TEST DI VERIFICA DI ALGEBRA 2

21 Dicembre 2007 — azioni di gruppi, anelli speciali, estensioni di campi

Testo con soluzioni

. . . . . .

N.B.: il simbolo $\diamondsuit$ *contrassegna gli esercizi un po' più complessi.*

1 — Determinare il numero di anagrammi dell'esclamazione "MAMMAMIA".

Soluzione: L'esclamazione "MAMMAMIA" è un elemento dell'insieme $\mathcal{P}_8$ di tutte le parole composte di 8 lettere scelte nell'alfabeto $\{M, A, I\}$. Sull'insieme $\mathcal{P}_8$ agisce il gruppo simmetrico $\mathcal{S}_8$ tramite permutazione delle posizioni delle lettere in ciascuna parola. Un "anagramma" della parola MAMMAMIA allora non è altro che un elemento della $\mathcal{S}_8$–orbita dell'elemento MAMMAMIA nell'$\mathcal{S}_8$–spazio $\mathcal{P}_8$: indichiamo tale orbita con $\mathcal{O}_{MAMMAMIA}$.

Dobbiamo dunque calcolare il numero di elementi di $\mathcal{O}_{MAMMAMIA}$. Dalla teoria generale abbiamo una biiezione

$$\mathcal{O}_{MAMMAMIA} \;\cong\; \mathcal{S}_8 \Big/ St_{MAMMAMIA}$$

dove $St_{MAMMAMIA}$ denota il sottogruppo stabilizzatore di MAMMAMIA, cioè l'insieme $\left\{ \sigma \in \mathcal{S}_8 \;\middle|\; \sigma.MAMMAMIA = MAMMAMIA \right\}$. Ora, una permutazione σ in $\mathcal{S}_8$ sta in $St_{MAMMAMIA}$ se e soltanto se permuta in sé, separatamente, i sottoinsiemi delle posizioni nelle quali si trovano le M, le A, e la I, cioè — rispettivamente — i sottoinsiemi $\{1, 3, 4\}$, $\{2, 5, 8\}$, e $\{7\}$. Pertanto si ha

$$St_{MAMMAMIA} \;=\; \mathcal{S}_{\{1,3,4,6\}} \times \mathcal{S}_{\{2,5,8\}} \times \mathcal{S}_{\{7\}} \;\subseteq\; \mathcal{S}_{\{1,2,\ldots,8\}} \;=:\; \mathcal{S}_8$$

In conclusione, da tutto questo otteniamo

$$\begin{aligned} \left|\mathcal{O}_{MAMMAMIA}\right| \;&=\; \left|\mathcal{S}_8 \Big/ St_{MAMMAMIA}\right| \;=\; \left|\mathcal{S}_8\right| \Big/ \left|St_{MAMMAMIA}\right| \;= \\ &=\; \left|\mathcal{S}_8\right| \Big/ \left|\mathcal{S}_{\{1,3,4,6\}} \times \mathcal{S}_{\{2,5,8\}} \times \mathcal{S}_{\{7\}}\right| \;=\; \left|\mathcal{S}_8\right| \Big/ \left|\mathcal{S}_{\{1,3,4,6\}}\right| \cdot \left|\mathcal{S}_{\{2,5,8\}}\right| \cdot \left|\mathcal{S}_{\{7\}}\right| \;= \\ &=\; 8! \Big/ 4! \cdot 3! \cdot 1! \;=\; 70 \end{aligned}$$

perciò il numero di anagrammi di "MAMMAMIA" è esattamente 70. □

2 — Determinare in quanti modi si possa colorare un ottagono regolare in modo che abbia quattro lati bianchi e quattro lati neri.

Soluzione: La soluzione si trova tramite il Teorema di Burnside, nel modo seguente.

Dopo aver numerato da 1 a 8 i lati dell'ottagono dato, sia $\mathcal{K}_8$ l'insieme di tutte le possibili colorazioni dell'ottagono: in termini matematici, $\mathcal{K}_8$ è l'insieme di tutte le possibili applicazioni $\mathcal{L} := \{1,\dots,8\} \xrightarrow{\kappa} \{B,N\}$ da $\{1,\dots,8\}$ — identificato con l'insieme $\mathcal{L}$ dei lati — a $\{B,N\}$ — identificato con l'insieme dei due colori "bianco" e "nero" — tali che

$$\Big|\big\{\,\ell\in\{1,\dots,8\}\,\big|\,\kappa(\ell)=B\,\big\}\Big| \;=\; 4 \;=\; \Big|\big\{\,\ell\in\{1,\dots,8\}\,\big|\,\kappa(\ell)=N\,\big\}\Big|\,.$$

Se poi rimuoviamo la numerazione dei lati, due applicazioni diverse possono dar luogo alla stessa "colorazione". Ciò accade se e soltanto se le due applicazioni si trovano nella stessa orbita per un'opportuna azione di un certo gruppo G su $\mathcal{K}_8$: pertanto, contare le colorazioni che in esame equivale a contare le G–orbite di tale azione in $\mathcal{K}_8$.

A meno di riordinamenti, possiamo sempre assumere che la nostra numerazione dei lati sia fatta in ordine progressivo: dunque, tale numerazione è univocamente determinata da:

– *a)* la scelta del *primo* lato da colorare,

– *b)* la scelta del *verso* (rotatorio) di percorrenza del perimetro dell'ottagono.

Da questo segue che si può passare da una qualsiasi numerazione ad una qualsiasi altra tramite un opportuno *movimento rigido* dell'ottagono, cioè una rotazione o un ribaltamento. Pertanto, il gruppo G del quale dobbiamo considerare un'azione su $\mathcal{K}_8$ è il gruppo dei movimenti rigidi dell'ottagono (regolare), cioè il gruppo diedrale D_8.

L'azione di D_8 su $\mathcal{K}_8$ che dobbiamo considerare è la seguente. D_8 agisce sull'ottagono per permutazione dei vertici: questo induce anche in modo canonico un'azione sull'insieme $\mathcal{L}$ dei lati dell'ottagono, identificati con le coppie di vertici adiacenti (cioè, appunto, estremi di uno stesso lato...). Questo a sua volta induce un'azione sull'insieme di applicazioni $\mathcal{K}_8$, ottenuta facendo precedere ad ogni applicazione l'azione *inversa* di D_8 sui lati! In definitiva, l'azione — esplicita — di D_8 su $\mathcal{K}_8$ che ci interessa è questa:

$$D_8\times\mathcal{K}_8\longrightarrow\mathcal{K}_8\;,\quad (\delta,\kappa)\;\mapsto\;\delta.\kappa\;:\left(\begin{array}{c}\mathcal{L}\xrightarrow{\qquad\delta.\kappa\qquad}\{B,N\}\\ \ell\;\mapsto\;(\delta.\kappa)(\ell):=\kappa.\big(\delta^{-1}(\ell)\big)\end{array}\right)$$

Se invece preferiamo descrivere ogni G–spazio X tramite la rappresentazione (cioè il morfismo di gruppi) $G\xrightarrow{\rho}\mathcal{S}(X)$, $g\mapsto g_X$, che corrisponde all'azione in esame, allora la rappresentazione di D_8 su $\mathcal{K}_8$ indotta da quella sull'insieme $\{1,2,\dots,8\}$ dei lati è data da

$$D_8\longrightarrow\mathcal{S}\big(\mathcal{K}_8\big)\;,\quad \delta\;\mapsto\;\delta_{\mathcal{K}_8}\;:\left(\begin{array}{c}\mathcal{K}_8\xrightarrow{\delta.\kappa}\mathcal{K}_8\\ \kappa\;\mapsto\;\kappa\circ\delta_{\mathcal{L}}^{-1}\end{array}\right)$$

((N.B.: ci vuol più tempo a leggerla (e a scriverla) che a capirla, 'sta costruzione...))

Una volta fissati il gruppo D_8 e la sua azione su $\mathcal{K}_8$, il numero N di orbite di tale azione è dato dalla formula esplicita fornita dal Teorema di Burnside: in generale, per l'azione di un gruppo G su un insieme X tale formula esprime il numero di G–orbite in X come

$$N \;=\; \big|G\big|^{-1} \sum_{g\in G} \big|X^g\big| \tag{1}$$

dove $X^g := \big\{ x \in X \,\big|\, g.x = x \big\}$ per ogni $g \in G$. Nel caso in esame, è $G := D_8$, $X := \mathcal{K}_8$, e la (1) diventa

$$N \;=\; \big|D_8\big|^{-1} \sum_{\delta\in D_8} \big|\mathcal{K}_8{}^{\delta}\big| \tag{2}$$

Poiché $\big|D_8\big| = 2\cdot 8 = 16$, ci resta soltanto da calcolare la cardinalità dei vari sottoinsiemi $\mathcal{K}_8{}^{\delta}$, i quali devono essere descritti uno per uno!

Per descrivere i vari $\mathcal{K}_8{}^{\delta}$ dobbiamo innanzi tutto descrivere gli elementi di $\mathcal{K}_8$. Dato che si tratta di applicazioni con dominio l'insieme finito $\{1,2,\dots,8\}$, le descriviamo tramite stringhe di otto elementi, precisamente le immagini, nell'ordine, degli elementi di $\{1,2,\dots,8\}$: in altre parole, ogni $\kappa \in \mathcal{K}_8$ sarà descritta come $\kappa \cong \big(\kappa(1),\kappa(2),\dots,\kappa(8)\big)$.

Inoltre, dobbiamo descrivere gli elementi di D_8. Questi si dividono in *rotazioni* (rispetto al centro dell'ottagono) e *ribaltamenti* (rispetto ad una diagonale o ad un asse dell'ottagono). Se indichiamo con ρ una rotazione di angolo $2\pi/8$, l'insieme di tutte le rotazioni è $\big\{ \rho^s \,\big|\, s = 1,2,\dots,7 \big\}$, con $\rho^0 = id$.

$\underline{\delta = id} \quad\Longrightarrow\quad \mathcal{K}_8{}^{\delta} = \mathcal{K}_8{}^{id} = \mathcal{K}_8 \quad\Longrightarrow\quad \big|\mathcal{K}_8{}^{\delta}\big| = \big|\mathcal{K}_8{}^{id}\big| = \big|\mathcal{K}_8\big| = \binom{8}{4,4} = \binom{8}{4} = 70$

Infatti, gli elementi di $\mathcal{K}_8$ sono tanti quanti i possibili modi di scegliere, tra gli 8 lati dell'ottagono, il sottoinsieme dei 4 elementi "bianchi" e quello dei 4 elementi "neri".

$\underline{\delta = \rho} \quad\Longrightarrow\quad \mathcal{K}_8{}^{\delta} = \mathcal{K}_8{}^{\rho} = \emptyset \quad\Longrightarrow\quad \big|\mathcal{K}_8{}^{\delta}\big| = \big|\mathcal{K}_8{}^{\rho}\big| = \big|\emptyset\big| = 0$

Infatti, se esistesse un $\kappa \cong \big(\kappa(1),\kappa(2),\dots,\kappa(8)\big) \in \mathcal{K}_8{}^{\rho}$, allora la condizione di ρ–invarianza determinerebbe che

$$\kappa(i+1) \;=\; \big(\kappa\,\rho^{-1}\big)\big(i+1\big) \;=\; \big(\kappa\,\rho^{-1}\big)\big(\rho(i)\big) \;=\; \kappa\big(\rho^{-1}\rho(i)\big) \;=\; \kappa(i) \qquad \forall\; i = 1,\dots,7$$

(per costruzione e per il fatto che $\rho(i) = i+1$, per ogni $i \,(\mathrm{mod}\, 8)$), cioè in complesso $\kappa(1) = \kappa(2) = \cdots = \kappa(8)$. Quindi nella colorazione κ tutti i lati dell'ottagono avrebbero lo stesso colore, il che è assurdo! Perciò $\mathcal{K}_8{}^{\rho} = \emptyset$.

$\underline{\delta = \rho^2} \quad\Longrightarrow\quad \Big|\mathcal{K}_8{}^{\delta}\Big| = \Big|\mathcal{K}_8{}^{\rho^2}\Big| = 2$

Infatti, se $\kappa \cong \big(\kappa(1),\kappa(2),\dots,\kappa(8)\big) \in \mathcal{K}_8{}^{\rho^2}$ allora, analogamente a prima, la condizione di ρ^2–invarianza implica $\kappa(i+2) = \kappa(i)$ per ogni $i \,(\mathrm{mod}\, 8)$, cioè $\kappa(1) = \kappa(3) = \kappa(5) = \kappa(7)$ e $\kappa(2) = \kappa(4) = \kappa(6) = \kappa(8)$. Quindi la colorazione κ è univocamente determinata dalla scelta dei due colori (necessariamente distinti!) del lato 1 e del lato 2, scelta che

per il resto è arbitraria! Ci sono allora esattamente due possibili scelte, precisamente $\big(\kappa(1),\kappa(2)\big) = (B,N)$ e $\big(\kappa(1),\kappa(2)\big) = (N,B)$; da questo allora si conclude che $\mathcal{K}_8^{\,\rho^2} = \big\{(B,N,B,N,B,N,B,N),(N,B,N,B,N,B,N,B)\big\}$ e così $\Big|\mathcal{K}_8^{\,\rho^2}\Big| = 2$.

$\underline{\delta = \rho^3} \quad\Longrightarrow\quad \mathcal{K}_8^{\,\delta} = \mathcal{K}_8^{\,\rho^3} = \emptyset \quad\Longrightarrow\quad \Big|\mathcal{K}_8^{\,\delta}\Big| = \Big|\mathcal{K}_8^{\,\rho^3}\Big| = 0$

Infatti, se esistesse $\kappa \cong \big(\kappa(1),\kappa(2),\dots,\kappa(8)\big) \in \mathcal{K}_8^{\,\rho^3}$, analogamente a prima la ρ^3–invarianza implicherebbe $\kappa(i+3) = \kappa(i)$ per ogni $i \,(\mathrm{mod}\, 8)$, quindi $\kappa(1) = \kappa(4) = \kappa(7) = \kappa(2) = \kappa(5) = \kappa(8) = \kappa(3) = \kappa(6)$. Quindi nella colorazione κ tutti i lati dell'ottagono avrebbero lo stesso colore, il che è assurdo! Perciò si ha necessariamente $\mathcal{K}_8^{\,\rho^3} = \emptyset$.

In alternativa, possiamo sfruttare la seguente osservazione. Se un gruppo G agisce su un insieme X, se H è un sottogruppo di G poniamo

$$X^H := \big\{ x \in X \,\big|\, h.x = x\,,\ \forall\, h \in H \big\} = \textstyle\bigcap_{h\in H} X^h$$

Allora, se $\langle g\rangle$ indica il sottogruppo di G generato da un qualsiasi elemento $g \in G$, dalle definizioni segue subito che $X^g = X^{\langle g\rangle}$. Nel caso in esame, osserviamo che $\big\langle \rho^3 \big\rangle = \langle \rho \rangle$, e quindi $\mathcal{K}_8^{\,\rho^3} = \mathcal{K}_8^{\langle \rho^3\rangle} = \mathcal{K}_8^{\langle \rho\rangle} = \mathcal{K}_8^{\,\rho} = \emptyset$ per quanto già visto, dunque $\mathcal{K}_8^{\,\rho^3} = \emptyset$.

$\underline{\delta = \rho^4} \quad\Longrightarrow\quad \Big|\mathcal{K}_8^{\,\delta}\Big| = \Big|\mathcal{K}_8^{\,\rho^4}\Big| = 6$

Infatti, se $\kappa \cong \big(\kappa(1),\kappa(2),\dots,\kappa(8)\big) \in \mathcal{K}_8^{\,\rho^4}$, la ρ^4–invarianza implica $\kappa(i+4) = \kappa(i)$ per ogni $i \,(\mathrm{mod}\, 8)$, cioè $\kappa(1) = \kappa(5) =$, $\kappa(2) = \kappa(6)$, $\kappa(3) = \kappa(5)$, $\kappa(4) = \kappa(8)$. Quindi la colorazione κ è univocamente determinata dalla scelta dei colori dei lati 1, 2, 3 e 4, che per il resto è arbitraria! Le scelte possibili allora sono $\binom{4}{2\,,\,2} = \binom{4}{2} = 6$, così che $\Big|\mathcal{K}_8^{\,\rho^4}\Big| = 6$.

$\underline{\delta = \rho^5} \quad\Longrightarrow\quad \mathcal{K}_8^{\,\delta} = \mathcal{K}_8^{\,\rho^5} = \emptyset \quad\Longrightarrow\quad \Big|\mathcal{K}_8^{\,\delta}\Big| = \Big|\mathcal{K}_8^{\,\rho^5}\Big| = 0$

Infatti, si ripresenta una situazione del tutto analoga a quella del caso di $\delta = \rho^3$, e quindi si può ripetere quella discussione. In particolare, si può sfruttare il fatto che $\big\langle \rho^5 \big\rangle = \langle \rho \rangle$, e quindi $\mathcal{K}_8^{\,\rho^5} = \mathcal{K}_8^{\langle \rho^5\rangle} = \mathcal{K}_8^{\langle \rho\rangle} = \mathcal{K}_8^{\,\rho} = \emptyset$. Oppure, si può osservare che dalle definizioni segue che, in generale, $X^{g^{-1}} = X^g$, e quindi poiché $\rho^5 = \big(\rho^3\big)^{-1}$ nel gruppo D_8, si ottiene in particolare che $\mathcal{K}_8^{\,\rho^5} = \mathcal{K}_8^{\,\rho^3} = \emptyset$.

$\underline{\delta = \rho^6} \quad\Longrightarrow\quad \Big|\mathcal{K}_8^{\,\delta}\Big| = \Big|\mathcal{K}_8^{\,\rho^6}\Big| = 2$

Infatti, la situazione è del tutto analoga a quella del caso $\delta = \rho^2$, per cui si può ripetere quella discussione. Oppure, osservando che $\rho^6 = \big(\rho^2\big)^{-1}$ nel gruppo D_8, si ottiene subito che $\mathcal{K}_8^{\,\rho^6} = \mathcal{K}_8^{\,\rho^2} = \big\{(B,N,B,N,B,N,B,N),(N,B,N,B,N,B,N,B)\big\}$ e così $\Big|\mathcal{K}_8^{\,\rho^6}\Big| = 2$.

$\underline{\delta = \rho^7} \quad\Longrightarrow\quad \mathcal{K}_8^{\,\delta} = \mathcal{K}_8^{\,\rho^7} = \emptyset \quad\Longrightarrow\quad \Big|\mathcal{K}_8^{\,\delta}\Big| = \Big|\mathcal{K}_8^{\,\rho^7}\Big| = 0$

Infatti, la situazione è del tutto analoga a quella del caso $\delta = \rho$, per cui si può ripetere quella discussione. Oppure, dato che $\rho^7 = \big(\rho^2\big)^{-1}$ nel gruppo D_8, si ottiene subito che $\mathcal{K}_8^{\,\rho^7} = \mathcal{K}_8^{\,\rho} = \emptyset$ per quanto già visto, e quindi $\Big|\mathcal{K}_8^{\,\rho^7}\Big| = 0$.

$\underline{\delta = \sigma_b}$ *ribaltamento rispetto a una bisettrice* $b \implies \left|\mathcal{K}_8{}^{\delta}\right| = \left|\mathcal{K}_8{}^{\sigma_b}\right| = \binom{4}{2\,,\,2} = \binom{4}{2} = 6$
Infatti, ci devono esserce due lati neri e due lati bianchi da una parte e dall'altra della bisettrice b. Inoltre, i lati neri, risp. i lati bianchi, si corrispondono da una parte all'altra di b secondo la simmetria speculare (cioè appunto la riflessione) rispetto a b stessa. Pertanto, la configurazione è determinata univocamente dalla (libera) scelta di come colorare i quattro lati da una parte di b in modo che due siano neri e due bianchi. Il numero di tali possibili scelte è $\binom{4}{2\,,\,2} = \binom{4}{2} = 6$, quindi $\left|\mathcal{K}_8{}^{\delta}\right| = \left|\mathcal{K}_8{}^{\sigma_b}\right| = 6$.

Si noti che esistono esattamente 4 bisettrici, dunque 4 movimenti del tipo ora analizzato.

$\underline{\delta = \tau_a}$ un *ribaltamento rispetto a un asse* $a \quad \implies \quad \left|\mathcal{K}_8{}^{\delta}\right| = \left|\mathcal{K}_8{}^{\tau_a}\right| = 6$
Infatti, l'asse a considerato taglia due lati ℓ e ℓ' opposti l'uno all'altro. Se di essi uno è nero e l'altro bianco, restano tre lati neri e tre lati bianchi, i quali devono essere disposti in modo specularmente simmetrico da una parte e dall'altra di a, il che è impossibile! Perciò ℓ e ℓ' devono essere dello stesso colore. Se tale colore è nero, restano due lati neri e quattro lati bianchi, in posizioni specularmente simmetriche da una parte e dall'altra di a: pertanto tale configurazione è univocamente determinata dalla (libera) scelta di come disporre due lati bianchi e uno nero da una stessa parte (prefissata) di a. Il numero di tali possibili scelte è $\binom{3}{2} = 3$. Allo stesso modo, ci sono esattamente altre 3 colorazioni per le quali i due lati tagliati dall'asse a sono bianchi. In totale dunque $\left|\mathcal{K}_8{}^{\delta}\right| = \left|\mathcal{K}_8{}^{\tau_a}\right| = 3 + 3 = 6$.

Si noti che esistono esattamente 4 assi, dunque 4 movimenti del tipo ora analizzato.

In conclusione, grazie all'analisi precedente la (2) diventa

$$N \;=\; \big|D_8\big|^{-1} \sum_{\delta \in D_8} \left|\mathcal{K}_8{}^{\delta}\right| \;=\; 16^{-1} \left(\sum_{n=0}^{7} \left|\mathcal{K}_8{}^{\rho^n}\right| + \sum_{b \text{ bisettrice}} \left|\mathcal{K}_8{}^{\sigma_b}\right| + \sum_{a \text{ asse}} \left|\mathcal{K}_8{}^{\tau_a}\right| \right) \;=$$

$$= \; 16^{-1} \Big(\big(70 + 0 + 2 + 0 + 6 + 0 + 2 + 0\big) + \big(6 + 6 + 6 + 6\big) + \big(6 + 6 + 6 + 6\big) \Big) \;=$$

$$= \; 16^{-1} \Big(80 + 24 + 24\Big) \;=\; 8$$

quindi la risposta finale è che il numero di anagrammi richiesto è $N = 8$. $\square$

3 — Dato il gruppo simmetrico $\mathcal{S}_8$, si consideri la sua azione naturale sull'insieme $X_8 := \{1, 2, 3, 4, 5, 6, 7, 8\}$. Sia poi $H := \big\langle (1, 3, 4)(7, 8), (2, 8, 3, 7) \big\rangle$ il sottogruppo di $\mathcal{S}_8$ generato dalle permutazioni $(1, 3, 4)(7, 8)$ e $(2, 8, 3, 7)$, e si consideri l'azione di H su X_8 indotta (per restrizione) da quella di $\mathcal{S}_8$.

(a) Calcolare le orbite dell'azione di H su X_8.

(b) Per ciascun elemento $x \in \{2, 5, 6\} \subseteq X_8$, calcolare (in H) il corrispondente sottogruppo stabilizzatore St_x.

(c) Determinare per quali coppie di elementi (x, y) con $x, y \in \{2, 5, 6\}$ si abbia che St_x è coniugato a St_y in H, cioè esista un $h \in H$ tale che $St_x = h\, St_y\, h^{-1}$.

Soluzione: *(a)* Indichiamo con $\sigma := (1,3,4)(7,8)$ e $\tau := (2,8,3,7)$ i due generatori del sottogruppo H. Per calcolare le orbite di H in X_8, che sono i sottoinsiemi $\mathcal{O}_x := \{\, h.x \,|\, h \in H \,\}$ al variare di $x \in X_8$, osserviamo che

$$\sigma(y) = y\,, \quad \tau(y) = y \quad \Longrightarrow \quad \mathcal{O}_y = H.y = \langle \sigma, \tau \rangle .y = \{y\} \qquad \forall\ y \in \{5, 6\}$$

così che $\mathcal{O}_5 = \{5\}$ e $\mathcal{O}_6 = \{6\}$. Per le altre orbite, osserviamo che l'azione di H a partire dall'elemento 1 ottiene la seguente successione di elementi:

$$1 \overset{\sigma}{\mapsto} 3 \overset{\tau}{\mapsto} 7 \overset{\tau}{\mapsto} 2 \overset{\tau}{\mapsto} 8 \overset{\tau}{\mapsto} 3 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 1$$

per cui abbiamo che $\mathcal{O}_1 \supseteq \{1, 3, 7, 2, 8, 4\}$. D'altra parte per quanto già visto abbiamo anche che $\{1, 3, 7, 2, 8, 4\} = X_8 \setminus \big(\mathcal{O}_5 \bigcup \mathcal{O}_6\big)$; poiché orbite distinte sono sempre disgiunte, abbiamo allora $\mathcal{O}_1 \supseteq X_8 \setminus \big(\mathcal{O}_5 \bigcup \mathcal{O}_6\big) = \{1, 3, 7, 2, 8, 4\}$. Pertanto, concludiamo che $\mathcal{O}_1 = \{1, 2, 3, 4, 7, 8\}$.

In conclusione, le orbite dell'azione di H su X_8 sono tre, e precisamente

$$\mathcal{O}_5 = \{5\}\,, \quad \mathcal{O}_6 = \{6\}\,, \quad \mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \mathcal{O}_4 = \mathcal{O}_7 = \mathcal{O}_8 = \{1, 2, 3, 4, 7, 8\}$$

(b) Tra i due generatori di H abbiamo che $\sigma(2) = 2$, quindi $\sigma \in St_2$, e in conseguenza si ha anche $\langle \sigma \rangle \subseteq St_2$. Più in generale, ogni elemento di $h \in H := \langle \sigma, \tau \rangle$ è della forma $h = \sigma^{s_1} \tau^{t_1} \sigma^{s_2} \tau^{t_2} \cdots \sigma^{s_k} \tau^{t_k}$ con $k \in \mathbb{N}$ e $s_i, t_i \in \mathbb{Z}$ per ogni indice i, e inoltre $(s_1, t_1) \neq (0, 0)$ e $s_2, t_2, s_3, \ldots, s_{k-1}, t_{k-1}, s_k \neq 0$ se $k > 1$. Poiché σ ha ordine 6 e τ ha ordine 4, possiamo anche assumere che siano $0 \leq s_1 \leq 5$, $0 \leq t_1 \leq 3$, $1 \leq s_2, s_3, \ldots, s_{k-1}, s_k \leq 5$, $1 \leq t_2, \ldots t_{k-1} \leq 3$, $0 \leq t_k \leq 3$, se $k > 1$. Infine, poiché $\sigma \in St_2$ abbiamo anche che

$$h \,=\, \sigma^{s_1} \tau^{t_1} \sigma^{s_2} \tau^{t_2} \cdots \sigma^{s_k} \tau^{t_k} \in St_2 \iff \sigma^{-s_1}\, h \,=\, \tau^{t_1} \sigma^{s_2} \tau^{t_2} \cdots \sigma^{s_k} \tau^{t_k} \in St_2$$

In definitiva, analizzando come i generatori σ e τ permettono di "spostarsi" da un punto all'altro dell'orbita $\mathcal{O}_2$, si trova chelo stabilizzatore St_2 è composto di tutti e soli gli elementi h che sono prodotti di fattori del tipo D_D oppure T dove

$$D_D \in \big\{\, \tau\, \sigma^d \tau\,,\ \tau^3 \sigma^p \tau\,,\ \tau^3 \sigma^d \tau^3,\ \tau \sigma^p \tau^3 \,\big|\, p \in \{2, 4\}\,,\, d \in \{1, 3, 5\} \,\big\}$$

è una permutazione che porta 2 in 2 "muovendosi" all'interno dell'insieme $\{2, 8, 3, 7\}$, mentre T (che "passa per 3") è a sua volta un prodotto $T = T_D \cdot (T_T)^e \cdot D_T$, con $e \in \mathbb{Z}$ e

$$\begin{aligned}
D_T \ &\in \big\{\, \tau\, \sigma^p \tau\,,\ \tau^3 \sigma^d \tau\,,\ \tau^3 \sigma^p \tau^3,\ \tau \sigma^d \tau^3 \,\big|\, p \in \{2, 4\}\,,\, d \in \{1, 3, 5\} \,\big\} && \textit{(sposta da 2 a 3)} \\
T_T \ &\in \big\{\, \sigma\, \tau^a \sigma\, \tau^c \sigma \,\big|\, a, c \in \{0, 1, 2, 3\} \,\big\} && \textit{(sposta da 3 a 3)} \\
T_D \ &\in \big\{\, \tau^3\, \sigma^p \tau\,,\ \tau \sigma^d \tau\,,\ \tau \sigma^p \tau^3,\ \tau^3 \sigma^d \tau^3 \,\big|\, p \in \{2, 4\}\,,\, d \in \{1, 3, 5\} \,\big\} && \textit{(sposta da 3 a 2)}
\end{aligned}$$

Per gli altri due casi, sia 5 che 6 sono fissati da ciascuno dei due generatori di H, quindi anche da ogni elemento di H; perciò in tal caso abbiamo $St_5 = H$ e $St_6 = H$.

(b) Dato che $St_5 = H = St_6$ mentre $St_2 \neq H$, abbiamo che per $x, y \in \{2, 5, 6$ si ha che St_x è coniugato a St_y se e soltanto se $(x, y) \in \big\{(5,5), (6,6), (5,6), (6,5)\big\}$. □

4 — Sia G un gruppo di ordine 56. Dimostrare che esiste in G sottogruppo normale non banale.

Soluzione: Detto p un primo che divida 56, indichiamo con ν_p il numero di p–sottogruppi di Sylow in G. Poiché la fattorizzazione di 56 in primi è $56 = 2^3 \cdot 7$, i primi che ci interessano sono 2 e 7.

L'idea è questa: se per un $p \in \{2, 3\}$ si ha $\nu_p = 1$, allora c'è uno ed un solo p–sottogruppo di Sylow, che chiamiamo H_p. Poiché però tutti i p–sottogruppi di Sylow in G sono coniugati, ciò vuol dire che H_p *è normale*, e quindi H_p è un sottogruppo normale non banale di G, come richiesto.

Per calcolare i numeri ν_p, dai Teoremi di Sylow sappiamo che

$$\nu_2 \equiv 1 \mod 2\,, \quad \nu_2 \big| 7\,, \qquad\qquad \nu_7 \equiv 1 \mod 7\,, \quad \nu_7 \big| 8$$

e quindi $$\nu_2 \in \{1, 3, 5, 7\}\,, \qquad \nu_7 \in \{1, 8\}\,.$$

Dimostriamo ora che dev'essere necessariamente $\nu_2 = 1$ oppure $\nu_7 = 1$.

Se $\nu_7 = 1$ siamo a posto. Altrimenti, osserviamo che ogni 7–sottogruppo di Sylow contiene un solo elemento di ordine 1, cioè l'elemento neutro e_G, e poi esattamente altri $7 - 1 = 6$ elementi di ordine 7. Inoltre, due distinti 7–sottogruppi di Sylow hanno necessariamente per intersezione il solo sottogruppo banale, cioè $\{e_G\}$. Pertanto, l'unione di tutti i 7–sottogruppi di Sylow, che chiamiamo $\mathbb{S}_7$, si compone dell'elemento neutro e_G e di esattamente $\nu_7 \cdot 6$ elementi di ordine 7. Avendo supposto che $\nu_7 \neq 1$, abbiamo allora $\nu_7 = 8$. Perciò la suddetta unione $\mathbb{S}_7$ contiene esattamente $1 + 8 \cdot 6 = 49$ elementi, di ordine 1 — il primo — oppure 7 — tutti gli altri. Rimangono in $G \setminus \mathbb{S}_7$ esattamente

$$\big|G \setminus \mathbb{S}_7\big| \;=\; |G| - |\mathbb{S}_7| \;=\; 56 - 49 \;=\; 7 \tag{3}$$

elementi. Infine, G contiene almeno un 2–sottogruppo di Sylow, sia H_2, il quale contiene esattamente $2^3 = 8$ elementi: di essi, l'elemento neutro ha ordine 2, mentre gli altri sette hanno ordine 2, oppure $2^2 = 4$, oppure $2^3 = 8$. In particolare, si ha $H_2 \bigcap \mathbb{S}_7 = \{e_G\}$, e quindi $\big(H_2 \setminus \{e_G\}\big) \subseteq \big(G \setminus \mathbb{S}_7\big)$. Pertanto, dalla (3) e da $\big|H_2 \setminus \{e_G\}\big| = 7$ otteniamo

che $G \setminus \mathbb{S}_7 = H_2 \setminus \{e_G\}$. In particolare, ciò significa che H_2 è l'*unico* 2–sottogruppo di Sylow di G, per cui $\nu_2 = 1$. Infatti, ogni altro 2–sottogruppo di Sylow di G avrebbe un elemento non banale h che non appartiene ad H_2, e quindi deve appartenere a $\mathbb{S}_7$: ma allora, per costruzione, l'ordine di g sarebbe 1, che è assurdo perché $g \neq e_G$, oppure sarebbe 7, mentre invece dev'essere 2, oppure 4, oppure 8, perché g è elemento non banale di un 2–sottogruppo di Sylow di G, e vale l'analisi degli ordini già fatta per il caso di H_2.

La conclusione è che se $\nu_7 \neq 1$ allora necessariamente si ha $\nu_2 = 1$. □

5 — Sia G un gruppo. In ciascuno dei due casi seguenti

(a) G ha ordine 40 — *(b)* G ha ordine 28

si determini se sia possibile scomporre G come prodotto semidiretto di due suoi sottogruppi non banali, cioè sia $G \cong H \ltimes N$ con H e N sottogruppi non banali di G, con N normale.

In caso affermativo, si specifichi l'ordine di ciascuno di tali sottogruppi, precisando quale sia l'ordine del sottogruppo normale.

Infine, si specifichino gli eventuali casi nei quali tale prodotto semidiretto risulti essere un prodotto *diretto*, cioè sia $G \cong H \times N$.

Soluzione: Detto p un primo che divida l'ordine di G, indichiamo con ν_p il numero di p–sottogruppi di Sylow in G. Se per un tale primo p si ha $\nu_p = 1$, allora c'è uno ed un solo p–sottogruppo di Sylow di G, che chiamiamo N_p. Dato che tutti i p–sottogruppi di Sylow in G sono coniugati, ciò implica che N_p è *normale* in G, non banale per costruzione.

(a) Per $|G| = 40 = 2^3 \cdot 5$, i primi da considerare sono 2 e 5. Per calcolare i numeri ν_p, dai Teoremi di Sylow sappiamo che

$$\nu_2 \equiv 1 \mod 2\,, \quad \nu_2 \Big| 5\,, \qquad\qquad \nu_5 \equiv 1 \mod 5\,, \quad \nu_5 \Big| 8$$

e quindi $\nu_2 \in \{1, 5\}$, $\nu_5 \in \{1\}$, cioè in particolare $\nu_5 = 1$. Dunque esiste in G un 5-sottogruppo di Sylow normale, sia N_5, il cui ordine è 5, e d'altra parte esiste almeno un 2-sottogruppo di Sylow, sia H_2, di ordine $2^3 = 8$. Chiaramente $H_2 \bigcap N_5 = \{e_G\}$, perché dev'essere un sottogruppo di G di ordine che divida $|H_2| = 2^3$ e anche $|N_5| = 5$, quindi di ordine 1. Allora il prodotto $H_2 \cdot N_5$, come sottoinsieme di G, è un sottogruppo di G di ordine multiplo di $|H_2| = 2^3$ e di $|N_5| = 5$, dunque multiplo di 40. Perciò $H_2 \cdot N_5 = G$, con $H_2 \bigcap N_5 = \{e_G\}$, $H_2 \leq G$ e $N_5 \trianglelefteq G$; pertanto si conclude che $G \cong H_2 \ltimes N_5$.

In generale, tale prodotto semidiretto potrebbe non essere diretto: infatti, esistono esempi in cui è proprio così, cioè in cui il sottogruppo H_2 *non* è normale in G.

(b) Per $|G| = 28 = 2^2 \cdot 7$, i primi da considerare sono 2 e 7. Per calcolare i numeri ν_p, dai Teoremi di Sylow sappiamo che

$$\nu_2 \equiv 1 \mod 2\,, \quad \nu_2 \Big| 7\,, \qquad\qquad \nu_7 \equiv 1 \mod 7\,, \quad \nu_7 \Big| 4$$

e quindi $\nu_2 \in \{1,7\}$, $\nu_7 \in \{1\}$, cioè in particolare $\nu_7 = 1$. Dunque esiste in G un 7-sottogruppo di Sylow normale, sia N_7, il cui ordine è 7, ed esiste anche almeno un 2-sottogruppo di Sylow, sia H_2, di ordine $2^2 = 4$. Chiaramente $H_2 \bigcap N_7 = \{e_G\}$, perché dev'essere un sottogruppo di G di ordine che divida $|H_2| = 2^2$ e anche $|N_7| = 7$, quindi di ordine 1. Allora il prodotto $H_2 \cdot N_7$, come sottoinsieme di G, è un sottogruppo di G di ordine multiplo di $|H_2| = 2^2$ e di $|N_7| = 7$, dunque multiplo di 28. Perciò $H_2 \cdot N_7 = G$, con $H_2 \bigcap N_7 = \{e_G\}$, $H_2 \leq G$ e $N_7 \trianglelefteq G$; pertanto si conclude che $G \cong H_2 \ltimes N_7$.

In generale, tale prodotto semidiretto potrebbe non essere diretto: in effetti, esistono esempi in cui accade proprio questo, cioè in cui il sottogruppo H_2 *non* è normale in G. □

6 — Determinare quanti gruppi abeliani esistono, a meno di isomorfismo, di ordine 1200 e di ordine 405. Inoltre, si determini esplicitamente uno di tali gruppi per ciascuna classe di isomorfismo.

Soluzione: Dalla teoria generale si ha che, se $n \in \mathbb{N}_+$ si fattorizza in $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ con $p_1, p_2, \ldots, p_k$ primi distinti e $e_1, e_2, \ldots, e_k \in \mathbb{N}_+$, allora il numero $N(n)$ di gruppi abeliani (a due a due non isomorfi) di ordine n è dato da $N(n) = \prod_{i=1}^{k} E_i$, dove E_i è il numero di partizioni del numero e_i (per ogni i). Inoltre, per ogni scelta di tali partizioni $\eta_i = (e_{i,1}, \ldots, e_{i,s_i})$ — cioè $e_{i,1} \geq \cdots \geq e_{i,s_i}$ e $e_{i,1} + \cdots + e_{i,s_i} = e_i$ (per ogni i) — si ha che

$$A(\eta_1, \ldots, \eta_k) := \mathbb{Z}_{p_1}^{e_{1,1}} \times \cdots \times \mathbb{Z}_{p_1}^{e_{1,s_1}} \times \mathbb{Z}_{p_2}^{e_{2,1}} \times \cdots \times \mathbb{Z}_{p_{k-1}}^{e_{k-1,s_{k-1}}} \times \mathbb{Z}_{p_k}^{e_{k,1}} \times \cdots \times \mathbb{Z}_{p_k}^{e_{k,s_k}}$$

è un gruppo abeliano di ordine n, due di tali gruppi corrispondenti a scelte diverse delle partizioni sono non isomorfi, ed ogni gruppo abeliano di ordine n è isomorfo ad uno dei gruppi $A(\eta_1, \ldots, \eta_k)$. Ora, nei casi specifici in esame si ha:

$n = 1200 \quad \Longrightarrow \quad n = 1200 = 2^4 3\, 5^2 \quad \Longrightarrow$

— le partizioni di $e_1 = 4$ sono $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$, dunque sono in tutto $E_1 = 5$;

— le partizioni di $e_2 = 1$ sono una sola, precisamente (1), e quindi $E_2 = 1$;

— le partizioni di $e_3 = 2$ sono $(2), (1,1)$, per cui $E_3 = 2$.

Dalla regola generale, concludiamo che, a meno di isomorfismi, esistono esattamente $N(1200) = 5 \cdot 1 \cdot 2 = 10$ gruppi abeliani (a due a due non isomorfi) di ordine 1200. Esplicitamente, essi sono i gruppi $A_2 \times A_3 \times A_5$ con

$$\begin{aligned} A_2 &\in \left\{ \mathbb{Z}_2^4, \mathbb{Z}_2^3 \times \mathbb{Z}_2^1, \mathbb{Z}_2^2 \times \mathbb{Z}_2^2, \mathbb{Z}_2^2 \times \mathbb{Z}_2^1 \times \mathbb{Z}_2^1, \mathbb{Z}_2^1 \times \mathbb{Z}_2^1 \times \mathbb{Z}_2^1 \times \mathbb{Z}_2^1 \right\} \\ A_3 &= \mathbb{Z}_3 \\ A_5 &\in \left\{ \mathbb{Z}_5^2, \mathbb{Z}_5^1 \times \mathbb{Z}_5^1 \right\} \end{aligned}$$

$\underline{n = 405} \implies n = 405 = 3^4 5 \implies$

— le partizioni di $e_1 = 4$ sono $(4), (3,1), (2,2), (2,1,1), (1,1,1,1)$, dunque sono in tutto $E_1 = 5$;

— le partizioni di $e_2 = 1$ sono una sola, precisamente (1), e quindi $E_2 = 1$.

Dalla regola generale, concludiamo che, a meno di isomorfismi, esistono esattamente $N(405) = 5 \cdot 1 = 5$ gruppi abeliani (a due a due non isomorfi) di ordine 405. Esplicitamente, essi sono i gruppi $A_3 \times A_5$ con

$$A_3 \in \left\{ \mathbb{Z}_3^4 \,,\, \mathbb{Z}_3^3 \times \mathbb{Z}_3^1 \,,\, \mathbb{Z}_3^2 \times \mathbb{Z}_3^2 \,,\, \mathbb{Z}_3^2 \times \mathbb{Z}_2^1 \times \mathbb{Z}_3^1 \,,\, \mathbb{Z}_3^1 \times \mathbb{Z}_3^1 \times \mathbb{Z}_3^1 \times \mathbb{Z}_3^1 \right\}, \quad A_5 = \mathbb{Z}_5 \,. \quad \square$$

7 — Si consideri il sottoinsieme $\mathbb{Z}_{\{7\}}$ dell'insieme $\mathbb{Q}$ dei numeri razionali così definito:

$$\mathbb{Z}_{\{7\}} := \left\{ 7^e a \;\middle|\; e \in \mathbb{Z} \,,\, a \in \big(\mathbb{Z} \setminus 7\,\mathbb{Z}\big) \right\} = \left\{ 7^{-n} z \;\middle|\; n \in \mathbb{N} \,,\, z \in \mathbb{Z} \right\}$$

(a) Dimostrare che $\mathbb{Z}_{\{7\}}$ è un dominio euclideo rispetto alla valutazione

$$v_{\{7\}} \colon \mathbb{Z}_{\{7\}} \longrightarrow \mathbb{N} \,, \qquad 7^z a \mapsto v_{\{7\}}\big(7^e a\big) := \big|a\big|$$

(b) Calcolare il gruppo $U\big(\mathbb{Z}_{\{7\}}\big)$ degli elementi invertibili di $\mathbb{Z}_{\{7\}}$.

<u>Soluzione</u>: *(a)* È immediato verificare che $\mathbb{Z}_{\{7\}}$ è un sottoanello unitario di $\mathbb{Q}$, e quindi è anche un dominio commutativo, perché tale è $\mathbb{Q}$ stesso.

Se $7^{e_1} a_1 \,, 7^{e_2} a_2 \in \mathbb{Z}_{\{7\}}$, con $e_1, e_2 \in \mathbb{Z}$ e $a_1, a_2 \in \mathbb{Z} \setminus \big(7\,\mathbb{Z}\big)$, allora si ha

$$7^{e_1} a_1 \cdot 7^{e_2} a_2 = 7^{e_1 + e_2}\, a_1 a_2 \,, \qquad \text{con} \quad e_1 + e_2 \in \mathbb{Z} \,, \quad a_1 a_2 \in \mathbb{Z} \setminus \big(7\,\mathbb{Z}\big)$$

(perché 7 è un primo in $\mathbb{Z}$!), e quindi

$$v_{\{7\}}\big(7^{e_1} a_1 \cdot 7^{e_2} a_2\big) := \big|a_1 a_2\big| = \big|a_1\big| \cdot \big|a_2\big| = v_{\{7\}}\big(7^{e_1} a_1\big) \cdot v_{\{7\}}\big(7^{e_2} a_2\big)$$

per cui l'applicazione $v_{\{7\}} \colon \mathbb{Z}_{\{7\}} \setminus \{0\} \longrightarrow \mathbb{N}_+$ è moltiplicativa — cioè (in questo caso) è un morfismo tra gli insiemi con operazioni $\big(\mathbb{Z}_{\{7\}} \setminus \{0\} \,;\, \cdot\big)$ e $\big(\mathbb{N}_+ \,;\, \cdot\big)$.

Inoltre, per $7^{e_1} a_1 \,, 7^{e_2} a_2 \in \mathbb{Z}_{\{7\}}$ come sopra operiamo la divisione euclidea in $\mathbb{Z}$:

$$a_1 = a_2\, q' + r' \,, \qquad q' \,, r' \in \mathbb{Z} \,, \quad \big|r'\big| < \big|a_2\big|$$

Allora gli elementi $q := 7^{e_1 - e_2}\, q'$ e $r := 7^{e_1}\, r'$ in $\mathbb{Z}_{\{7\}}$ danno

$$7^{e_1} a_1 = 7^{e_1} \big(a_2\, q' + r'\big) = 7^{e_2} a_2\, 7^{e_1 - e_2}\, q' + 7^{e_1}\, r' = 7^{e_2} a_2 \cdot q + r$$

così che, scrivendo r' come $r' = 7^m r''$ con $m \in \mathbb{N}$ e $r'' \in \mathbb{Z} \setminus \big(7\,\mathbb{Z}\big)$, abbiamo

$$v_{\{7\}}(r) \,=\, v_{\{7\}}\big(7^{e_1} r'\big) \,=\, v_{\{7\}}\big(7^{e_1+m} r''\big) \,:=\, \big|\, r'\big| \,\leq\, |\, r| \,<\, |\, a_2| \,=:\, v_{\{7\}}\big(7^{e_2} a_2\big)$$

e quindi in definitiva

$$7^{e_1} a_1 \;=\; 7^{e_2} a_2 \cdot q \,+\, r\;, \qquad q\,,\, r \in \mathbb{Z}_{\{7\}}\;,\;\; v_{\{7\}}(r) \,<\, v_{\{7\}}\big(7^{e_2} a_2\big)$$

In conclusione, quest'ultima proprietà e la moltiplicatività di $v_{\{7\}}$ significano proprio che $\mathbb{Z}_{\{7\}}$ è un dominio euclideo, rispetto alla valutazione $v_{\{7\}}$.

(b) Dato che $\mathbb{Z}_{\{7\}}$ è un dominio euclideo, dalla teoria generale sappiamo che

$$U\big(\mathbb{Z}_{\{7\}}\big) \;=\; \big\{\, \alpha \in \mathbb{Z}_{\{7\}} \,\big|\, v_{\{7\}}(\alpha) = v_{\{7\}}(1) \,\big\}$$

Nel caso in esame è $v_{\{7\}}(1) = 1$, quindi le definizioni e il calcolo diretto danno

$$\begin{aligned} U\big(\mathbb{Z}_{\{7\}}\big) \;&=\; \big\{\, \alpha \in \mathbb{Z}_{\{7\}} \,\big|\, v_{\{7\}}(\alpha) = v_{\{7\}}(1) = 1 \,\big\} \;= \\ &=\; \big\{\, 7^e a \in \mathbb{Z}_{\{7\}} \,\big|\, e \in \mathbb{Z}\,,\, a \in \mathbb{Z} \setminus \big(7\,\mathbb{Z}\big)\,,\, v_{\{7\}}\big(7^e a\big) := |\, a| = 1 \,\big\} \;=\; \big\{\, \pm\, 7^e \,\big|\, e \in \mathbb{Z} \,\big\} \end{aligned}$$

cioè $U\big(\mathbb{Z}_{\{7\}}\big) = \big\{\, \pm\, 7^e \,\big|\, e \in \mathbb{Z} \,\big\}$. $\square$

8 — Dato un dominio a fattorizzazione unica R, sia $Q(R)$ il suo campo dei quozienti, e sia $p \in R$ un elemento irriducibile — o, in altre parole, primo — di R. Si consideri il sottoinsieme $R_{(p)}$ di $Q(R)$ così definito:

$$R_{(p)} \;:=\; \Big\{\, q \in Q(R) \,\Big|\, q = n/d\,,\; n, d \in R\,,\; d \neq 0\,,\; M.C.D.(n, d\,) = 1\,,\; d \notin p\,R \,\Big\}$$

In altre parole, $R_{(p)}$ è l'insieme delle "frazioni" in $Q(R)$ il cui denominatore *non* sia multiplo di (o divisibile per) l'elemento p.

(a) Dimostrare che $R_{(p)}$ è un sottoanello di $Q(R)$.

(b) Dimostrare che $R_{(p)}$ è un dominio euclideo rispetto alla valutazione

$$v_p \colon R_p \setminus \{0\} \longrightarrow \mathbb{N}\,, \qquad n/d \,\mapsto\, v_p\big(n/d\big) := k \;\Longleftrightarrow\; n \in \big(p^k R \setminus p^{k+1} R\big)$$

(c) Calcolare il gruppo $U\big(R_p\big)$ degli elementi invertibili di R_p.

<u>Soluzione:</u> *(a)* Per costruzione R_p contiene R, quindi $R_p \neq \emptyset$. Inoltre, dati due elementi $n/d\,,\, n'/d' \in R_p$ si ha

$$n/d \,-\, n'/d' \;=\; \big(nd' - n'd\big)\Big/ d\,d'\;, \qquad n/d \cdot n'/d' \;=\; n\,n'\Big/ d\,d' \tag{4}$$

per ipotesi si ha $d, d' \notin p\,R$, quindi anche $d\,d' \notin p\,R$, perché p è primo in R. Se poi nella (4) riduciamo le frazioni ad avere numeratore e denominatore coprimi, il nuovo denominatore sarà comunque un divisore di $d\,d'$, e quindi ancora non apparterrà a $p\,R$, per cui — dalla (4) — possiamo concludere che $n/d - n'/d' \in R_p$ e parimenti $n/d \cdot n'/d' \in R_p$. Questo dimostra che R_p ùn sottoanello di $Q(R)$, q.e.d.

(b) Essendo un sottoanello di $Q(R)$, che è un dominio, anche R_p stesso è a sua volta un dominio. Ora, se $q = n/d$ e $q' = n'/d'$ sono due elementi di $R_p \setminus \{0\}$ — scritti come frazioni in forma ridotta, con $d, d' \in \big(R \setminus p\,R\big)$ — sia $n \in \big(p^k R \setminus p^{k+1} R\big)$ e $n' \in \big(p^{k'} R \setminus p^{k'+1} R\big)$, così che $v_p\big(n/d\big) := k$ e $v_p\big(n'/d'\big) := k'$. Allora si ha

$$q \cdot q' \;=\; n/d \cdot n'/d' \;=\; n\,n' \Big/ d\,d' \;, \qquad d\,d' \in \big(R \setminus p\,R\big) \;,\;\; n\,n' \in \big(p^{k+k'} R \setminus p^{k+k'+1} R\big) \tag{5}$$

(dove la prima proprietà è già stata verificata, mentre la prima segue dalle ipotesi e dal fatto che R è un dominio a fattorizzazione unica!). In altre parole, la (5) significa che

$$v_p\Big(n/d \cdot n'/d'\Big) \;:=\; v_p\Big(n\,n' \Big/ d\,d'\Big) \;=\; k \,+\, k' \;=\; v_p\big(n/d\big) \,+\, v_p\big(n'/d'\big)$$

perciò l'applicazione $v_p : R_p \setminus \{0\} \longrightarrow \mathbb{N}_+$ è moltiplicativa — cioè (in questo caso) è un morfismo tra gli insiemi con operazioni $\big(R_p \setminus \{0\}\,;\,\cdot\big)$ e $\big(\mathbb{N}_+\,;\,+\big)$.

Inoltre, per n/d e n'/d' in R_p come sopra, possiamo scrivere

$$n/d \;=\; p^{v_p(n/d)} \cdot \nu/d \quad , \qquad n'/d' \;=\; p^{v_p(n'/d')} \cdot \nu'/d'$$

dove adesso $\nu, \nu' \in \big(R \setminus p\,R\big)$ e quindi $d/\nu, d'/\nu' \in R_p$.

A questo punto, per poter "fare la divisione con resto" di n/d per n'/d', confrontiamo le rispettive valutazioni:

$\underline{v_p\big(n/d\big) \geq v_p\big(n'/d'\big)} \quad \Longrightarrow$

$$\Longrightarrow \quad n/d \,=\, p^{v_p(n/d)} \cdot \nu/d \,=\, p^{v_p(n/d) - v_p(n'/d')} \cdot \nu/d \cdot d'/\nu' \cdot p^{v_p(n'/d')} \cdot \nu'/d' \,=$$

$$= \, p^{v_p(n/d) - v_p(n'/d')} \cdot \nu\,d' \Big/ d\,\nu' \cdot n'/d' \quad \Longrightarrow$$

$$\Longrightarrow \quad n/d \;=\; q \cdot n'/d' \,+\, r \;, \quad q := p^{v_p(n/d) - v_p(n'/d')} \cdot \nu\,d' \Big/ d\,\nu' \in R_p \;,\; r := 0 \in R_p$$

$\underline{v_p\big(n/d\big) < v_p\big(n'/d'\big)} \quad \Longrightarrow \quad n/d \;=\; q \cdot n'/d' \,+\, r \;, \quad q := 0 \in R_p \;,\; r := n/d \in R_p \;,$
$v_p(r) = v_p\big(n/d\big) < v_p\big(n'/d'\big)$

In conclusione, in ogni caso "si può effettuare la divisione euclidea" come richiesto dagli assiomi, per cui — anche tenendo conto della moltiplicatività di v_p — abbiamo che R_p è effettivamente un dominio euclideo, rispetto alla valutazione v_p, q.e.d.

(b) Dato che R_p è un dominio euclideo, la teoria generale assicura che

$$U\big(R_p\big) \;=\; \big\{\, \alpha \in R_p \,\big|\, v_p(\alpha) = v_p(1) \,\big\}$$

Nel caso attuale si ha $v_p(1) = 0$, quindi le definizioni e il calcolo diretto danno

$$\begin{aligned} U\big(R_p\big) \;&=\; \big\{\, q = n/d \in R_p \;\big|\; v_p(q) = v_p(1) = 0 \,\big\} \;= \\ &=\; \Big\{\, n/d \in R_p \;\Big|\; n \in \big(p^k R \setminus p^{k+1} R\big)\,,\, v_p\big(n/d\big) := k = 0 \,\Big\} \;= \\ &=\; \big\{\, n/d \in Q(R) \;\big|\; n, d \in (R \setminus p\,R)\,\big\} \end{aligned}$$

dunque in definitiva $U\big(R_p\big) = \big\{\, n/d \in Q(R) \;\big|\; n, d \in (R \setminus p\,R)\,\big\}$. $\square$

9 — Nell'anello $\mathbb{Z}[i]$ degli interi di Gauss, si considerino i due ideali principali $I := (15 - 5\,i)$ e $J := (6 - 12\,i)$ generati rispettivamente dagli elementi $15 - 5\,i$ e $6 - 12\,i$.

(a) Calcolare un generatore dell'ideale $K := I \bigcap J$.

(b) Determinare tutti gli ideali dell'anello quoziente $\mathbb{Z}[i]/K$, precisando quali di essi siano primi e quali siano massimali.

(c) Per ciascuno dei due elementi $\overline{6 - 3\,i}$ e $\overline{1 + 5\,i}$ nell'anello unitario $\mathbb{Z}[i]/K$, si determini se ne esista o meno l'inverso. In caso negativo, si spieghi perché tale inverso non esiste; in caso affermativo, si calcoli tale inverso.

<u>Soluzione</u>: *(a)* L'anello $\mathbb{Z}[i]$ è un dominio euclideo, rispetto alla valutazione data dalla restrizione della norma ni $\mathbb{C}$. Pertanto, dalla teoria generale segue che esso è un dominio a ideali principali, e in esso l'intersezione di due ideali — principali! — $\big(a\big)$ e $\big(b\big)$ è a sua volta un ideale principale, generato dal $m.c.m.(a, b)$: in formule,

$$\big(a\big) \bigcap \big(b\big) \;=\; \big(m.c.m.(a, b)\big) \tag{6}$$

Inoltre, poiché un dominio a ideali principali — nel nostro caso $\mathbb{Z}[i]$ — è anche un dominio a fattorizzazione unica, il $m.c.m.(a, b)$ si può ottenere tramite la formula

$$m.c.m.(a, b) \;=\; a\,b \Big/ M.C.D.(a, b) \tag{7}$$

una volta che sia noto $M.C.D.(a, b)$. Infine quest'ultimo può essere calcolato esplicitamente — dato che $\mathbb{Z}[i]$ è un dominio euclideo — tramite l'algoritmo delle divisioni successive; in alternativa — dato che $\mathbb{Z}[i]$ è un dominio euclideo — lo si può ricavare a partire da una fattorizzazione di a e una di b in prodotto di irriducibili.

Eseguendo l'algoritmo delle divisioni successive, il calcolo diretto dà

$$\begin{aligned} 15 - 5\,i \;&=\; (6 - 12\,i\,) \cdot i \,+\, (3 - 11\,i\,) \\ 6 - 12\,i \;&=\; (3 - 11\,i\,) \cdot 1 \,+\, \underline{(3 - i\,)} \quad\mapsto\quad \textit{ultimo resto non nullo!} \\ 3 - 11\,i \;&=\; (3 - i\,) \cdot (2 - 3\,i\,) \,+\, \underline{0} \quad\mapsto\quad \textit{resto nullo!} \end{aligned}$$

e poiché sappiamo che, in generale, *l'ultimo resto non nullo è il M.C.D. cercato*, in questo caso si trova che

$$M.C.D.\big(15-5\,i\,,\,6-12\,i\big) \;=\; 3-i \tag{8}$$

N.B.: se si fattorizzano $(15-5\,i)$ e $(6-12\,i)$ in irriducibili, si trova

$$\begin{aligned} 15-5\,i \;&=\; (1+2\,i)\cdot(1-2\,i)^2\cdot(1+i) \\ 6-12\,i \;&=\; (1+i)\cdot(1-i)\cdot 3\cdot(1-2\,i) \end{aligned}$$

da egualmente si conclude che $M.C.D.\big(15-5\,i\,,\,6-12\,i\big) = (1+i)\cdot(1-2\,i) \;=\; 3-i$.

Tirando le somme, la (6), la (7) e la (8) insieme danno

$$\begin{aligned} K \;:=\; I\bigcap J \;:=\; \big(15-5\,i\big)\bigcap\big(6-12\,i\big) \;&=\; \big(m.c.m.(15-5\,i\,,\,6-12\,i\,)\big) \;= \\ &=\; \Big((15-5\,i\,)\,(6-12\,i\,)\Big/M.C.D.(15-5\,i\,,\,6-12\,i\,)\Big) \;= \\ &=\; \Big((15-5\,i\,)\,(6-12\,i\,)\Big/3-i\Big) \;=\; \big(30-60\,i\,\big) \end{aligned}$$

cioè in definitiva $K := I\bigcap J \;=\; \big(30-60\,i\,\big)$, per cui $(30-60\,i\,)$ è un possibile generatore come richiesto. Ogni altro generatore di K è associato a questo, cioè è multiplo di questo per un fattore in $U\big(\mathbb{Z}[i]\big) = \{1,-1,i,-1\,\}$: pertanto, in conclusione i possibili generatori di K sono tutti e soli i seguenti:

$$g \;:=\; 30-60\,i\,,\quad (-1)\cdot g \;=\; -30+60\,i\,,\quad i\cdot g \;=\; 60+30\,i\,,\quad (-i\,)\cdot g \;=\; -60-30\,i$$

(b) Poiché $\mathbb{Z}[i]$ è un anello a ideali principali, lo stesso è vero anche per il suo quoziente $\mathbb{Z}[i]\Big/K \;=\; \mathbb{Z}\Big/\big(30-60\,i\,\big)$. Dalla teoria generale sappiamo che:

(1) gli ideali di un anello quoziente $A\Big/K$ (come quello in esame) sono tutte e sole le immagini $\pi(E) = E\Big/I$, dove indichiamo con $\pi\colon A \longrightarrow\!\!\!\!\!\rightarrow\; A\Big/K$ la proiezione canonica, degli ideali E di A che contengano l'ideale K ;

(2) in un anello commutativo unitario (come sono quelli in esame) R , un ideale K è primo, risp. massimale, se e soltanto se $R\Big/K$ è un dominio, risp. un campo;

(3) in un anello commutativo unitario R a ideali principali, dati due ideali $E = (n)$ e $F = (d)$ si ha $E\subseteq F$ se e soltanto se $d\,\Big|\,n$, cioè d divide n (cioè n è multiplo di d).

Applichiamo queste idee al caso $A := \mathbb{Z}[i]$, $K := \big(30-60\,i\,\big)$. Per quanto appena osservato, dobbiamo trovare tutti gli ideali di $\mathbb{Z}[i]$ del tipo $E = \big(\eta\big)$ in cui il generatore η sia un divisore di $(30-60\,i\,)$. A tal fine, consideriamo una fattorizzazione di $(30-60\,i\,)$ in irriducibili: a tal scopo, osserviamo che

$$\begin{aligned} &30-60\,i \;=\; 30\cdot(1-2\,i\,) \;=\; 2\cdot 3\cdot 5\cdot(1-2\,i\,) \;=\; (1+i\,)\cdot(1-i\,)\cdot 3\cdot 5\cdot(1-2\,i\,) \;= \\ &=\; (1+i\,)\cdot(1-i\,)\cdot 3\cdot(1+2\,i\,)\cdot(1-2\,i\,)\cdot(1-2\,i\,) \;=\; (1+i\,)\cdot(1-i\,)\cdot 3\cdot(1+2\,i\,)\cdot(1-2\,i\,)^2 \end{aligned}$$

e i fattori $(1+i)$, $(1-i)$, 3, $(1+2\,i)$, $(1-2\,i)$ sono tutti irriducibili. Infatti, le loro norme sono rispettivamente 2, 9, 5, 5: ora, se n è uno di tali numeri, può essere fattorizzato in prodotto di due fattori scelti in $\big\{\,\|\zeta\|\,\big|\,\zeta\in\mathbb{Z}[i]\,\big\}\;=\;\big\{\,a^2+b^2\,\big|\,a,b\in\mathbb{Z}\,\big\}$ soltanto se uno dei due fattori è 1, per cui il fattore corrispondente in una (eventuale) fattorizzazione di n appartiene necessariamente a $\{1,-1,i,-i\}=U\big(\mathbb{Z}[i]\big)$; dunque tale fattore è invertibile in $\mathbb{Z}[i]$, e la fattorizzazione di n considerata è banale. Pertanto

$$30-60\,i\;=\;(1+i)\cdot(1-i)\cdot 3\cdot(1+2\,i)\cdot(1-2\,i)^2$$

è (una) fattorizzazione di $(30-60\,i)$ in irriducibili, nella quale i fattori irriducibili esplicitamente scritti sono a due a due non associati. Ne segue che l'insieme dei divisori di $(30-60\,i)$ è

$$Div\big(30-60\,i\big)=\left\{\epsilon\cdot(1+i)^{e_1}\,(1-i)^{e_2}\,3^{e_3}\,(1+2\,i)^{e_4}\,(1-2\,i)^{e_5}\;\middle|\;\begin{array}{c}0\le e_i\le 1\,,\;\forall\,i=1,\dots,4\\ 0\le e_5\le 2\,;\;\;\epsilon\in U\big(\mathbb{Z}[i]\big)\end{array}\right\}$$

Quindi, in conclusione — tenuto conto che d e $\epsilon\cdot d$ generano lo stesso ideale se $\epsilon\in U\big(\mathbb{Z}[i]\big)$ — l'insieme degli ideali di $\mathbb{Z}[i]\Big/K\;=\;\mathbb{Z}\Big/\big(30-60\,i\big)$ è

$$\left\{\Big(\overline{(1+i)}^{\,e_1}\,\overline{(1-i)}^{\,e_2}\,\overline{3}^{\,e_3}\,\overline{(1+2\,i)}^{\,e_4}\,\overline{(1-2\,i)}^{\,e_5}\Big)\;\middle|\;0\le e_i\le 1\,,\;\forall\,i=1,2,3,4\,;\;0\le e_5\le 2\right\}$$

dove $\overline{\zeta}\in\mathbb{Z}[i]\Big/K$ sta ad indicare la classe di un elemento $\zeta\in\mathbb{Z}[i]$.

Per determinare quali tra questi ideali siano primi e quali massimali, osserviamo che ognuno di essi è del tipo $\big(\overline{\zeta}\big)=\big(\zeta\big)\Big/K$, e si ha

$$\Big(\mathbb{Z}[i]\Big/K\Big)\Big/\big(\overline{\zeta}\big)\;\;=\;\;\Big(\mathbb{Z}[i]\Big/K\Big)\Big/\Big(\big(\zeta\big)\Big/K\Big)\;\;\cong\;\;\mathbb{Z}[i]\Big/\big(\zeta\big)\tag{9}$$

per il Teorema del Doppio Quoziente. Ora, dalla teoria generale sappiamo che

$$\big(\overline{\zeta}\big)\text{ primo, risp. massimale, in }\mathbb{Z}[i]\Big/K\;\iff\;\Big(\mathbb{Z}[i]\Big/K\Big)\Big/\big(\overline{\zeta}\big)\text{ dominio, risp. campo}\tag{10}$$

$$\big(\zeta\big)\text{ primo, risp. massimale, in }\mathbb{Z}[i]\;\iff\;\mathbb{Z}[i]\Big/\big(\zeta\big)\text{ dominio, risp. campo}\tag{11}$$

e inoltre, dato che $\mathbb{Z}[i]$ è un dominio euclideo,

$$\mathbb{Z}[i]\Big/\big(\zeta\big)\text{ è un dominio }\iff\zeta\text{ è irriducibile in }\mathbb{Z}[i]\iff\mathbb{Z}[i]\Big/\big(\zeta\big)\text{ è un campo}\tag{12}$$

Pertanto, dalle (10), (11) e (12) concludiamo che gli ideali primi di $\mathbb{Z}[i]\Big/K$ coincidono con quelli massimali, e sono esattamente tutti e soli i seguenti:

$$\big(\,\overline{1+i}\,\big)\quad,\qquad\big(\,\overline{1-i}\,\big)\quad,\qquad\big(\,\overline{3}\,\big)\quad,\qquad\big(\,\overline{1+2\,i}\,\big)\quad,\qquad\big(\,\overline{1-2\,i}\,\big)\quad.$$

(c) Stiamo cercando — se esistono — un $(a+b\,i\,)\in\mathbb{Z}[i]$ e un $(\alpha+\beta\,i\,)\in\mathbb{Z}[i]$ tali che

$$\overline{(a+b\,i\,)}\cdot\overline{(6-3\,i)}\;=\;\overline{1}\quad,\qquad\overline{(\alpha+\beta\,i\,)}\cdot\overline{(1+5\,i)}\;=\;\overline{1}\tag{13}$$

nell'anello $\mathbb{Z}[i]\Big/K\;=\;\mathbb{Z}[i]\Big/\big(30-60\,i\,\big)$. Ma la (13) equivale alle condizioni

$$\begin{aligned}\exists\,\big(a'+b'\,i\,\big)\in\mathbb{Z}[i]\quad&:\quad(a+b\,i\,)\cdot(6-3\,i)\;=\;1\;+\;\big(a'+b'\,i\,\big)\cdot(30-60\,i\,)\\ \exists\,\big(\alpha'+\beta'\,i\,\big)\in\mathbb{Z}[i]\quad&:\quad(\alpha+\beta\,i\,)\cdot(1+5\,i)\;=\;\overline{1}\;+\;\big(\alpha'+\beta'\,i\,\big)\cdot(30-60\,i\,)\end{aligned}$$

che, tramite il cambiamento di variabili da x' a $x'':=-x'$, possono essere riformulate così:

$$\exists\,\big(a''+b''\,i\,\big)\in\mathbb{Z}[i]\quad:\quad(a+b\,i\,)\cdot(6-3\,i)\;+\;\big(a''+b''\,i\,\big)\cdot(30-60\,i\,)\;=\;1\tag{14}$$

$$\exists\,\big(\alpha''+\beta''\,i\,\big)\in\mathbb{Z}[i]\quad:\quad(\alpha+\beta\,i\,)\cdot(1+5\,i)\;+\;\big(\alpha''+\beta''\,i\,\big)\cdot(30-60\,i\,)\;=\;1\tag{15}$$

Ora, la (14) e la (15) sono due *equazioni diofantee* nel dominio euclideo $\mathbb{Z}[i]$, e conosciamo un criterio per sapere se ammettano soluzioni e, in caso affermativo, per calcolarle!

Precisamente, il criterio per l'esistenza è che il M.C.D. tra i coefficienti dell'equazione deve dividere il termine noto. Nei casi in esame, abbiamo le fattorizzazioni in irriducibili

$$\begin{aligned}30-60\,i\;&=\;(1+i\,)\,(1-i\,)\,3\,(1+2\,i\,)\,(1-2\,i\,)^2\\ 6-3\,i\;=\;(-i\,)\cdot 3\,(1+2\,i\,)\quad&,\qquad 1+5\,i\;=\;(1+i\,)\,(3+2\,i\,)\end{aligned}\tag{16}$$

dove gli unici nuovi fattori che compaiono sono $(-i\,)$, che è invertibile, e $(3+2\,i\,)$, che è irriducibile — in breve, perché ha norma 13, che è irriducibile in $\mathbb{Z}$.

N.B.: naturalmente, è possibile calcolare i suddetti M.C.D. anche applicando l'algoritmo euclideo delle divisioni successive.

Ora, dalle fattorizzazioni in (16) otteniamo subito che

$$\begin{aligned}M.C.D.\big(6-3\,i\,,30-60\,i\,\big)\;&=\;1+2\,i\;\not|\;1\qquad\text{per la (14)}\\ M.C.D.\big(1+5\,i\,,30-60\,i\,\big)\;&=\;1+i\;\not|\;1\qquad\text{per la (15)}\end{aligned}$$

così che sia la (14) che la (15) *non* hanno soluzioni. Quindi, in conclusione, *non* esiste nell'anello unitario $\mathbb{Z}[i]\Big/K\;=\;\mathbb{Z}[i]\Big/\big(30-60\,i\,\big)$, un inverso dell'elemento $\overline{6-3\,i}$, né un inverso dell'elemento $\overline{1+5\,i}$. $\square$

10 — Nell'anello $\mathbb{Z}[i]$ degli interi di Gauss, si considerino i due elementi 30492 e 43560. Per ciascuno di essi, si determini se sia esprimibile come somma di due quadrati (in $\mathbb{Z}$); in caso affermativo, si scriva una tale espressione dell'elemento come somma di due quadrati.

Soluzione — per 30492: Operiamo la fattorizzazione in irriducibili di 30492 nell'anello $\mathbb{Z}$, che è un dominio a fattorizzazione unica: si ha

$$30492 \;=\; 2^2 \cdot 3^2 \cdot 7 \cdot 11^2 \tag{17}$$

Tra i fattori individuati, osserviamo che 7 è *un elemento irriducibile* nell'anello $\mathbb{Z}[i]$. Infatti, tale anello è un dominio euclideo, con valutazione definita da $v(\alpha+i\,\beta) := \alpha^2+\beta^2$, che è moltiplicativa. Allora, se si considera una qualunque fattorizzazione di 7 in $\mathbb{Z}[i]$, sia $7 = (\alpha + i\,\beta)\,(\gamma + i\,\delta)$, si ottiene anche

$$49 \;=\; v(7) \;=\; v(\alpha + i\,\beta)\,v(\gamma + i\,\delta) \;=\; \left(\alpha^2 + \beta^2\right)\left(\gamma^2 + \delta^2\right)$$

per cui, dalla fattorizzazione $49 = \left(\alpha^2 + \beta^2\right)\left(\gamma^2 + \delta^2\right)$ in $\mathbb{N}_+$, ricaviamo che

$$\left\{\, \alpha^2 + \beta^2\,,\, \gamma^2 + \delta^2 \,\right\} \;=\; \left\{1, 49\right\} \qquad \text{oppure} \qquad \left\{\, \alpha^2 + \beta^2\,,\, \gamma^2 + \delta^2 \,\right\} \;=\; \left\{7\right\} \quad .$$

Ma *il secondo caso è impossibile* — ché 7 *non* è somma di due quadrati, in $\mathbb{Z}$ — quindi si verifica necessariamente il primo: questo significa che $v(\alpha+i\,\beta) = 1$ oppure $v(\gamma+i\,\delta) = 1$, per cui rispettivamente sarà $\alpha + i\,\beta \in \left\{\pm 1\,,\pm i\,\right\}$ oppure $\gamma + i\,\delta \in \left\{\pm 1\,,\pm i\,\right\}$, e dunque in ogni caso la fattorizzazione $7 = (\alpha + i\,\beta)\,(\gamma + i\,\delta)$ è banale.

Pertanto, 7 è irriducibile in $\mathbb{Z}[i]$; poiché questo anello è un domino euclideo, è anche un dominio a fattorizzazione unica, e quindi ogni irriducibile è primo! In particolare, 7 è un elemento primo in $\mathbb{Z}[i]$.

Supponiamo ora che sia possibile esprimere 30492 come somma di due quadrati, diciamo

$$30492 \;=\; a^2 + b^2 \qquad (\,a, b \in \mathbb{Z}\,)$$

Allora abbiamo anche

$$30492 \;=\; a^2 + b^2 \;=\; (a + i\,b)\,(a - i\,b) \qquad \text{con} \quad (a + i\,b)\,,\,(a - i\,b) \in \mathbb{Z}[i]$$

Questa relazione insieme alla (17) ci dice che 7 divide il prodotto $(a+i\,b)\,(a-i\,b)$ in $\mathbb{Z}[i]$. Ma abbiamo visto che 7 è primo in $\mathbb{Z}[i]$, quindi necessariamente 7 divide $(a + i\,b)$ oppure $(a - i\,b)$, cioè esiste un elemento $\zeta_+ \in \mathbb{Z}[i]$ tale che $7 \cdot \zeta_+ = (a + i\,b)$ oppure esiste un elemento $\zeta_- \in \mathbb{Z}[i]$ $7 \cdot \zeta_- = (a - i\,b)$. In effetti, se indichiamo con $\omega \mapsto \overline{\omega}$ l'operazione di coniugazione sui numeri complessi, abbiamo che $\overline{(a \pm i\,b)} = (a \mp i\,b)$, e quindi

$$(a \mp i\,b) \;=\; \overline{(a \pm i\,b)} \;=\; \overline{7 \cdot \zeta_\pm} \;=\; \overline{7} \cdot \overline{\zeta_\pm} \;=\; 7 \cdot \overline{\zeta_\pm}$$

perciò se esiste un $\zeta_{\pm}$ come sopra esiste anche l'analogo $\zeta_{\mp}$, dato da $\zeta_{\mp} = \overline{\zeta_{\pm}}$; poiché uno dei due esiste certamente, si conclude che esistono entrambi ζ_+ e ζ_-, e sono l'uno il coniugato dell'altro! Ma allora abbiamo che

$$30492 \,=\, (a + i\,b)\,(a - i\,b) \,=\, 7 \cdot \zeta_+ 7 \cdot \zeta_- \,=\, 7^2 \cdot \zeta_+ \cdot \zeta_- \tag{18}$$

dunque 7^2 divide 30492 in $\mathbb{Z}[i]$. Poiché $\zeta_{\mp} = \overline{\zeta_{\pm}}$, nella (18) si ha $\zeta_+ \cdot \zeta_- \in \mathbb{Z}$, e quindi la (18) stessa dice che 30492 è *divisibile per* 7^2 *in* $\mathbb{Z}$: dato che $\mathbb{Z}$ è un dominio a fattorizzazione unica, questa conclusione contraddice la (16)!!!

Pertanto, possiamo concludere che *non è possibile esprimere* 30492 *come somma di due quadrati in* $\mathbb{Z}$.

— *per 43560:* Operiamo la fattorizzazione in irriducibili di 43560 nell'anello $\mathbb{Z}$, che è un dominio a fattorizzazione unica: si ha

$$43560 \,=\, 2^3 \cdot 3^2 \cdot 5 \cdot 11^2$$

Tra i fattori individuati, osserviamo che

$$2 \,=\, 1+1 \,=\, 1^2+1^2 \,=\, (1+i)\,(1-i)\,, \qquad 5 \,=\, 4+1 \,=\, 2^2+1^2 \,=\, (2+i)\,(2-i)$$

per cui possiamo riscrivere 43560 così:

$$\begin{aligned} 43560 \,&=\, 2^3 \cdot 3^2 \cdot 5 \cdot 11^2 \,=\, (1+i)\,(1-i)^3\,3^2\,(2+i)\,(2-i)\,11^2 \,= \\ &=\, (1+i)^3\,(1-i)^3\,3^2\,(2+i)\,(2-i)\,11^2 \,=\, (1+i)^3\,3\,(2+i)\,11 \cdot (1-i)^3\,3\,(2-i)\,11 \,= \\ &=\, (-198+66\,i\,) \cdot (-198-66\,i\,) \,=\, 198^2+66^2 \,=\, 39204+4356 \end{aligned}$$

Dunque è *possibile esprimere* 43560 *come somma di due quadrati in* $\mathbb{Z}$, e precisamente come $43560 = 39204 + 4356 = 198^2 + 66^2$. □

11 — Si consideri il sottoinsieme $\mathbb{Z}\big[\sqrt{-11}\,\big]$ dell'insieme $\mathbb{C}$ dei numeri complessi così definito:

$$\mathbb{Z}\big[\sqrt{-11}\,\big] \,:=\, \Big\{\, \zeta \in \mathbb{C} \;\Big|\; \exists\, a,b \in \mathbb{Z} \colon \zeta = a + b\,\sqrt{-11} = a + i\,b\,\sqrt{11} \,\Big\}$$

(a) Dimostrare che $\mathbb{Z}\big[\sqrt{-11}\,\big]$ è un sottoanello unitario di $\mathbb{C}$.

(b) Determinare se $\mathbb{Z}\big[\sqrt{-11}\,\big]$ *sia* — oppure *non sia* — un dominio euclideo, o un dominio a ideali principali, o un dominio a fattorizzazione unica.

<u>Soluzione</u>: *(a)* Per dimostrare che $\mathbb{Z}\big[\sqrt{-11}\,\big]$ sia un sottoanello unitario di $\mathbb{C}$ basta fare una verifica diretta (banale).

(b) Si consideri l'emento $12 \in \mathbb{Z}\big[\sqrt{-11}\,\big]$. Esso si fattorizza in $\mathbb{Z}\big[\sqrt{-11}\,\big]$ in due modi, precisamente

$$12 \,=\, 2 \cdot 2 \cdot 3 \quad , \qquad 12 \,=\, \big(1 + \sqrt{-11}\,\big) \cdot \big(1 - \sqrt{-11}\,\big) \tag{19}$$

e queste sono entrambe fattorizzazioni di 12 in fattori irriducibili!

Infatti, supponiamo che 2 si fattorizzi in $\mathbb{Z}\big[\sqrt{-11}\,\big]$ come $2 = f_1 \cdot f_2$. Allora, indicando con $\|z\|$ la norma di un numero complesso $z \in \mathbb{C}$, e osservando che $\|\zeta\| \in \mathbb{Z}$ per ogni $\zeta \in \mathbb{Z}\big[\sqrt{-11}\,\big]$, avremmo

$$4 \,=\, \|2\| \,=\, \|f_1 \cdot f_2\| \,=\, \|f_1\| \cdot \|f_2\|$$

che sarebbe una fattorizzazione di 4 in cui i fattori (di destra) appartengono all'insieme

$$N\Big(\mathbb{Z}\big[\sqrt{-11}\,\big]\Big) \bigcap \{\pm 1, \pm 2, \pm 4\} \,=\, \big\{\, a^2 + 11 \cdot b^2 \,\big|\, a, b \in \mathbb{Z} \,\big\} \bigcap \{\pm 1, \pm 2, \pm 4\} \,=\, \{1, 4\}$$

Pertanto è necessariamente $\|f_1\| = 1$ oppure $\|f_2\| = 1$, cioè rispettivamente $f_1 = \pm 1$ oppure $f_2 = \pm 1$, per cui la fattorizzazione $2 = f_1 \cdot f_2$ è banale (il fattore f_1 oppure f_2 è invertibile!), e quindi si conclude che 2 è irriducibile in $\mathbb{Z}\big[\sqrt{-11}\,\big]$, q.e.d.

Allo stesso modo si dimostra che è irriducibile 3, sfruttando il fatto che $\|3\| = 9$ e

$$N\Big(\mathbb{Z}\big[\sqrt{-11}\,\big]\Big) \bigcap \{\pm 1, \pm 3, \pm 9\} \,=\, \big\{\, a^2 + 11 \cdot b^2 \,\big|\, a, b \in \mathbb{Z} \,\big\} \bigcap \{\pm 1, \pm 3, \pm 9\} \,=\, \{1, 9\}$$

e anche che sono irriducibili $\big(1 + \sqrt{-11}\,\big)$ $\big(1 - \sqrt{-11}\,\big)$, perché $\Big|\big(1 \pm \sqrt{-11}\,\big)\Big| = 12$ e

$$N\Big(\mathbb{Z}\big[\sqrt{-11}\,\big]\Big) \bigcap \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\} \,=$$
$$=\, \big\{\, a^2 + 11 \cdot b^2 \,\big|\, a, b \in \mathbb{Z} \,\big\} \bigcap \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\} \,=\, \{1, 12\}$$

Dunque la (19) e l'analisi precedente ci assicurano che 12 è un elemento in $\mathbb{Z}\big[\sqrt{-11}\,\big] \setminus \{0\}$ che ammette due fattorizzazioni in irriducibili nelle quali il numero di fattori irriducibili è diverso: *tre* fattori nella fattorizzazione $12 = 2 \cdot 2 \cdot 3$, e *due* soli fattori invece nella fattorizzazione $12 = \big(1 + \sqrt{-11}\,\big) \cdot \big(1 - \sqrt{-11}\,\big)$. Pertanto, le due fattorizzazioni *non* sono equivalenti, e quindi il dominio $\mathbb{Z}\big[\sqrt{-11}\,\big]$ *non* è a fattorizzazione unica, q.e.d.

In alternativa, si potrebbe anche considerare l'elemento $15 \in \mathbb{Z}\big[\sqrt{-11}\,\big] \setminus \{0\}$, e osservare che esso ammette le due fattorizzazioni

$$15 \,=\, 3 \cdot 5 \quad , \qquad 15 \,=\, \big(2 + \sqrt{-11}\,\big) \cdot \big(2 - \sqrt{-11}\,\big) \tag{20}$$

le quali sono entrambe fattorizzazioni di 15 in fattori irriducibili!

Infatti, sappiamo già che 3 è irriducibile in $\mathbb{Z}\big[\sqrt{-11}\,\big]$, e possiamo dimostrare che anche 5, $\big(2+\sqrt{-11}\,\big)$ e $\big(2-\sqrt{-11}\,\big)$ sono irriducibili esattamente con lo stesso procedimento usato in precedenza.

Ora, i soli elementi invertibili di $\mathbb{Z}\big[\sqrt{-11}\,\big]$ sono +1 e -1, perciò i fattori 3 e 5 — nella prima fattorizzazione in (20) — *non* sono in associati né all'uno né all'altro dei fattori $\big(2+\sqrt{-11}\,\big)$ e $\big(2-\sqrt{-11}\,\big)$ — nella seconda fattorizzazione in (20). Perciò si conclude che le due fattorizzazioni di 15 in (20) *non* sono equivalenti, e quindi il dominio $\mathbb{Z}\big[\sqrt{-11}\,\big]$ *non* è a fattorizzazione unica, q.e.d. □

12 — Si consideri l'estensione di campi $\mathbb{Q}\subseteq\mathbb{Q}\big(\alpha\,\big)$, dove $\alpha := 7-5\,\sqrt[3]{2}$.

(a) Dimostrare che α è algebrico su $\mathbb{Q}$.

(b) Calcolare il grado e il polinomio minimo (su $\mathbb{Q}$) di α.

(c) Determinare esplicitamente una base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$.

(d) Determinare se $\mathbb{Q}(\alpha)$ contenga, oppure no, ciascuno dei seguenti numeri:

$$\beta := 3/2+\sqrt[4]{2}\ , \qquad \gamma := -1+\sqrt{2}\ .$$

<u>Soluzione</u>: *(a-b)* Per definizione, $\alpha := 7-5\,\sqrt[3]{2}\in\mathbb{Q}\Big(\sqrt[3]{2}\,\Big)$, quindi $\mathbb{Q}(\alpha)$ è un'estensione intermedia dell'estensione $\mathbb{Q}\subseteq\mathbb{Q}\Big(\sqrt[3]{2}\,\Big)$. Quest'ultima grado $\Big[\,\mathbb{Q}\Big(\sqrt[3]{2}\,\Big):\mathbb{Q}\,\Big]=3$, che è primo, quindi — in conseguenza diretta della moltiplicatività del grado — non esistono estensioni intermedie non banali di $\mathbb{Q}\subseteq\mathbb{Q}\Big(\sqrt[3]{2}\,\Big)$. Pertanto dev'essere necessariamente $\mathbb{Q}=\mathbb{Q}(\alpha)$ oppure $\mathbb{Q}(\alpha)=\mathbb{Q}\Big(\sqrt[3]{2}\,\Big)$: poiché il primo caso *non* si verifica (altrimenti sarebbe $\sqrt[3]{2}\in\mathbb{Q}\,$) si ha invece che $\mathbb{Q}(\alpha)=\mathbb{Q}\Big(\sqrt[3]{2}\,\Big)$. Quindi $\Big[\,\mathbb{Q}(\alpha):\mathbb{Q}\,\Big]=\Big[\,\mathbb{Q}\Big(\sqrt[3]{2}\,\Big):\mathbb{Q}\,\Big]=3$, per cui α è algebrico su $\mathbb{Q}$, di grado 3.

OPPURE, più brevemente, possiamo procedere così:

Per definizione, $\alpha := 7-5\,\sqrt[3]{2}\in\mathbb{Q}\Big(\sqrt[3]{2}\,\Big)$, e quest'ultimo campo è un'estensione di $\mathbb{Q}$, finita — di grado 3 — dunque anche algebrica: ne segue in particolare che α stesso è algebrico su $\mathbb{Q}$. Inoltre, dalla forma esplicita di α ricaviamo subito che

$$\mathbb{Q}(\alpha)\ =\ \mathbb{Q}\Big(7-5\,\sqrt[3]{2}\,\Big)\ =\ \mathbb{Q}\Big(-5\,\sqrt[3]{2}\,\Big)\ =\ \mathbb{Q}\Big(\sqrt[3]{2}\,\Big)$$

da cui in particolare otteniamo ancora che α è algebrico su $\mathbb{Q}$, e in aggiunta anche che ha grado $\Big[\,\mathbb{Q}(\alpha):\mathbb{Q}\,\Big]=\Big[\,\mathbb{Q}\Big(\sqrt[3]{2}\,\Big):\mathbb{Q}\,\Big]=3$.

Resta da calcolare il polinomio minimo di α su $\mathbb{Q}$; di esso sappiamo già che deve essere un polinomio in $\mathbb{Q}[x]$, monico e di grado 3, che è il grado di α su $\mathbb{Q}$ (allora sarà anche — automaticamente — irriducibile). Ora, dalla definizione di α segue che

$$\begin{aligned}&(\alpha-7\,)^3\ =\ \Big(-5\,\sqrt[3]{2}\,\Big)^3\ =\ -250\quad\Longrightarrow\quad p(\alpha)\ =\ 0\\ \text{con}\qquad &p(x)\ :=\ (x-7\,)^3+250\ =\ x^3-21\,x^2+147\,x-97\ \in\ \mathbb{Q}[x]\end{aligned}\tag{21}$$

Poiché $p(x)$ ha grado 3, la (21) significa proprio che $p(x)$ è il polinomio minimo di α su $\mathbb{Q}$.

(c) Dalla teoria generale sappiamo che, poiché il grado di α su $\mathbb{Q}$ è 3, una base di $\mathbb{Q}(\alpha)$ su $\mathbb{Q}$ è l'insieme $\left\{ 1 , \alpha , \alpha^2 \right\}$.

(d) Dato che $3/2 \in \mathbb{Q}$ e $-1 \in \mathbb{Q}$, si ha che

$$\beta := 3/2 + \sqrt[4]{2} \in \mathbb{Q}(\alpha) \iff \sqrt[4]{2} \in \mathbb{Q}(\alpha) \ , \qquad \gamma := -1 + \sqrt{2} \in \mathbb{Q}(\alpha) \iff \sqrt{2} \in \mathbb{Q}(\alpha)$$

Ora, $\sqrt[4]{2}$ è (algebrico) di grado 4 su $\mathbb{Q}$, quindi genera un'estensione di $\mathbb{Q}$ di grado 4, perciò *non può* appartenere all'estensione $\mathbb{Q}(\alpha)$, il cui grado su $\mathbb{Q}$ è 3, visto che $3 < 4$ (qui si sfrutta la *monotonia* — crescente — del grado, rispetto alle torri di estensioni).

Analogamente — ma con una lieve differenza! — $\sqrt{2}$ è (algebrico) di grado 2 su $\mathbb{Q}$, quindi genera un'estensione di $\mathbb{Q}$ di grado 2, perciò *non può* appartenere all'estensione $\mathbb{Q}(\alpha)$, il cui grado su $\mathbb{Q}$ è 3, visto che $2 \nmid 3$ (qui si sfrutta la *moltiplicatività* del grado, rispetto alle torri di estensioni). □

13 — Sia $\mathbb{K}$ un campo, e sia $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ una estensione algebrica semplice di grado n.

(a) Dimostrare che, se n è primo, allora $\mathbb{K}\big(\alpha^e\big) = \mathbb{K}(\alpha)$ per ogni $e \in \{0, 1, \ldots, n-1\}$.

(b) Dimostrare, fornendo un esempio esplicito, che se n non è primo, allora può esistere un $\overline{e} \in \{0, 1, \ldots, n-1\}$ tale che $\mathbb{K}\big(\alpha^{\overline{e}}\big) \subsetneqq \mathbb{K}(\alpha)$.

<u>Soluzione</u>: *(a)* Il campo $\mathbb{K}\big(\alpha^e\big)$ è un'estensione intermedia di $\mathbb{K} \subseteq \mathbb{K}(\alpha)$, cioè si ha $\mathbb{K} \subseteq \mathbb{K}\big(\alpha^e\big) \subseteq \mathbb{K}(\alpha)$. Ora, dalla teoria generale sappiamo che in una questa situazione il grado delle estensioni coinvolte è "moltiplicativo", cioè si ha

$$n := \big[\mathbb{K}(\alpha) : \mathbb{K}\big] = \big[\mathbb{K}(\alpha) : \mathbb{K}\big(\alpha^e\big)\big] \cdot \big[\mathbb{K}\big(\alpha^e\big) : \mathbb{K}\big] \tag{22}$$

Pertanto, $\big[\mathbb{K}\big(\alpha^e\big) : \mathbb{K}\big]$ è un divisore di $\big[\mathbb{K}(\alpha) : \mathbb{K}\big] =: n$. Poiché per ipotesi n è primo, si conclude che necessariamente

$$\big[\mathbb{K}\big(\alpha^e\big) : \mathbb{K}\big] = 1 \qquad \text{oppure} \qquad \big[\mathbb{K}\big(\alpha^e\big) : \mathbb{K}\big] = n$$

Se valesse il primo caso, si avrebbe che $\big[\mathbb{K}\big(\alpha^e\big) : \mathbb{K}\big] = 1$ implica $\mathbb{K}\big(\alpha^e\big) = \mathbb{K}$. Ma questo implicherebbe in particolare $a := \alpha^e \in \mathbb{K}$, e quindi α sarebbe radice del polinomio $x^e - a \in \mathbb{K}[x]$, che ha grado $\partial\big(x^e - a\big) = e$ *strettamente minore di* n. In conseguenza, α stesso avrebbe grado, su $\mathbb{K}$, minore o uguale ad e, e quindi strettamente minore di n, per cui in definitiva sarebbe $\big[\mathbb{K}(\alpha) : \mathbb{K}\big] \lneqq n$, contro l'ipotesi!

Pertanto, deve necessariamente valere il secondo caso, cioè dev'essere $\big[\mathbb{K}\big(\alpha^e\big) : \mathbb{K}\big] = n$. Ma allora la (22) dà $\big[\mathbb{K}(\alpha) : \mathbb{K}\big(\alpha^e\big)\big] = 1$, quindi $\mathbb{K}\big(\alpha^e\big) = \mathbb{K}(\alpha)$, q.e.d.

(b) Si consideri il caso $\mathbb{K} := \mathbb{Q}$ e $\alpha := \sqrt[4]{3}$. Si ha $\big[\mathbb{Q}\big(\sqrt[4]{3}\big) : \mathbb{Q}\big] = 4$, perché $\sqrt[4]{3}$ è radice del polinomio $x^4 - 3$ che è irriducibile in $\mathbb{Q}[x]$, per il criterio di Eisenstein. D'altra parte, $\alpha^2 = \big(\sqrt[4]{3}\big)^2$ è radice del polinomio $x^2 - 3$, che è irriducibile in $\mathbb{Q}[x]$, ancora per il criterio di Eisenstein, e quindi $\big[\mathbb{Q}\big(\alpha^2\big) : \mathbb{Q}\big] = 2$. Poiché invece abbiamo visto che $\big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] = 4$, si può concludere che per $\overline{e} := 2$ si ha $\mathbb{Q}\big(\alpha^{\overline{e}}\big) \subsetneqq \mathbb{Q}(\alpha)$, q.e.d. □

14 — *(a)* Costruire un campo $\mathbb{F}_8$ con 8 elementi.

(b) Determinare un generatore ω del gruppo moltiplicativo $\big(\mathbb{F}_8{}^* ; \cdot\big)$, dove $\mathbb{F}_8{}^* := \mathbb{F}_8 \setminus \{0\}$ e $\mathbb{F}_8$ è costruito come in *(a)*. In particolare, verificare esplicitamente che tale ω sia un generatore.

Soluzione: *(a)* Dalla teoria generale sappiamo che, per ogni primo p e per ogni $n \in \mathbb{N}_+$, esiste certamente un campo $\mathbb{F}_{p^n}$ con (esattamente) p^n elementi; inoltre, tutti i campi con p^n elementi sono fra loro isomorfi, quindi basta trovarne uno per conoscerli tutti. Infine, ogni tale campo ha necessariamente caratteristica p, e in particolare il suo sottocampo fondamentale è isomorfo a $\mathbb{Z}_p$. Pertanto, un tale campo $\mathbb{F}_{p^n}$ si può costruire così: si considera l'anello $\mathbb{Z}_p[x]$, e in esso un polinomio $f(x)$ che sia *irriducibile* e *di grado* n. Allora l'anello quoziente $\mathbb{Z}_p[x]\Big/\big(f(x)\big)$ sarà un campo — perché $f(x)$ è irriducibile — contenente (una copia isomorfa di) $\mathbb{Z}_p$ — l'insieme delle classi dei polinomi costanti — di grado n su $\mathbb{Z}_p$ — perché $f(x)$ ha grado n. Allora si ha

$$\Big|\mathbb{Z}_p[x]\Big/\big(f(x)\big)\Big| \;=\; \big|\mathbb{Z}_p{}^n\big| \;=\; \big|\mathbb{Z}_p\big|^n \;=\; p^n$$

quindi $F_{p^n} := \mathbb{Z}_p[x]\Big/\big(f(x)\big)$ è un campo con esattamente p^n elementi.

Applichiamo tutto ciò al caso in esame: poiché $8 = 2^3$, abbiamo $p = 2$ e $n = 3$. Quindi basta trovare un polinomio $f(x) \in \mathbb{Z}_2[x]$ di grado 3 che sia irriducibile. Si noti che, per un polinomio di grado 3, per appurare che sia irriducibile — in $\mathbb{Z}_2[x]$ — basta verificare che non abbia radici — in $\mathbb{Z}_2$.

Un tale polinomio è $f(x) = f_1(x) := x^3 + x + 1$. Un altro è $f_2(x) := x^3 + x^2 + 1$. In effetti, $f_1(x)$ e $f_2(x)$ sono gli unici due polinomi di grado 3 irriducibili in $\mathbb{Z}_2[x]$. Pertanto

$$F_8 \;=\; \mathbb{Z}_2[x]\Big/\big(x^3 + x + 1\big) \qquad \text{oppure} \qquad F_8 \;=\; \mathbb{Z}_2[x]\Big/\big(x^3 + x^2 + 1\big)$$

sono due soluzioni al nostro problema (che sono certamente *isomorfe*).

(b) Il gruppo moltiplicativo $\big(\mathbb{F}_8{}^* ; \cdot\big)$ ha esattamente $8 - 1 = 7$ elementi. Pertanto un suo generatore ω deve avere ordine 7. Poiché 7 è primo, ciò avviene per ogni elemento in $\mathbb{F}_8{}^*$ diverso dall'elemento identità, che è $\overline{1}$. In altre parole, *ogni elemento di* $\mathbb{F}_8{}^*$ *diverso da* $\overline{1}$ *è un generatore del gruppo* $\big(\mathbb{F}_8{}^* ; \cdot\big)$. Ad esempio, possiamo scegliere $\omega := \overline{x}$.

Come controprova, *verifichiamo che* $\omega := \overline{x}$ *ha effettivamente ordine 7.* Per questo ci occorre una descrizione esplicita di $\mathbb{F}_8{}^* := \mathbb{F}_8 \setminus \{0\}$. Dalla soluzione di *(a)* abbiamo

$$\begin{aligned} F_8 \;=\; \mathbb{Z}_2[x]\Big/\big(x^3+x+1\big) \;&=\; \big\{\,\overline{0}\,,\overline{1}\,,\overline{x}\,,\overline{1+x}\,,\overline{x^2}\,,\overline{1+x^2}\,,\overline{x+x^2}\,,\overline{1+x+x^2}\,\big\} \\ &=\; \big\{\,\overline{0}\,,\;\overline{1}\,,\;\overline{x}\,,\overline{1}+\overline{x}\,,\overline{x}^{\,2}\,,\overline{1}+\overline{x}^{\,2}\,,\overline{x}+\overline{x}^{\,2}\,,\overline{1}+\overline{x}+\overline{x}^{\,2}\,\big\} \end{aligned}$$

e quindi $\mathbb{F}_8{}^* = \big\{\,\overline{1}\,,\,\overline{x}\,,\overline{1}+\overline{x}\,,\overline{x}^{\,2}\,,\overline{1}+\overline{x}^{\,2}\,,\overline{x}+\overline{x}^{\,2}\,,\overline{1}+\overline{x}+\overline{x}^{\,2}\,\big\}$.

Ora, il calcolo esplicito ci dà

$$\omega = \overline{x}\,,\quad \omega^2 = \overline{x}^{\,2}\,,\quad \omega^3 = \omega^2\,\overline{x} = \overline{x}^{\,3} = -\big(\overline{1}+\overline{x}\,\big) = \overline{1}+\overline{x}$$

$$\omega^4 = \omega^3\,\overline{x} = \big(\overline{1}+\overline{x}\,\big)\,\overline{x} = \overline{x}+\overline{x}^{\,2}\,,\quad \omega^5 = \omega^4\,\overline{x} = \big(\overline{x}+\overline{x}^{\,2}\,\big)\,\overline{x} = \overline{x}^{\,2}+\overline{x}^{\,3} = \overline{1}+\overline{x}+\overline{x}^{\,2}$$

$$\omega^6 = \big(\omega^3\big)^2 = \big(\overline{1}+\overline{x}\,\big)^2 = \overline{1}+2\cdot\overline{x}+\overline{x}^{\,2} = \overline{1}+\overline{x}^{\,2}$$

$$\omega^7 = \omega^6\,\overline{x} = \big(\overline{1}+\overline{x}^{\,2}\big)\,\overline{x} = \overline{x}+\overline{x}^{\,3} = -\overline{1} = \overline{1}$$

dove abbiamo sfruttato più volte la relazione $\overline{x}^{\,3}+\overline{x}+\overline{1} = \overline{x^3+x+1} = \overline{0}$ e anche la relazione $-a = a$, valida in ogni anello di caratteristica 2.

La conclusione è che $\omega^7 = \overline{1}$, mentre $\omega^n \neq \overline{1}$ per ogni $n = 0, 1, \ldots, 6$; pertanto ω ha ordine (moltiplicativo) pari a 7, q.e.d. □

15 — Si consideri l'estensione di campi $\mathbb{Q} \subseteq \mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$.
(a) Determinare un elemento primitivo dell'estensione, e il suo polinomio minimo su $\mathbb{Q}$.
(b) Calcolare il gruppo di Galois $G\Big(\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)\Big/\mathbb{Q}\Big)$ dell'estensione.

<u>Soluzione</u>*: (a)* Chiaramente $\sqrt{3}$ ha grado 2 su $\mathbb{Q}$, e una base di $\mathbb{Q}\big(\sqrt{3}\,\big)$ su $\mathbb{Q}$ è $\big\{\,1\,,\,\sqrt{3}\,\big\}$. Analogamente, $\sqrt{5}$ ha grado 2 su $\mathbb{Q}$, e una base di $\mathbb{Q}\big(\sqrt{5}\,\big)$ su $\mathbb{Q}$ è $\big\{\,1\,,\,\sqrt{5}\,\big\}$. Da questo segue subito (vale in generale!) che l'insieme dei prodotti di tali basi

$$B \;:=\; \Big\{\,1\,,\,\sqrt{3}\,,\,\sqrt{5}\,,\,\sqrt{3}\,\sqrt{5}\,\Big\}$$

è un insieme di generatori di $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$ come spazio vettoriale su $\mathbb{Q}$. Inoltre, quanto affermato implica anche che $\big\{\,1\,,\,\sqrt{5}\,\big\}$ è un insieme di generatori di $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$ come spazio vettoriale su $\mathbb{Q}\big(\sqrt{3}\,\big)$, in quanto $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$ può anche essere interpretato come estensione $\Big(\mathbb{Q}\big(\sqrt{3}\,\big)\Big)\big(\sqrt{5}\,\big)$ di $\mathbb{Q}\big(\sqrt{3}\,\big)$ tramite $\sqrt{5}$. Pertanto $\Big[\,\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big) : \mathbb{Q}\big(\sqrt{3}\,\big)\Big] \leq 2$, e vale l'identità se e soltanto se $\sqrt{5} \notin \mathbb{Q}\big(\sqrt{3}\,\big)$. Ora, per quanto già detto si ha

$$\mathbb{Q}\big(\sqrt{3}\,\big) \;=\; \Big\{\,a+b\sqrt{3}\;\Big|\;a,b\in\mathbb{Q}\,\Big\} \tag{23}$$

e quindi

$$\sqrt{5} \;\notin\; \mathbb{Q}\big(\sqrt{3}\,\big) \quad\Longleftrightarrow\quad \nexists\, a,b\in\mathbb{Q} \,:\, \big(a+b\,\sqrt{3}\,\big)^2 = 5 \tag{24}$$

Ma il calcolo diretto dà

$$\left(a+b\sqrt{3}\right)^2 \;=\; a^2+3\,b^2+2\,a\,b\sqrt{3} \;=\; 5 \quad\Longleftrightarrow\quad \circledast\begin{cases} a^2+3\,b^2 \;=\; 5 \\ a\,b \;=\; 0 \end{cases} \tag{25}$$

e *non esistono soluzioni* in $\mathbb{Q}$ del sistema (in due incognite a e b) indicato con $\circledast$. In conclusione, da (23), (24) e (25) ricaviamo che $\sqrt{5}\notin\mathbb{Q}\big(\sqrt{3}\,\big)$, e quindi deduciamo che $\Big[\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big):\mathbb{Q}\big(\sqrt{3}\,\big)\Big]=2$. Sfruttando la moltiplicatività del grado, questo ci dà

$$\Big[\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big):\mathbb{Q}\Big] \;=\; \Big[\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big):\mathbb{Q}\big(\sqrt{3}\,\big)\Big]\cdot\Big[\mathbb{Q}\big(\sqrt{3}\,\big):\mathbb{Q}\Big] \;=\; 2\cdot 2 \;=\; 4 \tag{26}$$

Dunque l'estensione $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$ ha grado 4 su $\mathbb{Q}$; perciò, dall'analisi precedente e dalla (26) concludiamo anche che

$$B \;:=\; \Big\{1\,,\;\sqrt{3}\,,\;\sqrt{5}\,,\;\sqrt{3}\,\sqrt{5}\Big\} \quad\text{è base di } \mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big) \text{ su } \mathbb{Q}\,. \tag{27}$$

Cerchiamo ora un elemento primitivo dell'estensione $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)\Big/\mathbb{Q}$.

Consideriamo l'elemento $\alpha:=\sqrt{3}+\sqrt{5}\,\in\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$. Poiché $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$ ha grado 4 su $\mathbb{Q}$, le sole possibilità per il grado di α, indicato con $\partial(\alpha)$, sono $\partial(\alpha)=1$, $\partial(\alpha)=2$ oppure $\partial(\alpha)=4$. Il calcolo diretto ci dà

$$\alpha^2 \;\overset{*}{=}\; 8+2\,\sqrt{3}\,\sqrt{5} \qquad\Longrightarrow\qquad \alpha\notin\mathbb{Q}\,,\quad 2\,\sqrt{3}\,\sqrt{5}\;\overset{\bullet}{=}\;\alpha^2-8 \tag{28}$$

Quindi in particolare $\partial(\alpha)\neq 1$ perché $\alpha\notin\mathbb{Q}$. Inoltre dall'identità $\overset{*}{=}$ in (28) otteniamo che, per ogni $a,b\in\mathbb{Q}$, si ha

$$\alpha^2+a\,\alpha+b \;=\; 2\,\sqrt{3}\,\sqrt{5}+a\,\sqrt{3}+a\,\sqrt{5}+(8+b) \;\neq\; 0$$

in virtù della (27): e questo significa che $\partial(\alpha)\neq 2$. Pertanto, si ottiene che $\partial(\alpha)\neq 4$.

La conclusione è che α è un elemento di $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$ che ha grado su $\mathbb{Q}$ pari a 4, cioè esattamente il grado di $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$ stesso su $\mathbb{Q}$: ne segue allora che $\mathbb{Q}(\alpha)=\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)$, cioè *$\alpha$ è elemento primitivo dell'estensione* $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)\Big/\mathbb{Q}$.

Infine, ancora il calcolo diretto ci dà (usando la $\overset{\bullet}{=}$ in (28) per ottenere la $\overset{\star}{=}$ qui sotto)

$$\alpha^4=\Big(8+2\,\sqrt{3}\,\sqrt{5}\Big)^2 \;=\; 124+16\cdot 2\,\sqrt{3}\,\sqrt{5} \;\overset{\star}{=}\; 124+16\,\alpha^2-128 \;=\; 16\,\alpha^2-4 \;\Longrightarrow$$
$$\Longrightarrow\qquad p(\alpha)\;=\;0\,,\quad p(x)\;:=\;x^4-\,16\,x^2+\,4\;\in\mathbb{Q}[x]$$

Dunque α è radice del polinomio $p(x)$, che appartiene a $\mathbb{Q}[x]$, è monico e ha grado 4, cioè il grado di α su $\mathbb{Q}$. Allora *il polinomio minimo di α su $\mathbb{Q}$ è proprio* $p(x):=x^4-16\,x^2+4$.

(b) Per brevità indichiamo con $G := G\Big(\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)\Big/\mathbb{Q}\Big)$ il gruppo di Galois dell'estensione $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)\Big/\mathbb{Q}$. Consideriamo un qualsiasi automorfismo $\sigma \in G$: esso è univocamente determinato dalla sua azione sui generatori dell'estensione, che sono $\sqrt{3}$ e $\sqrt{5}$. Inoltre, $\sigma\big(\sqrt{3}\big)$ dev'essere un coniugato di $\sqrt{3}$, cioè una radice del polinomio minimo di $\sqrt{3}$ su $\mathbb{Q}$, che è x^2-3 ; le radici di quest'ultimo — in $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)$ — sono $\sqrt{3}$ e $-\sqrt{3}$, quindi in definitiva dev'essere $\sigma\big(\sqrt{3}\big) \in \big\{\sqrt{3}, -\sqrt{3}\big\}$. In modo del tutto analogo, troviamo che dev'essere $\sigma\big(\sqrt{5}\big) \in \big\{\sqrt{5}, -\sqrt{5}\big\}$. Ci sono dunque *al più* quattro possibili automorfismi $\sigma_{\pm,\pm} \in G$, dati da

$$\begin{aligned}
\sigma_{+,+} &: \quad \sqrt{3} \mapsto +\sqrt{3}\,, \;\; \sqrt{5} \mapsto +\sqrt{5} \\
\sigma_{+,-} &: \quad \sqrt{3} \mapsto +\sqrt{3}\,, \;\; \sqrt{5} \mapsto -\sqrt{5} \\
\sigma_{-,+} &: \quad \sqrt{3} \mapsto -\sqrt{3}\,, \;\; \sqrt{5} \mapsto +\sqrt{5} \\
\sigma_{-,-} &: \quad \sqrt{3} \mapsto -\sqrt{3}\,, \;\; \sqrt{5} \mapsto -\sqrt{5}
\end{aligned} \tag{29}$$

inoltre, rispetto alla base B di $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)$ data in (27) essi sarebbero descritti esplicitamente dalle formule

$$\begin{aligned}
\sigma_{+,+} &: \quad 1 \mapsto 1\,, \;\; \sqrt{3} \mapsto +\sqrt{3}\,, \;\; \sqrt{5} \mapsto +\sqrt{5}\,, \;\; \sqrt{3}\sqrt{5} \mapsto +\sqrt{3}\sqrt{5} \\
\sigma_{+,-} &: \quad 1 \mapsto 1\,, \;\; \sqrt{3} \mapsto +\sqrt{3}\,, \;\; \sqrt{5} \mapsto -\sqrt{5}\,, \;\; \sqrt{3}\sqrt{5} \mapsto -\sqrt{3}\sqrt{5} \\
\sigma_{-,+} &: \quad 1 \mapsto 1\,, \;\; \sqrt{3} \mapsto -\sqrt{3}\,, \;\; \sqrt{5} \mapsto +\sqrt{5}\,, \;\; \sqrt{3}\sqrt{5} \mapsto -\sqrt{3}\sqrt{5} \\
\sigma_{-,-} &: \quad 1 \mapsto 1\,, \;\; \sqrt{3} \mapsto -\sqrt{3}\,, \;\; \sqrt{5} \mapsto -\sqrt{5}\,, \;\; \sqrt{3}\sqrt{5} \mapsto +\sqrt{3}\sqrt{5}
\end{aligned} \tag{30}$$

volendo esprimersi tramite matrici, i vari $\sigma_{\pm,\pm}$ avrebbero matrici molto semplici:

$$\begin{aligned}
\sigma_{+,+} &\simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad
\sigma_{+,-} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \\
\sigma_{-,+} &\simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \qquad
\sigma_{-,-} \simeq \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}
\end{aligned} \tag{31}$$

Infine, osserviamo che gli endomorfismi di $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)$, come spazio vettoriale su $\mathbb{Q}$, univocamente determinati dalle matrici in (31) sono anche automorfismi di campo di $\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)$, e ristretti a $\mathbb{Q}$ coincidono con $id_{\mathbb{Q}}$: pertanto, essi appartengono al gruppo di Galois $G\Big(\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)\Big/\mathbb{Q}\Big) =: G$. Si noti in particolare che $\sigma_{+,+} = id_{\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right)}$.

In conclusione quindi abbiamo

$$G\Big(\mathbb{Q}\big(\sqrt{3},\sqrt{5}\big)\Big/\mathbb{Q}\Big) \;=\; \Big\{\, \sigma_{+,+} = id_{\mathbb{Q}\left(\sqrt{3},\sqrt{5}\right)}\,,\, \sigma_{+,-}\,,\, \sigma_{-,+}\,,\, \sigma_{-,-} \,\Big\}$$

dove i $\sigma_{\pm,\pm}$ sono gli automorfismi testé descritti.

Infine, la struttura di gruppo di $G\Big(\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)\Big/\mathbb{Q}\Big)$ è data dalle formule

$$\sigma_{+,+}\,\sigma_{\epsilon,\eta} \;=\; \sigma_{\epsilon,\eta}\;, \quad \sigma_{\epsilon,\eta}\,\sigma_{\epsilon,\eta} \;=\; \sigma_{+,+}\;, \quad \sigma_{\epsilon,\eta}\,\sigma_{\epsilon',\eta'} \;=\; \sigma_{\epsilon',\eta'}\,\sigma_{\epsilon,\eta} \qquad \forall\ \epsilon,\eta,\epsilon',\eta' \in \{+,-\}$$
$$\sigma_{\epsilon,\eta}\,\sigma_{\epsilon',\eta'} \;=\; \sigma_{\epsilon'',\eta''} \quad \forall\ \epsilon,\eta,\epsilon',\eta',\epsilon'',\eta'' : \big\{(\epsilon,\eta),(\epsilon',\eta'),(\epsilon'',\eta'')\big\} = \big\{(+,-),(-,+),(-,-)\big\}$$

che si ricavano dalle (29) — o dalle (30), o dalle (31) — tramite calcolo diretto dei prodotti (composizioni di automorfismi) in esame, e consentono di scrivere tutta la tabella moltiplicativa del gruppo. In conseguenza, esistono isomorfismi $G\Big(\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)\Big/\mathbb{Q}\Big) \cong \mathbb{Z}_2\times\mathbb{Z}_2$ di gruppi, per esempio quello dato da

$$\begin{aligned} G\Big(\mathbb{Q}\big(\sqrt{3},\sqrt{5}\,\big)\Big/\mathbb{Q}\Big) &\xrightarrow{\;\cong\;} \mathbb{Z}_2\times\mathbb{Z}_2 \\ \sigma_{+,+} &\longrightarrow \big(\overline{0},\overline{0}\,\big) \\ \sigma_{+,-} &\longrightarrow \big(\overline{0},\overline{1}\,\big) \\ \sigma_{-,+} &\longrightarrow \big(\overline{1},\overline{0}\,\big) \\ \sigma_{-,-} &\longrightarrow \big(\overline{1},\overline{1}\,\big) \end{aligned}$$

□