4.7.3

(1) $\alpha^5 - 2 = 0$ で アイゼンシュタインの判定法より x^5-2 は $\mathbb{Q}$ 上既約

よって α の $\mathbb{Q}$ 上の最小多項式は $x^5 - 2$

(2) $\mathrm{ch}\,\mathbb{Q} = 0$ より $\mathbb{Q}(\alpha)/\mathbb{Q}$ は分離拡大なのでガロア閉包を考えれる

(1)より α の共役は $\alpha,\ \alpha\zeta_5,\ \alpha\zeta_5^2,\ \alpha\zeta_5^3,\ \alpha\zeta_5^4$ である

よって $L = \mathbb{Q}(\alpha, \zeta_5)$ となる。

ここで $L \supset \mathbb{Q}(\alpha)$, $L \supset \mathbb{Q}(\zeta_5)$ で $[\mathbb{Q}(\alpha):\mathbb{Q}] = 5$, $[\mathbb{Q}(\zeta_5):\mathbb{Q}] = 4$ より

$[L:\mathbb{Q}]$ は 20 の倍数である。

$\mathrm{Gal}(L/\mathbb{Q})$ の元は α, ζ_5 を共役なものへ移すし、L は $\mathbb{Q}$ 上 α, ζ_5 で生成されるので

高々 $5 \times 4 = 20$ 個 ですから $|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] \leqq 20$.

ゆえに $[L:\mathbb{Q}] = 20$ とわかる

☆ガロアの推進定理を使うと

☆ $\mathrm{Gal}(L/\mathbb{Q}(\alpha)) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ より

$[L:\mathbb{Q}(\alpha)] = [\mathbb{Q}(\zeta_5):\mathbb{Q}] = 4$ であるから

よって $[L:\mathbb{Q}] = [L:\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] = 20$.

ただし、適用条件の確認に注意。

(3) (2)の議論より 題意は示されている

教科書はガロアの推進定理を使っている所、$[L:\mathbb{Q}]=20$ の時点で $\sigma(\alpha)$, $\sigma(\zeta_5)$ の候補は高々20コしかないので そのすべての候補が実現するしかないということが言える。

(4)

$$\begin{tikzcd}[column sep=small] & L \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\zeta_5) \arrow[dr, dash] & & \mathbb{Q}(\alpha) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd} \quad \longleftrightarrow \quad \begin{tikzcd}[column sep=small] & \{1\} \arrow[dl, dash] \arrow[dr, dash] & \\ H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] \\ & \mathrm{Gal}(L/K) & \end{tikzcd}$$

ガロアの基本定理より 上のように $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\alpha)$ に対応する H_1, H_2 が存在する。

このとき $[L:\mathbb{Q}(\zeta_5)] = 5 = |H_1|$　$[L:\mathbb{Q}(\alpha)] = 4 = |H_2|$

$X = \{\alpha, \alpha\zeta_5, \alpha\zeta_5^2, \alpha\zeta_5^3, \alpha\zeta_5^4\}$ への $\mathrm{Gal}(L/K)$ による置換表現 ρ について、

L は X で $\mathbb{Q}$ 上生成されているので $\ker\rho = \{1\}$ となり ρ は単射準同型

よって $\mathrm{Gal}(L/K) \cong \mathrm{Im}\,\rho$ である

ここで、H_1 の元は $\mathbb{Q}(\zeta_5)$ の元を不変に保つような $\mathrm{Gal}(L/K)$ の元なので

$\sigma \in \mathrm{Gal}(L/K)$, $\sigma(\alpha) = \zeta_5\alpha$, $\sigma(\zeta_5) = \zeta_5$ とおくと

$|H_1| = 5$ より $H_1 = \langle\sigma\rangle$ とかける。

同様にして H_2 の元は $\mathbb{Q}(\alpha)$ の元を不変に保つような $\mathrm{Gal}(L/K)$ の元なので

$\tau \in \mathrm{Gal}(L/K)$, $\tau(\alpha) = \alpha$, $\tau(\zeta_5) = \zeta_5^2$ とおくと　$H_2 = \langle\tau\rangle$ となる。

ここの部分構造に注目していて面白い

ここで、$\rho(H_1) = \langle(12345)\rangle$　$\rho(H_2) = \langle(2354)\rangle$

$\mathrm{Gal}(L/K) \supset H_1, H_2$ より　$\mathrm{Im}\,\rho \supset \rho(H_1), \rho(H_2)$ である。

したがって $\mathrm{Gal}(L/K) \cong \langle(12345), (2354)\rangle$

(別) $|\mathrm{Im}\,\rho| = 20$ で シローの定理から $H_1 \lhd G$ となるので とって H_1H_2 は部分群

$H_1H_2 \supset H_1, H_2$ より H_1H_2 は位数が20の倍数

よって $\mathrm{Im}\,\rho = H_1H_2$

どうして $\mathrm{Im}\,\rho = \rho(H_1), \rho(H_2)$ が ここまで言えるのかというと、$\rho(H_1) \ni h$, $\rho(H_2) \ni k$ として

$h^i k^j = h^{i'} k^{j'}$ とおくと　$h^{i-i'} k^{j-j'} = 1$

$h^{i-i'} \neq 1$, $k^{j-j'} \neq 1$ とすると　$\underbrace{h^{i-i'}}_{\text{位数5}} = k^{(j'-j)}$ 位数4 となり矛盾。

$(i, j = 0 \sim 4)$

よって $h^{i-i'} = 1$ or $k^{j-j'} = 1$ であるが、これは $i = i'$, $j = j'$ を意味する

このことより $(12345)^i(2354)^j$ の形で $\mathrm{Im}\,\rho$ の元は表されることがわかる。