体の拡大の理論としての Galois 理論(復習)

体の有限次拡大 L/K **が Galois 拡大**

$$\Updownarrow$$

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

$$\Updownarrow$$

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

$$\Updownarrow$$

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**

有限次代数拡大の基本的な不等式

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 : **正規拡大**

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

有限次代数拡大の基本的な不等式

特に $L = K(\alpha)$ **：単拡大のときは、**

$f(X) := \mathrm{Irr}(\alpha/K; X) \in K[X]$

： α **の** K **上の最小多項式とすれば**

$$\#(\mathrm{Conj}(\alpha, K) \cap L) \leq \#\mathrm{Conj}(\alpha, K) \leq \deg f$$

左の等号 $\Longleftrightarrow \mathrm{Conj}(\alpha, K) \subset K(\alpha)$

$\Longleftrightarrow K(\alpha)/K$: **正規拡大**

右の等号 $\Longleftrightarrow f$ **の根の個数が** $(\deg f)$ **個**

$\Longleftrightarrow K(\alpha)/K$: **分離拡大**

Galois 理論の基本定理

L/K: **Galois 拡大、** $\mathrm{G} := \mathrm{Gal}(\mathrm{L}/\mathrm{K})$**: Galois 群**

$\mathcal{H}_{\mathrm{G}} := \{\mathrm{H} |\ \mathrm{G}$ **の部分群** $\}$

$\mathcal{M}_{\mathrm{L}/\mathrm{K}} := \{\mathrm{M} |\ \mathrm{L}/\mathrm{K}$ **の中間体** $\}$

$$\begin{array}{ccc} \mathrm{M} & \longmapsto & \mathrm{Aut}(\mathrm{L}/\mathrm{M}) \\ & \Phi & \\ \mathcal{M}_{\mathrm{L}/\mathrm{K}} & \rightleftarrows & \mathcal{H}_{\mathrm{G}} \\ & \Psi & \\ \mathrm{L}^{\mathrm{H}} & \longleftarrow & \mathrm{H} \end{array}$$

Galois 理論の基本定理

- Φ, Ψ：**共に全単射で、互いに逆写像**
  ($\Phi \circ \Psi = \mathrm{id}_{\mathcal{H}_G}, \Psi \circ \Phi = \mathrm{id}_{\mathcal{M}_{L/K}}$**)**
- Φ, Ψ：**共に包含に関して順序逆同型**
  ($H_i \leftrightsquigarrow M_i$ **のとき、**$H_1 \subset H_2 \Leftrightarrow M_1 \supset M_2$**)**

“中間体と部分群とが一対一対応”

Galois 対応
(Galois correspondence)

方程式論としての Galois 理論

(根の置換としての Galois 群)

$f(X) \in K[X]$: 分離的 (重根を持たない) で
monic な n 次多項式

$W := \{w \in \overline{K} \mid f(w) = 0\}$: f の根全体
$=: \{w_1, \ldots, w_n\}$

$$f(X) = \prod_{i=1}^{n} (X - w_i)$$

f の K 上の **Galois 群** $\mathrm{Gal}(f/K)$:
"f の根 w_i 達の満たす K 係数の関係式を
保つような根の置換" 全体の成す群

方程式論としての Galois 理論
(根の置換としての Galois 群)

$R := K[X_1, \ldots, X_n]$: n 変数多項式環

$$\varphi : R \longrightarrow \overline{K} : \text{環準同型}$$
$$X_i \longmapsto w_i$$

$I = I(f/K) := \mathrm{Ker}\varphi$
: “f の根 w_i 達の K 係数の関係式” の ideal

$\mathrm{Gal}(f/K) := \{\sigma \in \mathfrak{S}_n | \sigma(I) \subset I\}$
: f の K 上の Galois 群

体拡大の Galois 群との関係

$L := \mathrm{Spl}(f/K) = K(W) = K(w_1, \ldots, w_n)$

: f の K 上の最小分解体

$\mathrm{Gal}(L/K) := \{\sigma : L \longrightarrow L \,|\, K\text{-同型}\}$

: 体拡大 L/K の Galois 群

$\sigma \in \mathrm{Gal}(L/K)$ は根の置換を引き起こす

$$\mathrm{Gal}(L/K) \subset \mathfrak{S}(W) \simeq \mathfrak{S}_n$$

$$\boxed{\mathrm{Gal}(L/K) = \mathrm{Gal}(f/K)}$$

Galois 拡大の特徴付け

体の有限次拡大 $\mathrm{L/K}$ が Galois 拡大

$$\Updownarrow$$

$\exists \mathrm{f(X)} \in \mathrm{K[X]}$:

- f: **分離的 (重根を持たない)**
- $\mathrm{L} = \mathrm{Spl(f/K)}$ **(**K **上の** f **の最小分解体)**

この時、$\mathrm{Gal(L/K)} = \mathrm{Gal(f/K)}$ **であった**

構成問題では、Galois 拡大は、
多項式の最小分解体として与えるのが通常

以下、低次の多項式に対し、

具体的に、その Galois 群を計算してみよう。

- **既約性判定**
  (Gauss の補題・Eisenstein の判定法など)
- **有限群・置換群の知識**
  (置換群のリスト・Sylow の定理
  ・有限群の表現論など)
- **「根の間の関係式」の候補**
  (判別式・分解式 (解核多項式) など)

以下、低次の多項式に対し、

具体的に、その Galois 群を計算してみよう

- **既約性判定**
  (Gauss の補題・Eisenstein の判定法など)
- **有限群・置換群の知識**
  (置換群のリスト・Sylow の定理
  ・有限群の表現論など)
- **「根の間の関係式」の候補**
  (判別式・分解式 (解核多項式) など)

以下、低次の多項式に対し、

具体的に、その Galois 群を計算してみよう

- 既約性判定
  (Gauss の補題・Eisenstein の判定法など)
- 有限群・置換群の知識
  (置換群のリスト・Sylow の定理
  ・有限群の表現論など)
- 「根の間の関係式」の候補
  (判別式・分解式 (解核多項式) など)

Gauss の補題

$f(X) \in \mathbb{Z}[X]$: **原始的 (係数の公約数が 1) に対し、**

f : $\mathbb{Q}[X]$ **内で既約**

$\Updownarrow$

f : $\mathbb{Z}[X]$ **内で既約**

($\mathbb{Z} \subset \mathbb{Q}$ でなくても、一般に
R : **PID とその商体** $K = \mathrm{Frac}(R)$ **で可)**

Eisenstein の既約性判定法

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbf{Z}[X]$$

或る素数 p に対し、

- $\forall i : p | a_i$
- $p^2 \nmid a_0$

$\Longrightarrow$ **f : $\mathbf{Z}[X]$ 内で既約**

($p \in \mathbf{Z}$ でなくても、一般に
R : PID とその素元 π で可)

分解式・解核多項式 (resolvent)

$R := K[\mathbf{X}] = K[X_1, \ldots, X_n]$: n 変数多項式環

$\mathfrak{S}_n \curvearrowright R$: 変数の置換で作用 $(\sigma(X_i) = X_{\sigma(i)})$

$P(\mathbf{X}) \in R$ に対し、
$$^{\sigma}P(\mathbf{X}) = \sigma(P)(\mathbf{X}) := P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

$G_P := \{\sigma \in \mathfrak{S}_n \,|\, {}^{\sigma}P = P\}$: P の固定群

$S_P := \mathrm{Ord}_{\mathfrak{S}_n}(P) = \{{}^{\sigma}P \,|\, \sigma \in \mathfrak{S}_n\}$: P の $\mathfrak{S}_n$-軌道

分解式・解核多項式 (resolvent)

$$G_P = \{\sigma \in \mathfrak{S}_n \,|\, {}^\sigma P = P\}$$

$$S_P = \mathrm{Ord}_{\mathfrak{S}_n}(P) = \{{}^\sigma P \,|\, \sigma \in \mathfrak{S}_n\}$$

$$\begin{array}{ccc} S_P & \simeq & \mathfrak{S}_n/G_P \\ {}^\sigma P & \leftrightsquigarrow & \sigma G_P \end{array}$$

(G-集合の準同型定理)

従って

$$\#S_P = \frac{n!}{\#G_P}$$

(Lagrange の定理!!)