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)

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

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

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

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

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)

- $H_i \leftrightsquigarrow M_i$ **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 **:** Galois **で、**$\mathrm{Gal}(L/M) = \Phi(M)$

- $\forall \sigma \in G$ **に対し、**

$$\sigma H \sigma^{-1} \leftrightsquigarrow \sigma(M)$$

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

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 (重根なし) n 次多項式

$$W := \{w \in \overline{K} \,|\, f(w) = 0\} =: \{w_1, \ldots, w_n\}$$

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

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

$$X_i \longmapsto w_i$$

$I = I(f/K) := \mathrm{Ker}\varphi$: "根の関係式" 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

$f(X) \in K[X]$: 分離的 (重根なし) n 次多項式

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

この時、L/K : Galois 拡大で、

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

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

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

体拡大の Galois 群との関係

体の有限次拡大 L/K が Galois 拡大

$$\Updownarrow$$

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

- f**: 分離的 (重根なし)**
- $L = \mathrm{Spl}(f/K)$ **(K 上の f の最小分解体)**

この時、$\mathrm{Gal}(L/K) = \mathrm{Gal}(f/K)$ となる。

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

体拡大の Galois 群との関係

体の有限次拡大 L/K が Galois 拡大

$$\Updownarrow$$

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

- f**: 分離的 (重根なし)**
- $L = \mathrm{Spl}(f/K)$ **(K 上の f の最小分解体)**

この時、$\mathrm{Gal}(L/K) = \mathrm{Gal}(f/K)$ となる。

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

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

f : $\boldsymbol{Q}[X]$ 内で既約

$\Updownarrow$

f : $\boldsymbol{Z}[X]$ 内で既約

($\boldsymbol{Z} \subset \boldsymbol{Q}$ 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

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in \boldsymbol{Z}[X]$$

或る素数 p に対し、

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

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

($p \in \boldsymbol{Z}$ 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)

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

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

$P(\boldsymbol{X}) \in R$ に対し、

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

$G_P := \{\sigma \in \mathfrak{S}_n | {}^{\sigma}P = P\}$: 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!!)

Lagrange の定理(の元々の形)

n 次多項式の根から作った有理式 u に対し、

全ての根の置換 $n!$ 個のうち
u を不変にする置換が m 個ならば、

$$m \mid n!$$

であり、u は根の置換により
$d := \dfrac{n!}{m}$ 個の異なる値を取る。

更にこのとき、
u は係数から作られる d 次多項式の根である。

分解式・解核多項式 (resolvent)

$f(X) \in K[X]$: **分離的**, $\deg f = n$

$W = \{w_1, \ldots, w_n\}$: f **の根全体**

$L := K(W) = \mathrm{Spl}(f/K)$

: f **の** K **上の (最小) 分解体**

$\varphi : R \longrightarrow L$ **: 全射環準同型**

$h \longmapsto h(w_1, \ldots, w_n)$

$I = I(f/K) := \mathrm{Ker}\varphi$ **とすると、**

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

分解式・解核多項式 (resolvent)

$P(\boldsymbol{X}) \in R$ **に対し、**

$$\varphi(P) = P(w_1, \ldots, w_n) \in L$$

$\varphi(P) \in L$ **の** K **上の共役は次の形:**

$\sigma \in \mathrm{Gal}(L/K) = \mathrm{Gal}(f/K)$ **に対し、**

$$\begin{aligned}\sigma(\varphi(P)) = \varphi({}^{\sigma}P) &= {}^{\sigma}P(w_1, \ldots, w_n) \\ &= P(w_{\sigma(1)}, \ldots, w_{\sigma(n)})\end{aligned}$$

しかし、この $\mathrm{Gal}(f/K)$ **が判らない。**

分解式・解核多項式 (resolvent)

とにかく、 $\mathrm{Gal}(f/K) \in \mathfrak{S}_n$ **なので、**

次の形ではある:

$\sigma \in \mathfrak{S}_n$ **に対し、**

$$\varphi({}^{\sigma}P) = {}^{\sigma}P(w_1, \ldots, w_n) = P(w_{\sigma(1)}, \ldots, w_{\sigma(n)})$$

(見た目上 $\#S_P$ **個)**

このうちのどれだけが実際の K **上の共役か ?**

分解式・解核多項式 (resolvent)

$P(\boldsymbol{X}) \in R$ に対し、

$$R(P;f)(T) := \prod_{Q \in S_P} (T - Q(w_1, \ldots, w_n))$$

$$= \prod_{\sigma \in \mathfrak{S}_n / G_P} (T - {}^{\sigma}P(w_1, \ldots, w_n))$$

$$\in K[T]$$

: P に関する f の**分解式 (resolvent)**

$R(P;f)(T)$ の K 上の既約分解の様式で
$\mathrm{Gal}(f/K)$ を識別する

分解式・解核多項式 (resolvent)

$P(\boldsymbol{X}) \in R$ に対し、

$$R(P;f)(T) := \prod_{Q \in S_P} (T - Q(w_1, \ldots, w_n))$$

$$= \prod_{\sigma \in \mathfrak{S}_n / G_P} (T - {}^{\sigma}P(w_1, \ldots, w_n))$$

$$\in K[T]$$

: P に関する f の**分解式 (resolvent)**

$R(P;f)(T)$ の K 上の既約分解の様式で

$\mathrm{Gal}(f/K)$ を識別する