

Weil 予想入門

ari

2016/9/22

目 次

1	Introduction	2
2	代数多様体とスキーム	4
2.1	代数多様体の定義	4
3	代数曲線とリーマン・ロッホの定理	5
3.1	Divisor	6
3.2	微分加群	6
3.3	リーマン・ロッホの定理	7
4	楕円曲線の定義	7
4.0.1	楕円曲線の定義	7
4.0.2	楕円曲線の性質	9
4.0.3	楕円曲線の写像	9
5	楕円曲線の性質	10
5.1	Invariant Differential	10
6	ヴェイユ予想の定式化と楕円曲線の場合の証明	11
6.1	ヴェイユ予想の定式化	11
6.2	楕円曲線の場合の証明	13
7	p 進表現	14
7.1	p 進表現の定義	14
7.2	p 進周期環の定義	14
7.3	p 進表現の分類	14
7.4	それ以外	14

8	p-adic 解析によるヴェイユ予想の証明	14
8.1	A formula for the number of \mathbb{F}_q points on a hypersurface . . .	14
8.2	The construction of <i>Theta</i>	15
8.3	Trace of certain linear maps on rings of formal power series .	15
9	スキームとスキームによる代数多様体の定義	16
9.1	エタール射	16
9.2	エタール基本群	16
10	数論のモチベーション	17
10.1	体とガロア理論	17
10.2	有限体とその絶対ガロア群	20
10.3	局所体と大域体	21
10.4	類体論の主定理の紹介	21

1 Introduction

数論幾何の入門として、楕円曲線の場合のヴェイユ予想について解説する。
今回の講演の Motivation を以下に記す。

- 『代数幾何の枠組み』で『数論の問題を考える』＝『数論幾何』
- s.t 氏に数論幾何はいいぞ！と言ってもらうこと。
- 数論幾何が難しすぎて、意味不明!となること
- 事実は一意であっても、証明と解釈は一意でないこと。

Motivation は標語的なので、内容を説明する。数論幾何とは、数論的な問題、例えば多項式の有理数解がどの程度あるのか、解の公式があるのかを調べていた。これらはガロア理論により、ガロア群を調べることに変更した。ガロア群は調べるのが難しく、 \mathbb{Q} でも最大アーベル拡大の場合しかわかっていない。そのため、一般のガロア群を調べるために、表現を考える。表現を考えるには作用する空間が必要となる。その空間が代数幾何で出てくるものつまり、解全体のなす図形やその図形の不変量、もっと言えば、代数多様体から誘導されるエタールコホモロジーである。今回はヴェイユ予想をもとに代数幾何的な道具である、楕円曲線と、その Tate Module に対し、TateModule への作用を基に解の個数について記述する様を説明していく。ヴェイユ予想の病的とまでも感じる美しい結果をみて、数論幾何の魅力を感じていただければ幸いである。今回の講演は s.t 氏が私に依頼したことで生まれた。そのため、s.t. 氏が満足することが私の目標である。講演では、時間の許す限り、説明をしたが、群環体の知識、および、最低限の代数幾何の知識を知っていることを仮定した。そのため、大学院に入学できるレベルの高度な数学力が要求する話とした。具体的な議論をするにはそれでも時間が足りなかった。

これは、数論幾何は(もしかしたら数学は)多くの複雑な道具が出現し、理解するためにはいくつものハードルをじっくり消化してはじめて、理解できることを意味している。そのため、中途半端に分かった気になるぐらいなら、わけがわからないと思ってくれてもいいと考えている。講演としてはなるべく、わかるように説明するつもりであるが、この内容からヴェイユ予想を一般の smooth projective Variety に拡張するのは容易ではない。また、ヴェイユ予想は今回のように楕円曲線に限れば具体的に証明できる。一般の場合も l -adic なコホモロジーや p -adic な方法など、複数の方法がある。問題は一つであっても、その解釈や証明は一通りでなく、それ次第でできる数学が異なることに触れておく。別の証明については、講演では一言も触れなかったが、余力があれば、説明したい。

さて、楕円曲線のヴェイユ予想であるが、今回は以下の順で説明する。

1. 代数多様体と代数曲線
2. 楕円曲線の定義
3. 楕円曲線の性質
4. ヴェイユ予想の証明

代数多様体と代数曲線については今回は証明しない。証明しないのは、ここを大幅に認めると楕円曲線は環論の知識がほとんどいらないことと、時間及び筆者の力量不足である。なので、この資料を公開する時は可能な限り証明をつけたい。また、定期的に証明をつけて、更新することがある。ここでわかってもらいたいことは、Projective Variety の定義と射の定義、および、一次元の特異性とリーマンロッホの定理である。リーマンロッホの定理があるので、以降の議論は線形代数敵に説明できる。楕円曲線の定義では、代数曲線として楕円曲線を定義し、それが $\text{Pic}(E)$ と同型であること、isogeny と isogeny が群の準同型となることについて説明する。これらは楕円曲線の基本であるので、それらを説明する。楕円曲線の性質では Dual Isogeny, Tate Module, Weil Pairing 等について説明する。特に射が Separable であれば、分岐次数が 1 になることと Tate Module への Frobenius の作用が degree で計算できることは面白い現象だと思う。最後にこれらの性質をあつめて、Weil 予想を証明する。

なお、今回話せなかった基礎的なガロア理論に関する部分、また、今後に向けた話も少しは記載する。その後、代数体のガロア群を調べることとガロア表現のモチベーションについて話す。ガロア表現を作るには幾何的に作る。古典的には楕円曲線の Tate Module

今回は具体的に楕円曲線の性質を調べ、Tate Module にかかる Frobenius の作用の仕方からヴェイユ予想を導く。

コホモロジー論的なものの見方についてとエタールコホモロジーコホモロジーについて、何も触れることができなかったのが、機会があれば触れたい。

TBD. 頑張って Weil Conjecture と自分に関する理解を説明する.

目標としては, etale Cohomology による Rationality の証明と Dwork による証明までやりたい.

最後に Appendix としてガロア理論やガロア群に関する数論のモチベーションについて記載した. ガロア理論はよく知らない人は参考にせよ.

代数幾何と楕円曲線 (具体例)

- 代数多様体の定義
- 代数曲線とリーマンロッホの定理
- 楕円曲線の定義とその性質

ヴェイユ予想の定式化と楕円曲線の場合の証明

- ヴェイユ予想の定式化
- 楕円曲線の場合の証明

ヴェイユ予想のお話

- ヴェイユコホモロジーと其の実現としてのエタールコホモロジー
- Trace Formula による有理点の証明

スキームとエタールコホモロジーの定義

- ヒルベルトの零点定理と代数多様体
- スキームの定義
- etale 射の定義
- etale cohomology の定義

p 進表現のお話

- p 進解析によるヴェイユ予想の有理性の証明
- p 進表現と p 進周期環

2 代数多様体とスキーム

2.1 代数多様体の定義

幾何学においては調べる対象である図形を定める. 代数幾何で扱う図形は主に代数多様体と呼ばれるものである. そのため, 代数多様体を一般的に定義する. 以降では, K を完全体とし, \bar{K} を K の代数閉包, $\text{Gal}_{\bar{K}/K}$ を絶対ガロア群とする.

Definition 2.1. V がアフィン代数多様体とは以下を満たすことである.

1. $V \subset \bar{K}^n$
2. $\bar{K}[X_1, \dots, X_n]$ のある素イデアル I が存在し, $V = \{(x_1, \dots, X_n) \in \bar{K}^n \mid \text{任意の } f \in I \text{ に対し } f(x_1, \dots, x_n) = 0\}$

Definition 2.2. V が K 上定義されているとは, I の生成元 f_1, \dots, f_n として, K 係数の多項式がとれることまた, K 有理点 $V(K)$ を $V \cap K^n$ で定める.

一般に I に対し, $V_I := \{(x_1, \dots, x_n) \in \bar{K}^n \mid \text{任意の } f \in I \text{ に対し } f(x_1, \dots, x_n) = 0\}$ と定める. また, $V \subset \bar{K}^n$ に対し, $I_V := \{f \in \bar{K}[X_1, \dots, X_n] \mid \text{任意の } V \text{ の元 } (x_1, \dots, x_n) \text{ に対し } f(x_1, \dots, x_n) = 0\}$ これは一般には可逆な操作ではない. そして, 一般的には $I_{V_I} = \sqrt{I}$ となる.

幾何学なので, これに位相を定めたい. ****あとで書く.

Definition 2.3. V の次元を以下で定める.

$$\dim V := \text{trans.deg}_{\bar{K}} K(\bar{V})$$

Definition 2.4. V が P でなめらかとは, $P \in V$ に対し微分の行列 $(\frac{\nabla f_i(P)}{\nabla x_j})_{ij}$ の rank が $n - \dim V$ と一致すること.

Definition 2.5. V が *Projetive Variety* とは

1. $V \subset \mathbb{P}^n(\bar{K})$
2. $\bar{K}[X_0, \dots, X_n]$ のある *homogeneous* な素イデアル I が存在し, $V = \{[(x_0, x_1, \dots, X_n)] \in \mathbb{P}^n(\bar{K}) \mid \text{任意の } f \in I \text{ に対し } f(x_1, \dots, x_n) = 0\}$

Proposition 2.6. $V \subset K^n = 0$ or $V \subset K^n = V$

局所的にアフィンなので, 次元や滑らかななども定義できる.

Definition 2.7. $\phi: V_1 \rightarrow V_2$ が *rational map* とは, $f_0, \dots, f_n \in \bar{K}(V_1)$ であって, 任意の点 $P \in V$ で値が定義されるものであり, $[f_0(P), \dots, f_n(P)] \in V$ と定義される

3 代数曲線とリーマン・ロッホの定理

代数曲線を定義し, 代数曲線でよく使われる, リーマン・ロッホの定理を紹介する.

Definition 3.1. 代数曲線とは 1 次元射影代数多様体をさす.

代数曲線の性質を AEC2 章にもとづきいくつか記載する. 特に証明はしない予定.

Proposition 3.2. C を curve, $P \in C$ が smooth とする. この時, $\bar{K}[C]_P$ は DVR となる.

ネーターローカル次元かつ, M_P/M_P^2 が 1 元生成されるので, 言える.

Definition 3.3. C を曲線とする. $P \in C$ を smooth な点とする. $\bar{K}[C]_P$ には以下で正規付値を与えられる.

$$\text{ord}_P : \bar{K}[C]_P \rightarrow \{0, 1, \dots\} \subset \infty$$

商体にも自然に拡張できる. M_P の生成元を *uniformizer* という.

Remark. $P \in C(K)$ なら, $K(C)$ は P での $K(C)$ の *uniformizer* を持つ.

Definition 3.4. $f \in \bar{K}(C)$ に対し $\text{ord}_P(f) < 0$ なら f は P で *pole* を持つという. また, $\text{ord}_P(f) \geq 0$ なら f は P で *regular* という.

Proposition 3.5. C をなめらかな曲線とし, $f \in \bar{K}(C)$ で $f \neq 0$ とする. C が *pole or zero* となる点はたかだか有限個である. もし, f が *pole* を一つも持たない場合 $f \in \bar{K}$ となる.

Example 3.6. C を代数曲線とし, $V \subset \mathbb{P}^n$ map を定める. これは一対一対応であり. $K(C)$ となっていない

これは後で直す

Proposition 3.7. C_1, C_2 を 1 次元代数多様体とする. $\text{morphism } f : C_1 \rightarrow C_2$ は定数写像か全射になる.

3.1 Divisor

3.2 微分加群

微分加群の一般論を概観する. A を環, M を A 加群とする. A から M への導分

Definition 3.8. C を曲線とする. C 上の微分形式のなす空間 Ω_C とは, $x \in \bar{K}(C)$ で生成する $\bar{K}(C)$ ベクトル空間を以下の関係で割ったものである.

1. $d(x + y) = dx + dy$
2. $d(xy) = ydx + xdy$
3. $da = 0 (a \in \bar{K})$

$\phi : C_1 \rightarrow C_2$ を曲線の非定数写像とする. これに対し, $\phi^* : K(C_2) \rightarrow K(C_1)$ が定まり, そこから, $\phi^* : \Omega_{C_2} \rightarrow \Omega_{C_1}$ が誘導される.

Proposition 3.9. C を代数曲線とする.

1. Ω_C は \bar{K}_C の 1 次元ベクトル空間となる.
2. $x \in \bar{K}_C$ に対し, dx が Ω_C 上基底であることと, $\bar{K}(C)$ が $\bar{K}(x)$ の有限次分離拡大であることは同値.
3. $\phi: C_1 \rightarrow C_2$ が非定数写像だとすると ϕ が *separable* と $\Omega_{C_2} \rightarrow \Omega_{C_1}$ が単射は同値.

Definition 3.10. $\omega \in \Omega_C$ に対し, ω に付随する *divisor* を

$$\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega)(P)$$

と書く.

Ω_C は $\bar{K}(C)$ 上一次元なので, 任意の ω に付随する divisor は同値となる.

3.3 リーマン・ロッホの定理

リーマン・ロッホの定**ここはちゃんと主張を述べる. ただし証明はしないかもしれない.

Theorem 3.11.

4 楕円曲線の定義

楕円曲線を代数多様体として定義する. その後, 具体的に代数多様体の性質をみる.

4.0.1 楕円曲線の定義

Definition 4.1. (E, O) が楕円曲線とは, E が *genus 1* の 1 次元非特異代数多様体であり, $O \in E$ となるもののことである. E が K 上定義されるとは, E が K 上定義され, $O \in E(K)$ となることである.

この定義がワイエルシュトラスの多項式の曲面と一致することをリーマン・ロッホを使い示す.

Proposition 4.2. *Let E be an elliptic curve defined over K .*

1. $x, y \in K(E)$ で写像

$$\phi : E \rightarrow \mathbb{P}^2, \phi = [x, y, 1]$$

が E/K 上で、以下のワイエルシュトラス方程式で与えられる曲線との同型を定める.

$$C : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

ただし、 $a_1, \dots, a_6 \in K$ で $\phi(O) \in [0, 1, 0]$ x, y は楕円曲線 E のワイエルシュトラス座標と呼ばれる.

2. うえで定めた E に対する、2つのワイエルシュトラス方程式は変数を以下のように変形することで得られる.

$$X = u^2X' + r, Y = u^3Y' + su^2 + t,$$

ただし、 $u \in K^\times, r, s, t \in K$

3. 逆に、任意のワイエルシュトラス方程式で与えられた *smooth* な曲線は K 上 $O = [0, 1, 0]$ を起点とする楕円曲線を定める.

Proof. 1. $\mathcal{L}(n(O))$ にリーマン・ロッホの定理を種数 1 で適用することで、

$$l(n(O)) = \dim \mathcal{L}(n(O)) = n$$

となる. これより、 $x, y \in K(E)$ を、 $\{1, x\}, \{1, x, y\}$ がそれぞれ、 $\dim \mathcal{L}(2(O)), \dim \mathcal{L}(3(O))$ の生成元とする. $n = 1$ の場合のリーマン・ロッホの定理より $l((O)) = 1$ となるので、 x は O で位数 2 の極を持ち、 y は O で位数 3 の極を持つ. $\mathcal{L}(6(O))$ は次元 6 のため、

$$1, x, y, x^2, xy, y^2, x^3$$

は以下の関係を満たす.

$$A_1 + A_2x + A_3y + \dots + A_7x^3 = 0$$

これは、 A_i を K の元として取れる. また、 A_6, A_7 の積は 0 とならない. これが 0 になると、極の位数の議論から、全ての A_i が 0 となるためである. 題意の方程式を得るため、 A_6, A_7 の係数をうまく掛け合わせて、 y^2, x^3 の 1 次の項を 1 としたい. そのため、 x を A_6A_7x, y を $-A_6A_7^2y$ にそれぞれ、置換し、 $A_6^3A_7^4$ で割ればよい. これにより求めるワイエルシュトラス方程式が得られる.

$$\phi : E \rightarrow \mathbb{P}^2, \phi = [x, y, 1]$$

は rational map を定め、像はワイエルシュトラス方程式で定められた曲線 C 内になる. すなわち, $\text{Im}(\phi) \subset C$ となる. この 2 つが同型であることを, C_1, C_2 が smooth curve で $\phi: C_1 \rightarrow C_2$ が次数 1 の morphism となっていることを示す. E が nonsingular なので, rational map ϕ は morphism になる. また, 代数曲線の間の morphism は定数写像か全射のどちらかであり, ϕ は O では極になり, 他は極にならないため, 定数写像でない. よって, 全射になる. ϕ が次数 1 であることを示す. $[x, 1]: E \rightarrow \mathbb{P}^1$ を考えると, x は O で位数 2 の極となり, 他の点では極となっていない. そのため $\deg \phi = 2$ となる, 同様に $[y, 1]$ は次数 3 となる. 定義から, $[K(E), K(x)] = 2, [K(E) : K(y)] = 3$ より, $[K(E) : K(x, y)] = 1$ となる. C が smooth であることを示す. C がある点 P で singular だとすると, AEC III.1.6 より $\psi: E \rightarrow \mathbb{P}^1$ で次数 1 となる ψ が存在する. すると, $\psi \circ \phi: E \rightarrow \mathbb{P}^1$ は次数 1 の map となり, E, \mathbb{P}^1 となり, は smooth なので, Cor2.4.1 より isomorphism となる. これは種数 1 の曲線と種数 0 の曲線が同型となること意味するため, 矛盾する.. よって C は smooth となることがわかる. これより E と C が同型であることがわかった.

2. $\{x, y\}, \{x', y'\}$ が E のワイエルシュトラス座標系とする.. この時, 基底の定義から, $x = u_1 x' + r, y = u_2 y' + s_2 x' + t$ と表せる. $u_1, u_2 \in K^\times$ ワイエルシュトラス多項式となること x', y' の係数は一致する. つまり, $u_1^3 = u_2^2$ となる. よって, $u = u_2/u_1, s = s_2/u^2$ とすることにより, 求める関係式は得られる.

3. 一旦保留する.

□

ワイエルシュトラス多項式で定義された方程式について一度概観する. 以降は計算簡略化のため $\text{Char} K \neq 2, 3$ とする. 極を $[0, 1, 0]$ とし, 非斉次化して, $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ を考える.

4.0.2 楕円曲線の性質

- j-invariant - differential

4.0.3 楕円曲線の写像

- isogeny - dual isogeny - Endmorphism

Isogeny について定義する.

Definition 4.3. E_1, E_2 を楕円曲線とする. $\phi: E_1 \rightarrow E_2$ が Isogeny とは ϕ が代数曲線の間の morphism になっており, $\phi(O) = O$ となること.

E_1 と E_2 が isogenous とは $E_1 \rightarrow E_2$ への const でない isogeny が存在すること。

deg 等も morphism の場合と同様に定義できる。また, $\deg[0] = 0$ と定める。

$\text{Hom}(E_1, E_2)$ で isogeny 全体の集合を表す。これはアーベル群になっている。

Propostion 4.4. 1. E/K を楕円曲線とする。

$$[m]: E \rightarrow E$$

は nonconstant な isogeny になる。

2. E_1, E_2 を楕円曲線とする。 $\text{Hom}(E_1, E_2)$ は torsion free \mathbb{Z} 加群となる。

上記は群の行き先を具体的に計算するぐらいしか見つからなかった。他にいい方法があれば証明を記述する。

Definition 4.5. E を楕円曲線とする。 m -torsion 群を $E[m]$, torsion 全体のなす群を E_{tor} と書く。

Isogeny の構成例

E/K を楕円曲線, $P \in E$ とする。

$$\tau_Q: E \rightarrow E, P \mapsto P + Q$$

は楕円曲線の間での代数曲線としての isomorphism を定める。 任意の morphism $\phi: E_1 \rightarrow E_2$ に対し, $\tau_{-\phi(O)} \circ \phi$ は isogeny になる。

Propostion 4.6. $\phi: E_1 \rightarrow E_2$ を楕円曲線の間での isogeny とする。

この時, $\phi(P + Q) = \phi(P) + \phi(Q)$ となる。

Isogeny の性質と $E \simeq \text{Pic}(E)$ より, 自然に導かれる。

Corllary 4.7. ϕ を non-zero の isogeny とする。 この時 $\text{Ker}(\phi)$ は有限群となる。

この辺証明雑です。

5 楕円曲線の性質

5.1 Invariant Differential

E を $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ を楕円曲線とする。 AEC III1.5 等に記載があるように

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

が零点も極も存在しない。

Proposition 5.1. $Q \in E$ とし、 τ_Q を Q 平行移動する射とする。このとき

$$\tau_Q^* \omega = \omega$$

Dual Isogeny を定義する。

Proposition 5.2. $\phi : E_1 \rightarrow E_2$ が次数 m の *non constant* な isogeny とする。このとき、

1. isogeny $\hat{\phi} : E_2 \rightarrow E_1$ で $\hat{\phi} \circ \phi = [m]$ となるものがただ一つ存在する。
2. $\hat{\phi}$ は以下の合成と等しい

$$\begin{aligned} E_2 &\rightarrow \text{Div} E_2 \xrightarrow{\phi^*} \text{Div} E_1 \rightarrow E_1 \\ P &\mapsto (P) - (O) \sum n_P(P) \rightarrow \sum [n_P]P \end{aligned}$$

Proof. 1. 一意性を示す。 $\hat{\phi} \circ \phi - \hat{\phi}' \circ \phi = [0]$ とする。 ϕ は nonconst より全射となる、そのため、 $\hat{\phi} = \hat{\phi}'$ となる。 ϕ が separable の場合か Frobenius の場合に示せばよい。

ϕ が separable 準同型定理もどきから示せる。

ϕ が Frobenius p 乗の場合に示せば、その合成から示せる。

$$[p]^* \omega = p\omega = 0$$

となり、分離的でない、そのため分離的でない部分については Frobenius を使って分解できるので、言えた。

2. 計算するとできる。本当は計算を書くべきだが、頭に入らない。

□

Definition 5.3. 上の条件を満たす $\hat{\phi}$ を *dual isogeny* という。

- Tate Module - Weil Pairing

6 ヴェイユ予想の定式化と楕円曲線の場合の証明

ヴェイユ予想を定式化し、楕円曲線の場合に示す。

6.1 ヴェイユ予想の定式化

まず、ヴェイユ予想を述べ、そこで出てくる用語について整理する。

Theorem 6.1. V を位数 q の有限体 \mathbb{F}_q 上定義された d 次元非特異代数多様体とする。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,

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

Riemann Hypothesis

ゼータ関数は

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

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

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

Betti Number

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らば, 任意の体の埋め込み $K \rightarrow \mathbb{C}$ に対し, $X(\mathbb{C})$ は複素多様体となる. その特異コホモロジー $H^i(X(\mathbb{C}), \mathbb{Q})$ が定義される. その次元 (Betti 数) は多項式 $P_i(T)$ の次数と等しい.

話すこと- ゼータ関数の定義ゼータ関数 $Z(V/\mathbb{F}_q; T)$ を定義する. ベキ級数の間の写像として, exponential を定義する.

$$\begin{aligned} \exp : \{F \in \mathbb{Q}[[T]] \mid F(0) = 0\} &\rightarrow \mathbb{Q}[[T]] \\ \sum_{k=1}^{\infty} a_k T^k &\rightarrow \sum_{n=0}^{\infty} \frac{(\sum_{k=1}^{\infty} a_k T^k)^n}{n!} \end{aligned}$$

像の各次数ごとに項を数えるとたかたが有限なので welldefined. また, 定数項が 1 となることに注意.

$$\begin{aligned} \log(1+): \{F \in \mathbb{Q}[[T]] \mid F(0) = 0\} &\rightarrow \mathbb{Q}[[T]] \\ \sum_{k=1}^{\infty} a_k T^k &\rightarrow \sum_{n=1}^{\infty} \frac{(-1)^{n-1} (\sum_{k=1}^{\infty} a_k T^k)^n}{n} \end{aligned}$$

とする. 同様にこれも welldefined. この時, $\exp \circ \log = \log \circ \exp = id$ となる. $\#V(F_{q^n})$ を有理点の位数とする.

Definition 6.2. ゼータ関数 $Z(V/\mathbb{F}_q; T)$ を以下で定義する.

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

- 代数多様体の定義 (古典的版, スキーム版)
- 代数多様体の還元
- \mathbb{C} 上の代数多様体が複素多様体になること - 特異コホモロジー. Betti 数が次元で Euler 標数はその交代和, つまり $\sum_{i=0}^{2d} (-1)^i \dim_{\mathbb{Q}} H^i X(\mathbb{C}), \mathbb{Q}$ となる.

6.2 楕円曲線の場合の証明

楕円曲線 E の場合に Weil 予想を示す. AEC に沿って示すので, コホモロジーの部分は特に触れない.

Example 6.3. V として, \mathbb{P}^N を取る. この時,

$$\#\mathbb{P}^N(\mathbb{F}_{q^n}) = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^N q^{ni}$$

となる. この時,

$$\log Z(\mathbb{P}^N/\mathbb{F}_q; T) = \sum_{n=1}^{\infty} \left(\sum_{i=0}^N q^{ni} \right) \frac{T^n}{n} = \sum_{i=0}^N -\log(1 - q^i T).$$

となる. これより

$$Z(\mathbb{P}^N/\mathbb{F}_q; T) = \frac{1}{(1-T)(1-qT)\dots(1-q^N T)}$$

となる.

標数 p の有限体の場合の楕円曲線での性質を調べる
 l を p と異なる整数とする.

$$\mathrm{End}(E) \rightarrow \mathrm{End}(T_l(E)), \phi \rightarrow \phi_l$$

が定まる.

$\det(\phi_l), \mathrm{tr}(\phi_l)$ を定義できる.

Proposition 6.4. $\phi \in \mathrm{End}(E)$ とする. この時,

$$\det(\phi_l) = \deg(\phi), \mathrm{tr}(\phi_l) = 1 + \deg(\phi) - \deg(1 - \phi).$$

となる. 特に, $\det(\phi_l), \mathrm{tr}(\phi_l)$ は l の取り方によらない.

これを使って $\#E(\mathbb{F}_q^n)$ を計算しよう.

Theorem 6.5. E/\mathbb{F}_q を楕円曲線とする,

$$\phi E : \rightarrow E, (x, y) \rightarrow (x^q, y^q)$$

を q 上 *Frobenius* とし, $a = q + 1 - \deg(\phi)$ とする.

1. $\alpha, \beta \in \mathbb{C}$ を $T^2 - aT + q$ の 2 つの根とする. この時, α と β は複素共役で, $|\alpha| = |\beta| = \sqrt{q}$ となる. また. $n \geq 1$ のとき,

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

2. Frobenius ϕ は以下を満たす.

$$\phi^2 - a\phi + q = 0$$

Proof. $a \in \mathbb{F}_q$ とすると $a^q = a$ は $a \in \mathbb{F}_q$ と同値になるので $E(\mathbb{F}_q) = \text{Ker}(1 - \phi) = \text{deg}(1 - \phi)$ となる. 一番最後よくわからない? \square

7 p 進表現

7.1 p 進表現の定義

7.2 p 進周期環の定義

7.3 p 進表現の分類

admissible 表現幾何的な状態を知る。

良い還元準安定還元潜在的準安定還元すべての代数多様体
に対応するものとして、p 進周期環によるクラス分け

7.4 それ以外

Tate-Sen ϕ, Γ

8 p-adic 解析によるヴェイユ予想の証明

p-adic 解析を使ってヴェイユ予想を示す.

8.1 A formula for the number of \mathbb{F}_q points on a hypersurface

\mathbb{F}_q 上の代数多様体 X のゼータ関数の有理性を示す. Lecture3(**あとで確認する. **) より, X が $\mathcal{A}_{\mathbb{F}_q}^d$ の $f \in \mathbb{F}_q[x_1, \dots, x_d]$ で定義された hypersurface の時に示せばよい. さらに, 帰納法に基づく簡単な議論と, inclusion-exclusion principle により, 証明すべき問題を以下の関数の有理性を示すことに帰着できる. (帰着の部分は後で示す.)

$$\tilde{Z}(X, t) := \exp\left(\sum_{n \geq 0} \frac{N'_n}{n} t^n\right).$$

であって,

$$N'_n = |\{u = (u_1, \dots, u_d) \in \mathbb{F}_{q^n}^d \mid f(u) = 0, u_i \neq 0 \text{ for all } i\}|$$

N'_n を \mathbb{F}_{q^n} の加法指標 (??) を用いて書き直す.

Lemma 8.1. $\epsilon \in \bar{\mathbb{Q}}_p$ を 1 の原始 p 乗根とする. この時, $\xi(u) := \epsilon^{\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(u)}$ は *nontrivial additive character* (const ではなく, 加法群から乗法群への準同型) になる.

Proof. $q^n = p$ の時, 位数 p の加法的巡回群を乗法的な巡回群に移すだけである. そのため, これは準同型となる.

$$\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p} : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_p$$

は加法的な全射準同型になっているので, Nontrivial な準同型になっている. \square

Remark. 有限体の間の拡大は巡回拡大のため,

$$\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(a) = a + a^p + \dots + a^{p^{n-1}}$$

ただし $q = p^e$

Lemma 8.2. ξ が *nontrivial additive character* なら, $\sum_{u \in \mathbb{F}_{q^n}} \chi(u) = 0$ となる.

あとで **

8.2 The construction of Theta

あとで **

8.3 Trace of certain linear maps on rings of formal power series

ζ 関数の有理性の証明に向け, 以下を示す.

Proposition 8.3. 任意の $X = V(f)$ ($f \in \mathbb{F}_q[x_1, \dots, x_n]$) に対し, 形式的べき級数 $\tilde{Z}(X, t)$ は $\frac{g(t)}{h(t)}$ と書ける. ただし, g, h は $\mathbb{C}[[t]]$ の元であって収束半径が ∞ となるもの.

$R = \mathbb{C}[x_1, \dots, x_N]$ とおき, \uparrow でその極大イデアルとする. $\alpha = (\alpha_1, \dots, \alpha_N) \in \mathbb{Z}_{\geq 0}^N$ とおき,

読みにくさこの上ない. どうしようか.

最後にスキームとエタールコホモロジーについて概観する? エタールコホモロジーがここまで細かいことになるとは理解できなかった。

9 スキームとスキームによる代数多様体の定義

9.1 エタール射

9.2 エタール基本群

エタール基本群

数論幾何入門

数論幾何の基本的な道具に触れる。ガロア理論 (圏論より)

体の理論で Hom による分類をする。

ガロア理論は、体を Fix した時にガロア群と拡大の間に圏同値があるよ。

ガロア理論数論なので、ガロア群に興味がある。ガロア群がどういう場合なら計算できるか? 数論的には、 \mathbb{Q} の絶対ガロア群を計算したい。じゃあ、どうしよう?

有限体の絶対ガロア群局所体のガロア群のアーベル部分代数体のガロア群のアーベル部分

ここまでは類体論でわかる。しかし、それ以降は計算できない。群は計算できない。⇒ならば、表現論だ。

群とは表現である。1. 群という非可換な対象を線形代数的に調べる方法 1. 古典的には群は表現 (作用) を考えられていた。

Open Problem 表現が完全に分類されたら、ガロア群は決定されるか? 数論上、重要な情報は表現に出てくると信じている (Philosophy)

実際に表現を構成しよう。

どうやって??? 有限群の表現論などを考える場合、群の構造がわかっていするため、表現を決定できる、あるいは表現したいものがわかるために、逆にこれに表現として実現できる群を決定できる。

表現として実現したい群がわからない場合、どうやって表現を作る・・・?
⇒ Etale Cohomology l 進、p 進で理論がぜんぜん違う。

Weil 予想の意味はわからない。

楕円曲線の場合の Weil 予想の証明はしてもいいけど、それは面白く無いと個人的に思っている。なぜなら、ロマンがないから。エタールコホモロジーらしさも圏論らしさもなくて、自分できっちり消化したいという人以外にはあまりおすすめできない。

スキームと代数多様体の一般論についてアフィンスキームが図形に見えるための努力

不分岐とは下と上が同じという話。

エタールコホモロジーが取れることについてなんとかなるのかな位相幾何との類似なんてもうほとんど忘れてしまった。

p 進が面白いかと言われたら、よくわかんと応える。 l 進が面白いかと言われたらそれもよくわかんと応える。

ただ、緻密な理論とその裏にあるわからない問題たちに興奮する。構造をきっちり決定すること自体に興味があるんだから、圏論は本来向いていると思う。

コホモロジーと L 関数 Cohomology と L 関数の間にどんなつながりがあるのかが全然わからない。

Cohomology から L 関数を構成する？

10 数論のモチベーション

10.1 体とガロア理論

数論の前提知識とモチベーション

- ガロア理論
- 有限体の絶対ガロア群
- 代数体の絶対ガロア群について．局所類体論と大域類体論，ガロア表現
⇒ etale cohomology(l, p 進表現)

ガロア理論を簡単に概観しよう．まず，体と，体同士の準同型を定義する．

Definition 10.1. K が体とは以下を満たす時である．

1. $+: K \times K \rightarrow K, \cdot: K \times K \rightarrow K$ が定義されている．
2. K は $+$ でアーベル群になり、その単位元を 0 と表す．
3. $K - \{0\}$ は \cdot について乗法群となり、その単位元を 1 と表す．
4. $a \cdot (b + c) = a \cdot b + a \cdot c$ となる．

Definition 10.2. 1. $+: K \times K \rightarrow K, \cdot: K \times K \rightarrow K$ が定義されている．

2. 任意の $a, b, c \in K$ に対し、 $(a + b) + c = a + (b + c)$ となる．
3. 任意の $a, b \in K$ に対し、 $a + b = b + a$ となる．
4. 任意の $a \in K$ に対し、 $a + 0 = 0 + a = a$ を満たす元 $0 \in K$ が存在する．
5. 任意の $a \in K$ に対し、 $a + b = b + a = 0$ を満たす元 $b \in K$ が存在する．
6. 任意の a, b に対し、 $a \cdot b = b \cdot a$ となる．
7. 任意の $a \in K$ に対し、 $a \cdot 1 = 1 \cdot a = a$ を満たす元 $1 \in K$ が存在する．
8. 任意の $a \in K - \{0\}$ に対し、 $a \cdot b = b \cdot a = 1$ となる $b \in K$ が存在する．

9. 任意の $a, b, c \in K$ に対し, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ となる.

ざっくりというなら, 足し算, 引き算, 掛け算, 割り算が定義できるものが体である.

Example 10.3. 実数全体のなす集合 \mathbb{R} は体をなす.

体同士の写像を定義しよう. 体 K, L に対し, $\text{Hom}(K, L)$ の元を $f: K \rightarrow L$ であって, 以下を満たすものとする.

1. $f(x + y) = f(x) + f(y)$

2. $f(xy) = f(x)f(y)$

3. $f(1) = 1$

Remark. $f(1) = 1$ を課さない定義であってもよい. ($f(1) = 1$ を満たさず, 残りの 2 つを満たす射は任意の元を 0 に映す写像のみである.) 体では基本, 拡大を考えるため, そのような写像に興味がない. って今回は $f(1) = 1$ を課した.

体同士の準同型には以下の性質がある.

Proposition 10.4. 体の準同型 $f: K \rightarrow L$ は単射である.

Proof. $a \in K$ に対し, $f(a) = 0$ となったとすると. a が 0 がでないとして, 乗法について逆元 a^{-1} を持つ. この時, $f(a \cdot a^{-1}) = 1$ となるが, これは $0 \cdot f(a^{-1}) = 1$ となり, 矛盾する. よって $a = 0$ となり, 単射が示された. \square

体同士の射は単射であるため, この射を通して, 体 K を体 L の部分集合とみなすことが多い. この時, 体 K を体 L の部分体といい, L を K の拡大体という. また体 L が体 K の拡大となってい時, 拡大 L/K と書く.

体の拡大を詳しくみていく.

Definition 10.5. 拡大 L/K に対し, $a \in L$ が K 上代数的であるとは, ある K 係数多項式 $f(X)$ が存在し, $f(a) = 0$ となることである. 任意の $a \in L$ が K 上代数的であるとき, L/K を代数拡大という. また, a に対し $f(a) = 0$ となる. 次数が最小のものを a の K での最小多項式という.

Definition 10.6. K が代数閉体とは, 任意の拡大 L/K が代数拡大である場合, $L = K$ となるものをさす. つまり, K 係数 1 変数多項式は必ず K 上一次式の積でかける.

Proposition 10.7. 任意の体 K に対し, 代数拡大体 L で L が代数閉体となるものが存在する.

Proof. 代数拡大に対してツォルンの補題から, 極大が取れる. ? 思った以上に具体的にかけた. \square

上の操作を代数閉包という，以降では包含を明確にするため，代数閉体を一つ Fix して，その部分体についてのみ議論する．

拡大 L/K 拡大に対しては K -準同型が定義できる． $f: L \rightarrow M$ が K -準同型とは， f が体の準同型であり，かつ， $f|_K = id_K$ となることである．

Definition 10.8. L/K が分離拡大とは，任意の $a \in L$ の最小多項式が分離多項式になること．分離多項式とは a で重根を持たない多項式のことである．

Proposition 10.9. K が標数 0 の体の時，任意の代数拡大 L/K は分離拡大になる．

Proof. $a \in L$ の K 上の最小多項式を $f(x)$ とする． $f(x)$ が分離多項式でないとする，ある a が存在し， $f'(a) = 0$ となること．

$$f(x) = \sum_{k=0}^n c_k x^k$$

とすると，

$$f'(x) = \sum_{k=1}^n k c_k x^{k-1}$$

となり， $f(x)$ が最小多項式なので， $f'(a) = 0$ から， $f'(x) = 0$ となる．標数 0 の場合は， $f'(x) = 0$ より， $f(x)$ は定数となる．最小多項式は定義から 1 次以上の多項式なので，定数とはならない．よって， L/K は分離拡大になる． \square

Proposition 10.10. 標数 p の時，既約多項式 $q(x) \in K[X]$ が重根を持つ必要十分条件は多項式 $g(y)$ が存在して， $g(y^p) = q(x)$ となること．

Proof. 必要性は微分が 0 になることより，明らか．十分性を示す． $q(x) = g(x^p)$ とかけたとする．今 α が q の解だとし， q の分解体を L とする． $g(a^p) = 0$ より．

$$q(x) = g(x^p) = (x - \alpha^p)h(x^p) = (x - \alpha)^p h(x^p)$$

となるので重根を持つことがわかる． \square

Definition 10.11. L/K が純非分離拡大とは， $L \setminus K$ の任意の元の最小多項式が非分離多項式となること．

Definition 10.12. K が完全体とは任意の代数拡大 L/K が分離拡大となること．

Proposition 10.13. 標数 p の体 K が完全体であることは任意の $a \in K$ に対し， $b^p = a$ となる $b \in K$ が存在すること

Proof. F が完全体でないとする。すると、既約多項式で分離的でないもの、すなわち、 $f(X) = g(x^p)$ とかけるものが存在する。そのため、もし、 $b^p = a$ となる $b \in K$ が存在したとすると、

$$f(x) = g(x^p) = \sum_{k=0}^n a_k x^{pk} = \sum_{k=0}^n b_k^p x^{pk} = \left(\sum_{k=0}^n b_k x^k \right)^p$$

とかけ、既約性に反する。 K が完全体の時に、任意の $a \in K$ に対し、 $b^p = a$ となる $b \in K$ が存在することを示す。 $X^p - a$ の K 上の分解体を L とする。この時、 $\alpha \in L$ で $\alpha^p = a$ となるものが存在する。これより、 $x^p - a = (x - \alpha)^p$ となるので、 α の最小多項式は $(x - \alpha)^p$ を割る、 K は完全体なので、 $x - \alpha \in K$ となる。 \square

Proposition 10.14. L/K を有限次分離拡大とすると、 L は単項生成できる。

Proposition 10.15. L/K が有限次拡大とすると、 L 上の K 自己同型の個数は $[L : K]$ 個以下となる。

Proposition 10.16. L/K が有限次分離拡大とすると、 L 上の K 自己同型の個数は $[L : K]$ 個となる。

Definition 10.17. L/K が有限次拡大とすると、 K_s を K 上分離な元のなす体とする。 L/K の分離次数を $[K_s : K]$ 、非分離次数を $[K : K_s]$ とする。

Definition 10.18. L/K が正規拡大とは、

Definition 10.19. L/K がガロア拡大とは、有限次分離拡大

- 有限次拡大
- 代数拡大
- 正規拡大
- 分離拡大
- ガロア拡大
- アーベル拡大

10.2 有限体とその絶対ガロア群

ガロア理論により、ガロア群と体の拡大の関係がわかった。しかし、具体的にガロア群がどういうものかはガロア理論では特に記述していない。そのため、具体的にガロア群を計算してみよう。特に、絶対ガロア群を求めたい。まずは有限体に対して調べてみよう。有限体 \mathbb{F}_q とその代数閉包を一つ固定して議論する。

Propostion 10.20. 有限体は体の位数のみで一意に決まる.

体の準同型であり, 位数の議論より, 有限体は Frobenius が全射となる. そのため, 有限体の分離拡大となる.

10.3 局所体と大域体

有限体では, 絶対ガロア群が計算できた. この情報を使って代数体を含めた大域体や局所体について情報をどこまで調べられるかを考えたい. まず, 局所体と大域体を定義しよう.

Definition 10.21. K が局所体とは, $\mathbb{Q}_p, \mathbb{F}_p((T))$ の有限次代数拡大体のことである. K が大域体とは, \mathbb{Q} , および $\mathbb{F}_p(T)$ の有限次代数拡大体のことである.

10.4 類体論の主定理の紹介

局所体、大域体の類体論がどこまで何を記述しているのかについて触れる。