CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2018–2019

Esame scritto del 9 Luglio 2019 — Sessione Estiva, II appello

Testo & Svolgimento

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

[1] — Sia $\eta \subseteq \mathbb{Z} \times \mathbb{Z}$ la relazione (binaria) in $\mathbb{Z}$ definita da

$$a \,\eta\, b \iff 2\,a^2 + 11\,b - 9 \equiv 2\,a - 7\,b^2 + 18 \pmod 9 \qquad \forall\ a\,,\, b \in \mathbb{Z}$$

(a) Dimostrare che la relazione η è un'equivalenza in $\mathbb{Z}$.

(b) Descrivere esplicitamente la classe di η–equivalenza $\big[-2\big]_\eta$.

[2] — Determinare tutti i valori di $z \in \mathbb{Z}$ che soddisfino simultaneamente le seguenti tre condizioni

$$\begin{aligned} \big[-26\big]_{14} \cdot \big[z\big]_{14} &= \big[16\big]_{14} \qquad \text{in } \mathbb{Z}_{14} \\ \big[33\big]_{30} \cdot \big[z\big]_{30} &= -\big[57\big]_{30} \qquad \text{in } \mathbb{Z}_{30} \\ \big[50\big]_{18} \cdot \big[z\big]_{18} &= \big[44\big]_{18} \qquad \text{in } \mathbb{Z}_{18} \end{aligned}$$

[3] — Sia E un insieme, e sia $\mathcal{S}(E)$ l'insieme di tutte le permutazioni di E in sé stesso, che è un gruppo rispetto all'operazione di composizione. Dato un sottoinsieme $F \big(\subseteq E\big)$ non vuoto di E, consideriamo i sottoinsiemi di $\mathcal{S}(E)$

$$G_F := \big\{\, \gamma \in \mathcal{S}(E) \,\big|\, \gamma(F) = F \,\big\} \quad , \qquad G_{(F)} := \big\{\, \gamma \in \mathcal{S}(E) \,\big|\, \gamma(f) = f\,,\ \forall\ f \in F \,\big\}$$

Dimostrare che:

(a) G_F è sottogruppo di $\big(\mathcal{S}(E)\,;\circ\big)$;

(b) $G_{(F)}$ è sottogruppo di $\big(\mathcal{S}(E)\,;\circ\big)$;

(c) $G_{(F)}$ è sottogruppo normale di G_F;

(d) $G_{(F)}$ è sottogruppo normale di $\big(\mathcal{S}(E)\,;\circ\big) \iff \big|E \setminus F\big| < 2$;

(e) il gruppo quoziente $G_F \Big/ G_{(F)}$ è isomorfo al gruppo $\big(\mathcal{S}(F)\,;\circ\big)$ di tutte le permutazioni dell'insieme F in sé stesso.

[4] — Determinare tutti i valori di $x \in \mathbb{Z}$ tali che

$$63224^{\,347} \cdot x \;\equiv\; -308 \pmod{21} \qquad \& \qquad -5 \leqslant x \leqslant +7$$

[5] — Sia $\mathbb{Z}\big[\sqrt{-8}\,\big] := \big\{\, a + b\sqrt{-8} \,\big|\, a, b \in \mathbb{Z} \,\big\}$ $\big(\subseteq \mathbb{C}\big)$.

(a) Dimostrare che $\mathbb{Z}\big[\sqrt{-8}\,\big]$ è un sottoanello di $\mathbb{C}$.

(b) Dimostrare che nell'anello $\mathbb{Z}\big[\sqrt{-8}\,\big]$ per ogni elemento non nullo e non invertibile esiste (almeno) una fattorizzazione come prodotto di elementi irriducibili.

(c) Dimostrare che nell'anello $\mathbb{Z}\big[\sqrt{-8}\,\big]$ esiste almeno un elemento non nullo e non invertibile che ha almeno due fattorizzazioni tra loro non equivalenti come prodotto di elementi irriducibili.

[6] — Dati $n\,, k \in \mathbb{N}$, indichiamo con $\mathbb{P}_k(n)$ il numero dei sottoinsiemi con k elementi in un insieme che abbia esattamente n elementi (*N.B.:* tale numero è indipendente dalla scelta di uno specifico insieme di n elementi). Dimostrare che

$$\mathbb{P}_3(\ell + t) \;=\; \mathbb{P}_3(\ell) \,+\, \mathbb{P}_2(\ell)\, t \,+\, \ell\, \mathbb{P}_2(t) \,+\, \mathbb{P}_3(t) \qquad\qquad \forall\;\; \ell\,, t \in \mathbb{N}\,.$$

— ⋆ —

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] — Affrontiamo separatamente i due quesiti proposti.

(a) Ricordiamo che una relazione binaria ρ in un insieme X è un'equivalenza se e solanto se è della forma $\rho = \rho_f$ dove $f : X \longrightarrow Y$ è un'applicazione e ρ_f è la relazione definita in X da $x' \,\rho_f\, x'' \iff f(a') = f(x'')$. Memori di questo, cerchiamo di riconoscere che la relazione in esame η è appunto della forma $\eta = \rho_f$ per un'opportuna applicazione $f : \mathbb{Z} \longrightarrow Y$. In particolare, la condizione $\eta = \rho_f$ si riscrive nella forma

$$a\,\eta\,b \iff a\,\rho_f\,b \iff f(a) = f(b) \qquad\qquad \forall\;\; a\,, b \in \mathbb{Z}$$

che significa che dobbiamo poter caratterizzare la relazione η con una condizione in cui siano "le variabili a e b siano separate". Con quest'idea a guidarci, osserviamo ora che per ogni $a\,,\,b \in \mathbb{Z}$ si ha

$$\begin{aligned} a\,\eta\,b \iff 2\,a^2 + 11\,b - 9 \equiv 2\,a - 7\,b^2 + 18 \pmod 9 \iff \\ \iff 2\,a^2 - 2\,a - 9 \equiv -7\,b^2 - 11\,b + 18 \pmod 9 \end{aligned}$$

dove nell'ultima espressione abbiamo effettivamente ottenuto una "separazione di variabili" (la a a sinistra e la b a destra). Ora, quest'ultima condizione andrebbe riscritta in forma $f(a) = f(b)$ dove f sia una stessa espressione che definisce un'opportuna funzione con dominio $\mathbb{Z}$; con questo obiettivo continuiamo la nostra elaborazione e troviamo (per ogni $a\,,\,b \in \mathbb{Z}$)

$$\begin{aligned} & a\,\eta\,b \iff 2\,a^2 - 2\,a - 9 \equiv -7\,b^2 - 11\,b + 18 \pmod 9 \iff \\ & \iff \overline{2}\,\overline{a}^{\,2} + \overline{2}\,\overline{a} - \overline{9} = -\overline{7}\,\overline{b}^{\,2} - \overline{11}\,\overline{b} + \overline{18} \ \big(\in \mathbb{Z}_9\big) \iff \overline{2}\,\overline{a}^{\,2} + \overline{2}\,\overline{a} = \overline{2}\,\overline{b}^{\,2} - \overline{2}\,\overline{b} \ \big(\in \mathbb{Z}_9\big) \iff \\ & \iff f\big(\overline{a}\,\big) = f\big(\overline{b}\,\big) \ \big(\in \mathbb{Z}_9\big) \end{aligned}$$

dove nella seconda riga (e a seguire) indichiamo con $\overline{z} \in \mathbb{Z}_9$ la classe di congruenza modulo 9 di un intero $z \in \mathbb{Z}$ e abbiamo sfruttato alcune ovvie identità in $\mathbb{Z}_9$ — precisamente $-\overline{7} = \overline{2}$, $-\overline{11} = -\overline{2}$ e $-\overline{9} = \overline{0} = \overline{18}$ — mentre nella terza riga f indica la funzione

$$f : \mathbb{Z} \longrightarrow Z_9 \ , \quad z \mapsto f(z) := \overline{2}\,\overline{x}^{\,2} - \overline{2}\,\overline{x} \qquad \big(\forall\, z \in \mathbb{Z}\big) \tag{1}$$

In conclusione quindi abbiamo $\eta = \rho_f$ per l'applicazione f definita in (1), e pertanto la relazione η è una equivalenza, q.e.d.

Naturalmente si può anche dimostrare *direttamente* che η è un'equivalenza provando che è riflessiva, transitiva e simmetrica: questo si fa tramite verifiche dirette, che richiedono calcoli e considerazioni — come l'uso di certe identità in $\mathbb{Z}_9$ — che in definitiva sono del tutto analoghe a quelle già considerate con il metodo che abbiamo illustrato qui sopra.

(b) Ricordiamo che per una equivalenza η in un insieme E la classe di η–equivalenza di un elemento $e \in E$ è il sottoinsieme $[\,e\,]_\eta$ di E definito da

$$[\,e\,]_\eta := \big\{\, e' \in E \,\big|\, e'\eta\, e \,\big\}$$

Quando poi l'equivalenza η è realizzata come $\eta = \rho_f$ per una certa applicazione $f : E \longrightarrow H$ (riprendendo la notazione usata al punto *(a)*), le definizioni stesse ci danno

$$e' \in [\,e\,]_\eta \iff e' \in [\,e\,]_{\rho_f} \iff e'\rho_f\, e \iff f(e') = f(e) \iff e' \in f^{-1}\big(f(e)\big)$$

da cui otteniamo

$$[\,e\,]_\eta := f^{-1}\big(f(e)\big) \tag{2}$$

Applicando tutto questo al caso di $E := \mathbb{Z}$, $e := -2$ e $\eta = \rho_f$ con la f come in (1) troviamo

$$\begin{aligned} [\,-2\,]_\eta &= f^{-1}\big(f(-2)\big) = f^{-1}\big(\overline{3}\,\big) = \big\{\, x \in \mathbb{Z} \,\big|\, f\big(\overline{x}\,\big) = \overline{3}\,\big\} = \\ &= \big\{\, x \in \mathbb{Z} \,\big|\, \overline{2}\,\overline{x}^{\,2} - \overline{2}\,\overline{x} = \overline{3}\,\big\} = \big\{\, x \in \mathbb{Z} \,\big|\, \overline{2}\,\overline{x}^{\,2} - \overline{2}\,\overline{x} - \overline{3} = \overline{0}\,\big\} \end{aligned} \tag{3}$$

così che $[\,-2\,]_\eta$ si rivela essere l'insieme di tutti e soli gli interi $z \in \mathbb{Z}$ la cui classe $\overline{z} \in \mathbb{Z}_9$ sia una delle radici del polinomio $P(\,\overline{x}\,) = \overline{2}\,\overline{x}^{\,2} - \overline{2}\,\overline{x} - \overline{3}$. Per quest'ultimo polinomio, scritto nella forma $P(\,\overline{x}\,) = a\,\overline{x}^{\,2} + b\,\overline{x} + c$, possiamo trovare le radici tramite la "formula ridotta"

$$\overline{x}_\pm \;=\; \Big(-\,b/2 \pm \sqrt{\big(-\,b/2\big)^2 - a\,c}\,\Big) \Big/ a$$

che ci dà — essendo $a = \overline{2}$, $b = -\overline{2}$, $a = -\overline{3}$ — esplicitamente

$$\overline{x}_\pm \;=\; \Big(\overline{1} \pm \sqrt{\overline{1}^{\,2} + \overline{2}\cdot\overline{3}}\,\Big)\cdot\overline{2}^{\,-1} \;=\; \Big(\overline{1} \pm \sqrt{\overline{1} + \overline{6}}\,\Big)\cdot\overline{5} \;=\; \Big(\overline{1} \pm \sqrt{\overline{7}}\,\Big)\cdot\overline{5} \;=$$

$$= \Big(\overline{1} \pm \sqrt{\overline{16}}\,\Big)\cdot\overline{5} \;=\; \big(\overline{1} \pm \overline{4}\big)\cdot\overline{5} \;=\; \begin{cases} \overline{5}\cdot\overline{5} \;=\; \overline{25} \;=\; \overline{7} \\ -\overline{3}\cdot\overline{5} \;=\; -\overline{15} \;=\; \overline{3} \end{cases}$$

cioè $\overline{x}_+ = \overline{7}$ e $\overline{x}_- = \overline{3}$. Da questo e dall'analisi precedente — in particolare dalla (3) — concludiamo allora che

$$[\,-2\,]_\eta \;=\; \big\{\, x \in \mathbb{Z} \;\big|\; \overline{x} \in \{\overline{7}, \overline{3}\}\,\big\} \;=\; \big\{\, x \in \mathbb{Z} \;\big|\; x \in \big(\overline{7} \cup \overline{3}\,\big)\,\big\} \;=$$

$$= \overline{7} \cup \overline{3} \;=\; \big(7 + 9\,\mathbb{Z}\big) \cup \big(3 + 9\,\mathbb{Z}\big)$$

cioè in sintesi $[\,-2\,]_\eta \;=\; \big(7 + 9\,\mathbb{Z}\big) \cup \big(3 + 9\,\mathbb{Z}\big)$.

Come osservazione finale, si noti che a priori sappiamo senz'altro che $[\,-2\,]_\eta \ni -2$, perché in ogni caso la classe di equivalenza di un elemento contiene l'elemento stesso; rispetto alla descrizione di $[\,-2\,]_\eta$ appena trovata, riconosciamo che -2 è elemento dell'insieme $[\,-2\,]_\eta \;=\; \big(7 + 9\,\mathbb{Z}\big) \cup \big(3 + 9\,\mathbb{Z}\big)$ in quanto

$$-2 = 7 + 9\cdot(-1) \;\in\; \big(7 + 9\,\mathbb{Z}\big) \;\subseteq\; \big(7 + 9\,\mathbb{Z}\big) \cup \big(3 + 9\,\mathbb{Z}\big) \;=\; [\,-2\,]_\eta$$

[2] — Ricordiamo che ogni equazione modulare — in $\mathbb{Z}_n$ — corrsiponde (biiettivamente) ad una ben precisa equazione congruenziale — modulo n , in $\mathbb{Z}$: precisamente, abbiamo

$$[\,a\,]_n \cdot [\,x\,]_n = [\,b\,]_n \quad \text{in } \mathbb{Z}_n \quad\Longleftrightarrow\quad a \cdot x \equiv b \pmod{n} \quad \text{in } \mathbb{Z}$$

Applicando questa osservazione alle tre equazioni modulari considerate nel problema in esame, troviamo che quest'ultimo equivale al problema di risolvere il seguente sistema di equazioni congruenziali in $\mathbb{Z}$:

$$\circledast \;:\; \begin{cases} -26\,x \;\equiv\; 16 \pmod{14} \\ \;\;\,33\,x \;\equiv\; -57 \pmod{30} \\ \;\;\,50\,x \;\equiv\; 44 \pmod{18} \end{cases} \tag{4}$$

Procediamo quindi a risolvere il sistema in (4). Operando semplificazioni dei coefficienti, dei termini noti e (quando necessario) dei moduli, in prima battuta il sistema

assegnato si trasforma come segue:

$$\circledast : \begin{cases} -26\,x \equiv 16 \pmod{14} \\ 33\,x \equiv -57 \pmod{30} \\ 50\,x \equiv 44 \pmod{18} \end{cases} \iff \begin{cases} 2\,x \equiv 2 \pmod{14} \\ 3\,x \equiv 3 \pmod{30} \\ -4\,x \equiv 8 \pmod{18} \end{cases} \iff$$

$$\iff \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{10} \\ 2\,x \equiv -4 \pmod{9} \end{cases} \iff \circledast_{\copyright} : \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 1 \pmod{10} \\ x \equiv 7 \pmod{9} \end{cases}$$

L'ultimo sistema $\circledast_{\copyright}$ ottenuto qui sopra è un sistema — equivalente a quello iniziale — in *forma cinese*, nel quale i moduli sono a due a due coprimi: possiamo quindi risolverlo tramite il *Teorema Cinese del Resto*. *Si noti* che tale sistema potremmo sostituirlo con un sistema equivalente un po' più semplice, precisamente

$$\begin{cases} x \equiv 1 \pmod{70} \\ x \equiv 7 \pmod{9} \end{cases}$$

in quanto nel sistema $\circledast_{\copyright}$ ottenuto le prime due equazioni hanno in comune (ovviamente!) la soluzione $x = 1$ è a questo punto tutte le altre soluzioni ad esse comuni sono congruenti alla soluzione particolare $x = 1$ modulo $7 \cdot 10 = 70$, così che in conclusione il sottosistema di $\circledast_{\copyright}$ formato dalle sue prime due equazioni è equivalente a quello formato dalla sola equazione $x \equiv 1 (\mathrm{mod}\ 70)$. D'altra parte, questa semplificazione del sistema $\circledast_{\copyright}$ si "paga" poi con qualche calcolo un po' meno immediato al momento di applicare il *Teorema Cinese del Resto*; per questa ragione rinunciamo ad adottare tale semplificazione 8ma si può sempre fare, il problema non cambia realmente).

Ora, volendo applicare il *Teorema Cinese del Resto* al sistema (in forma cinese) $\circledast_{\copyright}$, poniamo $R := 7 \cdot 10 \cdot 9 = 630$, $R_1 := 10 \cdot 9 = 90$, $R_2 := 7 \cdot 9 = 63$, $R_3 := 7 \cdot 10 = 70$, e consideriamo le tre equazioni congruenziali

$$R_1\,x_1 \equiv 1 \pmod{7}\,, \quad R_2\,x_2 \equiv 9 \pmod{10}\,, \quad R_3\,x_3 \equiv 7 \pmod{9} \tag{5}$$

Se x_1', rispettivamente x_2', rispettivamente x_3', è una soluzione della prima, rispettivamente della seconda, rispettivamente della terza equazione in (5), allora le soluzioni (tutte!) del sistema $\circledast_{\copyright}$ — e quindi anche del sistema iniziale $\circledast$ in (4) ad esso equivalente — sono date dalla formula

$$x \;=\; x_0 \pmod{R} \qquad \text{con} \qquad x_0 \;:=\; R_1\,x_1' + R_2\,x_2' + R_3\,x_3' \tag{6}$$

Procedendo con in calcoli, la (6) esplicitamente è

$$90\,x_1 \equiv 1 \pmod{7}\,, \quad 63\,x_2 \equiv 1 \pmod{10}\,, \quad 70\,x_3 \equiv 7 \pmod{9}$$

in cui semplificando i coefficienti e un termine noto — tramite $90 \equiv_7 -1$, $63 \equiv_{10} 3$ e $70 \equiv_9 7$, e poi anche $1 \equiv_{10} 21$ — ci riduciamo a

$$-x_1 \equiv 1 \pmod{7}\,, \quad 3\,x_2 \equiv 21 \pmod{10}\,, \quad 7\,x_3 \equiv 7 \pmod{9}$$

da cui otteniamo subito le soluzioni

$$x_1 \equiv -1 \pmod 7\,, \quad x_2 \equiv 7 \pmod{10}\,, \quad x_3 \equiv 1 \pmod 9$$

Tra queste, scegliendo i valori particolari $x'_1 := -1$, $x'_2 := 7$, $x'_3 := 1$ e sostituendoli nella formula in (6) otteniamo

$$x_0 \;:=\; R_1\,x'_1 + R_2\,x'_2 + R_3\,x'_3 \;=\; 90\cdot(-1) + 63\cdot 7 + 70\cdot 1 \;=\; -90 + 441 + 70 \;=\; 421$$

per cui in conclusione — sempre dalla (6) — le soluzioni del sistema di equazioni congruenziali iniziale sono date da $x \equiv 421 \pmod{630}$, cioè formano l'insieme

$$[\,421\,]_{630} \;=\; \big\{\, 421 + 630\,z \,\big|\, z \in \mathbb{Z} \,\big\} \tag{7}$$

In alternativa, si può procedere alla risoluzione del sistema $\circledast_{\copyright}$ per sostituzioni successive. Ad esempio, sostituendo la prima nella seconda, e poi nella terza, i calcoli espliciti danno

$$\circledast_{\copyright}\;:\; \begin{cases} x \equiv 1 \pmod 7 \\ x \equiv 1 \pmod{10} \\ x \equiv 7 \pmod 9 \end{cases} \implies \begin{cases} x = 1 + 7\,h \quad \big(h \in \mathbb{Z}\big) \\ 1 + 7\,h \equiv 1 \pmod{10} \\ x \equiv 7 \pmod 9 \end{cases} \implies$$

$$\implies \begin{cases} x = 1 + 7\,h \quad \big(h \in \mathbb{Z}\big) \\ 7\,h \equiv 0 \pmod{10} \\ x \equiv 7 \pmod 9 \end{cases} \implies \begin{cases} x = 1 + 7\,h \quad \big(h \in \mathbb{Z}\big) \\ h \equiv 0 \pmod{10} \\ x \equiv 7 \pmod 9 \end{cases} \implies$$

$$\implies \begin{cases} x = 1 + 7\,h \quad \big(h \in \mathbb{Z}\big) \\ h \equiv 10\,k \quad \big(k \in \mathbb{Z}\big) \\ x \equiv 7 \pmod 9 \end{cases} \implies \begin{cases} x = 1 + 7\cdot 10\,k = 1 + 70\,k \quad \big(k \in \mathbb{Z}\big) \\ x \equiv 7 \pmod 9 \end{cases} \implies$$

$$\implies \begin{cases} x = 1 + 70\,k \quad \big(k \in \mathbb{Z}\big) \\ 1 + 70\,k \equiv 7 \pmod 9 \end{cases} \implies$$

$$\implies \begin{cases} x = 1 + 70\,k \quad \big(k \in \mathbb{Z}\big) \\ 70\,k \equiv 6 \pmod 9 \end{cases} \implies \begin{cases} x = 1 + 70\,k \quad \big(k \in \mathbb{Z}\big) \\ 7\,k \equiv 6 \equiv 42 \pmod 9 \end{cases} \implies$$

$$\implies \begin{cases} x = 1 + 70\,k \quad \big(k \in \mathbb{Z}\big) \\ k \equiv 6 \pmod 9 \end{cases} \implies \begin{cases} x = 1 + 70\,k \quad \big(k \in \mathbb{Z}\big) \\ k = 6 + 9\,\ell \quad \big(\ell \in \mathbb{Z}\big) \end{cases} \implies$$

$$\implies x = 1 + 70\,(6 + 9\,\ell\,) = 421 + 630\,\ell \quad \big(\ell \in \mathbb{Z}\big) \implies x = 421 + 630\,\ell \quad \big(\ell \in \mathbb{Z}\big)$$

così in definitiva troviamo che le soluzioni del sistema di equazioni congruenziali in esame sono tutte e sole del tipo

$$x \;=\; 421 + 630\,\ell\;, \qquad \forall\;\ell \in \mathbb{Z}$$

cioè si tratta esattamente dello stesso insieme di soluzioni già descritto in (7), q.e.d.

[3] — Affrontiamo i vari quesiti uno ad uno, ma indichiamo anche come alcuni di essi possano essere trattati insieme. Intanto cominciamo, in generale, che un sottoinsieme $\mathcal{H}$ in un gruppo $\mathcal{G}$ è un *sottogruppo* (di $\mathcal{G}$) — e si scrive $\mathcal{H} \leq \mathcal{G}$ — se:

(I) $\mathcal{H}$ contiene l'elemento neutro del gruppo, cioè $1_{\mathcal{G}} \in \mathcal{H}$,

(II) $\mathcal{H}$ è chiuso per l'operazione nel gruppo $\mathcal{G}$, cioè $h'\,h'' \in \mathcal{H}$ per ogni $h', h'' \in \mathcal{H}$,

(III) $\mathcal{H}$ è chiuso per gli inversi, cioè $h^{-1} \in \mathcal{H}$ per ogni $h \in \mathcal{H}$.

Inoltre, un sottogruppo $\mathcal{H}$ in un gruppo $\mathcal{G}$ è *normale* — e si scrive $\mathcal{H} \trianglelefteq \mathcal{G}$ — se

(IV) $\mathcal{H}$ è chiuso per i coniugati, cioè $g\,h\,g^{-1} \in \mathcal{H}$ per ogni $h \in \mathcal{H}$ e $g \in \mathcal{G}$.

(a) Dobbiamo verificare le proprietà *(I)*, *(II)* e *(III)* qui sopra per il sottoinsieme $\mathcal{H} := G_F$ del gruppo $\mathcal{G} := \mathcal{S}(E)$. Ora, direttamente dalle definizioni troviamo che:

(I) l'elemento neutro del gruppo $\mathcal{S}(E)$ è id_E , che è la permutazione identica, data da $\mathrm{id}_E(e) = e$ per ogni $e \in E$, quindi in particolare $\mathrm{id}_E(F) = F$, che significa esattamente che $\mathrm{id}_E(f) \in G_F$, q.e.d.

(II) per ogni $\gamma', \gamma'' \in G_F$ abbiamo $\gamma'(F) = F$ e $\gamma''(F) = F$, perciò per la composizione $\gamma' \circ \gamma''$ si ha $(\gamma' \circ \gamma'')(F) = \gamma'\big(\gamma''(F)\big) = \gamma'(F) = F$, cioè in breve $(\gamma' \circ \gamma'')(F) = F$, il che significa proprio che $\gamma' \circ \gamma'' \in G_F$, q.e.d.

(III) per ogni $\gamma \in G_F$ abbiamo $\gamma(F) = F$, da cui applicando γ^{-1} — l'inverso di γ in $\mathcal{S}(E)$ — a entrambi i membri dell'identità otteniamo $F = \gamma^{-1}(F)$, cioè $\gamma^{-1}(F) = F$, il che significa proprio che $\gamma' \circ \gamma'' \in G_F$, q.e.d.

(b) Dobbiamo verificare le proprietà *(I)*, *(II)* e *(III)* qui sopra per il sottoinsieme $\mathcal{H} := G_{(F)}$ del gruppo $\mathcal{G} := \mathcal{S}(E)$. La situazione è del tutto simile a quella del punto *(a)* per G_F , praticamente si può ripetere tutta la stessa analisi parola per parola, soltanto che *invece di sfruttare/dimostrare una certa proprietà per il sottoinsieme F bisogna farlo per ogni singolo elemento $f \in F$* . Adesso svolgerò qui sotto tale dimostrazione (parallela a quella in *(a)*, e da essa indipendente) poi spiegherò un metodo alternativo con il quale si può ottenere il punto *(b)* dal punto *(a)*.

(I) l'elemento neutro del gruppo $\mathcal{S}(E)$ è id_E , che è la permutazione identica, data da $\mathrm{id}_E(e) = e$ per ogni $e \in E$, quindi in particolare $\mathrm{id}_E(f) = f$ per ogni $f \in F$, che significa esattamente che $\mathrm{id}_E(f) \in G_{(F)}$, q.e.d.

(II) per ogni $\gamma', \gamma'' \in G_{(F)}$ abbiamo $\gamma'(f) = f$ e $\gamma''(f) = f$ per ogni $f \in F$, perciò per la composizione $\gamma' \circ \gamma''$ si ha $(\gamma' \circ \gamma'')(f) = \gamma'\big(\gamma''(f)\big) = \gamma'(f) = f$, cioè in breve $(\gamma' \circ \gamma'')(f) = f$, per ogni $f \in F$, il che significa proprio che $\gamma' \circ \gamma'' \in G_{(F)}$, q.e.d.

(III) per ogni $\gamma \in G_{(F)}$ abbiamo $\gamma(f) = f$ per ogni $f \in F$, da cui applicando γ^{-1} — l'inverso di γ in $\mathcal{S}(E)$ — a entrambi i membri dell'identità otteniamo $f = \gamma^{-1}(f)$, cioè $\gamma^{-1}(f) = f$, per ogni $f \in F$, il che significa proprio che $\gamma' \circ \gamma'' \in G_{(F)}$, q.e.d.

In alternativa, osserviamo che abbiamo anche

$$G_{\{f\}} := \big\{\, \gamma \in \mathcal{S}(E) \,\big|\, \gamma(f) = f \,\big\} \qquad \forall\ f \in F$$

e *ciascuno di tali sottoinsiemi $G_{\{f\}}$ è un sottogruppo di $\mathcal{S}$* , grazie al punto *(a)* applicato più volte ai vari sottoinsiemi $\{f\}$ — al posto di F . Ma le definizioni danno anche

$$G_{(F)} \;=\; \bigcap_{f \in F} G_{\{f\}}$$

quindi $G_{(F)}$ è intersezione di una famiglia di sottogruppi, e in quanto tale sappiamo (per un risultato generale) che è a sua volta un sottogruppo; otteniamo così il punto *(b)* come conseguenza del punto *(a)*.

(c) Dai punti *(a)* e *(b)* sappiamo già che $G_{(F)}$ e G_F sono entrambi sottogruppi di $\mathcal{S}(E)$, e inoltre dalle definizioni segue che $G_{(F)} \subseteq G_F$; perciò possiamo concludere che $G_{(F)} \leq G_F$, cioè $G_{(F)}$ è sottogruppo di G_F. Per dimostrare che tale sottogruppo è *normale* in G_F dobbiamo ancora verificare la proprietà *(IV)* qui sopra per il sottoinsieme $\mathcal{H} := G_{(F)}$ del gruppo $\mathcal{G} := G_F$.

Ora, per ogni $\gamma \in G_{(F)}$ e $\eta \in G_F$ abbiamo $\gamma(f) = f$ e $\eta(F) = F$, come anche $\eta^{-1}(F) = F$, così che $\eta^{-1}(f) \in F$ per ogni $f \in F$. Perciò per la composizione $\eta \circ \gamma \circ \eta^{-1}$ si ha

$$\big(\eta \circ \gamma \circ \eta^{-1}\big)(f) = \eta\big(\gamma\big(\eta^{-1}(f)\big)\big) = \eta\big(\eta^{-1}(f)\big) = f \qquad \forall\ f \in F$$

— deove abbiamo sfruttato il fatto che $\gamma\big(\eta^{-1}(f)\big) = \eta^{-1}(f)$ perché $\big(\eta^{-1}(f) \in F$ e $\gamma \in G_{(F)}$ — cioè in breve $\big(\eta \circ \gamma \circ \eta^{-1}\big)(f) = f$, per ogni $f \in F$, il che significa esattamente che $\eta \circ \gamma \circ \eta^{-1} \in G_{(F)}$, q.e.d.

(d) Dobbiamo dimostrare che $G_{(F)}$ è sottogruppo normale di $\mathcal{S}(E)$ se e soltanto se $\big|E \setminus F\big| < 2$. Dal punto *(b)* sappiamo già che $G_{(F)}$ è sottogruppo di $\mathcal{S}(E)$, perciò ci resta soltanto da dimostrare che vale anche la condizione *(IV)* se e soltanto se $\big|E \setminus F\big| < 2$, cioè

$$\sigma \circ \gamma \circ \sigma^{-1} \in G_{(F)}\,, \quad \forall\ \gamma \in G_{(F)}\,,\ \sigma \in \mathcal{S}(E) \qquad \Longleftrightarrow \qquad \big|E \setminus F\big| < 2 \tag{8}$$

Procediamo dimostrando separatamente le implicazioni "$\Longleftarrow$" e "$\Longrightarrow$".

$\underline{(\Longleftarrow)}$: Supponiamo che $\big|E \setminus F\big| < 2$, dunque è $\big|E \setminus F\big| = 0$ oppure $\big|E \setminus F\big| = 1$.

Nel primo caso abbiamo la serie di implicazioni

$$\big|E \setminus F\big| = 0 \quad \Longrightarrow \quad E \setminus F = \emptyset \quad \Longrightarrow \quad F = E \quad \Longrightarrow \quad G_F = \mathcal{S}(E)$$

e allora la tesi è verificata perché sappiamo già che $G_{(F)} \trianglelefteq G_F = \mathcal{S}(E)$, per il punto *(c)*.

Nel secondo caso abbiamo analogamente

$$\big|E \setminus F\big| = 1 \quad \Longrightarrow \quad E \setminus F = \{e_0\}$$

cioè E è costituito dal suo sottoinsieme F e da un altro solo elemento e_0 che non appartiene ad F. In tal caso, per ogni $\gamma \in G_{(F)}$ abbiamo necessariamente $\gamma(e_0) = e_0$, perché se fosse $\gamma(e_0) \neq e_0$ avremmo $f_0 := \gamma(e_0) \in F$, e quindi

$$\gamma^{-1}(f_0) \;=\; \gamma^{-1}\big(\gamma(e_0)\big) \;=\; \big(\gamma^{-1} \circ \gamma\big)(e_0) \;=\; \mathrm{id}_E(e_0) \;=\; e_0 \;\notin\; F \tag{9}$$

mentre sappiamo che $\gamma^{-1} \in G_{(F)}$ — perché $\gamma \in G_{(F)}$ è un sottogruppo, per il punto *(b)* — e quindi dev'essere $\gamma^{-1}(f_0) \in F$ dato che $f_0 \in F$. Questo contraddice (9), dunque concludiamo che non può essere $\gamma(e_0) \neq e_0$ e quindi è necessariamente $\gamma(e_0) = e_0$.

A questo punto per ogni $\gamma \in G_{(F)}$ abbiamo $\gamma(f) = f$ per ogni $f \in F$ (per definizione), ma anche $\gamma(e_0) = e_0$; visto che $E = F \cup \{e_0\}$ concludiamo che $\gamma(e) = e$ per ogni $e \in E$, cioè $\gamma = \mathrm{id}_E$. Ma così otteniamo $G_{(F)} = \{\mathrm{id}_E\}$, e allora la tesi è ovvia.

$\underline{(\Longrightarrow)}$: Supponiamo che si abbia $\sigma \circ \gamma \circ \sigma^{-1} \in G_{(F)}\,, \quad \forall\ \gamma \in G_{(F)}\,,\ \sigma \in \mathcal{S}(E)$. Dimostriamo allora che $\big|E \setminus F\big| < 2$ procedendo per assurdo.

Supponiamo, per assurdo, che sia $\big|E \setminus F\big| \geq 2$. Possiamo allora scegliere due elementi distinti $e_+, e_- \in E \setminus F$, $e_+ \neq e_-$, e un elemento $f_0 \in F$ — il che è sempre possibile,

perché $F \neq \emptyset$, per ipotesi — e in relazione a questi considerare l'unica permutazione $\bar\sigma \in \mathcal{S}(A)$ definita da

$$\bar\sigma(f_0) := e_+ \ , \qquad \bar\sigma(e_+) := e_- \ , \qquad \bar\sigma(e_-) := f_0 \ , \qquad \bar\sigma(\ell) := \ell \quad \forall\ \ell \in E \setminus \big\{f_0\,, e_+\,, e_-\big\}$$

e l'unica $\bar\gamma \in G_{(F)}$ definita da

$$\bar\gamma(e_+) := e_-\,,\ \ \bar\gamma(e_-) := e_+\,,\ \ \bar\gamma(f) := f\ \ \forall\, f \in F\,,\ \ \bar\gamma(\ell) := \ell\ \ \forall\, \ell \in E \setminus \Big(F \cup \big\{f_0\,, e_+\,, e_-\big\}\Big)$$

Con queste si trova che

$$\big(\bar\sigma \circ \bar\gamma \circ \bar\sigma^{-1}\big)(f_0) \ = \ \bar\sigma\big(\bar\gamma\big(\bar\sigma^{-1}(f_0)\big)\big) \ = \ \bar\sigma\big(\bar\gamma(e_-)\big) \ = \ \bar\sigma(e_+) \ = \ e_- \notin F$$

così che per $f_0 \in F$ si ha $\big(\bar\sigma \circ \bar\gamma \circ \bar\sigma^{-1}\big)(f_0) \notin F$; da questo possiamo concludere che $\big(\bar\sigma \circ \bar\gamma \circ \bar\sigma^{-1}\big) \notin G_{(F)}$, il che contraddice l'ipotesi fatta e ci dà quindi un assurdo, q.e.d.

(e) Volendo dimostrare che il gruppo quoziente $G_F \Big/ G_{(F)}$ è isomorfo al gruppo $\mathcal{S}(F)$, cerchiamo un isomorfismo $\phi : G_F \Big/ G_{(F)} \lhook\joinrel\longrightarrow\!\!\!\!\!\rightarrow \mathcal{S}(F)$. Siccome il gruppo di partenza è un quoziente, cerchiamo di ottenere tale isomorfismo tramite il *Teorema Fondamentale di Omomorfismo*: a tal fine cerchiamo un morfismo $\varphi : G_F \longrightarrow \Gamma$ da G_F ad un opportuno gruppo Γ tale che $Ker\,(\varphi) = G_{(F)}$ e $Im\,(\varphi) = \mathcal{S}(F)$; quest'ultima richiesta ci spinge a cercare direttamente un tale φ con codominio $\Gamma = \mathcal{S}(F)$ e che sia suriettivo. Riassumendo, cerchiamo un *epimorfismo* (:= morfismo suriettivo) di gruppi $\varphi : G_F \longrightarrow\!\!\!\!\!\rightarrow \mathcal{S}(F)$ tale che $Ker\,(\varphi) = G_{(F)}$: se lo troveremo, il *Teorema Fondamentale di Omomorfismo* ci darà allora automaticamente un *isomorfismo*

$$\varphi_* : G_F \Big/ G_{(F)} = G_F \Big/ Ker\,(\varphi) \lhook\joinrel\longrightarrow\!\!\!\!\!\rightarrow \mathcal{S}(F) \tag{10}$$

dato da $\varphi_*\big(\gamma \circ G_{(F)}\big) = \varphi(\gamma)$ per ogni classe laterale $\big(\gamma \circ G_{(F)}\big) \in G_F \Big/ G_{(F)}$.

Ora, dalla definizione di G_F ricaviamo che esiste una ben definita applicazione

$$\varphi : G_F \longrightarrow\!\!\!\!\!\rightarrow \mathcal{S}(F) \quad , \qquad \gamma \ \mapsto\ \varphi(\gamma) := \gamma\Big|_F \tag{11}$$

dove $\gamma\Big|_F$ indica la restrizione della permutazione γ di E in sé stesso al sottoinsieme F di E. Infatti, per definizione di G_F abbiamo $\gamma(F) = F$, quindi $\gamma\Big|_F$ è una (ben definita) funzione da F in sé stesso: inoltre, $\gamma\Big|_F$ è certamente iniettiva perché è la restrizione di γ che è iniettiva per ipotesi, $\gamma\Big|_F$ è anche suriettiva perché $\gamma(F) = F$; perciò $\gamma\Big|_F$ è una funzione di biiettiva di F in sé, cioè $\gamma\Big|_F \in \mathcal{S}(F)$, q.e.d. In alternativa, dopo aver osservato che $\gamma\Big|_F$ è una funzione da F in sé stesso, osserviamo anche che dalle definizioni si ottiene subito

$$\big(\gamma' \circ \gamma''\big)\Big|_F \ = \ \gamma'\Big|_F \circ \gamma''\Big|_F \qquad\qquad \forall\ \gamma', \gamma'' \in G_F \tag{12}$$

allora da $\gamma \circ \gamma^{-1} = id_E = \gamma^{-1} \circ \gamma$ deduciamo subito che $\gamma\Big|_F \circ \gamma^{-1}\Big|_F = id_E = \gamma^{-1}\Big|_F \circ \gamma\Big|_F$, così la funzione $\gamma\Big|_F$ è invertibile — con inversa $\gamma^{-1}\Big|_F$ — quindi è una permutazione, q.e.d.

Osserviamo ora che *la funzione φ è suriettiva*. Infatti, per ogni $\chi \in \mathcal{S}(F)$ possiamo considerare la funzione

$$\gamma_\chi : E \longrightarrow E \ , \quad \gamma_\chi(f) := \chi(f) \ \ \forall\, f \in F \ , \quad \gamma_\chi(e) := e \ \ \forall\, e \in \big(E \setminus F\big)$$

cioè in sintesi γ_χ è caratterizzata da $\gamma_\chi\Big|_F = \chi$ e $\gamma_\chi\Big|_{(E\setminus F)} = id_{(E\setminus F)}$. Da questo è immediato riconoscere che γ_χ è una permutazione, cioè $\gamma_\chi \in \mathcal{S}(E)$, e più precisamente che $\gamma_\chi \in G_F$; inoltre abbiamo $\varphi(\gamma_\chi) := \gamma_\chi\Big|_F = \chi$. Concludiamo allora che per ogni $\chi \in \mathcal{S}(F$ esiste una $\gamma_\chi \in G_F$ tale che $\varphi(\gamma_\chi) = \chi$, dunque φ è *suriettiva*, q.e.d.

Notiamo poi che l'osservazione (12) significa che $\varphi\big(\gamma' \circ \gamma''\big) = \varphi\big(\gamma'\big) \circ \varphi\big(\gamma''\big)$ — per ogni $\gamma', \gamma'' \in G_F$ — cioè *la funzione φ data in (11) è un morfismo di gruppi*; siccome poi abbiamo visto che è suriettivo, tale φ è un epimorfismo. Allora il *Teorema Fondamentale di Omomorfismo* (per gruppi) ci dà un isomorfismo $\varphi_* : G_F \Big/ Ker\,(\varphi) \xhookrightarrow{\ \ } \mathcal{S}(F)$ e ci resta soltanto da dimostrare che $Ker\,(\varphi) = G_{(F)}$. Ma questo segue direttamente dalla costruzione, in quanto le dalle definizioni date fin qui otteniamo subito

$$\begin{aligned} Ker\,(\varphi) \ = \ \big\{\gamma \in G_F \,\big|\, \varphi(\gamma) = id_F\big\} \ = \ \big\{\gamma \in G_F \,\big|\, \gamma\Big|_F = id_F\big\} \ = \\ = \ \big\{\gamma \in G_F \,\big|\, \gamma(f) = f \ \ \forall\, f \in F\,\big\} \ =: \ G_{(F)} \end{aligned}$$

così che $Ker\,(\varphi) = G_{(F)}$, q.e.d.

In conclusione — riassumendo — abbiamo trovato un isomorfismo di gruppi esplicito come in (10), precisamente

$$\varphi_* \,:\, G_F \Big/ G_{(F)} \xhookrightarrow{\ \ } \mathcal{S}(F) \quad , \qquad \varphi_*\big(\gamma \circ G_{(F)}\big) \,=\, \gamma\Big|_F \quad \forall \ \ \gamma \in G_F \tag{13}$$

(b)–(c)–(e) — dimostrazione alternativa: Assumiamo di sapere già — come affermato nel punto *(a)* — che G_F sia un sottogruppo di $\mathcal{S}$. Possiamo allora procedere con la costruzione dell'isomorfismo (13) come sopra, il che dimostra i punto *(e)*. In questa procedimento, un passo intermedio è la costruzione del morfismo $\varphi : G_F \longrightarrow \mathcal{S}(F)$ in (10), per il quale poi (come visto in precedenza) troviamo facilmente che $Ker\,(\varphi) = G_{(F)}$. Ma dalla teoria generale sappiamo che il nucleo di un morfismo tra gruppi è sempre un sottogruppo normale, e quindi in particolare un sottogruppo, del gruppo che è dominio di tale morfismo: perciò nel caso in esame questo ci garantisce che $G_{(F)} = Ker\,(\varphi) \trianglelefteq G_F$, il che dimostra *(c)* e quindi a maggior ragione anche *(b)*.

[4] — Dobbiamo determinare tutti gli $x \in \mathbb{Z}$ tali che

$$63224^{\,347} \cdot x \ \equiv \ -308 \pmod{21} \qquad \& \qquad -\,5 \leqslant x \leqslant +7 \tag{14}$$

Per prima cosa, osserviamo che l'equazione modulare

$$63224^{\,347} \cdot x \ \equiv \ -308 \pmod{21} \tag{15}$$

in (14) può essere semplificata: infatti, tenendo conto che $63224 \equiv 14 \pmod{21}$ e $-308 \equiv 7 \pmod{21}$, la (15) è equivalente a

$$14^{347} \cdot x \,=\, 7 \pmod{21} \tag{16}$$

Ora riscriviamo la (+3) nella forma

$$7 \cdot 2 \cdot 14^{346} \cdot x \,=\, 7 \pmod{7 \cdot 3} \tag{17}$$

e osserviamo che il coefficiente dell'incognita, il termine noto e il modulo sono tutti divisibili er 7, per cui la (17) è equivalente a

$$2 \cdot 14^{346} \cdot x \,=\, 1 \pmod{3} \tag{18}$$

che è un'equazione congruenziale *modulo 3* — molto più semplice!!! Adesso osserviamo che $2 \equiv -1 \pmod{3}$ e $14 \equiv -1 \pmod{3}$, per cui la (18) diventa

$$-1 \cdot (-1)^{346} \cdot x \,=\, 1 \pmod{3} \quad , \qquad \text{cioè} \qquad -\,x \,=\, 1 \pmod{3}$$

e quindi in definitiva

$$x \,=\, -1 \pmod{3} \quad , \qquad \text{cioè} \qquad x \,\in\, \big(-1 + 3\,\mathbb{Z}\big)$$

In conclusione le condizioni in (+1) sono equivalenti a

$$x \,\in\, \big(-1 + 3\,\mathbb{Z}\big) \bigcap \big\{\, x \in \mathbb{Z} \,\big|\, -5 \leqslant x \leqslant +7 \,\big\}$$

perciò la soluzione al problema dato è

$$x \,\in\, \big\{-4\,, -1\,, +2\,, +5\,\big\}$$

[5] — Affrontiamo i vari quesiti uno ad uno.

(a) Ricordiamo che un sottoinsieme S di un anello A è un sottoanello di A se e soltanto se valgono le seguenti proprietà:

(a.1) $0_A \in S$,

(a.2) $(s_1 - s_2) \in S$ per ogni $s_1, s_2 \in S$;

(a.3) $(s_1\, s_2) \in S$ per ogni $s_1, s_2 \in S$.

Nel caso dell'anello $A := \mathbb{C}$ e del suo sottoinsieme $S := \mathbb{Z}\big[\sqrt{-8}\,\big]$ la verifica di tali proprietà si svolge come segue:

(a.1) $0_A = \big(0 + 0\,\sqrt{-8}\,\big) \in S := \mathbb{Z}\big[\sqrt{-8}\,\big]$ perché $0 \in \mathbb{Z}$,

(a.2) per ogni $s_1 = \big(a_1 + b_1\,\sqrt{-8}\,\big), s_2 = \big(a_2 + b_2\,\sqrt{-8}\,\big) \in S := \mathbb{Z}\big[\sqrt{-8}\,\big]$ si ha $(s_1 - s_2) = \big(a_1 + b_1\,\sqrt{-8}\,\big) - \big(a_2 + b_2\,\sqrt{-8}\,\big) = \big((a_1 - a_2) + (b_1 - b_2)\,\sqrt{-8}\,\big) \in S := \mathbb{Z}\big[\sqrt{-8}\,\big]$ perché $(a_1 - a_2) \in \mathbb{Z}$ e $(b_1 - b_2) \in \mathbb{Z}$,

(a.3) per ogni $s_1 = \big(a_1 + b_1\,\sqrt{-8}\,\big), s_2 = \big(a_2 + b_2\,\sqrt{-8}\,\big) \in S := \mathbb{Z}\big[\sqrt{-8}\,\big]$ si ha $(s_1\, s_2) = \big(a_1 + b_1\,\sqrt{-8}\,\big)\,\big(a_2 + b_2\,\sqrt{-8}\,\big) = \big((a_1 a_2 - 8\,b_1 b_2) + (a_1 b_2 + a_1 b_1)\,\sqrt{-8}\,\big) \in S := \mathbb{Z}\big[\sqrt{-8}\,\big]$ perché $(a_1 a_2 - 8\,b_1 b_2) \in \mathbb{Z}$ e $(a_1 b_2 + a_1 b_1) \in \mathbb{Z}$.

Pertanto possiamo concludere che $\mathbb{Z}\big[\sqrt{-8}\,\big]$ *è sottoanello di* $\mathbb{C}$, q.e.d.

(b) Dovendo dimostrare che nell'anello $\mathbb{Z}\big[\sqrt{-8}\,\big]$ ogni elemento non nullo e non invertibile ha (almeno) una fattorizzazione in prodotto di elementi irriducibili, cominciamo con l'osservare che esiste una funzione speciale

$$v : \mathbb{Z}\big[\sqrt{-8}\,\big] \longrightarrow\!\!\!\!\!\!\longrightarrow \mathbb{N} \quad , \qquad \big(a + b\sqrt{-8}\,\big) \mapsto v\big(a + b\sqrt{-8}\,\big) := a^2 + 8\,b^2 \tag{19}$$

— che chiameremo "valutazione", e coincide con la restrizione al sottoanello della funzione "norma" $\mathbb{C} \longrightarrow \mathbb{R}_{\geq 0}\,\big(\, z \mapsto N(z) := z\,\overline{z}\,\big)$ per numeri complessi — che ha la notevole proprietà di essere *moltiplicativa*, cioè tale che

$$v(\alpha\,\beta\,) \;=\; v(\alpha)\,v(\beta\,) \qquad\qquad \forall\;\; \alpha, \beta \in \mathbb{Z}\big[\sqrt{-8}\,\big] \tag{20}$$

Dall'esistenza di tale funzione "valutazione" segue un fatto importante:

$$U\big(\,\mathbb{Z}\big[\sqrt{-8}\,\big]\,\big) \;=\; \big\{\, \zeta \in \mathbb{Z}\big[\sqrt{-8}\,\big] \;\big|\; v(\zeta) = 1 \,\big\} \;=\; \{+1\,, -1\} \tag{21}$$

cioè gli elementi invertibili di $\mathbb{Z}\big[\sqrt{-8}\,\big]$ sono soltanto $+1$ e -1. Infatti, $+1$ e -1 sono ovviamente invertibili (con inversi $+1$ e -1 rispettivamente) per ogni $\alpha \in \mathbb{Z}\big[\sqrt{-8}\,\big]$ abbiamo che $\alpha \in U\big(\,\mathbb{Z}\big[\sqrt{-8}\,\big]\,\big)$, cioè α è invertibile, se e soltanto se esiste un $\eta \in \mathbb{Z}\big[\sqrt{-8}\,\big]$ tale che $\alpha\,\eta = 1$; ma in tal caso la (20) ci dà

$$v(\alpha)\,v(\eta) \;=\; v(\alpha\,\eta) \;=\; v(1) \;=\; 1$$

da cui ricaviamo $v(\alpha), v(\eta) = 1$ e quindi $\alpha\,, \eta \in \{+1\,, -1\}$, q.e.d.

Ora consideriamo un elmento $\vartheta \in \mathbb{Z}\big[\sqrt{-8}\,\big]$ che sia non nullo e non invertibile. In particolare, ne segue — tenendo conto della (21) — abbiamo che $v(\vartheta) > 1$.

Ora, se ϑ è *irriducibile*, è già fattorizzato (!) come vogliamo: la sua fattorizzazione in irriducibili è semplicemente $\alpha = \alpha$ (dove a destra abbiamo un prodotto di *un solo* fattore *irriducibile*. Se invece ϑ non è irriducibile, cioè è *riducibile*, allora esiste una sua fattorizzazione non banale del tipo $\vartheta = \alpha\,\beta$ con $\alpha \notin U\big(\,\mathbb{Z}\big[\sqrt{-8}\,\big]\,\big)$ e $\beta \notin U\big(\,\mathbb{Z}\big[\sqrt{-8}\,\big]\,\big)$, dunque $v(\alpha) > 1$ e $v(\beta\,) > 1$ in virtù di (21). Ora la (20) ci dà $v(\vartheta) = v(\alpha\,\beta\,) = v(\alpha)\,v(\beta\,)$ con $v(\alpha) > 1$ e $v(\beta\,) > 1$, da cui ricaviamo $v(\alpha) < v(\vartheta)$ e $v(\beta\,) < v(\vartheta)$. A questo punto, adottando il metodo di dimostrazione per *induzione forte* (facendo induzione su $v(\vartheta)$, che è un numero naturale!) possiamo fare l'Ipotesi Induttiva che ogni $\zeta \in \mathbb{Z}\big[\sqrt{-8}\,\big]$, non nullo e non invertibile, sia fattorizzabile in irriducibili: in particolare questa ipotesi si applica adesso a $\zeta := \alpha$ e $\zeta := \beta$, quindi possiamo assumere che esistano fattorizzazioni in irriducibili $\alpha = \kappa_1 \cdots \kappa_r$ e $\beta = \chi_1 \cdots \chi_s$. Ma allora

$$\vartheta \;=\; \alpha\,\beta \;=\; \kappa_1 \cdots \kappa_r \cdot \chi_1 \cdots \chi_s$$

per cui $\vartheta \;=\; \alpha\,\beta \;=\; \kappa_1 \cdots \kappa_r \cdot \chi_1 \cdots \chi_s$ è una fattorizzazione di ϑ in irriducibili, q.e.d.

N.B.: questa è *esattamente la stessa idea* che si usa per dimostrare in un anello euclideo ogni elemento non nullo e non invertibile ha una fattorizzazione in irriducibili...

(c) Consideriamo l'elemento $9 \in \mathbb{Z}\big[\sqrt{-8}\,\big]$, per il quale esistono le due fattorizzazioni

$$9 \;=\; 3 \cdot 3 \quad , \qquad 9 \;=\; \big(1 + \sqrt{-8}\,\big) \cdot \big(1 - \sqrt{-8}\,\big) \tag{22}$$

Osserviamo che in entrambe le fattorizzazioni in (22) tutti i fattori sono irriducibili. Infatti, per il fattore 3 abbiamo $v(3) = 9$, quindi una qualsiasi fattorizzazione $3 = \alpha\,\beta$ di 3 implicherà — per la (20) — una fattorizzazione $9 = v(3) = v(\alpha\,\beta) = v(\alpha)\,v(\beta)$ per cui $\big(v(\alpha), v(\beta)\big) \in \big\{(9\,,1)\,,(3\,,3)\,,(1\,,9)\big\}$; ma dalle definizioni vediamo che $v(\zeta) \neq 3$ per ogni $\zeta \in \mathbb{Z}\big[\sqrt{-8}\,\big]$, e quindi dev'essere $\big(v(\alpha), v(\beta)\big) = (9\,,1)$ oppure $\big(v(\alpha), v(\beta)\big) = (1\,,9)$, dunque $v(\beta) = 1$ o $v(\alpha) = 1$, per cui — dalla (21) — o β o α è invertibile e quindi la fattorizzazione $3 = \alpha\,\beta$ è banale; perciò in definitiva 3 è irriducibile. Analogamente per $\big(1 \pm \sqrt{-8}\,\big)$ — con i due segni possibili, trattati simultaneamente — ogni fattorizzazione $\big(1 \pm \sqrt{-8}\,\big) = \alpha\,\beta$ implica $v(\alpha)\,v(\beta) = v\big(1 \pm \sqrt{-8}\,\big) = 9$ e quindi di nuovo $\big(v(\alpha), v(\beta)\big) \in \big\{(9\,,1)\,,(3\,,3)\,,(1\,,9)\big\}$, così che si conclude come prima, trovando che la fattorizzazione $\big(1 \pm \sqrt{-8}\,\big) = \alpha\,\beta$ è banale; perciò in definitiva $\big(1 \pm \sqrt{-8}\,\big)$ è irriducibile, q.e.d.

Si noti che esistono molti altri elementi (non nulli e non invertibili) che ammettono almeno due fattorizzazioni in irriducibili non equivalenti. Ad esempio, in modo del tutto analogo a prima si può dimostrare che per $8 \in \mathbb{Z}\big[\sqrt{-8}\,\big]$ abbiamo le due fattorizzazioni

$$8 \;=\; 2 \cdot 2 \cdot 2 \quad , \qquad 8 \;=\; \sqrt{-8}\,\big(-\sqrt{-8}\,\big)$$

in irriducibili che sono tra loro non equivalenti; in questo caso, addirittura il numero di fattori irriducibili è diverso nei due casi.

[6] — Ricordiamo la definizione di $\mathbb{P}_k(n)$ — per ogni $n\,,k \in \mathbb{N}$ — che scritta in formule è questa:

$$\mathbb{P}_k(n) \;=\; \big|\,\mathcal{P}_k(X_n)\,\big| \;=\; \Big|\,\big\{\,Y \in \mathcal{P}(X_n)\,\big|\,|Y| = k\,\big\}\,\Big| \tag{23}$$

dove X_n indica un qualunque insieme tale che $|X_n| = n$, poi $\mathcal{P}(X_n)$ indica l'insieme delle parti di X_n, e infine $\mathcal{P}_k(n) = \Big|\,\big\{\,Y \in \mathcal{P}(X_n)\,\big|\,|Y| = k\,\big\}\,\Big|$.

Procediamo ora a dimostrare l'identità richiesta

$$\mathbb{P}_3(\ell + t) \;=\; \mathbb{P}_3(\ell) \,+\, \mathbb{P}_2(\ell)\,t \,+\, \ell\,\mathbb{P}_2(t) \,+\, \mathbb{P}_3(t) \qquad\qquad \forall\;\ell\,,t \in \mathbb{N}\,. \tag{24}$$

seguendo due metodi diversi e indipendenti.

<u>*Primo metodo:*</u> Dati $n\,,k \in \mathbb{N}$ consideriamo $n := \ell + t$. Fissato un qualunque insieme X_ℓ, rispettivamente X_t, con esattamente ℓ elementi, rispettivamente t elementi, consideriamo la loro unione disgiunta $X_{\ell+t} := X_\ell \coprod X_t$ che è un insieme con esattamente $n := \ell + t$ elementi. Consideriamo i seguenti sottoinsiemi di $\mathcal{P}_3(X_{\ell+t})$

$$\mathcal{P}_3^{r,s}(\ell + t) \;=\; \big\{\,Y \in \mathcal{P}_3(X_{\ell+t})\,\big|\,|Y \cap X_\ell| = r\,,\,|Y \cap X_t| = s\,\big\} \qquad\qquad \forall\;\;(r,s) \in \big\{(3\,,0),(2\,,1),(1\,,2),(0\,,3)\big\}$$

e osserviamo che essi formano una *partizione* di $\mathcal{P}_3(X_{\ell+t})$: in particolare, sono a due a due disgiunti e la loro unione è tutto $\mathcal{P}_3(X_{\ell+t})$. Come conseguenza di questo, ricordando che la cardinalità dell'unione disgiunta di alcuni sottoinsiemi è la somma delle cardinalità dei suddetti insiemi, abbiamo

$$\begin{aligned} \big|\mathcal{P}_3(X_{\ell+t})\big| \;&=\; \Big|\,\mathcal{P}_3^{3,0}(X_{\ell+t}) \coprod \mathcal{P}_3^{2,1}(X_{\ell+t}) \coprod \mathcal{P}_3^{1,2}(X_{\ell+t}) \coprod \mathcal{P}_3^{0,3}(X_{\ell+t})\,\Big| \;= \\ &=\; \big|\,\mathcal{P}_3^{3,0}(X_{\ell+t})\,\big| \,+\, \big|\,\mathcal{P}_3^{2,1}(X_{\ell+t})\,\big| \,+\, \big|\,\mathcal{P}_3^{1,2}(X_{\ell+t})\,\big| \,+\, \big|\,\mathcal{P}_3^{0,3}(X_{\ell+t})\,\big| \end{aligned} \tag{25}$$

Ora, nella formula qui sopra il primo termine è

$$\big|\mathcal{P}_3(X_{\ell+t})\big| \;=:\; \mathbb{P}_3(\ell+t) \tag{26}$$

mentre il primo e l'ultimo addendo nella somma finale sono rispettivamente

$$\big|\mathcal{P}_3(X_\ell)\big| =: \mathbb{P}_3(\ell) \quad \text{e} \quad \big|\mathcal{P}_3(X_{\ell+t})\big| =: \mathbb{P}_3(X_t) \tag{27}$$

in forza della (23). Inoltre, nella somma finale il secondo addendo è

$$\big|\,\mathcal{P}_3^{2,1}(X_{\ell+t})\,\big| = \mathbb{P}_2(\ell)\cdot t \tag{28}$$

Infatti, ogni $Y \in \mathcal{P}_3^{2,1}(X_{\ell+t})$ è l'unione disgiunta $Y = (Y\cap X_\ell)\coprod(Y\cap X_t)$ con $(Y\cap X_\ell) \in \mathcal{P}_2(X_\ell)$ e $(Y\cap X_t)\in\mathcal{P}_1(X_t)$ scelti liberamente, così che la coppia $\big(Y\cap X_\ell\,, Y\cap X_t\big)$ è scelta liberamente in $\mathcal{P}_2(X_\ell)\times\mathcal{P}_1(X_t)$, che è un insieme di cardinalità $\big|\,\mathcal{P}_2(X_\ell)\times\mathcal{P}_1(X_t)\,\big| = \big|\,\mathcal{P}_2(X_\ell)\,\big|\cdot\big|\,\mathcal{P}_1(X_t)\,\big| = \mathbb{P}_2(\ell)\cdot\mathbb{P}_1(t)$. Infine dalle definizioni troviamo subito che $\mathbb{P}_1(h) = h$ per ogni $h\in\mathbb{N}$, per cui in conclusione otteniamo la (28). Parallelamente, in modo del tutto analogo troviamo che

$$\big|\,\mathcal{P}_3^{1,2}(X_{\ell+t})\,\big| = \ell\cdot\mathbb{P}_2(t) \tag{29}$$

Per concludere, mettiamo insieme le (25)–(29) e otteniamo l'identità (24), q.e.d.

Secondo metodo: Osserviamo che la definizione stessa — data in (23) — di $\mathbb{P}_k(n)$ dice che $\mathbb{P}_k(n) = \binom{n}{k}$, dove l'ultimo simbolo indica il ben noto *coefficiente binomiale* chiamato "*n sopra k*". Ora, per quest'ultimo conosciamo l'espressione esplicita $\binom{n}{k} = \dfrac{n!}{k!\,(n-k)!}$, e quindi abbiamo

$$\mathbb{P}_k(n) \;=\; \frac{n!}{k!\,(n-k)!}$$

Sostituendo tale espressione nella (24) si ottiene una identità tra frazioni, che si dimostra facilmente per calcolo diretto.