

Galois 対応

L/K は有限次 Galois 拡大であると仮定する.

このとき, $\text{Gal}(L/K) = \{L \text{ の } K \text{ 上での体の自己同型全体}\}$ について,

$$|\text{Gal}(L/K)| = [L:K]$$

でかつ以下の一対一対応が得られる:

$$\{L/K \text{ の中間体全体}\} \xleftrightarrow{\sim} \{\text{Gal}(L/K) \text{ の部分群全体}\}$$

$$M \longmapsto \{\sigma \in \text{Gal}(L/K) \mid \sigma(a) = a \ (a \in M)\}$$

$$L^H = \{\beta \in L \mid \sigma(\beta) = \beta \ (\sigma \in H)\} \longleftarrow H$$

さらに,

(1) この対応は包含関係を逆転させる.

(2) L/L^H も Galois 拡大になり, $\text{Gal}(L/L^H) = H$. 特に $[L:L^H] = |H|$.

(3) L^H/K が Galois 拡大 $\iff H$ は $\text{Gal}(L/K)$ の正規部分群.

(2)より, 位数 r の $\text{Gal}(L/K)$ の部分群 H に対応する L/K の部分体 M は $[L:M] = r$ でかつ $\sigma(\beta) = \beta \ (\beta \in M, \sigma \in H)$ を満たすものになる.

よく使われる有限群の記号

Symmetric group

alternating group

$$S_n = (n \text{ 次の置換群}) \supset A_n = (n \text{ 次の交代群}) = \{n \text{ 次の偶置換全体}\},$$

$$C_n = (位数 n \text{ の巡回群}) = \langle \sigma \mid \sigma^n = 1 \rangle \cong \mathbb{Z}/n\mathbb{Z}.$$

cyclic group

$$D_n = (位数 2n \text{ の } n \text{ 次の二面体群}) = \langle \sigma, \tau \mid \sigma^n = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle.$$

dihedral group

$$D_3 \cong S_3, \quad \sigma \leftrightarrow (1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau \leftrightarrow (1, 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

$$\begin{aligned} S_3 &= \{1, (1, 2, 3), (1, 3, 2), (1, 2), (1, 3), (2, 3)\} \\ &= \{1, (1, 2, 3), (1, 2, 3)^2, (1, 2), (1, 2, 3)(1, 2), (1, 2, 3)^2(1, 2)\} \end{aligned}$$

$$C_3 \cong A_3 = \{1, (1, 2, 3), (1, 2, 3)^2\},$$

正規部分群になっていることを

↓

△ と書く,

$$V = \{1, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \cong C_2 \times C_2, \quad V \triangleleft S_4$$

Klein の四元群

問題 7-1 $F(x) = x^3 - 3$, $\alpha = \sqrt[3]{3}$, $\omega = \frac{-1 + \sqrt{-3}}{2}$ とおく. 以下を示せ.

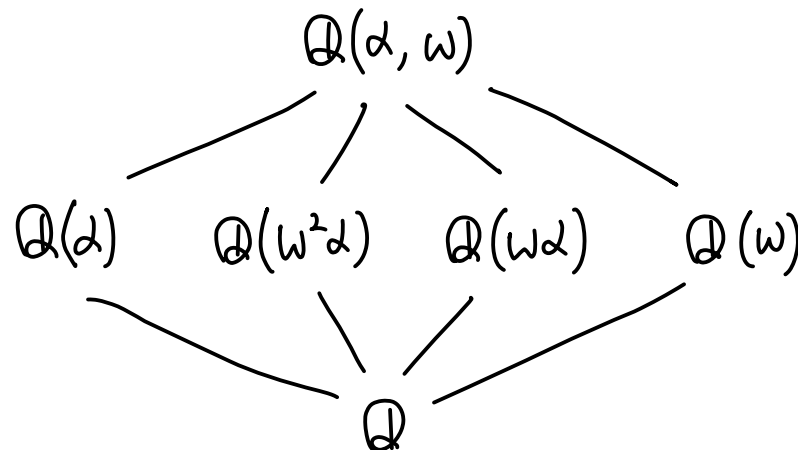
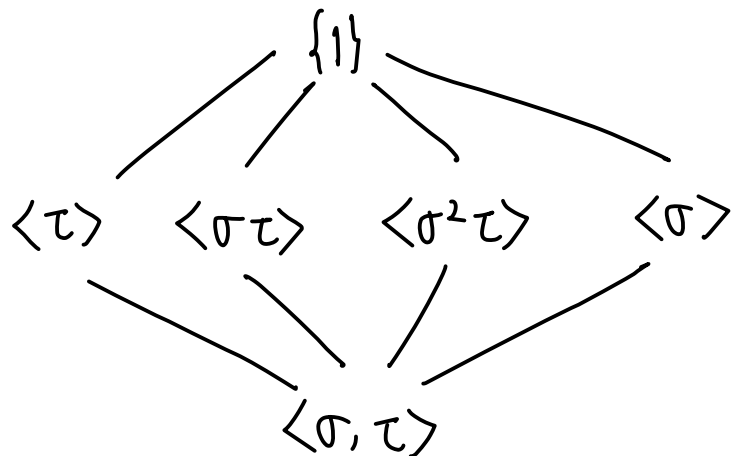
- (1) $F(x)$ は α の \mathbb{Q} 上での最小多項式である.
- (2) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha)$ に等しくない.
- (3) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3})$ に等しい. (特に $\mathbb{Q}(\alpha, \omega)$ は \mathbb{Q} の Galois 拡大になる.)

以下, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6$ を認めて使ってよい. (問題 3-5, 4-2 の解答例も参照)

- (4) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 σ, τ を次のように定義できる:

$$\sigma(f(\alpha)) = f(\omega\alpha) \quad (f(x) \in \mathbb{Q}(\omega)[x]), \quad \tau(g(\omega)) = g(\omega^2) \quad (g(x) \in \mathbb{Q}(\alpha)[x]).$$

- (5) $\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_3 \cong S_3$ ← 特に (b) をやってほしい.
- (6) $\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$ の部分群全体と $\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ の中間体の Galois 対応は 以下のようになっている:



問題 7-2 $F(x) = x^4 - 4x^2 + 2$, $\alpha = \sqrt{2+\sqrt{2}}$ とおく. 以下を示せ.

(1) $F(x)$ は α の \mathbb{Q} 上での最小多項式である.

(2) $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha)$ に等しい. ← $F(x)$ のすべての根が $\mathbb{Q}(\alpha)$ に含まれる.

(特に $\mathbb{Q}(\alpha)$ は \mathbb{Q} の Galois 拡大になる.)

(3) $\mathbb{Q}(\alpha)$ の体の自己同型 σ を $\sigma(f(\alpha)) = f(\sqrt{2-\sqrt{2}})$ ($f(x) \in \mathbb{Q}[x]$) 定義できる.

(4) $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle \cong C_4$

(5) $\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ の部分群全体と $\mathbb{Q}(\alpha)/\mathbb{Q}$ の中間体全体の Galois 対応は以下の図のようになっている:



□