

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)

自明に

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

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、

“ $\text{Aut}(L/K)$ 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

||

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**



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



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



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**

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

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

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

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

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

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