

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.

08-1

- (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.

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)

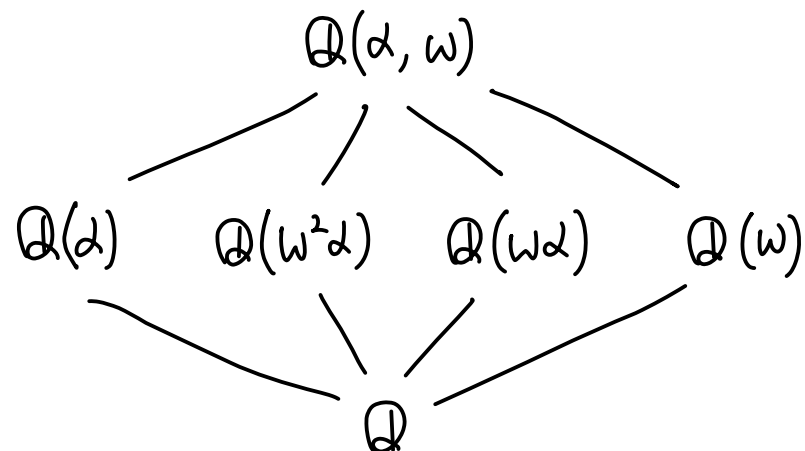
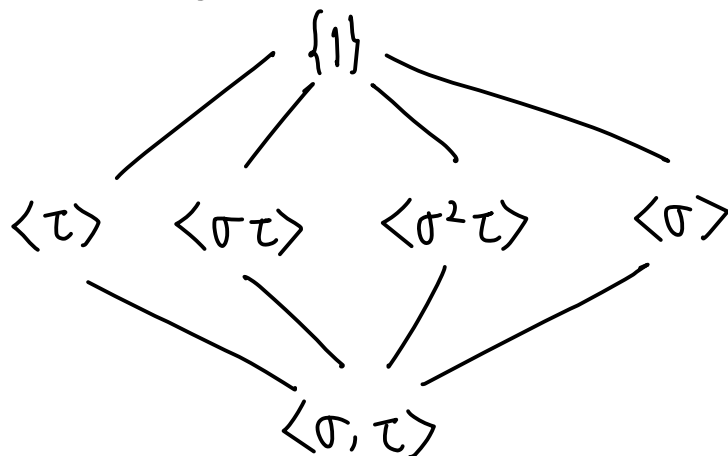
- (4) $\mathbb{Q}(\alpha, \omega)$ の体の自己同型 σ, τ を次のように定義できる:

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

- (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 7-1 解答例 ($F(x) = x^3 - 3$, $\alpha = \sqrt[3]{3}$, $\omega = \frac{-1 + \sqrt{-3}}{2}$, $\omega^3 = 1$, $\omega^2 + \omega + 1 = 0$.)

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

$F(x)$ は \mathbb{Q} 上で既約で $F(\alpha) = 0$ をみたすので, α の \mathbb{Q} 上での最小多項式である。

(2) $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\} \subset \mathbb{R}$ である. $\left(\begin{array}{l} \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(F(x)) \text{ より} \\ f(\alpha) \leftrightarrow \overline{f(x)} \end{array} \right)$

$F(x) = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \subset \mathbb{R}$ である。
ゆえに, $\mathbb{Q}(\alpha)$ は $F(x)$ の \mathbb{Q} 上での最小分解体ではない。

(3) $\alpha, \omega \in \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ より $\mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$. $\left. \begin{array}{l} \alpha, \omega\alpha, \omega^2\alpha \in \mathbb{Q}(\alpha, \omega) \text{ より } \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \subset \mathbb{Q}(\alpha, \omega), \end{array} \right\} \begin{array}{l} \text{ゆえに} \\ \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha). \end{array}$

$\alpha, \omega = \frac{-1 + \sqrt{-3}}{2} \in \mathbb{Q}(\alpha, \sqrt{-3})$ より $\mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \sqrt{-3})$ $\left. \begin{array}{l} \text{ゆえに} \\ \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3}). \end{array} \right\}$
 $\alpha, \sqrt{-3} = 2\omega + 1 \in \mathbb{Q}(\alpha, \omega)$ より, $\mathbb{Q}(\alpha, \sqrt{-3}) \subset \mathbb{Q}(\alpha, \omega)$

$$(4) [\mathbb{Q}(\omega) : \mathbb{Q}] = 2, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6 \text{ より}, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)] = \frac{[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]}{[\mathbb{Q}(\omega) : \mathbb{Q}]} = 3.$$

$$F(x) = x^3 - 3 \in \mathbb{Q}(\omega)[x], F(\alpha) = 0, \deg F(x) = 3 = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\omega)]$$

なので, $F(x)$ は $\mathbb{Q}(\omega)$ 上での α の最小多項式である,

ゆえに, 以下のようにして, $\mathbb{Q}(\alpha, \omega)$ の $\mathbb{Q}(\omega)$ 上での自己同型 σ を作れる:

$$\begin{array}{ccccc} \mathbb{Q}(\alpha, \omega) \cong \mathbb{Q}(\omega)[x]/(F(x)) & \cong & \mathbb{Q}(\omega\alpha, \omega) & = & \mathbb{Q}(\alpha, \omega) \\ f(\alpha) & \longleftrightarrow & \overline{f(x)} & \longleftrightarrow & f(\omega\alpha) \\ & \underbrace{\hspace{10em}}_{\sigma} & & & \end{array}$$

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6 \text{ より}, [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] = \frac{[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = 2,$$

$$G(x) = x^2 + x + 1 \text{ とおくと}, G(x) \in \mathbb{Q}(\alpha)[x], G(\omega) = 0, \deg G(x) = 2 = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)]$$

なので, $G(x)$ は $\mathbb{Q}(\alpha)$ 上での ω の最小多項式である,

ゆえに, 以下のようにして, $\mathbb{Q}(\alpha, \omega)$ の $\mathbb{Q}(\alpha)$ 上での自己同型 τ を作れる:

$$\begin{array}{ccccc} \mathbb{Q}(\alpha, \omega) \cong \mathbb{Q}(\alpha)[x]/(G(x)) & \cong & \mathbb{Q}(\alpha, \omega^2) & = & \mathbb{Q}(\alpha, \omega) \quad (\omega^2 = \omega^{-1}) \\ g(\omega) & \longleftrightarrow & \overline{g(x)} & \longleftrightarrow & g(\omega^2) \\ & \underbrace{\hspace{10em}}_{\tau} & & & \end{array}$$

(5) $\mathbb{Q}(\alpha, \omega)$ は $F(x) = x^3 - 3$ の \mathbb{Q} 上での最小分解体なので,

$\mathbb{Q}(\alpha, \omega)/\mathbb{Q}$ は有限次 Galois 拡大である.

$$\text{ゆえに, } |\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})| = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 6.$$

(4) の記号のもとで, $\sigma, \tau \in \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$ である. したがって,

$$1(\alpha) = \alpha, \quad 1(\omega) = \omega$$

$$\sigma(\alpha) = \omega\alpha, \quad \sigma(\omega) = \omega$$

$$\sigma^2(\alpha) = \omega^2\alpha, \quad \sigma^2(\omega) = \omega$$

$$\sigma^3(\alpha) = \alpha, \quad \sigma^3(\omega) = \omega$$

$$\tau(\alpha) = \alpha, \quad \tau(\omega) = \omega^2$$

$$\sigma\tau(\alpha) = \omega\alpha, \quad \sigma\tau(\omega) = \omega^2$$

$$\sigma^2\tau(\alpha) = \omega^2\alpha, \quad \sigma^2\tau(\omega) = \omega^2$$

$$\tau^2(\alpha) = \alpha, \quad \tau^2(\omega) = \omega^4 = \omega$$

$$\tau\sigma\tau(\alpha) = \omega^2\alpha, \quad \tau\sigma\tau(\omega) = \omega$$

ゆえに, この 1 は $\text{id}_{\mathbb{Q}(\alpha, \omega)}$

$$1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$$

は互いに異なるので,

$$\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}.$$

$$\text{さらに } \sigma^3 = \tau^2 = 1, \quad \tau\sigma\tau = \sigma^2 = \sigma^{-1},$$

$$\text{これより} \quad (\text{color: red; } \tau\sigma = \sigma^{-1}\tau)$$

$$\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) \cong D_3 \cong S_3.$$

(b) $G = \text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ ($\sigma^3 = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau$)

の部分群をすべて求めよう, $\overset{1}{\quad} \overset{3}{\quad} \overset{3}{\quad} \overset{2}{\quad} \overset{2}{\quad} \overset{2}{\quad} \leftarrow \text{元の位数}$

位数6の群 G の部分群の位数はその約数1, 2, 3, 6のどれかになる,

位数1 $\{1\}$ しかない,

位数2 位数2の部分群は位数2の元から生成される巡回群になる,

G の位数2の部分群全体は $\langle \tau \rangle, \langle \sigma\tau \rangle, \langle \sigma^2\tau \rangle$,

位数3 位数3の部分群は位数3の元から生成される巡回群になる,

G の位数3の部分群は $\langle \sigma \rangle = \langle \sigma^2 \rangle$ の1つだけ,

位数6 G の位数6の部分群は G そのものになる,

$L = \mathbb{Q}(\alpha, \omega)$ とおく, G の部分群 H に対応する L/\mathbb{Q} の部分体 L^H を求めよう.

$$[L : L^H] = |\text{Gal}(L/L^H)| = |H|, \quad [L^H : \mathbb{Q}] = \frac{[L : \mathbb{Q}]}{[L : L^H]} = \frac{|G|}{|H|} \text{ に注意せよ,}$$

$L^{\langle 1 \rangle}$ $L^{\langle 1 \rangle} = \{ \beta \in L \mid 1(\beta) = \beta \} = L = \mathbb{Q}(\alpha, \omega).$

$L^{\langle \tau \rangle}$ $\tau(\alpha) = \alpha$ より $\alpha \in L^{\langle \tau \rangle}$ なのて $\mathbb{Q}(\alpha) \subset L^{\langle \tau \rangle}$ であり,

$$[L^{\langle \tau \rangle} : \mathbb{Q}] = \frac{|G|}{|\langle \tau \rangle|} = \frac{6}{2} = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}] \text{ なのて } L^{\langle \tau \rangle} = \mathbb{Q}(\alpha).$$

$L^{\langle \sigma \tau \rangle}$ $\sigma\tau(\omega^2\alpha) = \sigma(\omega\alpha) = \omega^2\alpha$ なのて $\mathbb{Q}(\omega^2\alpha) \subset L^{\langle \sigma\tau \rangle}$ であり,

$$[L^{\langle \sigma\tau \rangle} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma\tau \rangle|} = \frac{6}{2} = 3 = [\mathbb{Q}(\omega^2\alpha) : \mathbb{Q}] \text{ なのて } L^{\langle \sigma\tau \rangle} = \mathbb{Q}(\omega^2\alpha).$$

$L^{\langle \sigma^2\tau \rangle}$ $\sigma^2\tau(\omega\alpha) = \sigma^2(\omega^2\alpha) = \omega^2\omega^2\alpha = \omega\alpha$ なのて $\mathbb{Q}(\omega\alpha) \subset L^{\langle \sigma^2\tau \rangle}$ であり,

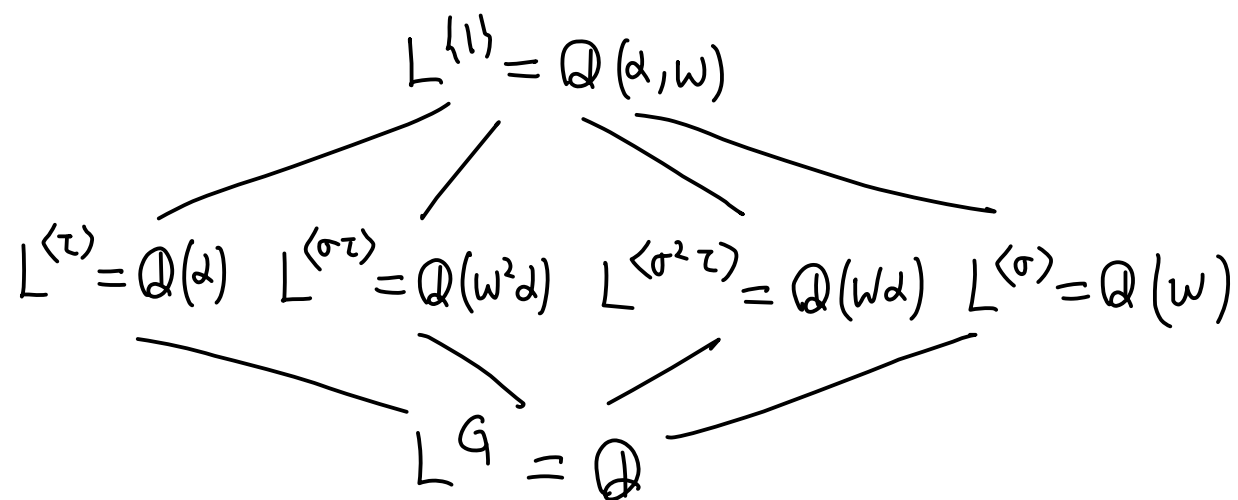
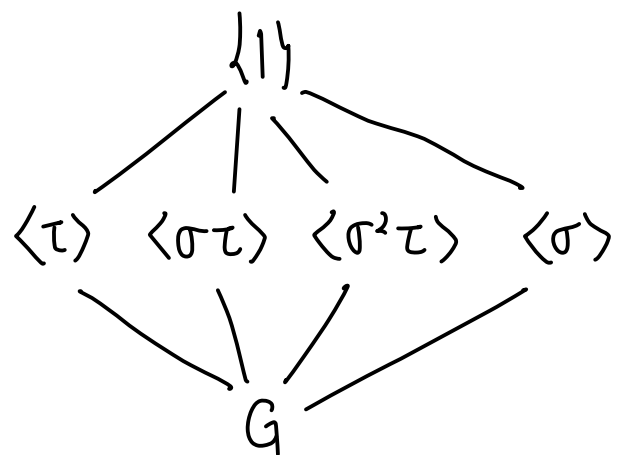
$$[L^{\langle \sigma^2\tau \rangle} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma^2\tau \rangle|} = \frac{6}{2} = 3 = [\mathbb{Q}(\omega\alpha) : \mathbb{Q}] \text{ なのて } L^{\langle \sigma^2\tau \rangle} = \mathbb{Q}(\omega\alpha).$$

$L^{\langle \sigma \rangle}$ $\sigma(\omega) = \omega$ より $\mathbb{Q}(\omega) \subset L^{\langle \sigma \rangle}$ であり

$$[L^{\langle \sigma \rangle} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma \rangle|} = \frac{6}{3} = 2 = [\mathbb{Q}(\omega) : \mathbb{Q}] \text{ なのて } L^{\langle \sigma \rangle} = \mathbb{Q}(\omega).$$

L^G $[L^G : \mathbb{Q}] = \frac{|G|}{|G|} = 1$ なのて $L^G = \mathbb{Q}.$

以上を図で描くと



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.
- (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:



問題 7-2 の解答例

$$F(x) = x^4 - 4x^2 + 2, \quad \alpha = \sqrt{2+\sqrt{2}} \quad \text{とおく.}$$

$$\alpha^2 = 2 + \sqrt{2}, \quad \alpha^4 = 6 + 4\sqrt{2} \quad \text{より,} \quad \alpha^4 - 4\alpha^2 + 2 = 0, \quad F(\alpha) = 0.$$

(1) $2 \nmid 1, 2 \nmid 0, 2 \nmid (-4), 2 \nmid 0, 2 \nmid 2, 2^2 \nmid 2$ と Eisenstein の判定法より,
 $F(x)$ は \mathbb{Q} 上で既約である.

$F(\alpha) = 0$ でもあるので, $F(x)$ は α の \mathbb{Q} 上での最小多項式である.

$$(2) \alpha = \sqrt{2+\sqrt{2}} \text{ の他に, } \beta = \sqrt{2-\sqrt{2}}, \quad \gamma = -\alpha, \quad \delta = -\beta \quad \text{とおく.}$$

$X^2 - 4X + X = 0$ の解は $X = 2 \pm \sqrt{2}$ なので $F(x)$ の根の全体は $\{\alpha, \beta, \gamma, \delta\}$ になる.

ゆえに $F(x)$ の \mathbb{Q} 上での最小分解体は $\mathbb{Q}(\alpha, \beta, \gamma, \delta) = \mathbb{Q}(\alpha, \beta)$ になる.

$$\frac{1}{\alpha} = \sqrt{\frac{1}{2+\sqrt{2}}} = \sqrt{\frac{2-\sqrt{2}}{2}} = \frac{\beta}{\sqrt{2}}, \quad \alpha^2 - 2 = \sqrt{2} \quad \text{より} \quad \beta = \frac{\sqrt{2}}{\alpha} = \frac{\alpha^2 - 2}{\alpha} \in \mathbb{Q}(\alpha).$$

ゆえに, $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \beta)$.

(3) 上と同様にして, $\alpha = \frac{\sqrt{2}}{\beta} = \frac{2-\beta^2}{\beta} \in \mathbb{Q}(\beta)$ なのて $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha, \beta)$.

ゆえに, $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$. $F(x)$ は β の \mathbb{Q} 上での最小多項式でもある.

以下のようにして, 体 $\mathbb{Q}(\alpha)$ の \mathbb{Q} 上での自己同型 σ を作れる:

$$\begin{array}{ccccc} \mathbb{Q}(\alpha) & \cong & \mathbb{Q}[x]/(F(x)) & \cong & \mathbb{Q}(\beta) = \mathbb{Q}(\alpha) \\ f(\alpha) & \longleftrightarrow & \overline{f(x)} & \longleftrightarrow & f(\beta) \\ & \searrow \quad \quad \quad \nearrow & & & \\ & \sigma & & & \end{array}$$

$$(4) \quad |\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})| = [\mathbb{Q}(\alpha):\mathbb{Q}] = \deg F(x) = 4.$$

$$\sigma(\alpha) = \beta = \frac{\alpha^2 - 2}{\alpha}$$

$$\sigma^2(\alpha) = \sigma(\beta) = \frac{\beta^2 - 2}{\beta} = \frac{-\sqrt{2}}{\beta} = -\alpha = \gamma$$

$$\sigma^3(\alpha) = \sigma(-\alpha) = -\sigma(\alpha) = -\beta = \delta$$

$$\sigma^4(\alpha) = \sigma(-\beta) = -\sigma(\beta) = -(-\alpha) = \alpha.$$

$1, \sigma, \sigma^2, \sigma^3$ は互いに異なるので

$$\text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{1, \sigma, \sigma^2, \sigma^3\},$$

さらに, $\sigma^4 = 1$ なのて

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

$$(5) G = \text{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \sigma^3\} \cong C_4 \text{ とおく.}$$

1 4 2 4 ← 元の位数.

G の部分群の全体は $\{1\}, \langle \sigma^2 \rangle, \langle \sigma \rangle = G$ の 3 つである.

$$\mathbb{Q}(\alpha)^{\{1\}} = \{\eta \in \mathbb{Q}(\alpha) \mid 1(\eta) = \eta\} = \mathbb{Q}(\alpha).$$

$$\sigma^2(\sqrt{2}) = \sigma^2(\alpha^2 - 2) = (-\alpha)^2 - 2 = \alpha^2 - 2 = \sqrt{2} \text{ より } \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle} \text{ であり,}$$

$$\sigma^2(\alpha) = -\alpha$$

$$[\mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma^2 \rangle|} = \frac{4}{2} = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \text{ なのて } \mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle} = \mathbb{Q}(\sqrt{2}).$$

$$[\mathbb{Q}(\alpha)^G : \mathbb{Q}] = \frac{|G|}{|G|} = 1 \text{ より } \mathbb{Q}(\alpha)^G = \mathbb{Q}.$$

以上を図で描くと,

$$\begin{array}{c} \{1\} \\ | \\ \langle \sigma^2 \rangle \\ | \\ G = \langle \sigma \rangle \end{array}$$

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