

楕円曲線と超幾何級数

K : field, $\text{char}(K) = p \geq 3$.

E/K : ell. curve, $\mathcal{O}_E$: str. sheaf of E .

Frobenius 写像

$$\text{Frob}: \mathcal{O}_E \rightarrow \mathcal{O}_E, f \mapsto f^p$$

は次の p -linear map $\varepsilon \in \mathbb{Z} \mid \varepsilon \cdot \varepsilon^p = 1$.

$$\text{Frob}: H^1(E, \mathcal{O}_E) \rightarrow H^1(E, \mathcal{O}_E).$$

Def

E : supersingular $\Leftrightarrow \text{Frob} = 0$.

E : ordinary $\Leftrightarrow \text{Frob} \neq 0$.

以下では次のように、楕円曲線は Legendre form $y^2 = x(x-1)(x-\lambda)$ として与えられる:

$$E_\lambda: y^2 = x(x-1)(x-\lambda) \quad (\lambda \neq 0, 1)$$

目標: Frob: $H^1(E_\lambda, \mathcal{O}_{E_\lambda}) \rightarrow H^1(E_\lambda, \mathcal{O}_{E_\lambda})$
を計算する.

$E_\lambda \subset \mathbb{P}^2(k)$ 内に斉次座標 (x, y, z) に移す.

$$E_\lambda: y^2 z = x(x - z)(x - \lambda z).$$

$$(Rem. \ x = \frac{x}{z}, \ y = \frac{y}{z})$$

2:2"

$$U_0 = \{[x, y, z] \in \mathbb{P}^2 \mid z \neq 0\},$$

$$U_1 = \{[x, y, z] \in \mathbb{P}^2 \mid y \neq 0\}$$

2つの open sets を考え

$$V_0 = E_\lambda|_{U_0}, \quad V_1 = E_\lambda|_{U_1}$$

すなわち, $\{V_0, V_1\}$ は E_λ の affine open covering 2"ある.

この2を, 複体

$$0 \rightarrow P(V_0, \mathcal{O}_{E_\lambda}) \oplus P(V_1, \mathcal{O}_{E_\lambda}) \xrightarrow{\delta} P(V_0 \cap V_1, \mathcal{O}_{E_\lambda}) \rightarrow 0$$

$$(f_0, f_1) \mapsto f_0 - f_1$$

を考えると

$$H^1(E_\lambda, \mathcal{O}_{E_\lambda}) \cong P(V_0 \cap V_1, \mathcal{O}_{E_\lambda}) / \text{Im}(\delta)$$

が得られる.

LEM

$$(i) \frac{f}{x} \in P(V_0 \wedge V_1, \mathcal{O}_{E\lambda})$$

$$(ii) \frac{f}{x} \notin \text{Im}(\delta)$$

$$(iii) \frac{f}{x^n} \in \text{Im}(\delta) \quad (\forall n \in \mathbb{Z}_{\geq 1}).$$

pf. (i) $V_0 \wedge V_1$ は V_0 内 $x \neq 0$ で def される.

$x \neq 0$ なら, $E\lambda$ の定義式 $y^2 = x(x - \lambda x - \lambda)$ より

$x \neq 0$ である.

$$\therefore \frac{f}{x} \in P(V_0 \wedge V_1, \mathcal{O}_{E\lambda}).$$

$$(ii) \frac{f}{x} \in \text{Im}(\delta) \text{ と仮定する.}$$

$$\therefore \text{このとき } \frac{f}{x} = f_0 - f_1 \text{ とする } f_0 \in P(V_0, \mathcal{O}_{E\lambda}),$$

$$f_1 \in P(V_1, \mathcal{O}_{E\lambda}) \text{ が存在する.}$$

$\frac{f}{x}$ は無限遠点 ∞ で 1 次の極を持つ.

また f_1 は無限遠点 ∞ で正則である.

よって f_0 は無限遠点 ∞ で 1 次の極を持ち, $E\lambda$ の他の点 x は正則になる.

よって

$$\omega(\infty) = \int f \in \bar{K}(E\lambda)^{\times} \mid (\infty) + \text{div}(\omega) \geq 0 \text{ かつ } 0 \neq$$

は定数の ω になることに矛盾する.

$$\therefore \frac{y}{x} \notin \text{Im}(\delta).$$

(iii) $n \leq 0$ のとき

$$\frac{y}{x^n} \in P(V_0, \mathcal{O}_{E\lambda})$$

$$\therefore \delta\left(\frac{y}{x^n}, 0\right) = \frac{y}{x^n} - 0 = \frac{y}{x^n}$$

$n \geq 2$ のとき

$U_0 \cap U_1$ において (x, y) と (u, u) の変数変換は

$$x = \frac{u}{q_1}, \quad y = \frac{1}{q_1}$$

と与えられるので、 $E\lambda$ の定義式より

$$q_1(1 + (\lambda+1)u - \lambda u q_1) = u^3$$

より成り立つことに注意すると、次が成り立つ:

$$\frac{y}{x^n} = \frac{q_1^{n-1}}{u^n}$$

$$= \frac{u^{2n-3}}{1 + (\lambda+1)u^2 - \lambda u q_1^{n-1}} \in P(V_1, \mathcal{O}_{E\lambda})$$

$$\therefore \delta\left(0, -\frac{y}{x^n}\right) = \frac{y}{x^n} \quad \square$$

$\Rightarrow$ の Lem と同型 $H^1(E_\lambda, \mathcal{O}_{E_\lambda}) \cong P(V_0 \wedge V_1, \mathcal{O}_{E_\lambda}) / \text{Im}(\delta)$
 より、 $\frac{q}{x}$ の $H^1(E_\lambda, \mathcal{O}_{E_\lambda})$ の基底 1 個 $\Rightarrow$ $\frac{q}{x}$ の基底 1 個、 $\frac{q}{x}$

$\frac{q}{x}$ は、基底 $\frac{q}{x}$ の Frob による $\frac{q}{x}$ への写像

$$\text{Frob}\left(\frac{q}{x}\right) = \frac{q^p}{x^p}$$

$$= \frac{q}{x^p} \cdot (y^2)^{\frac{1}{2}(p-1)}$$

$$= \frac{q}{x^p} \cdot x^{\frac{1}{2}(p-1)} (x-1)^{\frac{1}{2}(p-1)} (x-\lambda)^{\frac{1}{2}(p-1)}$$

$$= \frac{q}{x} \cdot \frac{1}{x^{\frac{1}{2}p}} \cdot \left\{ \sum_{i=0}^{\frac{1}{2}(p-1)} \binom{\frac{1}{2}(p-1)}{i} x^i (-1)^{\frac{1}{2}(p-1)-i} \right\} \cdot \left\{ \sum_{i=0}^{\frac{1}{2}(p-1)} \binom{\frac{1}{2}(p-1)}{i} x^i (-\lambda)^{\frac{1}{2}(p-1)-i} \right\}$$

$$\equiv (-1)^{\frac{1}{2}(p-1)} \frac{q}{x} \underbrace{\sum_{i=0}^{\frac{1}{2}(p-1)} \binom{\frac{1}{2}(p-1)}{i}^2 \lambda^i}_{\Phi(\lambda)} \pmod{\text{Im}(\delta)}$$

$$\uparrow \quad \bigoplus_{\substack{n \in \mathbb{Z} \\ n \neq 1}} \frac{q}{x^n} \in \text{Im}(\delta) \quad \Phi(\lambda) : \text{Legendre 多項式}$$

$\frac{q}{x}$ は、

$\frac{q}{x}$

$$E_\pi : \text{SuperSingular} \Leftrightarrow \Phi(\lambda) = 0$$

$\frac{q}{x}$ の基底 1 個

Thm (Igusa)

$\chi(\lambda) = 0$ は重根を持たない.

pf. まず, $\mathbb{C}$ 上の超幾何微分方程式

$$\lambda(1-\lambda) \frac{d^2 u}{d\lambda^2} + \{c - (a+b+1)\lambda\} \frac{du}{d\lambda} - abu = 0$$

は, $\lambda = 0$ の特解 z^n

$$F(a, b, c; \lambda) = \sum_{n=0}^{\infty} \frac{\Gamma(a+n) \Gamma(b+n) \Gamma(c)}{\Gamma(a) \Gamma(b) \Gamma(c+n)} \cdot \frac{\lambda^n}{n!}$$

という正則な解を持つ z を思い出す.

$\Rightarrow$ かつ $a = b = \frac{1}{2}$, $c = 1$ を代入する:

$$\lambda(1-\lambda) \frac{d^2 u}{d\lambda^2} + (1-2\lambda) \frac{du}{d\lambda} - \frac{1}{4}u = 0,$$

$$F\left(\frac{1}{2}, \frac{1}{2}, 1; \lambda\right) = \sum_{n=0}^{\infty} \left(\frac{\frac{1}{2} + (n-1)\frac{1}{2} \cdot \frac{1}{2} + (n-2)\frac{1}{2} \cdots \frac{1}{2}}{n!} \right)^2 \cdot \lambda^n$$

$0 \leq n \leq \frac{1}{2}(p-1)$ のとき

$$\frac{\frac{1}{2} + (n-1)\frac{1}{2} \cdot \frac{1}{2} + (n-2)\frac{1}{2} \cdots \frac{1}{2}}{n!}$$

$$= \frac{\frac{1}{2} + (n-1)\frac{1}{2} \cdots \frac{1}{2} \cdot \left(\frac{p-1}{2} - n\right)!}{n! \cdot \left(\frac{p-1}{2} - n\right)!}$$

$$= \frac{(-1)^n \frac{p}{2} - \frac{1}{2} - (n-1) \cdots \left(\frac{p}{2} - \frac{1}{2}\right) \cdot \left(\frac{p-1}{2} - n\right)!}{n! \cdot \left(\frac{p-1}{2} - n\right)!}$$

(mod p)

$$\begin{aligned} &\equiv \frac{(-1)^n \left(\frac{p-1}{2}\right)!}{n! \cdot \left(\frac{p-1}{2} - n\right)!} \pmod{p} \\ &\equiv (-1)^n \binom{\frac{1}{2}(p-1)}{n} \pmod{p} \end{aligned}$$

$$\frac{1}{2}(p-1) < n < p \text{ かつ}$$

$$\frac{\frac{1}{2} + (n-1)p \cdot \frac{1}{2} + (n-2)p \cdot \dots \cdot \frac{1}{2}}{n!} \equiv 0 \pmod{p}$$

以上より、 $F(\frac{1}{2}, \frac{1}{2}, 1; \lambda)$ の degree $(p-1)$ 次以下の部分からなる多項式を $\text{mod } p$ で考えると、左は $\Phi(\lambda)$ に一致するから分かる。

また、 $\Phi(\lambda)$ は $\text{mod } p$ で考えた DE

$$\lambda(1-\lambda) \frac{d^2 u}{d\lambda^2} + (1-2\lambda) \frac{du}{d\lambda} - \frac{1}{4}u = 0 \quad (*)$$

の解がある。

すなわち、 $\Phi(\lambda) = 0$ の重根 α を持つと決定する。

具体的に計算するときは $\Phi(0) \neq 0$ かつ $\Phi(1) \neq 0$ であるから、 $\alpha \neq 0, 1$ であることを注意する。

すなわち

$$\Phi(\lambda) = (\lambda - \alpha)^m f(\lambda) \quad (m \geq 2, f(\alpha) \neq 0)$$

と表すとき、 $(*)$ に代入する。

$$\lambda(1-\lambda) \cdot \{ m(m-1)(\lambda-\alpha)^{m-2} g + 2m(\lambda-\alpha)^{m-1} g' + (\lambda-\alpha)^m g'' \} \\ + (1-2\lambda) \cdot \{ m(\lambda-\alpha)^{m-1} g + (\lambda-\alpha)^m g' \} \\ - \frac{1}{4} (\lambda-\alpha)^m g = 0.$$

$$\div (\lambda-\alpha)^{m-2} \quad \lambda(1-\lambda) \cdot \{ m(m-1)g + 2m(\lambda-\alpha)g' + (\lambda-\alpha)^2 g'' \} \\ + (1-2\lambda) \cdot \{ m(\lambda-\alpha)g + (\lambda-\alpha)^2 g' \} \\ - \frac{1}{4} (\lambda-\alpha)^2 g = 0$$

$$\lambda=\alpha \quad \leadsto \quad \alpha(1-\alpha) \cdot m(m-1)g(\alpha) = 0$$

$$\leadsto g(\alpha) = 0 \quad (\odot \alpha \neq 0, 1, m \geq 2) \\ \dots \text{矛盾.} \quad \square$$

