Galois 対応 L/K は有限次 Galois 拡大であると仮定する．

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

$$|Gal(L/K)| = [L:K]$$

でかつ 以下の一対一対応が得られる：

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

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

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

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，$Gal(L/L^H) = H$．特に $[L:L^H] = |H|$．

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

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

よく使われる有限群の記号

Symmetric group　　alternating group

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

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

cyclic group

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

dihedral group

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

$$S_3 = \{1, (1,2,3), (1,3,2), (1,2), (1,3), (2,3)\}$$
$$= \{1, (1,2,3), (1,2,3)^2, (1,2), (1,2,3)(1,2), (1,2,3)^2(1,2)\}$$

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

正規部分群になっていることを $\triangleleft$ と書く。

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

$\subset S_4$

Kleinの四元群

$\boxed{\text{問題 7-1}}$ $F(x) = x^3 - 3$, $\alpha = \sqrt[3]{3}$, $\omega = \dfrac{-1+\sqrt{-3}}{2}$ 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:

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

(5) $\mathrm{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_3 \cong S_3$ ← 特に(6)をやってほしい.

(6) $\mathrm{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$ 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:

$$\begin{tikzcd}
 & \{1\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle \tau \rangle \arrow[dr, dash] & \langle \sigma\tau \rangle \arrow[d, dash] & \langle \sigma^2\tau \rangle \arrow[dl, dash] & \langle \sigma \rangle \arrow[dll, dash] \\
 & \langle \sigma, \tau \rangle & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q}(\alpha,\omega) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & \mathbb{Q}(\omega^2\alpha) \arrow[d, dash] & \mathbb{Q}(\omega\alpha) \arrow[dl, dash] & \mathbb{Q}(\omega) \arrow[dll, dash] \\
 & \mathbb{Q} & &
\end{tikzcd}$$

$\boxed{\text{問題7-2}}$ $F(x) = x^4 - 4x^2 + 2$, $\alpha = \sqrt{2+\sqrt{2}}$ 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) $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle \cong C_4$

(5) $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ 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:

$$
\begin{array}{ccc}
\{1\} & \qquad\qquad & \mathbb{Q}(\alpha) \\
| & & | \\
\langle \sigma^2 \rangle & & \mathbb{Q}(\sqrt{2}) \\
| & & | \\
\langle \sigma \rangle & & \mathbb{Q}
\end{array}
$$

$\square$