**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 $\alpha$ 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 $\sigma, \tau$ を次のように定義できる:

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

(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 $\alpha$ 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, $L=\mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha)$. $i=\frac{i\alpha}{\alpha}$ 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。

(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。

$[M:\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg F(x)=4$.

もしも $G(x)$ が $M$ 上既約でないならその根土 $i$ 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，$[\mathbb{Q}(i,\alpha):\mathbb{Q}]=[L:M][M:\mathbb{Q}]=2\times4=8$.

(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 $\mathbb{Q}(i,\alpha)$ の自己同型の, てを定めることができる:

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

$$f(\alpha) \longleftrightarrow \overline{f(x)} \longleftrightarrow f(i\alpha)$$

$$\sigma$$

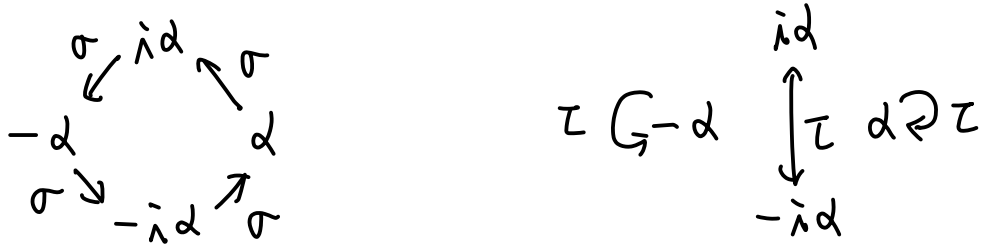
$$\mathbb{Q}(i,\alpha) = \mathbb{Q}(\alpha)(i) \cong \mathbb{Q}(\alpha)[x]/(G(x)) \cong \mathbb{Q}(\alpha)(-i) = \mathbb{Q}(-i,\alpha) = \mathbb{Q}(i,\alpha)$$

$$g(i) \longleftrightarrow \overline{g(x)} \longleftrightarrow g(-i)$$

$$\tau$$

(5) $|Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q})| = [\mathbb{Q}(i,\sqrt[4]{2}):\mathbb{Q}] = 8$.

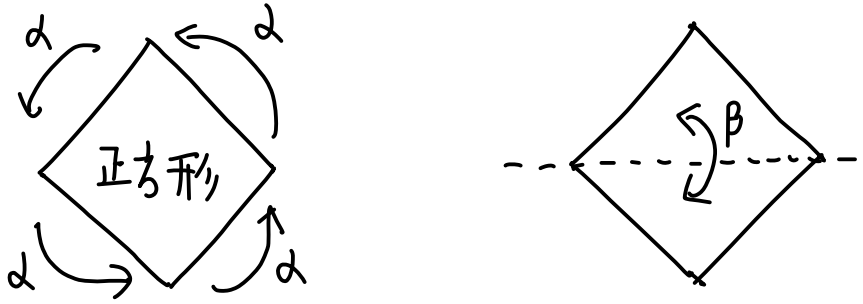
$\sigma$ と $\tau$ は $F(x) = x^4 - 2$ の4つの根に次のように作用している；







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







以上を比較すると，$Gal(\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q}) \cong D_4$ であることがわかる．

$$\sigma \longleftrightarrow \alpha$$
$$\tau \longleftrightarrow \beta$$

**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.

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

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

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

(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.)

□

**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,

$$(x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))$$

$$=((x-\sqrt{3})^2-(\sqrt{2})^2)((x+\sqrt{3})^2-(\sqrt{2})^2)=(x^2+1-2\sqrt{3}x)(x^2+1+2\sqrt{3}x)$$

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

$F(x)$ の $\mathbb{Q}$ 上での最小分解体を $L'$ 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 $\mathbb{Q}$ 上での最小分解体ので 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 $\mathbb{Q}$ 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 $\sigma$, $\tau$ を定めることができる：

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

$$f(\sqrt{2}) \longleftrightarrow \overline{f(x)} \longleftrightarrow f(-\sqrt{2})$$

$\sigma$

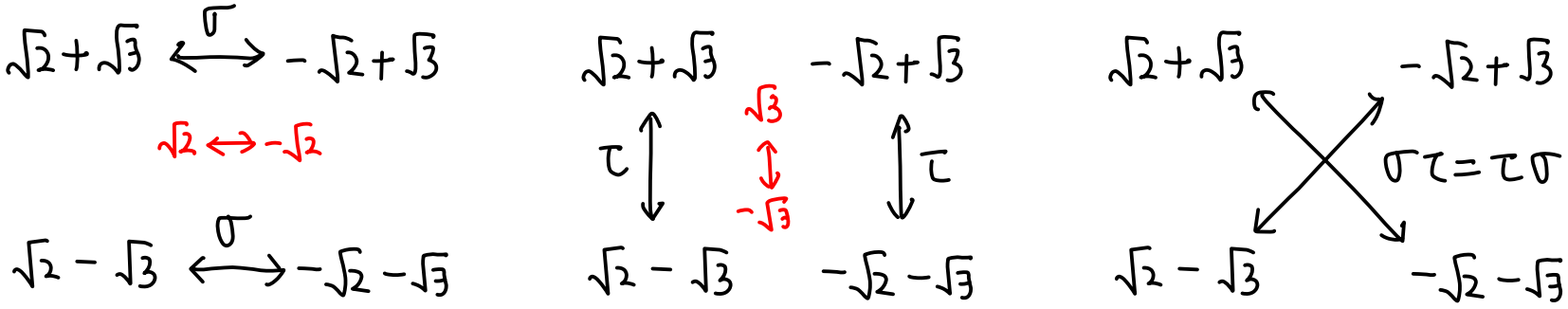
$$L=\mathbb{Q}(\sqrt{2})(\sqrt{3})\cong\mathbb{Q}(\sqrt{2})[x]/(H(x))\cong\mathbb{Q}(\sqrt{2})(-\sqrt{3})=L$$

$$g(\sqrt{3}) \longleftrightarrow \overline{g(x)} \longleftrightarrow g(-\sqrt{3})$$

$\tau$

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

$\sigma, \tau, \sigma\tau$ 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:




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, $\sigma, \tau, \sigma\tau$ 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,

$$Gal(L/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\} \cong \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \cong C_2 \times C_2,$$

Klein の四元群

□

**問題12-3** $F(x)=x^3-21x+28$ とおく、以下を示せ。 $K=\mathbb{Q}$, $n=3$

(1) $F(x)$ は $\mathbb{Q}$ 上既約である.

(2) $F(x)$ の3つの根を $\alpha,\beta,\gamma$ と書き, $D=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$ とおくと,
$D=126^2$ となる.

(3) $F(x)$ の $\mathbb{Q}$ 上での最小分解体を $L$ と書くと, $Gal(L/\mathbb{Q})\cong C_3$. 口

位数3の巡回群

$\cong A_3$ ← 3次の交代群

**解答例** $F(x)=x^3+ax+b=(x-\alpha)(x-\beta)(x-\gamma)$ のとき,

$D:=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-4a^3-27b^2$ となることを示そう.

$\alpha+\beta+\gamma=0$, $\alpha\beta+\alpha\gamma+\beta\gamma=a$, $\alpha\beta\gamma=-b$ なので,

$$\alpha^2+\beta^2+\gamma^2=(\alpha+\beta+\gamma)^2-2(\alpha\beta+\alpha\gamma+\beta\gamma)=-2a,$$

$$\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2=(\alpha\beta+\alpha\gamma+\beta\gamma)^2-2\alpha\beta\gamma(\alpha+\beta+\gamma)=a^2.$$

$F'(\alpha)=3\alpha^2+a=(\alpha-\beta)(\alpha-\gamma)$, $F'(\beta)=3\beta^2+a=(\beta-\alpha)(\beta-\gamma)$, $F'(\gamma)=3\gamma^2+a=(\gamma-\alpha)(\gamma-\beta)$ より,

$$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-F'(\alpha)F'(\beta)F'(\gamma)$$

$$=-\left(a^3+3\underbrace{(\alpha^2+\beta^2+\gamma^2)}_{=-2a}a^2+9\underbrace{(\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2)}_{=a^2}a+27\underbrace{\alpha^2\beta^2\gamma^2}_{=b^2}\right)$$

$$=-(a^3-6a^3+9a^3+27b^2)=-4a^3-27b^2.$$

(1) $F(x)=x^3-21x+28$ は $7\nmid 1,\ 7\mid 0,\ 7\mid -21,\ 7\mid 28,\ 7^2\nmid 28$ と Eisenstein の判定法より，$\mathbb{Q}$ 上既約である．

(2) 前ページの公式を $a=-21,\ b=28$ の場合に用いると，

$$D=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-4a^3-27b^2$$

$$=4\cdot 21^3-27\cdot 28^2=2^2\cdot 3^3\cdot 7^3-2^4\cdot 3^3\cdot 7^2$$

$$=2^2\cdot 3^3\cdot 7^2(7-2^2)=2^2\cdot 3^4\cdot 7^2=(2\cdot 3^2\cdot 7)^2=126^2.$$

(3) $F(x)$ の $\mathbb{Q}$ 上での最小分解体を $L$ と書き，$G=Gal(L/\mathbb{Q})$ とおく．

$F(x)$ が $\mathbb{Q}$ 上既約なので，$G$ の $\{\alpha,\beta,\gamma\}$ への作用は推移的になるので

$G\cong A_3$ または $G\cong S_3$ となる．

$\Delta=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$ とおくと，$\Delta^2=D=126^2$ より $\Delta=\pm 126\in\mathbb{Q}$ となる．

ゆえに，任意の $\sigma\in G$ について，$\sigma(\Delta)=\Delta$ となり，$\sigma$ は $\{\alpha,\beta,\gamma\}$ の偶置換になる．

これより，$G\cong A_3\cong C_3$．

□

**問題 12-4**　$F(x)=x^3+3x^2-3$ とおく，以下を示せ．

(1)　$F(x)$ は $\mathbb{Q}$ 上既約である．

(2)　$F(x)$ の3つの根を $\alpha,\beta,\gamma$ と書くとき，$D=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2$ とおくと，
$D=q^2$ となる．

(3)　$F(x)$ の $\mathbb{Q}$ 上での最小分解体を $L$ と書くと，$Gal(L/\mathbb{Q})\cong C_3$．

**解答例**　$F(x)=x^3+ax^2+b=(x-\alpha)(x-\beta)(x-\gamma)$ のとき，

$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-b(4a^3+27b)$　となることを示そう．

$\alpha+\beta+\gamma=-a$，$\alpha\beta+\alpha\gamma+\beta\gamma=0$，$\alpha\beta\gamma=-b$．

$F'(\alpha)=3\alpha^2+2a\alpha=(\alpha-\beta)(\alpha-\gamma)$，$F'(\beta)=3\beta^2+2a\beta=(\beta-\alpha)(\beta-\gamma)$，$F'(\gamma)=3\gamma^2+3a\gamma=(\gamma-\alpha)(\gamma-\beta)$ より，

$$(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-F'(\alpha)F'(\beta)F'(\gamma)=-\alpha\beta\gamma(3\alpha+2a)(3\beta+2a)(3\gamma+2a)$$

$$=\underbrace{-\alpha\beta\gamma}_{=b}(8a^3+12\underbrace{(\alpha+\beta+\gamma)}_{-a}a^2+18\underbrace{(\alpha\beta+\alpha\gamma+\beta\gamma)}_{=0}a+27\underbrace{\alpha\beta\gamma}_{-b})$$

$$=b(8a^3-12a^3-27b)=-b(4a^3+27b).$$

(1) $F(x)=x^3+3x^2-3$ は，$3\nmid 1$，$3\mid 3$，$3\mid 0$，$3\mid -3$，$3^2\nmid 3$ と Eisenstein の判定法より，
$\mathbb{Q}$ 上既約である．

(2) 前ページの公式を $a=3$，$b=-3$ に用いると，

$$D=(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2=-b(4a^3+27b)=3(4\cdot 3^3-27\cdot 3)=3^4=9^2$$

$3^3$，$3^3$，11

(3) $F(x)$ の $\mathbb{Q}$ 上での最小分解体を $L$ と書き，$G=\mathrm{Gal}(L/\mathbb{Q})$ とおく．
$F(x)$ は $\mathbb{Q}$ 上既約なので，$G$ の $\{\alpha,\beta,\gamma\}$ への作用は推移的になるので，
$G\cong A_3$ または $G\cong S_3$ となる．

$\Delta=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$ とおくと，$\Delta^2=D=9^2$ より，$\Delta=\pm 9\in\mathbb{Q}$ となる
ゆえに，任意の $\sigma\in G$ について，$\sigma(\Delta)=\Delta$ となり，$\sigma$ は $\{\alpha,\beta,\gamma\}$ の偶置換になる．
したがって，$G\cong A_3\cong C_3$．

□

**注意** $F(x-1)=(x-1)^3+3(x-1)^2-3=x^3-3x^2+3x-1+3x^2-6x+3-3=x^3-3x-1$．
$x^3-3x-1$ も $\mathbb{Q}$ 上既約になり，その $\mathbb{Q}$ 上での最小分解体は上と同じ $L$ になり，
$\mathrm{Gal}(L/\mathbb{Q})\cong A_3\cong C_3$ となる．

□