問題 12-1 $F(x) = x^4 - 2$, $\alpha = \sqrt[4]{2}$, $i = \sqrt{-1}$ 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 $\mathbb{Q}(\alpha, i)$ に等しい。

(3) $[\mathbb{Q}(\alpha, i) : \mathbb{Q}] = 8$。

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

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

(5) $\mathrm{Gal}(\mathbb{Q}(\alpha, i)/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_4$. □

($K = \mathbb{Q}$, $n = 4$ で $G \cong D_4$ になる例)

解答例 (1) $2 \nmid 1$, $2 \mid 0$, $2 \mid 0$, $2 \mid 0$, $2 \mid -2$, $2^2 \nmid -2$ なので Eisenstein の判定法より, $F(x) = x^4 - 2$ は $\mathbb{Q}$ 上の既約多項式である。$F(\alpha) = F(\sqrt[4]{2}) = (\sqrt[4]{2})^4 - 2 = 0$.
ゆえに, $F(x)$ は α の $\mathbb{Q}$ 上での最小多項式である。

(2) $F(x) = x^4 - 2$ の 4つの根は $\alpha, i\alpha, -\alpha, -i\alpha$ なので $F(x)$ の $\mathbb{Q}$ 上での最小分解体を L と書くと, $L = \mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha)$. $i = \dfrac{i\alpha}{\alpha}$ なので $i \in L$. このことから $L = \mathbb{Q}(i, \alpha)$ であることがわかる。

$\cap$ $\mathbb{Q}(i, \alpha)$

$\Downarrow$ $\mathbb{Q}(i, \alpha) \subset \mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha)$

(3) $L=\mathbb{Q}(i,\alpha)$, $M=\mathbb{Q}(\alpha)$ とおく. $L=M(i)$ である. $G(x)=x^2+1$ とおく.

$[M:\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg F(x)=4$. $\left(\because \mathbb{Q}(\alpha)\cong\mathbb{Q}[x]/(F(x))\right)$

もしも $G(x)$ が M 上既約でないならその根 i は M の元になるが,
$M=\mathbb{Q}(\sqrt[4]{2})\subset\mathbb{R}$ なのでそうならない. ゆえに $G(x)$ は M 上既約である.
$G(i)=i^2+1=0$ なので, $G(x)$ は $i=\sqrt{-1}$ の M 上での最小多項式になる.
これより, $[L:M]=[M(i):M]=\deg G(x)=2$.

以上より, $[\underbrace{\mathbb{Q}(i,\alpha)}_{=L}:\mathbb{Q}]=[L:M][M:\mathbb{Q}]=2\times 4=8$.

(4) $[\mathbb{Q}(i,\alpha):\mathbb{Q}(i)] = \dfrac{[\mathbb{Q}(i,\alpha):\mathbb{Q}]}{[\mathbb{Q}(i):\mathbb{Q}]} = \dfrac{8}{2} = 4 = \deg F(x)$, $F(\alpha)=0$ より,

$F(x)=x^4-2$ は $\alpha=\sqrt[4]{2}$ の $\mathbb{Q}(i)$上での最小多項式でもある.

上で $G(x)=x^2+1$ が $i=\sqrt{-1}$ の $\mathbb{Q}(\alpha)$上での最小多項式であることは示してある.

$F(x)$, $G(x)$ はそれぞれ $\mathbb{Q}(i)$, $\mathbb{Q}(\alpha)$上のそれぞれの根の最小多項式にもなっている.

したがって, 以下のようにして, 体 $\mathbb{Q}(i,\alpha)$ の自己同型 σ,τ を定めることができる:

$$\mathbb{Q}(i,\alpha) = \mathbb{Q}(i)(\alpha) \cong \mathbb{Q}(i)[x]/(F(x)) \cong \mathbb{Q}(i)(i\alpha) = \mathbb{Q}(i,i\alpha) = \mathbb{Q}(i,\alpha)$$

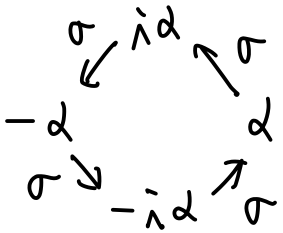
$$\begin{tikzcd} f(\alpha) \arrow[r, leftrightarrow] \arrow[rr, mapsto, bend right, "\sigma"'] & \overline{f(x)} \arrow[r, leftrightarrow] & f(i\alpha) \end{tikzcd}$$

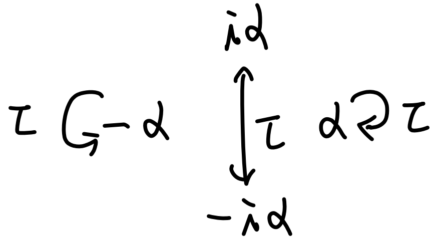
$$\mathbb{Q}(i,\alpha) = \mathbb{Q}(\alpha)(i) \cong \mathbb{Q}(\alpha)[x]/(G(x)) \cong \mathbb{Q}(\alpha)(-i) = \mathbb{Q}(-i,\alpha) = \mathbb{Q}(i,\alpha)$$

$$\begin{tikzcd} g(i) \arrow[r, leftrightarrow] \arrow[rr, mapsto, bend right, "\tau"'] & \overline{g(x)} \arrow[r, leftrightarrow] & g(-i) \end{tikzcd}$$

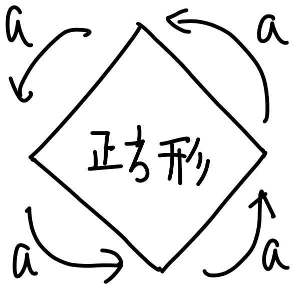
(5) $|\mathrm{Gal}(\mathbb{Q}(i,\alpha)/\mathbb{Q})| = [\mathbb{Q}(i,\alpha):\mathbb{Q}] = 8$.

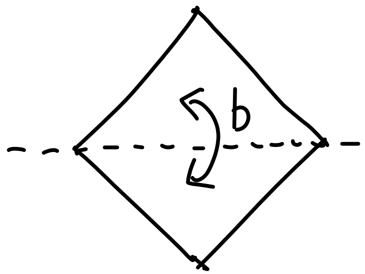
σとτは $F(x)=x^4-2$ の4つの根に次のように作用している;





4次の二面体群D_4は正方形を90°回転させる操作aと次の図の線対称変換bから生成される位数8の群であった;





以上を比較すると, $\mathrm{Gal}(\mathbb{Q}(i,\alpha)/\mathbb{Q}) \cong D_4$ であることがわかる.

$$\sigma \longleftrightarrow a$$
$$\tau \longleftrightarrow b$$

問題12-2 $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ とおく。以下を示せ。

(1) $F(x)=x^4-10x^2+1$ は $\alpha=\sqrt{2}+\sqrt{3}$ の $\mathbb{Q}$ 上での最小多項式である。

(2) $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ は $F(x)$ の $\mathbb{Q}$ 上での最小分解体である。

(3) $L/\mathbb{Q}$ は4次のGalois拡大である。

(4) L の $\mathbb{Q}$ 上での自己同型 σ,τ を次のように定めることができる：

$$\sigma(f(\sqrt{2}))=f(-\sqrt{2})\ \ (f(x)\in\mathbb{Q}(\sqrt{3})[x]),\quad \tau(g(\sqrt{3}))=g(-\sqrt{3})\ \ (g(x)\in\mathbb{Q}(\sqrt{2})[x]).$$

(5) $\mathrm{Gal}(L/\mathbb{Q})=\langle\sigma,\tau\rangle\cong C_2\times C_2$ （C_n は位数 n の巡回群）. □

F(x)の根全体の集合の置換群の中のKleinの四元群に一致。

（$K=\mathbb{Q}$, $n=4$ で $G\cong C_2\times C_2$ となる例）

解答例 （(1)～(4)は問題4-1の解答例ですでに示してあるとみなされる。）

(1), (2), (3)をまとめて示そう。

$$\begin{aligned}
&(x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))\\
&=((x-\sqrt{3})^2-(\sqrt{2})^2)((x+\sqrt{3})^2-(\sqrt{2})^2)=(x^2+1-2\sqrt{3}x)(x^2+1+2\sqrt{3}x)\\
&=(x^2+1)^2-(2\sqrt{3}x)^2=x^4+2x^2+1-12x^2=x^4-10x^2+1=F(x).
\end{aligned}$$

$F(x)$のQ上での最小分解体を $L' = \mathbb{Q}(\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3})$ と書こう。

$F(x)$の4つの根 $\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3}$ が $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ に含まれることより, $L' \subset L$.

$\sqrt{2} = \dfrac{(\sqrt{2}+\sqrt{3})+(\sqrt{2}-\sqrt{3})}{2}$, $\sqrt{3} = \dfrac{(\sqrt{2}+\sqrt{3})+(-\sqrt{2}+\sqrt{3})}{2}$ が L' に含まれることより, $L \subset L'$.

ゆえに, $L' = L = \mathbb{Q}(\sqrt{2},\sqrt{3})$. これで(2)が示された.

$\sqrt{2} \notin \mathbb{Q}$ より $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$ であることがわかり,

$\sqrt{3} \notin \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$ より, $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$ であることがわかる.

ゆえに, $[L:\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2\times 2 = 4$.

L は $F(x)$の Q上での最小分解体なので Galois 拡大でもある. これで(3)が示された.

$\dfrac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{3}-\sqrt{2}$, $\dfrac{(\sqrt{2}+\sqrt{3})-(\sqrt{3}-\sqrt{2})}{2} = \sqrt{2}$, $(\sqrt{3}-\sqrt{2})+\sqrt{2} = \sqrt{3}$ が $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ に含まれることから, $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2},\sqrt{3}) = L$ となることもわかる.

$[\mathbb{Q}(\alpha):\mathbb{Q}] = [L:\mathbb{Q}] = 4 = \deg F(x)$ より, $F(x)$ は $\alpha = \sqrt{2}+\sqrt{3}$ の Q上での最小多項式であることがわかる. これで(1)が示された.

(4) $G(x)=x^2-2$, $H(x)=x^2-3$ はそれぞれ $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$ 上のそれらの根の最小多項式とみなされるので, 以下のようにして, $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ の自己同型 σ, τ を定めることができる;

$$L=\mathbb{Q}(\sqrt{3})(\sqrt{2}) \cong \mathbb{Q}(\sqrt{3})[x]/(G(x)) \cong \mathbb{Q}(\sqrt{3})(-\sqrt{2})=L$$

$$\begin{tikzcd} f(\sqrt{2}) \arrow[r, leftrightarrow] \arrow[rr, mapsto, bend right, "\sigma"'] & \overline{f(x)} \arrow[r, leftrightarrow] & f(-\sqrt{2}) \end{tikzcd}$$

$$L=\mathbb{Q}(\sqrt{2})(\sqrt{3}) \cong \mathbb{Q}(\sqrt{2})[x]/(H(x)) \cong \mathbb{Q}(\sqrt{2})(-\sqrt{3})=L$$

$$\begin{tikzcd} g(\sqrt{3}) \arrow[r, leftrightarrow] \arrow[rr, mapsto, bend right, "\tau"'] & \overline{g(x)} \arrow[r, leftrightarrow] & g(-\sqrt{3}) \end{tikzcd}$$

(5) $|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 4$.

$\sigma, \tau, \sigma\tau$ は $F(x) = x^4 - 10x^2 + 1$ の4つの根の集合に次のように作用している:

$$\sqrt{2}+\sqrt{3} \overset{\sigma}{\longleftrightarrow} -\sqrt{2}+\sqrt{3}, \qquad \sqrt{2}-\sqrt{3} \overset{\sigma}{\longleftrightarrow} -\sqrt{2}-\sqrt{3} \qquad (\sqrt{2} \leftrightarrow -\sqrt{2})$$

$$\sqrt{2}+\sqrt{3} \overset{\tau}{\longleftrightarrow} \sqrt{2}-\sqrt{3}, \qquad -\sqrt{2}+\sqrt{3} \overset{\tau}{\longleftrightarrow} -\sqrt{2}-\sqrt{3} \qquad (\sqrt{3} \leftrightarrow -\sqrt{3})$$

$$\sqrt{2}+\sqrt{3} \longleftrightarrow -\sqrt{2}-\sqrt{3}, \qquad -\sqrt{2}+\sqrt{3} \longleftrightarrow \sqrt{2}-\sqrt{3} \qquad \sigma\tau = \tau\sigma$$

これより, $F(x)$ の4つの根を $\alpha_1 = \sqrt{2}+\sqrt{3}$, $\alpha_2 = -\sqrt{2}+\sqrt{3}$, $\alpha_3 = \sqrt{2}-\sqrt{3}$, $\alpha_4 = -\sqrt{2}-\sqrt{3}$ と書くとき, σ, τ, $\sigma\tau$ はそれぞれ置換 $(1,2)(3,4)$, $(1,3)(2,4)$, $(1,4)(2,3)$ に対応していることがわかる.

したがって,

Kleinの四元群

$$\mathrm{Gal}(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \simeq \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \simeq C_2 \times C_2. \qquad \square$$

一般の(係数が特殊な組み合わせでないような)4次方程式のGalois群はS_4に同型になる.

(体K上の)4次の既約多項式$F(x)$ (分離性も仮定)について,
4次方程式$F(x)=0$のGalois群(Lを$F(x)$のK上での最小分解体としたときの$\mathrm{Gal}(L/K)$)はS_4の推移的部分群に同型になる.

以上の2つの問題では, $\mathrm{Gal}(L/K)$はそれぞれ

$$D_4 \cong \langle (1,2,3,4),\ (2,4) \rangle \qquad (|D_4| = 8)$$

$$V \cong \langle (1,2)(3,4),\ (1,4)(2,3) \rangle \qquad (|V| = 4)$$

Kleinの4元群.

S_4の推移部分群は共役を除いて以下の5つしかない:

$$\underbrace{C_4 \cong \langle (1,2,3,4) \rangle}_{\mathrm{Gal}(\mathbb{Q}(i,\sqrt[4]{2}),\ \mathbb{Q}(\sqrt[4]{2}))\ \cong C_4},\ \underbrace{V,\ D_4}_{\text{ここを問題に出した.}},\ \underbrace{A_4,\ S_4}$$

$|A_4| = 12$
$|S_4| = 24$

S_3の推移的部分群は
$A_3 = C_3$, S_3
の2つしかない.
分離的
3次の既約多項式$=0$
の形の3次方程式のGalois群は上の2種類しかない.
判定は判別式を使ってできる.