

CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2018–2019

Esame scritto del 4 Febbraio 2019 — Sessione Estiva Anticipata, I appello

Testo & Svolgimento

..... *

[1] — Nell'insieme $\mathbb{Z}$ dei numeri interi si consideri la relazione ρ definita da

$$a \rho b \stackrel{\Delta}{\iff} (a^2 - b^2) \in 9\mathbb{Z} \quad \forall \ a, b \in \mathbb{Z}$$

- (a) Dimostrare che ρ è una equivalenza in $\mathbb{Z}$;
- (b) dimostrare che ρ non è compatibile con la somma in $\mathbb{Z}$;
- (c) descrivere esplicitamente la classe di ρ -equivalenza $[3]_\rho$;
- (d) descrivere l'insieme quoziente $\mathbb{Z}/\rho$.

[2] — Calcolare le ultime due cifre decimali — relativamente alla scrittura posizionale in base dieci — del numero $N := 87053214^{48301}$.

[3] — Sia $G := \text{GL}_2(\mathbb{Z}_3)$ il gruppo generale lineare delle matrici 2×2 invertibili a coefficienti in $\mathbb{Z}_3$, con l'operazione di prodotto righe per colonne, e sia

$$B := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid c = 0 \right\}, \quad H := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid c = 0, a d = 1 \right\}$$

Si ha allora che B è sottogruppo di $\text{GL}_2(\mathbb{Z}_3)$, mentre H è sottoinsieme di B .

- (a) Dimostrare che $H \trianglelefteq B$;
- (b) dimostrare che H è ciclico, determinandone esplicitamente un generatore;
- (c) descrivere esplicitamente il centro $Z(B)$ del gruppo B .

[4] — Sia G un gruppo, $K \leq G$ e $N \trianglelefteq G$. Dimostrare che

- (a) $KN = NK$;
- (b) $KN \leq G$;
- (c) $N \trianglelefteq KN$;
- (d) $(K \cap N) \trianglelefteq K$;
- (e) esiste un isomorfismo tra gruppi quoziente $K / (K \cap N) \cong (KN) / N$.

[5] — Sia E un insieme, sia $\mathbb{A}_E := \mathcal{P}(E)$ il suo insieme delle parti, e sia $E_0 \in \mathbb{A}_E$. Si consideri in $\mathbb{A}_E$ la relazione η_0 definita da

$$F' \eta_0 F'' \iff F' \cap E_0 = F'' \cap E_0 \quad \forall F', F'' \in \mathbb{A}_E$$

Dimostrare che:

- (a) η_0 è un'equivalenza in $\mathbb{A}_E$;
- (b) η_0 è compatibile con ciascuna delle tre operazioni $\cup$, $\cap$ e Δ in $\mathbb{A}_E$;
- (c) per ogni $F \in \mathbb{A}_E$, la classe di η_0 -equivalenza $[F]_{\eta_0}$ è sottoinsieme (di $\mathbb{A}_E$) chiuso per le due operazioni $\cup$ e $\cap$;
- (d) per ogni $F \in \mathbb{A}_E$, la classe di η_0 -equivalenza $[F]_{\eta_0}$ è sottoinsieme (di $\mathbb{A}_E$) chiuso per l'operazione $\Delta \iff [F]_{\eta_0} = [\emptyset]_{\eta_0}$;
- (e) prendendo in $\mathbb{A}_E := \mathcal{P}(E)$ la struttura di anello con Δ come “somma” e $\cap$ come “prodotto”, esiste un isomorfismo dall'anello quoziente $\mathbb{A}_E / \eta_0$ all'anello $(\mathcal{P}(E_0); \Delta, \cap)$.

[6] — Si consideri il dominio unitario $\mathbb{Z}[\sqrt{-15}]$ — sottoanello unitario di $\mathbb{C}$ generato da $\sqrt{-15}$ — e su di esso la funzione $v : \mathbb{Z}[\sqrt{-15}] \longrightarrow \mathbb{N}$ che ad ogni $\zeta = a + b\sqrt{-15}$ ($\in \mathbb{Z}[\sqrt{-15}]$) associa $v(\zeta) = v(a + b\sqrt{-15}) = a^2 + 15b^2$.

- (a) Dimostrare che $\mathbb{Z}[\sqrt{-15}]$ è un dominio a fattorizzazione (o “dominio atomico”);
- (b) dimostrare che non esiste $\zeta \in \mathbb{Z}[\sqrt{-15}]$ tale che $v(\zeta) = 2$ oppure $v(\zeta) = 8$;
- (c) dimostrare che $\mathbb{Z}[\sqrt{-15}]$ non è un dominio a fattorizzazione unica.

— ★ —

SVOLGIMENTO

N.B.: lo svolgimento qui presentato è molto lungo... Questo non significa che lo svolgimento ordinario di tale compito (nel corso di un esame scritto) debba essere altrettanto lungo. Semplicemente, questo lo è perché si approfitta per spiegare — in diversi modi, con lunghe digressioni, ecc. ecc. — in dettaglio e con molti particolari tutti gli aspetti della teoria toccati più o meno a fondo dal testo in questione.

[1] — Ricordando che la relazione ρ in $\mathbb{Z}$ è definita da

$$a \rho b \stackrel{\Delta}{\iff} (a^2 - b^2) \in 9\mathbb{Z} \quad \forall a, b \in \mathbb{Z}$$

procediamo alla soluzione dell'esercizio punto per punto.

(a) Dobbiamo dimostrare che ρ è una equivalenza in $\mathbb{Z}$; possiamo farlo seguendo due metodi diversi.

Primo metodo: verifichiamo direttamente che la relazione ρ gode delle tre proprietà che caratterizzano ogni equivalenza, cioè la *riflessività*, la *transitività*, la *simmetricità*.

I calcoli diretti ci danno:

$$(a^2 - a^2) = 0 = 9 \cdot 0 \in 9\mathbb{Z} \implies a \rho a \quad \forall a \in \mathbb{Z}$$

quindi ρ è *riflessiva*, q.e.d.; per la *transitività*, per ogni $a, b, c \in \mathbb{Z}$ si ha

$$\begin{aligned} a \rho b, b \rho c &\implies (a^2 - b^2), (b^2 - c^2) \in 9\mathbb{Z} \implies \\ &\implies \exists d, q \in \mathbb{Z} : a^2 - b^2 = 9d, b^2 - c^2 = 9q \implies \\ &\implies a^2 - c^2 = a^2 - b^2 + b^2 - c^2 = 9d + 9q = 9(d + q) \in 9\mathbb{Z} \implies a \rho c \end{aligned}$$

quindi ρ è *transitiva*, q.e.d.; per la *simmetricità* infine, per ogni $a, b \in \mathbb{Z}$ abbiamo

$$\begin{aligned} a \rho b &\implies (a^2 - b^2), (b^2 - c^2) \in 9\mathbb{Z} \implies \exists d \in \mathbb{Z} : a^2 - b^2 = 9d \implies \\ &\implies \exists (-d) \in \mathbb{Z} : b^2 - a^2 = 9(-d) \in 9\mathbb{Z} \implies b \rho a \end{aligned}$$

quindi ρ è *simmetrica*, q.e.d.

Secondo metodo: ricordiamo che, data una qualsiasi applicazione $f : X \longrightarrow Y$, la relazione ρ_f in X definita da $x_1 \rho_f x_2 \iff f(x_1) = f(x_2)$ — per ogni $x_1, x_2 \in X$ — è una equivalenza. Ora, osserviamo che la relazione ρ può essere caratterizzata così

$$a \rho b \stackrel{\Delta}{\iff} (a^2 - b^2) \in 9\mathbb{Z} \iff a^2 \equiv b^2 \pmod{9}; \iff (\pi_9 \circ \square)(a) = (\pi_9 \circ \square)(b)$$

(per ogni $a, b \in \mathbb{Z}$) dove $\pi_9 : \mathbb{Z} \longrightarrow \mathbb{Z}_9$ ($z \mapsto \bar{z} = [z]_9$) è la proiezione canonica da $\mathbb{Z}$ a $\mathbb{Z}_9 := \mathbb{Z}/\equiv_9$ mentre $\square : \mathbb{Z} \longrightarrow \mathbb{Z}$ ($z \mapsto z^2$) è la funzione “potenza al quadrato” in $\mathbb{Z}$.

Dunque i calcoli precedenti danno $a \rho b \iff (\pi_9 \circ \square)(a) = (\pi_9 \circ \square)(b)$, ma l'ultima condizione è quella che definisce la relazione $\rho_{(\pi_9 \circ \square)}$, dunque abbiamo $\rho = \rho_{(\pi_9 \circ \square)}$, e siccome sappiamo che quest'ultima è un'equivalenza possiamo concludere che ρ stessa è un'equivalenza, q.e.d.

(b) Per dimostrare che ρ non è compatibile con la somma in $\mathbb{Z}$, dobbiamo trovare quattro elementi $a', b', a'', b'' \in \mathbb{Z}$ tali che $a_1 \rho b_1, a_2 \rho b_2$, ma $(a_1 + a_2) \not\rho (b_1 + b_2)$, cioè

$$(a_1^2 - b_1^2) \in 9\mathbb{Z}, \quad (a_2^2 - b_2^2) \in 9\mathbb{Z}, \quad ((a_1^2 - b_1^2) - (a_2^2 - b_2^2)) \notin 9\mathbb{Z} \quad (1)$$

Ora, siccome $\rho = \rho_{(\pi_9 \circ \square)}$ — per quanto visto nella dimostrazione del punto (a) — dunque attraverso la proiezione canonica π_9 , di fatto è sufficiente cercare tali valori a_1, b_1, a_2, b_2 in $\{0, 1, 2, \dots, 7, 8\}$. Possiamo ad esempio scegliere $a_1 := 0, b_1 := 3, a_2 := 2, b_2 := 7$, per i quali si ha

$$\begin{aligned} a_1^2 - b_1^2 &= 0^2 - 3^2 = 0 - 9 = -9 = 9 \cdot (-1) \in 9\mathbb{Z} \implies a_1 \rho b_1 \\ a_2^2 - b_2^2 &= 2^2 - 7^2 = 4 - 49 = -45 = 9 \cdot (-5) \in 9\mathbb{Z} \implies a_2 \rho b_2 \end{aligned}$$

$$(a_1 + a_2)^2 - (b_1 + b_2)^2 = (0 + 2)^2 - (3 + 7)^2 = 2^2 - 10^2 = 4 - 100 = -96 \notin 9\mathbb{Z}$$

dove l'ultima formula ci dice appunto che $a_1 \not\equiv b_1$, q.e.d.

(c) Dovendo descrivere esplicitamente la classe di ρ -equivalenza $[3]_\rho$, ricordiamo che essa è definita da $[3]_\rho := \{z \in \mathbb{Z} \mid z \rho 3\}$. Ma siccome abbiamo visto — nel risolvere il quesito (a) — che $\rho = \rho_{(\pi_9 \circ \square)}$, otteniamo

$$\begin{aligned} [3]_\rho &:= \{z \in \mathbb{Z} \mid z \rho 3\} = \{z \in \mathbb{Z} \mid z \rho_{(\pi_9 \circ \square)} 3\} = \\ &= \{z \in \mathbb{Z} \mid (\pi_9 \circ \square)(z) = (\pi_9 \circ \square)(3)\} = \{z \in \mathbb{Z} \mid \bar{z}^2 = \bar{3}^2 = \bar{0}\} \end{aligned}$$

e allora un calcolo elementare ci mostra infine che $[3]_\rho = 3\mathbb{Z}$.

(d) Per definizione l'insieme quoziente $\mathbb{Z}/\rho$ è l'insieme i cui elementi sono le classi di ρ -equivalenza in $\mathbb{Z}$. Utilizzando il fatto che $\rho = \rho_{(\pi_9 \circ \square)}$, per ogni $z \in \mathbb{Z}$ la corrispondente classe di ρ -equivalenza è data da

$$\begin{aligned} [z]_\rho &= [z]_{\rho_{(\pi_9 \circ \square)}} = \{\zeta \in \mathbb{Z} \mid \zeta \rho_{(\pi_9 \circ \square)} z\} = \\ &= \{\zeta \in \mathbb{Z} \mid (\pi_9 \circ \square)(\zeta) = (\pi_9 \circ \square)(z)\} = (\pi_9 \circ \square)^{-1}((\pi_9 \circ \square)(z)) \end{aligned}$$

e quindi esiste una classe di equivalenza per ogni valore della funzione $(\pi_9 \circ \square)$, precisamente la classe formata dal sottoinsieme che controimmagine tramite la funzione $(\pi_9 \circ \square)$ di tale valore. Globalmente, questo è codificato dal *Teorema Fondamentale delle Applicazioni*, che ci garantisce che l'applicazione $(\pi_9 \circ \square) : \mathbb{Z} \longrightarrow \mathbb{Z}_9$ induce una biiezione $(\pi_9 \circ \square)_* : \mathbb{Z}/\rho_{(\pi_9 \circ \square)} \longleftarrow \longrightarrow \text{Im}(\pi_9 \circ \square)$ definita da $(\pi_9 \circ \square)_*([z]_{(\pi_9 \circ \square)}) := (\pi_9 \circ \square)(z)$.

Ora, facendo i calcoli in $\mathbb{Z}_9$ e osservando che $(\pi_9 \circ \square)(z) := \bar{z}^2 = \bar{z}^2$ otteniamo subito

$$\text{Im}(\pi_9 \circ \square) := \{(\pi_9 \circ \square)(z) \mid z \in \mathbb{Z}\} := \{\bar{z}^2 \mid z \in \mathbb{Z}\} := \{\bar{0}, \bar{1}, \bar{4}, \bar{7}\}$$

cos'ì abbiamo quattro valori in tutto per la funzione $(\pi_9 \circ \square)$: in corrispondenza, abbiamo in tutto esattamente quattro classi di ρ -equivalenza in $\mathbb{Z}/\rho = \mathbb{Z}/\rho_{(\pi_9 \circ \square)}$, date da

$$\begin{aligned} C_0 &:= (\pi_9 \circ \square)^{-1}(\bar{0}) = \{z \in \mathbb{Z} \mid \bar{z}^2 = \bar{0}\} = 3\mathbb{Z} = [0]_\rho \\ C_1 &:= (\pi_9 \circ \square)^{-1}(\bar{1}) = \{z \in \mathbb{Z} \mid \bar{z}^2 = \bar{1}\} = (1 + 9\mathbb{Z}) \cup (8 + 9\mathbb{Z}) = [1]_\rho \\ C_4 &:= (\pi_9 \circ \square)^{-1}(\bar{4}) = \{z \in \mathbb{Z} \mid \bar{z}^2 = \bar{4}\} = (2 + 9\mathbb{Z}) \cup (7 + 9\mathbb{Z}) = [2]_\rho \\ C_7 &:= (\pi_9 \circ \square)^{-1}(\bar{7}) = \{z \in \mathbb{Z} \mid \bar{z}^2 = \bar{7}\} = (4 + 9\mathbb{Z}) \cup (5 + 9\mathbb{Z}) = [4]_\rho \end{aligned}$$

dove sulla destra abbiamo descritto la classe come insieme e (all'estrema destra) l'abbiamo individuata indicandone un possibile rappresentante.

[2] — Trovare le ultime due cifre decimali del numero $N (\in \mathbb{N})$ significa trovarne il resto (non negativo) nella divisione per 100, cioè trovare quell'unico numero naturale $r \in \{0, 1, 2, \dots, 98, 99\}$ tale che $N = 100 \cdot q + r$ per un certo $q \in \mathbb{N}$ (che qui non ci interessa conoscere). Dunque r è l'unico numero intero nell'intervallo $\{0, 1, \dots, 99\}$ tale che $N = 100 \cdot q + r \equiv r \pmod{100}$, cioè $\overline{N} = \overline{r}$ in $\mathbb{Z}_{100}$ con $r \in \{0, 1, \dots, 99\}$.

Ora, nel caso in esame il numero N è della forma $N = B^E$. Da tale espressione segue che $\overline{N} = \overline{B^E} = \overline{B}^E$ in $\mathbb{Z}_{100}$, quindi una prima riduzione del problema (a una forma più semplice) si ottiene semplificando la rappresentazione della classe $\overline{B}$, cioè scegliendo un rappresentante “piccolo” — ad esempio, compreso tra 0 e 99, oppure tra -50 e +50 — per la classe di congruenza $\overline{B}$. Una ulteriore semplificazione può riguardare eventualmente l’“esponente” E , ma questa dipende dalla relazione tra B — o un qualsiasi rappresentante più semplice della sua classe di congruenza $\overline{B}$ — e il modulo 100, quindi dipenderà da un’analisi caso per caso. Nello specifico abbiamo $B := 87053214$, $E := 48301 \in \mathbb{N}$: perciò $\overline{B} = \overline{87053214} = \overline{14} \in \mathbb{Z}_{100}$, quindi

$$\overline{N} = \overline{87053214^{48301}} = \overline{87053214}^{48301} = \overline{14}^{48301} \quad (2)$$

A questo punto osserviamo che le potenze di $\overline{B} := \overline{14}$ stanno in $\mathbb{Z}_{100}$, che è un anello con 100 elementi: quindi tra le potenze con esponenti da 0 a 100 ce ne saranno almeno due che saranno uguali, pur avendo esponenti diversi — in formule, avremo $e', e'' \in \{0, 1, 2, \dots, 100\}$ con $e' < e''$ tali che $\overline{14}^{e'} = \overline{14}^{e''}$. Così ponendo $E_0 := e' \in \mathbb{N}$ e $k := e'' - e' \in \mathbb{N}_+$ avremo $\overline{B}^{E_0} = \overline{B}^{E_0+k}$; possiamo allora scegliere E_0 e k *minimi possibili* con queste proprietà (anche se a rigore non è necessario: serve soltanto a ottimizzare i passi successivi). Da questo segue che

$$\overline{B}^{E_0} = \overline{B}^{E_0+k} = \overline{B}^{E_0+k+k} = \dots = \overline{B}^{E_0+qk} \quad \forall q \in \mathbb{N}$$

A questo, se $E < E_0$ non facciamo nulla, ma se invece $E \geq E_0$ allora dividiamo $E' := (E - E_0)$ per k ottenendo $E' = qk + r$ con $0 \leq r < k$ e riscriviamo

$$\overline{N} := \overline{B}^E = \overline{B}^{E_0+(E-E_0)} = \overline{B}^{E_0+qk+r} = \overline{B}^{E_0+r} \quad (3)$$

così per calcolare N possiamo utilizzare la formula semplificata $N = B^{E_0+r}$ (con esponente più basso di E dato all’inizio). Si noti anche che non serve davvero fare la divisione di E' per k , ci basta conoscerne il resto r , cioè ci basta conoscere la classe resto di E' modulo k (descritta tramite il suo rappresentante canonico compreso tra 0 e $k-1$).

Per applicare tutto questo al caso di $B := \overline{14}$ possiamo procedere secondo due metodi.

Primo metodo: Il primo metodo è diretto: calcoliamo potenze di $B := \overline{14}$ cercando E_0 e k minimali con le proprietà richieste. I calcoli espliciti — direttamente in $\mathbb{Z}_{100}$, il che facilita i conti! — ci danno

$$\begin{aligned} \overline{14}^2 &= \overline{96} = -\overline{4}, & \overline{14}^3 &= (-\overline{4}) \cdot \overline{14} = -\overline{56} = \overline{44}, & \overline{14}^4 &= (\overline{14}^2)^2 = (-\overline{4})^2 = \overline{16} \\ \overline{14}^5 &= \overline{16} \cdot \overline{14} = \overline{24}, & \overline{14}^6 &= (\overline{14}^2)^3 = (-\overline{4})^3 = -\overline{64} = \overline{36} \\ \overline{14}^7 &= \overline{14}^5 \cdot \overline{14}^2 = \overline{24} \cdot (-\overline{4}), & \overline{14}^8 &= (\overline{14}^4)^2 = (\overline{16})^2 = \overline{56} = -\overline{44} \end{aligned}$$

Da queste formule otteniamo in particolare $\overline{14}^8 = -\overline{14}^3$, da cui segue subito che

$$\overline{14}^{13} = \overline{14}^8 \cdot \overline{14}^5 = -\overline{14}^3 \cdot \overline{14}^5 = -\overline{14}^8 = -(-\overline{14}^3) = \overline{14}^3$$

quindi in conclusione troviamo i valori (minimali!) $E_0 = 3$ e $k = 10$. Considerando ora il nostro esponente $E := 48301$ in (2) e dividendo $E' := E - E_0 = 48301 - 3 = 48298$ per $k = 10$ troviamo resto $r = 8$. Pertanto, da (2) e (3) otteniamo

$$\overline{N} := \overline{B}^E = \overline{14}^{4831} = \overline{14}^{3+8} = \overline{14}^{11}$$

La potenza $\overline{14}^{11}$ non è ulteriormente semplificabile; comunque, dai calcoli già effettuati otteniamo

$$\overline{N} := \overline{14}^{11} = \overline{14}^3 \cdot \overline{14}^8 = \overline{44} \cdot (-\overline{44}) = -\overline{36} = \overline{64}$$

quindi in conclusione abbiamo che $\overline{N} = \overline{64}$ in $\mathbb{Z}_{100}$, quindi *le ultime due cifre decimali di* $N := 87053214^{48301}$ *sono* 64.

Secondo metodo: Il secondo metodo opera una semplificazione, in quanto passiamo a fare calcoli in anelli $\mathbb{Z}_{d_i}$ dove i d_i saranno divisori di 100 — dunque gli anelli $\mathbb{Z}_{d_i}$ sono *più piccoli* di $\mathbb{Z}_{100}$, e in corrispondenza i calcoli sono più semplici. Tutto sta ad osservare che, dato che $100 = 4 \cdot 25$ con $\text{MCD}(4, 25) = 1$, il *Teorema Cinese del Resto* ci garantisce che per ogni $x, M \in \mathbb{Z}$ si ha

$$x \equiv M \pmod{100} \iff \begin{cases} x \equiv M \pmod{4} \\ x \equiv M \pmod{25} \end{cases}$$

Applicando questo a $M := N = B^E = 87053214^{48301}$, otteniamo

$$x \equiv 87053214^{48301} \pmod{100} \iff \circledast : \begin{cases} x \equiv 87053214^{48301} \pmod{4} \\ x \equiv 87053214^{48301} \pmod{25} \end{cases}$$

dove ovviamente il sistema di destra si semplifica in $\circledast' : \begin{cases} x \equiv 2^{48301} \pmod{4} \\ x \equiv 14^{48301} \pmod{25} \end{cases}$

perché $87053214 \equiv 2 \pmod{4}$ e $87053214 \equiv 14 \pmod{25}$.

Ora, per la prima equazione congruenziale osserviamo che $2^2 = 4 \equiv 0 \pmod{4}$ e quindi abbiamo subito $2^{48301} = 2^2 \equiv 0 \cdot 2^{48299} \equiv 0 \pmod{4}$; perciò il sistema $\circledast'$ si

semplifica in $\circledast'' : \begin{cases} x \equiv 0 \pmod{4} \\ x \equiv 14^{48301} \pmod{25} \end{cases}$. Per la seconda equazione congruenziale,

notiamo che $\text{MCD}(14, 25) = 1$, quindi *si può applicare il Teorema di Eulero*, che ci garantisce che $14^{\phi(25)} \equiv 1 \pmod{25}$: quindi se $48301 = \phi(25)q + r$ è la divisione di 48301 per $\phi(25)$ avremo

$$14^{48301} \equiv 14^{\phi(25)q+r} \equiv \left(14^{\phi(25)}\right)^q \cdot 14^r \equiv \left(1^{\phi(25)}\right)^q \cdot 14^r \equiv 14^r \pmod{25} \quad (4)$$

dove in effetti ci serve soltanto conoscere il resto r della divisione di 48301 per $\phi(25)$. In concreto, abbiamo $\phi(25) = \phi(5^2) = 5(4 - 1) = 20$, e ovviamente $48301 \equiv 1 \pmod{20}$,

così che il resto della divisione di 48301 per $\phi(25) = 20$ è $r = 1$. Perciò la (4) ci dà $14^{48301} \equiv 14^1 = 14 \pmod{25}$, dunque in conclusione il sistema $\circledast''$ si semplifica in

$$\circledast^\circ : \begin{cases} x \equiv 0 & (\text{mod } 4) \\ x \equiv 14 & (\text{mod } 25) \end{cases} \quad (5)$$

Resta ora soltanto da risolvere il sistema (5), e sceglierne l'unica soluzione compresa tra 0 e 99. Procedendo per sostituzioni successive, la prima equazione in (5) ha ovviamente soluzioni $x = 4k$ ($k \in \mathbb{Z}$), e sostituendo nella seconda otteniamo

$$\begin{aligned} x \equiv_{25} 14 &\iff 4k \equiv_{25} 14 \iff (-6) \cdot 4k \equiv_{25} (-6) \cdot 14 \iff \\ &\iff 1 \cdot k \equiv_{25} (-24)k \equiv_{25} -84 \equiv_{25} 16 \iff k \equiv_{25} 16 \iff k = 16 + 25h \quad (h \in \mathbb{Z}) \end{aligned}$$

da cui poi, sostituendo la formula trovata per k nell'espressione di $x = 4k$, otteniamo

$$x = 4k = 4(16 + 25h) = 64 + 100h \quad \forall k \in \mathbb{Z}$$

da cui selezioniamo l'unico valore compreso tra 0 e 99, che è $x_0 = 64$. Questo ci dice che $N := 87053214^{48301}$ — che è soluzione del sistema $\circledast$, per costruzione! — è congruente a 64 modulo 100: quindi *le ultime due cifre decimali di $N := 87053214^{48301}$ sono 64*.

[3] — Richiamiamo le definizioni. $G := \text{GL}_2(\mathbb{Z}_3)$ è il gruppo generale lineare delle matrici 2×2 invertibili a coefficienti in $\mathbb{Z}_3$ (con l'operazione di prodotto righe per colonne), e consideriamo $B \leq G$ e $H \subseteq B$ definiti da

$$B := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid c = 0 \right\}, \quad H := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid c = 0, a d = 1 \right\}$$

(a) Per dimostrare che $H \trianglelefteq B$ possiamo seguire due metodi.

Primo metodo: Il primo metodo consiste nel verificare direttamente che

— (a.1) $H \ni e_B$, dove e_B è l'elemento neutro del gruppo B , che è naturalmente la matrice identità $e_B = e_G = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Questo è chiaramente vero, perché $e_B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ con $a := 1 =: d$ e $b := 0 =: c$ è un elemento di H .

— (a.2) H è chiuso rispetto al prodotto, cioè per ogni $h_1, h_2 \in H$ si ha $h_1 h_2 \in H$. Per vederlo, sia $h_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$ e $h_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$: allora

$$h_1 h_2 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 \cdot a_2 + d_1 \cdot 0 & d_1 d_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix}$$

dove l'ultima matrice appartiene a H perché si ha $(a_1 a_2)(d_1 d_2) = a_1 d_1 \cdot a_2 d_2 = 1 \cdot 1 = 1$.

— (a.3) H è chiuso rispetto agli inversi, cioè per ogni $h \in H$ si ha $h^{-1} \in H$. Per vederlo, sia $h = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ e vediamo di capire come è fatta la matrice inversa h^{-1} .

Sappiamo già che esiste $h^{-1} \in B$, che possiamo scrivere nella forma $h^{-1} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$: per dimostrare che $h^{-1} \in H$ dobbiamo soltanto verificare che sia $a'd' = 1$. La condizione che h^{-1} sia inversa di h è $h h^{-1} = e_B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, che a conti fatti — sfruttando il calcolo già fatto prima per il prodotto di due matrici! — esplicitamente diventa

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = h h^{-1} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} a a' & a b' + b d' \\ 0 & d d' \end{pmatrix}$$

quindi

$$\begin{cases} a a' = 1 \\ a b' + b d' = 0 \\ d d' = 1 \end{cases} \iff \begin{cases} a' = a^{-1} \\ b' = -a^{-1} b d^{-1} \\ d' = d^{-1} \end{cases} \iff h^{-1} = \begin{pmatrix} a^{-1} & -a^{-1} b d^{-1} \\ 0 & d^{-1} \end{pmatrix}$$

Si noti che la formula trovata per h^{-1} è valida in effetti per ogni $h \in B$. Quando poi sia $h \in H$, si ha che $a d = 1$ e quindi anche $a^{-1} d^{-1} = (a d)^{-1} = 1^{-1} = 1$, perciò è anche $h^{-1} \in H$, q.e.d. In aggiunta, in tal caso — cioè per $h \in H$ — la formula per h^{-1} prende la forma un po' più semplice $h^{-1} = \begin{pmatrix} a^{-1} & -b \\ 0 & d^{-1} \end{pmatrix}$.

Secondo metodo: Il secondo metodo consiste nel trovare un qualche morfismo di gruppi $\varphi : B \longrightarrow \Gamma$ di cui H sia il nucleo — cioè $\text{Ker}(\varphi) = H$: infatti sappiamo senz'altro che $\text{Ker}(\varphi) \trianglelefteq B$ e quindi il nostro obiettivo sarebbe raggiunto.

Consideriamo l'applicazione $\varphi : B \longrightarrow U(\mathbb{Z}_3) = \mathbb{Z}_3 \setminus \{0\}$ data da $\varphi \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} := a d$. Il calcolo diretto ci dà

$$\begin{aligned} \varphi \left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \right) &= \varphi \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix} := \\ &:= (a_1 a_2) (d_1 d_2) = \varphi \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \cdot \varphi \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \end{aligned}$$

cioè $\varphi \left(\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \right) = \varphi \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \cdot \varphi \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ per due qualsiasi elementi $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix} \in B$: dunque φ è un morfismo di gruppi. Il suo nucleo è

$$\begin{aligned} \text{Ker}(\varphi) &:= \varphi^{-1} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B \mid \varphi \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = 1 \right\} = \\ &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B \mid a d = 1 \right\} =: H \end{aligned}$$

dunque è proprio $H = \text{Ker}(\varphi)$ e quindi possiamo concludere che $H \trianglelefteq B$, q.e.d.

(b) Per dimostrare che H è ciclico e determinarne esplicitamente un generatore, cominciamo col calcolare l'ordine di H . Per definizione, H è l'insieme di tutte le matrici

della forma $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ con $a, b, d \in \mathbb{Z}_3$ e $ad = 1$, quindi anche $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$ con $a \in U(\mathbb{Z}_3)$, $b \in \mathbb{Z}_3$. Dunque H è in biiezione (ovvia) con l'insieme $U(\mathbb{Z}_3) \times \mathbb{Z}_3 = (\mathbb{Z}_3 \setminus \{0\}) \times \mathbb{Z}_3$, che ha esattamente $(3-1) \cdot 3 = 2 \cdot 3 = 6$ elementi. Pertanto il nostro obiettivo diventa trovare in H un elemento h_+ di ordine 6, cioè tale che $h_+^6 = e_B$ mentre $h_+^n \neq e_B$ per ogni $0 < n < 6$. Un tale elemento è, ad esempio, $h_+ = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$. Infatti, teniamo conto che l'ordine di h_+ è necessariamente un divisore dell'ordine di H , che è 6, quindi può essere soltanto 1, 2, 3 o 6. Chiaramente non è 1 perché l'ordine è 1 soltanto per l'elemento neutro e_B , e invece nel nostro caso abbiamo $h_+ \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e_B$. Per gli altri casi, il calcolo diretto ci dà

$$h_+^2 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \neq e_B, \quad h_+^3 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}^2 \cdot \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq e_B$$

per cui l'ordine di h_+ non è né 2 né 3; per esclusione quindi esso è necessariamente 6, q.e.d. Per inciso, si noti anche che da $h_+^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ segue anche immediatamente che $h_+^6 = (h_+^3)^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e_B$

(c) Dovendo descrivere esplicitamente il centro $Z(B)$ del gruppo B , cominciamo ricordando che $Z(B) := \{ \underline{\beta} \in B \mid \underline{\beta} \underline{b} = \underline{b} \underline{\beta} \ \forall \underline{b} \in B \}$. Scrivendo $\underline{\beta} = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$ e $\underline{b} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ la condizione perché $\underline{\beta}$ stia nel centro diventa

$$\begin{aligned} \underline{\beta} \underline{b} = \underline{b} \underline{\beta} &\iff \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \iff \\ &\iff \begin{pmatrix} \alpha a & \alpha b + \beta d \\ 0 & \delta d \end{pmatrix} = \begin{pmatrix} a \alpha & a \beta + b \delta \\ 0 & d \delta \end{pmatrix} \iff \\ &\iff \begin{cases} \alpha a = a \alpha \\ \alpha b + \beta d = a \beta + b \delta \\ \delta d = d \delta \end{cases} \iff \alpha b + \beta d = a \beta + b \delta \end{aligned}$$

Ora, siccome chiediamo $\underline{\beta} \underline{b} = \underline{b} \underline{\beta}$ per ogni $\underline{b} \in B$, la condizione $\alpha b + \beta d = a \beta + b \delta$ dev'essere valida per ogni $a, d \in U(\mathbb{Z}_3)$, $b \in \mathbb{Z}_3$; in particolare, per $a = d = b = 1$ la condizione diventa $\alpha + \beta = \beta + \delta$, dunque $\alpha = \delta$. Allora la condizione $\alpha b + \beta d = a \beta + b \delta$ diventa la condizione $\alpha b + \beta d = a \beta + b \alpha$ e quindi, semplificando, la condizione $\beta d = a \beta$. In particolare scegliendo $a = -1$ e $d = 1$ questa condizione diventa $\beta = -\beta$, che implica necessariamente $\beta = 0$. Così in conclusione abbiamo trovato che ogni elemento del centro è necessariamente della forma $\underline{\beta} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$. D'altra

parte, è immediato verificare che, viceversa, ogni elemento in B della forma $\underline{\beta} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$ sta in $Z(B)$. Pertanto $Z(B) = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \mid \alpha \in U(\mathbb{Z}_3) \right\} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$.

[4] — Per ipotesi, G è un gruppo, $K \leq G$ e $N \trianglelefteq G$. Procediamo dunque a risolvere i diversi quesiti del problema in esame.

(a) Dobbiamo dimostrare che $KN = NK$. Osserviamo che

$$KN := \{ kn \mid k \in K, n \in N \} = \bigcup_{k \in K} \{ kn \mid n \in N \} = \bigcup_{k \in K} kN$$

e analogamente

$$NK := \{ nk \mid k \in K, n \in N \} = \bigcup_{k \in K} \{ nk \mid n \in N \} = \bigcup_{k \in K} Nk.$$

Ora, per l'ipotesi di normalità abbiamo che $kN = Nk$ per ogni $k \in K$, e questo insieme alle due catene di identità precedenti ci permette di concludere che

$$KN = \bigcup_{k \in K} kN = \bigcup_{k \in K} Nk = NK$$

cioè esattamente $KN = NK$, q.e.d.

(b) Dobbiamo ora dimostrare che $KN \leq G$: questo corrisponde a provare che:

- (b.1) $KN \ni e_G$, cioè KN contiene l'elemento neutro di G ;
- (b.2) $KN \cdot KN \subseteq KN$, cioè KN è chiuso rispetto al prodotto (di G);
- (b.3) $(KN)^{-1} \subseteq KN$, cioè KN è chiuso rispetto agli inversi (in G).

Per (b.1) basta osservare che $e_G = e_G e_G \in KN$ in quanto $e_G \in K$ e $e_G \in N$ perché K e N sono entrambi sottogruppi (di G).

Per (b.2), si noti che $KN \cdot KN = K(NK)N = K(KN)N = (KK)(NN) \subseteq KN$ grazie al punto (a) e al fatto che $KK \subseteq K$ e $NN \subseteq N$ perché K e N sono entrambi sottogruppi (di G).

Per (b.3) infine basta osservare che per ogni $kn \in KN$ — con $k \in K$ e $n \in N$ — si ha $(kn)^{-1} = n^{-1}k^{-1} \in NK = KN$ perché K e N sono entrambi chiusi rispetto agli inversi — in quanto sottogruppi di G — e perché $NK = KN$ in virtù del punto (a).

(c) Dobbiamo dimostrare che $N \trianglelefteq KN$, cioè N è sottogruppo normale di KN . Che sia un sottogruppo è ovvio, perché KN e N sono entrambi sottogruppi di G e inoltre $N = e_G N \subseteq KN$. Che sia anche *normale* segue direttamente dal fatto che N sia normale in G . Infatti, quest'ultima proprietà significa che $gN = Ng$ per ogni $g \in G$, ma allora a maggior ragione si ha $g'N = Ng'$ per ogni $g' \in KN$, dato che $KN \subseteq G$.

(d) Dobbiamo dimostrare che $(K \cap N) \trianglelefteq K$, cioè $K \cap N$ è sottogruppo normale di K . Che $K \cap N$ sia un sottogruppo è ovvio, perché è intersezione dei due sottogruppi K e N , e in generale ogni intersezione di sottogruppi è a sua volta un sottogruppo. D'altrar parte, sapendo che N è sottogruppo *normale* in G sappiamo che $gNg^{-1} = N$ per ogni $g \in G$, quindi anche $kNk^{-1} = N$ per ogni $k \in K$; ma allora abbiamo anche $k(K \cap N)k^{-1} = (kKk^{-1}) \cap (kNk^{-1}) = K \cap N$ per ogni $k \in K$, quindi il sottogruppo $K \cap N$ è *normale* in K , q.e.d.

(e) Infine vogliamo trovare un isomorfismo da $K / (K \cap N)$ a $(KN) / N$. Considerando il fatto che il gruppo di partenza è un quoziente, cerchiamo di ottenere un tale isomorfismo $\Phi : K / (K \cap N) \longrightarrow (KN) / N$ come applicazione del *Teorema Fondamentale di Omomorfismo*, a partire da un morfismo $\phi : K \longrightarrow H$ con dominio il gruppo K , codominio un certo gruppo H da precisare, che abbia per nucleo

$\text{Ker}(\phi) = (K \cap N)$ e per immagine il gruppo $(KN)/N$ — così che il gruppo H deve contenere $(KN)/N$ come suo sottogruppo.

Sia $\phi := (\pi_N \circ j_K) : K \xrightarrow{j_K} KN \xrightarrow{\pi_N} (KN)/N$ la composizione dell'immersione naturale j_K di K in KN e della proiezione canonica π_N di KN sul suo quoziente modulo N : dato che j_K e π_N sono due morfismi, la loro composizione $\phi := (\pi_N \circ j_K)$ è a sua volta un morfismo. Di più, ϕ è chiaramente suriettivo (per costruzione), quindi è un epimorfismo. Pertanto il *Teorema Fondamentale di Omomorfismo* ci assicura l'esistenza di un isomorfismo di gruppi

$$\Phi := \phi_* : K/\text{Ker}(\phi) \longrightarrow \text{Im}(\phi) = (KN)/N, \quad \bar{k} \mapsto \phi_*(\bar{k}) := \phi(k) = \bar{k} \quad (6)$$

dove $\bar{k}$ sta per $\bar{k} := k \pmod{\text{Ker}(\phi)}$ a sinistra e per $\bar{k} := k \pmod{N} \in (KN)/N$ a destra. Ora, dalle definizioni otteniamo che

$$\begin{aligned} \text{Ker}(\phi) &:= \{ k \in K \mid \phi(k) = \bar{e}_G \} = \\ &= \{ k \in K \mid kN = \pi_N(k) = \pi_N(j_K(k)) = \phi(k) = \bar{e}_G = e_G N \} = \\ &= \{ k \in K \mid kN = e_G N \} = \{ k \in K \mid k \in N \} = K \cap N \end{aligned}$$

dunque in definitiva $\text{Ker}(\phi) = K \cap N$, così che (6) è in effetti un isomorfismo di gruppi da $K/\text{Ker}(\phi) = K/(K \cap N)$ a $(KN)/N$, q.e.d.

Si noti anche che avendo dimostrato che $\text{Ker}(\phi) = K \cap N$ ne segue anche — automaticamente! — che $(K \cap N) \trianglelefteq K$, così che simultaneamente resta dimostrato (in modo indipendente) anche il punto (d).

[5] — Nell'insieme delle parti $\mathbb{A}_E := \mathcal{P}(E)$ dell'insieme E fissiamo $E_0 \in \mathbb{A}_E$ e la relazione η_0 definita da

$$F' \eta_0 F'' \stackrel{\Delta}{\iff} F' \cap E_0 = F'' \cap E_0 \quad \forall F', F'' \in \mathbb{A}_E \quad (7)$$

Andiamo ora a risolvere i diversi quesiti.

(a) Dovendo dimostrare che la relazione η_0 è un'equivalenza — cioè è riflessiva, transitiva e simmetrica — possiamo farlo con un approccio diretto, tramite un'analisi pedissequa. In alternativa, seguiamo invece un metodo più astuto e molto più rapido.

Per cominciare, introduciamo l'applicazione

$$\phi : \mathcal{P}(E) \longrightarrow \mathcal{P}(E_0), \quad F \mapsto \phi(F) := F \cap E_0 \quad \forall F \in \mathcal{P}(E) \quad (8)$$

che è chiaramente suriettiva; la definizione di η_0 in (7) ci dà allora la caratterizzazione

$$F' \eta_0 F'' \iff \phi(F') = \phi(F'') \quad \forall F', F'' \in \mathbb{A}_E$$

Ma quest'ultima è esattamente la condizione che definisce la relazione ρ_ϕ canonicamente associata a ϕ , dunque $\eta_0 = \rho_\phi$. Per teoria generale sappiamo che per ogni possibile funzione f la relazione associata ρ_f è sempre una equivalenza: pertanto anche η_0 , visto che coincide con ρ_ϕ , è a sua volta una equivalenza. Resta così provato il punto (a).

(b) Dobbiamo dimostrare che la relazione η_0 è compatibile con ciascuna delle tre operazioni $\cup$, $\cap$ e Δ . Anche in questo caso, si può procedere mediante un approccio diretto; ma invece, in alternativa, adottiamo un metodo più astuto e più rapido.

Ricordiamo il seguente risultato generale: Se $\varphi : (\Gamma; *) \longrightarrow (\Omega; \star)$ è un qualsiasi morfismo tra gruppoidi, l'equivalenza ρ_φ ad esso associata in Γ è compatibile con l'operazione $*$ in Γ .

Vogliamo applicare questo risultato tre volte, precisamente alle tre coppie di gruppoidi date $\Gamma := \mathcal{P}(E)$ e $\Omega := \mathcal{P}(E_0)$ prendendo la prima volta $* := \cup =: \star$, la seconda $* := \cap =: \star$ e la terza $* := \Delta =: \star$; come morfismo invece prenderemo $\varphi := \phi$ in tutti e tre i casi. Perciò, dobbiamo soltanto dimostrare che l'applicazione ϕ in (8) è un morfismo (di gruppoidi) rispetto — separatamente — a ciascuna delle operazioni $\cup$, $\cap$ e Δ . Ora, i calcoli espliciti ci danno

$$\phi(F' \cup F'') := (F' \cup F'') \cap E_0 = (F' \cap E_0) \cup (F'' \cap E_0) =: \phi(F') \cup \phi(F'')$$

— sfruttando la distributività a sinistra di $\cap$ rispetto a $\cup$ — quindi ϕ è un morfismo rispetto all'operazione $\cup$; analogamente,

$$\begin{aligned} \phi(F' \cap F'') &:= (F' \cap F'') \cap E_0 = (F' \cap F'') \cap (E_0 \cap E_0) = F' \cap F'' \cap E_0 \cap E_0 = \\ &= F' \cap E_0 \cap F'' \cap E_0 = (F' \cap E_0) \cap (F'' \cap E_0) =: \phi(F') \cap \phi(F'') \end{aligned}$$

— sfruttando l'associatività, la commutatività e l'idempotenza di $\cap$ — quindi ϕ è un morfismo rispetto all'operazione $\cap$; infine

$$\phi(F' \Delta F'') := (F' \Delta F'') \cap E_0 = (F' \cap E_0) \Delta (F'' \cap E_0) =: \phi(F') \Delta \phi(F'')$$

— sfruttando la distributività a sinistra di $\cap$ rispetto a Δ — quindi ϕ è un morfismo anche rispetto all'operazione Δ , q.e.d. Il punto (b) è così risolto.

(c) Ricordiamo che, per ogni $F \in \mathbb{A}_E := \mathcal{P}(E)$, la classe di η_0 -equivalenza $[F]_{\eta_0}$ è il sottoinsieme di $\mathcal{P}(E)$ definito da $[F]_{\eta_0} := \{ F' \in \mathcal{P}(E) \mid F' \eta_0 F \}$. Esso sarà chiuso per le due operazioni $\cup$ e $\cap$ se

$$(F' \cup F'') \in [F]_{\eta_0}, \quad (F' \cap F'') \in [F]_{\eta_0} \quad \forall F', F'' \in [F]_{\eta_0} \quad (9)$$

Per dimostrare la (9), osserviamo che dal punto (b) sappiamo che η_0 è compatibile con $\cup$ e con $\cap$; ma allora i calcoli diretti ci danno

$$\begin{aligned} F', F'' \in [F]_{\eta_0} &\implies F' \eta_0 F, F'' \eta_0 F \implies (F' \cup F'') \eta_0 (F \cup F) = F \implies \\ &\implies (F' \cup F'') \eta_0 F \implies (F' \cup F'') \in [F]_{\eta_0} \\ F', F'' \in [F]_{\eta_0} &\implies F' \eta_0 F, F'' \eta_0 F \implies (F' \cap F'') \eta_0 (F \cap F) = F \implies \\ &\implies (F' \cap F'') \eta_0 F \implies (F' \cap F'') \in [F]_{\eta_0} \end{aligned}$$

— dove sfruttiamo le due identità cruciali $F \cup F = F$ e $F \cap F = F$ — cioè appunto $(F' \cup F'') \in [F]_{\eta_0}$ e $(F' \cap F'') \in [F]_{\eta_0}$, q.e.d.

(d) Procedendo come per il punto (c) qui sopra, il nostro obiettivo è dimostrare che

$$(F' \Delta F'') \in [F]_{\eta_0} \quad \forall F', F'' \in [F]_{\eta_0} \quad \iff [F]_{\eta_0} = [\emptyset]_{\eta_0} \quad (10)$$

A tal fine, i calcoli ci danno

$$F', F'' \in [F]_{\eta_0} \implies F' \eta_0 F, F'' \eta_0 F \implies (F' \Delta F'') \eta_0 (F \Delta F) = \emptyset \implies \\ \implies (F' \Delta F'') \eta_0 \emptyset \implies (F' \Delta F'') \in [\emptyset]_{\eta_0}$$

— dove sfruttiamo l'identità cruciale $F \Delta F = \emptyset$ — e quindi troviamo che

$$(F' \Delta F'') \in [\emptyset]_{\eta_0} \quad \forall F', F'' \in [F]_{\eta_0}$$

e quindi abbiamo $(F' \Delta F'') \in [F]_{\eta_0}$ — per ogni $F', F'' \in [F]_{\eta_0}$ — se e soltanto se si ha $[F]_{\eta_0} = [\emptyset]_{\eta_0}$, cioè vale la (10), q.e.d.

Un *metodo alternativo* per risolvere il presente quesito (d) può essere il seguente.

Ricordiamo che l'insieme $\mathbb{A}_E := \mathcal{P}(E)$ rispetto alla operazione Δ è un gruppo (abeliano), il cui elemento neutro (lo “zero”) è $\emptyset$. Siccome la relazione η_0 è compatibile con l'operazione Δ , abbiamo subito (per un risultato generale) che la classe di η_0 –equivalenza dell'elemento neutro, cioè $[\emptyset]_{\eta_0}$, è un sottogruppo normale del gruppo $(\mathcal{P}(E); \Delta)$ — di fatti, è il sottogruppo normale associato alla congruenza (=equivalenza compatibile) η_0 nel gruppo $(\mathcal{P}(E); \Delta)$ (in effetti, ancor di più, η_0 è una congruenza nell'anello $(\mathcal{P}(E); \Delta, \cap)$, e perciò $[\emptyset]_{\eta_0}$ è un ideale in $(\mathcal{P}(E); \Delta, \cap)$; ciò sarà utile per il punto (e) qui avanti). In particolare $[\emptyset]_{\eta_0}$, come sottogruppo rispetto all'operazione Δ , è chiuso per Δ , q.e.d.

(e) Prendendo in $\mathbb{A}_E := \mathcal{P}(E)$ la struttura di anello con Δ come “somma” e $\cap$ come “prodotto”, dobbiamo dimostrare l'esistenza di un isomorfismo dall'anello quoziente $\mathbb{A}_E / \eta_0 = \mathcal{P}(E) / \eta_0$ all'anello $(\mathcal{P}(E_0); \Delta, \cap)$. Si noti che $\mathcal{P}(E) / \eta_0$ ha effettivamente la struttura canonica di anello quoziente perché l'equivalenza η_0 nell'anello $(\mathcal{P}(E); \Delta, \cap)$ è compatibile con entrambe le operazioni Δ e $\cap$, come già affermato al punto (b). Osserviamo anche che l'ideale di $\mathcal{P}(E)$ associato a η_0 è la classe $[\emptyset]_{\eta_0}$, quindi possiamo anche scrivere $\mathcal{P}(E) / \eta_0 = \mathcal{P}(E) / [\emptyset]_{\eta_0}$.

Visto che $\mathcal{P}(E) / \eta_0 = \mathcal{P}(E) / [\emptyset]_{\eta_0}$ è un anello quoziente, cerchiamo un isomorfismo $\Phi : \mathcal{P}(E) / [\emptyset]_{\eta_0} \hookrightarrow \mathcal{P}(E_0)$ ottenuto tramite il *Teorema Fondamentale di Omomorfismo (per Anelli)* nella forma $\Phi := \varphi_*$ dove $\varphi : \mathcal{P}(E) \twoheadrightarrow \mathcal{P}(E_0)$ sia un epimorfismo di anelli tale che $\text{Ker}(\varphi) = [\emptyset]_{\eta_0}$. Ora, se prendiamo $\varphi := \phi$ come in (8) sappiamo già — perché è stato dimostrato al punto (b) — che esso rispetta le operazioni Δ e $\cap$, dunque è morfismo di anelli, e inoltre è suriettivo, quindi è un epimorfismo. Calcoliamone ora il nucleo. L'elemento neutro dell'anello $(\mathcal{P}(E_0); \Delta, \cap)$ rispetto alla “somma” Δ — cioè lo “zero” di tale anello — è $\emptyset$, perciò $\text{Ker}(\varphi) = \text{Ker}(\phi) := \phi^{-1}(\emptyset)$. Ma per definizione è

$$\text{Ker}(\varphi) = \text{Ker}(\phi) := \phi^{-1}(\emptyset) = \{ F \in \mathcal{P}(E) \mid \phi(F) = \emptyset = \phi(\emptyset) \} = \\ = \{ F \in \mathcal{P}(E) \mid F \eta_0 \emptyset \} = [\emptyset]_{\eta_0}$$

dunque $\text{Ker}(\varphi) = [\emptyset]_{\eta_0}$, q.e.d. Così l'epimorfismo di anelli $\varphi := \phi : \mathcal{P}(E) \twoheadrightarrow \mathcal{P}(E_0)$ induce, tramite il *Teorema Fondamentale di Omomorfismo (per Anelli)*, un isomorfismo di anelli $\Phi := \varphi_* : \mathcal{P}(E) / [\emptyset]_{\eta_0} \hookrightarrow \mathcal{P}(E_0)$ definito esplicitamente dalla formula $\Phi(F \Delta [\emptyset]_{\eta_0}) = \Phi([F]_{\eta_0}) := \varphi(F)$ per ogni classe in $\mathcal{P}(E) / [\emptyset]_{\eta_0} = \mathcal{P}(E) / \eta_0$ — descritta come classe laterale $F \Delta [\emptyset]_{\eta_0}$ se penso al quoziente come $\mathcal{P}(E) / [\emptyset]_{\eta_0}$, e come classe di η_0 –equivalenza $[F]_{\eta_0}$ se penso al quoziente come $\mathcal{P}(E) / \eta_0$.

[6] — Nel dominio $\mathbb{Z}[\sqrt{-15}]$ consideriamo la funzione $v : \mathbb{Z}[\sqrt{-15}] \longrightarrow \mathbb{N}$ data da $v(\zeta) = v(a + b\sqrt{-15}) = a^2 + 15b^2$ per ogni $\zeta = a + b\sqrt{-15}$ ($\in \mathbb{Z}[\sqrt{-15}]$).

Osserviamo subito che la funzione $v : \mathbb{Z}[\sqrt{-15}] \longrightarrow \mathbb{N}$ è *moltiplicativa*, cioè è un morfismo dal gruppoide $(\mathbb{Z}[\sqrt{-15}]; \cdot)$ al gruppoide $(\mathbb{N}; \cdot)$; questo si verifica facilmente tramite un calcolo diretto, oppure osservando che v coincide con la restrizione $\mathbb{Z}[\sqrt{-15}]$ della funzione “norma” per numeri complessi — data da $N(\zeta) := \zeta \bar{\zeta}$ per ogni $\zeta \in \mathbb{C}$ — la quale come noto è moltiplicativa. In aggiunta, la funzione v permette di caratterizzare l'insieme $U(\mathbb{Z}[\sqrt{-15}]) := \{\varepsilon \in \mathbb{Z}[\sqrt{-15}] \mid \exists \eta \in \mathbb{Z}[\sqrt{-15}] : \varepsilon \eta = 1\}$ degli elementi invertibili (rispetto al prodotto) in $\mathbb{Z}[\sqrt{-15}]$ come segue:

$$U(\mathbb{Z}[\sqrt{-15}]) = \{\varepsilon \in \mathbb{Z}[\sqrt{-15}] \mid v(\varepsilon) = 1\} = \{+1, -1\} \quad (11)$$

Infatti, la seconda identità in (11) è ovvia; la prima invece segue dal procedimento seguente:

$$\begin{aligned} \varepsilon \in U(\mathbb{Z}[\sqrt{-15}]) &\implies \exists \eta \in \mathbb{Z}[\sqrt{-15}] : \varepsilon \eta = 1 \implies \\ &\implies v(\varepsilon) v(\eta) \stackrel{*}{=} v(\varepsilon \eta) = v(1) = 1 \implies v(\varepsilon) v(\eta) = 1 \implies \\ &\implies v(\varepsilon) \in U(\mathbb{Z}) \cap \mathbb{N} = \{+1, -1\} \cap \mathbb{N} = \{+1\} \implies v(\varepsilon) = 1 \end{aligned}$$

ci dà l'inclusione $U(\mathbb{Z}[\sqrt{-15}]) \subseteq \{\varepsilon \in \mathbb{Z}[\sqrt{-15}] \mid v(\varepsilon) = 1\} = \{+1, -1\}$, mentre l'inclusione inversa $U(\mathbb{Z}[\sqrt{-15}]) \supseteq \{+1, -1\} = \{\varepsilon \in \mathbb{Z}[\sqrt{-15}] \mid v(\varepsilon) = 1\}$ è ovvia.

(a) Per dimostrare che $\mathbb{Z}[\sqrt{-15}]$ è un dominio a fattorizzazione, dobbiamo dimostrare che ogni elemento $\zeta \in \mathbb{Z}[\sqrt{-15}]$ o è nullo — cioè è 0 — o è invertibile — cioè è +1 oppure -1 — o è un prodotto di fattori irriducibili. A tal fine, procediamo per induzione su $v(\zeta)$.

La *Base dell'Induzione* è data dal caso $v(\zeta) = 0$. Da questo segue necessariamente che $\zeta = 0$, e quindi la tesi è dimostrata. Dopo di questo potremmo passare direttamente al caso generale, però invece analizziamo esplicitamente il caso successivo, cioè quando $v(\zeta) = 1$, che è comunque istruttivo. Infatti, in tal caso abbiamo subito $\zeta \in U(\mathbb{Z}[\sqrt{-15}])$ per via della (11), e di nuovo la tesi è dimostrata.

Il *Passo Induttivo* si effettua così: per ogni $n \in \mathbb{N}_+$, assumiamo — è l'*Ipotesi Induttiva* — che la tesi sia vera per ogni $\lambda \in \mathbb{Z}[\sqrt{-15}]$ tale che $v(\lambda) \leq n$, e dimostriamo — questa è la *Tesi Induttiva* — che la tesi è vera anche per ogni $\eta \in \mathbb{Z}[\sqrt{-15}]$ tale che $v(\eta) = n$.

Sia dunque $\eta \in \mathbb{Z}[\sqrt{-15}]$ tale che $v(\eta) = n$. Nel caso in cui η sia *irriducibile*, la tesi è già dimostrata, in quanto η è prodotto di un unico fattore irriducibile (sé stesso!). In caso contrario, η è *riducibile*, dunque ammette una fattorizzazione non banale $\eta = \sigma \tau$ con $\sigma, \tau \in \mathbb{Z}[\sqrt{-15}]$ e $\sigma, \tau \notin U(\mathbb{Z}[\sqrt{-15}])$ in quanto la fattorizzazione è non banale. Allora abbiamo anche $v(\eta) = v(\sigma \tau) = v(\sigma) v(\tau)$ per la moltiplicatività della funzione v , con $v(\sigma), v(\tau) \neq 1$ perché $\sigma, \tau \notin U(\mathbb{Z}[\sqrt{-15}]) = \{+1, -1\}$ per via della (11). Ma adesso le condizioni $v(\sigma), v(\tau) \in \mathbb{N}_+$, $v(\sigma) v(\tau) = v(\eta) = n$ e $v(\sigma), v(\tau) \neq 1$ implicano anche $v(\sigma) \leq n$, $v(\tau) \leq n$. Quindi per *ipotesi induttiva* abbiamo che σ e τ sono entrambi prodotti (non banali, cioè con almeno un fattore, perché σ e τ non sono invertibili, per costruzione!) di fattori irriducibili: scrivendo $\sigma = p_1 p_2 \cdots p_h$ e $\tau = q_1 q_2 \cdots q_k$ con i p_i e i q_j irriducibili abbiamo allora $\eta = \sigma \tau = p_1 p_2 \cdots p_h q_1 q_2 \cdots q_k$ con i fattori p_i e i q_j irriducibili. Quindi la tesi vale anche per η , q.e.d.

(b) Per dimostrare che *non* esiste $\zeta \in \mathbb{Z}[\sqrt{-15}]$ tale che $v(\zeta) = 2$ oppure $v(\zeta) = 8$, procediamo per assurdo. Per cominciare, sia $\zeta \in \mathbb{Z}[\sqrt{-15}]$ tale che $v(\zeta) = 2$. Scrivendo esplicitamente $\zeta = a + b\sqrt{-15}$ con $a, b \in \mathbb{Z}$ la condizione $v(\zeta) = 2$ diventa $a^2 + 15b^2 = 2$, che è impossibile, perché non esistono $a, b \in \mathbb{Z}$ tali che $a^2 + 15b^2 = 2$. Analogamente, se $\zeta \in \mathbb{Z}[\sqrt{-15}]$ fosse tale che $v(\zeta) = 8$, scrivendo esplicitamente $\zeta = a + b\sqrt{-15}$ con $a, b \in \mathbb{Z}$ la condizione $v(\zeta) = 8$ darebbe $a^2 + 15b^2 = 8$, che di nuovo è impossibile, perché non esistono $a, b \in \mathbb{Z}$ tali che $a^2 + 15b^2 = 8$.

(c) Per dimostrare che $\mathbb{Z}[\sqrt{-15}]$ *non* è un dominio a fattorizzazione unica, ci basta trovare un elemento non nullo e non invertibile in $\mathbb{Z}[\sqrt{-15}]$ che abbia due fattorizzazioni in irriducibili non equivalenti. A tal fine, consideriamo l'elemento $16 \in \mathbb{Z}[\sqrt{-15}]$, che non è nullo né invertibile, e osserviamo che ammette le due fattorizzazioni $16 = 2 \cdot 2 \cdot 2 \cdot 2$ — con quattro fattori coincidenti — e $16 = (1 + \sqrt{-15}) \cdot (1 - \sqrt{-15})$ — con due fattori distinti, e non associati. Osserviamo ora che i fattori 2 , $(1 + \sqrt{-15})$ e $(1 - \sqrt{-15})$ sono tutti e tre irriducibili, perché dimostriamo che ogni loro fattorizzazione è necessariamente banale (cioè ha un fattore invertibile e l'altro associato all'elemento da fattorizzare): infatti,

$$\begin{aligned} 2 = \alpha\beta &\implies 4 = v(2) = v(\alpha\beta) = v(\alpha)v(\beta) \implies \\ &\implies (v(\alpha), v(\beta)) \in \{(1, 4), (4, 1), (2, 2)\} \implies (v(\alpha), v(\beta)) \in \{(1, 4), (4, 1)\} \implies \\ &\implies v(\alpha) = 1 \text{ oppure } v(\beta) = 1 \implies \alpha \in U(\mathbb{Z}[\sqrt{-15}]) \text{ oppure } \beta \in U(\mathbb{Z}[\sqrt{-15}]) \end{aligned}$$

— perché $4 = 2 \cdot 2$ è la fattorizzazione in primi di 4 in $\mathbb{N}_+$ e perché sappiamo dal punto (b) che *non può essere* $(v(\alpha), v(\beta)) = (2, 2)$ — e quindi la fattorizzazione $2 = \alpha\beta$, avendo un fattore invertibile, è banale. Analogamente abbiamo

$$\begin{aligned} (1 + \sqrt{-15}) = \gamma\delta &\implies 16 = v(1 + \sqrt{-15}) = v(\gamma\delta) = v(\gamma)v(\delta) \implies \\ &\implies (v(\gamma), v(\delta)) \in \{(1, 16), (16, 1), (2, 8), (8, 2), (4, 4)\} \implies \\ &\implies (v(\gamma), v(\delta)) \in \{(1, 16), (16, 1), (4, 4)\} \implies \\ &\implies v(\gamma) = 1 \text{ oppure } v(\delta) = 1 \text{ oppure } v(\gamma) = 4 = v(\delta) \implies \\ &\implies \gamma \in U(\mathbb{Z}[\sqrt{-15}]) \text{ oppure } \delta \in U(\mathbb{Z}[\sqrt{-15}]) \text{ oppure } v(\gamma) = 4 = v(\delta) \end{aligned}$$

— perché sappiamo dal punto (b) che $v(\gamma)$ e $v(\delta)$ *non possono essere né 2 né 8*; inoltre, è immediato verificare che $v(\gamma) = 4 = v(\delta) \iff \gamma, \delta \in \{+2, -2\}$, il che è incompatibile con $(1 + \sqrt{-15}) = \gamma\delta$ perché $(\pm 2) \cdot (\pm 2) = \pm 4 \neq (1 + \sqrt{-15})$. Pertanto uno dei due fattori γ e δ è necessariamente invertibile, e quindi la fattorizzazione $(1 + \sqrt{-15}) = \gamma\delta$ è banale. Infine, abbiamo anche

$$(1 - \sqrt{-15}) = \eta\theta \implies 16 = v(1 - \sqrt{-15}) = v(\eta\theta) = v(\eta)v(\theta)$$

da cui gli stessi passaggi di prima implicano che uno tra η e θ deve essere invertibile, per cui la fattorizzazione $(1 - \sqrt{-15}) = \eta\theta$ è banale.

In conclusione, abbiamo *due fattorizzazioni in irriducibili* $16 = 2 \cdot 2 \cdot 2 \cdot 2$ e $16 = (1 + \sqrt{-15}) \cdot (1 - \sqrt{-15})$ per uno stesso elemento *che sono non equivalenti* — basta osservare che hanno un diverso numero di fattori irriducibili: quattro la prima, due la seconda! — e pertanto $\mathbb{Z}[\sqrt{-15}]$ *non è dominio a fattorizzazione unica*, q.e.d.