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

ヴェイユ予想は 20 世紀の数論の方向性を決定づけた重要な定理であり，そこで使われた道具は現在の数論の研究においても重要な位置を占める．ヴェイユ予想物語では，そのヴェイユ予想を現代の知識を持って改めて解釈することを目標としている．これまでの講義では，代数の基礎，ヴェイユ予想やその証明のアイディアの元となった，リーマン予想とリフシッツ不動点定理について解説してきた．この講義では，そうした準備を元に，ヴェイユ予想の主張，及び，ヴェイユ予想がリーマン予想の類似であることの説明をする．また，楕円曲線という特別な場合において，実際にヴェイユ予想を証明する．ただし，楕円曲線には優れた解説書が多数存在するため，その証明は本書では特に記載しない．証明が気になる場合は，例えば [**?**] を参照するとよい．本書の概要を述べる．まずは代数多様体を述べる．

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

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

$\mathfrak{p}$ 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いう．また，$V \cap K^n$ を $V(K)$ と書き，K-有理点という．$\mathfrak{p}$ が明らかな時は V を代数多様体と書く．

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

射影代数多様体を定義する．射影代数多様体は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 (斉次イデアル)**.** イデアル $I \subset \overline{K}(X_1,\dots,X_n)$ が斉次イデアルとは，I の生成元 (f_i) で f_i が斉次多項式であるものが存在すること.

Definition 2.5 (射影空間)**.** 射影空間を $\mathbb{P}^n(\overline{K})$ を以下で定義する．

$$\mathbb{P}^n(\overline{K}) := \overline{K}^{n+1}\backslash\{O\}/\sim$$

ただし，同値関係 $a \sim b$ はある $\lambda \in \overline{K}$ が存在し，$a = \lambda b$ となることで定める．

Lemma 2.6. $[a] \in \mathbb{P}^n(\overline{K})$ とする． $[a]$ の代表元 a を一つ固定する. 斉次多項式 f に対し，$f(a) = 0$ ならば $[a]$ の任意の代表元 b に対し $f(b) = 0$ となる.

上の補題の条件を満たす時，$f([a]) = 0$ と書く.

Definition 2.7 (射影代数多様体)**.** $\mathfrak{p}$ を $\overline{K}[X_0,\dots,X_n]$ の斉次素イデアルとする．この時, $(V, \overline{K}[X_0,\dots,X_n]/\mathfrak{p})$ が射影代数多様体とは，以下が成り立つことである．

$$V = \{[t_0 : \cdots : t_n] \in \mathbb{P}^n(\overline{K}) |\ \text{任意の } f \in \mathfrak{p} \text{ に対し}, f(t_0 : \cdots : t_n) = 0\}$$

射影代数多様体とアフィン代数多様体には以下の関係がある．**********
あとで埋める
****

Remark. 特に *1* 次元射影代数多様体は，アフィン代数多様体に *1* 点 O を追加したものになる．

2.2 スキーム

代数多様体では代数閉体上の図形しか調べられない．そのため，より一般の図形に拡張できないかは考えられていた．その成功例として，スキームがある．スキームは理論が広大であり，なぜこのように考えるとよいかは初学者には理解しづらいかもしれない．ただ．スキームによって数論的な問題を幾何的に解釈できるようになるなど，様々な利点がある．

まず，代数幾何の重要な定理を述べる．

Theorem 2.8 (ヒルベルトの弱零点定理)**.** 代数閉体 K 上の代数多様体 $(V, K[X_1,\dots,X_n]/\mathfrak{p})$ に対し，$\mathrm{Spm}V$ を V の極大イデアル全体のなす集合とする．$V \to \mathrm{Spm}V, (t_1,\dots,t_n) \mapsto (\overline{X_1 - t_1},\dots,\overline{X_n - t_n})$ は全単射となる．

上の定理により，代数多様体では，関数 $K[X_1,\dots,X_n]/\mathfrak{p}$ の情報さえわかれば，V の情報はいらないことがわかる．つまり，代数多様体を調べる時は，関数だけを調べればよい．このことを逆手にとり，関数を多項式環から一般の単位的可換環に一般化したものがスキームである. この時，点も極大イデアルではなく素イデアルに一般化する．スキームは環付き空間 (空間と空間上の環の層の組) として定義される．空間や空間上の層がどのように定義されるかがわかる命題を証明なく列挙する．

Propostion 2.9. R を可換環とする．Spec$R$ を R の素イデアル全体のなす集合とする．$V(I)$ を I を含む素イデアル全体の集合とする. この時，$V(I)$ は閉集合系の公理を満たす．$D(I) := \mathrm{Spec}R\backslash V(I)$ とする．

Lemma 2.10. $D(f)$ は開集合基となる．すなわち，任意の開集合 $D(I)$ は $D(f)$ の和集合で表すことができる．また，Spec$R$ はコンパクトになる．

Propostion 2.11. Spec$R$ 上に,$\mathcal{O}_{\mathrm{SpecR}}(D(f)) = R_f$ を満たす可換環の層 $\mathcal{O}_{\mathrm{Spec}R}$ が存在する．

これらより，アフィンスキームが定義できる．

Definition 2.12. $(\mathrm{Spec}R, \mathcal{O}_{\mathrm{Spec}R})$ をアフィンスキームという．

アフィンスキームは実質，可換環と思える．

Propostion 2.13. 可換環の圏とアフィンスキームの圏は圏同値になる．

Remark. 代数多様体やスキームの射は定義が複雑だが，可換環だと思うことにより，環準同型と思える．

スキームはアフィンスキームを貼り合わせたものとして定義されるが，本講義ではアフィンスキームのみを扱うので，定義は省略する．

2.3 ヴェイユ予想

2.3.1 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 2.14. 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 の合同ゼータ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 2.15 (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

$$Z(V/\mathbb{F}_q;T) \in \mathbb{Q}(T)$$

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

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

Riemann Hypothesis ゼータ関数は $\mathbb{Z}$ 係数多項式 $P_i(T)$ を用いて，

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

とかける．さらに $P_i(T)$ を $\mathbb{C}$ 上分解すると以下を満たす．

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

Betti Number V が代数体 K 上定義された滑らかな代数多様体 X の $\mathfrak{l}$ を法とする還元で得られるとする．体の任意の埋め込み $K\to\mathbb{C}$ 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．この時，特異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．

2.4 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．$X=\mathrm{Spec}R$ をアフィンスキームとし，$|X|$ を X の閉点の集合とする．(R の極大イデアル全体の集合と一致する.) また $x\in|X|$ での剰余体を $\kappa(x)$ で表す．

Definition 2.16. $\mathbb{Z}$ 上有限生成な環 R とし，アフィンスキーム $X=\mathrm{Spec}R$ 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 $\mathrm{Spec}\mathbb{F}_q[X_1,\dots,X_n]/\mathfrak{p}$ とする. 確認しておくと，$X(\overline{\mathbb{F}_q}),\mathbb{F}_q[X_1,\dots,X_n]/\mathfrak{p}\otimes\overline{F}_q$ が,$\mathfrak{F}_q$ 上のアフィン代数多様体に一致する．これを V とかく. また，以下の関係が成り立つ．

Propostion 2.17.

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

Proof. 計算すればわかる．**********
あとで埋める
********** □

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

$$\zeta(V, d-s) = Z(V/\mathbb{F}_q; q^{-d+s}) = \pm q^{d\epsilon/2-s} Z(V/\mathbb{F}_q; q^{-s}) = \pm q^{d\epsilon/2-s}\zeta(V, s)$$

となり，s での値と $d-s$ での値の関係を述べている．

(2) は零点や極を取る場所を示している．Hasse-Weil のゼータ関数の場合に零点や極を取る点 s は $P_i(q^{-s}) = 0$ を満たす．これより．$|\alpha_{ij}| = q^{i/2}$ 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 となる．$|q^s|$ は s の実部になるので，上の式は 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．

2.5 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，基本的な性質を述べる．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．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 が楕円曲線である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)**.** 楕円曲線の間の射であって，f が $f(O) = O$ を満たす時，*Isogeny* という．

Remark. 射が何かは特に説明しない．

Theorem 3.3. 楕円曲線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. □

Remark. 足し算によって楕円曲線の間の射が一つ構成できた．また，足し算から掛け算も構成することができる．

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．

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

Proof. 証明略． □

3.2 Tate Module

上で定義した $[m]$ は楕円曲線の間の代数曲線としての射になっているだけでなく，アーベル群の間の準同型になっている．そこで，この射のカーネルがどうなっているかを調べる．$\mathrm{Ker}[m]$ 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 $\mathrm{Gal}_{\overline{K}/K}$ が作用しているが，その作用では，O を O に映し,$[m]$ と可換なので，$E[m]$ 上に G の作用が定義できる．$E[m]$ の逆極限を取る．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．

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

$\mathrm{char}(K)$ 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，$1-(\alpha^n+\beta^n)T+q^nT^2$. 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.

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

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．　□

References

[1] J.Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag,1992 参考文献の著者・名前など

[2] 参考文献の著者・名前など・・・