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.

```
1 E:=EllipticCurve([-1,0]);
2 > HasComplexMultiplication(E);
3 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 $\omega = fdx$ 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
>
> $$(\phi^*\omega)^\sigma = (\phi^* f dx)^\sigma = (f \circ \phi\ d(x \circ \phi))^\sigma = (f \circ \phi)^\sigma\ d(x \circ \phi)^\sigma = f^\sigma \circ \phi^\sigma\ d(x^\sigma \circ \phi^\sigma)$$
> $$(\phi^\sigma)^*\omega^\sigma = (\phi^\sigma)^* f^\sigma dx^\sigma = f^\sigma \circ \phi^\sigma\ d(x^\sigma \circ \phi^\sigma)$$
>
> 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 $\sigma = \mathrm{id}$ 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);
[ (0.00000000000000000000000000000000 : 1.00000000000000000000000000000000 :
0.00000000000000000000000000000000), (-2.41421356237309504880168872421 :
3.41421356237309504880168872421*i : 1.00000000000000000000000000000000),
(-1.00000000000000000000000000000000 : 0.00000000000000000000000000000000 :
1.00000000000000000000000000000000), (-0.41421356237309504880168724210 :
0.58578643762690495119831127579 0 : 1.00000000000000000000000000000000),
(0.00000000000000000000000000000000 : 0.00000000000000000000000000000000 :
1.00000000000000000000000000000000), (0.41421356237309504880168724210 :
0.58578643762690495119831127579 0*i : 1.00000000000000000000000000000000),
(1.00000000000000000000000000000000 : 0.00000000000000000000000000000000 :
1.00000000000000000000000000000000), (2.41421356237309504880168872421 :
3.41421356237309504880168872421 : 1.00000000000000000000000000000000),
(-1.00000000000000000000000000000000*i : -1.00000000000000000000000000000000 -
1.00000000000000000000000000000000*i : 1.00000000000000000000000000000000),
(-1.00000000000000000000000000000000*i : 1.00000000000000000000000000000000 +
1.00000000000000000000000000000000*i : 1.00000000000000000000000000000000),
(1.00000000000000000000000000000000*i : -1.00000000000000000000000000000000 +
1.00000000000000000000000000000000*i : 1.00000000000000000000000000000000),
(1.00000000000000000000000000000000*i : 1.00000000000000000000000000000000 -
1.00000000000000000000000000000000*i : 1.00000000000000000000000000000000) ]
```

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.

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E(\mathbb{C}) \\ {\scriptstyle x^{-1}}\downarrow & & \downarrow{\scriptstyle \sigma} \\ K/x^{-1}\mathfrak{a} & \xrightarrow{\xi'} & E^\sigma(\mathbb{C}) \end{array}$$

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.

```
1 > P<x>:=PolynomialRing(Integers());
2 > K:=NumberField(x^2+1);
3 > H:=HilbertClassField(K);
4 > E:=EllipticCurve([-1,0]);
5 > j:=jInvariant(E);
6 > j;
7 1728
8 > H;
9 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 $\mathcal{O}$ の有限素点を渡り, $\mathfrak{a}_{\mathfrak{p}} := \mathfrak{a}\mathcal{O}_{\mathfrak{p}}$ である.

Proof. あとで Silverman を見てみる. □

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 $\mathfrak{b}_{\mathfrak{p}}$ 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

$$\begin{array}{ccc} \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{\cdot x} & \mathfrak{b}^{-1}\mathfrak{a}/\mathfrak{a} \\ \downarrow \simeq & & \downarrow \simeq \\ \oplus_{\mathfrak{p}} \mathfrak{b}_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} & \xrightarrow{(\cdot x_{\mathfrak{p}})_{\mathfrak{p}}} & \oplus_{\mathfrak{p}} \mathfrak{b}_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \end{array}$$

を得る. $\mathfrak{b}$ を割る全ての素点 $\mathfrak{b}_{\mathfrak{p}}$ に対して $x_{\mathfrak{p}} \equiv 1 \bmod \mathfrak{b}_{\mathfrak{p}}$ と仮定する. このとき

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

であるから写像 $(\cdot x_{\mathfrak{p}})_{\mathfrak{p}}$ が恒等写像になり, 従って写像 $(\cdot x)$ も恒等写像である. 逆も同様にして分かる. □

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.

- $\alpha\mathcal{O}_K = \mathfrak{I}(y)$.

- $\mathfrak{a} \leq K$ 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.

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E(F^{ab}) \\ \downarrow{\scriptstyle \alpha y^{-1}} & & \downarrow{\scriptstyle [x,F]} \\ K/\mathfrak{a} & \xrightarrow{\xi} & E(F^{ab}) \end{array}$$

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

$$\begin{array}{ccc} K/\mathfrak{a} & \xrightarrow{\xi} & E(\mathbb{C}) \\ \downarrow{\scriptstyle y^{-1}} & & \downarrow{\scriptstyle \sigma} \\ K/y^{-1}\mathfrak{a} & \xrightarrow{\xi'} & E(\mathbb{C}) \end{array}$$

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, $\mathfrak{I}(y) \leq K$ 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. $\mathfrak{a} \leq K$ 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

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

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 $U \leq \mathbb{A}_F^\times$ 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.

$m \geq 3$ 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

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

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

$$\begin{array}{ccc} m^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{\xi} & E[m] \\ \downarrow{\scriptstyle \alpha y^{-1}} & & \downarrow{\scriptstyle \mathrm{id}} \\ m^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{\xi} & E[m] \end{array}$$

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

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

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

$$\begin{array}{ccccc} \oplus_{\mathfrak{p}} (m)_{\mathfrak{p}}^{-1} \mathfrak{a}_{\mathfrak{p}} / \mathfrak{a}_{\mathfrak{p}} & \xrightarrow{\simeq} & (m)^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{\xi} & E[m] \\ \downarrow{\scriptstyle \alpha N_{F/K}(x)_{\mathfrak{p}}^{-1}} & & \downarrow{\scriptstyle \alpha N_{F/K}(x)^{-1}} & & \downarrow{\scriptstyle [x,F]} \\ \oplus_{\mathfrak{p}} (m)_{\mathfrak{p}}^{-1} \mathfrak{a}_{\mathfrak{p}} / \mathfrak{a}_{\mathfrak{p}} & \xrightarrow{\simeq} & (m)^{-1}\mathfrak{a}/\mathfrak{a} & \xrightarrow{\xi} & E[m] \end{array}$$

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. □

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. □

Corollary 1.26: [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 $\mathcal{O}_K^\times \to (\mathcal{O}/\mathfrak{f})^\times$ 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. □

Corollary 1.27: [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 $\mathcal{O}_K^\times \to (\mathcal{O}/\mathfrak{p})^\times$ 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. □

Theorem 1.28: [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 $\mathfrak{p} \not| \mathfrak{f}$ を満たす素イデアルとする. このとき以下が成り立つ.

1. $E[\mathfrak{b}\mathfrak{f}] \subset K(\mathfrak{b}\mathfrak{f})$.
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 1.29: [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 $|a_{\mathfrak{P}}| \leq 2\sqrt{q_{\mathfrak{P}}}$ 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, $\prod_n a_n \ \ (^\forall n, a_n \neq 0)$ 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.

$$\sum_{\mathfrak{P}} \left| \frac{a_{\mathfrak{P}}}{q_{\mathfrak{P}}^{s}} \right| \leq \sum_{\mathfrak{P}} \frac{2q_{\mathfrak{P}}^{1/2}}{q_{\mathfrak{P}}^{\mathrm{Re}(s)}} = 2 \sum_{\mathfrak{P}} \frac{1}{q_{\mathfrak{P}}^{\mathrm{Re}(s)-1/2}} < 2 \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^{\mathrm{Re}(s)-1/2}}$$

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 1.30: [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 1.31: [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 1.32: [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 1.33: [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

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

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 1.34: [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)

$$\begin{aligned} N_{F/\mathbb{Q}}\mathfrak{P} &= \deg\phi_{\mathfrak{P}} \quad (\because [5, \text{p. 25, Proposition 2.11}]) \\ &= \deg[\widetilde{\psi_{E/F}(\mathfrak{P})}] \quad (\because \text{Proposition 1.24}) \\ &= \deg[\psi_{E/F}(\mathfrak{P})] \quad (\because \text{Proposition 1.33}) \\ &= N_{K/\mathbb{Q}}(\psi_{E/F}(\mathfrak{P})) \quad (\because [6, \text{p. 104, Corollary 1.5}]) \end{aligned}$$

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

$$\begin{aligned}
\#\tilde{E}(\mathbb{F}_\mathfrak{P}) &= \#\,\mathrm{Ker}(1-\phi_\mathfrak{P}) \\
&= \deg(1-\phi_\mathfrak{P}) \quad (\because [5, \text{p. 79, Corollary 5.5}], [5, \text{p. 72, Theorem 4.10(c)}]) \\
&= \deg[1-\widetilde{\psi_{E/F}(\mathfrak{P})}] \quad (\because \text{Proposition 1.24}) \\
&= \deg[1-\psi_{E/F}(\mathfrak{P})] \quad (\because \text{Proposition 1.33}) \\
&= N_{K/\mathbb{Q}}(1-\psi_{E/F}(\mathfrak{P})) \quad (\because [6, \text{p. 104, Corollary 1.5}]) \\
&= (1-\psi_{E/F}(\mathfrak{P}))(1-\overline{\psi_{E/F}(\mathfrak{P})}) \quad (\because \text{ノルムの定義}) \\
&= 1-\psi_{E/F}(\mathfrak{P})-\overline{\psi_{E/F}(\mathfrak{P})}+N_{F/\mathbb{Q}}(\mathfrak{P}) \quad (\because (1))
\end{aligned}$$

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 1.35: [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 1.34 より

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

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 1.36: [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 $p \not| 2D$ 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, $p \not| 2D$ 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 1.35 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 1.34 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,

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

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 1.34(3) より

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

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

$$\begin{aligned} L(E/\mathbb{Q}, s) &= \prod_{\mathfrak{p} \not| 2D} \frac{1}{1 - \overline{\left(\frac{D}{\pi}\right)_4}\pi N_{K/\mathbb{Q}}\mathfrak{p}^{-s}} \quad (\pi \equiv 1 \bmod 2 + 2i) \\ &= \sum_{\mathfrak{a}} \frac{\varepsilon(\mathfrak{a})\alpha}{N_{K/\mathbb{Q}}\mathfrak{a}^s} \quad (\mathfrak{a} = (\alpha),\ \alpha \equiv 1 \bmod 2 + 2i) \end{aligned}$$

と書ける. ただし

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

である.

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.*