ALGEBRA 2 16-06-2020

1 $\mathbb{Z}_5(\gamma)$:= campo estensione di $\mathbb{Z}_5$ t.c. $\gamma^4 - \gamma + 4 = 0$.

(a) Dimostrare che $[\mathbb{Z}_5(\gamma) : \mathbb{Z}_5] = 4$.

(b) Descrivere esplicitamente un $\phi \in \mathrm{Aut}(\mathbb{Z}_5(\gamma)/\mathbb{Z}_5)$

(c) Determinare il # di estensioni intermedie K: $\mathbb{Z}_5 \subseteq K \subseteq \mathbb{Z}_5(\gamma)$

Soluzione:

(a) $\gamma^4 - \gamma + 4 = 0 \Rightarrow \gamma$ è algebrico su $\mathbb{Z}_5$,

$p_\gamma^{\mathbb{Z}_5}(x)$ divide $x^4 - x + 4$ in $\mathbb{Z}_5[x]$,

e $d_\gamma := [\mathbb{Z}_5(\gamma) : \mathbb{Z}_5] = \partial(p_\gamma^{\mathbb{Z}_5}(x)) \leq 4 \Rightarrow$

$\Rightarrow \quad d_\gamma \in \{1, 2, 4\}$.

ORA: $d_\gamma = 1 \iff \gamma \in \mathbb{Z}_5$, (4) perché

$$(x^4 - x + 4)(\bar{z}) = \bar{z}^4 - \bar{z} + \bar{4} = \bar{1} - \bar{z} + \bar{4} = -\bar{z} \neq \bar{0}$$

$\forall \bar{z} \in \mathbb{Z}_5$, $\bar{z} \neq \bar{0}$

& $(x^4 - x + 4)(\bar{0}) = \bar{0}^4 - \bar{0} + \bar{4} = \bar{4} \neq \bar{0}$ $\Rightarrow$ $d_\gamma \neq 1$

$d_\gamma = 2 \iff \exists\, a, b, \alpha, \beta \in \mathbb{Z}_5$:

$$x^4 - x + 4 = (x^2 + ax + b)(x^2 + \alpha x + \beta) =$$

$$= x^4 + (a+\alpha)\cdot x^3 + (b + a\alpha + \beta)x^2 +$$

$$+ (b\alpha + a\beta)x + b\beta \iff$$

$$\iff \exists\, a, b, \alpha, \beta \in \mathbb{Z}_5 : \begin{cases} a + \alpha = 0 \\ b + a\alpha + \beta = 0 \\ b\alpha + a\beta = -1 \\ b\beta = 4 = -1 \end{cases} \iff$$

$$\iff \exists\, \underset{\alpha,\beta}{a,b} \in \mathbb{Z}_5 : \begin{cases} \alpha = -a \\ b - b^{-1} = +a^2 \\ +a\cdot(b + b^{-1}) = +1 \\ \beta = -b^{-1} \end{cases} \iff$$

$$\iff \left\{ \exists\, \underset{\alpha,\beta}{a,b} \in \mathbb{Z}_5 : \right. \begin{cases} \alpha = -a \\ a^2 = b - b^{-1} \\ a = (b + b^{-1})^{-1} \\ \beta = -b^{-1} \end{cases} \rightarrow$$

$$\rightarrow (b + b^{-1})^{-2} = a^2 = (b - b^{-1}) \Rightarrow$$

$$\Rightarrow 1 = (b - b^{-1})(b + b^{-1})^2 \Rightarrow b^3 = (b^2 - 1)(b^2 + 1)^2 \Rightarrow$$

$$\Rightarrow \underline{b^6 + b^4 - b^3 - b^2 - \bar{1} = \bar{0}} \text{ in } \mathbb{Z}_5, \; b \neq \bar{0} \Rightarrow$$

$$\Rightarrow (\bar{b}^4 = \bar{1}) \quad -\bar{b}^3 = \bar{0} \Rightarrow b = \bar{0}, \; \lightning \Rightarrow$$

$$\Rightarrow \boxed{d_\gamma \neq 2}$$

ALLORA $d_\gamma \in \{1, 2, 4\}$ MA $d_\gamma \neq 1$, $d_\gamma \neq 2$, $\Rightarrow$

$\Rightarrow d_\gamma = 4$, $\Rightarrow X^4 - X + 4$ è irriducibile in $\mathbb{Z}_5[X]$, e $\boxed{d_\gamma := [\mathbb{Z}_5(\gamma) : \mathbb{Z}_5] = 4}$

(b) Dalla teoria generale, sappiamo che $\mathbb{Z}_5(\gamma)/\mathbb{Z}_5$ è una estensione di Galois, con gruppo di Galois ciclico generato dall'automorfismo di Frobenius

$$\phi : \mathbb{Z}_5(\gamma) \longrightarrow \mathbb{Z}_5(\gamma)$$
$$\alpha \longmapsto \alpha$$

Per gli elementi $\alpha \in \mathbb{Z}_5$ $(\subseteq \mathbb{Z}_5(\gamma))$ si ha

$\phi(\alpha) = \alpha^5 = \alpha$, perché $\bar{z}^5 = \bar{z}$ $\forall \bar{z} \in \mathbb{Z}_5$

(piccolo teorema di Fermat)

e per il generatore γ di $\mathbb{Z}_5(\gamma)$ si ha

$$\phi(\gamma) := \gamma^5 = \gamma \cdot \gamma^4 = \gamma \cdot (\gamma - 4) = \gamma \cdot (\gamma + 1) =$$
$$= \gamma^2 + \gamma$$

N.B.: da (a) si ha $[\mathbb{Z}_5(\gamma) : \mathbb{Z}_5] = 4$,

perciò una base di $\mathbb{Z}_5(\gamma)$ su $\mathbb{Z}_5$ è $\mathcal{B} := \{1, \gamma, \gamma^2, \gamma^3\}$. Rispetto a tale base, l'automorfismo ϕ è descritto dalla matrice

$$M_\phi = \begin{pmatrix} 1 & 0 & 1 & 3 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 4 \\ 0 & 0 & 2 & 2 \end{pmatrix}$$

perché

$$\phi(1) = 1 = 1\cdot 1 + 0\cdot\gamma + 0\cdot\gamma^2 + 0\cdot\gamma^3$$

$$\phi(\gamma) = \gamma^2 + \gamma = 0\cdot 1 + 1\cdot\gamma + 1\cdot\gamma^2 + 0\cdot\gamma^3$$

$$\phi(\gamma^2) = \phi(\gamma)^2 = (\gamma^2+\gamma) = \gamma^4 + 2\cdot\gamma^2\cdot\gamma + \gamma^2 =$$

$$= \gamma - 4 + 2\cdot\gamma^3 + \gamma^2 = 1 + \gamma + \gamma^2 + 2\gamma^3 =$$

$$= 1\cdot 1 + 1\cdot\gamma + 1\cdot\gamma^2 + 2\cdot\gamma^3$$

$$\phi(\gamma^3) = \phi(\gamma)\cdot\phi(\gamma^2) = (\gamma+\gamma^2)(1+\gamma+\gamma^2+2\gamma^3) =$$

$$= \gamma + \gamma^2 + \gamma^3 + 2\gamma^4 + \gamma^2 + \gamma^3 + \gamma^4 + 2\gamma^5 =$$

$$= \gamma + \gamma^2 + \gamma^3 + 2(\gamma+1) + \gamma^2 + \gamma^3 + (\gamma+1) +$$

$$+ 2\cdot\gamma\cdot(\gamma+1) =$$

$$= (2+1)\cdot 1 + (1+2+1+2)\cdot\gamma + (1+1+2)\gamma^2 +$$

$$+ (1+1)\gamma^3 = 3\cdot 1 + 1\cdot\gamma + 4\cdot\gamma^2 + 2\gamma^3$$

(e) Siccome $\mathbb{Z}_5(\gamma)/\mathbb{Z}_5$ è di Galois, $\exists$ biiezione tra le estensioni intermedie $\mathbb{F}$ (i.e. $\mathbb{Z}_5 \subseteq \mathbb{F} \subseteq \mathbb{Z}_5(\gamma)$) e i sottogruppi del gruppo di Galois $Gal(\mathbb{Z}_5(\gamma)/\mathbb{Z}_5)$. Ma sappiamo che

$$Gal(\mathbb{Z}_5(\gamma)/\mathbb{Z}_5) \cong \mathbb{Z}_{4\,[\mathbb{Z}_5(\gamma):\mathbb{Z}_5]} = \mathbb{Z}_4$$

~~e siccome $\mathbb{Z}_4$~~ è un gruppo ciclico di ordine 4, quindi $\exists$ biiezione tra i sottogruppi di $\mathbb{Z}_4$ e i divisori di 4 (in generale, $\forall n \in \mathbb{N}_+$ si ha che $\exists$ biiezione

$$Sgr(\mathbb{Z}_n) \longleftrightarrow Div(n)$$
$$\Gamma \longleftrightarrow |\Gamma|$$
$$\langle [n/d]_n \rangle \longleftrightarrow d \quad)$$

Ma i divisori di $|\mathbb{Z}_4| = 4$ in $\mathbb{N}_+$ sono 1, 2 e 4, quindi in conclusione $\exists$ esattamente 3 campi $\mathbb{F}$ come richiesto.

2 → $R := \dfrac{\mathbb{Z}[u,v]}{(2u^2+uv+3v-8,\ u+v-3)}$

(a) Dim. che R non è campo

(b) Dim. che R è dominio euclideo

(c) Relativamente a (b), calcolare quoziente e resto nella divisione di $a := \overline{1-u^2+2v-u}$ per $b := \overline{u^2+uv+v}$.

Soluzione:

Osserviamo che (Teor. del Doppio Quot.)

$$R := \frac{\mathbb{Z}[u,v]}{(2u^2+uv+3v-8,\ u+v-3)} \cong$$

$$\cong \frac{\mathbb{Z}[u,v]/(u+v-3)}{(2u^2+uv+3v-8,\ u+v-3)/(u+v-3)} \cong$$

$$\cong \frac{\mathbb{Z}_4[\bar{v}]}{\left(2(3-\bar{v})^2+(\bar{v}-3)\bar{v}+3\bar{v}-8\right)} \cong \frac{\mathbb{Z}_4[\bar{v}]}{(\bar{v}^2-6\bar{v}+10)}$$

ORA, siccome il polinomio

$p(x) := x^2 - 6x + 10$ è irriducibile in $\mathbb{Z}[x]$

l'anello $R \cong \mathbb{Z}[\bar{v}] / (\bar{v}^2 - 6\bar{v} + 10)$

è un dominio.

(a) $R \equiv \mathbb{Z}[\bar{v}] / (\bar{v}^2 - 6\bar{v} + 10)$

NON è un campo, perché chiaramente elementi come $\bar{3}$ non sono invertibili (infatti, $\exists$ copia isomorfa di $\mathbb{Z}$ in R - è il sottoanello generato da 1 in R - e $\forall z \in \mathbb{Z} \subseteq R$ con $z \neq 0$ si ha che $\nexists z^{-1} \in R$).

(b) Siccome $x^2 - 6x + 10 = (x - (3+i))(x - (3-i))$

$\mathbb{Z}[x]$, il morfismo

$$\mathbb{Z}[\bar{v}] \longrightarrow \mathbb{Z}[i]$$

$$P(\bar{v}) \longmapsto P(3+i)$$

manda l'ideale $(\bar{v}^2 - 6\bar{v} + 10)$ in zero, e più precisamente $(\bar{v}^2 - 6\bar{v} + 10) = \ker(\varphi)$

((N.B.: qui si sfrutta il fatto che $b(x) := x^2 - 6x + 10$ sia monico, per cui ogni altro polinomio in $\mathbb{Z}[x]$ può essere "diviso-con-resto" per $b(x)$!!!))

allora (1ºss. Fond. di Omomorf.)

φ induce un isomorfismo

$$\varphi_* : \frac{\mathbb{Z}[\bar{\nu}]}{\ker(\varphi)} \xrightarrow{\sim} \mathrm{Im}(\varphi)$$

$$P(\bar{\nu}) + \ker(\varphi) \longmapsto P(3+i)$$

Ma siccome $\ker(\varphi) = (\bar{\nu}^2 - 6\bar{\nu} + 10)$

e $\mathrm{Im}(\varphi) = \mathbb{Z}[i]$ (ovvio...)

si ha

$$\varphi_* : \frac{\mathbb{Z}[\bar{\nu}]}{(\bar{\nu}^2 - 6\bar{\nu} + 10)} \xrightarrow{\sim} \mathbb{Z}[i]$$

Infine, questo più l'analisi

precedente ci dà un isomorfismo

$$\psi : R \xrightarrow{\cong} \mathbb{Z}[i]$$

$$[x] \longmapsto 3+i$$

$$[u] \longmapsto -i$$

$$[P(u,v)] \longmapsto P(-i, 3+i)$$

ORA, siccome $\mathbb{Z}[i]$ è un dominio euclideo, (e NON è un campo) si conclude che anche R è un dominio euclideo (e NON è un campo).

(c) Nell'isomorfismo ψ qui sopra si ha

$$a := \overline{1-u^2+2v-u} \xmapsto{\psi} 8+3i$$

$$b := \overline{u^2+uv+v} \xmapsto{\psi} 3-2i$$

e la divisione di $(8+3i)$ per $(3-2i)$ in $\mathbb{Z}[i]$ dà $8+3i = (3-2i)\cdot(1+2i) + (1-i)$

($1+2i$: quoziente; $1-i$: resto)

3 G gruppo di ordine 675.

(a) $\exists$ sempre una decomposizione in prod. semidir. di G non banale.

(b) Determinare una C.N.E.S. perché G sia risolubile.

(c) Determ. una C.N.E.S. perché G sia abeliano

(d) Se G è abeliano, determ. la sua possibile struttura ciclica secondo il 1° Teor. di Class. e il 2° Teor. di Class.

Soluzione:

(a) $|G| = 675 = 25 \cdot 27 = 5^2 \cdot 3^3$

$\Rightarrow$ (Σ_p := p-Sylow in G)

$|\Sigma_3| = 3^3 = 27$, $|\Sigma_5| = 5^2 = 25$

ν_p := # (p-Sylow in G) $\in \mathbb{N}_+$

$\nu_p \in (1+p\mathbb{N}) \cap \mathrm{Div}(n/p^\alpha)$ se $|G| = n$, $p^\alpha = |\Sigma_p|$

ALLORA per $p=3$ e $p=5$ si ha

$$\nu_3 \in (1+3\mathbb{N}) \cap \mathrm{Div}(5^2) = \{1, 25\}$$

$$\nu_5 \in (1+5\mathbb{N}) \cap \mathrm{Div}(3^3) = \{1\} \Rightarrow$$

$\Rightarrow \nu_5 = 1 \Rightarrow \exists!$ 5-Sylow, sia K_5, $\Rightarrow$

$\Rightarrow$ tale K_5 è caratteristico in G,

in particolare $K_5 \trianglelefteq G$, i.e. K_5 è normale.

INOLTRE $\exists$ 3-Sylow in G, sia Σ_3.

ORA: ① $K_5 \trianglelefteq G$, $\Sigma_3 \leq G$

$$|K_5| = 5^2, \quad |\Sigma_3| = 3^3 \Rightarrow$$

$$\Rightarrow |K_5 \cap \Sigma_3| \;\Big|\; \mathrm{MCD}(5^2, 3^3) = 1 \Rightarrow$$

$$\Rightarrow |K_5 \cap \Sigma_3| = 1, \Rightarrow K_5 \cap \Sigma_3 = \{1_G\}$$

② $K_5 \times \Sigma_3 \xrightarrow{\mu} G$ è iniettiva

$(x, \sigma) \longmapsto x \cdot \sigma$

(perché $K_5 \cap \Sigma_3 = \{1_G\}$) con

$\mathrm{Im}(\mu) = K_5 \cdot \Sigma_3$ (per definizione)

QUINDI

$$|K_5 \cdot \Sigma_3| = |\mu(K_5 \times \Sigma_3)| \overset{\text{perché } \mu \text{ è iniettiva}}{=} |K_5 \times \Sigma_3| =$$

$$= |K_5| \cdot |\Sigma_3| = 5^2 \cdot 3^3 = |G|, \Rightarrow$$

$$\Rightarrow |K_5 \cdot \Sigma_3| = |G| \quad \& \quad K_5 \cdot \Sigma_3 \leq G \Rightarrow K_5 \cdot \Sigma_3 = G$$

DUNQUE $G \cong K_5 \rtimes_{\Phi} \Sigma_3$

per un certo morfismo di gruppi

$$\Phi : \Sigma_3 \longrightarrow (Aut_G(K_5); \circ)$$

con K_5 e Σ_3 non banali.

(b) Da $G \cong K_5 \rtimes_{\Phi} \Sigma_3$ segue che

$$K_5 \trianglelefteq G \text{ con } G/K_5 \cong \Sigma_3 \quad (\star)$$

MA $|K_5| = 5^2$, 5 primo $\Rightarrow K_5$ è abeliano, $\Rightarrow K_5$ è risolubile

Σ_3 è 3-gruppo, con 3 primo $\Rightarrow \Sigma_3$ è risolubile

((N.B.: il secondo ragionamento vale anche per K_5, che è p-gruppo per $p = 5$))

ALLORA:

$(K_5$ risolubile$) + (\Sigma_3$ risolubile$) + (\star) \Rightarrow$

$\Rightarrow$ G è risolubile.

QUINDI G è sempre risolubile.

(c) Abbiamo che

G abeliano $\Rightarrow$ ogni $H \leq G$ è abeliano

QUINDI G abeliano $\Rightarrow$ K_5 e Σ_3 abeliani

INOLTRE $G \cong K_5 \underset{\Phi}{\times} \Sigma_3$

G è abeliano

$\mapsto$ "$\underset{\Phi}{\times}$" è un "$\times$"
CIOÈ
il prodotto semidiretto è diretto
CIOÈ
Φ è banale
($\Phi(\sigma) := id_{K_5}$ $\forall \sigma \in \Sigma_3$)

QUINDI

COND. NECESSARIA perché G sia abeliano è che K_5 e Σ_3 abeliani e Φ banale] $\circledast$

VICEVERSA, se

K_5 e Σ_3 abeliani
&
Φ banale $\longrightarrow$ allora si ha

perché Φ è banale

$$G \cong K_5 \underset{\Phi}{\rtimes} \Sigma_3 \cong K_5 \times \Sigma_3$$

abeliano, perché è prodotto diretto di gruppi abeliani.

QUINDI la C.N. ⊛ di pag. 13 è anche C.S.

DUNQUE

C.N.E.S. perché G sia abeliano è

K_5 è abeliano, Σ_3 è abeliano

$\Phi: \Sigma_3 \to Aut(K_5)$ è banale $\longrightarrow$ ⊛

NOTA: in certi casi l'ultima condizione in ⊛ è superflua (segue dalle altre due). Precisamente

$|\Sigma_3| = 3^3 \Rightarrow \forall \sigma \in \Sigma_3$ si ha $ord(\sigma) \in \{3^e\}_{e=0,1,2,3}$

$|K_5| = 5^2 \longrightarrow K_5 \cong \begin{cases} \mathbb{Z}_{25} \\ \mathbb{Z}_5 \times \mathbb{Z}_5 \end{cases} \Rightarrow$

$\Rightarrow \mathrm{Aut}_g(K_5) \cong$ ~~A_5~~

$\mathrm{Aut}_g(\mathbb{Z}_{25}) \cong U(\mathbb{Z}_{25})$ ← ordine $\phi(25) = 20$

$\mathrm{Aut}_g(\mathbb{Z}_5 \times \mathbb{Z}_5) \cong GL_2(\mathbb{Z}_5)$

ORDINE $(5^2-1)\cdot(5^2-5) =$
$= 24 \cdot 20 = \underline{3 \cdot 2^5 \cdot 5}$

ALLORA

<u>1° CASO</u> $\mathrm{Aut}_g(K_5)$ ha ordine 20

<u>2° CASO</u> $\mathrm{Aut}_g(K_5)$ ha ordine $3 \cdot 2^5 \cdot 5$

mentre $\mathrm{ord}(\sigma) \in \{3^e\}_{e=0,1,2,3;} \quad \forall \sigma \in \Sigma_3$

QUINDI $\mathrm{ord}(\Phi(\sigma)) \in \mathrm{Div}(3^3) \cap \mathrm{Div}\begin{pmatrix} 20 \\ \text{oppure} \\ 3 \cdot 2^5 \cdot 5 \end{pmatrix}$

$\Rightarrow$ nel <u>1° caso</u> è SEMPRE $\mathrm{ord}(\Phi(\sigma)) = 1$

cioè $\Phi(\sigma) = id_{K_5}, \quad \forall \sigma \in \Sigma_3$

cioè Φ è banale

nel <u>2° caso</u> invece può essere (anche)
$\Phi(\sigma) = 3$, e in effetti $\exists$ sempre
un Φ t.c. $\Phi(\sigma') = 3$ per
qualche $\sigma' \in \Sigma_3$

(d) $|G| = 675 = 5^2 \cdot 3^3$

1° Teor. di Clas. (+ divisori):

$G \cong$ uno dei 6 gruppi seguenti:

$\mathbb{Z}_{5^2 \cdot 3^3} = \mathbb{Z}_{675}$

$\mathbb{Z}_{5^2 \cdot 3^2} \times \mathbb{Z}_{3^1} = \mathbb{Z}_{225} \times \mathbb{Z}_3$

$\mathbb{Z}_{5^2 \cdot 3^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \cong \mathbb{Z}_{75} \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_{5^1 \cdot 3^3} \times \mathbb{Z}_{5^1} = \mathbb{Z}_{135} \times \mathbb{Z}_5$

$\mathbb{Z}_{5^1 \cdot 3^2} \times \mathbb{Z}_{5^1 \cdot 3^1} = \mathbb{Z}_{45} \times \mathbb{Z}_{15}$

$\mathbb{Z}_{5^1 \cdot 3^1} \times \mathbb{Z}_{5^1 \cdot 3^1} \times \mathbb{Z}_{3^1} = \mathbb{Z}_{15} \times \mathbb{Z}_{15} \times \mathbb{Z}_3$

2° Teor. di Class. (+ p-Sylow):

$G \cong$ uno dei 6 gruppi seguenti:

$\mathbb{Z}_{5^2} \times \mathbb{Z}_{3^3} = \mathbb{Z}_{25} \times \mathbb{Z}_{27}$, $\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{3^3} = \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_{27}$

$\mathbb{Z}_{5^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^1} = \mathbb{Z}_{25} \times \mathbb{Z}_9 \times \mathbb{Z}_3$

$\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^1} = \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_9 \times \mathbb{Z}_3$

$\mathbb{Z}_{5^2} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} = \mathbb{Z}_{25} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

4 $\omega := 7 - (\sqrt[3]{5})^2 \in \mathbb{R}$

(a) Dim. che ω è algebrico su $\mathbb{Q}$, e calcolarne il polinomio minimo.

(b) Determinare la minima estensione normale $\mathbb{Q}^\omega/\mathbb{Q}$ t.c. $\mathbb{Q}^\omega \supseteq$

(c) Determinare se $\exists$ campo K : $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}^\omega$ con $K/\mathbb{Q}$ normale di grado 3.

Soluzione:

(a) $\omega := 7 - (\sqrt[3]{5})^2 \in \mathbb{Q}(\sqrt[3]{5})$ - con $\sqrt[3]{5}$ algebrico su $\mathbb{Q}$ di grado 3 - con polinomio minimo $X^3 - 5$ -

QUINDI ω è algebrico su $\mathbb{Q}$, con grado d_ω che divide $[\mathbb{Q}(\omega):\mathbb{Q}] = 3$, dunque $d_\omega \in \{1, 3\}$.

MA $d_\omega = 1 \iff \omega \in \mathbb{Q} \iff (\sqrt[3]{5})^2 \in \mathbb{Q} \iff$
$\iff 5 \cdot \sqrt[3]{5} = ((\sqrt[3]{5})^2)^2 \in \mathbb{Q} \iff \sqrt[3]{5} \in \mathbb{Q}$
e siccome $\sqrt[3]{5} \notin \mathbb{Q}$, ossia $d_\omega \neq 1$;
$\Rightarrow d_\omega = 3$.

DUNQUE

$$\underbrace{\mathbb{Q} \subseteq \mathbb{Q}(\omega)}_{\text{grado 3}} \subseteq \mathbb{Q}(\sqrt[3]{5}) \Rightarrow$$

$\Rightarrow \mathbb{Q}(\sqrt[3]{5}) / \mathbb{Q}(\omega)$ ha grado 1, $\Rightarrow$

$\Rightarrow \mathbb{Q}(\omega) = \mathbb{Q}(\sqrt[3]{5})$

Il polinomio minimo $p_\omega^{\mathbb{Q}}(t)$ di ω su $\mathbb{Q}$ è monico, in $\mathbb{Q}[t]$, con grado 3.

ORA (*) $\omega := 7 - (\sqrt[3]{5})^2 \Rightarrow$

$\Rightarrow \omega - 7 = -(\sqrt[3]{5})^2 \Rightarrow$

$\Rightarrow (\omega - 7)^3 = -5^2 = -25 \Rightarrow$

$\Rightarrow \omega^3 - 21 \cdot \omega^2 + 147 \cdot \omega - 343 = -25 \Rightarrow$

$\Rightarrow \omega^3 - 21 \cdot \omega^2 + 147 \cdot \omega - 318 = 0 \Rightarrow$

$\Rightarrow p(\omega) = 0$ con

$p(x) := x^3 - 21 \cdot x^2 + 147 \cdot x - 318 \in \mathbb{Q}[x]$

$p(x)$ monico, $\partial(p(x)) = 3$

$\Longrightarrow p(x) = p_\omega^{\mathbb{Q}}(x)$,

cioè $p_\omega^{\mathbb{Q}}(t) \equiv t^3 - 21 \cdot x^2 + 147 \cdot x - 318$

N.B.: se si parte direttamente da (*) si trova che $p(\omega) = 0$, $\Rightarrow \omega$ è algebrico su $\mathbb{Q}$, di grado al più 3

INOLTRE il criterio di Eisenstein per $p=3$ dà che $p(x)$ è irriducibile

$\Longrightarrow p(x) = p_\omega^{\mathbb{Q}}(x)$, come prima.

(b) $\mathbb{Q}^\omega \supseteq \omega$, $\mathbb{Q}^\omega \supseteq \mathbb{Q} \Rightarrow \mathbb{Q}^\omega \supseteq \mathbb{Q}(\omega)$,
ω è radice di x^3-5 $\qquad$ $\mathbb{Q}(\sqrt[3]{5})$

$\mathbb{Q}^\omega$ contiene ogni radice α' di x^3-5

Le α_+ è radice di x^3-5 con $\alpha_+ \neq \alpha := \sqrt[3]{5}$

$\Rightarrow \alpha^3 = 5$, $\alpha_+^3 = 5$, $\Rightarrow$

$\Rightarrow (\alpha \cdot \alpha_+^{-1})^3 = 5 \cdot 5^{-1} = 1 \Rightarrow$

$\Rightarrow \zeta_3 := \alpha \cdot \alpha_+^{-1}$ è radice di x^3-1,

con $\zeta_3 \neq 1 \Longrightarrow$

$\Longrightarrow \zeta_3$ è radice 3ª primitiva di 1

$\Rightarrow \boxed{\alpha_+ = \zeta_3 \cdot \alpha}$

MORALE: $\mathbb{Q}^\omega \ni \alpha, \zeta_3\alpha, \zeta_3^2 \cdot \alpha = \zeta_3^{-1} \cdot \alpha$

$\Longrightarrow \mathbb{Q}^\omega \supseteq \mathbb{Q}(\alpha, \zeta)$

MA $\mathbb{Q}(\alpha, \zeta)$ è il campo di spezzamento di x^3-5 su $\mathbb{Q}$, $\Rightarrow \mathbb{Q}(\alpha,\zeta)/\mathbb{Q}$ è normale, $\Rightarrow \mathbb{Q}^\omega = \mathbb{Q}(\alpha, \zeta)$.

(*) $\mathbb{Q}^\omega/\mathbb{Q}$ è normale, $\mathrm{char}(\mathbb{Q})=0$, $\Rightarrow$

$\Rightarrow$ $\mathbb{Q}^\omega/\mathbb{Q}$ è estensione finita di Galois, $\Rightarrow$

$\Rightarrow$ $\exists$ biezione tra estensioni intermedie $\mathbb{K}$ (di $\mathbb{Q}^\omega/\mathbb{Q}$) t.c. $\mathbb{K}/\mathbb{Q}$ sia normale e sottogruppi normali di $G := \mathrm{Gal}(\mathbb{Q}^\omega/\mathbb{Q})$, data da

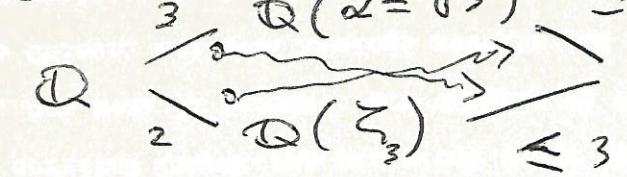
$$\mathbb{K} \longmapsto \mathrm{Gal}(\mathbb{Q}^\omega/\mathbb{K})$$

$$(\mathbb{Q}^\omega)^H \longleftarrow\!\shortmid\; H$$

ORA, $|G| = |\mathrm{Gal}(\mathbb{Q}^\omega/\mathbb{Q})| =$

$= [\mathbb{Q}^\omega : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}] = 6$

perché



si dà $[\mathbb{Q}(\alpha, \zeta_3) : \mathbb{Q}] = 3 \cdot 2 = 2 \cdot 3 = 6$

(N.B.: $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ perché $p^{\mathbb{Q}}_{\zeta_3}(x) = x^2 + x + 1$)

POI $G := \mathrm{Gal}(\mathbb{Q}^\omega/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q})$

contiene i due automorfismi

$$\rho : \mathbb{Q}(\alpha, \zeta_3) \longrightarrow \mathbb{Q}(\alpha, \zeta_3)$$

$$\alpha \longmapsto \alpha\,\zeta_3$$
$$\zeta_3 \longmapsto \zeta_3$$
$$q \longmapsto q, \quad \forall\, q \in \mathbb{Q}$$

$$\tau : \mathbb{Q}(\alpha, \zeta_3) \longrightarrow \mathbb{Q}(\alpha, \zeta_3)$$

$$\alpha \longmapsto \alpha$$
$$\zeta_3 \longmapsto \zeta_3^2$$
$$q \longmapsto q, \quad \forall\, q \in \mathbb{Q}$$

per i quali si ha (nel gruppo G)

$$\rho^3 = id_{\mathbb{Q}(\alpha,\zeta_3)}, \qquad \tau^2 = id_{\mathbb{Q}(\alpha,\zeta_3)}$$

$$\rho \circ \tau = \tau \circ \rho^2$$

Ricordando al monomorfismo

$$\phi : G := Gal(\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q}) \hookrightarrow \mathfrak{S}(R_f) \cong \mathfrak{S}_3$$
$$\sigma \longmapsto \sigma|_{R_f}$$

dove $\mathbb{Q}(\alpha, \zeta_3) = \mathbb{Q}^{\omega} =: \mathbb{Q}^{sp}_{f(x)} =$

= campo di spezzamento di $f(x) := x^3 - 5$ su $\mathbb{Q}$

e $R_f := \{\text{radici di } f(x) \text{ (in } \mathbb{Q}^a)\} =$

$= \{\alpha, \alpha\zeta_3, \alpha\zeta_3^2\} = \{\alpha_1, \alpha_2, \alpha_3\}$

si ha $\phi(\rho) = (\alpha_1 \to \alpha_2 \to \alpha_3) \simeq (1,2,3)$

& $\phi(\tau) = (\alpha_2 \rightleftarrows \alpha_3) \simeq (2,3)$

QUINDI

$$G := Gal(\mathbb{Q}(\alpha, \zeta_3)/\mathbb{Q}) \underset{\phi}{\cong} \phi(G) = \langle (1,2,3), (2,3) \rangle \cong D_3$$

con

$\langle (1,2,3), (2,3) \rangle :=$ sottogr. di S_3 generato da $(1,2,3)$ e $(2,3)$

e $D_3 :=$ gruppo diedrale su 3 elementi

<u>ORA</u> $D_3 \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_3$, con $\mathbb{Z}_2 \cong \langle \tau \rangle$, $\mathbb{Z}_3 \cong \langle \rho \rangle$

con $\nu_3 = 1$, $\nu_2 = 3$, così i sottogruppi di D_3 sono:

- 1! di ordine 1: $\{id\}$,
- 1! di ordine 6: D_3,
- 1! di ordine 3: $\langle \rho \rangle = \langle (1,2,3) \rangle$
- 3 di ordine 2: $\{id, (2,3)\}$, $\{id, (3,1)\}$, $\{id, (1,2)\}$

di questi, quelli normali sono:
$\{id\}$, D_3, $\langle \rho \rangle =: N$

INFINE, passando alle estensioni intermedie associate, troviamo

$$\mathbb{K}_1 := (\mathbb{Q}^\omega)^{\{id\}} = \mathbb{Q}^\omega \Rightarrow [\mathbb{K}_1 : \mathbb{Q}] = 6 \neq 3$$

$$\mathbb{K}_2 := (\mathbb{Q}^\omega)^{D_3} = (\mathbb{Q}^\omega)^{Gal(\mathbb{Q}^\omega/\mathbb{Q})} = \mathbb{Q} \Rightarrow$$

$$\Rightarrow [\mathbb{K}_2 : \mathbb{Q}] = 1 \neq 3$$

$$\mathbb{K}_3 := (\mathbb{Q}^\omega)^N = (\mathbb{Q}^\omega)^{\langle e \rangle} =$$

$$= (\mathbb{Q}(\alpha, \zeta_3))^{\langle (\alpha, \alpha\zeta_3, \alpha\zeta_3^2) \rangle}$$

Inoltre, sappiamo che

$$[\mathbb{K}_3 : \mathbb{Q}] = [(\mathbb{Q}^\omega)^N : \mathbb{Q}] =$$

$$= (Gal(\mathbb{Q}^\omega/\mathbb{Q}) : N) =$$

$$= (D_3 : N) = (D_3 : \langle (1,2,3) \rangle) = 2$$

quindi $[\mathbb{K}_3 : \mathbb{Q}] = 2 \neq 3$

$\Rightarrow \nexists$ $\mathbb{K}$ estensione t.c. $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{Q}^\omega$, $\mathbb{K}/\mathbb{Q}$ normale e $[\mathbb{K} : \mathbb{Q}] = 3$.