本日 (12/15)

2009 年度数学講究説明会

- 時間: 17:00 〜 (1 時間〜1 時間半程度)
- 教室: 11-511 教室

来年度「数学講究 A・B」参加希望者は
必ず出席のこと

多項式の既約性判定

- 一般には難しい
- 体の個別の議論が関係する
- しばしば最終的には虱潰しで
  場合を潰すことになる

- しかしながら多項式の既約性は
  (特に Galois 理論で) 非常に重要な議論
- 様々な実例計算でも重要

- 計算機代数の基本事項として研究されている

多項式の既約性判定

以下、専ら Q 上 (Z 上) で、
しばしば有効に用いられる基本手筋を見るが、
これで必ず判定できる訳ではない。

$Q[X]$ での既約性判定の**アルゴリズム**
(必ず有限回の計算で完了する手順)
は存在するが、

しばしば大きな虱潰しを伴い、
人間の手計算には向かない。

様々な計算代数ソフトウェア上で実装され、
有効に用いられ、研究を支えている。

Gaußの補題

$f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \boldsymbol{Z}[X]$

が原始的 ($\gcd(a_0, a_1, \ldots, a_n) = 1$**) ならば**

(特に $f(X) \in \boldsymbol{Z}[X]$ **: monic ならば)**

$f(X)$ **:** $\boldsymbol{Q}$ **上既約** $\Longleftrightarrow$ $f(X)$ **:** $\boldsymbol{Z}$ **上既約**

系

$f(X) \in \boldsymbol{Z}[X]$ **: monic**

$a \in \boldsymbol{Q}$ **が** f **の根 (**$f(a) = 0$**)** $\Longrightarrow$ $a \in \boldsymbol{Z}$

Eisenstein の既約性判定法

$f(X) = X^n + \cdots + a_1 X + a_0 \in \boldsymbol{Z}[X]$ **: monic**

$\exists p$ **: 素数**

- $\forall i : p \mid a_i$ **(即ち** $f(X) \equiv X^n \pmod{p}$**)**
- $p^2 \nmid a_0$

$\Longrightarrow$ $f(X)$ **:** $\boldsymbol{Z}$ **上既約 (従って** $\boldsymbol{Q}$ **上でも既約)**

素数を法とする判定

$f(X) = X^n + \cdots + a_1 X + a_0 \in \boldsymbol{Z}[X]$ **: monic**

素数 p **に対し、**
$\overline{f}(X) := X^n + \cdots + \overline{a_1} X + \overline{a_0} \in \boldsymbol{F}_p[X]$ **とする**

$\exists p$ **: 素数に対し** $\overline{f}(X)$ **:** $\boldsymbol{F}_p$ **上既約**

$\Longrightarrow$ $f(X)$ **:** $\boldsymbol{Z}$ **上既約 (従って** $\boldsymbol{Q}$ **上でも既約)**

注: 以上の事柄

- **Gaußの補題**
- **Eisenstein の既約性判定法**
- **素数を法とする判定**

は、Z および Q でなくても、

- R **: 単項 ideal 整域 (PID)**
- $Q = \mathrm{Frac}(R)$ **:** R **の商体**

に関して成立する (証明も同様)

さて、中間試験も終わり、

後半の主題はいよいよ

Galois 理論

である。

体の拡大の理論としての Galois 理論

体拡大 L/K の様子を、

自己同型群 $\mathrm{Aut}(L/K)$ で統制する

Galois 理論の基本定理

$\Vert$

中間体と部分群との対応

有限次代数拡大の基本的な不等式 (再掲)

L/K: **有限次 (代数) 拡大**

$K \subset L \subset \Omega$: **代数閉体**

$$\#\mathrm{Aut}(L/K) \leq \#\mathrm{Emb}_K(L, \Omega) \leq [L : K]$$

左の等号 $\Longleftrightarrow$ L/K : **正規**

右の等号 $\Longleftrightarrow$ L/K : **分離**

$\mathrm{Aut}(L/K)$ **が望む限り大きくなるのは、**
L/K **が正規かつ分離的のとき**

有限次代数拡大の基本的な不等式 (再掲)

L/K: **有限次 (代数) 拡大**

$K \subset L \subset \Omega$: **代数閉体**

$$\#\mathrm{Aut}(L/K) \leq \#\mathrm{Emb}_K(L, \Omega) \leq [L : K]$$

左の等号 $\Longleftrightarrow$ L/K : **正規**

右の等号 $\Longleftrightarrow$ L/K : **分離**

$\mathrm{Aut}(L/K)$ **が望む限り大きくなるのは、**
L/K **が正規かつ分離的のとき**

体の拡大の理論としての Galois 理論

“Galois 拡大” とは、

“$\mathrm{Aut}(L/K)$ が充分大きく、
体拡大 L/K を統制できる拡大”

実際の所、

L/K が正規かつ分離的、

即ち、$\#\mathrm{Aut}(L/K) = [L : K]$ であることが、

Galois 理論 (中間体と部分群との対応)
が機能するのに重要

体の拡大の理論としての Galois 理論

“Galois 拡大” とは、

“$\mathrm{Aut}(L/K)$ が充分大きく、
体拡大 L/K を統制できる拡大”

実際の所、

L/K が正規かつ分離的、

即ち、$\#\mathrm{Aut}(L/K) = [L : K]$ であることが、

Galois 理論 (中間体と部分群との対応)
が機能するのに重要

体の有限次拡大 L/K が Galois 拡大

$$\Updownarrow$$

$$L^{\mathrm{Aut}(L/K)} = K$$

$$\Updownarrow$$

$$\#\mathrm{Aut}(L/K) = [L : K]$$

$$\Updownarrow$$

L/K : 正規拡大 かつ 分離拡大

この時、$\mathrm{Aut}(L/K) = \mathrm{Gal}(L/K)$ と書き、
L/K の Galois 群 と呼ぶ。