第3回ヴェイユ予想物語 楕円曲線のヴェイユ予想

ari

1/29

Contents

1 Introduction

楕円曲線のヴェイユ予想を楕円曲線には深入りせずに証明する．ヴェイユがいくつかの特別な場合を示したことから，1940 年台にヴェイユ予想は楕円曲線のいくつかの性質は時間の都合上，認めて証明をする．

プロットは，以下の通り．

- 代数多様体 (Affine のみ)Projective はそれを無限遠点を加えたものととして定義する．及び smooth の定義
- 代数多様体の射の定義 (しないかも)
- ヴェイユ予想の主張
- 合同ゼータ関数と Hasse-Weil のζ関数の関係
- リーマン予想との類似
- 楕円曲線の定義
- 楕円曲線の性質
  - 有理点全体が群になること
  - Isogeny と [m] 倍写像の　存在

  - Frobenius と degree
  - Tate-Module
  - Weil-Pairing
- Weil-Conjecture の証明

代数多様体や楕円曲線の一般論については，今回は記述せず，最低限の範囲でコンパクトに止めた資料にする．目標は合計 15P 程度でまとめること．

2 代数多様体とヴェイユ予想

この章ではヴェイユ予想の主張を述べる．以下では，簡単のため，K を完全体とし，$\overline{K}$ を K の代数閉包とし，G で $\overline{K}/K$ のガロア群とする．

2.1 代数多様体

代数多様体を定義する．

2.1.1 アフィン代数多様体

Definition 2.1 (アフィン代数多様体)**.** $\mathfrak{p}$ を $\overline{K}[X_1,\dots,X_n]$ 上の素イデアルとする．以下を満たす時，V をアフィン代数多様体という．

$$V = \{(t_1,\dots t_n) \in \overline{K}^n \mid \text{任意の } f \in \mathfrak{p} \text{ に対し}, f(t_1,\dots t_n) = 0\}$$

$\mathfrak{p}$ の生成元を K 係数で取れる場合，V は K 上定義されていると書く．また，$V \cap K^n$ を $V(K)$ と書く．

Definition 2.2 (次元)**.** V をアフィン代数多様体とする．V の次元を $\mathrm{Frac}(\overline{K}[X_1,\dots,X_n]/\mathfrak{p})/\overline{K}$ の超越次数で定める. V の次元を $\dim V$ と書く．

Definition 2.3 (smooth)**.** $f_1,\dots,f_m$ を $\mathfrak{p}$ の生成元とする．$P \in V$ で *smooth* とは，以下を満たすことである．

$$\mathrm{rank}\Big(\frac{\partial f_i(P)}{\partial X_j}\Big)_{ij} = n - \dim V$$

2.1.2 射影代数多様体

射影代数多様体については説明する．アフィン代数多様体に無限遠を付け加えたようなものであり，アフィン代数多様体による被覆を取ることができる．

Definition 2.4 (射影代数多様体)**.**

2.1.3 代数多様体の間の射

2.2 ヴェイユ予想

2.2.1 ゼータ関数とヴェイユ予想

代数多様体のヴェイユ予想を記述する．

Definition 2.5. V を有限体 $\mathbb{F}_q$ 上定義された射影代数多様体とする．この時，V の合同 ζ 関数を以下で定義する．

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

Theorem 2.6 (ヴェイユ予想)**.** V を有限体 $\mathbb{F}_q$ 上定義された d 次元の *smooth* な射影代数多様体とする．この時以下が成り立つ．

Rationality ゼータ関数 $Z(V/\mathbb{F}_q;T)$ は $\mathbb{Q}(T)$ の元となる．

Functional equation あるオイラー標数 $\epsilon \in \mathbb{Z}$ が存在し，

$$Z(V/\mathbb{F}_q;\frac{1}{q^dT}) = \pm q^{d\epsilon/2}Z(V/\mathbb{F}_q;T) \tag{1}$$

Riemann Hypothesis ゼータ関数は

$$Z(V/\mathbb{F}_q;T) = \frac{P_1(T)\dots P_{2d-1}(T)}{P_0(T)\dots P_{2N}(T)} \tag{2}$$

とかけ，任意の $P_i(T)$ は $\mathbb{Z}$ 係数多項式となる．さらにこれを $\mathbb{C}$ 上分解すると以下を満たす．

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

Betti Number

任意の体の埋め込み $K \to \mathbb{C}$ に対し，$X(\mathbb{C})$ は複素多様体であり，その特異コホモロジー $H^i(X(\mathbb{C}),\mathbb{Q})$ が定義される．V が代数体 K 上定義された非特異代数多様体 X の $\mathfrak{p}$ を法とする還元で得られるなるとする．この時，得意コホモロジーの次元 *(Betti* 数*)* は多項式 $P_i(T)$ の次数と等しい．

2.3 ヴェイユ予想とリーマン予想

ヴェイユ予想とリーマン予想の類似について説明する．ここでは，スキームや代数多様体について曖昧に用語を使う. 類似に関する概要の説明のため，不正確であることについては容赦されたい．まず，合同ゼータ関数が (リーマン) ゼータ関数の類似であることを説明する．リーマンゼータ関数は

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$$

で定義されること思い出そう．この無限積は全ての素数を走る．ここで素数と極大イデアルが一対一に対応することに注意するとリーマンゼータ関数は以下のようにかくこともできる．

$$\zeta(s) = \prod_{\mathfrak{m}} \frac{1}{1-\#(\mathbb{Z}/\mathfrak{m})^{-s}}$$

ただし，$\mathfrak{m}$ は $\mathbb{Z}$ の極大イデアルを走る．上のようにリーマンゼータ関数を解釈することで，ゼータ関数を代数幾何的に一般化できる．X をスキームとした時，$|X|$ を X の閉点の集合とする．また $x \in |X|$ での剰余体を $\kappa(x)$ で表す．

Definition 2.7. X を $\mathrm{Spec}\mathbb{Z}$ 上 *of finite type* なスキームとする．この時,X の *Hasse-Weil* のゼータ関数を以下で定める．

$$\zeta(X, s) = \prod_{x \in |X|} \frac{1}{1 - \#(\kappa(x))^{-s}}$$

X として $\mathrm{Spec}\mathbb{Z}$ を取ると，Hasse-Weil のゼータ関数はリーマンゼータ関数に一致する．また，代数体 K の整数環 O_K とする．X として，$\mathrm{Spec}O_K$ を取るとデデキントゼータ関数となる．

Hasse-Weil のゼータ関数と合同ゼータ関数の関係をみる．X を $\mathrm{Spec}\mathbb{F}_q[X_1, \ldots, X_n]/\mathfrak{p}$ とする. この時，$X(\overline{\mathbb{F}_q})$ が, 最初に定義した (古典的な意味での) 代数多様体 V に一致する．また，以下の関係が成り立つ．

Propostion 2.8. V を $\mathbb{F}_q$ 上の代数多様体とする．この時, 合同ゼータ関数と *Hasse-Weil* のゼータ関数には以下が成り立つ．

$$\zeta(V, s) = \exp\left(\sum_{m=1}^{\infty} \#V(\mathbb{F}_{q^m}) \frac{q^{-sm}}{m}\right)$$

Proof. 計算すればわかる． □

ヴェイユ予想の等式 (1)(2) の意味は上を通して理解される．Hasse-Weil のゼータ関数でみると，(1) は s での値と $d - s$ での値の関係を述べている．(2) は Hasse-Weil のゼータ関数の零点や極が $|\alpha_{ij}| = q^{i/2}$ となる複素数を用いて，

$$1 - \alpha_{ij} q^{-s} = 0$$
$$\alpha_{ij} = q^{s}$$

を満たす s として得られる．つまり,s の実部が $i/2$ という主張をしている．そのため，リーマン予想の類似と考えられている．

2.4 Trace Fomula とヴェイユ予想

余力があれば, コホモロジーについても記載する．********** あとで埋める**********

3 楕円曲線の性質

この章では，楕円曲線を定義して，基本的な定義を述べる．この章では事実を列挙するだけで，基本的に証明は述べない．それは結果を使うだけで楕円曲線のヴェイユ予想が示せるのと，楕円曲線自体の理論は他に優れた参考書が多数存在し，中途半端に解説する価値を見いだせないためである．参考文献は最後に上げたので参考にして欲しい．楕円曲線は最も基本的な代数多様体であり，様々な重要な性質を持つ．ここでは，数論的な性質．特に楕円曲線の有理点全体が群構造を持つこととその群構造から誘導される Tate-Module について説明する．こ Tate-Module はガロア表現の最も基本的な例であり，ヴェイユ予想を解く上でも重要な役割を果たす．以下では，簡単のため，体 K の標数は 2 でも 3 でもないとする．

3.1 楕円曲線の定義

Definition 3.1 (楕円曲線)**.** K 上定義された射影代数多様体 V が楕円曲線とはある既約な二変数多項式 $Y^2 - X^3 - aX - b$ が存在し，以下が成り立つことである．

$$V = \{O\} \cup \{(x, y) \in \overline{K}^2 | y^2 - x^3 - ax - b = 0\}$$

Definition 3.2 (Isogeny)**.** 楕円曲線の間の射 f が $f(O) = O$ を満たす時，*Isogeny* という．

Theorem 3.3. 楕円曲線の有理点全体には足し算が定義でき，その足し算に対しアーベル群になる．

Proof. 証明略．元を具体的に構成するといえる．具体的な構成は********** あとで埋める********** □

足し算を用いることで，楕円曲線には写像が定義できる

Theorem 3.4. E/K を K 上定義された楕円曲線とする．この時，以下で定義する楕円曲線の間の射が存在する．

$$[m] : E \to E, P \mapsto P + \cdots + P \tag{3}$$

余談，疑問. 上の写像もっときれいに書けないかな．

Proof. 証明略．計算するとでる． □

3.2 Tate Module

Ker$[m]$ を $E[m]$ と書く．

Propostion 3.5. m が $\mathrm{char}(K)$ と互いに素の時，以下が成り立つ．

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

Proof. 証明略．Dual Isogeny を考え．射が分離的であり，次数 $\deg[m] = m^2$ となることからわかる． □

Remark. $p = \mathrm{char}K$ とする．この時，以下のどちらかが成り立つ．

$$E[p^e] = O$$
$$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$$

つまり，標数と同じ素数上で考えるか，異なる素数上で考えるかで起きる現象が異なる．

また，楕円曲線 E にはガロア群 G が作用しているが，O を O に映し,$[m]$ はガロア群の作用と可換なので，$E[m]$ は G が作用している．上の話を逆極限を取る．それが楕円曲線の Tate-Module である．

Definition 3.6. E を楕円曲線とする．$l \in \mathbb{Z}$ を素数とする．*l-adic Tate Module* を以下で定義する．

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

char(K) と l が異なる時，$E[l^n] \simeq \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ より，$T_l(E) \simeq \mathbb{Z}_l \times \mathbb{Z}_l$ となる．E の有理点全体を決定するのは難しいが，Tate Module は非常に簡単な形になっている．これは最も基本的なガロア表現である．また，Isogeny$\phi : E \to E$ に対し，$\phi_l : T_l(E) \to T_l(E)$ が誘導される．これからさらに，以下が従う．

Theorem 3.7. E を標数 p の楕円曲線とする．フロベニウス写像 $\phi_q E \to E, (x, y) \to (x^q, y^q)$ に対し,$\phi_l : T_l(E) \to T_l(E)$ が誘導され，以下が成り立つ．

$$\det\phi_l = q \tag{4}$$

$$\#Ker(1 - \phi) = \det(1 - \phi_l) \tag{5}$$

Proof. 証明略．Weil Pairing と代数多様体での Frobenius の性質から証明する． □

Remark. $\#E(\mathbb{F}_q) = \#Ker(1 - \phi)$ となるので，上の式から有理点の個数が具体的に計算することができる．

4 楕円曲線のヴェイユ予想の証明

上で示したこと様々な性質から楕円曲線のヴェイユ予想を実際に計算して示そう．楕円曲線の場合は，ヴェイユ予想は以下となる．

Theorem 4.1. 有限体 $\mathbb{F}_q$ 上の楕円曲線 E に対し，以下が成り立つ．

$$Z(E/\mathbb{F}_q; T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)}$$

ただし，α,β は複素共役で，$\alpha + \beta \in \mathbb{Z}$ かつ，$|\alpha| = |\beta| = \sqrt{q}$ となる．さらに，

$$Z(E/\mathbb{F}_q; \frac{1}{qT}) = Z(E/\mathbb{F}_q; T).$$

Proof. ϕ_l の特性多項式 $T^2 - \mathrm{Tr}\phi_l T + \det\phi_l$ の判別式が 0 以上になることを示す．それは，上記の二次式に任意の実数を代入しても 0 以上になることが言えればよい.

$$\det(\frac{n}{m} - \phi_l) = \frac{\det(n - m\phi_l)}{m^2} = \frac{\#\ker(n - m\phi_l)}{m^2} \geq 0$$

が成り立つ．$\mathbb{Q}$ が $\mathbb{R}$ 上稠密なので，任意の実数を代入しても 0 以上になる．

$\det\phi_l = q$ より，$T^2 - \mathrm{Tr}\phi_l T + \det\phi_l = 0$ の $\mathbb{C}$ 上の解を α,β とすると，$\alpha\beta = q$ であり，α,β が複素共役になるので，$|\alpha| = |\beta| = \sqrt{q}$ となる．

また,ϕ_l を代数閉体上まで拡張し，ジョルダン標準形を考えると，2 行 2 列の行列で対角成分が α,β となる. これより，$(\phi_l)^n$ の特性多項式は，$1 - (\alpha^n + \beta^n)T + q^n T^2$. となる．これより，

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

$Z(E/\mathbb{F}_q; T)$ を上の等式を用いて，計算する.

$$\log Z(E/\mathbb{F}_q; T) = \sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{q^n})T^n}{n}$$

$$= \sum_{n=1}^{\infty} \frac{(1-\alpha^n-\beta^n+q^n)T^n}{n}$$
$$= -\log(1-T)+\log(1-\alpha T)+\log(1-\beta T)-\log(1-qT).$$

となる．これより，

$$Z(E/\mathbb{F}_q;T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

となる. また，

$$\begin{aligned} Z(E/\mathbb{F}_q;1/qT) &= \frac{(qT-\alpha)(qT-\beta)}{(qT-1)(qT-q)} \\ &= \frac{\alpha\beta(\beta T-1)(\alpha T-1)}{q(qT-1)(T-1)} \\ &= Z(E/\mathbb{F}_q;T) \end{aligned}$$

となる．□