"ALGEBRA 2"

– scritto del 15 Luglio 2020 –

— · —

$\boxed{1}$ $\boxed{\text{Hp:}}$ Γ gruppo abeliano di ordine $|\Gamma| = p^e$, con p primo, $e \in \mathbb{N}_+$.

$(\star)$ $\forall H, K \leq G : |H| = |K|$, si ha $H \cong K$.

$\boxed{\text{Th:}}$ Determinare la struttura di Γ a meno di isomorfismi.

Soluzione:

Per i risultati di classificazione dei gruppi abeliani finiti, Γ è della forma

$$\Gamma = \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}} = \bigtimes_{k=1}^{n} \mathbb{Z}_{p^{e_k}}$$

con $n \in \mathbb{N}_+$, $e_1, \dots, e_n \in \mathbb{N}_+$, $e_1 \geq \cdots \geq e_n$, $e_1 + \cdots + e_n = e$.

1° CASO: SE $n=1$, $\Rightarrow \Gamma = \mathbb{Z}_{p^e}$ è ciclico, e allora sappiamo che per ogni divisore d di $|\Gamma|$ esiste 1! sottogruppo di Γ di ordine d: in particolare, vale la $(\star)$ — con "=" al posto di "≅" — e non c'è problema.

DUNQUE $(e_1, \ldots, e_n) = e$, CIOÈ
$\Gamma \cong \mathbb{Z}_{p^e}$, è una possibilità sempre legittima.

2° CASO: SE $n \neq 1$, $\Rightarrow \Gamma$ non è ciclico.

Consideriamo due sottocasi:

$(2\text{-}1)$: $\nexists\ k \in \{1, \ldots, n-1\} : e_k \geq 2$;

ALLORA è $e_k = 1 \ \forall k = 1, \ldots, n$, $\Rightarrow$

$\Rightarrow (e_1, \ldots, e_n) = (1, \ldots, 1) \Rightarrow$

$$\Rightarrow \Gamma \cong \underbrace{\mathbb{Z}_{p^1} \times \cdots \times \mathbb{Z}_{p^1}}_{e} = \mathbb{Z}_p^{\times e}$$

In tal caso se $\Gamma' \leq \Gamma$ con $|\Gamma'| = p^{e'}$ allora chiaramente è $\Gamma' \cong \mathbb{Z}_p^{\times e'}$, quindi vale la $(\star)$

$\underline{(2.2)}$: $\exists\ k \in \{1, \dots, n-1\} : e_k \geq 2$

ALLORA $\mathbb{Z}_{p^{e_k}}$ contiene un sottogruppo H' t.c. $|H'| = p^2$, e un altro sottogruppo K' t.c. $|K'| = p$;

INOLTRE $\mathbb{Z}_{p^{e_{k+1}}}$ contiene un sottogruppo K'' t.c. $|K''| = p$. $\Rightarrow$

$\Rightarrow$ $\mathbb{Z}_{p^{e_k}} \times \mathbb{Z}_{p^{e_{k+1}}}$ contiene i due sottogruppi $\dot{H} := H' \times \{\bar{0}\}$ e $\dot{K} := K' \times K''$; per essi si ha

$|\dot{H}| = p^2 = p \cdot p = |K'| \cdot |K''| = |K' \times K''| = |\dot{K}|$

dunque, $|\dot{H}| = |\dot{K}|$,

$\underline{\text{MA}}$ $\dot{H} \cong H' \cong \mathbb{Z}_{p^2}$ perché H' è sottogruppo del gruppo ciclico $\mathbb{Z}_{p^{e_k}}$ e come tale è a sua volta ciclico; invece $\dot{K} := K' \times K'' \cong \mathbb{Z}_p \times \mathbb{Z}_p$ perché $|K'| = |K''| = p$ implica $K' \cong \mathbb{Z}_p \cong K''$. Così $\dot{H} \cong \mathbb{Z}_{p^2} \ncong \mathbb{Z}_p \times \mathbb{Z}_p \cong \dot{K}$

INFINE, consideriamo in Γ i sottogruppi H e K corrispondenti ai sottogruppi

$$\cdots \times \{\bar{0}\} \times \underset{(k)}{H'} \times \underset{(k+1)}{\{\bar{0}\}} \times \{\bar{0}\} \times \cdots \leq \bigtimes_{h=1}^{n} \mathbb{Z}_{p^{e_h}}$$

$$\cdots \times \{\bar{0}\} \times \underset{(k)}{K'} \times \underset{(k+1)}{K''} \times \{\bar{0}\} \times \cdots \leq \bigtimes_{h=1}^{n} \mathbb{Z}_{p^{e_h}}$$

Allora $H, K \leq \Gamma$, e ovviamente

$$H \cong H' \times \{0\} =: \dot{H}, \quad K \cong K' \times K'' =: \dot{K}$$

così $|H| = |\dot{H}| = p^2 = |\dot{K}| = |K|$,

cioè $|H| = |K|$,

<u>MA</u> $H \cong \dot{H}' \ncong \dot{K} \cong K$,

cioè $H \ncong K$, sebbene sia $|H| = |K|$.

PERTANTO questi esempi di H e K ci mostrano che Γ <u>non</u> soddisfa la condizione $(\star)$. Viceversa, <u>se</u> sappiamo a priori che Γ gode della $(\star)$, allora quanto visto dimostra che <u>non</u> si verifica il CASO (<u>2.2</u>).

CONCLUSIONE, i gruppi Γ del tipo in esame sono tutti e soli quelli per cui si verifica il caso $\underline{1}$ o il caso $\underline{(2.2)}$, cioè

$$\Gamma \cong \mathbb{Z}_{p^e}$$

oppure $\Gamma \cong \mathbb{Z}_p^{\times e}$. $\square$

$\boxed{2}$ $\boxed{\text{Hp:}}$ A è anello commutativo unitario, $I \trianglelefteq A$,

$$I[x] := \left\{ p(x) = \sum_{k=0}^{n} a_k x^k \in A[x] \;\middle|\; a_k \in I, \forall k = 0, \dots, n \right\}$$

$\boxed{\text{Th:}}$ (a) $I[x] \trianglelefteq A[x]$

(b) $I[x] = (I)_{A[x]} :=$ ideale di $A[x]$ generato da I

(c) I è primo $\Rightarrow$ $I[x]$ è primo

(d) I è massimale $\not\Rightarrow$ $I[x]$ è massimale (dare un controesempio esplicito).

Soluzione:

(a) $\exists$ morfismo di anelli

$$\varphi : A[x] \longrightarrow (A/I)[x]$$
$$\sum_{k=0}^{n} a_k x^k \longmapsto \sum_{k=0}^{n} (a_k + I)\, x^k$$

tale che $I[x] = \mathrm{Ker}(\varphi) \trianglelefteq A[x]$;

perciò $I[x] \trianglelefteq A[x]$, q.e.d.

(b) Per definizione, $(I)_{A[x]}$ è il minimo (per "$\subseteq$") ideale di $A[x]$ che contenga I.

ORA, $\forall\, J \trianglelefteq A[x]$ t.c. $J \supseteq I$ si ha

$J \supseteq I,\ J \trianglelefteq A[x] \implies J \supseteq I \cdot x^k \quad \forall\, k \in \mathbb{N} \implies$

$\implies J \supseteq \sum_{k=0}^{n} I x^k, \quad \forall\, n \in \mathbb{N}, \implies$

$\implies J \supseteq I[x]$; $\implies$ PERCIÒ ogni ideale J di $A[x]$ contenente I contiene anche $I[x]$; ma $I[x] \supseteq I$ e $I[x] \trianglelefteq A[x]$ per (a), quindi $I[x]$ è minimo con tali proprietà, quindi

$$I[x] = (I)_{A[x]}, \quad \text{q.e.d.}$$

(c+d) Il morfismo $\varphi : A[x] \longrightarrow (A/I)[x]$

dato in (a) è chiaramente suriettivo;

$\Rightarrow$ dal Teorema Fondamentale di Omomorfismo (per anelli) e da $Ker(\varphi) = I[x]$ ricaviamo che

$$A[x] \big/ I[x] = A[x] \big/ Ker(\varphi) \cong Im(\varphi) = (A/I)[x]$$

dunque $$A[x] \big/ I[x] \cong (A/I)[x]$$

<u>ORA</u>: I primo $\Rightarrow A/I$ dominio $\Rightarrow$

$\Rightarrow (A/I)[x]$ dominio $\Rightarrow$

$\Rightarrow A[x] \big/ I[x]$ dominio $\Rightarrow I[x]$ è primo

il che dimostra la (c).

I massimale $\Rightarrow A/I$ campo $\Rightarrow$

$\Rightarrow (A/I)[x]$ dominio, <u>ma</u> NON campo (mai!), $\Rightarrow A[x] \big/ I[x]$ NON campo $\Rightarrow$

$\Rightarrow I[x]$ NON è massimale.

Per un esempio esplicito, sia

$A := \mathbb{Z}$, $\quad I := 3\mathbb{Z} = (3)$, per cui

$$I[x] = (3\mathbb{Z})[x] = \{ p(x) = \sum_{k=0}^{n} 3c_k x^k \mid c_k \in \mathbb{Z}, \forall k \}$$

tale ideale non è massimale in $\mathbb{Z}[x]$, lo possiamo vedere direttamente osservando che l'ideale

$$J := (3, x) := \{ q(x) = \sum_{k=0}^{n} d_k x^k \mid d_0 \in 3\mathbb{Z}, d_k \in \mathbb{Z}\ \forall k \}$$

ci dà $\quad I[x] \subsetneq J \subsetneq \mathbb{Z}[x]$. $\square$

$\boxed{3}$ $\quad R := \mathbb{Z}[\sqrt{-3}]$

$\boxed{\text{Th:}}$ (a) R è dominio

(b) R è dom. a fattorizzazione.

(c) R è dom. a fattoriz. unica?

Se si, dimostrarlo. Se NO, trovare un irriducibile $q \in R$ che non sia primo.

Soluzione:

(a) 1° metodo: $R := \mathbb{Z}[\sqrt{-3}]$ è isomorfo al sottoanello unitario R' di $\mathbb{C}$ generato da $\sqrt{-3}$ $(\in \mathbb{C})$. Siccome $\mathbb{C}$ è un campo, il suo sottoanello R' è un dominio, e quindi anche R $(\equiv R')$ è un dominio.

<u>2° metodo:</u> $\exists$ un morfismo suriettivo

$$\begin{aligned} \mathbb{Z}[x] &\xrightarrow{\pi} \mathbb{Z}[\sqrt{-3}] \\ p(x) &\longmapsto p(\sqrt{-3}) \end{aligned}$$

con nucleo $\mathrm{Ker}(\pi) = (x^2+3)$, per cui $\mathbb{Z}[\sqrt{-3}] = \mathrm{Im}(\pi) \cong \dfrac{\mathbb{Z}[x]}{\mathrm{Ker}(\pi)} = \dfrac{\mathbb{Z}[x]}{(x^2+3)}$

Il polinomio x^2+3 in $\mathbb{Z}[x]$ è monico (quindi primitivo) e irriducibile in $\mathbb{Q}[x]$ - perché $\nexists$ radici di x^2+3 in $\mathbb{Q}$ - quindi x^2+3 è anche irriducibile in $\mathbb{Z}[x]$. Ma $\mathbb{Z}[x]$ è un dominio a fattorizzazione unica (perché lo è $\mathbb{Z}$, e per il Teorema di Trasporto), quindi ogni suo irriducibile è primo, onde il polinomio x^2+3 è primo, $\Rightarrow$

$\Rightarrow$ l'ideale principale $(x^2+3)\cdot\mathbb{Z}[x]$ è primo, $\Rightarrow$ l'anello quoziente

$$\frac{\mathbb{Z}[x]}{(x^2+3)\,\mathbb{Z}[x]} \qquad \left(\cong \mathbb{Z}[\sqrt{-3}\,]\right) \text{ è}$$

un dominio, $\Rightarrow$ $\mathbb{Z}[\sqrt{-3}\,]$ è dominio.

(b) La funzione

$$v : \mathbb{Z}[\sqrt{-3}\,] \longrightarrow \mathbb{N} \amalg \{-\infty\}$$
$$a+b\sqrt{-3} \longmapsto a^2+3b^2$$

ha la "proprietà moltiplicativa", cioè

$$v(\zeta'\cdot\zeta'') = v(\zeta')\cdot v(\zeta'') \qquad (*)$$
$$\forall\, \zeta', \zeta'' \in \mathbb{Z}[\sqrt{-3}\,]$$

(pensando a $\mathbb{Z}[\sqrt{-3}\,] \subseteq \mathbb{C}$, tale v è la restrizione a $\mathbb{Z}[\sqrt{-3}\,]$ della norma sui numeri complessi).

Dunque v è una "funzione di valutazione" per $\mathbb{Z}[\sqrt{-3}\,]$, e pertanto $\mathbb{Z}[\sqrt{-3}\,]$ è un dominio a fattorizzazione, q.e.d.

(e) $R := \mathbb{Z}[\sqrt{-3}]$ NON è un dominio a fattorizzazione unica, in quanto contiene l'elemento $q = 2$ che è irriducibile <u>ma</u> NON primo.

<u>INFATTI</u>:

(I) $q := 2$ è irriducibile in R.

Infatti, se $q = \alpha \cdot \beta$ è una fattorizzazione, dalla (*) abbiamo che

$$4 = 2^2 = \nu(2) = \nu(\alpha \cdot \beta) \overset{(*)}{=} \nu(\alpha) \cdot \nu(\beta) \Rightarrow$$

$$\Rightarrow (\nu(\alpha), \nu(\beta)) \in \{(1,4), (2,2), (4,1)\}$$

<u>MA</u> $(\nu(\alpha), \nu(\beta)) = (2,2)$ è impossibile,

perché $\alpha = x + y\sqrt{-3}$ (con $x, y \in \mathbb{Z}$) $\Rightarrow$

$$\Rightarrow \nu(\alpha) = \nu(x + y\sqrt{-3}) = x^2 + 3 \cdot y^2 \boxed{\neq 2}$$

QUINDI è $(\nu(\alpha), \nu(\beta)) \in \{(1,4), (4,1)\}$,

CIOÈ $\nu(\ ) = 1$ o $\nu(\ ) =$, $\Rightarrow$

$\Rightarrow$ (poiché $x^2 + 3y^2 = 1 \iff x = \pm 1,\ y = 0$)

$$\alpha = \pm 1 \quad \text{o} \quad \beta = \pm 1 \Rightarrow$$

$\Rightarrow$ la fattorizzazione $q = \alpha \cdot \beta$ è banale.

(II) $q := 2$ NON è primo in R.

Infatti, abbiamo

$$q := 2 \mid 2 \cdot 2 = 4 = 1^2 + 3 \cdot 1^2 = (1+\sqrt{-3})(1-\sqrt{-3}),$$

così $q := 2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$

MA $q := 2 \nmid (1 \pm \sqrt{-3})$

in quanto $\forall\ \beta = x + y\sqrt{-3} \in R$ si ha

$$q \cdot \beta = 2x + 2y\sqrt{-3}, \quad \text{così}$$

$$q \cdot \beta = 1 \pm \sqrt{-3} \iff \begin{cases} 2x = 1 \\ 2y = \pm 1 \end{cases} \quad ⚡ \quad (x, y \in \mathbb{Z})$$

Quindi $q := 2$ divide il prodotto $(1+\sqrt{-3}) \cdot (1-\sqrt{-3}) = 4$ ma NON divide nessuno dei due fattori, $\Rightarrow$

$\Rightarrow$ $q := 2$ NON è primo, q.e.d.

$\boxed{4}$ $\mathbb{K} := \mathbb{Q}(\sqrt[3]{7}, \sqrt{3}, i)$

$\boxed{\text{Th:}}$ (a) Calcolare $[\mathbb{K} : \mathbb{Q}]$.

(b) Dimostrare che $\mathbb{K}$ è campo di spezzamento su $\mathbb{Q}$ di $h(x) := (x \quad)(x^2-3)$ e di $k(x) := (x^3-7)(x^2+1)$.

(c) Dimostrare che $G := Gal(\mathbb{K}/\mathbb{Q})$ non è abeliano.

Soluzione:

(a) Per costruzione è $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ e $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, quindi

$d := [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] \in \{2, 4\}$. Ma

$$\underbrace{\mathbb{Q} \underbrace{\subseteq \mathbb{Q}(\sqrt{3})}_{2} \underset{?}{\subseteq} \mathbb{Q}(\sqrt{3}, i)}_{d}, \text{ quindi}$$

$d = 2 \iff ? = 1 \iff \mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3}) \iff$

$\iff i \in \mathbb{Q}(\sqrt{3}) \iff \exists$ radice $\alpha \in \mathbb{Q}(\sqrt{3})$ di x^2+1

MA $\alpha = q_0 + q_1\sqrt{3} \in \mathbb{Q}(\sqrt{3}) \implies$

$$\Rightarrow \quad \alpha^2 = (q_0^2 + 3q_1^2) + 2 q_0 q_1 \sqrt{3} \quad \Rightarrow$$

$\Rightarrow$ [α è radice di x^2+1 $\iff$

$$\iff \alpha^2 + 1 = 0 \iff (q_0^2 + 3q_1 + 1) + 2q_0 q_1 \sqrt{3} = 0$$

$$\iff \begin{cases} q_0^2 + 3q_1^2 + 1 = 0 \\ 2q_0 q_1 = 0 \end{cases} \iff$$

$$\iff \begin{cases} 3q_1^2 + 1 = 0 \\ \quad \text{o} \\ q_0^2 + 1 = 0 \\ q_0 = 0 \\ \quad \text{o} \\ q_1 = 0 \end{cases} \iff \left.\begin{cases} q_1^2 = -3^{-1} & \lightning \\ \quad \text{o} \\ q_0^2 = -1 & \lightning \\ q_0 = 0 \\ \quad \text{o} \\ q_1 = 0 \end{cases}\right]$$

DUNQUE $\not\exists$ radice $\alpha \in \mathbb{Q}(\sqrt{3})$ di x^2+1,

$$\Rightarrow \mathbb{Q}(\sqrt{3}) \subsetneq \mathbb{Q}(\sqrt{3}, i), \Rightarrow$$

$$\Rightarrow [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4.$$

<u>ORA</u> $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, $\Rightarrow$

$$\Rightarrow 3 \mid [\mathbb{Q}(\sqrt{3}, i, \sqrt[3]{2}) =: K : \mathbb{Q}] = [K : \mathbb{Q}]$$

& $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4 \Rightarrow 4 \mid [K : \mathbb{Q}]$

Quindi ~~abbiamo~~

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt[3]{7}) \arrow[dr, dash, "q"] & \\
\mathbb{Q} \arrow[ur, dash, "3"] \arrow[rr, dash, "\partial"] \arrow[dr, dash, "4"'] & & \mathbb{K} \\
 & \mathbb{Q}(\sqrt{3}, i) \arrow[ur, dash, "t"'] &
\end{tikzcd}$$

dove

$\mathbb{K} = \mathbb{Q}(\sqrt[3]{7}, \sqrt{3}, i) =$

$= \left(\mathbb{Q}(\sqrt{3}, i)\right)(\sqrt[3]{7})$ ha grado t su $\mathbb{Q}(\sqrt{3}, i)$ con $t \leq 3$ (= grado di $\sqrt[3]{7}$ su $\mathbb{Q}$). Allora

$$\partial := [\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\sqrt{3}, i)] \cdot [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] =$$

$$= t \cdot 4 \Rightarrow \partial = t \cdot 4$$

&

$$\partial := [\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}(\sqrt[3]{7})] \cdot [\mathbb{Q}(\sqrt[3]{7}) : \mathbb{Q}] =$$

$$= q \cdot 3 \Rightarrow \partial = q \cdot 3$$

Perciò $t \cdot 4 = \partial = q \cdot 3$, con $t \leq 3 \Rightarrow$

$\Rightarrow \boxed{\partial = 3 \cdot 4}$ $(t = 3,\ q = 4)$

cioè $[\mathbb{K} : \mathbb{Q}] = \partial = 3 \cdot 4 = \boxed{12}$

(b) $h(x) := (x^3-7)(x^2-3)$ ha radici

- radici di (x^3-7): $\sqrt[3]{7}$, $\zeta_3\sqrt[3]{7}$, $\zeta_3^2\sqrt[3]{7}$

  con ζ_3 := radice 3ª primitiva di 1

- radici di (x^2-3): $\sqrt{3}$, $-\sqrt{3}$

MA $\quad \zeta_3 = \dfrac{-1 \pm \sqrt{-3}}{2} = \dfrac{-1 \pm i\cdot\sqrt{3}}{2} \in \mathbb{K}$,

$\Rightarrow$ $\mathbb{K}$ contiene ζ_3, e allora

$\mathbb{K} \supseteq \mathbb{Q}_{h(x)}$:= e. d. sp. di $h(x)$ su $\mathbb{Q}$

INOLTRE $\quad \mathbb{Q}(\zeta_3) = \mathbb{Q}(i\cdot\sqrt{3}) \subseteq \mathbb{Q}(i, \sqrt{3})$

ALLORA

$$\mathbb{Q}_{h(x)} = \mathbb{Q}(\sqrt[3]{7}, \zeta_3\cdot\sqrt[3]{7}, \zeta_3^2\sqrt[3]{7}, \sqrt{3}, -\sqrt{3}) =$$

$$= \mathbb{Q}(\sqrt[3]{7}, \zeta_3, \sqrt{3}) = \mathbb{Q}(\sqrt[3]{7}, i\cdot\sqrt{3}, \sqrt{3}) =$$

$$= \mathbb{Q}(\sqrt[3]{7}, i, \sqrt{3}) =: \mathbb{K}, \Rightarrow \mathbb{K} = \mathbb{Q}_{h(x)}, \text{ q.e.d.}$$

ANALOGAMENTE,

$k(x) := (x^3-7)(x^2+1)$ ha radici

$\sqrt[3]{7}$, $\zeta_3\sqrt[3]{7}$, $\zeta_3^2\sqrt[3]{7}$, i, $-i$, $\Rightarrow$

$$\Rightarrow \mathbb{Q}_{k(x)} = \mathbb{Q}(\sqrt[3]{7}, \zeta_3, i) = \mathbb{Q}(\sqrt[3]{7}, i\cdot\sqrt{3}, i) =$$

$$= \mathbb{Q}(\sqrt[3]{7}, \sqrt{3}, i) =: \mathbb{K}, \Rightarrow \mathbb{K} = \mathbb{Q}_{k(x)}, \text{ q.e.d.}$$

(c) Se p.a. $G := Gal(\mathbb{K}/\mathbb{Q})$ fosse abeliano, tutti i suoi sottogruppi sarebbero normali quindi tutte le estensioni intermedie $\mathbb{F} : \mathbb{Q} \subseteq \mathbb{F} \subseteq \mathbb{K}$ sarebbero normali su $\mathbb{Q}$.

<u>INVECE</u> $\exists\ \mathbb{F} := \mathbb{Q}(\sqrt[3]{7})$ t.c.

$\mathbb{F} \subseteq \mathbb{K}$, $\mathbb{F} \supseteq \mathbb{Q}$, <u>MA</u> $\mathbb{F}/\mathbb{Q}$ <u>NON</u> è normale, in quanto $p^{\mathbb{Q}}_{\sqrt[3]{7}}(x) = x^3 - 7$ ha in $\mathbb{F}$ la radice $\sqrt[3]{7}$ ma non le altre!

——— ∘ ———

$\boxed{5}$ $\boxed{\text{Hp:}}$ G gruppo, $|G| = 441$

$\boxed{\text{Th:}}$ (a) Dimostrare che G è prodotto semidiretto, con fattori non banali.

(b) Dimostrare che G è risolubile.

<u>Soluzione:</u>

(a) $|G| = 441 = 49 \cdot 9 = 7^2 \cdot 3^2 \Rightarrow$

$\Rightarrow \exists$ in G dei 7-Sylow e dei 3-Sylow.

$\forall\, p \in \{3, 7\}$, sia $\nu_p := \#\, p$-Sylow in G

<u>ORA</u>: $\nu_3 \in (1+3\mathbb{N}) \cap \{1, 7, 49\} = \{1, 7, 49\}$,

$\nu_7 \in (1+7\mathbb{N}) \cap \{1, 3, 9\} = \{1\} \Rightarrow \nu_7 = 1 \Rightarrow$

$\Rightarrow \exists!$ 7-Sylow K_7 in G, che allora è caratteristico, e in particolare è normale

Sia poi H_3 un 3-Sylow. Allora

$|H_3| = 3^2$, $|K_7| = 7^2$

$|H_3 \cap K_7| \,\big|\, \mathrm{MCD}(3^2, 7^2) = 1 \Rightarrow |H_3 \cap K_7| = 1 \Rightarrow$

$\Rightarrow H_3 \cap K_7 = \{e_G\}$; inoltre

$\mu : H_3 \times K_7 \longrightarrow G \quad (h, k) \longmapsto h \cdot k$

ha immagine $\mathrm{Im}(\mu) = H_3 \cdot K_7 = G$,

perché $H_3 \leq H_3 \cdot K_7$, $K_7 \leq H_3 \cdot K_7$, $\quad H_3 \cdot K_7 \leq G$

(perché $H_3 \leq G$ e $K_7 \trianglelefteq G$), quindi il

teorema di Lagrange ci dà

$$\left.\begin{array}{l} 3^2 = |H_3| \,\big|\, |H_3 \cdot K_7| \\ 7^2 = |K_7| \,\big|\, |H_3 K_7| \end{array}\right\} \Rightarrow 3^2 \cdot 7^2 \,\big|\, |H_3 \cdot K_7| \leq |G| = 3^2 \cdot 7^2 \Bigg\} \Rightarrow H_3 \cdot K_7 = G$$

<u>ALLORA</u>: $\left.\begin{array}{l} H_3 \leq G,\ K_7 \trianglelefteq G \\ H_3 \cap K_7 = \{e_G\},\ H_3 \cdot K_7 = G \end{array}\right\} \Rightarrow G = H_3 \ltimes K_7$ OK

(b) $\exists$ un risultato generale che dice che

$$N \trianglelefteq G, \quad \begin{matrix} N \text{ risolubile} \\ G/N \text{ risolubile} \end{matrix} \models\Rightarrow G \text{ risolubile} \quad (\bullet)$$

<u>ORA</u>, per il gruppo G in esame

sia $N := K_7$; allora $N := K_7 \trianglelefteq G$,

e $|K_7| = 7^2 = p^2$ con $p := 7$ $\underbrace{\text{primo}}$ $\Rightarrow$

$\Rightarrow K_7$ è abeliano, $\Rightarrow N := K_7$ è risolubile

Inoltre, $G = H_3 \ltimes K_7 \Rightarrow$

$$\Rightarrow G/N = (H_3 \ltimes K_7)/K_7 \cong H_3,$$

con $|H_3| = 3^2 = p^2$ con $p := 3$ $\underbrace{\text{primo}}$ $\Rightarrow$

$\Rightarrow H_3$ è abeliano $\Rightarrow H_3$ è risolubile $\Rightarrow$

$\Rightarrow G/N \; (\cong H_3)$ è risolubile.

ALLORA applicando $(\bullet)$ otteniamo che G è risolubile, q.e.d. $\square$