

Università degli Studi di Roma “Tor Vergata”

CdL in Matematica

ALGEBRA 2

prof. Fabio GAVARINI

a.a. 2024–2025

Esame scritto del 26 Gennaio 2026 — 5° appello, sessione invernale

N.B.: compilare il compito in modo sintetico ma **esauriente**, spiegando chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.

..... *

[1] — Per ciascuno dei due possibili valori di $n \in \{675, 588\}$, si richiede di:

(a) determinare il numero di gruppi abeliani, a due a due non isomorfi, di ordine n ;

(b) per ciascuna classe di isomorfismo dei gruppi abeliani di ordine n trovata al punto (a), determinare esplicitamente uno dei gruppi nella classe.

[2] — Determinare il numero di anagrammi distinti per ciascuna delle due parole

“KIKKIRIKI” e “KIAKKIERARE”

[3] — Siano G_{35} e G_{36} due gruppi di ordine rispettivamente $|G_{35}| = 35$ e $|G_{36}| = 36$, e sia $\mathbb{Z}_{34}$ il gruppo degli interi modulo 34 (rispetto all'operazione di addizione tra classi resto).

(a) Determinare tutti i possibili omomorfismi $\varphi : G_{35} \longrightarrow G_{36}$ e quelli $\psi : G_{36} \longrightarrow G_{35}$, precisando quali di essi — eventualmente — siano *monomorfismi*, *epimorfismi* o *isomorfismi*.

(b) Dimostrare che un qualunque gruppo prodotto semidiretto del tipo $\mathbb{Z}_{34} \rtimes G_{35}$ è necessariamente un prodotto *diretto*.

(c) Dimostrare che ogni prodotto semidiretto del tipo $\mathbb{Z}_{34} \rtimes G_{35}$ è abeliano, ed è isomorfo al gruppo (additivo) $\mathbb{Z}_{1190}$.

[4] — Si consideri il sottoinsieme $\mathbb{Z}[\sqrt{-5}]$ del campo $\mathbb{C}$ definito da

$$\mathbb{Z}[\sqrt{-5}] := \left\{ z \in \mathbb{C} \mid \exists a, b \in \mathbb{Z} : z = a + b\sqrt{-5} \right\}$$

- (a) Dimostrare che $\mathbb{Z}[\sqrt{-5}]$ è sottoanello di $\mathbb{C}$.
- (b) Dimostrare che l'anello $\mathbb{Z}[\sqrt{-5}]$ è un dominio a fattorizzazione.
- (c) Determinare tutte le possibili fattorizzazioni in prodotto di fattori irriducibili per l'elemento 210 nell'anello $\mathbb{Z}[\sqrt{-5}]$.
- (d) Determinare se l'anello $\mathbb{Z}[\sqrt{-5}]$ sia un dominio a ideali principali.

[5] — Si consideri in $\mathbb{Z}[x]$ il polinomio

$$p(x) := 10x^6 + 5x^5 - 5x^4 - 18x^2 - 9x + 9$$

e per ogni campo $\mathbb{K}$ tale che $p(x) \in \mathbb{K}[x]$, si denoti con $\mathbb{K}_{p(x)}$ il campo di spezzamento su $\mathbb{K}$ del polinomio $p(x)$.

(a) Fattorizzare $p(x)$ in prodotto di fattori irriducibili nei diversi anelli $\mathbb{A}[x]$ per ogni $\mathbb{A} \in \{ \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C} \}$.

(b) Calcolare il grado $[\mathbb{K}_{p(x)} : \mathbb{K}]$ dell'estensione di campi $\mathbb{K}_{p(x)} / \mathbb{K}$ per $\mathbb{K} \in \{ \mathbb{Q}, \mathbb{R}, \mathbb{C} \}$.

(c) Calcolare il gruppo di Galois $\mathcal{G}_{p(x)}^{\mathbb{K}} := \text{Gal}(\mathbb{K}_{p(x)} / \mathbb{K})$ del polinomio $p(x)$ sul campo $\mathbb{K}$ per $\mathbb{K} \in \{ \mathbb{Q}, \mathbb{R}, \mathbb{C} \}$.

ALGEBRA 2

26/01/2026

— 0 —

[1] $[Hp: n \in \{675, 588\}]$

$[Th: (a)]$ Per $\{A \text{ gruppo abeliano} : |A| = n\} =: Ab_n$,
calcolare il numero di classi di isomorfismo in Ab_n .

(b) Dare un rappresentante per ciascuna
classe di isomorfismo in Ab_n .

Sol.:

$$(a) \quad n := 675 = 5^2 \cdot 3^3 \Rightarrow$$

$$\Rightarrow |Ab_{675} / \cong| = |\Pi_2| \cdot |\Pi_3| = 2 \cdot 3 = 6$$

dove $\Pi_k := \{\text{partizioni di } k\}$, e

$$\Pi_2 = \{(2), (1,1)\}, \quad \Pi_3 = \{(3), (2,1), (1,1,1)\}$$

$$n := 588 = 2^2 \cdot 7^2 \cdot 3^1 \Rightarrow$$

$$\Rightarrow |Ab_{588} / \cong| = |\Pi_2| \cdot |\Pi_7| \cdot |\Pi_1| = 2 \cdot 2 \cdot 1 = 4$$

(b) Per $n := 675 = 5^3 \cdot 3^3$ si ha

$$\mathcal{W}_{675}/\cong = \{ [\mathbb{Z}_5 \times \mathbb{Z}_{3^3}]_{\cong} = [\mathbb{Z}_{675}]_{\cong},$$

$$[\mathbb{Z}_{5^2} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^1}]_{\cong} = [\mathbb{Z}_{225} \times \mathbb{Z}_3]_{\cong} = [\mathbb{Z}_{75} \times \mathbb{Z}_9]_{\cong},$$

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

$$[\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{3^3}]_{\cong} = [\mathbb{Z}_{135} \times \mathbb{Z}_5]_{\cong},$$

$$[\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{3^2} \times \mathbb{Z}_{3^1}]_{\cong} = [\mathbb{Z}_{45} \times \mathbb{Z}_{15}]_{\cong},$$

$$[\mathbb{Z}_{5^1} \times \mathbb{Z}_{5^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1} \times \mathbb{Z}_{3^1}]_{\cong} = [\mathbb{Z}_{15} \times \mathbb{Z}_{15} \times \mathbb{Z}_3]_{\cong} \}$$

e per $n := 588 = 2^3 \cdot 3^2 \cdot 7^1$ si ha

$$\mathcal{W}_{588}/\cong = \{ [\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^1}]_{\cong} = [\mathbb{Z}_{588}]_{\cong},$$

$$[\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{3^1}]_{\cong} = [\mathbb{Z}_{84} \times \mathbb{Z}_7]_{\cong},$$

$$[\mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{3^1}]_{\cong} = [\mathbb{Z}_{294} \times \mathbb{Z}_2]_{\cong},$$

$$[\mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{3^1}]_{\cong} = [\mathbb{Z}_{42} \times \mathbb{Z}_{14}]_{\cong} \}$$

[2] Determinare il # di anagrammi di
 "KIKKIRIKI" e "KIACKIERARE".

Sol.:

Per "KIKKIRIKI" e

$$\left| \frac{S_9}{S_4 \times S_4 \times S_1} \right| = \binom{9}{4, 4, 1} = \frac{9!}{4! 4! 1!} =$$

$$= \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4!}{4! \cdot 3 \cdot 2 \cdot 1!} = 630$$

Per "KIACKIERARE" e

$$\left| \frac{S_{11}}{S_3 \times S_2 \times S_2 \times S_2 \times S_2} \right| = \binom{11}{3, 2, 2, 2, 2} =$$

$$= \frac{11!}{3! 2! 2! 2! 2!} = \frac{11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = 41580$$

[3] [Hp: $G_n :=$ gruppo con $|G_n| = n$

[TL: (a) Trovare tutti i morfismi

$$\varphi: G_{35} \longrightarrow G_{36}, \text{ precisando}$$

quali siano mono-, epi-, o iso-.

(b) IDEM di (a) per $\psi: G_{36} \longrightarrow G_{35}$

(c) Dimostrare che è sempre

$$G_{35} \times \mathbb{Z}_{34} \cong G_{35} \times \mathbb{Z}_{34}$$

(d) Dimostrare che $G_{35} \times \mathbb{Z}_{34}$ è sempre abeliano, ed è isomorfo a $\mathbb{Z}_{1260}$.

Sol:.

(a) $\forall \varphi: G_{35} \longrightarrow G_{36}$ si ha

$$k := |\text{Ker}(\varphi)| \mid \delta_N |G_{35}| = 35,$$

$$i := |\text{Im}(\varphi)| \mid \delta_N |G_{36}| = 36,$$

$$\text{Im}(\varphi) \cong G_{35}/\text{Ker}(\varphi) \Rightarrow i := |\text{Im}(\varphi)| = |G_{35}/\text{Ker}(\varphi)|$$

$$\begin{array}{ccc} 35/k = i & \Leftarrow & 35/k = |G_{35}|/|\text{Ker}(\varphi)| \\ \Downarrow & & \Downarrow \end{array}$$

$$35 = i \cdot k \Rightarrow i \mid 35$$

ALLORA si ha

$$i \delta_N 36 \quad \& \quad i \delta_N 35 \Rightarrow i \delta_N \text{MCD}(36, 35) = 1$$

$$| \text{Im}(\varphi) | =: i = 1 \quad \Leftrightarrow \quad i = 1$$

$$\text{Im}(\varphi) = \{ e_{G_{36}} \} \Rightarrow \varphi \text{ è banale (costante)}$$

In particolare,

φ non è mono-,

né epi-, né iso-.

$$G_{35} \xrightarrow{\varphi} G_{36}$$
$$g \longmapsto \varphi(g) = e_{G_{36}}$$

(b) Come in (a), $\forall \psi: G_{36} \rightarrow G_{35}$ si ha

$$k := |\ker(\psi)| \delta_N |G_{36}| = 36$$

$$i := |\text{Im}(\psi)| \delta_N |G_{35}| = 35 \Rightarrow i \delta_N 35$$

$$\& \quad i \cdot k = |G_{36}| = 36 \Rightarrow i \delta_N 36 \quad \Rightarrow$$

$$\Rightarrow i \delta_N \text{MCD}(35, 36) = 1 \Rightarrow i = 1 \Rightarrow$$

$$\Rightarrow \psi: G_{36} \rightarrow G_{35} \text{ è banale (costante)}$$

$$\text{cioè } g \longmapsto \psi(g) = e_{G_{35}}, \quad \forall g \in G_{36}.$$

In particolare, ψ non è mono-, né epi-,
né iso-.

(c) Ogni prodotto semidiretto $\mathbb{Z}_{34} \rtimes_{\Phi} G_{35}$

come insieme è il prodotto cartesiano

$\mathbb{Z}_{34} \times G_{35}$, con l'operazione data da

$$(\bar{a}, g) * (\bar{b}, \gamma) := (\bar{a} + \Phi(g)(\bar{b}), g \cdot \gamma) \quad (*)$$

$$\forall (\bar{a}, g), (\bar{b}, \gamma) \in \mathbb{Z}_{34} \times G_{35}$$

dove $\Phi: G_{35} \longrightarrow \text{Aut}_g(\mathbb{Z}_{34}; +)$ è un morfismo del gruppo G_{35} al gruppo

$\text{Aut}_g(\mathbb{Z}_{34}; +)$ degli automorfismi di $\mathbb{Z}_{34}$.

INOLTRE, dalla (*) segue che $\mathbb{Z}_{34} \rtimes_{\Phi} G_{35}$ è il prodotto diretto se e soltanto se Φ è il morfismo costante (= banale) dato da $\Phi(g) = \text{id}_{\mathbb{Z}_{34}}$, $\forall g \in G$.

ORA, sappiamo che $\text{Aut}_g(\mathbb{Z}_{34}; +) \cong U(\mathbb{Z}_{34})$

e che $|U(\mathbb{Z}_{34})| = \varphi(34) = \varphi(17 \cdot 2) = (17-1) \cdot (2-1) = 16$

dunque $|\text{Aut}_g(\mathbb{Z}_{34}; +)| = |\mathbb{Z}_{34}| = 16$.

Allora $\Phi: G_{35} \longrightarrow \text{Aut}_g(\mathbb{Z}_{34}; +)$ è un morfismo da un gruppo di ordine 35 a uno di ordine 16; siccome $\text{MCD}(35, 16) = 1$, come in (a) e (b) si ha che Φ è costante, ora $\mathbb{Z}_{34} \rtimes_{\Phi} G_{35}$ è diretto, q.e.d.

$$(d) |G_{35}| = 35 = 5 \cdot 7, \Rightarrow \text{ponendo}$$

$$\left. \begin{aligned} v_5 &:= \#(5\text{-Sylow in } G_{35}) \\ v_7 &:= \#(7\text{-Sylow in } G_{35}) \end{aligned} \right\} \Rightarrow$$

$$\Rightarrow \left\{ \begin{aligned} v_5 &\in \text{Div}_N(7) \cap (1+5N) = \{1\} \Rightarrow v_5 = 1 \\ v_7 &\in \text{Div}_N(5) \cap (1+7N) = \{1\} \Rightarrow v_7 = 1 \end{aligned} \right\} \Rightarrow$$

$$\Rightarrow \left\{ \begin{aligned} \exists! 5\text{-Sylow } K_5 &\trianglelefteq G_{35} \\ \exists! 7\text{-Sylow } K_7 &\trianglelefteq G_{35} \end{aligned} \right\} \Rightarrow G_{35} \geq K_5 \cdot K_7 \quad (\text{sottogruppo})$$

$$\text{e } |K_5 \cdot K_7| \in \text{Div}(5) \cap \text{Div}(7) = \{1\} \Rightarrow$$

$$\Rightarrow |K_5 \cap K_7| = 1 \Rightarrow K_5 \cap K_7 = \{1_{G_{35}}\}$$

$$\text{e } |K_5 \cdot K_7| \in \text{Mul}(5) \cap \text{Mul}(7) = 5N_+ \cap 7N_+ = 35 \cdot N_+$$

$$\text{and } |K_5 \cdot K_7| = 3 \cdot k, k \in N_+$$

$$\underline{\text{MA}} \quad K_5 \cdot K_7 \leq G_{35} \Rightarrow |K_5 \cdot K_7| \leq |G_{35}| = 35 \quad \Rightarrow$$

$$\Rightarrow |K_5 \cdot K_7| = 35 \Rightarrow K_5 \cdot K_7 = G_{35}$$

$$\text{e } K_5 \cap K_7 = \{1_{G_{35}}\} \Rightarrow G_{35} \cong K_5 \times K_7 \quad (\text{prodotto diretto})$$

$$\text{con } |K_5| = 5 \Rightarrow K_5 \cong \mathbb{Z}_5$$

$$|K_7| = 7 \Rightarrow K_7 \cong \mathbb{Z}_7$$

$$\mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$$

per il TEOREMA
CINESE DEL RESTO

ORA abbiamo che $G \cong \mathbb{Z}_{35}$

e per (b) si ha

$$G_{35} \rtimes_{\Phi} \mathbb{Z}_{34} \cong G_{35} \times \mathbb{Z}_{34}$$

quindi è $G_{35} \rtimes_{\Phi} \mathbb{Z}_{34} \cong \quad \times \mathbb{Z}_{34} \cong \mathbb{Z}_{35} \times \mathbb{Z}_{34}$

che è un prodotto diretto di gruppi abeliani;

QUINDI è a sua volta abeliana.

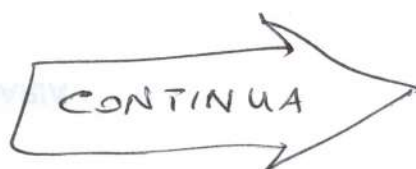
INFINE, siccome $\text{MCD}(35, 34) = 1$,

il TEOREMA CINESE DEL RESTO ci dà

$$\mathbb{Z}_{35} \times \mathbb{Z}_{34} \cong \mathbb{Z}_{35 \cdot 34} = \mathbb{Z}_{1190}$$

e quindi

$$G_{35} \rtimes_{\Phi} \mathbb{Z}_{34} \cong \mathbb{Z}_{1190}, \quad \text{q.e.d.}$$



$$[4] \quad \mathbb{Z}[\sqrt{-5}] := \{ z \in \mathbb{C} \mid \exists a, b \in \mathbb{Z} : z = a + b\sqrt{-5} \}$$

Th: (a) $\mathbb{Z}[\sqrt{-5}]$ è sottanello di $\mathbb{C}$.

(b) " " " " un D.F.

(c) Trovare tutte le fattorizzazioni in
irriducibili di 210 in $\mathbb{Z}[\sqrt{-5}]$.

(d) Determinare se $\mathbb{Z}[\sqrt{-5}]$ ha un D.I.P.

Sol:

(a) VERIFICA DIRETTA ---

$$0_{\mathbb{C}} = 0_{\mathbb{Z}} + 0_{\mathbb{Z}} \cdot \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] \quad \underline{ok}$$

$$\forall (a' + b'\sqrt{-5}), (a'' + b''\sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}] \quad \text{si ha}$$

$$(a' + b'\sqrt{-5}) - (a'' + b''\sqrt{-5}) =$$

$$= \underbrace{(a' - a'')}_{\substack{\uparrow \\ \mathbb{Z}}} + \underbrace{(b' - b'')\sqrt{-5}}_{\substack{\uparrow \\ \mathbb{Z}}} \in \mathbb{Z}[\sqrt{-5}] \quad \underline{ok}$$

$$(a' + b'\sqrt{-5}) \cdot (a'' + b''\sqrt{-5}) =$$

$$= \underbrace{(a'a'' - 5b'b'')}_{\substack{\uparrow \\ \mathbb{Z}}} + \underbrace{(a'b'' + a''b')\sqrt{-5}}_{\substack{\uparrow \\ \mathbb{Z}}} \in \mathbb{Z}[\sqrt{-5}] \quad \underline{ok}$$

(b) Per (a), $\mathbb{Z}[\sqrt{-5}]$ è sottoanello di $\mathbb{C}$

$\mathbb{C}$ è campo $\Rightarrow \mathbb{C}$ è dominio $\Rightarrow \mathbb{Z}[\sqrt{-5}]$ è dominio

INOLTRE, $\exists$ l'applicazione

$$v: \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{N} \cup \{-\infty\}$$

$$a + b\sqrt{-5} \longmapsto a^2 + 5 \cdot b^2$$

che è moltiplicativa, quindi è una valutazione per $\mathbb{Z}[\sqrt{-5}]$, in particolare

$$v(z' \cdot z'') = v(z') \cdot v(z'') \quad \text{e} \quad \text{Im}(v) \subseteq \mathbb{N}$$

$$\text{insieme a} \quad v(z) = 0 \iff z = 0$$

ci danno

$$v(z' - z'') = v(z') \cdot v(z'') \geq v(z')$$

$$\forall z', z'' \in \mathbb{Z}[\sqrt{-5}] \setminus \{0\}$$

Si dimostra allora, per induzione forte su $n := v(z)$, che ogni $z \in \mathbb{Z}[\sqrt{-5}] \setminus \{0\}$ ha una fattorizzazione in irriducibili, e cioè $\mathbb{Z}[\sqrt{-5}]$ è un dominio a fattorizzazione.

PIÙ IN GENERALE : $\mathbb{Z}[\sqrt{-5}]$ è $\Rightarrow \mathbb{Z}[\sqrt{-5}]$ è
(in generale) DOMINIO DI VALUTAZIONE DOMINIO A FATTORIZZAZIONE

(c) Osserviamo che se $z = \alpha \cdot \beta$ in $\mathbb{Z}[\sqrt{-5}]$,
allora $v(z) = v(\alpha) \cdot v(\beta)$ in $\mathbb{N}$,

cioè una fattorizzazione di z in $\mathbb{Z}[\sqrt{-5}]$
induce una fattorizzazione di $v(z)$ in $\mathbb{N}$.

ALLORA, se $v(z)$ è primo in $\mathbb{N}$,

la fattorizzazione $v(z) = v(\alpha) \cdot v(\beta)$

è banale in $\mathbb{N}$, cioè $v(\alpha) = 1$ o $v(\beta) = 1$,

il che implica subito

$$\alpha \in \{+1, -1\} = U(\mathbb{Z}[\sqrt{-5}])$$

$$\text{e } \beta \in \{+1, -1\} = U(\mathbb{Z}[\sqrt{-5}])$$

quindi la fattorizzazione $z = \alpha \cdot \beta$ in

$\mathbb{Z}[\sqrt{-5}]$ è banale; perciò si ha che

z è irriducibile in $\mathbb{Z}[\sqrt{-5}]$.

IN BREVE: $\forall z \in \mathbb{Z}[\sqrt{-5}] \setminus \{0\}$ si ha

$v(z)$ primo
in $\mathbb{N}$

$\Rightarrow$

z irriducibile
in $\mathbb{Z}[\sqrt{-5}]$

ORA: $\otimes 210 = 2 \cdot 5 \cdot 3 \cdot 7 \nrightarrow$ fattorizzazione in $\mathbb{Z} (\leq \mathbb{Z}[\sqrt{-5}])$

e inoltre $(\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-5}])$

$$2 = \alpha \cdot \beta \Rightarrow 4 = \sqrt{2} = \sqrt{\alpha} \cdot \sqrt{\beta} \Rightarrow$$

$$\Rightarrow \begin{cases} \sqrt{\alpha} = 2 = \sqrt{\beta} \rightarrow \text{IMPOSSIBILE} \\ \sqrt{\alpha} = 4, \sqrt{\beta} = 1 \\ \sqrt{\alpha} = 1, \sqrt{\beta} = 4 \end{cases} \begin{matrix} \rightarrow \text{IMPOSSIBILE} \\ \rightarrow \beta \in U(\mathbb{Z}[\sqrt{-5}]) \\ \rightarrow \alpha \in U(\mathbb{Z}[\sqrt{-5}]) \end{matrix} \Rightarrow$$

(perché $a^2 + 5b^2 \neq 2, \forall a, b \in \mathbb{Z}$)

$\Rightarrow$ la fattorizzazione $2 = \alpha \cdot \beta$ è banale $\Rightarrow$

$\Rightarrow$ 2 è irriducibile in $\mathbb{Z}[\sqrt{-5}]$

e analogamente

$$3 = \alpha \cdot \beta \Rightarrow 9 = \sqrt{3} = \sqrt{\alpha} \cdot \sqrt{\beta} \Rightarrow$$

$$\Rightarrow \begin{cases} \sqrt{\alpha} = 3 = \sqrt{\beta} \rightarrow \text{IMPOSSIBILE} \\ \{\sqrt{\alpha}, \sqrt{\beta}\} = \{9, 1\} \Rightarrow \end{cases}$$

$\Rightarrow$ 3 è irriducibile in $\mathbb{Z}[\sqrt{-5}]$

$$7 = \alpha \cdot \beta \Rightarrow 49 = \sqrt{7} = \sqrt{\alpha} \cdot \sqrt{\beta} \Rightarrow$$

$$\Rightarrow \begin{cases} \sqrt{\alpha} = 7 = \sqrt{\beta} \rightarrow \text{IMPOSSIBILE} \\ \{\sqrt{\alpha}, \sqrt{\beta}\} = \{49, 1\} \Rightarrow \end{cases}$$

$\Rightarrow$ 7 è irriducibile in $\mathbb{Z}[\sqrt{-5}]$

INVECE per 5 si ha

$$5 = \alpha \cdot \beta \Rightarrow 25 = \nu(5) = \nu(\alpha) \cdot \nu(\beta) \Rightarrow$$

$$\Rightarrow \left\{ \nu(\alpha), \nu(\beta) \right\} = \{25, 1\} \Rightarrow 5 = \alpha \cdot \beta \text{ è fattoriz. banale}$$

$$\nu(\alpha) = 5 = \nu(\beta) \Rightarrow \alpha = \pm \sqrt{-5}, \beta = \mp \sqrt{-5} \Rightarrow$$

$$\Rightarrow 5 = (+\sqrt{-5})(+\sqrt{-5}) \quad e \quad 5 = (-\sqrt{-5}) \cdot (-\sqrt{-5})$$

sono fattorizzazioni non banali,
equivalenti; $\Rightarrow$ 5 non è irriducibile
in $\mathbb{Z}[\sqrt{-5}]$

P01 $\pm \sqrt{-5}$ ha valutarione

$$\nu(\pm \sqrt{-5}) = 5 \text{ primo in } \mathbb{N}_+,$$

QUINDI, per l'osservazione di pag. 8, si ha

$\pm \sqrt{-5}$ è irriducibile in $\mathbb{Z}[\sqrt{-5}]$

ANQUE da $\otimes \quad 210 = 2 \cdot 5 \cdot 3 \cdot 7$

ricaviamo la fattorizzazione in irriducibili

$$\textcircled{I} \quad 210 = 2 \cdot \sqrt{-5} \cdot \sqrt{-5} \cdot 3 \cdot 7$$

insieme a tutte le varianti equivalenti
ottenute sostituendo alcuni fattori con dei
fattori associati (come $2 \mapsto -2$, $3 \mapsto -3$, ecc.)

Le altre fattorizzazioni - non equivalenti -
vengono dal riscrivere la fattorizzazione

$$\textcircled{*} \quad 210 = 2 \cdot 5 \cdot 3 \cdot 7$$

osservando che

irriducibili in $\mathbb{Z}[\sqrt{-5}]$

$$\begin{aligned} 2 \cdot 3 &= 6 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \\ 3 \cdot 7 &= 21 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}) \\ 2 \cdot 7 &= 14 = (3 + \sqrt{-5}) \cdot (3 - \sqrt{-5}) \end{aligned}$$

da cui otteniamo:

$$\textcircled{\text{II}} \quad 210 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}) \cdot \sqrt{-5} \cdot \sqrt{-5} \cdot 7$$

$$\textcircled{\text{III}} \quad 210 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}) \cdot 2 \cdot \sqrt{-5} \cdot \sqrt{-5}$$

$$\textcircled{\text{IV}} \quad 210 = (3 + \sqrt{-5}) \cdot (3 - \sqrt{-5}) \cdot \sqrt{-5} \cdot \sqrt{-5} \cdot 3$$

che, insieme a tutte le loro "varianti" (cambiando
fattori con altri associati), e insieme a $\textcircled{\text{I}}$,
ci danno tutte le possibili fattorizzazioni
di 210 in irriducibili in $\mathbb{Z}[\sqrt{-5}]$.

(d) Se $\mathbb{Z}[\sqrt{-5}]$ fosse un D.I.P., allora sarebbe
anche un D.F.U., ma il risultato in (c)
ci dice che invece NON è un D.F.U., $\Rightarrow$ non è D.I.P.

[5] [Hp]: $p(x) := 10x^6 + 5x^5 - 5x^4 - 18x^2 - 9x + 9$
in $\mathbb{Z}[x]$

e $K_{p(x)} :=$ campo di spezzamento di $p(x)$ su K
 $\forall K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

[Th]: (a) Fattorizzare $p(x)$ in irriducibili
in $A[x]$, $\forall A \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

(b) Calcolare $[K_{p(x)} : K]$, $\forall K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

(c) Calcolare il gruppo di Galois

$$G_{p(x)}^K := \text{Gal}(K_{p(x)}/K) \quad \forall K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}.$$

Sol.: (a) $p(x) = (x+1) \cdot (10x^5 - 5x^4 - 18x + 9) =$

$$= (x+1) \cdot (2x-1) \cdot (5x^4 - 9) =$$

fattorizzazione in
irriducibili
in $\mathbb{Z}[x]$ e $\mathbb{Q}[x]$

$$= (x+1) \cdot (2x-1) \cdot (\sqrt{5} \cdot x^2 - 3)(\sqrt{5} \cdot x^2 + 3) =$$

in $\mathbb{R}[x]$

$$= (x+1) \cdot (2x-1) \cdot (\sqrt[4]{5} \cdot x - \sqrt{3})(\sqrt[4]{5} \cdot x + \sqrt{3}) \cdot (\sqrt{5} \cdot x^2 + 3) =$$

$$= (x+1)(2x-1)(\sqrt[4]{5} \cdot x - \sqrt{3})(\sqrt[4]{5} \cdot x + \sqrt{3}) \cdot (\sqrt[4]{5} \cdot x + i\sqrt{3})(\sqrt[4]{5} \cdot x - i\sqrt{3})$$

Da questo segue anche che

in $\mathbb{C}[x]$

$$\{\text{radici di } p(x)\} =$$

in $\mathbb{R} (\in \mathbb{C}, \notin \mathbb{Q})$

$$= \left\{ -1, +\frac{1}{2}, \alpha_+ := \frac{\sqrt{3}}{\sqrt[4]{5}}, \alpha_- := -\frac{\sqrt{3}}{\sqrt[4]{5}}, \beta_+ := i \cdot \frac{\sqrt{3}}{\sqrt[4]{5}}, \beta_- := -i \cdot \frac{\sqrt{3}}{\sqrt[4]{5}} \right\}$$

in $\mathbb{Q} (\in \mathbb{R}, \in \mathbb{C})$ in $\mathbb{C} (\notin \mathbb{Q}, \notin \mathbb{R})$

(b) Dall'analisi in (a) - in particolare, dalla descrizione dell'insieme delle radici di $p(x)$ - si trova che:

$$\begin{aligned}
 \mathbb{Q}_{p(x)} &= \mathbb{Q}(-1, +\frac{1}{2}, \alpha_+, \alpha_-, \beta_+, \beta_-) = \\
 &= \mathbb{Q}(\alpha_+, \alpha_-, \beta_+, \beta_-) = \\
 &= \mathbb{Q}\left(\frac{\sqrt{3}}{\sqrt[4]{5}}, -\frac{\sqrt{3}}{\sqrt[4]{5}}, i\frac{\sqrt{3}}{\sqrt[4]{5}}, -i\frac{\sqrt{3}}{\sqrt[4]{5}}\right) = \\
 &= \mathbb{Q}\left(\frac{\sqrt{3}}{\sqrt[4]{5}}, i\right)
 \end{aligned}$$

$\nearrow \in \mathbb{Q}$ $\nearrow \notin \mathbb{Q}$

con

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\frac{\sqrt{3}}{\sqrt[4]{5}}\right) \subseteq \mathbb{Q}\left(\frac{\sqrt{3}}{\sqrt[4]{5}}, i\right) = \mathbb{Q}_{p(x)}$$

$\uparrow$ grado 4 $\uparrow$ grado 2

e quindi, per moltiplicatività del grado,

$$\boxed{[\mathbb{Q}_{p(x)} : \mathbb{Q}] = 4 \cdot 2 = 8}$$

$$\begin{aligned}
 \mathbb{R}_{p(x)} &= \mathbb{R}(-1, +\frac{1}{2}, \alpha_+, \alpha_-, \beta_+, \beta_-) = \mathbb{R}(\beta_+, \beta_-) = \\
 &= \mathbb{R}(\beta_+) = \mathbb{R}(\beta_-) = \mathbb{R}(i)
 \end{aligned}$$

$\nearrow \in \mathbb{R}$ $\nearrow \notin \mathbb{R}$

quindi $\boxed{[\mathbb{R}_{p(x)} : \mathbb{R}] = [\mathbb{R}(i) : \mathbb{R}] = 2}$

INFINE

$\mathbb{C}_{p(x)} = \mathbb{C}$ perché $\mathbb{C}$ contiene tutte le radici di $p(x)$, quindi

$$[\mathbb{C}_{p(x)} : \mathbb{C}] = [\mathbb{C} : \mathbb{C}] = 1$$

(c) Dai risultati in (b) abbiamo che

$$|\mathcal{G}_{p(x)}^{\mathbb{Q}}| = [\mathbb{Q}_{p(x)} : \mathbb{Q}] = 8$$

$$|\mathcal{G}_{p(x)}^{\mathbb{R}}| = [\mathbb{R}_{p(x)} : \mathbb{R}] = 2$$

$$|\mathcal{G}_{p(x)}^{\mathbb{C}}| = [\mathbb{C}_{p(x)} : \mathbb{C}] = 1$$

da cui segue che:

$$\mathcal{G}_{p(x)}^{\mathbb{C}} = \{\text{id}_{\mathbb{C}_{p(x)}=\mathbb{C}}\}$$

$$\mathcal{G}_{p(x)}^{\mathbb{R}} = \left\{ \text{id}_{\mathbb{R}_{p(x)}=\mathbb{R}}, \sigma = \text{conjugazione in } \mathbb{C} \right\}$$

$(a+ib) \xrightarrow{\sigma} a-ib$

mentre la descrizione di $\mathcal{G}_{p(x)}^{\mathbb{Q}}$ richiede un'analisi più fine.

Ripensiamo $\mathbb{Q}_{p(x)} = \mathbb{Q}(\sqrt[3]{4/\sqrt{5}}, i)$ come

ottenuto dalla torre di estensioni

$$\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(i, \sqrt[4]{3/5})$$

con gradi

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2 \quad \text{perché } i \text{ ha}$$

polinomio minimo $x^2 + 1$ su $\mathbb{Q}$

e

$$[\mathbb{Q}(i, \sqrt[4]{3/5}) : \mathbb{Q}] = 4 \quad \text{perché } \alpha_+ := \frac{\sqrt[4]{3}}{\sqrt[4]{5}}$$

ha polinomio minimo $x^4 - 3$

(si vede dalla fattorizzazione di $5x^4 - 3$ in $\mathbb{C}[x]$)

ORA $\text{Gal}(\mathbb{Q}(i) : \mathbb{Q}) = \langle \sigma' \rangle \cong \mathbb{Z}_2$ con

$$\sigma' : \mathbb{Q}(i) \rightarrow \mathbb{Q}(i), \quad a + ib \mapsto a - ib$$

che si estende canonicamente a $\sigma \in G_{\mathbb{Q}(i, \alpha_+)}^{\mathbb{Q}}$

data da

$$\begin{array}{ccc} \mathbb{Q}(i, \alpha_+) & \xrightarrow{\sigma} & \mathbb{Q}(i, \alpha_+) \\ i \mapsto & \longrightarrow & \sigma(i) = \sigma'(i) = -i \\ \alpha_+ \mapsto & \longrightarrow & \sigma(\alpha_+) = \alpha_+ \end{array}$$

(cioè $\sigma \in \text{Gal}(\mathbb{Q}(i, \alpha_+) / \mathbb{Q}(\alpha_+))$)

INOLTRE α_+ è radice di $x^4 - 3/5$,

tutte le radici di $(x^4 - 3/5)$ sono della forma

$\omega_4^k \cdot \alpha_+$ con $k \in \{0, 1, 2, 3\}$, $\omega_4 =$ radice primitiva
4^a di 1,

MA i è una tale radice ω_4 ,

così $\{\text{radici di } x^4 - 9/5\} = \{\alpha_+, i\alpha_+, -\alpha_+, -i\alpha_+\}$

e $\exists \rho \in \text{Gal}(\mathbb{Q}(i, \alpha_+)/\mathbb{Q}(i))$ dato da

$$\rho: \mathbb{Q}(i, \alpha_+) = (\mathbb{Q}(i))(\alpha_+) \longrightarrow \mathbb{Q}(i, \alpha_+)$$

$$\alpha_+ \longmapsto \rho(\alpha_+) = i \cdot \alpha_+$$

$$\hat{q} \longmapsto \rho(\hat{q}) = \hat{q}, \quad \forall \hat{q} \in \mathbb{Q}(i)$$

con $\langle \rho \rangle \cong (\mathbb{Z}_4; +) = \text{gruppo ciclico di ordine 4}$

ORA, siccome $\rho|_{\mathbb{Q}(i)} = \text{id}_{\mathbb{Q}(i)}$, si ha

$$\langle \rho \rangle \cap \langle \sigma \rangle = \{\text{id}_{\mathbb{Q}_{p(x)}}\} \text{ in } \mathcal{G}_{p(x)}^{\mathbb{Q}}$$

con $|\langle \rho \rangle| = 4$, $|\langle \sigma \rangle| = 2$,

QUINDI $\mathcal{G}_{p(x)}^{\mathbb{Q}} \supseteq \langle \rho \rangle \cdot \langle \sigma \rangle$

$$\text{con } |\langle \rho \rangle \cdot \langle \sigma \rangle| = |\langle \rho \rangle \times \langle \sigma \rangle| = 4 \cdot 2 = 8$$

$$\text{e siccome è } |\mathcal{G}_{p(x)}^{\mathbb{Q}}| = [\mathbb{Q}_{p(x)} : \mathbb{Q}] = 8$$

$$\text{è sicuramente } \mathcal{G}_{p(x)}^{\mathbb{Q}} = \langle \rho \rangle \cdot \langle \sigma \rangle \cong \langle \rho \rangle \times \langle \sigma \rangle$$

$$\text{così } \mathcal{G}_{p(x)}^{\mathbb{Q}} \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \text{ intrinsecamente}$$

INOLTRE, osserviamo che

$$\langle e \rangle \trianglelefteq G_{p(x)}^{\mathbb{Q}} \quad (\text{sottogruppo normale})$$

perché

$$\langle e \rangle = \text{Gal}(\mathbb{Q}(i, \alpha_+)/\mathbb{Q}(i)) \leq \text{Gal}(\mathbb{Q}(i, \alpha_+)/\mathbb{Q})$$

e nella torre $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(i, \alpha_+)$

la sottestensione $\mathbb{Q} \subseteq \mathbb{Q}(i)$ è normale

oppure, più semplicemente,

perché $\langle e \rangle$ è un sottogruppo in $G_{p(x)}^{\mathbb{Q}}$
di di

$$G_{p(x)}^{\mathbb{Q}} : \langle e \rangle = \frac{|G_{p(x)}^{\mathbb{Q}}|}{|\langle e \rangle|} = \frac{8}{4} = 2$$

e, in qualunque gruppo, ogni sottogruppo di indice 2 è sempre normale.

ALLORA da $G_{p(x)}^{\mathbb{Q}} \cong \langle e \rangle \times \langle \sigma \rangle$

con $\langle \sigma \rangle \leq G_{p(x)}^{\mathbb{Q}}$ e $\langle e \rangle \trianglelefteq G_{p(x)}^{\mathbb{Q}}$

segue che $G_{p(x)}^{\mathbb{Q}} = \langle e \rangle \rtimes_{\Phi} \langle \sigma \rangle \cong \mathbb{Z}_4 \rtimes_{\Phi} \mathbb{Z}_2$
prodotto semidiretto di $\langle \sigma \rangle$ con $\langle e \rangle$
con $\Phi: \langle \sigma \rangle \rightarrow \text{Aut}_G(\langle e \rangle)$

Per capire com'è fatto il prodotto
 semidiretto (in breve, chiamo il
 morfismo di gruppi $\Phi: \langle \sigma \rangle \longrightarrow \text{Aut}_G(\langle e \rangle)$)
 calcoliamo $\sigma \circ \rho \circ \sigma^{-1}$ in $G_{p(k)}$. Si ha

$$\sigma \circ \rho \circ \sigma^{-1}: \begin{cases} i \xrightarrow{\sigma^{-1}} -i \xrightarrow{\rho} -i \xrightarrow{\sigma} i \\ \alpha_+ \xrightarrow{\sigma^{-1}} \alpha_+ \xrightarrow{\rho} i\alpha_+ \xrightarrow{\sigma} -i\alpha_+ \end{cases}$$

con cui

$$\rho^3 = \rho^{-1}: \begin{cases} i \xrightarrow{\rho} i \xrightarrow{\rho} i \xrightarrow{\rho} i \\ \alpha_+ \xrightarrow{\rho} i\alpha_+ \xrightarrow{\rho} i^2\alpha_+ = -\alpha_+ \xrightarrow{\rho} -i\alpha_+ \end{cases}$$

con cui $\sigma \circ \rho \circ \sigma^{-1} = \rho^{-1}$

dunque è

$$\Phi: \langle \sigma \rangle \longrightarrow \text{Aut}_G(\langle e \rangle)$$

$$\begin{array}{ccc} \text{id}_{Q_{p(k)}} & \xrightarrow{\quad} & \text{id}_{\langle e \rangle} \\ \sigma & \xrightarrow{\quad} & \left(\begin{array}{ccc} \langle e \rangle & \xrightarrow{\Phi(\sigma)} & \langle e \rangle \\ \rho^k & \xrightarrow{\quad} & \sigma \circ \rho^k \circ \sigma^{-1} = \rho^{-k} \end{array} \right) \end{array}$$

è dato da $\Phi(\text{id}_{Q_{p(k)}}) = \text{id}_{\langle e \rangle}$

e $\Phi(\sigma) = (\rho^k \xrightarrow{\quad} \rho^{-k})$

PERTANTO, nella identificazione

isemistia $G_{p(x)}^{\mathbb{Q}} \simeq \langle e \rangle \times \langle \sigma \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$

la struttura di prodotto semidiretto (non banale!)

di $G_{p(x)}^{\mathbb{Q}} \cong \langle e \rangle \rtimes_{\Phi} \langle \sigma \rangle \cong \mathbb{Z}_4 \rtimes_{\Phi} \mathbb{Z}_2$

è descritta da

$$(e^h, \sigma^a) \cdot (e^k, \sigma^b) = (e^{h+\Phi(\sigma^a)(e^k)}, \sigma^{a+b}) = \\ = (e^{h-a \cdot k}, \sigma^{a+b})$$

per $\langle e \rangle \rtimes_{\Phi} \langle \sigma \rangle$, e da

$$(\bar{h}, \bar{a}) \cdot (\bar{k}, \bar{b}) = (\overline{h-a \cdot k}, \bar{a} + \bar{b})$$

per $\mathbb{Z}_4 \rtimes_{\Phi} \mathbb{Z}_2 \quad (\forall \bar{a} \in \mathbb{Z}_4, \forall \bar{b} \in \mathbb{Z}_2)$