有限体と局所体

take

平成 28 年 9 月 29 日

目 次

1 Introduction

9/6 第 1 章 Algberaic Varieties

2 有限体で遊ぼう

有限体は非常にいい性質を多数持つ．今回は以下の定理を示し，有限体に慣れ親しむことが目標である．

Theorem 2.1. $\mathbb{F}_q$ の n 次拡大は $x^{q^n}-x$ の最小分解体である．また, $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)=\hat{\mathbb{Z}}$ となる．

私は有限体以外に位数無限の絶対ガロア群が計算できる例を知らない．それほど，珍しい例である．また，上の定理の前半で述べたように，n 次拡大はある方程式の最小分解体になる．これは拡大次数さえ指定すれば，その条件を満たす体がただひとつ存在することを示している．これは体の拡大がまさに連綿としたタワーのように連なっているように見えて，非常に気持ちがいい．この感動をともに分かち合うことが本合宿第一日目の目標である．まず，テーマである有限体の定義を与えよう．

Definition 2.2. 体 K が有限体とは，K の位数が有限かつ，体であること．

さて, 位数有限な体にはどういうものがあるだろうか？まずはよく高校数学などでも行われる mod が考えやすいのではないだろうか．つまり $\mathbb{Z}/(a)$ が位数有限な体になる時を考えてみたい．

Lemma 2.3. $\mathbb{Z}/(a)$ が位数有限の環となることは，a が 0 でないことと同値である．

Proof. a が 0 の時, $x \equiv y \bmod 0$ は $x = y$ と等しくなる. つまり, $\mathbb{Z}/(0) = \mathbb{Z}$ となる．逆に a が 0 がでないとすると, 任意の $b \in \mathbb{Z}$ に対し,$b = ca+d(0 \leq d < a)$ と書けるため,$b \equiv d$ となる a 以下の整数が存在する．そのため位数が有限となる．環となるのは環の一般論より従う． □

これで，$\mathbb{Z}/(a)$ が有限の環となることがわかった．では実際に体になる例を考えてみよう．

Lemma 2.4. p を素数とする. $\mathbb{Z}/(p)$ は体になる．$a \neq 0 in \mathbb{Z}/(p)$ となったとすると, ．ある $b \in \mathbb{Z}$ が存在し，$b \equiv a$ となる．仮定より，b と p は互いに素となるので，$(b, p) = 1$ となる．つまり，$bx + py = 1$ と書けるこれより ,x の $\mathbb{Z}/(p)$ での像と a の積は *1* になる．よって *0* 以外の全ての元は逆元を持つことがわかり，体となる．

逆に素数でない場合は体とならないことを示す．

Lemma 2.5. a が素数でないとすると $\mathbb{Z}/(a)$ は体ではない．a が素数でないため，$mn = a$ とかける整数 m, n が存在する．すると，$m\dot{n} = 0 \ mod \ a$ より．体でないことがわかった．

これらより，$\mathbb{Z}/(a)$ が体であることと，a が素数であることは同値となる．- 有限体の演算に慣れよう．- 有限体は位数で一意に定まる．- Frobenius で固定される＝もともと- 有限体の絶対ガロア群⇒辻さん向けかな． - 0 次元のヴェイユ予想

2.1 局所体

- $\mathbb{Z}_p$ の定義と逆極限- $\mathbb{Q}_p$ の演算- $\mathbb{Q}_p$ に 1 のべき乗があるか？

2.2 楕円曲線

- 1 次元のヴェイユ予想 (数えて遊ぼう) - 次元- Projective Variety - Pic(E) と Isogeny - Endmorphism - Autmorphism - SpecZ の構造層の定義- Proper Scheme - Etale Morphism