

**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  $\alpha$  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  $\mathbb{Q}(\alpha)$  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.

$\mathbb{Q}$  上の方程式  $x^3 - 3 = 0$  の  
Galois 対応の記述

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)

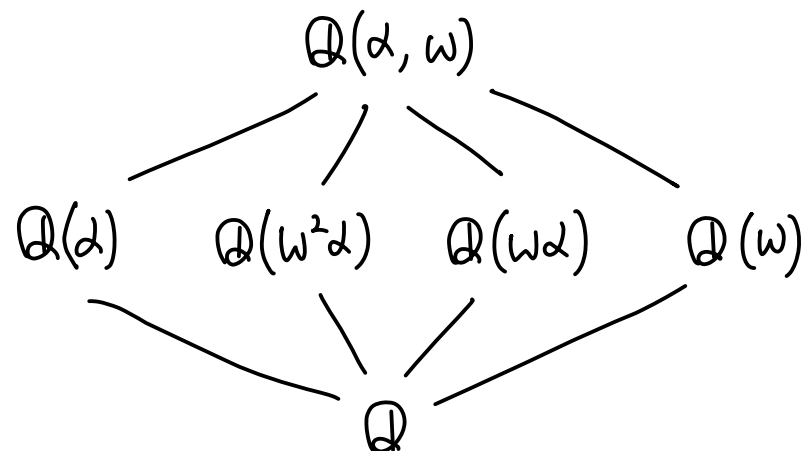
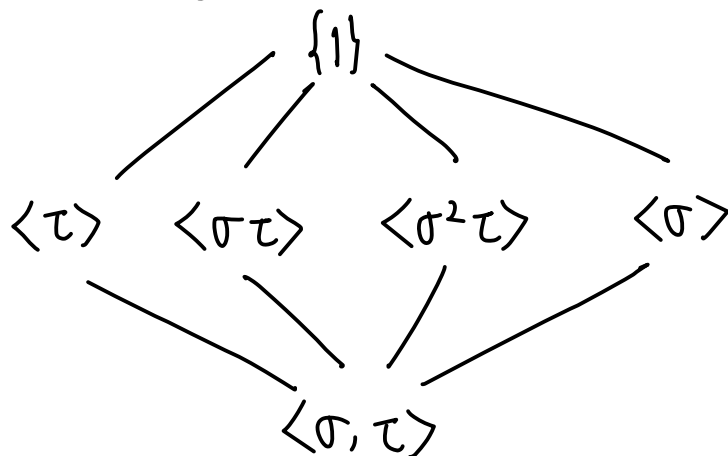
- (4)  $\mathbb{Q}(\alpha, \omega)$  の体の自己同型  $\sigma, \tau$  を次のように定義できる:

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

- (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.

- (b)  $\text{Gal}(\mathbb{Q}(\alpha, \omega)/\mathbb{Q})$  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. ( $x^3 - 3$  が  $\mathbb{Q}$  に根を持たないこともその  $\mathbb{Q}$  上既約性からわかる.) ← どうしてか?

$F(x)$  は  $\mathbb{Q}$  上で既約で  $F(\alpha) = 0$  をみたすので,  $\alpha$  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.  $\left( \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(F(x)) \text{ より } f(\alpha) \leftrightarrow \overline{f(x)} \right)$

$F(x) = (x - \alpha)(x - \omega\alpha)(x - \omega^2\alpha)$  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)  $\alpha, \omega = \frac{\omega\alpha}{\alpha} \in \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$  より  $\mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ .  
 $\alpha, \omega\alpha, \omega^2\alpha \in \mathbb{Q}(\alpha, \omega)$  より  $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \subset \mathbb{Q}(\alpha, \omega)$ .  
 ゆえに  $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ .

$\alpha, \omega = \frac{-1 + \sqrt{-3}}{2} \in \mathbb{Q}(\alpha, \sqrt{-3})$  より  $\mathbb{Q}(\alpha, \omega) \subset \mathbb{Q}(\alpha, \sqrt{-3})$ .  
 $\alpha, \sqrt{-3} = 2\omega + 1 \in \mathbb{Q}(\alpha, \omega)$  より,  $\mathbb{Q}(\alpha, \sqrt{-3}) \subset \mathbb{Q}(\alpha, \omega)$ .  
 ゆえに  $\mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha, \sqrt{-3})$ .

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

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

$G_\alpha(x)$  は  $\mathbb{Q}(w)$  上の  $\alpha$  の最小多項式

なので,  $F(x)$  は  $\mathbb{Q}(w)$  上での  $\alpha$  の最小多項式である,  $\mathbb{Q}(w)(\alpha) \cong \mathbb{Q}(w)[x]/(G_\alpha(x))$

ゆえに, 以下のようにして,  $\mathbb{Q}(\alpha, w)$  の  $\mathbb{Q}(w)$  上での自己同型  $\sigma$  を作れる:  $\deg G_\alpha(x) = 3$

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

$$f(\alpha) \mapsto \overline{f(x)} \mapsto f(w\alpha)$$

$F(x)$  は  $\mathbb{Q}(w)$  上既約で  $w\alpha$  を根になるので,  $F(x)$  は  $w\alpha$  の  $\mathbb{Q}(w)$  上での最小多項式にもなっている.

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

$G(x) = x^2 + x + 1$  とおくと,  $G(x) \in \mathbb{Q}(\alpha)[x]$ ,  $G(w) = 0$ ,  $\deg G(x) = 2 = [\mathbb{Q}(\alpha, w) : \mathbb{Q}(\alpha)]$   
 なので,  $G(x)$  は  $\mathbb{Q}(\alpha)$  上での  $w$  の最小多項式である.

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

$$\mathbb{Q}(\alpha, w) \cong \mathbb{Q}(\alpha)[x]/(G(x)) \cong \mathbb{Q}(\alpha, w^2) = \mathbb{Q}(\alpha, w) \quad (w^2 = w^{-1})$$

$$g(w) \mapsto \overline{g(x)} \mapsto g(w^2)$$

上と同様に  $G(x)$  は  $w^2$  の  $\mathbb{Q}(\alpha)$  上での最小多項式にもなっている.

(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.

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

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

- ①  $1(\alpha) = \alpha, \quad 1(\omega) = \omega$
- ②  $\sigma(\alpha) = \omega\alpha, \quad \sigma(\omega) = \omega$
- ③  $\sigma^2(\alpha) = \omega^2\alpha, \quad \sigma^2(\omega) = \omega$   
 $\underline{\sigma^3(\alpha) = \alpha, \quad \sigma^3(\omega) = \omega}$
- ④  $\tau(\alpha) = \alpha, \quad \tau(\omega) = \omega^2$
- ⑤  $\sigma\tau(\alpha) = \omega\alpha, \quad \sigma\tau(\omega) = \omega^2$
- ⑥  $\sigma^2\tau(\alpha) = \omega^2\alpha, \quad \sigma^2\tau(\omega) = \omega^2$   
 $\underline{\tau^2(\alpha) = \alpha, \quad \tau^2(\omega) = \omega^4 = \omega}$   
 $\underline{\tau\sigma\tau(\alpha) = \omega^2\alpha, \quad \tau\sigma\tau(\omega) = \omega}$

ゆえに, この 1 は  $id_{\mathbb{Q}(\alpha, \omega)}$   
 $1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau$

は互いに異なるので,

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

さらに  $\underline{\sigma^3 = \tau^2 = 1}, \quad \underline{\tau\sigma\tau = \sigma^2 = \sigma^{-1}},$   
 これより ( $\tau\sigma = \sigma^{-1}\tau$ )

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

$D_3 = \langle \sigma, \tau \mid \sigma^3 = \tau^2 = 1, \tau\sigma\tau = \sigma^{-1} \rangle$   
 $\| = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$

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

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

の部分群をすべて求めよう.  $1 \quad 3 \quad 3 \quad 2 \quad \underbrace{2 \quad 2}_{\leftarrow \text{元の位数}} \leftarrow \text{自分で確認せよ.}$

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,

(Lagrangeの定理より)  $\uparrow$

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  $G = \langle \sigma, \tau \rangle$  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  $L/\mathbb{Q}$  の中間体  $L^H$  を求めよう.

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

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

$$L^H = \{ \beta \in L \mid \rho(\beta) = \beta \ (\forall \rho \in H) \}$$

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

$\mathbb{Q}$  上のベクトル空間として,

$$\mathbb{Q}(\alpha) \subset L^{\langle \tau \rangle}$$

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

両方  $\mathbb{Q}$  上での次元が3

$$\text{ゆえに } \mathbb{Q}(\alpha) = L^{\langle \tau \rangle}$$

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

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

上と同様

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

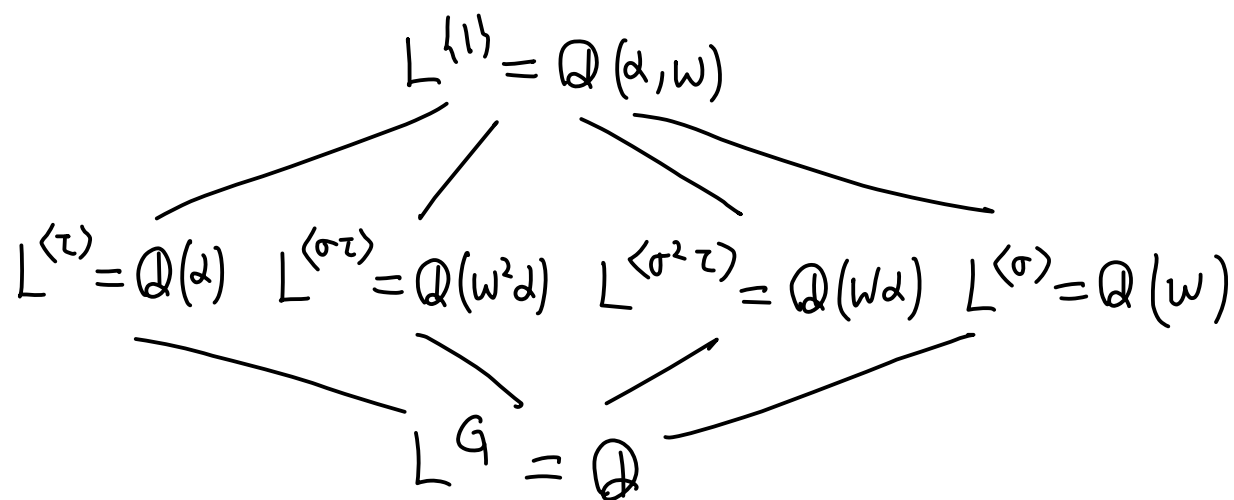
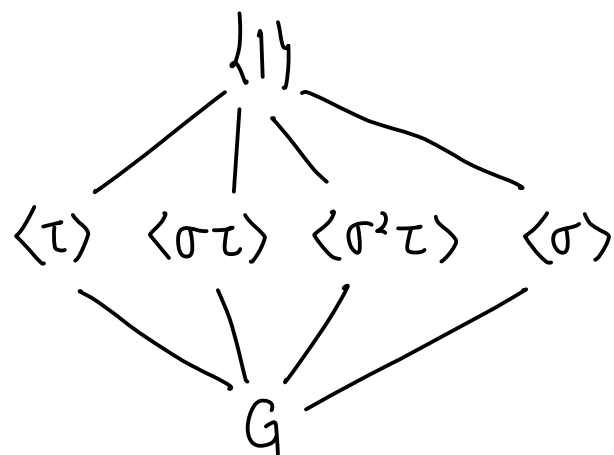
$$[L^{\langle \sigma^2 \tau \rangle} : \mathbb{Q}] = \frac{|G|}{|\langle \sigma^2 \tau \rangle|} = \frac{6}{2} = 3 = [\mathbb{Q}(\omega\alpha) : \mathbb{Q}] \text{ なのて } L^{\langle \sigma^2 \tau \rangle} = \mathbb{Q}(\omega\alpha).$$

$L^{\langle \sigma \rangle}$   $\sigma(\omega) = \omega$  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



上の図は  $\mathbb{Q}$  上での方程式  $x^3 - 3 = 0$  がどのように解けて行くかを記述しているといえる。

$$\left\{ \begin{array}{ll} L = \mathbb{Q}(\alpha, \omega) & \longleftrightarrow x^3 - 3 = 0 \text{ を解き切った結果} \\ L/\mathbb{Q} \text{ の中間体} & \longleftrightarrow x^3 - 3 = 0 \text{ を解く途中の様子} \\ L^{<\tau>} = \mathbb{Q}(\alpha) & \longleftrightarrow x^3 - 3 = 0 \text{ の解の1つ } \alpha \text{ が得られた様子} \\ L^{<\sigma>} = \mathbb{Q}(\omega) & \longleftrightarrow x^3 - 3 = 0 \text{ を解き切るために必要な } \omega \text{ が得られた様子} \end{array} \right.$$

**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  $\alpha$  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  $\mathbb{Q}(\alpha)$  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  $\sigma$  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:



$\mathbb{Q}$  上の方程式

$$x^4 - 4x^2 + 2 = 0$$

に関する Galois 対応を  
求める問題



### 問題 7-2 の解答例

$x^2 = 2 \pm \sqrt{2}$ ,  $x = \sqrt{2 \pm \sqrt{2}}$ ,  $-\sqrt{2 \pm \sqrt{2}}$  と解ける.

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

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

(1)  $2 \nmid 1$ ,  $2 \mid 0$ ,  $2 \mid (-4)$ ,  $2 \mid 0$ ,  $2 \nmid 2$ ,  $2^2 \nmid 2$  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  $\alpha$  の  $\mathbb{Q}$  上での最小多項式である.

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

$X^2 - 4X + 2 = 0$  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.

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

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  $\beta$  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  $\sigma$  を作れる:

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

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

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

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

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

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

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

$\text{III}$   
 $C_1$     $\text{III}$   
 $C_2$     $\text{III}$   
 $C_4$

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

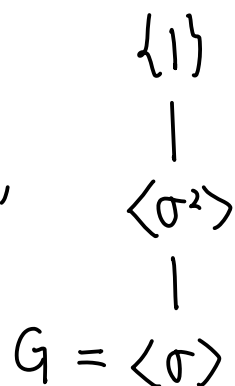
$\left( \begin{array}{l} \sqrt{2} = \alpha^2 - 2 \text{ より } \sigma^2(\alpha) = -\alpha \text{ のこと} \\ \sigma^2(\sqrt{2}) = \sqrt{2}. \end{array} \right)$

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

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

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

以上を図で描くと,



$\mathbb{Q}(\alpha)^{\{1\}} = \mathbb{Q}(\alpha)$

$\mathbb{Q}(\alpha)^{\langle \sigma^2 \rangle} = \mathbb{Q}(\sqrt{2})$

$\mathbb{Q}(\alpha)^{\langle \sigma \rangle} = \mathbb{Q}$

$x^2 = 2 \pm \sqrt{2}$  を解くと  
解は  $\alpha = \sqrt{2 + \sqrt{2}}$  で書ける.

$X^2 - 4X + 2 = 0$  は  
 $X = 2 \pm \sqrt{2}$  と解ける.