

# たいとる

おーさー

ひづけ

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Preparation of Algebra and Set</b>	<b>3</b>
2.1	環論の基本	3
2.1.1	環の定義と基本的性質	3
2.1.2	素イデアルと極大イデアル	3
2.1.3	多項式環とべき級数環	3
2.2	体とガロア理論	3
2.2.1	体の定義と代数拡大	3
2.2.2	体の超越拡大	4
2.2.3	体の分離拡大	4
2.2.4	体の正規拡大	5
2.2.5	ガロア理論	6
2.2.6	Frobenius と有限体	6
2.2.7	Trace と Norm	6
2.3	ガロアコホモロジー	6
<b>3</b>	<b>Basic Knowledge of p-adic Number</b>	<b>6</b>
<b>4</b>	<b>離散付値の一般論</b>	<b>7</b>
<b>5</b>	<b>代数多様体とヴェイユ予想</b>	<b>9</b>
<b>6</b>	<b>p-adic 解析によるヴェイユ予想の証明</b>	<b>9</b>
6.1	A formula for the number of $\mathbb{F}_q$ points on a hypersurface	9
6.2	The construction of $\Theta$	10
6.3	Trace of certain linear maps on rings of formal power series	12
6.4	The Rationality of the Zeta function	14
<b>7</b>	<b>スキームとスキームによる代数多様体の定義</b>	<b>16</b>
7.1	エタール射	16
7.2	エタール基本群	16

<b>8</b>	<b>数論のモチベーション</b>	<b>17</b>
8.1	体とガロア理論 . . . . .	17
8.2	有限体とその絶対ガロア群 . . . . .	17
<b>A</b>	<b>圏論</b>	<b>18</b>
<b>B</b>	<b>類体論</b>	<b>18</b>
B.1	類体論の主定理の紹介 . . . . .	18

## 1 Introduction

WeilConjecture に関する Dwork の結果とそれ以降のリジットとクリスタリンについて解説する.

### 1. $p$ 進数体の基礎

- 定義 (3 通り) or 4(Witt)
- 局所体であること.
- Hensel の補題
- $\log/\exp$  の定義
- 乗法群の構造の決定

### 2. 体の拡大と完備化

- Trace と Norm
- 分岐, 不分岐
- 整数環の拡大
- 付の延長
- 無限次元拡大と完備化

### 3. $p$ -adic な関数について

- $\mathbb{Z}_p$  での連続関数
- $\mathbb{Z}_p[[T]]$  の既約なべき級数について
- $\mathbb{C}_p[[T]]$  の元がいつ  $\mathbb{Q}(T)$  の元になるか.

### 4. Weil Conjecture の証明 (Dwork の結果)

- クリスタリンコホモロジーについて? (notes on crystalline cohomology)

## 2 Preparation of Algebra and Set

この本で使う基礎的な集合論や代数について解説する。目標は以下の2つである。

- Trace/Norm の定義
- Frobenius の定義とその性質

### 2.1 環論の基本

環論の基礎を紹介する。

#### 2.1.1 環の定義と基本的性質

環の定義や、環の基本的性質 (直積, 単元, イデアル) について説明する。

#### 2.1.2 素イデアルと極大イデアル

#### 2.1.3 多項式環とべき級数環

### 2.2 体とガロア理論

#### 2.2.1 体の定義と代数拡大

**Definition 2.1.** 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 2.2.** 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 2.3.** 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.  $a$  が 0 がでないとする, 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 2.4.** 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 2.5.**  $K$  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 2.6.** 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.

## 2.2.2 体の超越拡大

## 2.2.3 体の分離拡大

**Definition 2.7.**  $L/K$  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 2.8.**  $K$  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 2.9.** 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  $\alpha$  が  $q$  の解だとし,  $q$  の分解体を  $L$  とする.  $g(\alpha^p) = 0$  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 2.10.**  $L/K$  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 2.11.**  $K$  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 2.12.** 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,  $\alpha$  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 2.13.**  $L/K$  を有限次分離拡大とすると,  $L$  は単項生成できる.

**Proposition 2.14.**  $L/K$  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 2.15.**  $L/K$  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 2.16.**  $L/K$  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.

## 2.2.4 体の正規拡大

**Definition 2.17.** 任意の  $a \in L$  の  $K$  での最小多項式が  $L$  上  $l$  次式の積に分解する体である時  $L/K$  を正規拡大という.

**Definition 2.18.**  $L/K$  がガロア拡大とは, 分離かつ正規拡大であること.

### 2.2.5 ガロア理論

### 2.2.6 Frobenius と有限体

Frobenius と有限体の性質をみる.

**Definition 2.19.** 以下で定義される写像を *Frobenius* 写像という.

$$\text{Frob} : \mathbb{F}_q \rightarrow \mathbb{F}_q, a \mapsto a^q$$

Frobenius は同様に,  $\mathbb{F}_q[x] \rightarrow \mathbb{F}_q[x]$  にも拡張される. この時, 以下が成り立つ.

**Proposition 2.20.**  $f = \sum_{i=0}^n a_i X^i \in \mathbb{F}_q[X]$  に対し,  $f(X^q) = \sum_{i=0}^n a_i X^{iq} = (\sum_{i=0}^n a_i X^i)^q = f(X)^q$  となる.

*Proof.* 右辺の拡大次数が  $q$  で割れないところは必ず  $q$  が係数に入ること, フェルマーの小定理から  $a^q = a$  となるので, 従う. \*\*\*\*\* あとで細かい証明を埋める \*\*\*\*\*  $\square$

### 2.2.7 Trace と Norm

## 2.3 ガロアコホモロジー

## 3 Basic Knowledge of p-adic Number

$p$  進数と局所体の基礎について調べる.

$p$  を素数とする.

**Definition 3.1.**  $pr_n : \mathbb{Z}/p^n \rightarrow \mathbb{Z}/p^{n+1}, 1 \mapsto 1$  とする.  $\mathbb{Z}_p$  を以下で定義する.

$$\{(x_1, x_2, \dots, x_n, \dots) \in \prod_n \mathbb{Z}/p^n \mid pr_n(x_n) = x_{n+1}\}$$

$\mathbb{Z}/(p^n)$  が環となっており,  $pr_n$  が環準同型なので, 直積環の部分環になっている.

**Remark.** これは逆極限である.

これを  $p$  進整数環といい,  $\mathbb{Z}_p$  と書く. この環の性質を見ていく.  $S := \{1, \dots, p-1\}$  とする.  $(x_n)_n \in \mathbb{Z}_p$  に対し, 形式的な和  $a = \sum_{i=0}^n a_i p^i (a_i \in S)$  が任意の  $n$  に対し,  $a \equiv x_n \pmod{p^{n+1}}$  となる時,  $a$  を  $p$  進数展開という.

**Proposition 3.2.** 任意の  $(x_n)_n \in \mathbb{Z}_p$  に対し, ただ一つの  $p$  進数展開が存在する.

*Proof.*  $(a_n)_n \in S^{\mathbb{Z}_{\geq 0}}$  で, 任意の  $n$  に対し,  $x_n \equiv \sum_{i=0}^{n-1} a_i p^i \pmod{p^n}$  となるものがただ一つ存在することを示せばいい.  $x_n \equiv \sum_{i=0}^n a_i p^i \pmod{p^{n+1}}$  となる  $a_n$  がただ一つ存在することを帰納法で示す. これが示されればよい. なぜなら, もし, 一意でないとする, ある  $m$  に対し, 上を満たす  $a_n$  が一意でないことがわかるので, 矛盾する. また,  $(a_n)_n$  が条件を満たすので, 存在もわかる.

$\square$

余談, 疑問. いい言葉が思い浮かばない.

\*\*\*\*\*下の部分はちょっと知らない\*\*\*\*\* まず, 逆極限を定義する.

**Definition 3.3.**  $C$  を圏とし,  $I$  を友向順序集合とする. すなわち, 任意の  $i, j$  に対し,  $i < k, j < k$  となる  $k$  が存在する.  $I$  を順序により射をいれることで圏だと思える. この時, 関手  $F; I \rightarrow C$  を用いて,  $C$  の逆極限を定義する. これを

添字の間の圏はどうするか? 非常にづらい状態になっている.

$\mathbb{Z}[[T]]$  の元  $f(T) = \sum_{i=0}^{\infty} a_i T^i$  とする. ここには自然に加法と乗法が定義される. この  $T$  を  $p$  に置き換え, 形式的に加法と乗法を定義する.

$p$  進展開を定義する.

**Proposition 3.4.**  $S$  を  $\{0, 1, \dots, p-1\}$  とする.  $(x_n)_{n \geq 0} \in \mathbb{Z}_p$  に対し, ある  $(a_k) \in S^{\mathbb{N}}$  がただ一つ存在し, 任意に  $n$  に対し以下が成り立つ.

$$x_n \equiv \sum_{k=0}^n a_k p^k \pmod{p^{n+1}}. \quad (1)$$

*Proof.*  $n$  について帰納的に示す.  $n=0$  の場合は明らかに上の式が成り立つ  $a_0$  がただ一つ存在する.  $0, \dots, n-1$  で成り立つとする.  $p x_n - x_{n-1} = 0$  より,  $a \in S$  がただ一つ存在し,

$$x_n - p^n a - \sum_{k=0}^{n-1} \overline{a_k p^k} \equiv 0 \pmod{p^{n+1}}$$

となる. よって成り立つ. □

以降の話は完備離散付値環にも自然に拡張できるが, 簡単のため  $\mathbb{Z}_p$  の場合に説明する.

**Theorem 3.5 (Hensel's lemma).**  $\mathbb{Z}_p$  係数の多項式  $f(T) \in \mathbb{Z}_p[T]$  が剰余体  $\mathbb{F}_p$  上で, 2 つの互いに素な多項式  $\phi, \psi \in \mathbb{F}_p[T]$  を用いて  $\bar{f} = \phi \cdot \psi$  とかけたとする. この時, 以下を満たす  $\mathbb{Z}_p$  係数多項式  $g, h$  が存在する.

- $f = g \cdot h$
- $\bar{g} = \phi, \bar{h} = \psi$
- $\deg g = \deg \phi$

\*\*\*\*\* あとで埋める \*\*\*\*\*

Hensel の補題の応用を 2 つ述べる.

**Corollary 3.6.**  $p \geq 3$  とする.  $\mathbb{Z}_p$  上に存在する 1 の  $p$  べき根は  $p-1$  乗根.

**Corollary 3.7.**  $\mathbb{Q}_p$  上の既約多項式  $f(T) = \sum a_n T^n$  が  $a_0 \in \mathbb{Z}_p$  とする.

## 4 離散付値の一般論

**Theorem 4.1 (Hensel's lemma).**  $K$  を完備離散付値環とする.

剰余体との関係と主単数群を定義する.

Exponential と Log が定義できること

付値の延長について示す.

**Theorem 4.2.** 完備離散付値体  $K$  の付値を  $v_K$  とする. 有限次元代数拡大  $L$  に対し付値は  $v_L$  に一意に延長できる. また, その付値は完備離散付値となり, 以下が成り立つ.

- $v_L(x) = \frac{1}{[L:K]} v_K(N_{L/K}(x))$
- $L$  の完備離散付値環  $O_L$  は,  $O_K$  の  $L$  での整閉包
- $n = ef$ . ただし,  $e$  は  $v_L(\pi_K) = ev_L(\pi_L), f = [F_L : F_k]$

*Proof.* ノルムが付値の延長になること.  $L/K$  が有限次元拡大の時,  $N_{L/K}(x)$  を以下で定める.  $\cdot x : L \rightarrow L, a \mapsto ax$  は  $K$ -vector space の自己準同型を定めるので, 表現行列が取れる. その表現行列の行列式をノルムで定める.

余談, 疑問. 基底のとり方に本当によらない? 元と先で基底取り替えたら変わるように思えてきた.

まず,  $x \in K$  に対して, 積が定める行列は  $xE$  になるので,  $N_{L/K}(x) = x^{[L:K]}$  となる. これより,  $x \in K$  に対し,  $v_L(x) = v_K(x)$  となることがわかる.  $v_L(xy) = v_L(x) + v_L(y)$  はノルムが体の乗法群から体の乗法群への準同型になっているので, 成り立つ.

$v_L(x) \geq v_L(y)$  とする.  $v_L(x+y) = v_L(y) + v_L(x/y + 1)$  となるので任意の  $v_L(z) \geq 0$  に対し,  $v_L(z+1) \geq 0$  を示せば良い.  $z$  の  $K$  での最小多項式を

$$f(T) = T^m + a_1 T^{m-1} + \cdots + a_m$$

とする. この時  $N_{L/K}(z) = N_{L/K(z)} \circ N_{K(z)/K}(z) = a_m^{[L:K]/m}$  となるので,  $v_K(a_m) = v_L(a_m) \geq 0$  となる. 完備離散付値の既約多項式は  $v_K(a_m) \geq 0$  ならば,  $v_K(a_i) \geq 0$  となる. また,  $z+1$  の最小多項式は  $f(T-1)$  となり, その定数項は  $\sum (-1)^{m-k} a_k$  となる. 上より,  $v_L(\sum (-1)^{m-k} a_k) \geq 0$  となるので, 言えた.

離散付値環の元が整であること  $v_L$  については上の証明より明らか.

整ならば離散付値環の元であること  $x^m = a_1 x^{m-1} + \cdots + a_m$  となったとする. これより,  $v_L(x^m) \geq v_L(a_i x^i) \geq v_L(x^i)$  となるので, 離散付値環の元であることがわかる.

付値の一意性  $\lambda$  を  $L$  の離散付値とする.  $v_L$  と  $\lambda$  が一致することを示す. 整ならば, 離散付値環の元であることは上から明らかで  $v_L$  が定める離散付値環の元も整なので,  $O_L \subset O_\lambda$  となる. 逆の包含を示す.  $O_\lambda$  の極大イデアルを  $\mathfrak{p}_\lambda$  とする. すると,  $O_L \subset \mathfrak{p}_\lambda$  は素イデアルあつて,  $\mathfrak{p}_K \subset O_L \subset \mathfrak{p}_\lambda$  より  $0$  ではないので,  $\mathfrak{p}_L$  となる. これから  $v_L(x) < 0$  とすると,  $v_L(x^{-1}) > 0$  となり,  $\lambda(x^{-1}) > 0$  となるので,  $\lambda(x) < 0$  となる. これより, 逆の包含も言えた.

次元の公式 整基底として,  $\langle \pi_L^i \rangle$  が取れる.

完備性

□

無限次元拡大は完備とも離散とも限らない.

$\mathbb{C}_p$  は完備化で  $\mathbb{C}_p$  は代数閉体



## 5 代数多様体とヴェイユ予想

代数多様体を定義し、ヴェイユ予想を述べる。

## 6 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。ここでいう p-adic 解析とは  $\mathbb{Z}_p, \mathbb{C}_p$  のべき級数の理論を使って、有理性を示すということである。証明の概略をのべる。ゼータ関数自体は  $\mathbb{Z}$  係数の形式的べき級数で、これがユークリッドノルムで絶対収束し、かつ、p-adic 位相でも収束する場合に  $\mathbb{Q}$  係数の有理型関数となるという命題がある。この条件を満たすことを使う。実に対する収束は位数の議論なので、射影空間の場合に比較することで簡単に示せる。p-adic 付値については、いくつかの方法を準備する。Trace を使って示す。それを最大限活用する。

### 6.1 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 6.1.**  $\epsilon \in \bar{\mathbb{Q}}_p$  を 1 の原始  $p$  冪根とする。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。 □

**Remark.** 有限体の間の拡大は巡回拡大のため、

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

ただし  $q = p^e$

**Lemma 6.2.**  $\chi$  が *nontrivial additive character* なら、 $\sum_{u \in \mathbb{F}_{q^n}} \chi(u) = 0$  となる。

*Proof.*  $\chi(t) \neq 0$  とする.

$$\sum_{u \in \mathbb{F}_{q^n}} \chi(u) = \sum_{u \in \mathbb{F}_{q^n}} \chi(u+t) = \chi(t) \sum_{u \in \mathbb{F}_{q^n}} \chi(u)$$

となる. 仮定より  $\chi(t) \neq 0$  となるので, いえた.  $\square$

$f \in \mathbb{F}_q[x_1, \dots, x_n], \phi_n : \mathbb{F}_{q^n} \rightarrow \bar{\mathbb{Q}}_p$  を nontrivial additive character とする.  $a \in \mathbb{F}_{q^n}$  が 0 でない時,  $\sum_{v \in \mathbb{F}_{q^n}} \phi_n(va) = 0$  となる. また,  $a = 0$  の時は  $q^n$  となる. これより

$$\sum_{u \in (\mathbb{F}_{q^n}^*)^d} \sum_{v \in \mathbb{F}_{q^n}} \phi_n(vf(u)) = N'_n q^n.$$

また,  $v = 0$  の時の和が  $(q^n - 1)^d$  となるので,

$$\sum_{u \in (\mathbb{F}_{q^n}^*)^d} \sum_{v \in \mathbb{F}_{q^n}} \phi_n(vf(u)) = N'_n q^n - (q^n - 1)^d. \quad (2)$$

となる. この節では, (1) の左辺を  $u_1, \dots, u_n, v$  にタイヒミュラーリフトをしたものの解析的関数に代入する.  $a \in \mathbb{F}_{p^m}$  に対し,  $\mathbb{Q}_p$  の  $m$  次の不分岐拡大体 (剰余体が  $\mathbb{F}_{p^m}$ ) の整数環の元  $\tilde{a}$  で *reduciton* ですると  $a$  になるものを一つ *Fix* する. これをタイヒミュラーリフトという.

$a \in \mathbb{F}_{q^n}$  に対し, 以下の性質を持つ  $\Theta \in \mathbb{Q}_p(\varepsilon)[[T]]$  を作る.

**P1**  $\Theta$  の収束半径が 1 より大きい.

**P2** 任意の  $n \in \mathbb{Z}_{\geq 0}, a \in \mathbb{F}_{q^n}$  に対し,

$$\varepsilon^{\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(a)} = \Theta(\tilde{a})\Theta(\tilde{a}^q) \cdots \Theta(\tilde{a}^{q^n-1}) \quad (3)$$

$$f = \sum c_m x^m \in \mathbb{F}_q[X_1, \dots, X_d]$$

\*\*\*\*\* あとで埋める \*\*\*\*\*

## 6.2 The constructrion of $\Theta$

上で書いた  $\Theta$  を具体的に構成する.  $q = p$  の時に示せば, 以下より一般に示せる.  $q = p^e$  とする  $p$  の時に上の性質を満たすべき級数を  $\Theta_1(X)$  とする. この時,  $\Theta(X) = \Theta_1(X)\Theta_1(X^p) \cdots \Theta_1(X^{p^{e-1}})$  とすればよい. これは収束半径が 1 以上のものの積なので, 明らかに収束半径が 1 以上になり,

$$\varepsilon^{\text{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(a)} = \prod_{i=0}^{ne-1} \Theta_1(\tilde{a}^{p^i}) = \prod_{j=0}^{n-1} \Theta(\tilde{a}^{q^j})$$

となるので. 以降では  $q = p$  とする. ベキ級数をいくつか定義する. まず.

$$(1+y)^x := 1 + \sum_{n=1}^{\infty} \frac{x(x-1) \cdots (x-n+1)}{n!} y^n$$

とする. これは  $\mathbb{Q}[[x, y]]$  の元となる.

余談, 疑問. ベキ級数を集合的に定義しようとするとうどうするんだっけ? 多項式環をイデアル  $(x)$  で割って完備化する?

$$F(x, y) = (1+y)^x (1+y^p)^{\frac{x^p-x}{p}} \dots (1+y^{p^n})^{\frac{x^{p^n}-x^{p^{n-1}}}{p^n}}$$

これは  $n+1$  次の factor  $(1+y^{p^n})^{\frac{x^{p^n}-x^{p^{n-1}}}{p^n}}$  が  $1+(y^{p^n})$  の元となる．そのため，べき級数  $F(x, y)$  の各係数は有限和なので，well-defined.  $F(x, y)$  には以下が成り立つ．

**Proposition 6.3.**  $F(x, y) \in \mathbb{Z}_p[[x, y]]$

これを示すために以下の補題を示す．

**Lemma 6.4.**  $f \in \mathbb{Q}_p[[x, y]]$  が  $f(0, 0) = 1$  を満たすとする．この時,  $f \in \mathbb{Z}_p[[x, y]]$  は以下と同値．

$$\frac{f(x^p, y^p)}{f(x, y)^p} \in 1 + p(x, y)\mathbb{Z}_p[[x, y]]$$

**Remark.** これは  $n$  変数の多項式でも成り立つが記号が複雑になるため，2 変数の場合にのみ示す．

余談，疑問． $p(x, y)$  は多項式に見えるがイデアルである．きっと，これはこの2つがほとんど差がないということを示してるのだと思う．

*Proof.*  $\Rightarrow$  を示す

形式的べき級数の定数項  $f(0, 0) = 1$  が単元になっているので， $f(x, y) \in \mathbb{Z}_p[[x, y]]^\times$  となる．同様に  $f(x, y)^p \in \mathbb{Z}_p[[x, y]]^\times$  となる． $g(x, y) = f(x, y)^{p-1}$  とする． $g(x, y)f(x, y)^p = 1$  より，係数を比較すると  $g(0, 0)f(0, 0) = 1$  となり， $g(0, 0) = 1$  となる．よって， $f(x^p, y^p)g(x, y) \in (x, y)\mathbb{Z}_p[[x, y]]$  となる．また， $f(x^p, y^p) \equiv f(x, y)^p \pmod{p}$  なので， $\pmod{p}$  すると 1 になる．よって．言えた．

$\Rightarrow$  を示す

$f(x, y) = \sum a_{nm}x^n y^m$  と書く．仮定より，ある  $g(x, y) \in 1 + p(x, y)\mathbb{Z}_p[[x, y]]$  が存在し

$$\sum a_{nm}x^{pn}y^{pm} = \left(\sum a_{nm}x^n y^m\right)^p \left(\sum b_{nm}x^n y^m\right)$$

となる．上の式の  $x^n y^m$  次の係数を  $c_{nm}$  と書く．次数に関する帰納法で示す．具体的には， $i \leq n, j \leq m$  でどちらか一方は少なくとも真に不等号になっているときに成り立つと仮定して， $a_{nm} \in \mathbb{Z}_p$  を示す．上の等式の左辺に着目すると， $p|n, p|m$  以外の時は  $c_{nm} = 0$  となる．そのため， $p|n, p|m$  とする．右辺をみると  $c_{nm} = pa_{nm} + Q_1 \dots + Q_r$  と書ける．ただし  $Q_i = Nb_{i'j'}a_{i''j''}$ ．帰納法の仮定より， $Q_1 + \dots + Q_r \in \mathbb{Z}_p$  また，右辺に着目すると， $c_{nm} = a_{n/pm/p}$  となる．また， $Q_j \notin p\mathbb{Z}_p$  の時， $i, j$  の少なくとも一方が 1 以上の場合， $b_{ij} \in p\mathbb{Z}_p$  となることから  $b_{00}$  がかかっており，また， $p$  が素数であることから上以外の場合は  $p$  で割れることがわかる．これより， $Q_j = a_{n/pm/p}^p$  となる． $a_{n/pm/p} \equiv a_{n/pm/p}^p \pmod{p}$  より， $Q_j \equiv c_{nm} \pmod{p}$  となるので， $pa_{nm} \in p\mathbb{Z}_p$  となることがわかる．よって  $a_{nm} \in \mathbb{Z}_p$  となる．□

命題を示そう．

*Proof.*  $F(0, 0) = 1$  より，上の lemma から  $\frac{F(x^p, y^p)}{F(x, y)^p} \in 1 + p\mathbb{Z}_p$  となることを示せばよい．

$$\frac{F(x^p, y^p)}{F(x, y)^p} = \frac{(1+y^p)^p x \cdot (1+y^{p^2})^{\frac{x^{p^2}-x^p}{p}} \dots}{(1+y)^{px} (1+y^p)^{x^p-x} \cdot (1+y^{p^2})^{\frac{x^{p^2}-x^p}{p}} \dots} = \left(\frac{1+y^p}{(1+y)^p}\right)^x$$

となる． $1+y \in \mathbb{Z}_p[[y]]$  より，上の式は  $(1+pw)^x$  ただし， $w \in \mathbb{Z}_p[[y]]$  とかける．

$$(1+pw)^x = 1 + \sum_{m \geq 1} \frac{x(x-1) \dots (x-m+1)}{m!} p^m w^m$$

とかけ，係数の付値を計算することで言える．

□

余談, 疑問. 計算が最後面倒くさくなった

$\varepsilon \in \overline{\mathbb{Q}_p}$  を 1 の  $p$  乗根とする.  $\lambda = 1 - \varepsilon$  とする. この時以下が成り立つ.

**Lemma 6.5.**  $|\lambda| = \left(\frac{1}{p}\right)^{1/p-1}$

\*\*\*\*\*後で\*\*\*\*\*

$\Theta(t) = F(t, \lambda)$  とする. まず, これが収束半径が 1 以上であることを示す.

**Lemma 6.6.**  $\Theta(t)$  の収束半径は少なくとも  $p^{1/p-1} 1$  となる.

後で後で

**Lemma 6.7.** 任意の  $n \geq 1, a \in \mathbb{F}_{p^n}$  に対し,

$$\varepsilon^{\text{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(a)} = \Theta(\tilde{a})\Theta(\tilde{a}^p) \cdots \Theta(\tilde{a}^{p^{n-1}}).$$

\*\*あとで\*\*

### 6.3 Trace of certain linear maps on rings of formal power series

この subsection では,  $\zeta$  関数の有理性の証明に向け, 以下を示す.

**Proposition 6.8.** 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  $\infty$  となるもの.

この定理を示すための準備を行う. 記号の簡略化のため,  $\mathbb{C}_p[x_1, \dots, x_N]$  を  $R$  で表す.  $\alpha = (\alpha_1, \dots, \alpha_N) \in \mathbb{Z}_{\geq 0}^N$  とおく.  $x^\alpha = x_1^{\alpha_1} \cdots x_N^{\alpha_N}$  また,  $|\alpha| = \sum \alpha_i$  とする.  $\mathfrak{m}$  を  $R$  の極大イデアルとする.  $R$  には極大イデアルにより位相を定める.  $R$  の極大イデアルがただひとつなことは, 係数形式的べき級数環の単数は定数項が単元であることと  $R \setminus R^\times$  は定数項が常に 0 になる形式的べき級数全体で, イデアルとなることからわかる.  $\text{ord}(h)$  を  $h \in \mathfrak{m}^r$  を満たす最大の  $r$  とする.  $R$  には  $\mathfrak{m}$  による位相を定める.

**Remark.**  $R$  は  $d(f, g) = p^{-\text{ord}(f-g)}$  では距離空間にならない. なぜ??? 非アルキメデス距離ではない. そもそも一変数の場合も最小次数の方が order だ. 例えば  $f = x - y^3, g = x - z^3$ , とすると,  $d(f, g) = 1/p, d()$  三角不等式を満たさないことがわかる??

さて,  $\mathbb{C}_p$ -位相ベクトル空間の準同型  $A: R \rightarrow R$  を考えたい. 元を使って写像の行き先を書くと,  $A(x_\beta) = \sum a_{\alpha\beta} x_\alpha (a_{\alpha\beta} \in \mathbb{C}_p)$  となる. この時,  $(a)_{\alpha\beta}$  を行列の一般化だと解釈する. 実際に  $(a)_{\alpha\beta}$  の成分で 0 でないものが有限個の時は像が 0 でない部分に制限することで, 行列表示できる. この時,  $A$  が finite support を持つという. 各次数には, 有限和しかされないの, finite support でなくても, 成分表示を用いて積を記述できる.

準同型の中で重要なものをいくつか定義する.  $H \in R$  に対し,  $\Phi_H: R \rightarrow R, f \mapsto H \cdot f$  と定める. これは  $\mathbb{C}_p$ -linear かつ連続になる.  $H = \sum h_\alpha x^\alpha$  に対し,  $\Phi_H$  は  $(h_{\alpha-\beta})_{\alpha\beta}$  となる. ただし,  $\alpha - \beta \notin \mathbb{Z}_{\geq 0}^N$  の時は  $h_{\alpha-\beta} = 0$  とする. 他に重要な例として,  $T_q: R \rightarrow R, \sum_\alpha a_\alpha x^\alpha \mapsto \sum_\alpha a_{q\alpha} x^\alpha, \Phi_{q,H} = T_q \circ \Phi_H$  がある.

$$\Phi_{q,H}(x^\beta) = T_q\left(\sum h_\alpha x^{\alpha+\beta}\right) = T_q\left(\sum h_{\alpha-\beta} x^\alpha\right) = \sum h_{q\alpha-\beta} x^{q\alpha}$$

となる. よって,  $\Phi_{q,H}$  は  $(h_{q\alpha-\beta})_{\alpha,\beta}$  とかける.

**Lemma 6.9.**  $\Phi_H \circ T_q = \Phi_{q,H_q}$  となる．ただし,  $H_q(x_1, \dots, x_N) = H(x_1^q, \dots, x_N^q)$ .

*Proof.* 定義に従い．左辺と右辺を計算して一致することを確認する．左辺を計算する．

$$\begin{aligned}\Phi_H \circ T_q(\sum b_\beta x^\beta) &= \Phi_H(\sum b_{q\beta} x^\beta) \\ &= \sum_\gamma \sum_{\alpha+q\beta=\gamma} h_\alpha b_\beta x^\gamma\end{aligned}$$

右辺を計算する． $H_q = \sum h_\alpha x^{q\alpha}$  に注意すると

$$\begin{aligned}T_q \circ \Phi_{H_q}(\sum b_\beta x^\beta) &= T_q(\sum_\gamma \sum_{q\alpha+\beta=\gamma} h_\alpha b_\beta x^\gamma) \\ &= \sum_\gamma \sum_{q\alpha+\beta=q\gamma} h_\alpha b_\beta x^\gamma\end{aligned}$$

となる．これより，以下が言えればよい．

$$\sum_{\alpha+q\beta=\gamma} h_\alpha b_\beta = \sum_{q\alpha+\beta=q\gamma} h_\alpha b_\beta$$

それは右辺で  $q\alpha + \beta = q\gamma$  から  $\beta$  が  $q$  で割れることから従う．

□

$A : R \rightarrow R$  に対し,  $\sum (a_{\alpha\alpha})$  が収束する時, それを  $\text{Trace} A$  と書く． $R_0$  を  $H = \sum h_\alpha x^\alpha \in R$  であって, ある  $M > 0$  が存在し任意の  $\alpha \in \mathbb{Z}_{\geq 0}^N$  に対し,  $|h_\alpha|_p \leq \left(\frac{1}{p}\right)^{M|\alpha|}$  を満たすもの全体からなる集合とする．

**Remark.**  $H \in R_0$  なら, 収束半径が 1 以上の収束べき級数となる．

**Lemma 6.10.**  $R_0$  は  $R$  の *subring* となる． $j_1, \dots, j_N$  を整数とし,  $H \in R_0$  とする．この時,  $H(x_1^{j_1}, \dots, x_N^{j_N}) \in R_0$  となる．

*Proof.*  $|h_1 - h_2|_p \leq \max\{|h_1|_p, |h_2|_p\}$  より部分環になる．また, べき乗の場合,  $(j_1\alpha_1, \dots, j_N\alpha_N)$  乗の係数が  $h_\alpha$  になるので,  $j_i$  の最大値を  $j$  とし,  $M/j$  を取ればよい．

□

**Proposition 6.11.**  $H \in R_0$  とし, ある  $q \geq 2$  に対し,  $\Phi = \Phi_{q,H}$  とする．任意の  $s \geq 1$  に対し,  $\Phi^s$  の  $\text{Trace}$  は *well-defined* である．また,

$$(q^s - 1)^N \text{Trace}(\Phi^s) = \sum_u H(u) H(u^q) \dots H(u^{q^{s-1}})$$

右辺の  $\text{sum}$  は  $u = (u_1, \dots, u_N) \in \mathbb{C}_p^N$  で, 任意の  $i$  に対し,  $u_i^{q^s-1} = 1$  を満たす  $u$  を走る．

*Proof.*  $s = 1$  の時示す． $\Phi$  は  $(h_{q\alpha-\beta})_{\alpha\beta}$  と書けることに注意する．これより  $\text{Trace} \Phi = \sum h_{(q-1)\alpha}$  となる．これは  $H \in R_0$  より,  $|h_{(q-1)\alpha}|_p \leq \left(\frac{1}{p}\right)^{M|\alpha|}$  となるので,  $\alpha \rightarrow \infty$  の時,  $|h_{(q-1)\alpha}|_p \rightarrow 0$  となるので, べき級数が収束する．また,  $\sum h_\alpha$  は収束半径が 1 以上なので,  $|u|_p = 1$  とすると,  $\sum h_\alpha u^\alpha$  は収束する． $U \subset \mathbb{C}_p$  を 1 の  $q-1$  乗根全体とする．

$$\begin{aligned}\sum_{u \in U^N} H(u) &= \sum_{u \in U^N} \sum_{\alpha \in \mathbb{Z}_{\geq 0}^N} h_\alpha u^\alpha \\ &= \sum_{\alpha \in \mathbb{Z}_{\geq 0}^N} h_\alpha \sum_{u \in U^N} u^\alpha\end{aligned}$$

$$= \sum_{a \in \mathbb{Z}_{\geq 0}^N} h_a \prod_{i=1}^N \left( \sum_{u_i \in U} u_i^{\alpha_i} \right)$$

$q-1|\alpha_i$  の時は  $\sum_{u_i \in U} u_i^{\alpha_i} = q-1$  となり, それ以外では 0 になる.

$$= (q-1)^N \sum_{a \in (q-1)\mathbb{Z}_{\geq 0}^N} h_a = (q-1)^N \text{Trace}(\Phi)$$

$q-1|\alpha_i$  の時は  $\sum_{u_i \in U} u_i^{\alpha_i} = q-1$  となり, それ以外では 0 になる.  $s \geq 2$  の時は上で示した lemma を使って,

$$\Phi^s = (T_q \circ \Phi_H)^s = T_q^s \circ \Phi_{H_{q^s-1}}$$

となり, これについて計算することで, ( $q$  を  $q^s$  に置き換えることで)

$$(q^s-1)^N \text{Trace}(\Phi^s) = \sum_u H(u)H(u^q) \dots h(u^{q^{s-1}})$$

となる. □

$A : R \rightarrow R$  に対し,

$$\det(Id - tA) := \sum_{m \geq 0} (-1)^m \left( \sum_{\sigma} \varepsilon(\sigma) a_{\alpha_1 \sigma(\alpha_1) \dots \alpha_m \sigma(\alpha_m)} \right) t^m$$

を定める. これを  $A$  の特性べき級数という. このべき級数の各項が収束していなければ定義できない.

**Lemma 6.12.**  $H \in R_0$  の時,  $\Phi = \Phi_{q,H}$  の任意の特性べき級数が収束し, 収束半径は  $\infty$  となる.

**Proposition 6.13.**  $A : R \rightarrow R$  が  $\det(Id - tA)$  と  $\text{Trace}(A^s)$  が定義できている時,

$$\det(Id - tA) = \exp\left(- \sum_{s \geq 1} \frac{\text{Trace}(A^s)}{s} t^s\right)$$

**Corollary 6.14.**  $H \in R_0, \Phi = \Phi_{q,H}$  とすると任意の  $q \geq 2$  に対し,

$$\det(Id - t\Phi) = \exp\left(- \sum_{s \geq 1} \frac{\text{Trace}(\Phi)^s}{s} t^s\right)$$

**Lemma 6.15.** 任意の  $n \geq 1$  に対し,  $G \in R = \mathbb{C}_p[[y, x_1, \dots, x_d]]$  defined in  $G(y, x)$  は  $R_0$  になる.

## 6.4 The Rationality of the Zeta function

$\zeta$  関数の有理性を示す. そのためには以下の命題を使う.

**Proposition 6.16.**  $Z(t) = \sum_{n \geq 0} a_n t^n \in \mathbb{Z}[[T]]$  が以下を満たすとする.

1. 任意の  $n \geq 0$  に対し,  $|a_n|_{\infty} \leq C s^n$  となる  $C, s \geq 0$  が存在する.
2.  $Z$  を自然な埋め込みで  $\mathbb{C}_p[[T]]$  とみなす. この時, ある収束半径が  $\infty$  となる  $g, h \in \mathbb{C}_p[[T]]$  が存在し,  $Z = \frac{h}{g}$  となる.

この時、 $Z(t) \in \mathbb{Q}(T)$  の元となる。

上の命題を示すために、補題を一つ用意する。

**Lemma 6.17.**  $K$  を体とし、 $f = \sum_{n \geq 0} a_n T^n \in K[[T]]$  とし、行列  $A_{i,N} = (a_{i+\alpha+\beta})_{0 \leq \alpha, \beta \leq N}$  とする。 $f$  が rational であることは、ある  $N$  が存在し、十分大きい任意の  $i$  に対し、 $\det A_{i,N} = 0$  となること。

*Proof.*  $\Rightarrow$  を示す

$f$  が有理的であることは、ある 0 でない多項式  $g(T) = \sum b_n T^n \in K[T]$  が存在し、 $f(T)g(T) \in K[T]$  となること。つまり、 $f(T)g(T)$  の十分大きい時次数の係数が 0 になることと同値である。これは係数を直接計算することで、十分大きい  $i$  に対して、ある  $N$  が存在し、

$$a_i b_N + a_{i+1} b_{N-1} + \cdots + a_{i+N} b_0 = 0$$

と同値であることがわかる。また、上のような  $g(T)$  が存在すると、 $\beta = (b_i)_{0 \leq i \leq N}$  とすると

$$A_{i,N} \beta = \begin{pmatrix} a_i & \cdots & a_{i+N} \\ \vdots & \ddots & \vdots \\ a_{i+N} & \cdots & a_{i+2N} \end{pmatrix} \begin{pmatrix} b_N \\ \vdots \\ b_0 \end{pmatrix} = \begin{pmatrix} \sum_k a_{i+k} b_{N-k} \\ \vdots \\ \sum_k a_{i+N+k} b_{N-k} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

となる。これより、 $f$  が有理的であるとき、 $A_{i,N} x = 0$  は非自明な解を持つため、 $\det A_{i,N} = 0$  となる。

$\Leftarrow$  を示す

$$l_i = (a_i \quad \cdots \quad a_{i+N})$$

とする。 $N$  を任意の  $i \geq i_0$  に対し、条件を満たす最小の  $N$  とする。この時、ある  $i'$  が存在し、 $\det A_{i',N-1} \neq 0$  となる。もし、任意の  $i \geq i_0$  に対し、 $\det A_{i,N-1} \neq 0$  とする。この時、 $l_{i+N} \in \sum_{k=0}^{N-1} K l_{i+k}$  となるので、 $\det A_{i,N} = 0, \det A_{i,N-1} \neq 0$  より、 $l_{i+N} \in \sum_{j=0}^{N-1} K l_{i+j}$  となる。これを繰り返すことにより、任意の  $i$  に対し、

$$l_i \in \sum_{j=0}^{N-1} K l_{i+j}$$

となる。この時、 $A_{i,N} x = 0$  となる非自明な  $x$  が存在するので、これを  $\beta$  として取れば、 $f$  が rational であることがわかる。そのため、任意の  $i \geq i_0$  に対し、 $\det A_{i,N-1} \neq 0$  となることを示せばよい。任意の  $i \geq 0$  に対し、 $\det A_{i-1,N-1} = 0$  となると、 $N$  の最小性に矛盾する。そのため、 $\det A_{i,N-1} = 0$  ならば、 $\det A_{i+1,N-1} = 0, \det A_{i-1,N-1} = 0$  となることを示せばよい。 $\det A_{i,N-1} = 0$  ならば、 $\det A_{i+1,N-1} = 0$  のみを示す。 $-1$  の場合も同様にすればできる。

$$l'_i = (a_i \quad \cdots \quad a_{i+N-1})$$

とする。仮定より、 $l'_i, \dots, l'_{i+N-1}$  は線形従属となる。 $l'_{i+1}, \dots, l'_{i+N-1}$  が線形従属である場合は特に示すことはない。そのため、 $l'_{i+1}, \dots, l'_{i+N-1}$  が線形独立とする。この時、 $A_{i,N-1} = 0$  より、 $l'_i = \sum_{j=1}^{N-1} c_j l'_{i+j}$  となる。よって、 $A_{i,N}$  の一列目の各成分を  $a_{i+} - \sum_{j=1}^{N-1} c_j a_{i+l+j}$  に置き換えて、行列式を計算すると、1 列目が第  $N$  成分以外全て 0 になるので、 $0 = \det A_{i,N} = \det A_{i+1,N-1} \delta$ 。ただし、 $(-1)^N \delta = a_{i+N} - \sum_{j=1}^{N-1} c_N a_{i+N+j}$  となる。 $\delta$  が 0 とすると、 $l_i, \dots, l_{i+N}$  が線形従属となり、各  $l_k$  の第 2 成分以降をみると、 $l'_{i+1}, \dots, l'_{i+N}$  が線形従属になる。これより、どちらが 0 であっても、 $l'_{i+1}, \dots, l'_{i+N}$  が線形従属になる。よって示された。

□

補題が示されたので命題を証明する.

\*\*\*\*あとで\*\*\*\*\*

実際に定理を示そう

**Theorem 6.18.**  $X$  を有限体  $\mathbb{F}_q$  上の代数多様体とする. この時  $Z(X, T)$  は  $\mathbb{Q}$  上の有理型関数となる.

読みにくさこの上ない. どうか.

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?

## 7 スキームとスキームによる代数多様体の定義

### 7.1 エタール射

### 7.2 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.  $\Rightarrow$  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...?  $\Rightarrow$  Etale Cohomology 1 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、よくわかんて応える。l 進が面白いかと言われたらそれもよくわからんと応える。

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？

## 8 数論のモチベーション

### 8.1 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  $\Rightarrow$  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 8.1.**  $K$  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。

- 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

### 8.2 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。

**Proposition 8.2.** 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。

## A 圏論

この本で使った圏論的な知識についてまとめておく.

**Definition A.1.** 逆極限

## B 類体論

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 B.1.**  $K$  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.

### B.1 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.

## References

[表示形式] <http://foo/foofoo.html>

「foo」