たいとる

おーさー

ひづけ

Contents

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

2 Prepartion 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.* $+ : K \times K \to K, \cdot : K \times K \to K$ 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，$\mathrm{Hon}(K, L)$ の元を $f : K \to L$ 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．

Propostion 2.3. 体の準同型 $f : K \to L$ 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 がでないとすると，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． □

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．

体の拡大を詳しくてみていく．

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．

Propostion 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． □

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．$f : L \to M$ 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．

Propostion 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と，ある a が存在し，$f'(a) = 0$ となること．

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

とすると，

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

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． □

Propostion 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 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． □

Definition 2.10. L/K が純非分離拡大とは，$L\backslash K$ 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．

Propostion 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，

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

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． □

Propostion 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．

Propostion 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．

Propostion 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 *1* 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 *Frobenisu* 写像という．

$$Frob : \mathbb{F}_q \quad \to \mathbb{F}_q \quad , a \mapsto a^q$$

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

Propostion 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********** □

2.2.7 Trace と Norm

2.3 ガロアコホモロジー

3 Basic Knowledge of p-adic Number

これは一冊の本を目指すので，p 進と同時に初等的な代数，幾何，解析の知識も解説する．p 進数と局所体の基礎について解説する．

p を素数とする．

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

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

これは，$\mathbb{Z}/(p^n)$ 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 進整数環という．この性質を見ていく．

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

Definition 3.2. C を圏とし，$\mathcal{I}$ 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．$\mathcal{I}$ を順序により射をいれることで圏だと思うことできる．この時，関手 $F; \mathcal{I} \to C$ 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？非常につ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．

Propostion 3.3. S を $\{0,1,\ldots,p-1\}$ 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．

$$x_n \equiv \sum_{k=0}^{n} a_k p^k \mathrm{mod} p^{n+1}. \tag{1}$$

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．$0,\ldots,n-1$ で成り立つとする．$pr_n(x_n) - x_{n-1} = 0$ より，$a \in S$ がただ一つ存在し，

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

となる．よって成り立つ． □

4 離散付値の一般論

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．

6.1 A formula for the number of $\mathbb{F}_q$ points on a hypersuface

$\mathbb{F}_q$ 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 $\mathcal{A}^d_{\mathbb{F}_q}$ の $f \in \mathbb{F}_q[x_1, dots, x_d]$ で定義された hypersuface 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．)

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

であって，

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

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，$\xi(u) := \epsilon^{\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p}(u)}$ 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．

$$\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_p} : \mathbb{F}_{q^n} \to \mathbb{F}_p$$

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，

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

ただし $q = p^e$

Lemma 6.2. χ が *nontivial 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． □

$f \in \mathbb{F}_q[x_1, dots, x_n], \phi_n : \mathbb{F}_{q^n} \to \bar{\mathbb{Q}_p}$ を nontrivail 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，

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

となる．この節では，(1) の左辺を $u_1, \ldots, u_n, v$ 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 Θ 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，

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

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

********** あとで埋める**********

6.2 The constructrion of Θ

上で書いた Θ 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，$\Theta(X) = \Theta_1(X)\Theta_1(X^p)\ldots\Theta_1(X^{ep-1})$ 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，

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

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

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

とする．これは $\mathbb{Q}[[x, y]]$ の元となる．

余談，疑問. べき級数を集合的に定義しようとするとどうするんだっけ？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．

Propostion 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. *Lefrtarrow* 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，$f(x^p, y^p) \equiv f(x,y)^p \mathrm{mod} p$ なので,mod$p$ 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

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

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，$i \le n, j \le m$ 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 $c_{nm} = pa_{nm} + Q_1 \cdots + Q_r$ と書ける．ただし $Q_i = N b_{i'j'} a_{i''j''}$. 帰納法の仮定より，$Q_1 + \cdots + Q_r \in \mathbb{Z}_p$ 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，$Q_j = a^p_{n/pm/p}$ となる．$a_{n/pm/p} \equiv a^p_{n/pm/p} \mathrm{mod} p$ より，$Q_j \equiv c_{nm} \mathrm{mod} p$ 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.

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

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．

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

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，

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

あとで **

6.3 Trace of certaion 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．

Propostion 6.8. 任意の $X = V(f)(f \in \mathbb{F}_q[x_1, \ldots, x_n])$ 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．

$R = \mathbb{C}_l[x_1, \ldots, x_N]]$ とおき，$\mathfrak{m}$ でその極大イデアルとする．$\alpha = (\alpha_1, \ldots, \alpha_N) \in \mathbb{Z}^N_{\geq 0}$ とおく，$x^\alpha = x_1^{\alpha_1} \ldots x_N^{\alpha_N}$ また，$|\alpha| = \sum \alpha_i$ とする．$ord(h)$ を $h \in \mathfrak{m}^r$ を満たす最大の r とする．また，体係数形式的べき級数環は $R^\times = \mathbb{C}_p^\times$ となり，さらに，$R \backslash R^\times$ は定数項が常に 0 になるもの全体になるので，イデアルとなる．これより，局所環となることがわかる．

6.4 The Rationality of the Zeta function

ζ 関数の有理性を示す．そのためには以下の命題を使う．

Propostion 6.9. $Z(t) = \sum_{n \geq 0} a_n t^n \in \mathbb{Z}[[T]]$ 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 ∞ 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 6.10. 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，$f(T)\dot{g}(T) \in K[T]$ となること．つまり，$f(T)\dot{g}(T)$ 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

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

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

$$l_i = \begin{pmatrix} a_i & \dots & a_{i+N} \end{pmatrix}$$

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 β 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．

$$l'_i = \begin{pmatrix} a_i & \dots & a_{i+N-1} \end{pmatrix}$$

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 $a_{i+} - \sum_{j=1}^{N-1} c_l a_{i+l+j}$ 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．δ 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 6.11. 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．

読みにくすさこの上ない．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？

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、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⇒ 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. $+ : K \times K \to K, \cdot : K \times K \to K$ 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．

Propostion 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$\mathrm{m}\ \mathbb{F}_p(T)$ 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」