CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2018–2019

Esame scritto del 10 Settembre 2019 — Sessione Autunnale, I appello

Testo & Svolgimento

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

[1] — Sia E un insieme con almeno due elementi, sia $\mathcal{P}(E)$ l'insieme delle parti di E, sia $\underline{2}^E$ l'insieme delle funzioni caratteristiche su E, e sia $\Pi_2(E)$ l'insieme di tutte le partizioni di E indicizzate da un insieme $\underline{2} := \{0\,,1\}$ di due elementi, cioè partizioni del tipo $\big\{E_0\,,E_1\big\}$, per le quali in aggiunta si abbia $E_0 \neq E_1$.

(a) Si consideri in $\underline{2}^E$ l'operazione "$\cdot$" definita da $\big(\eta' \cdot \eta''\big)(e) := \eta'(e) \cdot \eta''(e)$ per ogni $e \in E$. Determinare esplicitamente una funzione $\Psi : \underline{2}^E \longrightarrow \mathcal{P}(E)$ che sia invertibile e tale che $\Psi\big(\eta' \cdot \eta''\big) = \Psi\big(\eta'\big) \cup \Psi\big(\eta''\big)$ per ogni $\eta', \eta'' \in \underline{2}^E$.

(b) Siano $\eta_{\mathbf{0}}\,, \eta_{\mathbf{1}} \in \underline{2}^E$ le due funzioni caratteristiche costanti, definite rispettivamente da $\eta_{\mathbf{0}}(e) := 0$ e $\eta_{\mathbf{1}}(e) := 1$ per ogni $e \in E$. Determinare esplicitamente una funzione $\Omega : \underline{2}^E \setminus \big\{\eta_{\mathbf{0}}\,, \eta_{\mathbf{1}}\big\} \longrightarrow \Pi_2(E)$ che sia invertibile.

[2] — Si dimostri *utilizzando esplicitamente il Principio di Induzione Semplice*, che per ogni $n \in \mathbb{N}$ con $n \geq 3$ vale la disuguaglianza

$$2 \cdot 3^n - 5 \;>\; 5 \cdot 2^n + 2$$

[3] — Per un qualsiasi gruppo G, consideriamo gli elementi $[\,h\,,k\,] := h\,k\,h^{-1}\,k^{-1}$ — per ogni $h\,,k \in G$ — e il sottogruppo da essi generato in G, indicato con

$$G' \;:=\; \Big\langle \big\{\, [\,h\,,k\,] := h\,k\,h^{-1}\,k^{-1} \;\big|\; h\,,k \in G \,\big\} \Big\rangle$$

Dimostrare che:

(a) $G' \trianglelefteq G$, cioè G' è sottogruppo *normale* di G;

(b) per ogni endomorfismo $\phi \in End\,(G)$ del gruppo G si ha $\phi\big(G'\big) \subseteq G'$;

(c) il gruppo quoziente $G \Big/ G'$ è abeliano.

[4] — Sia A un anello, e sia I un ideale (bilatero) di A. Dimostrare che l'anello quoziente $A\Big/I$ è commutativo se soltanto se si ha $\big(a'a''-a''a'\big)\in I$ per ogni $a',a''\in A$.

[5] — Sia D un dominio euclideo, sia $d\in D$ un elemento *irriducibile* in D, e sia (d) l'ideale principale di D generato dall'elemento d.

Dimostrare che l'anello quoziente $D\Big/(d)$ è un campo.

((*Suggerimento:* si pensi al caso $D=\mathbb{Z}\,...$))

[6] — Nell'anello $\mathbb{Z}[\,i\,]$ degli interi di Gauss, sia $I:=\big(1-3\,i\,,\,5+i\big)$ l'ideale generato dai due elementi $1-3\,i$ e $5+i$.

(a) Determinare esplicitamente un generatore d dell'ideale I.

(b) Per il generatore d dell'ideale I trovato al punto *(a)*, determinare esplicitamente elementi $r\,,s\in\mathbb{Z}[\,i\,]$ tali che $d\,=\,r\,(1-3\,i\,)\,+\,s\,(5+i\,)$.

— $\star$ —

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 esiste una funzione "standard"

$$\Phi:\underline{2}^E\longrightarrow\mathcal{P}(E)\ ,\quad \eta\mapsto\Phi(\eta):=\eta^{-1}(1)=\big\{\,e\in E\,\big|\,\eta(e)=1\,\big\}\quad\forall\ \eta\in\underline{2}^E\qquad(1)$$

che è effettivamente invertibile. Per tale funzione si ha $\Phi\big(\eta'\cdot\eta''\big)=\Phi\big(\eta'\big)\cap\Phi\big(\eta''\big)$ per ogni $\eta',\eta''\in\underline{2}^E$, ma in generale *non* è $\Phi\big(\eta'\cdot\eta''\big)=\Phi\big(\eta'\big)\cup\Phi\big(\eta''\big)$ per ogni $\eta',\eta''\in\underline{2}^E$.

Perciò la soluzione al quesito *(a)* non è data dalla (1), ma da una sua lieve variante, che ora introduciamo. Precisamente, consideriamo la funzione

$$\Psi:\underline{2}^E\longrightarrow\mathcal{P}(E)\ ,\quad \eta\mapsto\Psi(\eta):=\eta^{-1}(0)=\big\{\,e\in E\,\big|\,\eta(e)=0\,\big\}\quad\forall\ \eta\in\underline{2}^E\qquad(2)$$

Abbiamo allora che tale Ψ è una funzione del tipo richiesto. Infatti:

[1]: Ψ è funzione invertibile. Infatti, per ogni $E' \in \mathcal{P}(E)$ definiamo la funzione

$$\eta_{E'} : E \longrightarrow \underline{2} \ , \quad e \mapsto \eta_{E'}(e) := \begin{cases} 0 \ , & \forall\, e \in E' \\ 1 \ , & \forall\, e \notin E' \end{cases}$$

per la quale ovviamente si ha $\eta_{E'} \in \underline{2}^E$; complessivamente abbiamo allora la funzione

$$\Psi' : \mathcal{P}(E) \longrightarrow \underline{2}^E \ , \quad E' \mapsto \Psi'\big(E'\big) := \eta_{E'} \qquad \forall\ E' \in \mathcal{P}(E)$$

Osserviamo ora che tale Ψ' è la funzione inversa di Ψ. Infatti

$$\big(\Psi' \circ \Psi\big)(\eta) \ = \ \Psi'\big(\Psi(\eta)\big) \ = \ \Psi'\big(\eta^{-1}(0)\big) \ = \ \eta_{\eta^{-1}(0)} \ = \ \eta \qquad \forall\ \eta \in \underline{2} \tag{3}$$

dove l'ultima uguaglianza segue immediatamente dalle definizioni; d'altra parte è anche

$$\big(\Psi \circ \Psi'\big)\big(E'\big) \ = \ \Psi\big(\Psi'\big(E'\big)\big) \ = \ \Psi\big(\eta_{E'}\big) \ = \ \eta_{E'}^{-1}(0) \ = \ E' \qquad \forall\ E' \in \mathcal{P}(E) \tag{4}$$

dove di nuovo l'ultima uguaglianza segue direttamente dalle definizioni.

Riassumendo, la (3) ci dice che $\big(\Psi' \circ \Psi\big)(\eta) = \eta$ per ogni $\eta \in \underline{2}^E$, dunque $\Psi' \circ \Psi = \mathrm{id}_{\underline{2}^E}$, mentre la (4) assicura che $\big(\Psi \circ \Psi'\big)\big(E'\big) = E'$ per ogni $E' \in \mathcal{P}(E)$, dunque $\Psi \circ \Psi' = \mathrm{id}_{\mathcal{P}(E)}$. Perciò $\Psi' \circ \Psi = \mathrm{id}_{\underline{2}^E}$ e $\Psi \circ \Psi' = \mathrm{id}_{\mathcal{P}(E)}$, quindi Ψ' è l'inversa di Ψ, q.e.d.

[2]: Ψ soddisfa le identità $\Psi\big(\eta' \cdot \eta''\big) \ = \ \Psi\big(\eta'\big) \cup \Psi\big(\eta''\big)$ per ogni $\eta', \eta'' \in \underline{2}^E$. Infatti, i calcoli diretti ci danno

$$\begin{aligned} \Psi\big(\eta' \cdot \eta''\big) \ &:= \ \big(\eta' \cdot \eta''\big)^{-1}(0) \ = \ \big\{\, e \in E \,\big|\, \big(\eta' \cdot \eta''\big)(e) = 0 \,\big\} \ = \\ &= \ \big\{ e \in E \,\big|\, \eta'(e) = 0 \ \text{ oppure } \ \eta''(e) = 0 \big\} \ = \ \big\{ e \in E \,\big|\, \eta'(e) = 0 \big\} \bigcup \big\{ e \in E \,\big|\, \eta''(e) = 0 \big\} \ = \\ &= \ \big(\eta'\big)^{-1}(0) \bigcup \big(\eta''\big)^{-1}(0) \ = \ \Psi\big(\eta'\big) \cup \Psi\big(\eta''\big) \end{aligned}$$

(b) La funzione $\Psi : \underline{2}^E \longrightarrow \mathcal{P}(E)$ considerata in (2) associa ad ogni funzione caratteristica η in E il sottoinsieme di E dato da $\Psi(\eta) := \eta^{-1}(0)$; se ad esso aggiungiamo il sottoinsieme $\eta^{-1}(1)$, abbiamo una coppia non ordinata di sottoinsiemi $\big\{\eta^{-1}(0)\,, \eta^{-1}(1)\big\}$ associata a η . Inoltre, se prendiamo $\eta \notin \big\{\eta_{\mathbf{0}}\,, \eta_{\mathbf{1}}\big\}$, allora in aggiunta abbiamo $\eta^{-1}(0) \neq \emptyset$ (perché $\eta \neq \eta_{\mathbf{1}}$) e $\eta^{-1}(1) \neq \emptyset$ (perché $\eta \neq \eta_{\mathbf{0}}$). Ma allora $\eta^{-1}(0)$ e $\eta^{-1}(1)$ sono due sottoinsiemi di E entrambi *non vuoti* e complementari l'uno dell'altro (per costruzione!) dunque tali che $\eta^{-1}(0) \cup \eta^{-1}(1) = E$ e $\eta^{-1}(0) \cap \eta^{-1}(1) = \emptyset$, così è anche $\eta^{-1}(0) \neq \eta^{-1}(0)$.

In conclusione, $\big\{E_0 := \eta^{-1}(0)\,, E_1 := \eta^{-1}(1)\big\}$ è una partizione di E, e più precisamente $\big\{E_0\,, E_1\big\} \in \Pi_2(E)$. Questo definisce quindi una funzione del tipo richiesto

$$\Omega \ : \ \underline{2}^E \setminus \big\{\eta_{\mathbf{0}}\,, \eta_{\mathbf{1}}\big\} \longrightarrow \Pi_2(E) \ , \quad \eta \mapsto \Omega(\eta) := \big\{E_0 := \eta^{-1}(0)\,, E_1 := \eta^{-1}(1)\big\}$$

Dimostriamo ora dare che tale Ω è invertibile, costruendone esplicitamente l'inversa. A tal fine, per ogni $\pi := \big\{E_0\,, E_1\big\} \in \Pi_2(E)$ consideriamo la funzione caratteristica in E

$$\eta_\pi : E \longrightarrow \underline{2} \ , \quad e \mapsto \eta_\pi(e) := \begin{cases} 0 \ , & \forall\, e \in E_0 \\ 1 \ , & \forall\, e \in E_1 \end{cases} \qquad \forall\ e \in E \tag{5}$$

Si noti che η_π è effettivamente una funzione ben definita (!) proprio perché π è una partizione di E: inoltre, siccome per ipotesi in $\pi := \{E_0, E_1\}$ abbiamo $E_0 \neq \emptyset$ e $E_1 \neq \emptyset$, per costruzione abbiamo anche $\eta_\pi \neq \eta_{\mathbf{1}}$ e $\eta_\pi \neq \eta_{\mathbf{0}}$. Pertanto la (5) ci dà una ben definita funzione

$$\Omega' : \Pi_2(E) \longrightarrow \underline{2}^E \setminus \{\eta_{\mathbf{0}}, \eta_{\mathbf{1}}\} \quad , \qquad \pi \mapsto \Omega'(\pi) := \eta_\pi$$

A questo punto un semplice calcolo diretto mostra che $\Omega' \circ \Omega = \mathrm{id}_{\underline{2}^E \setminus \{\eta_{\mathbf{0}}, \eta_{\mathbf{1}}\}}$ — perché $\big(\Omega' \circ \Omega\big)(\eta) = \eta$ per ogni $\eta \in \underline{2}^E \setminus \{\eta_{\mathbf{0}}, \eta_{\mathbf{1}}\}$ — e analogamente che $\Omega \circ \Omega' = \mathrm{id}_{\Pi_2(E)}$ — perché $\big(\Omega \circ \Omega'\big)(\pi) = \pi$ per ogni $\pi \in \Pi_2(E)$; possiamo quindi concludere che Ω' è la funzione inversa di Ω, e dunque Ω stessa è invertibile, q.e.d.

[2] — Come richiesto procediamo per induzione semplice, osservando che nel caso in esame la *base* dell'induzione è il caso $n = 3$.

Base dell'Induzione: $n = 3$ — Dobbiamo dimostrare che vale l'enunciato per $n = 3$, cioè che vale la disuguaglianza

$$2 \cdot 3^3 - 5 \; > \; 5 \cdot 2^3 + 2 \tag{6}$$

Ma questa è soltanto una mera verifica: infatti, il membro di sinistra in (6) è

$$2 \cdot 3^3 - 5 \; = \; 2 \cdot 27 - 5 \; = \; 54 - 5 \; = \; 49$$

mentre il membro di destra è

$$5 \cdot 2^3 + 2 \; = \; 5 \cdot 8 + 2 \; = \; 40 + 2 \; = \; 42$$

e siccome effettivamente $49 > 42$ concludamo che la (6) è effettivamente valida, q.e.d.

Passo Induttivo: $n \implies n+1 \;\big(\forall\, n \geq 3\big)$ — Dobbiamo dimostrare che, per ogni $n \geq 3$, *se* vale l'enunciato per n, cioè vale la disuguaglianza

Ipotesi Induttiva: $\qquad 2 \cdot 3^n - 5 \; > \; 5 \cdot 2^n + 2 \tag{7}$

allora vale anche l'enunciato per $n+1$, cioè vale la disuguaglianza

Tesi Induttiva: $\qquad 2 \cdot 3^{n+1} - 5 \; > \; 5 \cdot 2^{n+1} + 2 \tag{8}$

Procediamo quindi a ottenere la (8) sfruttando la (7). I calcoli diretti, operando opportune maggiorazioni successive, ci danno

$$\begin{aligned} 2 \cdot 3^{n+1} - 5 \; &= \; 2 \cdot 3^n \cdot 3 - 5 \; = \; 2 \cdot 3^n \cdot (2+1) - 5 \; = \; 2 \cdot 3^n \cdot 2 + 2 \cdot 3^n - 5 \; \overset{\circledast}{>} \\ &\overset{\circledast}{>} 2 \cdot 3^n \cdot 2 + 5 \cdot 2^n + 2 \; = \; 4 \cdot 3^n + 5 \cdot 2^n - 5 \cdot 2^{n+1} + 5 \cdot 2^{n+1} + 2 \; = \\ &= \; 4 \cdot 3^n + 5 \cdot 2^n \cdot (1-2) + 5 \cdot 2^{n+1} + 2 \; = \; 4 \cdot 3^n - 5 \cdot 2^n + 5 \cdot 2^{n+1} + 2 \; \overset{\circledcirc}{>} \\ &\overset{\circledcirc}{>} 5 \cdot 2^{n+1} + 2 \end{aligned}$$

dunque in conclusione $2 \cdot 3^{n+1} - 5 \; > \; 5 \cdot 2^{n+1} + 2$, cioè vale la (8). In questo procedimento, per la maggiorazione "$\overset{\circledast}{>}$" abbiamo sfruttato l'ipotesi induttiva (7) mentre la

maggiorazione "$\overset{\circledcirc}{>}$" segue subito dalla disuguaglianza

$$4 \cdot 3^n - 5 \cdot 2^n \ > \ 0 \qquad\qquad \forall \ n \geq 1$$

la quale a sua volta può essere dimostrata anch'essa per induzione semplice, oppure più velocemente può essere ottenuta come segue: per ogni $n \geq 1$ si ha

$$4 \cdot 3^n - 5 \cdot 2^n \ > \ 0 \iff 4 \cdot 3^n \ > \ 5 \cdot 2^n \iff \big(3/2\big)^n \ > \ 5/4 \iff 3/2 \ > \ 5/4$$

e infine osserviamo che l'ultima disuguaglianza è valida visto che $3/2 = 6/4 > 5/4$.

[3] — Rispondiamo ai vari quesiti uno alla volta.

(a) Per definizione G' è un sottogruppo di G, perciò dobbiamo soltanto dimostrare che è *normale*, cioè — usando una delle varie caratterizzazioni della "normalità" di un sottogruppo — che si ha

$$g\,G'\,g^{-1} \ \subseteq \ G' \qquad \forall \ g \in G \tag{9}$$

Ora, la (9) si può ottenere come caso particolare di *(b)*: infatti per ogni $g \in G$ abbiamo $g\,G'\,g^{-1} = \gamma_g\big(G'\big)$ dove γ_g è la funzione

$$\gamma_g : G \longrightarrow G \quad , \qquad y \mapsto \gamma_g(y) := g\,y\,g^{-1} \qquad \big(\forall \ y \in G\big)$$

e un calcolo immediato mostra che $\gamma_g \in \mathit{End}\,(G)$, cioè tale γ_g è un endomorfismo di G: infatti $\gamma_g\big(y'\,y''\big) = g\,\big(y'\,y''\big)\,g^{-1} = g\,y'\,g\,g^{-1}\,y''\,g^{-1} = \gamma_g\big(y''\big)\,\gamma_g\big(y''\big)$ per $y', y'' \in G$.

In alternativa, possiamo dimostrare direttamente la (9) come segue. Dato che G' è generato dagli elementi $[\,h\,,k\,] := h\,k\,h^{-1}\,k^{-1}$, abbiamo che la (9) è equivalente a

$$g\,[\,h\,,k\,]\,g^{-1} \ \in \ G' \qquad\qquad \forall \ g\,,h\,,k \in G$$

e quindi andiamo a dimostrare che quest'ultima condizione è effettivamente soddisfatta: questosegue subito dal calcolo diretto, che ci dà (per ogni $g\,,h\,,k \in G$)

$$\begin{aligned} g\,[\,h\,,k\,]\,g^{-1} \ &= \ g\,h\,k\,h^{-1}\,k^{-1}\,g^{-1} \ = \ g\,h\,g^{-1}\,g\,k\,g^{-1}\,g\,h^{-1}\,g^{-1}\,g\,k^{-1}\,g^{-1} \ = \\ &= \ g\,h\,g^{-1}\,g\,k\,g^{-1}\,\big(g\,h\,g^{-1}\big)^{-1}\big(g\,k\,g^{-1}\big)^{-1} \ = \ \Big[\,g\,h\,g^{-1}\,,\,g\,k\,g^{-1}\Big] \ \in \ G' \end{aligned}$$

Si noti che, in definitiva, in questo calcolo abbiamo ottenuto che

$$\gamma_g\big([\,h\,,k\,]\big) \ = \ \big[\,\gamma_g(h)\,,\gamma_g(k)\,\big] \qquad\qquad \forall \ g\,,h\,,k \in G \tag{10}$$

che a sua volta segue direttamente dal fatto che ogni γ_g è un (endo)morfismo di G.

(b) Questo risultato generalizza il punto *(a)*, e si ottiene estendendo il ragionamento usato in quel caso. Dunque, dovendo dimostrare che per ogni $\phi \in \mathit{End}\,(G)$ si ha

$$\phi\big(G'\big) \ \subseteq \ G' \qquad \forall \ g \in G$$

cominciamo osservando che tale proprietà è equivalente (per ogni $\phi \in \mathit{End}\,(G)$) a

$$\phi\big([\,h\,,k\,]\big) \ \in \ G' \qquad\qquad \forall \ g\,,h\,,k \in G$$

Ma questo segue subito dalla proprietà

$$\phi\big([\,h\,,k\,]\big) \;=\; \big[\,\phi(h)\,,\,\phi(k)\,\big] \qquad\qquad \forall\;\; h\,,k \in G \tag{11}$$

che è la diretta generalizzazione della (10), e si ottiene allo stesso modo tramite un calcolo esplicito, precisamente (per ogni $g\,,h\,,k \in G$)

$$\begin{aligned}\phi\big([\,h\,,k\,]\big) \;=\; \phi\big(\,h\,k\,h^{-1}\,k^{-1}\big) \;=\; \phi(h)\,\phi(k)\,\phi\big(h^{-1}\big)\,\phi\big(k^{-1}\big) \;= \\ =\; \phi(h)\,\phi(k)\,\phi(h)^{-1}\phi(k)^{-1} \;=\; \big[\,\phi(h)\,,\,\phi(k)\,\big] \;\in\; G'\end{aligned}$$

(c) Osserviamo che un gruppo Γ è abeliano (cioè commutativo) se e soltanto se si ha $x\,y \,=\, y\,x$ per ogni $x\,,y \in \Gamma\,,$ e questa condizione è equivalente a

$$[\,x\,,\,y\,] \;=\; 1_{_G} \qquad\qquad \forall\;\; x\,,\,y \in \Gamma \tag{12}$$

dove $1_{_G}$ indica l'elemento neutro del gruppo Γ. Dimostriamo allora che vale la (12) per il gruppo $\Gamma := G\Big/G'$. Indicando con $\overline{z} := z\,G'$ la classe laterale (sinistra, ma uguale alla destra, perché il sottogruppo G' è normale) modulo G' di un qualsiasi elemento $z \in G\,,$ il calcolo diretto ci dà

$$\big[\,\overline{x}\,,\,\overline{y}\,\big] \;:=\; \overline{x}\,\overline{y}\,\overline{x}^{\,-1}\overline{y}^{\,-1} \;=\; \overline{x\,y\,x^{-1}y^{-1}} \;=\; \overline{[\,x\,,\,y\,]} \;=\; \overline{1_{_G}} \qquad\qquad \forall\;\; \overline{x}\,,\,\overline{y} \in G\Big/G'$$

— dove l'ultima uguaglianza segue dal fatto che $[\,x\,,\,y\,] \in G'$, per definizione — che è proprio la (12) per il gruppo $\Gamma := G\Big/G'$ in quanto $\overline{1_{_G}}$ è l'elemento neutro di $G\Big/G'$.

[4] — Osserviamo che un anello R è commutativo se e soltanto se si ha $x\,y \,=\, y\,x$ per ogni $x'\,,x'' \in R\,,$ e questa condizione è equivalente a

$$x'\,,\,x'' \,-\, x''\,x' \;=\; 0_{_R} \qquad\qquad \forall\;\; x'\,,\,x'' \in R \tag{13}$$

dove $0_{_R}$ indica l'elemento neutro per la somma nell'anello R. Dimostriamo allora che vale la (13) per l'anello quoziente $R := A\Big/I\,,$ nel quale indichiamo con $\overline{z} := z + I$ la classe laterale modulo I di un qualsiasi elemento $z \in R$. Tramite calcolo diretto si ottiene

$$\overline{x'}\,\overline{x''} \,-\, \overline{x''}\,\overline{x'} \;:=\; \overline{x'}\,\overline{x''} \,-\, \overline{x''}\,\overline{x'} \;=\; \overline{x'\,x'' \,-\, x''\,x'} \;=\; \overline{0_{_A}} \qquad\qquad \forall\;\; \overline{x'}\,,\,\overline{x''} \in A\Big/I$$

— dove l'ultima uguaglianza segue da $\big(x'\,x'' \,-\, x''\,x'\big) \,\in\, I\,,$ per definizione — che è proprio la (13) per $R := A\Big/I$ dato che $\overline{0_{_A}}$ è l'elemento neutro per la somma in $A\Big/I\,.$

[5] — Sappiamo già che l'anello quoziente $D\Big/(d\,)$ è un commutativo e unitario. Per dimostrare che è un campo ci resta soltanto da provare che ogni elemento diverso da zero ha un inverso, cioè che

$$\forall\;\; \overline{a} \in D\Big/(d\,) \setminus \big\{\,\overline{0}\,\big\} \;\;,\quad \exists\,\overline{a'} \in D\Big/(d\,) \;\;:\;\; \overline{a}\,\overline{a'} \,=\, \overline{1} \tag{14}$$

Ora, osserviamo che

$$\overline{a}\,\overline{a'} = \overline{1} \iff \overline{a\,a'} = \overline{1} \iff a\,a' \equiv 1 \mod (d) \iff \big(a\,a' - 1\big) \in (d) \iff$$
$$\iff \exists\ b' \in D\ :\ a\,a' - 1 = d\,b' \iff \text{l'e.d. } a\,x + d\,y = 1 \text{ in } D \text{ ha soluzioni}$$

pertanto otteniamo che dimostrare la (14) equivale a dimostrare che

$$\forall\ \overline{a} \in D\Big/(d) \setminus \big\{\,\overline{0}\,\big\}\ ,\quad \exists \text{ soluzioni dell'equazione diofantea } a\,x + d\,y = 1 \tag{15}$$

Ora, per ipotesi $\overline{a} \neq \overline{0}$, che equivale a $a \notin (d) := D\,d$, cioè *a non è multiplo di d*; quest'ultima condizione, dato che d è irriducibile, equivale a dire che $\text{M.C.D.}(a\,,d) = 1$ — si noti che esiste senz'altro il $\text{M.C.D.}(a\,,d)$, perché D è un dominio euclideo.

Sempre perché D è un dominio euclideo, il $\text{M.C.D.}(a\,,d)$ può essere espresso con una identità di Bézout, dunque esistono $r\,,s \in D$ tali che $\text{M.C.D.}(a\,,d) = a\,r + d\,s$. Insieme a $\text{M.C.D.}(a\,,d) = 1$ questo ci dà

$$\exists\ r\,,s \in D\ :\ a\,r + d\,s = 1$$

e ciò significa che per l'equazione diofantea in (15) c'è almeno la soluzione $(x, y) := (r, s)$.

[6] — Ricordiamo che l'anello degli interi di Gauss $\mathbb{Z}[\,i\,]$ è *euclideo*, con valutazione $v : \mathbb{Z}[\,i\,] \longrightarrow \mathbb{N}$ definita da $v(a + i\,b) := a^2 + b^2$ per ogni $a + i\,b \in \mathbb{Z}[\,i\,]$. In particolare tale valutazione è *moltiplicativa*, cioè si ha $v(\alpha\,\beta) = v(\alpha)\,v(\beta)$ per ogni $\alpha\,,\beta \in \mathbb{Z}[\,i\,]$.

Da questo fatto segue che si può usare l'algoritmo delle divisioni successive per calcolare il M.C.D. tra due qualunque elementi in $\mathbb{Z}[\,i\,]$, nonché una identità di Bézout per tale M.C.D.; questo a sua volta permette anche di risolvere ogni equazione diofantea. In particolare, da questo segue anche che ogni ideale $\mathbb{Z}[\,i\,]$ è principale, e se è generato da due elementi sarà anche generato (singolarmente) dal M.C.D. tra tali elementi, che potremo calcolare esplicitamente come osservato poc'anzi.

(a) Applichiamo ora tali idee generali al caso in esame. Iniziamo effettuando il calcolo di $\text{M.C.D.}\big(1-3\,i\,,\,5+i\big)$ tramite l'algoritmo euclideo delle divisioni successive. I calcoli espliciti sono

$$\begin{aligned} 1 - 3\,i &= (5+i)\,0 + (1-3\,i\big) && \text{con}\quad v(1-3\,i) = 10 < 26 = v(5+i) \\ 5 + i &= (1-3\,i)\,i + 2 && \text{con}\quad v(2) = 4 < 10 = v(1-3\,i) \\ 1 - 3\,i &= 2\,(-i) + (1-i) && \text{con}\quad v(1-i) = 2 < 4 = v(2) \\ 2 &= (1-i)\,(1+i) + 0 \end{aligned}$$

da cui otteniamo che $\text{M.C.D.}\big(1-3\,i\,,-2+7\,i\big) \sim (1-i)$; si noti che le varie divisioni con resto qui sopra sono ottenute tramite i seguenti calcoli in $\mathbb{C}$:

$$(1-3\,i)\,(5+i)^{-1} = \frac{(1-3\,i)\,(5-i)}{v(5+i)} = \frac{2-16\,i}{26} = \left(\frac{1}{13} - \frac{3}{13}\,i\right) + (0+0\,i)\ ,$$
$$(1-3\,i) - (5+i)\,0 = (1-3\,i)$$

$$(5+i)\,(1-3\,i)^{-1} \;=\; \frac{(5+i)\,(1+3\,i)}{v(1-3\,i)} \;=\; \frac{2+16\,i}{10} \;=\; \left(\frac{1}{5}+\frac{3}{5}\,i\right) + i \;\;,$$
$$(5+i) \;-\; (1-3\,i)\,i \;=\; 2$$
$$(1-3\,i)\,2^{-1} \;=\; \frac{(1-3\,i)\,2}{v(2)} \;=\; \frac{2-6\,i}{4} \;=\; \left(\frac{1}{2}-\frac{1}{2}\,i\right) - i \;\;,$$
$$(1-3\,i) \;-\; 2\,(-i) \;=\; (1-i)$$
$$2\,(1-i)^{-1} \;=\; \frac{2\,(1+i)}{v(1-i)} \;=\; \frac{2+2\,i}{2} \;=\; 1+i \;\;,$$
$$2 \;-\; (1-i)\,(1+i) \;=\; 0$$

Si noti anche che in alcuni casi si può fare la divisione in modo diverso (ma altrettanto valido): ad esempio, siccome si ha anche

$$(1-3\,i)\,2^{-1} \;=\; \frac{(1-3\,i)\,2}{v(2)} \;=\; \frac{2-6\,i}{4} \;=\; \left(\frac{1}{2}+\frac{1}{2}\,i\right) - 2\,i \;\;,$$
$$(1-3\,i) \;-\; 2\,(-2\,i) \;=\; (1+i)$$

da cui otteniamo la divisione euclidea di $(1-3\,i)$ per 2 nella forma

$$1-3\,i \;=\; 2\,(-2\,i) \;+\; (1+i) \qquad\qquad \text{con} \quad v(1+i)=2<4=v(2)$$

A seguire poi la successiva e ultima divisione nell'algoritmo sarà (ovviamente)

$$2 \;=\; (1+i)\,(1-i) \;+\; 0$$

In ogni caso, abbiamo trovato che $\text{M.C.D.}\big(1-3\,i\,,-2+7\,i\big) \sim (1-i)$: per quanto già osservato in premessa, questo significa che $d \,=\, \text{M.C.D.}\big(1-3\,i\,,\,5+i\big) \,=\, (1-i)$ è un generatore dell'ideale $I := \big(1-3\,i\,,\,5+i\big)$ generato dai due elementi $1-3\,i$ e $5+i$. Analogamente, anche $(1+i)$ è a sua volta un generatore di I, il che concorda col fatto che $(1+i) \sim (1-i)$, in quanto $(1+i) = (1-i)\,i$ dove il fattore i è invertibile in $\mathbb{Z}[\,i\,]$.

(b) Dobbiamo trovare un'espressione della forma $d \,=\, r\,(1-3\,i) \,+\, s\,(5+i)$ per il generatore d dell'ideale $I := \big(1-3\,i\,,\,5+i\big)$ trovato in risposta al punto *(a)*, osserviamo — come spiegato in premessa — che ciò significa trovare una identità di Bézout per $d \,:=\, \text{M.C.D.}\big(1-3\,i\,,\,5+i\big)$. A tal fine consideriamo l'opzione $d = (1-i)$ e riprendiamo le formule per le divisioni trovate al punto *(a)* con l'algoritmo euclideo, precisamente

$$\begin{aligned} 1-3\,i \;&=\; (5+i)\,0 \;+\; (1-3\,i\big) \\ 5+i \;&=\; (1-3\,i)\,i \,+\, 2 \\ 1-3\,i \;&=\; 2\,(-i) \,+\, (1-i) \\ 2 \;&=\; (1-i)\,(1+i) \,+\, 0 \end{aligned}$$

Scartando l'ultima formula, in ciascuna delle altre riscriviamo il resto in funzione degli altri termini, ottenendo

$$(1-3\,i\big) \overset{(1)}{=} 1-3\,i + (5+i)\,(-0) \;\;,\quad 2 \overset{(2)}{=} 5+i + (1-3\,i)\,(-i) \;\;,\quad (1-i) \overset{(3)}{=} 1-3\,i + 2\,(+i)$$

e poi sfruttando tali identità otteniamo, per sostituzioni successive, la catena di identità

$$\begin{aligned}(1-i\,) \overset{(3)}{=} (1-3\,i\,) + 2\,(+i\,) \overset{(2)}{=} (1-3\,i\,) + \big((5+i\,) + (1-3\,i\,)\,(-i\,)\big)\,(+i\,) \;\; = \\ = \;\; (5+i\,)\,i + (1-3\,i\,)\,2 \overset{(1)}{=} (5+i\,)\,i + \big((5+i\,)\,0 + (1-3\,i\,)\big)\,2 \;\; = \\ = \;\; (1-3\,i\,)\,2 + (5+i\,)\,i\end{aligned}$$

— dove l'ultimo passaggio di fatto è superfluo — da cui otteniamo in definitiva l'identità

$$(1-i\,) \;\; = \;\; 2\,(1-3\,i\,)\,2 + i\,(5+i\,)$$

che è appunto un'identità di Bézout come richiesto nella forma

$$(1-i\,) \;\; = \;\; r\,(1-3\,i\,) + s\,(5+i\,) \qquad \text{con} \quad r=2\,, \;\; s=i\,.$$

Analogamente possiamo trovare un'identità di Bézout per il generatore $d = (1+i\,)$.

Si noti che in ogni caso la soluzione *non è unica*, in quanto facendo i calcoli in modo un po' diverso si possono ottenere altre identità di Bézout per il generatore d considerato. A titolo di (ulteriore) esempio, svolgendo l'algoritmo delle divisioni successive con divisioni un po' diverse si può trovare

$$\begin{aligned} 1-3\,i \;\; &= \;\; (5+i\,)\,0 + (1-3\,i\,\big) && \text{con} \quad v(1-3\,i\,) = 10 < 26 = v(5+i\,) \\ 5+i \;\; &= \;\; (1-3\,i\,)\,2\,i + (-1-i\,) && \text{con} \quad v(-1-i\,) = 4 < 10 = v(1-3\,i\,) \\ 1-3\,i \;\; &= \;\; (-1-i\,)\,(1+2\,i\,) + 0 \end{aligned}$$

da cui otteniamo che $\text{M.C.D.}\big(1-3\,i\,,\, 5+i\big) \sim (-1-i\,)$ e poi — per sostituzioni successive — l'identità di Bézout $(-1-i\,) = r\,(1-3\,i\,) + s\,(5+i\,)$ con $r=(-2i\,)$ e $s=1$.