「ガロア理論入門」演習問題略解

大阿久 俊則

問題 1.1 (1) $\alpha-1=\sqrt{5}$ より $(\alpha-1)^2=5$，すなわち $\alpha^2-2\alpha-4=0$．よって $f(x)=x^2-2x-4$ とおけば，$f(\alpha)=0$ が成立する．上の変形から $f(x)=(x-1-\sqrt{5})(x-1+\sqrt{5})$ であることがわかるが，この右辺の 1 次式の係数は有理数でないから，$f(x)$ は $\mathbb{Q}[x]$ においては 1 次式の積に分解できない．（正確に言うと，$\mathbb{C}[x]$ が UFD なので素元分解が一通りであり，これ以外には分解できないことを用いている．）よって $f(x)$ は $\mathbb{Q}$ 上既約であるから，$f(x)$ が α の $\mathbb{Q}$ 上の最小多項式である．あるいは命題 2.2 と ±1, ±2, ±4 が $f(x)=0$ の根ではないことから $f(x)$ が $\mathbb{Q}$ 上既約であることがわかる．以上により $[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg f=2$ である．1 と α （または 1 と $\sqrt{5}$）が $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の基底となる．

(2) $2\alpha+1=\sqrt{-3}$ より $(2\alpha+1)^2=-3$，すなわち $4\alpha^2+4\alpha+4=0$．よって $f(x)=x^2+x+1$ は $f(\alpha)=0$ を満たす．$f(x)=\left(x-\dfrac{-1+\sqrt{-3}}{2}\right)\left(x-\dfrac{-1-\sqrt{-3}}{2}\right)$ であり右辺の 1 次式の係数は有理数でない（実数でもない）ので $f(x)$ は $\mathbb{Q}$ 上既約であるから α の最小多項式である．（あるいは $f(\pm1)\neq0$ と命題 2.2 を用いてもよい．）以上により $[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg f=2$ である．1 と α （または 1 と $\sqrt{-3}$）が $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の基底となる．

(3) $f(x)=x^3-4$ とおくと $f(\alpha)=0$ が成立する．$f(\pm1)\neq0$, $f(\pm2)\neq0$, $f(\pm4)\neq0$ であるから命題 2.2 により $f(x)$ は $\mathbb{Q}$ 上既約である．（あるいは例 1.5 と同様に示すこともできる．）以上により $[\mathbb{Q}(\alpha):\mathbb{Q}]=\deg f=3$ である．1, $\alpha=\sqrt[3]{4}$, $\alpha^2=2\sqrt[3]{2}$ が $\mathbb{Q}(\alpha)$ の $\mathbb{Q}$ 上の基底となる．なお，これから $\mathbb{Q}(\sqrt[3]{4})=\mathbb{Q}(\sqrt[3]{2})$ であることがわかる．

問題 1.2 $\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $f(x)=x^3-2$ である．（例 1.5 より．または命題 2.2 またはアイゼンシュタインの判定法から $f(x)$ が $\mathbb{Q}$ 上既約であるから．）よって $[\mathbb{Q}(\sqrt[3]{2}),\mathbb{Q}]=3$ である．次に $g(x)=x^2+1=(x-i)(x+i)$ であり $\pm i$ は $\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{R}$ には属さないから $g(x)$ は $\mathbb{Q}(\sqrt[3]{2})$ 上既約である．$g(i)=0$ であるから $g(x)$ は i の $\mathbb{Q}(\sqrt[3]{2})$ 上の最小多項式である．よって $[\mathbb{Q}(\sqrt[3]{2})(i):\mathbb{Q}(\sqrt[3]{2})]=2$ であるから，

$$[\mathbb{Q}(i,\sqrt[3]{2})):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2})(i):\mathbb{Q}]=[\mathbb{Q}(\sqrt[3]{2})(i):\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=2\cdot3=6.$$

1, $\sqrt[3]{2}$, $\sqrt[3]{4}$, i, $i\sqrt[3]{2}$, $i\sqrt[3]{4}$ が $\mathbb{Q}(i,\sqrt[3]{2})$ の $\mathbb{Q}$ 上の基底となる．

問題 1.3 $\sqrt{3}$ の $\mathbb{Q}$ 上の最小多項式は $f(x)=x^2-3$ であるから，1, $\sqrt{3}$ は $\mathbb{Q}(\sqrt{3})$ の $\mathbb{Q}$ 上の基底である．

また $i\sqrt{2}=\sqrt{-2}$ の最小多項式は $g(x)=x^2+2$ である．実際，$g(x)=(x-i\sqrt{2})(x+i\sqrt{2})$ であり右辺の 1 次式の係数は $\mathbb{Q}(\sqrt{3})\subset\mathbb{R}$ には含まれないから $g(x)$ は $\mathbb{Q}(\sqrt{3})$ 上既約で

ある．これと $g(i\sqrt{2}) = 0$ から $g(x)$ が $i\sqrt{2}$ の最小多項式であることがわかる．よって $\mathbb{Q}(\sqrt{3}, i\sqrt{2}) = \mathbb{Q}(\sqrt{3})(i\sqrt{2})$ の $\mathbb{Q}(\sqrt{3})$ 上の基底として $1, i\sqrt{2}$ がとれる．以上により $[\mathbb{Q}(i\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ であり，$1, \sqrt{3}, i\sqrt{2}, i\sqrt{6}$ が $\mathbb{Q}(i\sqrt{2}, \sqrt{3})$ の $\mathbb{Q}$ 上の基底である．

問題 2.1 それぞれの多項式を $f(x)$ とする．

(1) $f(\pm 1) \neq 0$ であるから命題 2.2 より $f(x)$ は $\mathbb{Q}$ 上既約である．

(2) $f(-1)$ より $f(x)$ を $x+1$ で割り算すると $f(x) = (x^2+1)(x+1)$. x^2+1 は $\mathbb{Q}$ 上既約だからこれは $\mathbb{Q}$ 上の既約分解である．

(3) $12, 8, 6$ は 2 の倍数であり，定数項 6 は $2^2 = 4$ の倍数ではないから，$p = 2$ として Eisenstein の判定法を用いて $f(x)$ は $\mathbb{Q}$ 上既約であることがわかる．

(4) 展開すると，$f(x) = x^4 + 5x^3 + 10x^2 + 10x + 5$ となるので，$p = 5$ として Eisenstein の判定法を適用すれば $f(x)$ は $\mathbb{Q}$ 上既約であることがわかる．

(5) $f(x+1)$ は (4) によって $\mathbb{Q}$ 上既約だから $f(x)$ も $\mathbb{Q}$ 上既約である．実際 $f(x)$ が既約でないとすると $f(x) = g(x)h(x)$ を満たす 1 次以上の $g, h \in \mathbb{Q}[x]$ が存在するが，このとき $f(x+1) = g(x+1)h(x+1)$ であり $g(x+1)$ と $h(x+1)$ の次数は 1 以上であるから，$f(x+1)$ が既約であることに反する．

(6) $x^6 - 1 = (x^3-1)(x^3+1) = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$ と分解できる．ここで $x^2 \pm x + 1$ は $x = \pm 1$ を代入したとき 0 にならないから $\mathbb{Q}$ 上既約である．よってこれは $\mathbb{Q}[x]$ における既約分解である．

問題 2.2 (1) $\alpha^2 = i$ より $\alpha^4 = -1$ となる．

(2) まず $\alpha \notin \mathbb{Q}(i)$ を示す．$\alpha \in \mathbb{Q}(i)$ と仮定すると，ある有理数 a, b が存在して

$$\alpha = \frac{1+i}{\sqrt{2}} = a + bi$$

が成立する．実部と虚部を比較して $a = b = \dfrac{1}{\sqrt{2}} = \dfrac{\sqrt{2}}{2}$ を得るが，$\sqrt{2}$ は無理数であるからこれは矛盾である．よって α は $\mathbb{Q}(i)$ に属さないから α の $\mathbb{Q}(i)$ 上の最小多項式の次数は 2 以上である．一方 $g(x) = x^2 - i \in \mathbb{Q}(i)[x]$ とおくと，$g(\alpha) = 0$ が成立する．従って $g(x)$ が α の $\mathbb{Q}(i)$ 上の最小多項式である．

(3) まず $i = \alpha^2 \in \mathbb{Q}(\alpha)$ より $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, i) = \mathbb{Q}(i)(\alpha)$ であることに注意する．(2) と定理 1.1 より $[\mathbb{Q}(\alpha)(i), \mathbb{Q}(i)] = 2$ であるから，

$$[\mathbb{Q}(\alpha), \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}] = [\mathbb{Q}(\alpha, i), \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 2 \times 2 = 4$$

(4) $f(x) = x^4 + 1 \in \mathbb{Q}[x]$ は $f(\alpha) = 0$ を満たすから $I(\alpha)$ に属する．よって $f(x)$ は α の $\mathbb{Q}$ 上の最小多項式 $f_\alpha(x)$ の倍元である．一方 (3) と定理 1.1 より $f_\alpha(x)$ の次数は 4 であるから，$f(x) = f_\alpha(x)$ が α の $\mathbb{Q}$ 上の最小多項式であり，特に既約である．

（別解） $f(x)=x^4+1$ とおくと，

$$f(x+1)=(x+1)^4+1=x^4+4x^3+6x^2+4x+2$$

となるから，Eisenstein の判定法を $p=2$ として適用すれば $f(x+1)$ は $\mathbb{Q}$ 上既約である．従って問題 2.1 の (5) と同じ論法で $f(x)$ も $\mathbb{Q}$ 上既約である．

問題 3.1 (1) $x^2+x-1=0$ の根 α,β は $\dfrac{-1\pm\sqrt{5}}{2}$ であり，共に $\mathbb{Q}(\sqrt{5})$ に含まれる．逆に $\sqrt{5}=\alpha-\beta$ であるから，$\sqrt{5}$ は $\mathbb{Q}(\alpha,\beta)$ に含まれる．以上により x^2+x-1 の分解体 L は $\mathbb{Q}(\alpha,\beta)=\mathbb{Q}(\sqrt{5})$ である．（あるいは，$\mathbb{Q}\subsetneq L\subset\mathbb{Q}(\sqrt{5})$ と $[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]=2$ から $L=\mathbb{Q}(\sqrt{5})$.）$\sqrt{5}$ の最小多項式は x^2-5 であるから，分解体の拡大次数は 2 である．

(2) $x^4-1=(x^2-1)(x^2+1)=(x-1)(x+1)(x-i)(x+i)$ より分解体は $\mathbb{Q}(i)$ であり，拡大次数は 2 である．

(3) $x^6-1=(x^3-1)(x^3+1)=(x-1)(x+1)(x^2+x+1)(x^2-x+1)$ であり，$x^2\pm x+1=0$ の根は $x=\mp\dfrac{1\pm\sqrt{-3}}{2}$ であるから，$x^6-1=0$ の根はすべて $\mathbb{Q}(\sqrt{-3})$ に含まれる．逆に $\sqrt{-3}=\dfrac{1+\sqrt{-3}}{2}-\dfrac{1-\sqrt{-3}}{2}$ であるから $\mathbb{Q}(\sqrt{-3})$ は x^6-1 の分解体に含まれる．以上により x^6-1 の分解体は $\mathbb{Q}(\sqrt{-3})$ である．$\sqrt{-3}$ の最小多項式は x^2+3 であるから，分解体の拡大次数は 2 である．

（別解）極形式により $z^6=1$ を満たす複素数は

$$\omega=\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}=\frac{1+\sqrt{3}i}{2}$$

とおくと $z=\omega^k$ $(k=0,1,2,3,4,5)$ である．よって x^6-1 の分解体は $\mathbb{Q}(\omega)=\mathbb{Q}(\sqrt{3}i)$ である．

(4) $x^3-8=(x-2)(x^2+2x+4)$ であり $x^2+2x+4=0$ の根は $x=-1\pm\sqrt{-3}$ であるから x^3-8 の分解体は $\mathbb{Q}(\sqrt{-3})$ である．$\sqrt{-3}$ の最小多項式は x^2+3 であるから，分解体の拡大次数は 2 である．

（別解）極形式により $z^3=8$ を満たす複素数は

$$\omega=\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}=\frac{-1+\sqrt{3}i}{2}$$

とおくと $z=2\omega^k$ $(k=0,1,2)$ である．よって x^6-1 の分解体は $\mathbb{Q}(\omega)=\mathbb{Q}(\sqrt{3}i)$ である．

(5) $z=r(\cos\theta+i\sin\theta)$ を極形式とすると

$$z^4=r^4(\cos 4\theta+i\sin 4\theta)=-4=4(\cos\pi+i\sin\pi)$$

を満たす複素数は

$$\begin{aligned} z_k&=\sqrt{2}\left(\cos\frac{\pi+2k\pi}{4}+i\sin\frac{\pi+2k\pi}{4}\right)\qquad(k=0,1,2)\\ &=1+i,\ -1+i,\ -1-i,\ 1-i \end{aligned}$$

の 3 個である．これらはすべて $\mathbb{Q}(i)$ に含まれ，逆に $i = \frac{1}{2}\{(1+i)+(-1+i)\}$ は x^4+1 の分解体に含まれる．よって x^4+1 の分解体は $\mathbb{Q}(i)$ である．i の $\mathbb{Q}$ 上の最小多項式は x^2+1 だから $\mathbb{Q}(i)$ は 2 次拡大である．

（別解）$x^4+4 = (x^2+2)^2 - 4x^2 = (x^2+2x+2)(x^2-2x+2)$ より $x^4+4=0$ の根は $x = \pm 1 \pm i$ (複号は任意）の 4 つであることがわかるから，$\mathbb{Q}$ 上の分解体は $\mathbb{Q}(i)$ である．

問題 3.2 $\alpha = \sqrt{2}+i$ とおく．$\alpha \in \mathbb{Q}(\sqrt{2}, i)$ より $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}, i)$ が成立する．一方，

$$\frac{1}{\alpha} = \frac{1}{\sqrt{2}+i} = \frac{\sqrt{2}-i}{3}$$

であるから，$\frac{1}{2}(\alpha + 3\alpha^{-1}) = \sqrt{2}$ と $\frac{1}{2}(\alpha - 3\alpha^{-1}) = i$ は $\mathbb{Q}(\alpha)$ に属する．よって $\mathbb{Q}(\sqrt{2}, i) \subset \mathbb{Q}(\alpha)$ である．以上により $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\alpha)$ が示された．例 1.7 により $\mathbb{Q}(\sqrt{2}, i)$ は $\mathbb{Q}$ の 4 次拡大である．

次に $\alpha = \sqrt{2}+i$ の最小多項式を求める．$(\alpha - \sqrt{2})^2 = i^2 = -1$ より $\alpha^2 + 3 = 2\sqrt{2}\alpha$. 両辺を 2 乗して整理すると $\alpha^4 - 2\alpha^2 + 9 = 0$. 従って $f(x) = x^4 - 2x^2 + 9$ は $f(\alpha) = 0$ を満たし，一方，α の最小多項式の次数は $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ だから，$f(x)$ が α の最小多項式である．

問題 6.1 $\omega = \dfrac{-1+\sqrt{3}i}{2}$ とおくと $f(x) := x^3 - 3 = (x - \sqrt[3]{3})(x - \sqrt[3]{3}\omega)(x - \sqrt[3]{3}\omega^2)$ であるから，$x^3 - 3$ の $\mathbb{Q}$ 上の分解体は $L = \mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{3}\omega, \sqrt[3]{3}\omega^2) = \mathbb{Q}(\sqrt[3]{3}, \omega) = \mathbb{Q}(\sqrt[3]{3}, \sqrt{3}i)$ である．$f(\pm 1) \neq 0$, $f(\pm 3) \neq 0$ より（または Eisenstein の判定法より）$f(x)$ は $\mathbb{Q}$ 上既約だから $f(x)$ は $\sqrt[3]{3}$ の $\mathbb{Q}$ 上の最小多項式である．従って $[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3$ である．一方，$\mathbb{Q}(\sqrt[3]{3}) \subset \mathbb{R}$ より $\sqrt{3}i \notin \mathbb{Q}(\sqrt[3]{3})$ であるから $\sqrt{3}i$ の $\mathbb{Q}(\sqrt[3]{3})$ 上の最小多項式は x^2+3 である．以上により

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{3})]\,[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 2 \cdot 3 = 6$$

であるから $G := \mathrm{Gal}(L/\mathbb{Q})$ の位数は 6 である．一方，G は $f(x)$ の根の集合 $A = \{\sqrt[3]{3}, \sqrt[3]{3}\omega, \sqrt[3]{3}\omega^2\}$ への作用（置換）から決まるから G は A_3 の部分群とみなせるが，$|G| = |A_3| = 6$ であるから $G \cong A_3$ である．

問題 6.2 $L = \mathbb{Q}(\sqrt{2}i, \sqrt{3})$ は $f(x) = (x^2+2)(x^2-3)$ の $\mathbb{Q}$ 上の分解体であるから，ガロア群 $G = \mathrm{Gal}(L/\mathbb{Q})$ は $f(x)$ の根の集合 $A = \{\sqrt{2}i, -\sqrt{2}i, \sqrt{3}, -\sqrt{3}\}$ への作用から決まる．よって G は S_4 の部分群とみなせる．$\sqrt{2}i$ は実数でないから $\mathbb{Q}(\sqrt{3})$ には属さない．よって $\sqrt{2}i$ の $\mathbb{Q}(\sqrt{3})$ 上の最小多項式は x^2+2 であるから，

$$|G| = [L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{3})]\,[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

となる．$\sigma \in G$ とすると補題 6.1 より $\sigma(\sqrt{2}i) = \pm\sqrt{2}i$, $\sigma(\sqrt{3}) = \pm\sqrt{3}$ でなければならない．従って A の可能な置換は高々4 個であるが，$|G| = 4$ であるから，G はこの 4 個の置換に対応する元からなる．A の元を順に $1, 2, 3, 4$ とみなせば，

$$G = \{\mathrm{id},\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\}$$

である．これはアーベル群であり $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})$ に同型である．

問題 6.3 (1) $\alpha^4+1=0$ と $(-1)^4=i^4=(-i)^4=1$ より, $\alpha, i\alpha, -\alpha, -i\alpha$ はすべて x^4+1 の根である．x^4+1 は 4 次式だから根は高々4 個であり，これらがすべての根である．従って $x^4+1=(x-\alpha)(x-i\alpha)(x+\alpha)(x+i\alpha)$ と分解される．$i=\alpha^2$ より，x^4+1 の $\mathbb{Q}$ 上の分解体 L は

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

である．

(2) 問題 2.2 により x^4+1 は $\mathbb{Q}$ 上既約であるから α の $\mathbb{Q}$ 上の最小多項式である．よって $[L:\mathbb{Q}]=[\mathbb{Q}(\alpha):\mathbb{Q}]=4$.

(3) $i=\alpha^2$ より

$$\begin{aligned}
\sigma_2(i\alpha)&=\sigma_2(\alpha^3)=\sigma_2(\alpha)^3=(i\alpha)^3=-i\alpha^3=-ii\alpha=\alpha,\\
\sigma_2(-\alpha)&=-\sigma_2(\alpha)=-i\alpha, \qquad \sigma_2(-i\alpha)=-\sigma_2(i\alpha)=-\alpha,\\
\sigma_3(i\alpha)&=\sigma_3(\alpha^3)=\sigma_3(\alpha)^3=(-\alpha)^3=-\alpha^3=-i\alpha,\\
\sigma_3(-\alpha)&=-\sigma_3(\alpha)=\alpha, \qquad \sigma_3(-i\alpha)=-\sigma_3(i\alpha)=i\alpha,\\
\sigma_4(i\alpha)&=\sigma_4(\alpha^3)=\sigma_4(\alpha)^3=(-i\alpha)^3=i\alpha^3=ii\alpha=-\alpha,\\
\sigma_4(-\alpha)&=-\sigma_4(\alpha)=i\alpha, \qquad \sigma_4(-i\alpha)=-\sigma_4(i\alpha)=\alpha
\end{aligned}$$

となるから，$\alpha, i\alpha, -\alpha, -i\alpha$ を順に $1,2,3,4$ として G を A_4 の部分群とみなすと，

$$\sigma_1=\mathrm{id}, \quad \sigma_2=(1\ 2)(3\ 4), \quad \sigma_3=(1\ 3)(2\ 4), \quad \sigma_4=(1\ 4)(2\ 3),$$

となる．

(4) G は (3) で求めた 4 つの置換からなる G の部分群である．σ_2, σ_3, σ_4 は位数 2 であり，

$$\sigma_2\sigma_3=\sigma_3\sigma_2=\sigma_4, \quad \sigma_2\sigma_4=\sigma_4\sigma_2=\sigma_3, \quad \sigma_3\sigma_4=\sigma_4\sigma_3=\sigma_2$$

が成立することがわかるので $G\cong(\mathbb{Z}/2\mathbb{Z})\oplus(\mathbb{Z}/2\mathbb{Z})$ である．たとえば $\sigma_2\leftrightarrow(\overline{1},\overline{0})$, $\sigma_3\leftrightarrow(\overline{0},\overline{1})$ とすると $\sigma_4=\sigma_2\sigma_3\leftrightarrow(\overline{1},\overline{1})$ となる．

(別解) $i=\alpha^2$ と $\alpha+(-i\alpha)=\dfrac{1+i}{\sqrt{2}}+\dfrac{1-i}{\sqrt{2}}=\sqrt{2}$, $\alpha+i\alpha=\dfrac{1+i}{\sqrt{2}}+\dfrac{-1+i}{\sqrt{2}}=\sqrt{2}i$ より $\sqrt{2}$ と $i=\sqrt{2}i/\sqrt{2}$ は $\mathbb{Q}(\alpha)$ に属する．逆に α は $\sqrt{2}$ と i で表せるから $\mathbb{Q}(\sqrt{2},i)$ に属する．従って $L=\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2},i)$ は $g(x)=(x^2-2)(x^2+1)$ の $\mathbb{Q}$ 上の分解体ともみなせ，

$$|G|=[L:\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},i),\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2\cdot 2=4$$

となることがわかる．$\sigma\in G$ に対して $\sigma(\sqrt{2})=\pm\sqrt{2}$, $\sigma(i)=\pm i$ であるから，$B=\{\sqrt{2},-\sqrt{2},i,-i\}=\{1,2,3,4\}$ みなすと，$\sigma|_B$ は id, $(1\ 2)$, $(3\ 4)$, $(1\ 2)(3\ 4)$ の 4 つのどれかであるが，$|G|=4$ よりこれらが G の引き起こす B の置換のすべてである．従って G は S_4 の部分群

$$\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

に同型である．さらにこれは加法群 $(\mathbb{Z}/2\mathbb{Z})\oplus(\mathbb{Z}/2\mathbb{Z})$ に同型である．

問題 7.1 問題 6.2 より $G = \mathrm{Gal}(L/\mathbb{Q})$ は，$f(x) = (x^2+2)(x^2-3)$ の根の集合 $A = \{\sqrt{2}i, -\sqrt{2}i, \sqrt{3}, -\sqrt{3}\}$ の置換（A の元をこの順に $1,2,3,4$ とする）で表現すると，

$$G = \{\mathrm{id},\ (1\ 2),\ (3\ 4),\ (1\ 2)(3\ 4)\}$$

であった．$(1\ 2)$ に対応する G の元を σ，$(3\ 4)$ に対応する G の元を τ とする．$\sigma, \tau, \sigma\tau$ の位数が 2 であることから，G の $\{\mathrm{id}\}$ と G 以外の（すなわち自明でない）部分群は位数 2 であり

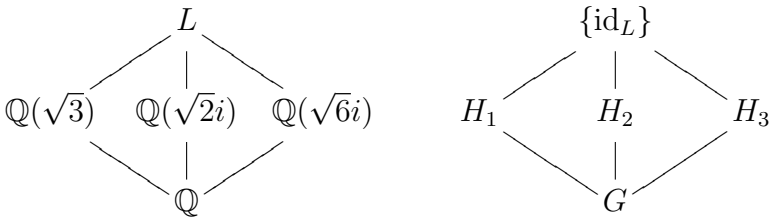
$$H_1 = \langle\sigma\rangle = \{\mathrm{id}, \sigma\}, \qquad H_2 = \langle\tau\rangle = \{\mathrm{id}, \tau\}, \quad H_3 = \langle\sigma\tau\rangle = \{\mathrm{id}, \sigma\tau\}$$

の 3 つである．G はアーベル群だから，部分群はすべて正規部分群である．

$\sigma(\sqrt{3}) = \sqrt{3}$ より $L^{H_1} \supset \mathbb{Q}(\sqrt{3})$ であるが，定理 7.2 の (2) より $[L^{H_1} : \mathbb{Q}] = |G|/|H_1| = 2$ が成立し，一方 $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ であるから $L^{H_1} = \mathbb{Q}(\sqrt{3})$ を得る．

同様にして，$\tau(\sqrt{2}i) = \sqrt{2}i$ より $L^{H_2} = \mathbb{Q}(\sqrt{2}i)$, $(\sigma\tau)(\sqrt{6}i) = \sqrt{6}i$ より $L^{H_3} = \mathbb{Q}(\sqrt{6}i)$ であることがわかる．

また，$L^{\{\mathrm{id}\}} = L$, $L^G = \mathbb{Q}$ である．H_1, H_2, H_3 の間には包含関係はないので，これらの中間体の包含関係は下のようになる．



（別解）$\sqrt{2}i \notin \mathbb{Q}(\sqrt{3})$ より $\sqrt{2}i$ の $\mathbb{Q}(\sqrt{3})$ 上の最小多項式は x^2+2 であるから，1 と $\sqrt{2}i$ は L の $\mathbb{Q}(\sqrt{3})$ 上の基底である．また 1 と $\sqrt{3}$ は $\mathbb{Q}(\sqrt{3})$ の $\mathbb{Q}$ 上の基底であるから，$1, \sqrt{2}i, \sqrt{3}, \sqrt{6}i$ は $L = \mathbb{Q}(\sqrt{2}i, \sqrt{3})$ の $\mathbb{Q}$ 上の基底である． $c_1, c_2, c_3, c_4 \in \mathbb{Q}$ とすると，

$$\begin{aligned}
\sigma(c_1 + c_2\sqrt{2}i + c_3\sqrt{3} + c_4\sqrt{6}i) &= c_1 - c_2\sqrt{2}i + c_3\sqrt{3} - c_4\sqrt{6}i,\\
\tau(c_1 + c_2\sqrt{2}i + c_3\sqrt{3} + c_4\sqrt{6}i) &= c_1 + c_2\sqrt{2}i - c_3\sqrt{3} - c_4\sqrt{6}i,\\
\sigma\tau(c_1 + c_2\sqrt{2}i + c_3\sqrt{3} + c_4\sqrt{6}i) &= c_1 - c_2\sqrt{2}i - c_3\sqrt{3} + c_4\sqrt{6}i
\end{aligned}$$

より

$$\begin{aligned}
L^{H_1} &= \{c_1 + c_2\sqrt{2}i + c_3\sqrt{3} + c_4\sqrt{6}i \mid c_2 = c_4 = 0\} = \mathbb{Q} + \mathbb{Q}\sqrt{3} = \mathbb{Q}(\sqrt{3}),\\
L^{H_2} &= \{c_1 + c_2\sqrt{2}i + c_3\sqrt{3} + c_4\sqrt{6}i \mid c_3 = c_4 = 0\} = \mathbb{Q} + \mathbb{Q}\sqrt{2}i = \mathbb{Q}(\sqrt{2}i),\\
L^{H_3} &= \{c_1 + c_2\sqrt{2}i + c_3\sqrt{3} + c_4\sqrt{6}i \mid c_2 = c_3 = 0\} = \mathbb{Q} + \mathbb{Q}\sqrt{6}i = \mathbb{Q}(\sqrt{6}i)
\end{aligned}$$

問題 7.2 $\omega = \dfrac{-1+\sqrt{3}i}{2}$, $\alpha = \sqrt[3]{3}$ とおくと G は x^3-3 の根の集合 $A = \{\alpha, \alpha\omega, \alpha\omega^2\}$（$A$ の元を $1,2,3$ とする）の置換として S_3 と同型である．$x^2+x+1 = (x-\omega)(x-\omega^2)$ より G の元 σ に対して $\sigma(\omega)$ は ω または ω^2 である．また $\sigma(\alpha)$ は α, $\alpha\omega$, $\alpha\omega^2$ のいずれ

かである．σ は $\sigma(\omega)$ と $\sigma(\alpha)$ で定まるから，高々6 通りであるが，$|G| = |S_3| = 6$ より，この 6 通りの可能性がすべて G の元として実現される．従って特に

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

を満たす $\sigma, \tau \in G$ が存在して

$$G = \{\mathrm{id}_L, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$$

となる．これらの元の ω と A への作用は下の表のようになる．

	id_L	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
ω	ω	ω	ω	ω^2	ω^2	ω^2
α	α	$\alpha\omega$	$\alpha\omega^2$	α	$\alpha\omega$	$\alpha\omega^2$
$\alpha\omega$	$\alpha\omega$	$\alpha\omega^2$	α	$\alpha\omega^2$	α	$\alpha\omega$
$\alpha\omega^2$	$\alpha\omega^2$	α	$\alpha\omega$	$\alpha\omega$	$\alpha\omega^2$	α

この表から，G の元を A への作用によって S_3 の元と同一視すると，

$$\sigma = (1\ 2\ 3), \qquad \sigma^2 = (1\ 3\ 2), \qquad \tau = (2\ 3), \qquad \sigma\tau = (1\ 2), \qquad \sigma^2\tau = (1\ 3)$$

となることがわかる．

S_3 の部分群は S_3 と $\{\mathrm{id}\}$ 以外は位数が 2 または 3 だから巡回群となり，

$$H_1 = \langle\tau\rangle = \{\mathrm{id}_L, \tau\}, \quad H_2 = \langle\sigma\tau\rangle = \{\mathrm{id}_L, \sigma\tau\}, \quad H_3 = \langle\sigma^2\tau\rangle = \{\mathrm{id}_L, \sigma^2\tau\},$$
$$A_3 = \langle\sigma\rangle = \{\mathrm{id}_L, \sigma, \sigma^2\}$$

の 4 つである．このうち A_3 のみが正規部分群である（S_3 の 3 次の巡回置換は σ と σ^2 のみだから）．各々の部分群に対応する固定体は

$$L^{H_1} = \mathbb{Q}(\alpha), \quad L^{H_2} = \mathbb{Q}(\alpha\omega^2), \quad L^{H_3} = \mathbb{Q}(\alpha\omega), \quad L^{A_3} = \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$$

であることを示す．まず，Eisenstein の判定法により $f(x) = x^3 - 3$ は $\mathbb{Q}$ 上既約であり，$f(x) = (x-\alpha)(x-\alpha\omega)(x-\alpha\omega^2)$ であるから，$f(x)$ は $\alpha, \alpha\omega, \alpha\omega^2$ の $\mathbb{Q}$ 上の最小多項式である．従って

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha\omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha\omega^2) : \mathbb{Q}] = 3$$

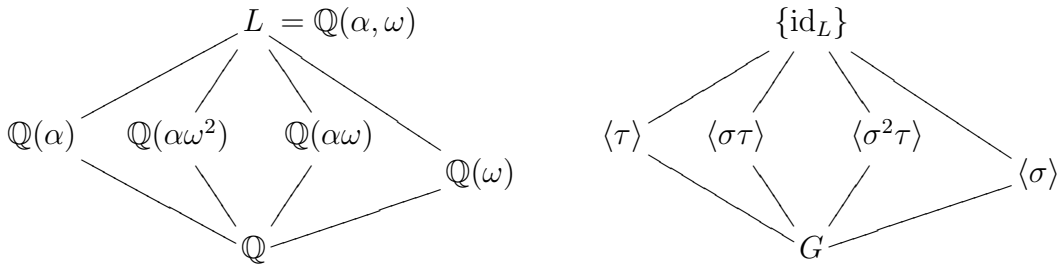
である．H_1 については，$\tau(\alpha) = \alpha$ より $\mathbb{Q}(\alpha) \subset L^{H_1}$ であり，定理 7.2 より

$$[L^{H_1} : \mathbb{Q}] = \frac{|G|}{|H_1|} = 3 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

であるから，$L^{H_1} = \mathbb{Q}(\alpha)$ が成立する．同様にして $L^{H_2} = \mathbb{Q}(\alpha\omega^2)$ と $L^{H_3} = \mathbb{Q}(\alpha\omega)$ が成立することが示される．

また，A_3 については，$\sigma(\omega) = \omega$ より $\mathbb{Q}(\omega) \subset L^{A_3}$ であるが，$[\mathbb{Q}[\omega] : Q] = 2$（$\omega$ の $\mathbb{Q}$ 上の最小多項式が $x^2 + x + 1$ であるから）と $[L^{A_3}] = |G|/|A_3| = 2$ より $L^{A_3} = \mathbb{Q}(\omega)$ が

成立する．H_1, H_2, H_3, A_3 の間に包含関係はないので，中間体の包含関係は下のようになる．



問題 7.3 $\alpha=\dfrac{1+i}{\sqrt{2}}$ とおくと，x^4+1 の根の集合は $A=\{\alpha,i\alpha,-\alpha,-i\alpha\}$ である．A の元をこの順に $1,2,3,4$ として G の元を S_4 の元と同一視すると，G は

$$\sigma_1=\mathrm{id},\quad \sigma_2=(1\ 2)(3\ 4),\quad \sigma_3=(1\ 3)(2\ 4),\quad \sigma_4=(1\ 4)(2\ 3)$$

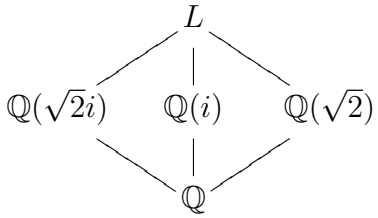
の 4 個の元からなる（問題 6.3 の解答より）．$\sigma_2,\sigma_3,\sigma_4$ の位数は 2 であるから，$\{\mathrm{id}\}$ と G 以外の G の部分群は

$$H_2=\langle\sigma_2\rangle=\{\mathrm{id},\sigma_2\},\quad H_3=\langle\sigma_3\rangle=\{\mathrm{id},\sigma_3\},\quad H_4=\langle\sigma_4\rangle=\{\mathrm{id},\sigma_4\}$$

の 3 つである．$\sigma_2(\alpha+i\alpha)=\sigma_2(\alpha)+\sigma_2(i\alpha)=i\alpha+\alpha$ より σ_2 は $(1+i)\alpha=\sqrt{2}i$ を固定する．よって $L^{H_2}\supset\mathbb{Q}(\sqrt{2}i)$ であるが，$[L^{H_2}:\mathbb{Q}]=|G|/|H_2|=2$ かつ $[\mathbb{Q}(\sqrt{2}i):\mathbb{Q}]=2$（$\sqrt{2}i$ の $\mathbb{Q}$ 上の最小多項式が x^2+2 だから）より $L^{H_2}=\mathbb{Q}(\sqrt{2}i)$ が成立する．

$\sigma_3(\alpha^2)=\sigma_3(\alpha)^2=(-\alpha)^2=\alpha^2$ より σ_3 は $\alpha_2=i$ を固定する．これから上と同様に拡大次数を比較して $L^{H_3}=\mathbb{Q}(i)$ を得る．

$\sigma_4(\alpha-i\alpha)=\sigma_4(\alpha)+\sigma_4(-i\alpha)=-i\alpha+\alpha$ より σ_4 は $(1-i)\alpha=\sqrt{2}$ を固定する．これから拡大次数を比較して $L^{H_4}=\mathbb{Q}(\sqrt{2})$ を得る．H_2, H_3, H_4 の間に包含関係はないから中間体の包含関係は下のようになる．



（別解 1）問題 2.2 より x^4+1 は $\mathbb{Q}$ 上既約であるから定理 1.1 より，L の $\mathbb{Q}$ 上のベクトル空間としての基底として，1, α ,$\alpha^2=i$, $\alpha^3=i\alpha$ がとれる．L の任意の元 β は $c_1,c_2,c_3,c_4\in\mathbb{Q}$ によって

$$\beta=c_1+c_2\alpha+c_3i+c_4i\alpha$$

と表され，$i=\alpha^2$ より

$$\sigma_2(i)=\sigma_2(\alpha)^2=(i\alpha)^2=-i,\quad \sigma_3(i)=(-\alpha)^2=\alpha^2=i,\quad \sigma_4(i)=(-i\alpha)^2=-\alpha^2=-i$$

であることに注意すると，

$$\sigma_2(\beta) = c_1 + c_2 i\alpha - c_3 i + c_4\alpha,$$
$$\sigma_3(\beta) = c_1 - c_2\alpha + c_3 i - c_4 i\alpha,$$
$$\sigma_4(\beta) = c_1 - c_2 i\alpha - c_3 i - c_4\alpha$$

を得る．これから

$$\sigma_2(\beta) = \beta \quad \Leftrightarrow \quad c_2 = c_4,\, c_3 = 0 \quad \Leftrightarrow \quad \beta = c_1 + c_2(1+i)\alpha = c_1 + c_2\sqrt{2}i$$

が成立するから $L^{H_2} = \mathbb{Q}(\sqrt{2}i)$ である．

$$\sigma_3(\beta) = \beta \quad \Leftrightarrow \quad c_2 = 0,\, c_4 = 0 \quad \Leftrightarrow \quad \beta = c_1 + c_3 i$$

より $L^{H_3} = \mathbb{Q}(i)$,

$$\sigma_4(\beta) = \beta \quad \Leftrightarrow \quad -c_2 = c_4,\, c_3 = 0 \quad \Leftrightarrow \quad \beta = c_1 - c_2(1-i)\alpha = c_1 - c_2\sqrt{2}$$

より $L^{H_4} = \mathbb{Q}(\sqrt{2})$ である．

（別解 2）$i = \alpha^2$, $\sqrt{2} = (1-i)\alpha = (1-\alpha^2)\alpha$ より $L = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$ であることがわかる．$i \notin \mathbb{Q}(\sqrt{2})$ より i の $\mathbb{Q}(\sqrt{2})$ 上の最小多項式は x^2+1 であるから，1 と i が L の $\mathbb{Q}(\sqrt{2})$ 上の基底である．$\mathbb{Q}(\sqrt{2})$ の $\mathbb{Q}$ 上の基底は 1 と $\sqrt{2}$ だから，$1, \sqrt{2}, i, \sqrt{2}i$ は L の $\mathbb{Q}$ 上の基底である．

$$\sigma_2(\sqrt{2}) = \sigma_2((1-i)\alpha) = (1+i)i\alpha = -\sqrt{2}, \qquad \sigma_3(\sqrt{2}) = (1-i)(-\alpha) = -\sqrt{2}$$
$$\sigma_4(\sqrt{2}) = (1+i)(-i\alpha) = \sqrt{2}$$

と $\sigma_2(i) = -i$, $\sigma_3(i) = i$, $\sigma_4(i) = -i$ より $L^{H_2} = \mathbb{Q}(\sqrt{2}i)$, $L^{H_3} = \mathbb{Q}(i)$, $L^{H_4} = \mathbb{Q}(\sqrt{2})$ であることがわかる (L の元の基底による表示または拡大次数の比較により）．

問題 7.4 (1) $f(x) = x^4 - 2$, $\alpha = \sqrt[4]{2}$ とおくと，1 の原始 4 乗根として $\exp\left(\frac{\pi i}{2}\right) = i$ がとれるから，$\mathbb{C}[x]$ において

$$x^4 - 2 = (x-\alpha)(x-i\alpha)(x-i^2\alpha)(x-i^3\alpha) = (x-\alpha)(x-i\alpha)(x+\alpha)(x+i\alpha)$$

と既約分解される．従って $L = \mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\sqrt[4]{2}, i)$ である．($i = i\alpha/\alpha \in L$ より.)

(2) Eisenstein の判定法 ($p = 2$ とする) により $x^4 - 2$ は $\mathbb{Q}$ 上既約であるから $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ である．一方 $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ と $i \notin \mathbb{R}$ より i の $\mathbb{Q}(\sqrt[4]{2})$ 上の最小多項式は x^2+1 であるから $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. 従って

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 4 = 8$$

(3) G の元 σ は α を $x^4 - 2$ の根，すなわち $\alpha, i\alpha, -\alpha, -i\alpha$ のいずれかにうつし，i を $i, -i$ のいずれかにうつすから，全部で 8 通りの可能性があるが，(2) により $|G| = 8$ で

あるから，これらがすべて G の元で実現される．よって 題意を満たす $\sigma, \tau \in G$ が存在する．

(4) (3) から

$$G = \langle\sigma\rangle \cup \tau\langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$$

であることがわかる．($\langle\sigma\rangle$ によるコセット分解から，またはこれらが (3) で考察した 8 通りの可能性に対応することから.）あるいは

$$G = \langle\sigma\rangle \cup \langle\sigma\rangle\tau = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

としてもよい．α, $i\alpha$, $-\alpha$, $-i\alpha$ を順に $1, 2, 3, 4$ として G の元を S_4 の元とみなす.

$$\sigma(\alpha) = i\alpha, \quad \sigma(i\alpha) = \sigma(i)\sigma(\alpha) = ii\alpha = -\alpha, \quad \sigma(-\alpha) = -i\alpha, \quad \sigma(-i\alpha) = \alpha$$

より $\sigma = (1\ 2\ 3\ 4)$ である．また

$$\tau(\alpha) = \alpha, \quad \tau(i\alpha) = \tau(i)\tau(\alpha) = -i\alpha, \quad \tau(-\alpha) = -\alpha, \quad \sigma(-i\alpha) = i\alpha$$

より $\tau = (2\ 4)$ である．G の他の元を置換で表すと

$$\sigma^2 = (1\ 3)(2\ 4), \quad \sigma^3 = (1\ 4\ 3\ 2), \quad \tau\sigma = (1\ 4)(2\ 3), \quad \tau\sigma^2 = (1\ 3), \quad \tau\sigma^3 = (1\ 2)(3\ 4)$$

(5) G の自明でない部分群の位数は 2 または 4 である．位数 2 の部分群は位数 2 の元で生成されるから,

$$H_1 = \langle\tau\rangle, \quad H_2 = \langle\tau\sigma\rangle, \quad H_3 = \langle\tau\sigma^2\rangle, \quad H_4 = \langle\tau\sigma^3\rangle, \quad H_5 = \langle\sigma^2\rangle$$

の 5 個である．ここで置換の計算から

$$\sigma\tau = \tau\sigma^3, \quad \sigma^2\tau = \tau\sigma^2, \quad \sigma^3\tau = \tau\sigma$$

となることがわかるので,

$$\sigma\tau\sigma^{-1} = \sigma\tau\sigma^3 = (\tau\sigma^3)\sigma^3 = \tau\sigma^2, \qquad \sigma(\tau\sigma)\sigma^{-1} = \sigma\tau = \tau\sigma^3,$$
$$\sigma(\tau\sigma^2)\sigma^{-1} = \sigma\tau\sigma = \tau, \qquad \sigma(\tau\sigma^3)\sigma^{-1} = \sigma\tau\sigma^2 = \tau\sigma$$

より H_1, H_2, H_3, H_4 は正規部分群ではない．一方，$k = 0, 1, 2, 3$ に対して

$$(\tau\sigma^k)\sigma^2(\tau\sigma^k)^{-1} = \tau\sigma^{k+2}\sigma^{-k}\tau = \tau\sigma^2\tau = \sigma^2$$

であるから，H_5 は正規部分群である．

次に位数 4 の部分群を求める．巡回群は $H_6 := \langle\sigma\rangle$ のみである．それ以外の位数 4 の部分群は位数 2 の 2 つの元で生成される．それらの可能な ${}_5C_2 = 10$ 個の組み合わせを試してみると

$$H_7 = \langle\tau, \sigma^2\rangle = \{\mathrm{id}, \tau, \sigma^2, \tau\sigma^2\}, \qquad H_8 = \langle\tau\sigma, \sigma^2\rangle = \{\mathrm{id}, \tau\sigma, \sigma^2, \tau\sigma^3\}$$

の 2 つがあることがわかる．位数 4 の部分群 H_6, H_7, H_8 はすべて正規部分群である．これは実際に確かめても良いが、一般に次の事実が成立することからもわかる．

• 有限群 G の指数 2 の部分群 H (すなわち $|G|/|H| = 2$) は正規部分群である．

証明）$G \setminus H$ の元 σ をとると左と右のコセット分解より $G = H \cup \sigma H = H \cup H\sigma$ を得るが，これは共に共通部分を持たない和集合なので $\sigma H = H\sigma = G \setminus H$ でなければならない．従って $\sigma H \sigma^{-1} = H$, すなわち H は正規部分群である．

(6) $\tau = (2\ 4)$ は α を固定するから $L^{H_1} \supset \mathbb{Q}(\alpha)$ であるが，$[L^{H_1} : \mathbb{Q}] = |G|/|H_1| = 4 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ より $L^{H_1} = \mathbb{Q}(\alpha)$ が成立する．

$\tau\sigma^2 = (1\ 4)(2\ 3)$ は α と $-i\alpha$ を交換するから，$(1-i)\alpha$ を固定する．$\beta = (1-i)\alpha$ とおくと $\beta^4 = -4\alpha^4 = -8$ より β は $g(x) = x^4 + 8$ の根である．$g(x)$ が $\mathbb{Q}$ 上既約であることを示そう．まず命題 2.2 により $g(x)$ は $\mathbb{Q}[x]$ において 1 次式の約元を持たないことがわかるから，もし $g(x)$ が $\mathbb{Q}$ 上既約でなければ 2 つの 2 次式の積に分解される．命題 2.2 により 2 つの 2 次式は整数係数として良い．従ってある整数 a, b, c, d が存在して

$$x^4 + 8 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd$$

が成立する．これから特に $a + c = ad + bc = 0$ となるが $c = -a$ を第 2 式に代入して　$b = d$ よって $bd = d^2 = 8$．8 は平方数ではないからこれは矛盾である．以上により $g(x)$ は $\mathbb{Q}$ 上既約であることが示された．よって $[\mathbb{Q}((1-i)\alpha) : \mathbb{Q}] = 4$ であるから $L^{H_2} = \mathbb{Q}((1-i)\alpha)$ が成立する．

同様にして $L^{H_4} = \mathbb{Q}((1+i)\alpha)$ であることがわかる．

$\tau\sigma^2 = (1\ 3)$ は $i\alpha$ を固定するから $L^{H_3} = \mathbb{Q}(i\alpha)$ である．

$\sigma(i) = i$ より σ^2 は i を固定する．また σ^2 は α と $-\alpha$ を固定するから $-\alpha^2 = -\sqrt{2}$ すなわち $\sqrt{2}$ を固定する．これと拡大次数を比較して $L^{H_5} = \mathbb{Q}(\sqrt{2}, i)$ を得る．

$\sigma(i) = i$ と拡大次数の比較から $L^{H_6} = \mathbb{Q}(i)$ を得る．

$L^{H_7} = L^{H_1} \cap L^{H_5} = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\sqrt{2}, i) \supset \mathbb{Q}(\sqrt{2})$ と拡大次数の比較から $L^{H_7} = \mathbb{Q}(\sqrt{2})$ がわかる．

$((1-i)\alpha)^2 = -2i\sqrt{2}$ より $L^{H_8} = L^{H_1} \cap L^{H_5} = \mathbb{Q}((1-i)\alpha) \cap \mathbb{Q}(\sqrt{2}, i) \supset \mathbb{Q}(\sqrt{2}i)$ が成立する．これと拡大次数の比較により $L^{H_8} = \mathbb{Q}(\sqrt{2}i)$ を得る．$L \supset \mathbb{Q}$ の中間体の包含関係は下のようになる．