mathfrak{b}]}(R)-12\sum_{Q\in E[\mathfrak{a}\mathfrak{b}]}(Q) \\
\operatorname{div}(\Theta_{E,\mathfrak{a}}(\beta X)) &= \beta^*\operatorname{div}(\Theta_{E,\mathfrak{a}}(X)) \\
&= \beta^*\left(12N\mathfrak{a}(O)-12\sum_{P\in E[\mathfrak{a}]}(P)\right) \\
&= 12N\mathfrak{a}\sum_{R\in E[\mathfrak{b}]}(R)-12\sum_{P\in E[\mathfrak{a}]}\sum_{R\in\beta^{-1}P}(R) \\
&= 12N\mathfrak{a}\sum_{R\in E[\mathfrak{b}]}(R)-12\sum_{Q\in E[\mathfrak{a}\mathfrak{b}]}(Q)
\end{aligned}$$

となる．$\Theta_{E,\mathfrak{a}}$ は K 上の有理関数なので, 主張の等式は λ 倍 $(\lambda\in K^\times)$ しか違わない．よって

$$\begin{aligned}
\lambda &:= \frac{\prod_{R\in E[\mathfrak{b}]}\Theta_{E,\mathfrak{a}}(X+R)}{\Theta_{E,\mathfrak{a}}(\beta X)} \\
&= \frac{\prod_{R\in E[\mathfrak{b}]}\gamma^{-12}\Delta(E)^{N\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]-O}(x(X+R)-x(P))^{-6}}{\gamma^{-12}\Delta(E)^{N\mathfrak{a}-1}\prod_{P\in E[\mathfrak{a}]-O}(x(\beta X)-x(P))^{-6}} \\
&= \frac{\Delta(E)^{(N\mathfrak{a}-1)N\mathfrak{b}-(N\mathfrak{a}-1)}}{\gamma^{12N\mathfrak{b}-12}}\frac{\prod_{R\in E[\mathfrak{b}]}\prod_{P\in E[\mathfrak{a}]-O}(x(X+R)-x(P))^{-6}}{\prod_{P\in E[\mathfrak{a}]-O}(x(\beta X)-x(P))^{-6}}
\end{aligned}$$

とおき, $\lambda=1$ を示せばよい．特に λ が定数であることは分かっているので一点 X での値を見ればよく, $X\to O$ とすると

$$\begin{aligned}
\lambda &= \frac{\Delta(E)^{(N\mathfrak{a}-1)(N\mathfrak{b}-1)}}{\gamma^{12(N\mathfrak{b}-1)}}\frac{\prod_{R\in E[\mathfrak{b}]}\prod_{P\in E[\mathfrak{a}]-O}(x(R)-x(P))^{-6}}{\prod_{P\in E[\mathfrak{a}]-O}(x(\beta O)-x(P))^{-6}} \\
&= \frac{\Delta(E)^{(N\mathfrak{a}-1)(N\mathfrak{b}-1)}}{\gamma^{12(N\mathfrak{b}-1)}}\prod_{P\in E[\mathfrak{a}]-O}(x(O)-x(P))^{-6}\frac{\prod_{R\in E[\mathfrak{b}]-O}\prod_{P\in E[\mathfrak{a}]-O}(x(R)-x(P))^{-6}}{\prod_{P\in E[\mathfrak{a}]-O}(x(\beta O)-x(P))^{-6}} \\
&= \frac{\Delta(E)^{(N\mathfrak{a}-1)(N\mathfrak{b}-1)}}{\gamma^{12(N\mathfrak{b}-1)}}\prod_{P\in E[\mathfrak{a}]-O}\left(\frac{x(O)-x(P)}{x(\beta O)-x(P)}\right)^{-6}\prod_{\substack{P\in E[\mathfrak{a}]-O\\ R\in E[\mathfrak{b}]-O}}(x(R)-x(P))^{-6}
\end{aligned}$$

となる．ここで $(x(O)-x(P))/(x(\beta O)-x(P))$ を正確に計算する．$P\neq O$ であるから $\lim_{X\to O}x(X)/x(\beta X)$ を計算すればよい．形式群のところで $X=(x,y)$ をパラメータ z で展開すると $x(z)=1/z^2+\dots$ となったことを思い出すと,

$$\lim_{X\to O}\frac{x(X)}{x(\beta X)}=\lim_{z\to 0}\frac{\dfrac{1}{z^2}+\dots}{\dfrac{1}{(\beta z+\dots)^2}+\dots}=\beta^2$$

を得る．よって

$$\lambda=\frac{\Delta(E)^{(N\mathfrak{a}-1)(N\mathfrak{b}-1)}}{\gamma^{12(N\mathfrak{b}-1)}\beta^{12(N\mathfrak{a}-1)}}\prod_{\substack{P\in E[\mathfrak{a}]-O\\ R\in E[\mathfrak{b}]-O}}(x(R)-x(P))^{-6}$$

を得る．Theorem 2.9 の証明と同様にして $\lambda \in K^\times$ は global unit, すなわち $\lambda \in \mathcal{O}_K^\times$ が示せる．

任意の K の有限素点 $\mathfrak{p}$ を固定し，その正規化付値を v, そして $\bar{K}$ まで延長したものも v と書くことにする．$m = v(\beta)$ とする．また，$\mathfrak{p}$ で good reduction となる E/K の model を取ってよいので $v(\Delta(E)) = 0$ としてよい．このとき

$$\begin{aligned} v(\lambda) &= (N\mathfrak{a}-1)(N\mathfrak{b}-1)v(\Delta(E)) - 12(N\mathfrak{b}-1)v(\gamma) - 12(N\mathfrak{a}-1)v(\beta) - 6\sum_{\substack{P\in E[\mathfrak{a}]-O\\ R\in E[\mathfrak{b}]-O}} v(x(R)-x(P)) \\ &= -12(N\mathfrak{b}-1)n - 12(N\mathfrak{a}-1)m - 6\sum_{\substack{P\in E[\mathfrak{a}]-O\\ R\in E[\mathfrak{b}]-O}} v(x(R)-x(P)) \end{aligned}$$

と計算できる．まず $\mathfrak{p} \nmid \mathfrak{a}$ のときを考える．このとき

$$\begin{aligned} \sum_{R\in E[\mathfrak{b}]-O} v(x(R)-x(P)) &= \sum_{R\in E[\mathfrak{p}^a]-O} v(x(R)-x(P)) + \sum_{R\in E[\mathfrak{b}]-E[\mathfrak{p}^m]} v(x(R)-x(P)) \\ &= \sum_{a=1}^{m}\sum_{R\in E[\mathfrak{p}^a]-E[\mathfrak{p}^{a-1}]} v(x(R)-x(P)) + \sum_{R\in E[\mathfrak{b}]-E[\mathfrak{p}^m]} v(x(R)-x(P)) \\ &= \sum_{a=1}^{m}\sum_{R\in E[\mathfrak{p}^a]-E[\mathfrak{p}^{a-1}]} \frac{-2}{N\mathfrak{p}^a - N\mathfrak{p}^{a-1}} \\ &= \sum_{a=1}^{m}(N\mathfrak{p}^a - N\mathfrak{p}^{a-1})\frac{-2}{N\mathfrak{p}^a - N\mathfrak{p}^{a-1}} \\ &= -2m \end{aligned}$$

であり，$n = v(\gamma) = 0$ であるから

$$v(\lambda) = -12(N\mathfrak{b}-1)n - 12(N\mathfrak{a}-1)m + 12(N\mathfrak{a}-1)m = 0$$

を得る．次に $\mathfrak{p}|\mathfrak{a}$ のときを考える．このとき $(\mathfrak{a},\mathfrak{b}) = 1$ より $\mathfrak{p} \nmid \mathfrak{b}$ であるから，先程行った $\sum_{P\in E[\mathfrak{a}]-O, R\in E[\mathfrak{b}]-O}$ の部分の計算を $\mathfrak{a}$ と $\mathfrak{b}$ で入れ替えることで全く同様の計算ができる．

$\omega_K := \#\mathcal{O}_K^\times$ とおき，ある $\varepsilon \in K^\times$ を用いて $\lambda = \varepsilon^{\omega_K}$ と書けることを示せば，$\varepsilon \in \mathcal{O}_K^\times$ かつ $\lambda = 1$ を得る．まず

$$\varepsilon = \frac{\Delta(E)^{(N\mathfrak{a}-1)(N\mathfrak{b}-1)/\omega_K}}{\gamma^{12(N\mathfrak{b}-1)/\omega_K}\beta^{12(N\mathfrak{a}-1)/\omega_K}} \prod_{\substack{P\in(E[\mathfrak{a}]-O)/\pm 1\\ R\in E[\mathfrak{b}]-O}} (x(R)-x(P))^{-12/\omega_K}$$

とおけば $\lambda = \varepsilon^{\omega_K}$ が成り立つ．あとは $\varepsilon \in K^\times$ であること，すなわち ε の各因子の指数が整数ならばよい．K は虚二次体なので $\omega_K | 12$ であることは明らか．まず $\omega_K = 2$, すなわち $K \neq \mathbb{Q}(i), \mathbb{Q}(\omega)$ のときは，$(\mathfrak{a}, 6) = 1$ より $\omega_K | (N\mathfrak{a}-1)$ がすぐ分かる．$\omega_K = 4$, すなわち $K = \mathbb{Q}(i)$ のときは $\mathfrak{a} = (a+bi)$ とおき $\mathfrak{a}$ と 6 が互いに素なので $(a,b) \equiv (0,1), (1,0) \bmod 2$ しかなく，$N\mathfrak{a}-1$ を直接計算することにより示せる．$K = \mathbb{Q}(\omega)$ も同様である． □

Lemma 2.14

$\mathfrak{b} \le \mathcal{O}_K$ を $\mathfrak{a}$ と互いに素な非自明なイデアル，$Q \in E[\mathfrak{b}]$ を位数がちょうど $\mathfrak{b}$ の点とする．$\mathfrak{c} \le \mathcal{O}_K$ が $\mathfrak{b}$ と互いに素なイデアルならば $\sigma_\mathfrak{c} = (\mathfrak{c}, K(\mathfrak{b})/K)$ は以下を満たす．

$$\Theta_{E,\mathfrak{a}}(Q)^{\sigma_\mathfrak{c}} = \Theta_{E,\mathfrak{a}}(cQ)$$

ここで $c \in \mathcal{O}_K$ は $\mathfrak{c}$ の $\mathcal{O}_K$ 加群としての生成元である．

Proof. まず $\Theta_{E,\mathfrak{a}}$ は E の同型類に依らなかったので E は K 上定義されているとしてよい．したがって $\Theta_{E,\mathfrak{a}}(Q)^{\sigma_\mathfrak{c}} = \Theta_{E,\mathfrak{a}}^{\sigma_\mathfrak{c}}(Q^{\sigma_\mathfrak{c}}) = \Theta_{E,\mathfrak{a}}(Q^{\sigma_\mathfrak{c}})$ であるから，$\Theta_{E,\mathfrak{a}}(Q^{\sigma_\mathfrak{c}}) = \Theta_{E,\mathfrak{a}}(cQ)$ を示せばよい．類体論より $[x, K]|_{K(\mathfrak{b})} = \sigma_\mathfrak{c}$ となるように，有限イデール $x \in \mathbb{A}_K^\times$ で，$\mathfrak{p}|\mathfrak{b}$ となる有限素点 $\mathfrak{p}$ に対して $x_\mathfrak{p} = 1$ かつ $\mathfrak{I}(x) = \mathfrak{c}$ となるものを取ることができる．

大域類体論のイデール ver. より写像

$$C_K \overset{[,K]}{\twoheadrightarrow} G(K^{ab}/K) \overset{\mathrm{res}}{\twoheadrightarrow} G(K(\mathfrak{b})/K)$$

を得る．この写像の $\sigma_{\mathfrak{c}} \in G(K(\mathfrak{b})/K)$ の引き戻しの一つを $x \in C_K$ とすれば，$[x, K]|_{K(\mathfrak{b})} = \sigma_{\mathfrak{c}}$ とできる．さらに

$$(G(K(\mathfrak{b})/K) \simeq)\, \mathbb{A}_K^\times / K^\times \left(\prod_{\mathfrak{p} \nmid \mathfrak{b}} U_{\mathfrak{p}}^{(0)} \prod_{\mathfrak{p} | \mathfrak{b}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \right) \simeq I_{\mathfrak{b}} / S_{\mathfrak{b}}$$

という同型があった．この同型において

$$[x, K]|_{K(\mathfrak{b})} \mapsto [(x_{\mathfrak{p}})_{\mathfrak{p}}] \mapsto [\mathfrak{I}(x)]$$

と対応するから，$[\mathfrak{c}] = [\mathfrak{I}(x)]$ が成り立つ．特に $K^\times \left(\prod_{\mathfrak{p} \nmid \mathfrak{b}} U_{\mathfrak{p}}^{(0)} \prod_{\mathfrak{p} | \mathfrak{b}} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \right)$ の元をかけても同値類は変わらないので，$\mathfrak{p} | \mathfrak{b}$ なる $\mathfrak{p}$ に対して $x_{\mathfrak{p}} = 1$ となる $x \in \mathbb{A}_K^\times$ を用いて $[\mathfrak{c}] = [\mathfrak{I}(x)]$ が成り立つとしてよい．よって $\mathfrak{c}$ と $\mathfrak{I}(x)$ は $s\mathcal{O}_K$ 倍 ($s \equiv 1 \bmod \mathfrak{b}$) だけ異なる．$\sigma_{\mathfrak{c}}$ の引き戻し x は $K^\times$ だけのあいまいさがあるので，$s^{-1}x$ を改めて x と取ることにすれば $\mathfrak{c} = \mathfrak{I}(x)$ が成り立つとしてよい．

Proposition 1.16 において $F = K$ として適用すれば $\alpha_{E/K}(x)\mathcal{O}_K = \mathfrak{I}(x) = \mathfrak{c}$ を得，さらに可換図式

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "\alpha_{E/K}(x)x^{-1}"'] & E(K^{ab}) \arrow[d, "{[x,K]}"] \\ K/\mathfrak{a} \arrow[r, "\xi"] & E(K^{ab}) \end{tikzcd}$$

を得る．ここで，点 Q は位数が $\mathfrak{b}$ なので x^{-1} 倍写像は $E[\mathfrak{b}]$ において恒等写像である．

正確に記述する．x 倍写像の定義

$$\begin{tikzcd} \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\cdot x"] \arrow[d, "\simeq"] & \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \arrow[d, "\simeq"] \\ \oplus_{\mathfrak{p}} \mathfrak{b}_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \arrow[r, "(\cdot x_{\mathfrak{p}})_{\mathfrak{p}}"] & \oplus_{\mathfrak{p}} \mathfrak{b}_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \end{tikzcd}$$

を思い出す．このとき x 倍写像が恒等写像であるためには $\mathfrak{b}$ を割る有限素点 $\mathfrak{p}$ に対して $x_{\mathfrak{p}}$ 倍写像が恒等写像であることを示せばよい．しかしこれは $x_{\mathfrak{p}}$ の取り方，つまり $\mathfrak{p} | \mathfrak{b}$ となる有限素点 $\mathfrak{p}$ に対して $x_{\mathfrak{p}} = 1$ となるように取っていたので ok.

したがって

$$\Theta_{E,\mathfrak{a}}(Q^{[x,K]}) = \Theta_{E,\mathfrak{a}}(\alpha_{E/K}(x)Q) = \Theta_{E,\mathfrak{a}}(ucQ) = \Theta_{E,\mathfrak{a}}(cQ)$$

を得る．ただし $\alpha_{E/K}(x)\mathcal{O}_K = \mathfrak{c}$ より，ある $u \in \mathcal{O}_K^\times$ が存在し $\alpha_{E/K}(x) = uc$ が成り立ち，そして $\Theta_{E,\mathfrak{a}} \circ [u] = \Theta_{E,\mathfrak{a}}$ であることに注意する．

$Q^{[x,K]} = \alpha(x)Q$ をちゃんと証明する．同型 $\xi : \mathbb{C}/\mathfrak{a} \simeq E(\mathbb{C})$ を固定する．このとき可換図式

$$\begin{tikzcd} \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "\alpha(x)x^{-1}"'] & E[\mathfrak{b}] \arrow[d, "{[x,K]}"] \\ \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] & E[\mathfrak{b}] \end{tikzcd}$$

が成り立っている．ただし x^{-1} 倍写像は恒等写像であったことに注意．ξ は $\mathcal{O}_K$ 加群の準同型であるから

$$Q^{[x,K]} = \xi \circ \alpha(x) \text{ 倍} \circ \xi^{-1}(Q) = \xi\left(\xi^{-1}(\alpha(x)Q)\right) = \alpha(x)Q$$

となる．

□

Corollary 2.15

$\mathfrak{b} \le \mathcal{O}_K$ を $\mathfrak{a}$ と互いに素なイデアル, $Q \in E[\mathfrak{b}]$ を位数がちょうど $\mathfrak{b}$ の点とする. $\mathfrak{p} \le \mathcal{O}_K$ を $\mathfrak{b}$ を割る素イデアル, $\pi \in \mathcal{O}$ をその生成元の一つとする. $\mathfrak{b}' := \mathfrak{b}/\mathfrak{p} \le \mathcal{O}_K$ は非自明なイデアルであるとする. このとき

$$N_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \begin{cases} \Theta_{E,\mathfrak{a}}(\pi Q) & (\mathfrak{p}|\mathfrak{b}') \\ \Theta_{E,\mathfrak{a}}(\pi Q)^{1-\mathrm{Frob}_\mathfrak{p}^{-1}} & (\mathfrak{p} \nmid \mathfrak{b}') \end{cases}$$

が成り立つ. ここで $\mathrm{Frob}_\mathfrak{p} = (\mathfrak{p}, K(\mathfrak{b}')/K)$ である.

Proof. 今までと同様に, E は K 上定義されていると仮定してよい. さらに大域類体論のイデール ver. から同型

$$G(K(\mathfrak{b})/K) \simeq \mathbb{A}_K^\times / K^\times \left(\prod_{\mathfrak{p} \nmid \mathfrak{b}} U_\mathfrak{p}^{(0)} \times \prod_{\mathfrak{p}|\mathfrak{b}} U_\mathfrak{p}^{(n_\mathfrak{p})} \right)$$

が成り立っていたことを思い出すと,

$$G(K(\mathfrak{b})/K(\mathfrak{b}')) \simeq \left(\prod_{\mathfrak{p} \nmid \mathfrak{b}'} U_\mathfrak{p}^{(0)} \times \prod_{\mathfrak{p}|\mathfrak{b}'} U_\mathfrak{p}^{(n_\mathfrak{p})} \right) \Big/ \left(\prod_{\mathfrak{p} \nmid \mathfrak{b}} U_\mathfrak{p}^{(0)} \times \prod_{\mathfrak{p}|\mathfrak{b}} U_\mathfrak{p}^{(n_\mathfrak{p})} \right) \simeq U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}$$

が成り立つ. ここで $n = v_\mathfrak{p}(\mathfrak{b}')$ である.

> $n_0 = v_{\mathfrak{p}_0}(\mathfrak{b}')$, すなわち $\mathfrak{b} = \mathfrak{p}_0 \cdot \mathfrak{b}' = \mathfrak{p}_0 \cdot (\mathfrak{p}_0^{n_0}\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_m^{n_m})$ と素イデアル分解されているとする. $n_0 = 0$ ならば
>
> $$\frac{\prod_{\mathfrak{p} \nmid \mathfrak{b}'} U_\mathfrak{p}^{(0)} \times \prod_{\mathfrak{p}|\mathfrak{b}'} U_\mathfrak{p}^{(n_\mathfrak{p})}}{\prod_{\mathfrak{p} \nmid \mathfrak{b}} U_\mathfrak{p}^{(0)} \times \prod_{\mathfrak{p}|\mathfrak{b}} U_\mathfrak{p}^{(n_\mathfrak{p})}} = \frac{\prod_{i=0} U_{\mathfrak{p}_i}^{(0)} \times \prod_{i=1}^m U_{\mathfrak{p}_i}^{(n_i)}}{\{1\} \times \prod_{i=0}^m U_{\mathfrak{p}_i}^{(n_i)}} = \frac{U_{\mathfrak{p}_0}^{(0)}}{U_{\mathfrak{p}_0}^{(1)}}$$
>
> となる. $n_0 \ge 1$ ならば
>
> $$\frac{\prod_{\mathfrak{p} \nmid \mathfrak{b}'} U_\mathfrak{p}^{(0)} \times \prod_{\mathfrak{p}|\mathfrak{b}'} U_\mathfrak{p}^{(n_\mathfrak{p})}}{\prod_{\mathfrak{p} \nmid \mathfrak{b}} U_\mathfrak{p}^{(0)} \times \prod_{\mathfrak{p}|\mathfrak{b}} U_\mathfrak{p}^{(n_\mathfrak{p})}} = \frac{\{1\} \times \prod_{i=0}^m U_{\mathfrak{p}_i}^{(n_i)}}{\{1\} \times \prod_{i=0}^m U_{\mathfrak{p}_i}^{(n_i)}} = \frac{U_{\mathfrak{p}_0}^{(n_0)}}{U_{\mathfrak{p}_0}^{(n_0+1)}}$$
>
> となる.

よって求めるものは

$$N_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \prod_{x \in U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}} \Theta_{E,\mathfrak{a}}(Q^{[x,K]})$$

となる. ただし積は $U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}$ の代表元を渡る. 同型 $\xi : \mathbb{C}/\mathfrak{a} \simeq E(\mathbb{C})$ を固定すると, Proposition 1.16 より $[x, K]$ の $E[\mathfrak{b}]$ への作用は, $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ への $\alpha(x)x^{-1}$ 倍写像に変換されるのであった. ここで,

$$\alpha(x)\mathcal{O}_K = \mathfrak{I}(x) = \mathcal{O}_K \quad (\because x \in U_\mathfrak{p}^{(n)})$$

であるから $\alpha(x) \in \mathcal{O}_K^\times$, すなわち $\alpha(x) \in \mathrm{Aut}(E)$ である. よって $Q = f(t)$ となる $t \in \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a}$ を取ると,

$$\Theta_{E,\mathfrak{a}}(Q^{[x,K]}) = \Theta_{E,\mathfrak{a}}(\alpha(x)f(x^{-1}t)) = \Theta_{E,\mathfrak{a}}(f(x^{-1}t))$$

を得る. 分解 $\mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} = \oplus_{\mathfrak{q}|\mathfrak{b}} (\mathfrak{b}_\mathfrak{q})^{-1}\mathfrak{a}_\mathfrak{q}/\mathfrak{a}_\mathfrak{q}$ において $t = (t_\mathfrak{q})_\mathfrak{q}$ と対応しているとすると, x^{-1} 倍写像は $\mathfrak{p}$ 成分にのみしか影響を与えないから,

$$x^{-1}t = (x_\mathfrak{q}^{-1}t_\mathfrak{q})_\mathfrak{q}, \quad x_\mathfrak{q}^{-1}t_\mathfrak{q} = \begin{cases} t_\mathfrak{q} & (\mathfrak{q} \ne \mathfrak{p}) \\ x_\mathfrak{p}^{-1}t_\mathfrak{p} = t_\mathfrak{p} + t_\mathfrak{p}(x_\mathfrak{p}^{-1} - 1) & (\mathfrak{q} = \mathfrak{p}) \end{cases} \tag{5}$$

となる. したがって

$$f(x^{-1}t) = f((x_\mathfrak{p}^{-1}t_\mathfrak{p})_\mathfrak{p}) = f(t_{\mathfrak{q}_1}, t_{\mathfrak{q}_2}, \ldots, t_\mathfrak{p} + t_\mathfrak{p}(x_\mathfrak{p}^{-1} - 1), t_{\mathfrak{q}_m}, \ldots) = f((t_\mathfrak{q})_\mathfrak{q}) + f(t_\mathfrak{p}(x_\mathfrak{p}^{-1} - 1)) =: Q + R$$

を得る. t は位数が $\mathfrak{b}$ であるから $x^{-1}t$ も位数 $\mathfrak{b}$ で, したがって $Q + R$ も位数 $\mathfrak{b}$ である. さらに $x_\mathfrak{p} \in U_\mathfrak{p}^{(n)}$ より $R \in E[\mathfrak{p}]$ が分かる.

$\pi \in \mathfrak{p}$ に対して $\pi t_\mathfrak{p}(x_\mathfrak{p}^{-1}-1) \in \mathfrak{b}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$ を示せばよい．$x_\mathfrak{p}^{-1} \equiv 1 \bmod \mathfrak{p}^n$ であるから，ある $\beta \in \mathcal{O}_\mathfrak{p}$ を用いて $x_\mathfrak{p}^{-1}-1 = \pi^n\beta$ と書ける．したがって $\pi^{n+1}t_\mathfrak{p}\beta \in \mathfrak{b}_\mathfrak{p}\mathfrak{a}_\mathfrak{p}$ を示せばよい．$\mathrm{ord}_\mathfrak{p}(\mathfrak{b}) = n+1$ であるから $\pi^{n+1}\beta \in \mathfrak{b}_\mathfrak{p} = \mathfrak{b}\mathcal{O}_\mathfrak{p}$ は ok．さらに $t_\mathfrak{p}$ はそもそも $\mathfrak{a}_\mathfrak{p}$ の元である．ok.

さらに式 (5) をみることで，x を異なる同値類で取り替えれば点 R も異なることが容易に分かる．あとは $Q+R$ を計算すればよい.

$n \geq 1$ のとき．$\#(U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}) = N\mathfrak{p} = \#E[\mathfrak{p}]$ であることが知られている．このとき distribution relation を用いて

$$\prod_{x \in U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}} \Theta_{E,\mathfrak{a}}(Q^{[x,K]}) = \prod_{R \in E[\mathfrak{p}]} \Theta_{E,\mathfrak{a}}(P+R) = \Theta_{E,\mathfrak{a}}(\pi P)$$

を得る．$n=0$ のとき $\#(U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}) = N\mathfrak{p}-1$ であることが知られている．式 (5) より $Q^{[x,K]}$ は位数がちょうど $\mathfrak{b}$ であるから $Q+R$ も位数がちょうど $\mathfrak{b}$ である．よって $Q+R \notin E[\mathfrak{b}']$ である．しかし $\#(U_\mathfrak{p}^{(n)}/U_\mathfrak{p}^{(n+1)}) = N\mathfrak{p}-1 = E[\mathfrak{p}]-1$ より，ある $R_0 \in E[\mathfrak{p}]$ が存在して $Q+R_0 \in E[\mathfrak{b}']$ が成り立つ．このとき distribution relation から

$$N_{K(\mathfrak{b})/K(\mathfrak{b}')}\Theta_{E,\mathfrak{a}}(Q) = \prod_{R_0 \neq R \in E[\mathfrak{p}]} \Theta_{E,\mathfrak{a}}(P+R) = \Theta_{E,\mathfrak{a}}(\pi Q)/\Theta_{E,\mathfrak{a}}(Q+R_0) \tag{6}$$

を得る．今 $\mathfrak{b}'$ が非自明であるという仮定から Lemma 2.14 を用いることで

$$\Theta_{E,\mathfrak{a}}(Q+R_0)^{\mathrm{Frob}_\mathfrak{p}} = \Theta_{E,\mathfrak{a}}(\pi(Q+R_0)) = \Theta_{E,\mathfrak{a}}(\pi Q)$$

が成り立つ．つまり $\Theta_{E,\mathfrak{a}}(Q+R_0) = \Theta_{E,\mathfrak{a}}(\pi Q)^{\mathrm{Frob}_\mathfrak{p}^{-1}}$ を得る．これを式 (6) に代入すれば ok. □

参考文献

[1] Alexandre Daoud, *The Coates-Wiles Theorem.*

[2] Magma, *Computational Algebra System*, http://magma.maths.usyd.edu.au/magma/.

[3] Roset, *???*

[4] Karl Rubin, *Elliptic Curves with Complex Multiplication and the Conjecture of Birch and Swinnerton-Dyer.*

[5] Silverman, *AEC.*

[6] Silverman, *Adv.*