

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**



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



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



L/K : 正規拡大 かつ 分離拡大

この時、 $\text{Aut}(L/K) = \text{Gal}(L/K)$ 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

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

左の等号 $\iff L/K$: 正規拡大

右の等号 $\iff L/K$: 分離拡大

有限次代数拡大の基本的な不等式

特に $L = K(x)$: 単拡大のときは、

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

: x の K 上の最小多項式とすれば

$$\#(\text{Conj}(x, K) \cap L) \leq \#\text{Conj}(x, K) \leq \deg f$$

左の等号 $\iff \text{Conj}(x, K) \subset K(x)$

$\iff K(x)/K$: 正規拡大

右の等号 $\iff f$ の根の個数が $(\deg f)$ 個

$\iff K(x)/K$: 分離拡大

Galois 理論の基本定理

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

$\mathcal{H}_G := \{H \mid G \text{ の部分群} \}$

$\mathcal{M}_{L/K} := \{M \mid L/K \text{ の中間体} \}$

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

Galois 理論の基本定理

- Φ, Ψ : 共に全単射で、互いに逆写像
($\Phi \circ \Psi = \text{id}_{\mathcal{H}_G}, \Psi \circ \Phi = \text{id}_{\mathcal{M}_{L/K}}$)
- Φ, Ψ : 共に包含に関して順序逆同型
($H_i \leftrightarrow M_i$ 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

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

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

f の K 上の **Galois 群** $\text{Gal}(f/K)$:

“ 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)

$R := K[X_1, \dots, X_n]$: n 変数多項式環

$\varphi : R \longrightarrow \bar{K}$: 環準同型

$X_i \longmapsto w_i$

$I = I(f/K) := \text{Ker}\varphi$

: “ f の根 w_i 達の K 係数の関係式” の ideal

$\text{Gal}(f/K) := \{\sigma \in \mathfrak{S}_n \mid \sigma(I) \subset I\}$

: f の K 上の **Galois 群**

体拡大の Galois 群との関係

$L := \text{Spl}(f/K) = K(W) = K(w_1, \dots, w_n)$
: f の K 上の最小分解体

$\text{Gal}(L/K) := \{\sigma : L \rightarrow L \mid K\text{-同型}\}$
: 体拡大 L/K の **Galois 群**

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

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

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

Galois 拡大の特徴付け

体の有限次拡大 L/K が **Galois 拡大**



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

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

この時、 $\text{Gal}(L/K) = \text{Gal}(f/K)$ 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)

Gauss の補題

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

$f : \mathbf{Q}[X]$ 内で既約



$f : \mathbf{Z}[X]$ 内で既約

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

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

$\implies f : \mathbf{Z}[X]$ 内で既約

($p \in \mathbf{Z}$ でなくても、一般に

$R : \mathbf{PID}$ とその素元 π で可)

分解式・解核多項式 (resolvent)

$R := K[\mathbf{X}] = K[X_1, \dots, X_n]$: 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、

$${}^\sigma P(\mathbf{X}) = \sigma(P)(\mathbf{X}) := P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

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

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

分解式・解核多項式 (resolvent)

$$G_P = \{\sigma \in \mathfrak{S}_n \mid \sigma P = P\}$$

$$S_P = \text{Ord}_{\mathfrak{S}_n}(P) = \{\sigma P \mid \sigma \in \mathfrak{S}_n\}$$

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

(G-集合の準同型定理)

従って

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

(Lagrange の定理!!)