ALGEBRA 2 — 2007/2008

Prof. Fabio Gavarini

Sessione estiva — prova scritta del 17 Giugno 2008

Svolgimento completo

N.B.: lo svolgimento qui presentato è chilometrico... Questo non vuol dire *che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba essere altrettanto lungo. Semplicemente, questo lo è perché si è colta l'occasione per spiegare — anche in diversi modi, con lunghe digressioni, ecc. ecc. — in dettaglio e con dovizia di particolari tutti gli aspetti della teoria toccati in maggiore o minore misura dal testo in esame.*

. . . . . * . . . . . .

[1] — Si consideri l'anello quoziente $R := \mathbb{Z}[i]\Big/\big(3-i\,,\,2\big)$.

(a) Calcolare tutti i divisori di zero di R .

(b) Determinare se esista in R l'inverso dell'elemento $\overline{2+i}$. In caso negativo, spiegare perché tale inverso non esista; in caso affermativo, calcolare esplicitamente tale inverso.

(c) Determinare se esista in R l'inverso dell'elemento $\overline{5+i}$. In caso negativo, spiegare perché tale inverso non esista; in caso affermativo, calcolare esplicitamente tale inverso.

<u>Soluzione</u>: Poiché l'anello $\mathbb{Z}[i]$ è un dominio a ideali principali (in quanto è anche un dominio euclideo!), in particolare l'ideale $I := \big(3-i\,,\,2\big)$ sarà principale, cioè del tipo $I = (d\,)$, dove necessariamente si avrà $d = M.C.D.\big(3-i\,,\,2\big)$, che può essere calcolato tramite l'algoritmo euclideo delle divisioni successive. Inoltre, avremo che

$$R := \mathbb{Z}[i]\Big/\big(3-i\,,\,2\big) = \mathbb{Z}[i]\Big/\big(d\big) \text{ è dominio } \iff \text{ è campo } \iff d \text{ è irriducibile in } \mathbb{Z}[i]$$

Perciò, per risolvere il nostro problema, conviene descrivere I tramite il suddetto generatore d, quindi calcoliamo quest'ultimo. L'algoritmo euclideo ci dà

$$\begin{aligned} 3-i &= 2\cdot(1-i) + (1+i) \\ 2 &= (1-i)\cdot(1+i) + 0 \end{aligned}$$

quindi abbiamo $d = M.C.D.\big(3-i\,,\,2\big) = 1+i$. In particolare, $d = 1+i$ è irriducibile in $\mathbb{Z}[i]$: ciò si vede, ad esempio, osservando che la sua valutazione — tramite la norma dei numeri complessi — è $v(1+i) := 1^2+1^2 = 2$ che è un primo in $\mathbb{N}_+$. Pertanto

$$R := \mathbb{Z}[i]\Big/\big(3-i\,,\,2\big) = \mathbb{Z}[i]\Big/\big(1+i\big) \tag{1}$$

è un campo, ed in particolare un dominio. Quindi in R non esistono divisori di zero, il che risolve il punto *(a)*.

Dalla (1) possiamo capire quale campo è R, attraverso i teoremi di isomorfismo (per anelli). La successione di passaggi logici è questa:

$$R \,:=\, \mathbb{Z}[i]\Big/\big(3-i\,,\,2\big) \,=\, \mathbb{Z}[i]\Big/\big(1+i\big) \overset{(I)}{\cong}$$
$$\overset{(I)}{\cong} \Big(\mathbb{Z}[x]\Big/\big(x^2+1\big)\Big)\Bigg/\Big(\big(1+x\,,\,x^2+1\big)\Big/\big(x^2+1\big)\Big) \overset{(II)}{\cong} \mathbb{Z}[x]\Big/\big(1+x\,,\,x^2+1\big) \overset{(III)}{\cong}$$
$$\overset{(III)}{\cong} \Big(\mathbb{Z}[x]\Big/\big(1+x\big)\Big)\Bigg/\Big(\big(1+x\,,\,x^2+1\big)\Big/\big(1+x\big)\Big) \overset{(IV)}{\cong} \mathbb{Z}\Big/2\mathbb{Z} \,=:\, \mathbb{Z}_2$$

in cui abbiamo sfruttato i seguenti fatti:

— esiste un isomorfismo $\Phi : \mathbb{Z}[x]\Big/\big(x^2+1\big) \overset{\cong}{\hookrightarrow\!\!\!\!\rightarrow} \mathbb{Z}[i]$ dato da $\overline{f(x)} \mapsto f(i)$; esso a sua volta è indotto dall'epimorfismo $\Phi' : \mathbb{Z}[x] \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}[i]$ dato da $f(x) \mapsto f(i)$. Poiché $\Phi'\Big(\big(1+x\,,\,x^2+1\big)\Big) = \big(1+i\,,\,i^2+1\big) = \big(1+i\big)$, si ha anche $\Phi\Big(\big(1+x\,,\,x^2+1\big)\Big/\big(x^2+1\big)\Big) = \big(1+i\big)$. Per questa ragione, Φ induce dunque un isomorfismo il cui inverso è proprio quello in (I) qui sopra.

— il Teorema del Doppio Quoziente ci dà l'isomorfismo in (II) qui sopra.

— ancora il Teorema del Doppio Quoziente, applicato "in senso inverso", ci dà l'isomorfismo in (III).

— esiste un epimorfismo $\Psi' : \mathbb{Z}[x] \longrightarrow\!\!\!\!\!\rightarrow \mathbb{Z}$ dato da $p(x) \mapsto p(-1)$. Esso induce un isomorfismo $\Psi : \mathbb{Z}[x]\Big/\big(1+x\big) \overset{\cong}{\hookrightarrow\!\!\!\!\rightarrow} \mathbb{Z}$ dato da $\Psi\Big(\overline{p(x)}\Big) = \Psi'\big(p(x)\big) = p(-1)$. Ora, poiché

$$\Psi'\Big(\big(1+x\,,\,x^2+1\big)\Big) \,=\, \big(1+(-1)\,,\,(-1)^2+1\big) \,=\, \big(2\big) \,=\, 2\,\mathbb{Z}$$

tramite l'isomorfismo Ψ abbiamo anche

$$\Psi\Big(\,\overline{\big(1+x\,,\,x^2+1\big)}\,\Big) \,=\, \big(1+(-1)\,,\,(-1)^2+1\big) \,=\, \big(2\big) \,=\, 2\,\mathbb{Z}$$

e quindi Ψ induce anche l'isomorfismo (IV) qui sopra.

In conclusione, R è (isomorfo a) il campo $\mathbb{Z}_2$.

Ripercorrendo la catena di isomorfismi considerata qui sopra, si trova che in definitiva l'isomorfismo risultante $R = \mathbb{Z}[i]\Big/\big(1+i\big) \overset{\cong}{\hookrightarrow\!\!\!\!\rightarrow} \mathbb{Z}_2$ è dato semplicemente da

$$R \,=\, \mathbb{Z}[i]\Big/\big(1+i\big) \overset{\cong}{\hookrightarrow\!\!\!\!\rightarrow} \mathbb{Z}_2\,, \quad R \ni \big[(a+i\,b)\big]_{(1+i)} \,\mapsto\, [a]_2 - [b]_2 \,=\, [a]_2 + [b]_2 \,\in \mathbb{Z}_2 \qquad (2)$$

dove la notazione $[x]_q$ indica la classe di x modulo q in un anello quoziente del tipo $A\Big/(q)$ con $x, q \in A$, e abbiamo tenuto conto del fatto che in $\mathbb{Z}_2$ si ha $[u]_2 - [v]_2 \,=\, [u]_2 + [v]_2$.

In alternativa, la (2) si può ottenere anche così.

Per cominciare, poiché $\big[(1+i)\big]_{(1+i)} = \big[0\big]_{(1+i)}$ in $R = \mathbb{Z}[i]\Big/\big(1+i\big)$, si ha subito

$$\big[2\big]_{(1+i)} \,=\, \big[(1+i)\cdot(1-i)\big]_{(1+i)} \,=\, \big[(1+i)\big]_{(1+i)} \cdot \big[(1-i)\big]_{(1+i)} \,= \\ =\, \big[0\big]_{(1+i)} \cdot \big[(1-i)\big]_{(1+i)} \,=\, \big[0\big]_{(1+i)}$$

Pertanto se $a, a' \in \mathbb{Z}$ verificano $\big[a\big]_2 = \big[a'\big]_2 \in \mathbb{Z}_2$ allora si ha anche $[a]_{(1+i)} = \big[a'\big]_{(1+i)} \in R$. Ma allora si ha pure $[i]_{(1+i)} = [-1]_{(1+i)} = [1]_{(1+i)}$. Possiamo allora concludere che

$$R \ni \big[(a+i\,b)\big]_{(1+i)} \,=\, [a]_{(1+i)} + [i]_{(1+i)} \cdot [b]_{(1+i)} \,=\, [a]_{(1+i)} + [b]_{(1+i)} \,\cong\, [a]_2 + [b]_2 \,\in \mathbb{Z}_2$$

che ci ridà la (2).

Ora, la (2) in particolare dà

$$\big[(2+i)\big]_{(1+i)} \,\cong\, [2]_2 + [1]_2 = [1]_2 \,\in \mathbb{Z}_2\,, \quad \big[(5+i)\big]_{(1+i)} \,\cong\, [5]_2 + [1]_2 = [0]_2 \,\in \mathbb{Z}_2$$

Perciò l'elemento $\big[(2+i)\big]_{(1+i)}$, risp. $\big[(5+i)\big]_{(1+i)}$, in R è invertibile, risp. non è invertibile, perché nell'isomorfismo $R \cong \mathbb{Z}_2$ corrisponde all'elemento $[1]_2$, risp. $[0]_2$, che è invertibile, risp. non è invertibile.

Per farla più breve, si può ragionare come segue (e questo è il *metodo pratico più semplice*). Operando la divisione euclidea per $(1+i)$ troviamo

$$\big[(2+i)\big]_{(1+i)} \,=\, \big[(1+i)\cdot 1 + 1\big]_{(1+i)} \,=\, \big[(1+i)\big]_{(1+i)} + [1]_{(1+i)} \,= \\ =\, [0]_{(1+i)} + [1]_{(1+i)} \,=\, [1]_{(1+i)}$$

$$\big[(5+i)\big]_{(1+i)} \,=\, \big[(1+i)\cdot(3-i\,2)+0\big]_{(1+i)} \,=\, \big[(1+i)\big]_{(1+i)} \cdot \big[(3-i\,2)\big]_{(1+i)} \,= \\ =\, [0]_{(1+i)} + \big[(3-i\,2)\big]_{(1+i)} \,=\, [0]_{(1+i)}$$

e quindi concludiamo che $\big[(2+i)\big]_{(1+i)} = [1]_{(1+i)}$ è invertibile, e il suo inverso è ovviamente $\big[(2+i)\big]^{-1}_{(1+i)} = [1]^{-1}_{(1+i)} = [1]_{(1+i)}$. Invece, al contrario, $\big[(5+i)\big]_{(1+i)} = [0]_{(1+i)}$ non è invertibile. Questo risolve i punti *(b)* e *(c)*. □

(continua . . .)

[2] — Sia G un gruppo di ordine 20.

(a) Se G è abeliano, calcolarne esplicitamente la struttura (a meno di isomorfismi).

(b) Se G non è abeliano, determinare esplicitamente il numero dei suoi p–sottogruppi di Sylow, per ogni primo p.

(c) Costruire esplicitamente un gruppo G di ordine 20 non abeliano.

Soluzione: *(a)* Se G è abeliano, dal teorema di classificazione dei gruppi abeliani finiti sappiamo che, siccome G ha ordine $20 = 2^2 \cdot 5$, dev'essere necessariamente isomorfo ad uno dei due gruppi seguenti:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \quad , \qquad \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20}$$

In particolare, se si verifica il secondo caso allora G è ciclico.

(b) Per ogni primo p, sia ν_p il numero di p–sottogruppi di Sylow di G. Ora, poiché G ha ordine $20 = 2^2 \cdot 5$, i soli primi che dividono il suo ordine sono 2 e 5: quindi $\nu_2 \geq 1$, $\nu_5 \geq 1$ e $\nu_p = 0$ per ogni primo p diverso da 2 e da 5.

Ogni 2–sottogruppo di Sylow di G è necessariamente abeliano, perché di ordine p^2 con $p = 2$ che è primo. In modo analogo (più semplice), anche ogni 5–sottogruppo di Sylow di G è abeliano, perché di ordine $p = 5$, che è primo.

Quando G è abeliano — caso *(a)* — ogni suo sottogruppo è normale: ciò vale in particolare per tutti i p–sottogruppi di Sylow, che sono tra loro coniugati, e quindi in effetti coincidono (per ciascun p fissato): in altre parole, si ha $\nu_p = 1$ per ogni primo p. Quando invece G *non* è abeliano, *e* tutti i p–sottogruppi di Sylow (per ogni primo p) sono *abeliani*, si ha necessariamente $\nu_p > 1$ per qualche primo p. Infatti, se fosse $\nu_p \leq 1$ per ogni primo p allora tutti i p–Sylow sarebbero normali, unici (per ciascun p), commuterebbero gli uni con gli altri, e G ne sarebbe il prodotto diretto: ma ogni prodotto diretto di gruppi abeliani è a sua volta abeliano, il che darebbe una contraddizione!

Nel nostro caso, dato che i 2–Sylow e i 5–Sylow sono effettivamente abeliani, concludiamo che dev'essere $\nu_2 > 1$ oppure $\nu_5 > 1$ (eventualmente entrambi).

Dalla teoria generale abbiamo anche che

$$\nu_2 \,\Big|\, 5 \,, \quad \nu_2 \equiv 1 \mod 2 \,, \qquad \nu_5 \,\Big|\, 4 \,, \quad \nu_5 \equiv 1 \mod 5 \,,$$

da cui deduciamo che $\nu_2 \in \{1, 5\}$, $\nu_5 \in \{1\}$.

Supponiamo ora che G sia non abeliano. Dato che il caso $(\nu_2, \nu_5) = \{1, 1\}$ corrisponde, per quanto già detto, al caso in cui invece G sia abeliano, abbiamo ora necessariamente $(\nu_2, \nu_5) = \{5, 1\}$. Pertanto G contiene esattamente cinque 2–sottogruppi di Sylow, e un unico 5–sottogruppo di Sylow.

(c) Sia ora G un gruppo di ordine 20 non abeliano. Alla luce di quanto visto nel trattare i punti *(a)* e *(b)*, indichiamo con S_2 uno dei cinque 2–sottogruppi di Sylow di G, e con N_5 il suo unico 5–sottogruppo di Sylow. Per unicità, tale N_5 è sottogruppo *normale* di

G. Inoltre, S_2 e N_5 hanno intersezione banale, perché hanno ordini coprimi (e si applica il Teorema di Lagrange), e allora il prodotto insiemistico

$$S_2 \cdot N_5 \; := \; \big\{ s \cdot n \,\big|\, s \in S_2 \,,\, n \in N_5 \big\}$$

ha esattamente cardinalità $\big|S_2 \cdot N_5\big| = \big|S_2\big| \cdot \big|N_5\big| = 4 \cdot 5 = 20 = \big|G\big|$; quindi $S_2 \cdot N_5 = G$.

Riassumendo, abbiamo (indicando con e_G l'elemento neutro del gruppo G)

$$S_2 \leq G \;, \quad N_5 \trianglelefteq G \;, \quad S_2 \bigcap N_5 = \{e_G\} \;, \quad S_2 \cdot N_5 = G \;.$$

Complessivamente, questo significa che $G = N_5 \rtimes S_2$, cioè G è prodotto semidiretto del sottogruppo S_2 con il sottogruppo normale N_5; tale prodotto si realizza tramite un morfismo di gruppi $\Phi : S_2 \longrightarrow Aut(N_5)$. Quindi, per costruire un esempio di gruppo G di ordine 20 non abeliano dobbiamo costruire i gruppi S_2 e N_5 ed il morfismo Φ; inoltre, tale Φ deve essere *non banale*, altrimenti S_2 commuterebbe con N_5 e il prodotto semidiretto sarebbe un prodotto diretto, che risulterebbe *abeliano*, che è il caso che non ci interessa.

Per i due (sotto)gruppi abbiamo

$$\big|S_2\big| = 2^2 = 4 \implies S_2 \cong Z_2 \times \mathbb{Z}_2 \quad \text{oppure} \quad S_2 \cong Z_4 \;, \qquad \big|N_5\big| = 5 \implies N_5 \cong Z_5 \;.$$

Quindi possiamo *scegliere* di prendere $S_2 := \mathbb{Z}_2 \times \mathbb{Z}_2$ oppure $S_2 := \mathbb{Z}_4$, mentre $N_5 := \mathbb{Z}_5$.

N.B.: nel seguito, con la notazione $[z]_q$ indichiamo l'elemento dell'anello $\mathbb{Z}_q$ che è la classe resto modulo q di $z \in \mathbb{Z}$.

Inoltre, da $N_5 := Z_5$ segue che $Aut(N_5) = Aut(\mathbb{Z}_5) \cong U(\mathbb{Z}_5)$, dove l'isomorfismo (canonico) è dato da

$$\begin{array}{rcl} Aut(N_5) \,=\, Aut(\mathbb{Z}_5) & \xrightarrow{\;\cong\;} & U(\mathbb{Z}_5) \\ \varphi & \longrightarrow & \varphi\big([1]_5\big) \end{array}$$

Viceversa, indicheremo con φ_z la *controimmagine*, in $Aut(\mathbb{Z}_5)$, della classe $[z]_5 \in U(\mathbb{Z}_5)$ rispetto all'isomorfismo di cui sopra. Esplicitamente, ogni automorfismo φ_z è dato da $\varphi_z\big([a]_5\big) := [az]_5$, per ogni $[a]_5 \in \mathbb{Z}_5$.

Si noti anche che $\big(U(\mathbb{Z}_5)\,;\,\cdot\big) \cong \big(\mathbb{Z}_4\,;\,+\big)$: un isomorfismo tra tali gruppi può esser scelto in due (e soltanto due) modi diversi, precisamente

$$\begin{array}{rcl} U(\mathbb{Z}_5) & \xrightarrow{\;\cong\;} & \mathbb{Z}_4 \\ [1]_5 & \longrightarrow & [0]_4 \\ [2]_5 & \longrightarrow & [1]_4 \\ [3]_5 & \longrightarrow & [3]_4 \\ [4]_5 & \longrightarrow & [2]_4 \end{array} \qquad\qquad \begin{array}{rcl} U(\mathbb{Z}_5) & \xrightarrow{\;\cong\;} & \mathbb{Z}_4 \\ [1]_5 & \longrightarrow & [0]_4 \\ [2]_5 & \longrightarrow & [3]_4 \\ [3]_5 & \longrightarrow & [1]_4 \\ [4]_5 & \longrightarrow & [2]_4 \end{array}$$

Tuttavia, *non è necessario* per i nostri scopi presenti fissare un tale isomorfismo.

Da $U(\mathbb{Z}_5) \cong \mathbb{Z}_4$ segue immediatamente che in ogni caso, sia che $S_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, sia che $S_2 = \mathbb{Z}_4$, esiste sempre un morfismo *non banale* $\Phi : S_2 \longrightarrow Aut(\mathbb{Z}_5) \cong U(\mathbb{Z}_5) \cong \mathbb{Z}_4$.

Nel caso $S_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, esiste *un solo* morfismo non banale, precisamente

$$\Phi_\bullet : S_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \xrightarrow{\cong} Aut(\mathbb{Z}_5)$$
$$\big([0]_2,[0]_2\big) \mapsto \varphi_1 \ , \quad \big([1]_2,[0]_2\big) \mapsto \varphi_4 \ , \quad \big([0]_2,[1]_2\big) \mapsto \varphi_4 \ , \quad \big([1]_2,[1]_2\big) \mapsto \varphi_4 \ .$$

Nel caso $S_2 = \mathbb{Z}_4$ invece esistono *esattamente due* morfismi non banali, che corrispondono — componendo Φ con un fissato isomorfismo $Aut(\mathbb{Z}_5) \cong \mathbb{Z}_4$ — ai due soli automorfismi del gruppo $\mathbb{Z}_4$; tali morfismi sono

$$\Phi_{(2)} : S_2 = \mathbb{Z}_4 \xrightarrow{\cong} Aut(\mathbb{Z}_5) \ , \qquad [0]_4 \mapsto \varphi_1 \ , \quad [1]_4 \mapsto \varphi_2 \ , \quad [2]_4 \mapsto \varphi_4 \ , \quad [3]_4 \mapsto \varphi_3$$
$$\Phi_{(3)} : S_2 = \mathbb{Z}_4 \xrightarrow{\cong} Aut(\mathbb{Z}_5) \ , \qquad [0]_4 \mapsto \varphi_1 \ , \quad [1]_4 \mapsto \varphi_3 \ , \quad [2]_4 \mapsto \varphi_4 \ , \quad [3]_4 \mapsto \varphi_2$$

Infatti, ciascuno di essi è univocamente determinato dall'immagine di $[1]_4$, che deve essere un elemento di ordine 4 nel gruppo $Aut(\mathbb{Z}_5)$, e le due sole possibilità per un tale elemento sono appunto φ_2 e φ_3.

Per concludere, richiamiamo brevemente la costruzione generale. Dati due gruppi S, N, ed un morfismo di gruppi $\Phi : S \longrightarrow Aut(N)$, il prodotto semidiretto $N \rtimes_\Phi S$ di S con N tramite Φ è l'insieme prodotto cartesiano $N \times S$ dotato dell'operazione $\star$ così definita:

$$\big(n,s\big) \star \big(n',s'\big) \ := \ \big(n \cdot \Phi(s)(n') \, , \, s \cdot s'\big) \qquad\qquad \forall \ \big(n,s\big), \big(n',s'\big) \in N \times S$$

Scegliendo ora $S := S_2 \in \big\{ \mathbb{Z}_2 \times \mathbb{Z}_2 \, , \, \mathbb{Z}_4 \big\}$ come sopra e $\Phi \in \big\{ \Phi_\bullet \, , \, \Phi_{(2)} \, , \, \Phi_{(3)} \big\}$ secondo i casi, otteniamo i seguenti prodotti semidiretti:

— *primo caso:* $\qquad N_5 \rtimes_{\Phi_\bullet} S_2 \ = \ \mathbb{Z}_5 \times \big(\mathbb{Z}_2 \times \mathbb{Z}_2\big) \qquad$ (come insieme)

con operazione

$$\big([n]_5,([r]_2,[s]_2)\big) \star \big([n']_5,([r']_2,[s']_2)\big) := \Big([n]_5 + \Phi_\bullet\big([r]_2,[s]_2\big)\big([n']_5\big), ([r]_2,[s]_2) + ([r']_2,[s']_2)\big)\Big) =$$
$$= \ \Big([n]_5 + \Phi_\bullet\big([r]_2,[s]_2\big)\big([n']_5\big) \, , \, ([r+r']_2,[s+s']_2)\Big) \ =$$
$$= \ \Big([n]_5 + \varphi_4^{\,1-\delta_{[r]_2,[0]_2}\,\delta_{[r]_2,[0]_2}}\big([n']_5\big) \, , \, ([r+r']_2,[s+s']_2)\Big) \ =$$
$$= \ \Big([n]_5 + \big(\big[4^{1-\delta_{[r]_2,[0]_2}\,\delta_{[r]_2,[0]_2}} n'\big]_5\big) \, , \, ([r+r']_2,[s+s']_2)\Big) \ =$$
$$= \ \Big([n]_5 + \big(\big[(-1)^{1-\delta_{[r]_2,[0]_2}\,\delta_{[r]_2,[0]_2}} n'\big]_5\big) \, , \, ([r+r']_2,[s+s']_2)\Big) \ =$$
$$= \ \Big([n]_5 + \big(\big[(-1)^{1-\delta_{[r]_2,[0]_2}\,\delta_{[r]_2,[0]_2}} n'\big]_5\big) \, , \, ([r+r']_2,[s+s']_2)\Big) \ =$$
$$= \begin{cases} \Big([n]_5 + \big(\big[-n'\big]_5\big) \, , \, ([r+r']_2,[s+s']_2)\Big) & \text{se } \big([r]_2,[s]_2\big) \neq \big([0]_2,[0]_2\big) \\ \Big([n]_5 + \big(\big[n'\big]_5\big) \, , \, ([r+r']_2,[s+s']_2)\Big) & \text{se } \big([r]_2,[s]_2\big) = \big([0]_2,[0]_2\big) \end{cases}$$

— *secondo caso:* $N_5 \rtimes_{\Phi_{(2)}} S_2 \,=\, \mathbb{Z}_5 \times \mathbb{Z}_4$ (come insieme)

con operazione

$$\begin{aligned}\big([n]_5,[s]_4\big)\star\big([n']_5,[s']_4\big) &:= \Big([n]_5+\Phi_{(2)}\big([s]_4\big)\big([n']_5\big),[s]_4+[s']_4\Big) \,= \\ &= \Big([n]_5+\Phi_{(2)}\big([1]_4\big)^s\big([n']_5\big)\,,\,\big[s+s'\big]_4\Big) \,=\, \Big([n]_5+\varphi_2^s\big([n']_5\big)\,,\,\big[s+s'\big]_4\Big) \,= \\ &= \Big([n]_5+\big[2^s n'\big]_5\,,\,\big[s+s'\big]_4\Big) \,=\, \Big(\big[n+2^s n'\big]_5\,,\,\big[s+s'\big]_4\Big)\end{aligned}$$

— *terzo caso:* $N_5 \rtimes_{\Phi_{(3)}} S_2 \,=\, \mathbb{Z}_5 \times \mathbb{Z}_4$ (come insieme)

con operazione

$$\begin{aligned}\big([n]_5,[s]_4\big)\star\big([n']_5,[s']_4\big) &:= \Big([n]_5+\Phi_{(3)}\big([s]_4\big)\big([n']_5\big),[s]_4+[s']_4\Big) \,= \\ &= \Big([n]_5+\Phi_{(3)}\big([1]_4\big)^s\big([n']_5\big)\,,\,\big[s+s'\big]_4\Big) \,=\, \Big([n]_5+\varphi_3^s\big([n']_5\big)\,,\,\big[s+s'\big]_4\Big) \,= \\ &= \Big([n]_5+\big[3^s n'\big]_5\,,\,\big[s+s'\big]_4\Big) \,=\, \Big(\big[n+3^s n'\big]_5\,,\,\big[s+s'\big]_4\Big)\end{aligned}$$

Quelli qui indicati sono in effetti *tutti e soli* — a meno di isomorfismi — i gruppi di ordine 20 non abeliani.

N.B.: la richiesta del testo era molto più ridotta — bastava esporre esplicitamente *uno* qualsiasi dei tre esempi suesposti. □

(continua . . .)

[3] — Sia G un gruppo, e sia A un sottogruppo normale di G che sia anche abeliano.

(a) Dimostrare che l'azione di G su sé stesso per coniugazione induce un'azione $\big(G/A\big) \times A \longrightarrow A\,,\ \big(\overline{g}, a\big) \mapsto \overline{g}.a$, del gruppo quoziente G/A sul gruppo A.

(b) Dimostrare che l'azione di cui in *(a)* è un'azione per automorfismi del gruppo A, cioè

$$\overline{g}.\big(a' \cdot a''\big) \ = \ \big(\overline{g}.a'\big) \cdot \big(\overline{g}.a''\big) \qquad\qquad \forall\ \overline{g} \in G/A\,,\ a', a'' \in A$$

Presentiamo due possibili metodi risolutivi:

<u>*Primo metodo:*</u> Si consideri l'azione di coniugazione $G \times G \longrightarrow G\,,\ (g, \gamma) \mapsto g.\gamma := g\,\gamma\,g^{-1}$, di G su sé stesso. Poiché A è sottogruppo *normale*, tale azione si restringe ad una ben definita applicazione

$$G \times A \longrightarrow A\,, \quad (g, \alpha) \mapsto g.\alpha := g\,\alpha\,g^{-1} \qquad\qquad \forall\ g \in G\,,\ \alpha \in A$$

Inoltre, questa applicazione è *un'azione* — del gruppo G sull'insieme A — perché tutte le proprietà che devono essere soddisfatte lo sono automaticamente in quanto lo sono già per l'azione di coniugazione di G su sé stesso.

Ora, poiché A è *abeliano* si ha $a.\alpha := a\,\alpha\,a^{-1} = \alpha$ per ogni $a \in A$ e $\alpha \in A$, e quindi anche $(g\,a).\alpha = g.(a.\alpha) = g.\alpha$ per ogni $g \in G\,,\ a \in A\,,\ \alpha \in A$. Pertanto, in particolare,

$$\big(g\,a'\big).\alpha = \big(g\,a''\big).\alpha \qquad\qquad \forall\ g \in G\,,\ a', a'' \in A\,,\ \alpha \in A$$

Da quest'ultima proprietà segue allora che l'applicazione

$$\big(G/A\big) \times A \longrightarrow A\,, \quad \big(\overline{g}, \alpha\big) \mapsto \overline{g}.\alpha := g.\alpha\ \big(= g\,\alpha\,g^{-1}\big) \qquad \forall\ \overline{g} = gA \in G/A\,,\ \alpha \in A$$

è ben definita, nel senso che il valore di $\big(\overline{g}.\alpha\big)$ dipende sì dalla classe laterale $\overline{g} = gA$, ma *non* dipende invece dalla scelta del rappresentante $g \in \overline{g} = gA$ utilizzato per descriverla.

Dato che A è sottogruppo *normale* di G, l'insieme G/A delle sue classi laterali è un gruppo (con l'operazione indotta da quella di G). Pertanto, ha senso chiedersi se l'applicazione $\big(G/A\big) \times A \longrightarrow A$ considerata qui sopra sia *un'azione* — del gruppo G/A sull'insieme A. Ora, la verifica che l'applicazione $\big(G/A\big) \times A \longrightarrow A$ soddisfi effettivamente tutti gli assiomi di un'azione è immediata, in quanto tali assiomi discendono facilmente dalla costruzione e dal fatto che valgono le analoghe proprietà per l'azione di coniugazione di G su sé stesso. Esplicitamente, la verifica è questa: detti $e_{_G}$ ed $e_{_{G/A}}$ gli elementi neutri dei gruppi G e G/A, e considerati elementi qualsiasi $\overline{g_1}, \overline{g_2} \in G/A$ e $a, a', a'' \in A$, si ha

$$e_{_{G/A}}.a = \big(\overline{e_{_G}}\big).a := e_{_G}.a = a$$
$$\big(\,\overline{g_1} \cdot \overline{g_2}\,\big).a = \big(\,\overline{g_1 g_2}\,\big).a = \big(g_1\,g_2\big).a = g_1.\big(g_2.a\big) = \overline{g_1}.\big(\,\overline{g_2}.a\big)$$

Questo risolve il punto *(a)*.

Per il punto *(b)*, osserviamo che l'azione di G/A su A è un'azione per automorfismi perché lo è l'azione originale — di G su G stesso — dalla quale essa è derivata, e lo è

così anche quella "intermedia" — di G su A — ottenuta per restrizione dalla prima. In concreto, la verifica esplicita di quanto richiesto è la seguente:

$$\overline{g}.\big(a'\cdot a''\big) := g.\big(a'\cdot a''\big) = \big(g.a'\big)\cdot\big(g.a''\big) =: \big(\overline{g}.a'\big)\cdot\big(\overline{g}.a''\big)\,,\ \ \forall\ \overline{g}\in G/A\,,\ a',a''\in A \quad (3)$$

dove l'identità $g.\big(a'\cdot a''\big) = \big(g.a'\big)\cdot\big(g.a''\big)$, cioè appunto il fatto che l'azione di coniugazione sia un'azione per automorfismi, si verifica direttamente, così (per ogni $g\in G\,,\ a\in A$):

$$g.\big(a'\cdot a''\big) := g\cdot\big(a'\cdot a''\big)\cdot g^{-1} = g\cdot a'\cdot a''\cdot g^{-1} = g\cdot a'\cdot g^{-1}\cdot g\cdot a''\cdot g^{-1} =: \big(g.a'\big)\cdot\big(g.a''\big)$$

<u>*Secondo metodo:*</u> Si ricordi che, in generale, ogni azione $\nu : G\times S\longrightarrow S$ di un gruppo G su un insieme S equivale al dato di un morfismo (di gruppi) $\varphi : G\longrightarrow \mathcal{S}(S)$ dal gruppo G al gruppo $\mathcal{S}(S)$ delle permutazioni — nel quale il prodotto è la composizione — dell'insieme S in sé stesso. La corrispondenza è data da

$$\nu : G\times S\longrightarrow S \qquad \Longrightarrow \qquad \begin{array}{l} \varphi_\nu : G\longrightarrow \mathcal{S}(S) \\ \qquad g\ \mapsto\ \varphi_\nu(g) : \left\{ \begin{array}{l} S\longrightarrow\!\!\!\!\!\rightarrow\ S \\ s\mapsto \varphi_\nu(g)(s) := \nu(g,s) \quad \forall\ s\in S \end{array}\right. \end{array}$$

e in senso inverso invece è espressa da

$$\varphi : G\longrightarrow \mathcal{S}(S) \qquad \Longrightarrow \qquad \begin{array}{l} \nu_\varphi : G\times S\longrightarrow S \\ \qquad (g,s)\ \mapsto\ \nu_\varphi(g,s) := \varphi(g)(s) \quad \forall\ g\in G\,,\ s\in S \end{array}$$

Inoltre, quando S è a sua volta un gruppo, un'azione $\nu : G\times S\longrightarrow S$ è un'azione per automorfismi — nel senso della (3) qui sopra — se e soltanto se il corrispondente morfismo $\varphi : G\longrightarrow \mathcal{S}(S)$ è a valori nel sottogruppo $Aut(S)$ di $\mathcal{S}(S)$, nel qual caso allora scriveremo piuttosto $\varphi : G\longrightarrow Aut(S)$.

Nel caso in esame, l'azione — per automorfismi! — del gruppo G su sé stesso corrisponde al morfismo $\varphi : G\longrightarrow Aut(G)$, la cui immagine (per definizione) è il sottogruppo $Aut(G)$ degli automorfismi *interni* di G. Come prima, il sottogruppo A di G è mandato in sé da tutti gli automorfismi interni di G, perché è normale. Perciò, componendo ciascuno di questi automorfismi con la restrizione ad A si ottiene un'applicazione $\varphi' : G\longrightarrow A^A$, dove A^A è l'insieme di tutte le applicazioni da A in A. Inoltre, è immediato verificare che, più precisamente, $Im(\varphi')\subseteq Aut(A)$, e quindi abbiamo in effetti un'applicazione $\varphi' : G\longrightarrow Aut(A)$; infine, dal fatto che φ sia un morfismo segue subito che *anche tale* φ' *è a sua volta un morfismo* (di gruppi). Pertanto, alla luce di quanto su esposto, si conclude che il morfismo $\varphi' : G\longrightarrow Aut(A)$ corrisponde ad un'azione del gruppo G sul gruppo A.

Ora, per costruzione φ' è data da

$$\varphi' :\ g\mapsto\varphi'(g) : \left\{ \begin{array}{l} A\longrightarrow\!\!\!\!\!\rightarrow\ A \\ \alpha\mapsto \varphi'(g)(\alpha) = g\,\alpha\,g^{-1} \quad \forall\ \alpha\in A \end{array}\right. , \qquad \forall\, g\in G$$

In particolare, dato che A è abeliano si ha

$$\varphi'(a)(\alpha) = a\,\alpha\,a^{-1} = \alpha \quad \forall\,\alpha\in A\,,\ \forall\, a\in A\,, \qquad \Longrightarrow \qquad \varphi'(a) = id_A \quad \forall\, a\in A$$

e la conclusione si può esprimere simbolicamente scrivendo che $A \subseteq Ker(\varphi')$, cioè A è contenuto nel nucleo di φ'. Ma allora, il morfismo $\varphi' : G \longrightarrow Aut(A)$ induce univocamente uno ed un solo morfismo $\varphi'_\bullet : G/A \longrightarrow Aut(A)$ tale che il diagramma

$$\begin{array}{ccc} G & \xrightarrow{\varphi'} & Aut(A) \\ {\scriptstyle \pi_A}\downarrow & & \uparrow{\scriptstyle j} \\ G/A & \xrightarrow[\varphi'_\bullet]{} & Im(\varphi') \end{array}$$

(nel quale $G \xrightarrow{\pi_A} G/A$ è la proiezione canonica e $Im(\varphi') \xrightarrow{j} Aut(A)$ è l'immersione insiemistica) sia *commutativo*: in altre parole, si ha $j \circ \varphi'_\bullet \circ \pi_A = \varphi'$, il che significa esattamente che $\varphi'_\bullet(\overline{g}) = \varphi'(g)$ per ogni $\overline{g} = gA \in G/A$.

N.B.: quest'ultimo fatto si verifica *esattamente come* l'analogo risultato espresso dal *Teorema Fondamentale di Omomorfismo* (per gruppi).

Per concludere, abbiamo trovato un morfismo di gruppi $\varphi'_\bullet : G/A \longrightarrow Aut(A)$, indotto univocamente dal morfismo $\varphi : G \longrightarrow Aut(G)$ corrispondente all'azione di G su sé stesso per coniugazione. Per quanto già richiamato, tale morfismo φ' corrisponde ad una e una sola azione *per automorfismi* di G su A, che a sua volta in definitiva è indotta da quella di G su sé stesso (per coniugazione). □

(continua . . .)

[4] — Si consideri il polinomio $f(x) := \big(x^3-5\big)\big(x^3+7\big) \in \mathbb{Q}[x]$, e si indichino con $\mathbb{Q}_f$ e G_f rispettivamente il campo di spezzamento e il gruppo di Galois di $f(x)$ su $\mathbb{Q}$.

(a) Descrivere esplicitamente l'estensione $\mathbb{Q} \subseteq \mathbb{Q}_f$. In particolare, calcolarne il grado ed una base.

(b) Determinare la struttura di G_f come gruppo astratto.

(c) Descrivere esplicitamente G_f come gruppo di automorfismi dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}_f$.

(d) Determinare se il gruppo G_f sia risolubile oppure no.

Soluzione: *(d)* Applicando direttamente il Teorema di Abel-Ruffini si ha che

Il gruppo di Galois G_f è risolubile
se e soltanto se
l'estensione $\mathbb{Q} \subseteq \mathbb{Q}_f$ è risolubile per radicali
se e soltanto se
le radici del polinomio $f(x)$ si ottengono tutte tramite estrazione di radici n–esime (per opportuni n) di opportuni elementi del campo base $\mathbb{Q}$ dell'estensione.

Ora, le radici di $f(x) := \big(x^3-5\big)\big(x^3+7\big)$ sono ovviamente tutte e sole le radici terze di 5 e di -7 , che sono elementi di $\mathbb{Q}$: così otteniamo che G_f è *risolubile per radicali*, dunque — per quanto appena ricordato — risolubile, il che risolve *(d)*.

(a) Per definizione, il campo $\mathbb{Q}_f$ è l'estensione di $\mathbb{Q}$ generata dalle radici — in una opportuna chiusura algebrica, quale ad esempio $\mathbb{Q}^a_{\mathbb{C}}$ — del polinomio $f(x)$. Per quanto osservato sopra, tali radici sono

$$\sqrt[3]{5}\,,\ \ \zeta_3\,\sqrt[3]{5}\,,\ \ {\zeta_3}^2\,\sqrt[3]{5}\,,\qquad \sqrt[3]{-7} = -\sqrt[3]{7}\,,\ \ \zeta_3\,\sqrt[3]{-7} = -\zeta_3\,\sqrt[3]{7}\,,\ \ {\zeta_3}^2\,\sqrt[3]{-7} = -{\zeta_3}^2\,\sqrt[3]{7}$$

dove ζ_3 indica una radice terza primitiva di 1: precisamente, le prime tre sono radici del fattore $\big(x^3-5\big)$, e le ultime tre sono radici del fattore $\big(x^3+7\big)$.

Pertanto abbiamo

$$\mathbb{Q}_f \ = \ \mathbb{Q}\Big(\sqrt[3]{5}\,,\ \zeta_3\,\sqrt[3]{5}\,,\ {\zeta_3}^2\,\sqrt[3]{5}\,,\ \sqrt[3]{7}\,,\ \zeta_3\,\sqrt[3]{7}\,,\ {\zeta_3}^2\,\sqrt[3]{7}\Big) \ = \ \mathbb{Q}\Big(\sqrt[3]{5}\,,\ \sqrt[3]{7}\,,\ \zeta_3\Big) \tag{4}$$

dove la prima uguaglianza segue dalla costruzione, e la seconda è ovvia (spero).

Ci occupiamo adesso di calcolare una base e il grado dell'estensione $\mathbb{Q} \subseteq \mathbb{Q}\Big(\sqrt[3]{5}\,,\sqrt[3]{7}\,,\zeta_3\Big)$. Osserviamo che

– *[1]* $\Big[\mathbb{Q}\big(\sqrt[3]{7}\big) : \mathbb{Q}\Big] = 3$, perché il polinomio minimo di $\sqrt[3]{7}$ su $\mathbb{Q}$ è x^3-7 ; dalla teoria generale, sappiamo allora che una base di $\mathbb{Q}\big(\sqrt[3]{7}\big)$ su $\mathbb{Q}$ è $\Big\{1\,,\ \sqrt[3]{7}\,,\ \big(\sqrt[3]{7}\big)^2\Big\}$;

– *[2]* $\Big[\mathbb{Q}(\zeta_3) : \mathbb{Q}\Big] = 2$, perché il polinomio minimo di ζ_3 su $\mathbb{Q}$ è x^2+x+1 ; per la teoria generale allora una base di $\mathbb{Q}(\zeta_3)$ su $\mathbb{Q}$ è $\big\{1\,,\,\zeta_3\big\}$;

– *[3]* $\Big[\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big) : \mathbb{Q}\Big] \leq 2\cdot 3 = 6$, perché (per teoria generale) l'insieme di tutti i prodotti degli elementi di una base di $\mathbb{Q}\big(\sqrt[3]{7}\big)$ su $\mathbb{Q}$ — che son 3 — e di una base di $\mathbb{Q}(\zeta_3)$ su $\mathbb{Q}$ — che son 2 — è un insieme di generatori di $\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\big)$ come spazio vettoriale su $\mathbb{Q}$;

– *[4]* $\big[\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big]=6\,,$ perché l'estensione $\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)$ di $\mathbb{Q}$ contiene le estensioni intermedie $\mathbb{Q}\big(\sqrt[3]{7}\,\big)$ e $\mathbb{Q}(\zeta_3)\,,$ che hanno grado rispettivamente 3 e 2 su $\mathbb{Q}\,;$ per la moltiplicatività del grado (nelle torri di estensioni finite) allora si ha che $\big[\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big]\in 6\,\mathbb{N}_+$ — cioè è multiplo (non nullo) di 6 — e questo insieme alla *[3]* dà quanto enunciato;

– *[5]* una base di $\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)$ su $\mathbb{Q}$ è $\Big\{1\,,\,\sqrt[3]{7}\,,\big(\sqrt[3]{7}\big)^2\,,\,\zeta_3\,,\,\zeta_3\,\sqrt[3]{7}\,,\,{\zeta_3}^2\big(\sqrt[3]{7}\big)^2\Big\}\,,$ per quanto esposto ai punti *([1–4]*;

– *[6]* $\big[\mathbb{Q}\big(\sqrt[3]{5}\,\big):\mathbb{Q}\big]=3\,,$ e $\mathbb{Q}\big(\sqrt[3]{5}\,\big)$ ha base $\Big\{1\,,\,\sqrt[3]{5}\,,\big(\sqrt[3]{5}\,\big)^2\Big\}$ su $\mathbb{Q}\,,$ come in *[1]*;

– *[7]* $\big[\mathbb{Q}\big(\sqrt[3]{5}\,,\,\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)\big]\le 3\,,$ perché

$$\mathbb{Q}\big(\sqrt[3]{5}\,,\,\sqrt[3]{7}\,,\,\zeta_3\,\big)\;=\;\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,,\,\sqrt[3]{5}\,\big)\;=\;\Big(\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)\Big)\big(\sqrt[3]{5}\,\big)$$

e il polinomio minimo di $\sqrt[3]{5}$ su $\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)$ necessariamente divide il polinomio minimo di $\sqrt[3]{5}$ su $\mathbb{Q}\,,$ che è $x^3-5\,;$

– *[8]* $\big[\mathbb{Q}\big(\sqrt[3]{5}\,,\,\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)\big]=3\,,$ perché per la *[6]* sappiamo che tale grado, che è anche il grado del polinomio minimo di $\sqrt[3]{5}$ su $\mathbb{Q}\,,$ sia esso $p(x)\,,$ è al più 3; d'altra parte, sappiamo più precisamente che $p(x)$ divide $x^3-5\,:$ allora $p(x)$ ha grado minore di 3 se e soltanto se x^3-5 è *riducibile* sul campo $\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)\,,$ il che significa necessariamente che esso ha una radice α in $\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)\,,$ cioè esiste un $\alpha\in\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)$ tale che $\alpha^3=5\,.$ Ma dalla *(3)* possiamo dedurre che questo è impossibile, perché gli elementi di $\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)$ sono tutti e soli della forma

$$q_1\cdot 1\,+\,q_2\cdot\sqrt[3]{7}\,+\,q_3\cdot\big(\sqrt[3]{7}\big)^2\,+\,q_4\cdot\zeta_3\,+\,q_5\cdot\zeta_3\,\sqrt[3]{7}\,+\,q_6\cdot{\zeta_3}^2\,\big(\sqrt[3]{7}\big)^2$$

(con $q_1\,,\,\ldots\,,\,q_6\in\mathbb{Q}\,$), e non si verifica *mai*

$$\Big(q_1\cdot 1\,+\,q_2\cdot\sqrt[3]{7}\,+\,q_3\cdot\big(\sqrt[3]{7}\big)^2\,+\,q_4\cdot\zeta_3\,+\,q_5\cdot\zeta_3\,\sqrt[3]{7}\,+\,q_6\cdot{\zeta_3}^2\,\big(\sqrt[3]{7}\big)^2\Big)^3\;=\;5$$

– *[9]* $\big[\mathbb{Q}_f:\mathbb{Q}\big]=18\,,$ perché

$$\mathbb{Q}_f\;=\;\mathbb{Q}\big(\sqrt[3]{5}\,,\,\sqrt[3]{7}\,,\,\zeta_3\,\big)\qquad\text{per la (4),}$$

$$\big[\mathbb{Q}\big(\sqrt[3]{5}\,,\,\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big]\;=\;\big[\mathbb{Q}\big(\sqrt[3]{5}\,,\,\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)\big]\cdot\big[\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big]$$

per la moltiplicatività del grado nelle torri di estensioni finite,

$$\big[\mathbb{Q}\big(\sqrt[3]{5}\,,\,\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big)\big]\;=\;3\,,\qquad\big[\mathbb{Q}\big(\sqrt[3]{7}\,,\,\zeta_3\,\big):\mathbb{Q}\big]\;=\;6$$

per la *[8]* e per la *[4]* rispettivamente.

– *[10]* una base di $\mathbb{Q}_f$ su $\mathbb{Q}$ è

$$\left\{ {\zeta_3}^z \left(\sqrt[3]{7}\right)^s \left(\sqrt[3]{5}\right)^c \;\middle|\; 0 \le z \le 1\,;\; 0 \le s\,, c \le 2 \right\}$$

perché $\mathbb{Q}_f = \mathbb{Q}\big(\sqrt[3]{5}\,,\, \sqrt[3]{7}\,,\, \zeta_3\,\big) = \Big(\mathbb{Q}\big(\sqrt[3]{7}\,,\, \zeta_3\,\big)\Big)\big(\sqrt[3]{5}\,\big)$, perciò, in generale, una base come richiesta si può sempre ottenere moltiplicando tutti gli elementi di una base di $\mathbb{Q}\big(\sqrt[3]{7}\,,\, \zeta_3\,\big)$ su $\mathbb{Q}\big(\sqrt[3]{5}\,\big)$ con tutti gli elementi di una base di $\mathbb{Q}\big(\sqrt[3]{5}\,\big)$ su $\mathbb{Q}$, e infine, in particolare, nel nostro caso si possono scegliere tali basi come in *[5]* e in *[6]*.

La *[9]* e la *[10]*, insieme a tutta la discussione precedente, risolvono il punto *(a)*.

(b) Dobbiamo determinare la struttura di G_f *come gruppo astratto*, cioè la sua classe di isomorfismo. Cominciamo cercando di ottenere il massimo dalla conoscenza dell'ordine di $\big|G_f\big|$ di G_f , che abbiamo già calcolato. Per quanto già visto in *(a)*, abbiamo

$$\big|G_f\big| \;=\; \big[\mathbb{Q}_f : \mathbb{Q}\big] \;=\; 18 \;=\; 2 \cdot 3^2$$

Quindi, per i Teoremi di Sylow, G_f possiede un 2–sottogruppo di Sylow, che indichiamo con S_2 , di ordine 2 , e un 3–sottogruppo di Sylow, che indichiamo con S_3 , di ordine 3^2 .

A questo punto, per il Teorema di Lagrange abbiamo

$$\big(G_f : S_3\big) \;=\; \big|G_f\big| \Big/ \big|S_3\big| \;=\; \big(2 \cdot 3^2\big) \Big/ 3^2 \;=\; 2$$

cioè il S_3 ha indice 2 in G_f . Ma allora, per un risultato generale,

$$S_3 \trianglelefteq G_f \;, \quad \text{cioè} \quad S_3 \text{ è sottogruppo normale di } G_f$$

Pertanto nel seguito scriveremo $N_3 := S_3$, giusto per ricordarci che si tratta di un sottogruppo *normale*.

(*N.B.: per chi non l'avesse mai visto, ricordo come si dimostra 'sto fatto generale, che si esprime così:* $H \le G\,,\; \big(G : H\big) = 2 \implies H \trianglelefteq G$.

Per ipotesi le classi laterali destre di H *in* G *sono due, diciamo* g_dH , g'_dH . *D'altra parte, una di queste due classi dev'essere* H *stesso, perciò possiamo assumere che sia* $g'_d = e_G$ *(l'elemento neutro di* G*): quindi 'ste classi sono* g_dH , H , *per un certo* $g_d \in H$. *Allora per ogni* $g \in G$ *abbiamo*

$$g \in H \implies gH = H \;, \qquad g \in \big(G \setminus H\big) = g_dH \implies gH = g_dH \tag{5}$$

proprio perché $G \setminus H$ *è costituito dalla sola classe* g_dH .

Analogamente, le classi laterali sinistre sono due, e una di esse dev'essere necessariamente $H = He_G$, *quindi sono* Hg_s , H , *per un certo* $g_s \in H$. *Quindi, per ogni* $g \in G$,

$$g \in H \implies Hg = H \;, \qquad g \in \big(G \setminus H\big) = Hg_s \implies Hg = Hg_s \tag{6}$$

Ora, le classi laterali destre costituiscono una partizione di G *, quindi* $G = g_d H \coprod H$ *, dove il simbolo* $\coprod$ *indica l'unione disgiunta. Analogamente abbiamo la partizione in classi laterali sinistre* $G = H g_s \coprod H$ *. Ma allora*

$$g_d H \coprod H = G = H g_s \coprod H \quad \Longrightarrow \quad g_d H = G \setminus H = H g_s \tag{7}$$

A questo punto, mettendo insieme la (5), la (6) e la (7), per ogni $g \in G$ *abbiamo:*

$$g \in H \implies gH = H = Hg\,, \qquad g \in \big(G \setminus H\big) \implies gH = g_d H = G \setminus H = H g_s = Hg$$

dunque in ogni caso $gH = Hg$*, per ogni* $g \in G$*, e quindi* H *è normale in* G*, q.e.d.* $\Big)$

A questo punto abbiamo due sottogruppi di G_f, che sono $S_2 \leq G_f$, $N_3 := S_3 \trianglelefteq G_f$, il secondo dei quali è normale; quindi l'insieme $S_2 \cdot N_3 = N_3 \cdot S_2$ dei loro prodotti (in un ordine o nell'altro) è anch'esso un sottogruppo di G_f. Per costruzione, gli ordini di S_2 e di N_3 sono coprimi, quindi per il Teorema di Lagrange abbiamo $S_2 \bigcap N_3 = \{e_G\}$. In aggiunta, il prodotto dei loro ordini (per costruzione) è proprio l'ordine di $S_2 \cdot N_3 = N_3 \cdot S_2$, che è anche l'ordine di G_f: dunque $S_2 \cdot N_3 = N_3 \cdot S_2 = G_f$. In sintesi, si ha

$$S_2 \leq G_f\,, \quad N_3 \trianglelefteq G_f\,, \quad S_2 \bigcap N_3 = \{e_G\}\,, \quad S_2 \cdot N_3 = G_f$$

Da questo possiamo concludere, per un risultato generale, che $G_f = S_2 \ltimes_\Phi N_3$, cioè

$$G_f \text{ è (isomorfo a un) prodotto semidiretto di } S_2 \text{ con } N_3\,. \tag{8}$$

che dipende ovviamente da uno specifico morfismo di gruppi $\Phi : S_2 \longrightarrow Aut(N_3)$.

Per capire quale sia — nel caso specifico — tale morfismo $\Phi : S_2 \longrightarrow Aut(N_3)$, e quindi come sia fatto il prodotto semidiretto $G_f = S_2 \ltimes_\Phi N_3$ di cui in (8), vediamo come sono fatti i due fattori S_2 e N_3. Il primo fattore è ovvio:

$$\big|S_2\big| = 2 \quad \Longrightarrow \quad S_2 \cong \mathbb{Z}_2 \tag{9}$$

cioè S_2 è isomorfo a $\big(\mathbb{Z}_2\,; +\big)$, il gruppo ciclico con due elementi. Per il secondo abbiamo

$$\big|N_3\big| = 3^2 \quad \Longrightarrow \quad N_3 \cong \mathbb{Z}_{3^2} \text{ oppure } N_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \tag{10}$$

perché applichiamo due risultati generali (con $p = 3$): per ogni gruppo Γ, il primo è

$$\big|\Gamma\big| = p^2\,,\ p \text{ primo} \quad \Longrightarrow \quad \Gamma \text{ è abeliano}$$

mentre il secondo è un caso particolare del Teorema di Classificazione dei Gruppi Abeliani:

$$\Gamma \text{ è abeliano}\,,\ \big|\Gamma\big| = p^2\,,\ p \text{ primo} \quad \Longrightarrow \quad \Gamma \cong \mathbb{Z}_{p^2} \text{ oppure } \Gamma \cong \mathbb{Z}_p \times \mathbb{Z}_p$$

Dunque la (10) ci dà $N_3 \cong \mathbb{Z}_{3^2} = \mathbb{Z}_9$ oppure $N_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. I due casi si distinguono così: nel primo, N_3 contiene un elemento di ordine 9, nel secondo invece no.

A questo punto — e soltanto ora (prima potevamo farne a meno) — usiamo la nostra conoscenza esplicita di chi sia effettivamente il gruppo G_f in esame, e in particolare il fatto che sia un gruppo di Galois! Precisamente, osserviamo che G_f è il gruppo di Galois del polinomio $f(x) := \big(x^3 - 5\big)\big(x^3 + 7\big)$, che ha grado 6, quindi ha (al più) 6 radici (nell'estensione $\mathbb{Q}_f$): allora G_f agisce come gruppo di permutazioni delle 6 radici, e precisamente si identifica ad un sottogruppo del gruppo simmetrico $\mathcal{S}_6$ su 6 elementi. Ora, *in* $\mathcal{S}_6$ *non esistono elementi di ordine 9*, quindi lo stesso vale per G_f , e in particolare allora *non esistono elementi di ordine 9 nel sottogruppo* N_3 . Perciò dev'essere necessariamente

$$N_3 \;\cong\; \mathbb{Z}_3 \times \mathbb{Z}_3 \tag{11}$$

(*N.B.:* in realtà, sappiamo pure qualcosa di più preciso. Infatti, G_f permuta *separatamente* le radici dei due fattori $\big(x^3 - 5\big)$ e $\big(x^3 + 7\big)$ di $f(x)$, quindi si identifica ad un sottogruppo del prodotto diretto di gruppi simmetrici $\mathcal{S}_3 \times \mathcal{S}_3$)

Adesso dunque abbiamo, per le (8), (9) e (11),

$$G_f \;=\; S_2 \ltimes_\Phi N_3 \;\cong\; \mathbb{Z}_2 \ltimes_\Phi \big(\,\mathbb{Z}_3 \times \mathbb{Z}_3\big) \tag{12}$$

dove Φ è un morfismo di gruppi $\Phi : \mathbb{Z}_2 \cong S_2 \longrightarrow Aut(N_3) \cong Aut(\mathbb{Z}_3)$.

Ricordiamo che, dati due gruppi G_1 e G_2 e un morfismo di gruppi $G_1 \xrightarrow{\Phi} Aut(G_2)$, detto $G_1 \ltimes_\Phi G_2$ il corrispondente prodotto *semidiretto* e $G_1 \times G_2$ il corrispondente prodotto *diretto*, si ha

$$G_1 \ltimes_\Phi G_2 \;\cong\; G_1 \times G_2 \quad\Longleftrightarrow\quad G_1 \xrightarrow{\Phi} Aut(G_2) \text{ è il morfismo costante} \tag{13}$$

dove chiamiamo "morfismo costante" ogni morfismo di gruppi che mandi gli elementi del gruppo di partenza (il *dominio* del morfismo) — in questo caso, G_1 — nell'elemento neutro del gruppo di arrivo (il *codominio* del morfismo) — in questo caso, $Aut(G_2)$.

Quando G_1 e G_2 sono entrambi abeliani, il loro prodotto diretto è anch'esso abeliano; al contrario, se $G_1 \xrightarrow{\Phi} Aut(G_2)$ *non è costante*, allora il prodotto semidiretto (non banale!) $G_1 \ltimes_\Phi G_2$ *non è abeliano*. Pertanto, la (13) ci dà

$$G_1\,,\; G_2 \text{ abeliani} \quad\Longrightarrow\quad \Big(G_1 \ltimes_\Phi G_2 \text{ è abeliano} \;\Longleftrightarrow\; \Phi \text{ è costante}\Big) \tag{14}$$

Puntiamo ora ad applicare la (14) a $G_1 := S_2 \cong \mathbb{Z}_2$ e $G_2 := N_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ (abeliani!).

Per calcolare $\Phi : G_1 := S_2 \cong \mathbb{Z}_2 \longrightarrow Aut(\mathbb{Z}_3) \cong Aut(N_3) = Aut(G_2)$, osserviamo che

$$Aut\big(\,(\,\mathbb{Z}_3\,;+)\big) \;\cong\; \big(U(\mathbb{Z}_3)\,;\,\cdot\,\big) \;\cong\; (\,\mathbb{Z}_2\,;+) \tag{15}$$

dove gli isomorfismi considerati sono

$$Aut\big(\,(\,\mathbb{Z}_3\,;+)\big) \xrightarrow{\cong} \big(U(\mathbb{Z}_3)\,;\,\cdot\,\big)\;, \quad \varphi \mapsto \varphi\big([1]_3\big)\;,$$
$$\big(U(\mathbb{Z}_3)\,;\,\cdot\,\big) \xrightarrow{\cong} (\,\mathbb{Z}_2\,;+)\;, \qquad [1]_3 \mapsto [0]_2\;,\;\; [2]_3 \mapsto [1]_2\;.$$

Quindi quel che stiamo cercando è — "attraverso" i vari isomorfismi — un morfismo di gruppi $\Phi : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$. Ma di tali morfismi ne esistono soltanto due, e precisamente

$$\begin{aligned} &\Phi_+ : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \ , \qquad [0]_2 \mapsto [0]_2 \ , \quad [1]_2 \mapsto [0]_2 \ , \\ &\Phi_- : \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2 \ , \qquad [0]_2 \mapsto [0]_2 \ , \quad [1]_2 \mapsto [1]_2 \ . \end{aligned}$$

Tra questi due, *il morfismo costante* è Φ_+ : quindi, attraverso gli isomorfismi in (15) — o i loro inversi — è chiaro che Φ_+ corrisponde al morfismo costante da S_2 a $Aut(\mathbb{N}_3)$ — che manda ogni elemento di S_2 in id_{N_3} — mentre Φ_- corrisponde ad un morfismo non costante (l'unico esistente, in effetti). Ma allora, applicando la (13) e la (14) a $G_1 := S_2 \cong \mathbb{Z}_2$ e $G_2 := N_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ otteniamo

$$\begin{aligned} &S_2 \ltimes_{\Phi_+} N_3 \ \big(\ = S_2 \times N_3 \big) \quad \text{è abeliano} \\ &S_2 \ltimes_{\Phi_-} N_3 \ \big(\ \ncong S_2 \times N_3 \big) \quad \text{non è abeliano} \end{aligned} \tag{16}$$

In conclusione, dalla (12) e dalla (16) ci basta sapere se G_f sia abeliano oppure no — e per capir questo, dobbiamo guardarlo più da vicino... — per stabilire se sia

$$G_f \ \cong \ S_2 \ltimes_{\Phi_+} N_3 \ \cong \ \mathbb{Z}_2 \times \big(\mathbb{Z}_3 \times \mathbb{Z}_3 \big) \quad \text{oppure} \quad G_f \ \cong \ S_2 \ltimes_{\Phi_-} N_3 \ \cong \ \mathbb{Z}_2 \ltimes_{\Phi_-} \big(\mathbb{Z}_3 \times \mathbb{Z}_3 \big)$$

Consideriamo i due automorfismi $\sigma, \tau \in G_f$ — nel nostro gruppo di Galois — dati da

$$\begin{aligned} &\sigma\big(\sqrt[3]{5}\,\big) := \zeta_3\,\sqrt[3]{5}\,, \qquad \sigma\big(\sqrt[3]{7}\,\big) := \zeta_3\,\sqrt[3]{7}\,, \qquad \sigma\big(\zeta_3\big) := \zeta_3 \\ &\tau\big(\sqrt[3]{5}\,\big) := \sqrt[3]{5}\,, \qquad \tau\big(\sqrt[3]{7}\,\big) := \zeta_3\,\sqrt[3]{7}\,, \qquad \tau\big(\zeta_3\big) := \zeta_3^{\,2} \end{aligned}$$

Per definizione abbiamo allora

$$\begin{aligned} (\tau \circ \sigma)\big(\sqrt[3]{5}\,\big) \ = \ \tau\big(\sigma\big(\sqrt[3]{5}\,\big)\big) \ = \ \tau\big(\zeta_3\,\sqrt[3]{5}\,\big) \ = \ \tau\big(\zeta_3\big)\,\tau\big(\sqrt[3]{5}\,\big) \ = \ \zeta_3^{\,2}\,\sqrt[3]{5} \\ (\sigma \circ \tau)\big(\sqrt[3]{5}\,\big) \ = \ \sigma\big(\tau\big(\sqrt[3]{5}\,\big)\big) \ = \ \sigma\big(\sqrt[3]{5}\,\big) \ = \ \zeta_3\,\sqrt[3]{5} \end{aligned}$$

dunque $(\tau \circ \sigma)\big(\sqrt[3]{5}\,\big) \neq (\sigma \circ \tau)\big(\sqrt[3]{5}\,\big)$, e quindi $\tau \circ \sigma \neq \sigma \circ \tau$. Questo prova che G_f *non* è *abeliano*, e pertanto possiamo concludere che

$$G_f \ \cong \ S_2 \ltimes_{\Phi_+} N_3 \ \cong \ S_2 \times N_3 \ \cong \ \mathbb{Z}_2 \times \big(\mathbb{Z}_3 \times \mathbb{Z}_3 \big)$$

(c) Per descrivere $G_f = Gal\big(\mathbb{Q}_f/\mathbb{Q}\big)$, ricordiamo — per la (4) — che $\mathbb{Q}_f$ è generato su $\mathbb{Q}$ da tre elementi, precisamente $\mathbb{Q}_f = \mathbb{Q}\Big(\sqrt[3]{5}\,,\ \sqrt[3]{7}\,,\ \zeta_3\Big)$. Pertanto, ogni automorfismo $\sigma \in G_f$ è determinato dalla sua azione sui generatori $\sqrt[3]{5}$, $\sqrt[3]{7}$ e ζ_3 . In particolare, un tale σ permuta tra loro i coniugati di $\sqrt[3]{5}$ — cioè le radici del suo polinomio minimo — che sono $\sqrt[3]{5}$, $\zeta_3\,\sqrt[3]{5}$ e $\zeta_3^{\,2}\,\sqrt[3]{5}$; analogamente, σ permuta tra loro i coniugati di $\sqrt[3]{7}$, cioè $\sqrt[3]{7}$, $\zeta_3\,\sqrt[3]{7}$ e $\zeta_3^{\,2}\,\sqrt[3]{7}$, e permuta tra loro i coniugati di ζ_3 , cioè ζ_3 e $\zeta_3^{\,2} = \zeta_3^{\,-1} = -1-\zeta_3$. Pertanto in definitiva l'automorfismo σ è determinato univocamente dalla terna

$$\big(\,\sigma\big(\sqrt[3]{5}\,\big)\,,\,\sigma\big(\sqrt[3]{7}\,\big)\,,\,\sigma(\zeta_3)\big) \ \in \ \big\{\zeta_3^{\,r}\,\sqrt[3]{5}\,\big\}_{r=0,1,2} \times \big\{\zeta_3^{\,s}\,\sqrt[3]{7}\,\big\}_{s=0,1,2} \times \big\{\zeta_3^{\,i}\big\}_{i=1,2} \tag{17}$$

per cui si hanno esattamente $3 \cdot 3 \cdot 2 = 18$ scelte e quindi $\big|G_f\big| = 18$, come è giusto che sia perché sappiamo a priori che dev'essere $\big|G_f\big| = [\mathbb{Q}_f : \mathbb{Q}] = 18$.

Come notazione per tutti i $\sigma \in G_f$, basandoci sulla (17), indichiamo con $\sigma_{r,s,i}$ quell'unico automorfismo che corrisponde alla scelta della terna di esponenti (r,s,i) nella (17); abbiamo dunque

$$\sigma_{r,s,i} \,:\; \sqrt[3]{5} \mapsto {\zeta_3}^r \sqrt[3]{5}\,,\; \sqrt[3]{7} \mapsto {\zeta_3}^s \sqrt[3]{7}\,,\; \zeta_3 \mapsto {\zeta_3}^i\,, \qquad \forall\, (r,s,i) \in \{0,1,2\}\times\{0,1,2\}\times\{1,2\}$$

in particolare, ritroviamo l'identità come $\sigma_{(0,0,1)} = id_{\mathbb{Q}_f}$.

Infine, quanto fatto finora descrive $G(f)$ soltanto come insieme (di automorfismi di $\mathbb{Q}_f$ su $\mathbb{Q}$), ma non descrive la sua struttura di gruppo. A tal fine, cominciamo osservando che

$$G_f \;=\; \big\langle \sigma_5\,, \sigma_7\,, \tau \big\rangle \tag{18}$$

dove $\sigma_5 := \sigma_{1,0,1}$, $\sigma_7 := \sigma_{0,1,1}$ e $\tau := \sigma_{0,0,2}$, in quanto il calcolo diretto ci dà

$$\sigma_{r,s,i} \;=\; {\sigma_5}^r \circ {\sigma_7}^s \circ \tau^i \qquad\qquad \forall\, (r,s,i) \in \{0,1,2\}\times\{0,1,2\}\times\{1,2\}$$

Consideriamo ora i seguenti sottogruppi:

$$C_5 := \big\langle \sigma_5 \big\rangle\,, \qquad C_7 := \big\langle \sigma_7 \big\rangle\,, \qquad C_2 := \big\langle \tau \big\rangle$$

Dalle definizioni segue che σ_5, σ_7 e τ hanno ordine rispettivamente 3, 3 e 2: quindi

$$C_5 \;:=\; \big\langle \sigma_5 \big\rangle \;\cong\; \mathbb{Z}_3\,, \qquad C_7 \;:=\; \big\langle \sigma_7 \big\rangle \;\cong\; \mathbb{Z}_3\,, \qquad C_2 \;:=\; \big\langle \tau \big\rangle \;\cong\; \mathbb{Z}_2 \tag{19}$$

Consideriamo poi i sottogruppi

$$D_5 := \big\langle \sigma_5\,, \tau \big\rangle\,, \qquad D_7 := \big\langle \sigma_7\,, \tau \big\rangle\,, \qquad P_{5,7} := \big\langle \sigma_5\,, \sigma_7 \big\rangle$$

Per costruzione, D_5 agisce in modo non banale sui due generatori $\sqrt[3]{5}$ e ζ_3, e banalmente invece su $\sqrt[3]{7}$ (in altre parole, "lo lascia fermo"); perciò possiamo identificare tale sottogruppo di G_f a G_{x^3-5}, il gruppo di Galois del polinomio $x^3 - 5$. Ora, dovrebbe esser chiaro — da precedenti esperienze, magari... — che

$$D_5 \;:=\; \big\langle \sigma_5\,, \tau \big\rangle \;\cong\; G_{x^3-5} \;\cong\; \big\langle \tau \big\rangle \ltimes \big\langle \sigma_5 \big\rangle \;\cong\; \mathbb{Z}_2 \ltimes \mathbb{Z}_3 \tag{20}$$

con struttura moltiplicativa in $\big\langle \tau \big\rangle \ltimes \big\langle \sigma_5 \big\rangle$ determinata da $\tau \circ \sigma_5 \circ \tau^{-1} = {\sigma_5}^2$, che corrisponde in $\mathbb{Z}_2 \ltimes \mathbb{Z}_3$ a $[r]_2 * [s]_3 * [-r]_2 = [2s]_3$. In particolare, D_5 è un gruppo simmetrico, precisamente $D_5 \cong \mathcal{S}\big(\sqrt[3]{5}\,, \zeta_3 \sqrt[3]{5}\,, {\zeta_3}^2 \sqrt[3]{5}\big) \cong \mathcal{S}_3$.

In modo del tutto analogo, abbiamo che D_7 si identifica a G_{x^3-7}, il gruppo di Galois del polinomio $x^3 - 7$ (che è anche quello di $x^3 + 7$, peraltro!), e allora

$$D_7 \;:=\; \big\langle \sigma_7\,, \tau \big\rangle \;\cong\; G_{x^3-7} \;\cong\; \big\langle \tau \big\rangle \ltimes \big\langle \sigma_7 \big\rangle \;\cong\; \mathbb{Z}_2 \ltimes \mathbb{Z}_3 \tag{21}$$

con struttura moltiplicativa in $\big\langle\tau\big\rangle \ltimes \big\langle\sigma_7\big\rangle$ determinata da $\tau \circ \sigma_7 \circ \tau^{-1} = {\sigma_7}^2$, che corrisponde di nuovo in $\mathbb{Z}_2 \ltimes \mathbb{Z}_3$ a $[r]_2 * [s]_3 * [-r]_2 = [2s]_3$. In particolare, D_7 è a sua volta un gruppo simmetrico, precisamente $D_7 \cong \mathcal{S}\big(\sqrt[3]{7}\,,\, \zeta_3\,\sqrt[3]{7}\,,\, {\zeta_3}^2\,\sqrt[3]{7}\big) \cong \mathcal{S}_3$.

Infine, per $P_{5,7}$ abbiamo che $\sigma_5 \circ \sigma_7 = \sigma_7 \circ \sigma_5$, e quindi

$$P_{5,7} \;:=\; \big\langle \sigma_5\,,\,\sigma_7 \big\rangle \;\cong\; \big\langle \sigma_5 \big\rangle \times \big\langle \sigma_7 \big\rangle \;\cong\; \mathbb{Z}_3 \times \mathbb{Z}_3 \tag{22}$$

Complessivamente, dalle (18–22) otteniamo che

$$G_f \;=\; \big\langle \sigma_5\,,\sigma_7\,,\,\tau \big\rangle \;\cong\; \big\langle \tau \big\rangle \ltimes \Big(\big\langle \sigma_5 \big\rangle \times \big\langle \sigma_7 \big\rangle \Big) \;\cong\; \mathbb{Z}_2 \ltimes \big(\mathbb{Z}_3 \times \mathbb{Z}_3 \big) \tag{23}$$

con struttura moltiplicativa in $\big\langle\tau\big\rangle \ltimes \Big(\big\langle\sigma_5\big\rangle \times \big\langle\sigma_7\big\rangle\Big)$ determinata da $\tau \circ \sigma_7 \circ \tau^{-1} = {\sigma_7}^2$, $\tau \circ \sigma_5 \circ \tau^{-1} = {\sigma_5}^2$, che corrisponde a $[r]_2 * \big([s]_3\,,[u]_3\big) * [-r]_2 = \big([2s]_3\,,[2u]_3\big)$ in $\mathbb{Z}_2 \ltimes \big(\mathbb{Z}_3 \times \mathbb{Z}_3\big)$. In conclusione, gli elementi di G_f sono dati da $\sigma_{r,s,i} = {\sigma_5}^r \circ {\sigma_7}^s \circ \tau^i$ (per ogni $(r,s,i) \in \{0,1,2\}\times\{0,1,2\}\times\{1,2\}$), e le regole di calcolo per il prodotto di due tali elementi si riducono alla sola formula

$$\sigma_{r_1,s_1,i_1} \circ \sigma_{r_2,s_2,i_2} \;=\; {\sigma_5}^{r_1} \circ {\sigma_7}^{s_1} \circ \tau^{i_1} \circ {\sigma_5}^{r_2} \circ {\sigma_7}^{s_2} \circ \tau^{i_2} \;=\; {\sigma_5}^{r_1+r_2} \circ {\sigma_7}^{s_1+s_2} \circ \tau^{i_1+i_2}$$

per tutte le terne $(r_1,s_1,i_1),(r_2,s_2,i_2) \in \{0,1,2\}\times\{0,1,2\}\times\{1,2\}$.

Questo completa la descrizione del gruppo G_f .

<u>Nota</u>: dalla descrizione di G_f in (23) abbiamo $G_f \cong \mathbb{Z}_2 \ltimes \big(\mathbb{Z}_3 \times \mathbb{Z}_3\big)$. Dunque G_f contiene il sottogruppo normale $\mathbb{Z}_3 \times \mathbb{Z}_3$, che è abeliano, e quindi *risolubile*. Inoltre, il quoziente di G_f per tale sottogruppo normale è isomorfo a $\mathbb{Z}_2$ (l'altro fattore del prodotto semidiretto), che è abeliano, e quindi *risolubile*. Da un risultato di teoria generale segue allora che anche G_f è risolubile (come già osservato nel dimostrare *(d)*).

Si noti che il procedimento che abbiamo seguito è del tutto generale, e prova questo: se abbiamo un gruppo prodotto semidiretto $G = H \ltimes N$, con N risolubile e $H \cong G/N$ risolubile, allora anche G stesso è a sua volta risolubile. □