

やはり楕円曲線…!!楕円曲線は全てを解決する…!!

(どろ" おど")

@dorhodo

October 16, 2025

- ① 発表の前に
- ② 楕円曲線とは何か
- ③ 有限体の楕円曲線

°ρ°(どろ" おど) という意味不明な名前で YouTube とか Twitter とかやってる人.

残念ながらそれ以外に自己紹介するほどのことがない.
専門家でも何でもない量産型高校生なので注意が必要

この発表では

- K を体
- $\text{char}(K)$ を K の標数 (自然な環準同型 $\phi : \mathbb{Z} \rightarrow K$ の核 $\ker(\phi)$ の生成元で負でない最小のもの)
- p を素数
- q を p のべき

楕円曲線とは？

定義 (不完全)

$a_1, \dots, a_6 \in K$ とするとき,

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

を満たす $(x, y) \in K^2$ の組に無限遠点を加えたものを K 上の楕円曲線という.

また, $\text{char}(K) \neq 2, 3$ の場合は適切な変数変換を施すことで

$$E : y^2 = x^3 + ax + b$$

の形に書き換えることができる.

定義・改 (まだ不完全)

体 K に対し $a_1, \dots, a_6 \in K$ とするとき,

$$\begin{aligned} E : Y^2Z + a_1XYZ + a_3YZ^2 \\ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \end{aligned}$$

となる $[X, Y, Z] \in K^3$ を

$$\begin{aligned} [X, Y, Z] &\sim [X', Y', Z'] \\ \stackrel{\text{def}}{\iff} &\exists k \in K, X' = kX, Y' = kY, Z' = kZ \end{aligned}$$

という同値関係で割ったものを K 上の楕円曲線という.

先程の定義だと曲線が特異点をもっている可能性があり、その点では接線を定義することができず面倒なので少し条件を加える.

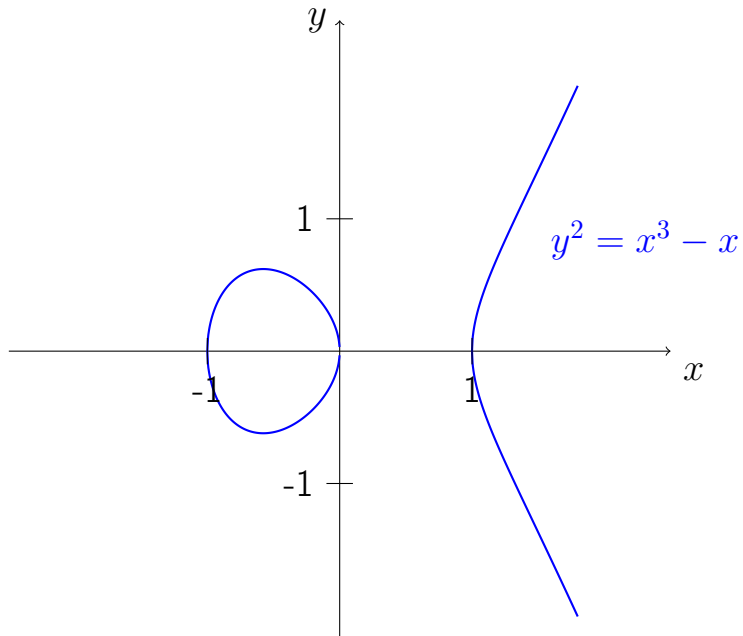
楕円曲線の判別式

($\text{char}(K) \neq 2, 3$ である K 上の) 曲線
 $E : y^2 = x^3 + ax + b$ に対し、その判別式 Δ を

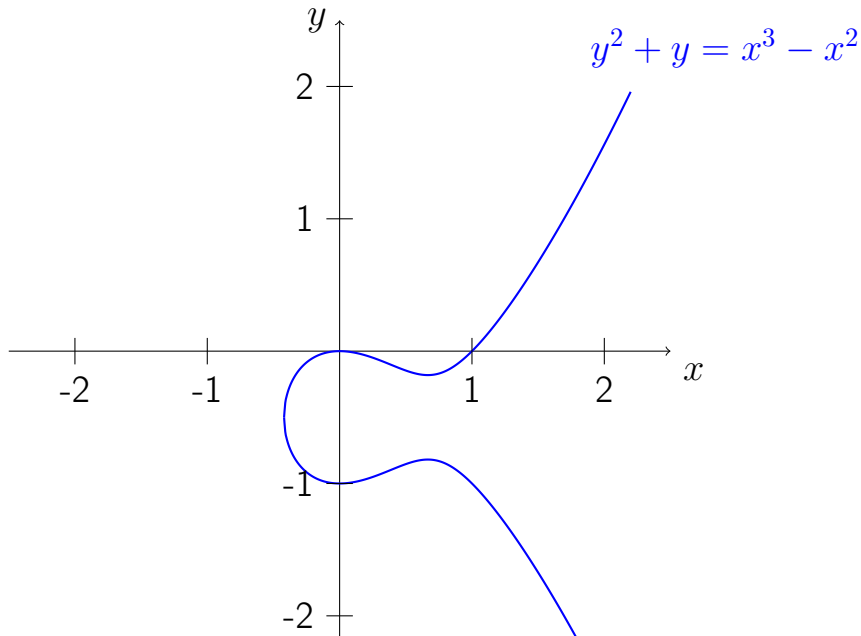
$$\Delta = -16(4a^3 + 27b^2)$$

と定義すると、 $\Delta \neq 0$ のとき、 E は特異点をもたない.

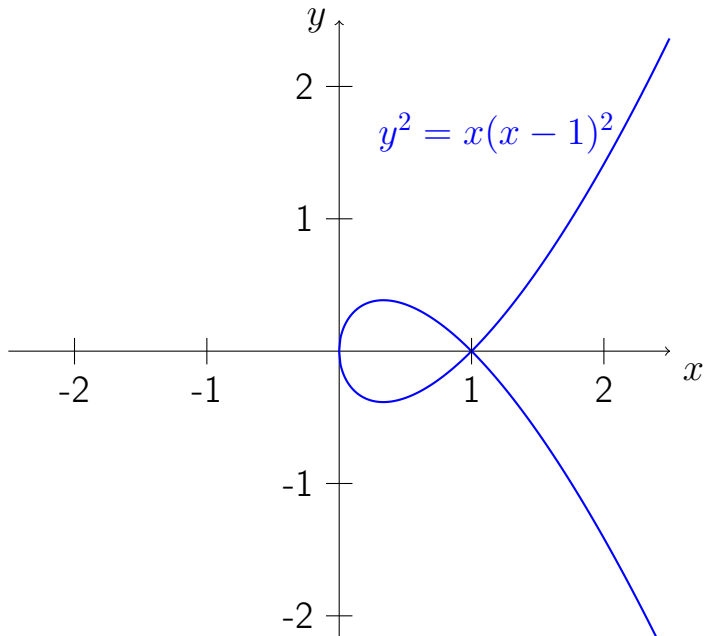
例： $y^2 = x^3 - x$



例その 2: $y^2 + y = x^3 - x^2$

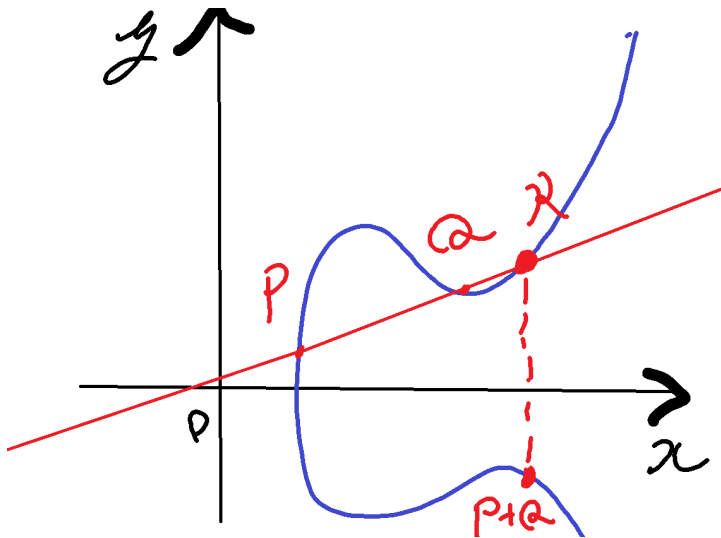


じゃない例: $y^2 = x(x - 1)^2$



K 上の楕円曲線 E 上の点 P, Q に対し, $P + Q$ は P と Q を通る直線 ($P = Q$ なら接線) と E との交点で P, Q でない点 R に対し, R と x 軸に対称な点 $-R$
無限遠点 O に対しては $P + O = P, P + (-P) = O$ のように定義すると, 一般に E はこの加法についてのアーベル群を形成

計算例



楕円曲線 $E_1 : f_1(x, y) = 0$, $E_2 : f_2(x, y) = 0$ に対しその関数体 (曲線上の有理関数のなす体) をそれぞれ

$$K(E_1) := K[x, y]/(f_1), \quad K(E_2) := K[x, y]/(f_2)$$

とすると, 楕円曲線間の写像 $\phi : E_1 \rightarrow E_2$ に対し

$$\phi^* : K(E_2) \rightarrow K(E_1), \quad \phi^* f = f \circ \phi$$

という写像が誘導される.

楕円曲線間の写像 $\phi : E_1 \rightarrow E_2$ に対し, その次数を定数なら 0, そうでないなら

$$\deg(\phi) := [K(E_1) : \phi^* K(E_2)]$$

と定義する.

- 有限体とはなにか
- Hasse の定理と証明の概要
- より一般の場合について (Weil 予想)

有限体とは？

位数が有限の体のこと. 一般にこの位数は素数 p の冪で表せる.

位数 p の有限体は

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$$

に $\text{mod } p$ での加減乗除を入れた体である.

この代数閉包 $\overline{\mathbb{F}_p}$ に対し, $\mathbb{F}_{p^n}$ を

$$\mathbb{F}_{p^n} := \{x \in \overline{\mathbb{F}_p} \mid x^{p^n} = x\}$$

と定義すると, これは位数 p^n の唯一の有限体となる.

例

$p = 3$ のときを考えてみる. このとき, 位数 3 の有限体 $\mathbb{F}_3$ とは

$$\mathbb{F}_3 = \{0, 1, 2\}$$

という集合に mod 3 での四則演算を入れた体である.
計算例

$$1 + 1 + 1 = 0$$

$$0 - 1 = 2$$

$$2 \times 2 = 1$$

$$1 \div 2 = 2$$

$\mathbb{F}_9$ を考える. これは $\mathbb{F}_3$ の 2 次拡大なので, 2 次の既約多項式 $f(x)$ の根を添加した体を考えれば, それが $\mathbb{F}_9$ である.

$f(x) = x^2 + 1$ を考えると,
 $0^2 + 1 = 1, 1^2 + 1 = 2, 2^2 + 1 = 2$ より, これは $\mathbb{F}_3$ 上既約であるので, これの $\overline{\mathbb{F}_3}$ 上の根の一つを α とおくと,

$$\mathbb{F}_9 = \{x + \alpha y \mid x, y \in \mathbb{F}_3\}$$

となる.

$$(1 + \alpha) + (1 + 2\alpha) = 2 + 3\alpha = 2$$

$$(2 + 2\alpha) - \alpha = 2 + \alpha$$

$$(1 + \alpha)(2 + \alpha) = 2 + 3\alpha + \alpha^2 = 2 + 0 - 1 = 1$$

$$1 \div (1 + 2\alpha) = 2 + 2\alpha$$

定理

p を素数, m, n を正整数とするとき, 以下が成り立つ.

- $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{mn}}$ は Galois 拡大
- $\text{Gal}(\mathbb{F}_{p^{mn}}/\mathbb{F}_{p^n}) \cong \mathbb{Z}/m\mathbb{Z}$

また, $\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$ の生成元を **Frobenius 写像** といい, Frob_q と書く.

Frobenius 写像を用いると, 位数 p^n の有限体は

$$\mathbb{F}_{p^n} = \{x \in \overline{\mathbb{F}_p} \mid \text{Frob}_p^n(x) = x\}$$

という風にも表せる.

より一般に, 写像 f に対し $f(x) = x$ となる点のことを f の不動点という.

Hasse の定理

q を素数 p の冪, E を $\mathbb{F}_q$ 上の楕円曲線とするとき, 以下が成り立つ.

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

例

$q = 5, E : y^2 = x^3 + x + 1$ のとき,
 $x^3 + x + 1$ に $x = 0 \sim 4$ を代入すると $1, 3, 1, 1, 4$
 y^2 に $y = 0 \sim 4$ を代入すると $0, 1, 4, 4, 1$
よって,

$$\#E(\mathbb{F}_5) = \{O, (0, 1), (0, 4), (2, 1), (2, 4), \\ (3, 1), (3, 4), (4, 2), (4, 3)\}$$

$$\text{なので } |5 + 1 - \#E(\mathbb{F}_5)| = |5 + 1 - 9| = 3 \leq 2\sqrt{5}$$

Tate 加群に対する Frobenius 写像の作用の表現を考える.

逆極限とは？

定義

集合 X_n ($n = 1, 2, \dots$) と写像

$f_n : X_{n+1} \rightarrow X_n$ ($n = 1, 2, \dots$) からなる系列

$$\dots \xrightarrow{f_4} X_4 \xrightarrow{f_3} X_3 \xrightarrow{f_2} X_2 \xrightarrow{f_1} X_1$$

に対し,

$$\varprojlim_n X_n := \left\{ (a_n)_{n \geq 1} \in \prod_{n \geq 1} X_n \mid \forall n \geq 1, f_n(a_{n+1}) = a_n \right\}$$

をこの系列の**逆極限** (または射影極限) という.

例 (p 進整数環)

定義

環 $\mathbb{Z}/p^n\mathbb{Z}$ ($n = 1, 2, \dots$) と自然な準同型

$f_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ ($n = 1, 2, \dots$) からなる系列

$$\dots \xrightarrow{f_4} \mathbb{Z}/p^4\mathbb{Z} \xrightarrow{f_3} \mathbb{Z}/p^3\mathbb{Z} \xrightarrow{f_2} \mathbb{Z}/p^2\mathbb{Z} \xrightarrow{f_1} \mathbb{Z}/p\mathbb{Z}$$

に対し,

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

を p 進整数環 といい, $\mathbb{Z}_p$ と書く.

- $\mathbb{Z}_p$ は整域である. ($ab = 0 \Leftrightarrow a = 0$ or $b = 0$)
- $\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\} \subset \mathbb{Z}_p$
- 任意の $x \in \mathbb{Z}_p$ は
$$x = \sum_{n=0}^{\infty} a_n p^n \quad (a_n \in \mathbb{Z} \cap [0, p-1])$$
と書ける

Galois 表現とは, ベクトル空間や環上の自由加群への絶対 Galois 群の作用を, その加群の自己準同型 (線形写像) で実現したものである.

体 K に対し, その分離閉包 $\overline{K}$ の Galois 群 $\text{Gal}(\overline{K}/K)$ を K の絶対 Galois 群といい, G_K とも書く.

例

- $G_{\mathbb{C}} = \text{Gal}(\mathbb{C}/\mathbb{C}) = 1$
- $G_{\mathbb{R}} = \text{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$

絶対 Galois 群について考えることで, K のすべての Galois 拡大について考えられる! が...

Galois 理論の基本定理が成り立たない！？

$$\{G_K \text{の部分群}\} \overset{1:1 \text{ じゃない}}{\longleftrightarrow} \{\overline{K}/K \text{の中間体}\}$$

⇒ Krull 位相という自然な位相を入れて位相群にし,

$$\{G_K \text{の閉部分群}\} \overset{1:1}{\longleftrightarrow} \{\overline{K}/K \text{の中間体}\}$$

有限体 $\mathbb{F}_q$ の絶対 Galois 群は

$$\begin{aligned} G_{\mathbb{F}_q} &= \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \varprojlim_n \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ &\cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}} \end{aligned}$$

となる.

$\hat{\mathbb{Z}}$ について

$\hat{\mathbb{Z}}$ は $\mathbb{Z}$ の副有限完備化で, $\mathbb{Z}$ を稠密な部分群として含む.
開部分群として $n\hat{\mathbb{Z}}$ を含み, $\hat{\mathbb{Z}}/n\hat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$
また,

$$\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

とも表せる.

定義

E を複素数体, 有限体, l 進体のいずれかとし, V を E 上のベクトル空間とすると, G_K の Galois 表現とは, Krull 位相において連続な準同型

$$\rho : G_K \rightarrow \mathrm{GL}(V)$$

のことである. ここで, E が複素数体と有限体の場合は離散位相を, l 進体の場合は l 進位相を入れる.

楕円曲線の等分点

m を 2 以上の整数とする. このとき, K 上の楕円曲線 E に対し, E の m 等分点 (m ねじれ点) を

$$E[m] := \{P \in E(\overline{K}) \mid mP = O\}$$

と定義する. ($\overline{K}$ は K の分離閉包)
 $\text{char}(K)$ が 0 もしくは m と互いに素のとき,

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

となる. ($\text{char}(K)$ が m と互いに素でない場合は省略.)

$P \in E[m]$ には $\sigma \in G_K$ が作用し,

$$m\sigma(P) = \sigma(mP) = \sigma(O) = O$$

となるので, 表現

$$G_K \rightarrow \text{Aut}(E[m]) \cong \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

を得るが, $\mathbb{Z}/m\mathbb{Z}$ は標数 0 でないため, 行列が扱いにくい.
そのため, p 進整数環を構成したときと同じ方法を使う.

定義

E を楕円曲線, l を素数とする. このとき,

$$T_l(E) := \varprojlim_n E[l^n]$$

を E の (l 進) Tate 加群という.

$\text{char}(K) \neq l$ なら,

$$T_l(E) \cong \varprojlim_n (\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}) = \mathbb{Z}_l \times \mathbb{Z}_l$$

先ほどと同様に

$$G_K \rightarrow \mathrm{Aut}(T_l(E)) \cong \mathrm{GL}_2(\mathbb{Z}_l)$$

という表現が得られ, 更に $\mathbb{Z}_l \subset \mathbb{Q}_l$ により,

$$\rho : G_K \rightarrow \mathrm{GL}_2(\mathbb{Q}_l)$$

という l 進表現が得られる.

定理

楕円曲線 E に対し, $\psi \in \text{End}(E)$ とすると, 表現

$$\text{End}(E) \longrightarrow \text{End}(T_l(E)), \quad \psi \longmapsto \psi_l$$

が存在し, 以下が成り立つ

$$\det(\psi_l) = \deg(\psi), \quad \text{Tr}(\psi_l) = 1 + \deg(\psi) - \deg(1 - \psi)$$

$\phi := \rho(\text{Frob}_q) \in \text{GL}_2(\mathbb{Q}_l)$ とすると,

$$\det(\phi) = \deg(\text{Frob}_q) = q$$

$$\begin{aligned} \text{Tr}(\phi) &= 1 + \deg(\text{Frob}_q) - \deg(1 - \text{Frob}_q) \\ &= q + 1 - \#\ker(1 - \text{Frob}_q) \end{aligned}$$

ここで, $\ker(1 - \text{Frob}_q) = \{P \mid P - \text{Frob}_q(P) = O\}$ となることから, $\ker(1 - \text{Frob}_q) = \#E(\mathbb{F}_q)$

$\det(\phi) = q$, $\text{Tr}(\phi) = q + 1 - \#E(\mathbb{F}_q) =: a_q$ より, ϕ の固有多項式は

$$\det(T - \phi) = T^2 - \text{Tr}(\phi)T + \det(\phi) = T^2 - a_q T + q$$

これらの根 α, β について考える.

ここで, 任意の $\frac{m}{n} \in \mathbb{Q}$ に対し,

$$\det \left(\frac{m}{n} - \phi \right) = \frac{\deg(m - n\phi)}{n^2} \geq 0$$

となるため, 有理数の稠密性より, 全ての实数 T に対し $\det(T - \phi) \geq 0$ となる.

よって, α, β は等しいか共役な複素数となる. なのでこれの絶対値は解と係数の関係より

$$\alpha\beta = q, |\alpha||\beta| = |\alpha|^2 = |\beta|^2 = q$$

$$\therefore |\alpha| = |\beta| = \sqrt{q}$$

$$\begin{aligned} |q + 1 - \#E(\mathbb{F}_q)| &= |a_q| \\ &= |-\alpha - \beta| \\ &\leq |\alpha| + |\beta| \\ &= 2\sqrt{q} \end{aligned}$$

より題意は示された.

定理

正の整数 n に対し,

$$\#E(\mathbb{F}_{q^n}) = 1 + q^n - \alpha^n - \beta^n$$

先ほどの考えを ϕ^n に適用させると, この固有値が α^n, β^n となるので証明ができる.

定義

$\mathbb{F}_q$ 上の非特異代数多様体 $X/\mathbb{F}_q$ に対しその合同ゼータ関数を

$$Z(X/\mathbb{F}_q; T) := \exp \left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n} \right)$$

と定義する.

この合同ゼータ関数に対し, Riemann 予想の類似を考えたのが次の Weil 予想である.

Weil 予想

合同ゼータ関数は $\mathbb{Q}$ 係数の有理式で表され関数等式をもち,

$$Z(X/\mathbb{F}_q; T) = \frac{P_1(T) \cdots P_{2\dim(X)-1}(T)}{P_0(T)P_2(T) \cdots P_{2\dim(X)}(T)}$$

と因数分解され各 $P_i(T)$ は

$$P_i(T) = \prod_{j=1}^{b_i} (1 - \alpha_{ij}T), \quad |\alpha_{ij}| = q^{i/2}$$

と因数分解される.

楕円曲線 E の合同ゼータ関数は

$$\begin{aligned} Z(E/\mathbb{F}_q; T) &= \exp \left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n} \right) \\ &= \exp \left(\sum_{n=1}^{\infty} \frac{(1 + q^n - \alpha^n - \beta^n) T^n}{n} \right) \\ &= \exp(-\log(1 - T) - \log(1 - qT) \\ &\quad + \log(1 - \alpha T) + \log(1 - \beta T)) \\ &= \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)} = \frac{1 - a_q T + qT^2}{(1 - T)(1 - qT)} \end{aligned}$$

$$\zeta_{E/\mathbb{F}_q}(s) := Z(E/\mathbb{F}_q; q^{-s}) = \frac{(1 - \alpha q^{-s})(1 - \beta q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

と変数変換すると, α, β はある実数 θ を用いて
 $\alpha = q^{1/2+i\theta}, \beta = q^{1/2-i\theta}$ と書けることから零点は
 $\operatorname{Re}(s) = \frac{1}{2}$ となる.

また, 分子分母を展開した式

$$\zeta_{E/\mathbb{F}_q}(s) = \frac{1 - a_q q^{-s} + q^{1-2s}}{1 - q^{-s} - q^{1-s} + q^{1-2s}}$$

に対し, s を $1-s$ にすると

$$\begin{aligned}\zeta_{E/\mathbb{F}_q}(1-s) &= \frac{1 - a_q q^{s-1} + q^{2s-1}}{1 - q^{s-1} - q^s + q^{2s-1}} \\ &= \frac{(1 - a_q q^{-s} + q^{1-2s})q^{2s-1}}{(1 - q^{-s} - q^{1-s} + q^{1-2s})q^{2s-1}} \\ &= \zeta_{E/\mathbb{F}_q}(s)\end{aligned}$$

となり, 関数等式が成立する.

この講義での Hasse の定理の証明の鍵となっていたのは, Tate 加群に対する Frobenius 写像の表現を考えることだった.

⇒ 一般の代数多様体 X に対しても, Tate 加群のような $\mathbb{Q}_l$ 上のベクトル空間を考えたい!

⇒ エタールコホモロジー (l 進コホモロジー) の誕生!

定理 (Grothendieck)

$\mathbb{F}_q$ 上の非特異代数多様体 X に対し, $\text{Frob}_q : X \rightarrow X$ から誘導される写像

$\text{Frob}_q^* : H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_l) \rightarrow H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_l)$ を考えると

$$Z(X/\mathbb{F}_q; T) = \prod_{i=0}^{2\dim X} \det(1 - T \text{Frob}_q^* | H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_l))^{(-1)^{i+1}}$$

参考文献

- J.H.Silverman (2009). The Arithmetic of Elliptic Curves, 2nd edition Springer. J.H. シルヴァーマン (著) 鈴木治郎 (訳) (2023). 楕円曲線の数論—基礎概念からアルゴリズムまで— 共立出版
- J.Neukirch (1999). Algebraic Number Theory Springer. J. ノイキルヒ (著), 足立 恒雄 (監訳), 梅垣 敦紀 (翻訳) (2012). 代数的整数論 丸善出版
- 三枝洋一 (2024). 数論幾何入門: モジュラー曲線から大定理・大予想へ 森北出版
- D. シグマ (2017). 楕円曲線と保型形式の美しいところ 暗黒通信団

ご清聴ありがとうございました