資料08-1

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

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

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:

$$\begin{tikzcd}[column sep=small]
 & & \{1\} \arrow[dll, no head] \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\langle\tau\rangle & \langle\sigma\tau\rangle & \langle\sigma^2\tau\rangle & \langle\sigma\rangle \\
 & & \langle\sigma,\tau\rangle \arrow[ull, no head] \arrow[ul, no head] \arrow[u, no head] \arrow[ur, no head] &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & & \mathbb{Q}(\alpha,\omega) \arrow[dll, no head] \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \\
\mathbb{Q}(\alpha) & \mathbb{Q}(\omega^2\alpha) & \mathbb{Q}(\omega\alpha) & \mathbb{Q}(\omega) \\
 & & \mathbb{Q} \arrow[ull, no head] \arrow[ul, no head] \arrow[u, no head] \arrow[ur, no head] &
\end{tikzcd}$$

問題7-1 解答例

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

(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からも$\mathbb{Q}$上での既約性がわかる.) ← どうしてか?

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

$F(x) = (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha)$ の$\mathbb{Q}$上での最小分解体は $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha) \not\subset \mathbb{R}$ 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) $[\mathbb{Q}(\omega):\mathbb{Q}]=2$, $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]=6$ より, $[\mathbb{Q}(\alpha,\omega):\mathbb{Q}(\omega)]=\dfrac{[\mathbb{Q}(\alpha,\omega):\mathbb{Q}]}{[\mathbb{Q}(\omega):\mathbb{Q}]}=3.$

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

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

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

$\parallel$ $\mathbb{Q}(\omega)(\alpha)\cong\mathbb{Q}(\omega)[x]/(G_\alpha(x))$

$\deg G_\alpha(x)=3$

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:

$$\begin{array}{ccccccc}\mathbb{Q}(\alpha,\omega) & \xrightarrow{\sim} & \mathbb{Q}(\omega)[x]/(F(x)) & \xrightarrow{\sim} & \mathbb{Q}(\omega\alpha,\omega) & = & \mathbb{Q}(\alpha,\omega)\\ f(\alpha) & \longmapsto & \overline{f(x)} & \longmapsto & f(\omega\alpha) & & \end{array}$$
$$f(\alpha)\overset{\sigma}{\longmapsto} f(\omega\alpha)$$

$F(x)$ は $\mathbb{Q}(\omega)$ 上既約で $\omega\alpha$ を根にもつので, $F(x)$ は $\omega\alpha$ の $\mathbb{Q}(\omega)$ 上での最小多項式にもなっている。

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

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

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:

$$\begin{array}{ccccccc}\mathbb{Q}(\alpha,\omega) & \xrightarrow{\sim} & \mathbb{Q}(\alpha)[x]/(G(x)) & \xrightarrow{\sim} & \mathbb{Q}(\alpha,\omega^2) & = & \mathbb{Q}(\alpha,\omega)\quad(\omega^2=\omega^{-1})\\ g(\omega) & \longmapsto & \overline{g(x)} & \longmapsto & g(\omega^2) & & \end{array}$$
$$g(\omega)\overset{\tau}{\longmapsto} g(\omega^2)$$

上と同様に $G(x)$ は ω^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、$|\mathrm{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})| = [\mathbb{Q}(\alpha,\omega):\mathbb{Q}] = 6$.

(4) の記号のもとで、$\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\alpha,\omega)/\mathbb{Q})$ である。そして、

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

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

③ $\sigma^2(\alpha)=\omega^2\alpha$, $\sigma^2(\omega)=\omega$

$\underline{\sigma^3(\alpha)=\alpha,\ \sigma^3(\omega)=\omega}$

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

⑤ $\sigma\tau(\alpha)=\omega\alpha$, $\sigma\tau(\omega)=\omega^2$

⑥ $\sigma^2\tau(\alpha)=\omega^2\alpha$, $\sigma^2\tau(\omega)=\omega^2$

$\underline{\tau^2(\alpha)=\alpha,\ \tau^2(\omega)=\omega^4=\omega}$

$\underline{\tau\sigma\tau(\alpha)=\omega^2\alpha,\ \tau\sigma\tau(\omega)=\omega}$

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

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

は互いに異なるので、

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

さらに $\underline{\sigma^3=\tau^2=1}$, $\underline{\tau\sigma\tau=\sigma^2=\sigma^{-1}}$.

$(\tau\sigma=\sigma^{-1}\tau)$

これより

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

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

$= \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$

$\cong$

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

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

の部分群をすべて求めよう。 $1 \quad 3 \quad 3 \quad 2 \quad \underbrace{2 \quad 2}$ ← 元の位数

← 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。

(Lagrangeの定理より)

<u>位数1</u> $\{1\}$ しかない。

<u>位数2</u> 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 $\langle\tau\rangle, \langle\sigma\tau\rangle, \langle\sigma^2\tau\rangle$。

<u>位数3</u> 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。

<u>位数6</u> 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。

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

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

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

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

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

$\mathbb{Q}$上のベクトル空間として、

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

両方 $\mathbb{Q}$上での次元が3

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

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

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

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

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

上と同様

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

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

$\underline{L^G}$ $[L^G:\mathbb{Q}]=\dfrac{|G|}{|G|}=1$ なので $L^G=\mathbb{Q}$.

以上を図で描くと

$$
\begin{tikzcd}[column sep=small]
 & & & \{1\} \arrow[dlll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drrr, dash] & & & \\
\langle\tau\rangle \arrow[drrr, dash] & & \langle\sigma\tau\rangle \arrow[dr, dash] & & \langle\sigma^2\tau\rangle \arrow[dl, dash] & & \langle\sigma\rangle \arrow[dlll, dash] \\
 & & & G & & &
\end{tikzcd}
$$

$$
\begin{tikzcd}[column sep=tiny]
 & & & L^{\{1\}} = \mathbb{Q}(\alpha,\omega) \arrow[dlll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drrr, dash] & & & \\
L^{\langle\tau\rangle} = \mathbb{Q}(\alpha) \arrow[drrr, dash] & & L^{\langle\sigma\tau\rangle} = \mathbb{Q}(\omega^2\alpha) \arrow[dr, dash] & & L^{\langle\sigma^2\tau\rangle} = \mathbb{Q}(\omega\alpha) \arrow[dl, dash] & & L^{\langle\sigma\rangle} = \mathbb{Q}(\omega) \arrow[dlll, dash] \\
 & & & L^{G} = \mathbb{Q} & & &
\end{tikzcd}
$$

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みなせる.

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

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 $\sigma(f(\alpha)) = f(\sqrt{2-\sqrt{2}})$ $(f(x) \in \mathbb{Q}[x])$ と定義できる.

(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:

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

$\mathbb{Q}$ 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.

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

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

(1) $2 \nmid 1$, $2 \mid 0$, $2 \mid (-4)$, $2 \mid 0$, $2 \mid 2$, $2^2 \nmid 2$ 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) $\alpha = \sqrt{2+\sqrt{2}}$ 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.

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

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

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

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:

$$
\begin{tikzcd}
\mathbb{Q}(\alpha) \arrow[r, "\sim"] & \mathbb{Q}[x]/(F(x)) \arrow[r, "\sim"] & \mathbb{Q}(\beta) = \mathbb{Q}(\alpha) \\
f(\alpha) \arrow[r, mapsto] \arrow[rr, mapsto, bend right, "\sigma"'] & \overline{f(x)} \arrow[r, mapsto] & f(\beta)
\end{tikzcd}
$$

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

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

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

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

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

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

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

さらに, $\sigma^4 = 1$ なので

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

(5) $G = \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = \langle \sigma \rangle = \{\underset{1}{1}, \underset{4}{\sigma}, \underset{2}{\sigma^2}, \underset{4}{\sigma^3}\} \cong C_4$ とおく。

← 元の位数.

G の部分群の全体は $\underset{\substack{\cong \\ C_1}}{\{1\}}, \underset{\substack{\cong \\ C_2}}{\langle \sigma^2 \rangle}, \underset{\substack{\cong \\ C_4}}{\langle \sigma \rangle} = G$ の3つである。

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

($\sqrt{2} = \alpha^2 - 2$ で $\sigma^2(\alpha) = -\alpha$ なので $\sigma^2(\sqrt{2}) = \sqrt{2}$.)

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

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

(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,

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

$x^2 = 2 \pm \sqrt{2}$ 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.