$\boxed{4.16.2}$ (1) $\alpha(t) \in \mathbb{F}_2[t]$ が与式の根だとすると

最初に $\mathbb{F}_2[t]$ は一意分解
$\mathbb{F}_2(t)$ はその商体
であることは
把握しておく

$\alpha(t)$ について $4 \deg \alpha(t) = 0$ が成り立つので

$\deg \alpha(t) < 1$ より $\alpha(t) = 1, 0$ であるが代入して確かめると

$1, 0$ は根ではない。よって与式は $\mathbb{F}_2(t)$ 上に根を持たない。

よって与式は既約でないとすると $\mathbb{F}_2[t]$ の2次式に分解されるときである。

$$(与式) = (x^2 + ax + b)(x^2 + cx + d) \quad a, b, c, d \in \mathbb{F}_2[t] \text{ とおくと}$$

$$(右辺) = x^4 + ax^3 + bx^2 + cx^3 + acx^2 + bcx + dx^2 + dax + bd$$
$$= x^4 + (a+c)x^3 + (b+d+ac)x^2 + (bc+da)x + bd$$

ゆえに
$$\begin{cases} a + c = 0 & \cdots ① \\ b + d + ac = t + 1 & \cdots ② \\ bc + da = t & \cdots ③ \\ bd = t^3 & \cdots ④ \end{cases}$$

① より $a = -c$

③に代入して $c(b-d) = t$.

よって $0 \leq \deg c \leq 1$ である

$\deg c = 0$ のとき $c = 1$ である

$\deg c = 1$ のとき $c = t, t+1$ である

このとき ①〜④ は $\begin{cases} a = 1 \\ b + d = t \\ bd = t^3 \end{cases}$ となる.

$c = t$ のとき $a = t$ なので ②, ③ は

$b + d = t^2 + t + 1$, $b + d = 1$ となり矛盾

$c = t+1$ のときは ③ より

$(t+1)(b+d) = t$ となり矛盾

$bd = t^3$ より $\deg b \neq \deg d$ であるが

$b + d = t$ より これは矛盾 (最高次の係数を比べる)

これらより 与式は $\mathbb{F}_2(t)$ 上既約であることが分かる.

また 与式の微分は $t$ で $\neq 0$ なので 与式は分離多項式

$b_1 = a_2 = t + 1 \qquad b_2 = a_1 a_3 = 0$

$b_3 = a_4 a_1^2 + a_3^2 = t^2$

よって $g(y) = y^3 + (t+1)y^2 + t^2$
$= (y + t)(y^2 + y + t)$

また $c_1 = b_1 b_2 + b_3 \qquad c_2 = b_2^3 + b_3^2 + b_1^3 b_3$
$= t^2$
$$= t^4 + (t+1)^3 t^2$$
$$= t^2(t^2 + t^3 + t^2 + t + 1)$$
$$= t^2(t^3 + t + 1)$$

また $h(z) = z^2 + t^2 z + t^2(t^3 + t + 1)$ これより $h(z)$ は既約.

$a_1 = 0, \quad d_1 = 1 \in (K(t_1)^\times)^2$

$c_1 = t, \quad a_4 c_1^{-2} = t^3 \cdot t^{-2} = t$ で

$d_2 d_1^{-2} = t$ より $\quad a_4 c_1^{-2} \in \{\alpha d_2 d_1^{-2} + \beta^2 + \beta \mid \alpha \in \mathbb{F}_2, \beta \in K\}$

したがって

$$\mathrm{Gal}(L/K) \cong \mathbb{Z}/4\mathbb{Z}$$

(2) (1)と同様に根 $\alpha(t) \in \mathbb{F}(t)$ をもつとして次数を調べると $\deg \alpha(t) < 1$

よって $\alpha(t) = 1, 0$ であるが、どちらも根ではない。

また、定数項が $t^3$ から $t^5$ へ変わっただけなので (1)と同様にして

与式は $\mathbb{F}_2(t)$ 上既約かつ分離的多項式であることがわかる。

$$b_1 = t+1, \quad b_2 = 0, \quad b_3 = t^2$$

(1)と同様で $g(y) = (y+t)(y^2+y+t+1)$

〃 $h(z) = z^2 + t^2 z + t + t^2(t+1)$ で $h$ は既約

$a_4 \, r_2^{-2} = t^5 \cdot t^{-2} = t^3$ で

$a_4 r_2^{-2} \in \{\alpha d_2 d_1^2 + \beta^2 + \beta \mid \alpha \in \mathbb{F}_2, \beta \in K\}$ とすると

$t^3 = \alpha t + \beta^2 + \beta$ を満たす $\alpha \in \mathbb{F}_2$, $\beta \in K$ が存在する

$\alpha \in \mathbb{F}_2$ より $\alpha$ の次数は1より小さいが両辺の次数を比較すると矛盾

よって $a_4 r_2^{-2} \notin \{\alpha d_2 d_1^2 + \beta^2 + \beta \mid \alpha \in \mathbb{F}_2, \beta \in K\}$ であるので

$$\mathrm{Gal}(L/K) \cong D_4$$

(3). (1), (2)と同様にして $\mathbb{F}_2(t)$ 上に与式は根をもたない。

(1)と同様に $\mathbb{F}_2[t]$ の2次式に分解されるとすると、

$$\begin{cases} a+c = 0 & \cdots ① \\ b+d+ac = t^4+t+1 & \cdots ② \\ ad+bc = t^2+t & \cdots ③ \\ bd = t^6+t^3+t^2 & \cdots ④ \end{cases}$$

④より $bd = t^2(t^4+t+1)$.

例1.12, 10より $t^4+t+1$ は既約より素元である。

よって $b, d$ のどちらか一方のみ次数は4以上

ここで対称性より $\deg b \geq 4$ とする

このとき $\deg d \leq 2$ である よって ②の次数比較から $\deg ac = 4$

①で $a=c$ であるので $\deg a = \deg c = 2$ となる必要がある

しかし、③から $a(b+d) = t^2+t$ の次数比較に矛盾

したがって 与式は $\mathbb{F}_2[t]$ 上既約, また(1), (2)と同様に分離的多項式

$$b_1 = t^4+t+1, \quad b_2 = 0, \quad b_3 = (t^2+t)^2 = t^4+t^2$$

よって

$$\begin{aligned} g(y) &= y^3 + (t^4+t+1)y^2 + t^4+t^2 \\ &= y^3 + (t^2+t+1)y^2 + t^4+t^2 \\ &= (y+t)(y^2+(t^2+1)y+t^3+t) \\ &= (y+t)(y+t+1)(y+t^2+t) \end{aligned}$$

したがって $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

(4) 与式は $\mathbb{F}_2(t)$ 上に根を持たない。

2次式の積に分解されるとすると

例1.2.10 (P72)

$$\begin{cases} a+c = 1 & \cdots ① \\ b+d+ac = 0 & \cdots ② \\ bc+da = (t^2+t+1) & \cdots ③ \\ bd = t(t+1)(t^2+t+1) & \cdots ④ \end{cases}$$

④で $t^2+t+1$ は素元なので $b, d$ のどちらか一方のみ $(t^2+t+1)$ の倍元。

対称性より $b = (t^2+t+1)b'$ とおくとすると

また③より $a(b+d) = (t^2+t+1)$ よって $a$ を $a = (t^2+t+1)a'$ とおけば

このとき①は $a'(b+d) = 1$ よって $a' = 1$ より

$a = t^2+t+1$, また $d = (t^2+t+1)ca' + (t^2+t+1)b'$

$= (t^2+t+1)(ca'+b')$

$d = 0$ とすると④より矛盾で、$d \neq 0$ としても $d$ が $t^2+t+1$ の倍元になるのでこれも④より矛盾

したがって与式は分離性既約多項式である。

$b_1 = a_2 = 0$, $b_2 = a_1 a_3 = t^2+t+1$,

$b_3 = a_4 a_1^2 + a_3^2 = t^2+t+t^4+t^2+1 = t^4+t+1$

よって $g(y) = y^3 + (t^2+t+1)y + (t^2+t+1)$

アイゼンシュタインの判定法より これは既約

$c_1 = b_1 b_2 + b_3 = t^4+t+1$

$c_2 = b_2^3 + b_3^2 + b_1^3 b_3 = (t^2+t+1)^3 + (t^2+t+1)^2 = (t^2+t+1)^2(t^2+t)$

よって $h(z) = z^2 + (t^2+t+1)z + (t^2+t+1)^2(t^2+t)$

$= \{z + t(t^2+t+1)\}\{z + (t+1)(t^2+t+1)\}$

よって $\mathrm{Gal}(L/K) \cong A_4$

解を持つとすると、その解は $(t^2+t+1)$ の倍元であることを利用すると因数分解できる。

(5) 1. 与式はアイゼンシュタインの判定法より既約分離多項式

$b_1 = a_2 = 0 \qquad b_2 = a_1 a_3 = 0$

$b_3 = a_4 a_1^2 + a_3^2 = t^2$

よって $\quad g(y) = y^3 + t^2$

次数の関係より これは既約.

また $\quad c_1 = b_1 b_2 + b_3 = t^2$

$c_2 = b_2^3 + b_3^2 + b_1^3 b_3 = t^4$

よって $\quad h(z) = z^2 + t^2 z + t^4$

次数の関係などから $h(z)$ は既約.

したがって $\quad \mathrm{Gal}(L/K) \cong \mathfrak{S}_4$