

体の拡大の理論としての Galois 理論(復習)

L/K : 体の拡大

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

- $H \subset G$: 部分群に対し、
 $L^H := \{x \in L \mid \forall \sigma \in H : \sigma(x) = x\}$
: H の**固定体 (fixed field)**
- $M : L/K$ の中間体に対し、
 $\text{Aut}(L/M) = \{\sigma \in G \mid \forall x \in M : \sigma(x) = x\}$
: 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)

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

Galois 理論の基本定理

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

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

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

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

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
($H_i \rightsquigarrow M_i$ 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

- $H_i \leftrightarrow M_i$ のとき、
$$H_1 \cap H_2 \leftrightarrow M_1 M_2$$
$$\langle H_1, H_2 \rangle \leftrightarrow M_1 \cap M_2$$
- $M \in \mathcal{M}_{L/K}$ に対し、 L/M : **Galois** で、 $\text{Gal}(L/M) = \Phi(M)$
- $\forall \sigma \in G$ に対し、
$$\sigma H \sigma^{-1} \leftrightarrow \sigma(M)$$
- 特に、 $H \triangleleft G \iff M/K$: **Galois** で、この時、 $G/H \simeq \text{Gal}(M/K)$

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

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

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

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

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

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

$f : \mathbb{Q}[X]$ 内で既約



$f : \mathbb{Z}[X]$ 内で既約

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

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

$\implies f : \mathbf{Z}[X]$ 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!!)

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

$$d := \frac{n!}{m} \text{ 個の異なる値を取る。}$$

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, $\deg f = n$

$W = \{w_1, \dots, w_n\}$: f の根全体

$L := K(W) = \text{Spl}(f/K)$: f の K 上の (最小) 分解体

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

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

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

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

分解式・解核多項式 (resolvent)

$P(X) \in R$ に対し、

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

$\varphi(P) \in L$ の K 上の共役は次の形:

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

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

しかし、この $\text{Gal}(f/K)$ が判らない

分解式・解核多項式 (resolvent)

とにかく $\text{Gal}(f/K) \subset \mathfrak{S}_n$ なので、
次の形のうちのどれかではある：

$\sigma \in \mathfrak{S}_n$ に対し、

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

(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)

$P(X) \in R$ に対し、

$$\begin{aligned} R(P; f)(T) &:= \prod_{Q \in S_P} (T - Q(w_1, \dots, w_n)) \\ &= \prod_{\sigma \in \mathfrak{S}_n / G_P} (T - {}^\sigma P(w_1, \dots, w_n)) \\ &\in K[T] \end{aligned}$$

: 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

$\text{Gal}(f/K)$ を識別する

分解式・解核多項式 (resolvent)

$R(P; f)(T)$ の K 上の既約分解の様式

$$\updownarrow \quad 1:1$$

$\text{Gal}(f/K) \setminus \mathfrak{S}_n / G_P$ (両側剰余類分解)

実際には、

G_P が程々の大きさになる P を巧く取って、
 $\text{Gal}(f/K)$ を選り分けていく

分解式・解核多項式 (resolvent)

自明な場合:

- $P = X_1$

$$G_P = \mathfrak{S}_{n-1}, \quad S_P = \{X_1, \dots, X_n\}$$

$$R(P; f)(T) = \prod_{i=1}^n (T - w_i) = f(T)$$

- P : 対称式

$$G_P = \mathfrak{S}_n, \quad S_P = \{P\}$$

$$R(P; f)(T) = T - P(w_1, \dots, w_n) \in K[T]$$

→ これでは役に立たない

例: 判別式 (discriminant)

$$\Delta = \prod_{1 \leq i < j \leq n} (X_i - X_j) \in R : \text{差積}$$

$$\Delta(f) = \prod_{1 \leq i < j \leq n} (w_i - w_j)$$

$$D(f) = \Delta(f)^2 : f \text{ の判別式} \in K$$

$$G_\Delta = \mathfrak{A}_n, \quad S(\Delta) = \{\Delta, -\Delta\}$$

$$R(\Delta; f)(T) = T^2 - D(f) \in K[T]$$

$$R(\Delta; f)(T) : K \text{ 上可約} \iff \text{Gal}(f/K) \subset \mathfrak{A}_n$$

それでは、

佳いお年を