楕円曲線のヴェイユ予想

ari

平成 29 年 12 月 3 日

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，ヴェイユ予想の着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，楕円曲線の一般論については定理を記載するのみで，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 [1] を参照するとよい．最後にヴェイユ予想におけるリフシッツ不動点定理の関係を概要程度に説明し，Weil 予想でどのようにエタールコホモロジーが活躍するかを説明する．

2 Algebraic Variety

この章ではヴェイユ予想の舞台となる代数多様体について述べる．以下では，簡単のため，K を完全体とし，$\overline{K}$ を K の代数閉包とする．

2.1 Algebraic Variety

2.1.1 Affine Algebraic Variety

アフィン代数多様体を定義する. アフィン代数多様体は多項式方程式の解によって定義される．

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

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

$\mathfrak{p}$ が明らかな時は V で代数多様体を表す．$\mathfrak{p}$ の生成元を K 係数で取れる場合，代数多様体 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．

Remark. V がアフィン代数多様体の時、$\{f\in\overline{K}[X_1,\dots,X_n] \mid \text{任意の } (x_1,\dots,x_n)\in V \text{ に対し、} f(x_1,\dots,x_n)=0\}$ は $\mathfrak{p}$ と一致する.

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

Definition 2.3 (なめらか)**.** $f_1,\dots,f_m$ を $\mathfrak{p}$ の生成元とする．$P\in V$ が以下を満たすときなめらかという．

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

2.1.2 Projective Algebraic Variety

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ものであり，局所的にはアフィン代数多様体だとみなすことができる.

Definition 2.4 (斉次イデアル)**.** イデアル $I\subset\overline{K}[X_1,\dots,X_n]$ に対し，I の生成元 $<f_1,\dots,f_k>$ であって，全ての f_i が斉次多項式であるものが存在する時 I を斉次イデアルという．

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，ある $\lambda\in\overline{K}$ が存在し，$a=\lambda b$ となる時, 同値関係 $a\sim b$ と定める.

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．

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

射影代数多様体とアフィン代数多様体に"無限遠"を付け加えたようなものとなっている．具体的には以下が成り立つ．

Propostion 2.8. $(V,\overline{K}[X_0,\dots,X_n]/\mathfrak{p})$ を射影代数多様体とする．

$$U_i:=\{[\frac{t_0}{t_i},\dots,\frac{t_{i-1}}{t_i},\frac{t_{i+1}}{t_i},\frac{t_n}{t_i}]\in V\mid t_i\neq 0\}$$

とする. 任意の $f\in\mathfrak{p}$ に対し，$f(X_1,\dots,X_i,1,X_{i+1},X_n)$ で生成される $\overline{K}[X_1,\dots,X_n]$ のイデアルを $\mathfrak{p}_i$ とする. この時，$(U_i,\overline{K}[X_1,\dots,X_n]/\mathfrak{p}_i)$ はアフィン代数多様体となる．

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．アフィン代数多様体から射影代数多様体を作ることもできる．

2.2 Scheme

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，より一般の係数の図形に拡張できないかを考えたい．スキームはそうした拡張の成功例である．ただ，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．しかし, 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なるなど, 様々な利点がある．まず，スキーム論的に問題を考えるようになった代数幾何の重要な定理を述べる．

Theorem 2.9 (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，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．

ヒルベルトの零点定理により，代数多様体では，代数多様体上の関数全体のなす環 $K[X_1,\dots,X_n]/\mathfrak{p}$ の情報さえわかれば，V の情報は自動的に復元できることがわかる．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，スキームでは、関数を多項式環から一般の単位的可換環に拡張して考えてみる. この時，スキームの底空間も極大イデアルのなす集合ではなく素イデアルのなす集合に一般化する．これらを組み合わせ, 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うなっているかを証明なく述べる．

Propostion 2.10. R を可換環とし，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．$I=(f)$ の時，$V(I),D(I)$ をそれぞれ，$V(f),D(f)$ と書く．

Lemma 2.11. $D(f)$ 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 2.12. Spec$R$ 上に,$\mathcal{O}_{\mathrm{Spec}R}(D(f))=R_f$ 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 2.13. $(\mathrm{Spec}R, \mathcal{O}_{\mathrm{Spec}R})$ 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 2.14. 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．

Definition 2.15 (S 上のスキーム)**.** スキーム X と射 $X \to S$ の組を S 上のスキームという．$S = \mathrm{Spec}R$ の場合，R 上のスキームという．

Definition 2.16 (有理点)**.** K を体とする．K 上のスキームの射 $\mathrm{Spec}K \to X$ を K-有理点という．

Propostion 2.17. 体 K 上のスキーム $X = \mathrm{Spec}K[X_1, \ldots, X_n]/\mathfrak{p}$ とする．この時，K-有理点全体の集合は $V = \{(t_1, \ldots, t_n) \in K^n \mid$ 任意の $f \in \mathfrak{p}$ に対し，$f(t_1, \ldots t_n) = 0\}$ と一致する．

Proof. アフィンスキームの圏と可換環の圏の圏同値から，K-有理点は $\tilde{g} : K[X_1, \ldots, X_n]/\mathfrak{p} \to K$ となる準同型と一対一に対応する．この準同型は剰余環の普遍性から $g : K[X_1, \ldots, X_n] \to K$ への準同型であって，kernel が $\mathfrak{p}$ を含むものと一対一に対応する．$g(X_i) = a_i$ とすると $\mathrm{Ker}f = (X_1 - a_1, \ldots, X_n - a_n)$ となる．$(X_1 - a_1, \ldots, X_n - a_n) \supset \mathfrak{p}$ は任意の $f \in \mathfrak{p}$ に対し，$f(a_1, \cdots, a_n) = 0$ と同値となり，示された． □

Remark. 準同型 $f, g : K[X_1, \ldots, X_n]/\mathfrak{p} \to K$ が $f = h \circ g$ と書けた場合，$\mathrm{Ker}f = \mathrm{Ker}g$ は一致する．そのため,$(X_1 - a_1, \ldots, X_n - a_n), (X_1 - b_1, \ldots, X_n - b_n) \in K^n$ が異なる場合,$X_i \mapsto a_i$, となる準同型 π_a と $X_i \mapsto b_i$ となる準同型 π_b に対し，$\pi_b = h \circ \pi_a$ となる準同型 h は存在しない.

3 Weil Conjecture

3.1 Statement of Weil Conjecture

代数多様体のヴェイユ予想を記述する．

Definition 3.1. 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 3.2 (ヴェイユ予想)**.** V を有限体 $\mathbb{F}_q$ 上定義された d 次元のなめらか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，

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

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．

3.2 Weil and Riemann

ヴェイユ予想とリーマン予想の類似について説明する．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

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

で定義された．この無限積は全ての素数を走る．$\mathbb{Z}$ では, 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 3.3. $\mathbb{Z}$ 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．$\mathbb{F}_q$ 上の代数多様体 $(V,\overline{\mathbb{F}_q}[X_1,\dots,X_n]/\mathfrak{p}$ とする. X を $\mathrm{Spec}\mathbb{F}_q[X_1,\dots,X_n]/\mathfrak{p}\cap\mathbb{F}_q[X_1,\dots,X_n]$ とする. 以下の関係が成り立つ．

Propostion 3.4.

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

Proof. $\#k(x) = q^{m_x}$ とする.log をとると,

$$\begin{aligned}\sum_{x\in|X|} -\log(1-\#k(x)^s) &= \sum_{x\in|X|}\sum_{n=1}^{\infty} q^{-m_x sn}/n \\ &= \sum_{x\in|X|}\sum_{n=1}^{\infty} m_x q^{-m_x sn}/nm_x \\ &= \sum_{n=1}^{\infty}\sum_{x\in|X|,m_x|n} m_x \frac{q^{-ns}}{n}\end{aligned}$$

となる. よって,

$$\sum_{x\in|X|,m_x|n} m_x = \#V(\mathbb{F}_{q^n})$$

を示せばよい. 生成元の行き先だけで決まるので, $\mathrm{Hom}(\mathbb{F}_q[X_1,\ldots,X_n]/\mathfrak{p}\cap\mathbb{F}_q[X_1,\ldots,X_n],\mathbb{F}_{q^n}) \simeq \mathrm{Hom}(\mathbb{F}_{q^n}[X_1,\ldots,X_n]/\mathfrak{p}\cap \mathbb{F}_{q^n}[X_1,\ldots,X_n],\mathbb{F}_{q^n})$ となり, $\#V(\mathbb{F}_{q^n}) = \#\mathrm{Hom}(\mathbb{F}_{q^n}[X_1,\ldots,X_n]/\mathfrak{p}\cap\mathbb{F}_{q^n}[X_1,\ldots,X_n]/,\mathbb{F}_{q^n})$ となるので, $\mathrm{Hom}(\mathbb{F}_q[X_1,\ldots,X_n]/\mathfrak{p},\mathbb{F}_{q^n})$ の個数がわかればよい. $x\in|X|$ に対し、$m_x = \#Gal(\mathbb{F}_{q^{m_x}}/\mathbb{F}_q)$ 個の射が kernel が一致する. これより, 閉点 x に対し, 射が m_x 個存在することがわかる. また, 射が存在すれば, その kernel に一致する閉点が存在する. よって,

$$\sum_{x\in|X|,m_x|n} m_x = \#V(\mathbb{F}_{q^n})$$

となる. □

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. リーマン予想の等式から,$|\alpha_{ij}| = q^{i/2}$ となる複素数を用いて,

$$\begin{aligned}1-\alpha_{ij}q^{-s} &= 0 \\ \alpha_{ij} &= q^s\end{aligned}$$

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.

4 Elliptic Curve

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.

4.1 Definition of Elliptic Curve

Definition 4.1 (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 $4a^3 + 27b^2 \neq 0$ となる，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．

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

Definition 4.2 (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 4.3. 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 4.4. 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．

$$[m] : E \to E, P \mapsto P + \cdots + P$$

Proof. 証明略． □

4.2 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 4.5. 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，$E[m]$ 上にガロア群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 4.6. 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．これが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 4.7. 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,$\phi_l^q : T_l(E) \to T_l(E)$ が誘導され，以下が成り立つ．

$$\det\phi_l^q = q$$
$$\#\mathrm{Ker}(m - n\phi^q) = \det(m - n\phi_l^q)(p \text{ は } m \text{ を割らない})$$

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. $\#E(\mathbb{F}_q) = \#\mathrm{Ker}(1 - \phi^q)$ となるので，上の式から有理点の個数が *Tate Module* から計算できることがわかる．

5 Proof of Weil Conjecture of Elliptic Curves

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 5.1. 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 を q 乗の Frobenius 写像．ϕ_l を Frobenius から誘導される Tate Module の間の準同型とする．有理点の個数は上の定理から $1 - \phi_l$ が誘導する行列の行列式で計算できる．ϕ_l の特性多項式 $\det(T - \phi_l) = T^2 - \mathrm{Tr}\phi_l T + \det\phi_l$ となるので，行列式は $1 - \mathrm{Tr}\phi_l + \det\phi_l$ となる．これの解 α, β が複素共役になることを示す．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．(n が p の倍数のときは上の等式は成り立たないが，n/m をうまく取り替えることにより正当化できる．) $\det\phi_l = q$ より，$\alpha\beta = q$ であり，α, β が複素共役になるので，$|\alpha| = |\beta| = \sqrt{q}$ となる．また，$\alpha + \beta = q - \#E(\mathbb{F}_q)$ より，整数になる．ϕ_l をの場合の結果を使って，$(\phi_l)^n$ の場合に計算する．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 になり，n 乗した行列の対角成分は α^n,β^n となる．そのため，$(\phi_l)^n$ の特性多項式は，$T^2-(\alpha^n+\beta^n)T+q^n$ となる．これより，

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

$Z(E/\mathbb{F}_q;T)$ 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． □

Remark. $\mathbb{C}$ 上の楕円曲線は複素多様体として，*1* 次元トーラスとなるので，*Betti* 数についての予想も成り立っていることがわかる．

6 Trace Fomula and Weil Conjecture

ヴェイユ予想と Trace Formula との関係を説明する．位相幾何での Lefschetz Trace Formula は以下のようなものであった．

Theorem 6.1 (Lefschetz Fixed Point Theorem)**.** M をコンパクト位相多様体,$\phi;M\to M$ を連続写像とする．$Fix(\phi):=\{x\in M\mid \phi(x)=x\}$ とおく，ϕ の固定点が高々有限で非退化で孤立的なら，

$$\#Fix(\phi) = \sum(-1)^i \mathrm{Tr}(\phi^*|H^i(M,\mathbb{Q}))$$

Remark. 詳しくないため誤りがある可能性あり．

これは不動点に関する予想であった．ヴェイユ予想の証明でみたように，有理点は Frobenius 写像の不動点と解釈できる．そこから，あるよい性質を満たすコホモロジーが存在し，以下が成り立つとする．

Theorem 6.2. X を体 $\mathbb{F}_q$ 上の滑らかな d 次元射影的代数多様体とし,*Frobenius* 射 $\phi : X \to X$ の固定点集合を $Fix(\phi)$ とおく．このとき，

$$\#X(\mathbb{F}_{q^m}) = \#Fix(\phi^m) = \sum_{i=0}^{2d}(-1)^i \mathrm{Tr}((\phi^*)^m; H^i_{\text{ét}}(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_l))$$

がなりたつ．

Remark. 詳しくないため誤っている可能性がある．また，*Frobenius* でなくても有限体でなくても成り立つ．

この時，$H^i_{\text{ét}}(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_l))$ の Frobenius 射が誘導する作用の固有値を $\alpha_{i,1}, \ldots, \alpha_{i,k_i}$ とすると

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2d}(-1)^i(\alpha^m_{i,1} + \cdots + \alpha^m_{i,k_i})$$

がなりたつ．また

$$P_i(T) := \det(1 - T\phi^*; H^i(X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mathbb{Q}_l)) = \prod(1 - \alpha_{i,j}T)$$

とすると，

$$Z(X;T) = \prod_{i=0}^{2d}(P_i(T))^{-1^{i+1}} = \frac{P_1(T)P_3(T)\ldots P_{2d-1}(T)}{P_0(T)\ldots P_{2d}(T)}$$

となる．これより有理関数であることはすぐわかる．また，関数等式も実際に計算すればでる．Betti 数についても，以下のような特異コホモロジーとの比較同型が存在すれば，丁寧に計算することで示せる．

Theorem 6.3 (特異コホモロジーとの比較同型)**.** $\mathbb{C}$ 上のスキーム X に対し, 以下が成り立つ．

$$H^i_{\text{ét}}(X, \mathbb{Q}_l) \simeq H^i(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_l$$

つまり，都合のよいコホモロジーが定義できれば，ヴェイユ予想のリーマン予想の類似以外の証明がほとんど自動的に示すことができる．グロタンディークはこうした都合のよい性質が成り立つエタールコホモロジーの定義に成功し，リーマン予想以外の部分の証明を行った．さらにモチーフに関する Standard 予想という予想をたて，そこからリーマン予想部分も自動で成り立つことを示した．しかし，Standard 予想自体は現在も未解決であり，ヴェイユ予想はドリーニュが別の方法で示したのである．

References

[1] J.Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag,1992

[2] Q.Liu. Algebraic Varieties and Arithmetic Curves.oxford university press,2006

[3] H.Hida Sapporo Summer School on Number Theory Hokkaido University http://eprints3.math.sci.hokudai.ac.jp/1922/ ,2008