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

例 (複二次式)

$f(X) = X^4 - 4aX^2 + 4b \in K := \mathbf{Q}(a, b)$

4 **根:** $w_1, w_2, w_3 = -w_1, w_4 = -w_2$

$X_1 + X_3, X_2 + X_4 \in I(f/K)$

$\mathrm{Gal}(f/K) \subset \langle \alpha, \beta \rangle \simeq D_4$ **(4 次の二面体群)**

ここに $\alpha = (1\ 2\ 3\ 4), \beta = (2\ 4)$

a, b **の値によっては、**
$\mathrm{Gal}(f/K)$ **が** D_4 **より小さくなることもある**

例 (複二次式)

$$X^4 - 4aX^2 + 4b = 0$$

$$X = \pm\sqrt{2a \pm 2\sqrt{a^2 - b}}$$

$$= \pm\sqrt{a + \sqrt{b}} \pm \sqrt{a - \sqrt{b}}$$

$\mathrm{Gal}(f/K)$ **が** D_4 **より小さくなる場合:**

(1) X^2 **の多項式として可約** $(a^2 - b = \square)$
(2) 二重根号が外せる $(b = \square)$
(3) 二重根号は外せないが、中の根号が共通
$(a^2 - b = b\cdot\square)$

例 (複二次式)

$$X^4 - 4aX^2 + 4b = 0$$

$$X = \pm\sqrt{2a \pm 2\sqrt{a^2 - b}}$$

$$= \pm\sqrt{a + \sqrt{b}} \pm \sqrt{a - \sqrt{b}}$$

$\mathrm{Gal}(f/K)$ **が** D_4 **より小さくなる場合:**

(1) X^2 **の多項式として可約** $(a^2 - b = \square)$
(2) 二重根号が外せる $(b = \square)$
(3) 二重根号は外せないが、中の根号が共通
$(a^2 - b = b\cdot\square)$

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

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

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

体の拡大の理論としての Galois 理論(復習)

L/K : **体の拡大**

$G := \mathrm{Aut}(L/K) = \{\sigma \in \mathrm{Aut}(L) \,|\, \sigma|_K = \mathrm{id}\}$

- $H \subset G$: **部分群に対し、**
  $L^H := \{x \in L \,|\, \forall \sigma \in H : \sigma(x) = x\}$
  : H **の固定体 (fixed field)**

- M : L/K **の中間体に対し、**
  $\mathrm{Aut}(L/M) = \{\sigma \in G \,|\, \forall x \in M : \sigma(x) = x\}$
  : L **の** M **上の自己同型群**

体の拡大の理論としての Galois 理論(復習)

自明に

$$\mathrm{Aut}(L/L^H) \supset H, \quad L^{\mathrm{Aut}(L/M)} \supset M$$

ここで $=$ が成り立つか ？

一般には成り立たないが、Galois 拡大なら OK

体の拡大の理論としての Galois 理論(復習)

自明に

$$\mathrm{Aut}(L/L^H) \supset H, \quad L^{\mathrm{Aut}(L/M)} \supset M$$

ここで $=$ が成り立つか ?

一般には成り立たないが、Galois 拡大なら OK

体の拡大の理論としての Galois 理論(復習)

自明に

$$\mathrm{Aut}(L/L^H) \supset H, \quad L^{\mathrm{Aut}(L/M)} \supset M$$

ここで $=$ が成り立つか ?

一般には成り立たないが、Galois 拡大なら OK

体の拡大の理論としての Galois 理論(復習)

“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”

Galois 理論の基本定理
$\Vert$
中間体と部分群との対応

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**

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)

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)

Galois 理論の基本定理

- $H_i \leftrightsquigarrow M_i$ **のとき、**
$$H_1 \cap H_2 \leftrightsquigarrow M_1 M_2$$
$$\langle H_1, H_2 \rangle \leftrightsquigarrow M_1 \cap M_2$$

- $M \in \mathcal{M}_{L/K}$ **に対し、**
L/M **:** $\mathbf{Galois}$ **で、**$\mathrm{Gal}(L/M) = \Phi(M)$

- $\forall \sigma \in G$ **に対し、**
$$\sigma H \sigma^{-1} \leftrightsquigarrow \sigma(M)$$

- **特に、**$H \lhd G \Longleftrightarrow M/K$ **:** $\mathbf{Galois}$ **で、**
この時、$G/H \simeq \mathrm{Gal}(M/K)$

Galois 拡大の特徴付け

体の有限次拡大 L/K が Galois 拡大

$$\Updownarrow$$

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

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

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