CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2023–2024

Esame scritto del 17 Giugno 2024 — Sessione Estiva, I appello

N.B.: compilare il compito in modo sintetico ma **esauriente**, *spiegando chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.*

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

[1] — Si considerino l'insieme $\mathbf{V}_I := \{ \text{parole della lingua italiana} \}$ e l'insieme di lettere $\Lambda := \{F, E, R, N\}$. Si consideri poi in $\mathbf{V}_I$ la relazione $\rtimes$ definita da

$$\mathcal{P}_1 \rtimes \mathcal{P}_2 \iff \begin{array}{c} \text{“ la parola } \mathcal{P}_1 \text{ contiene al più tante lettere} \\ \text{di } \Lambda \text{ quante ne contiene la parola } \mathcal{P}_2 \text{ ”} \end{array}$$

dove le lettere, se compaiono più di una volta, vanno contate una volta sola (dunque *senza "molteplicità"*).

(a) Si dimostri che la relazione $\rtimes$ è una relazione di preordine in $\mathbf{V}_I$.

(b) Si dimostri che la relazione $\bowtie := \rtimes \cap \rtimes^{-1}$ è una relazione di equivalenza in $\mathbf{V}_I$.

(c) Determinare la cardinalità dell'insieme quoziente $\left| \mathbf{V}_I \Big/ \bowtie \right|$.

(d) Descrivere esplicitamente ciascuna classe di $\bowtie$–equivalenza in $\mathbf{V}_I$.

[2] — Dato un anello unitario A, si consideri l'anello unitario $Mat_{3\times 3}(A)$ delle matrici 3×3 a coefficienti in A (rispetto all'ordinaria somma tra matrici e al prodotto righe per colonne) e il suo gruppo degli elementi invertibili

$$GL_3(A) := \left\{ M \in Mat_{3\times 3}(A) \,\middle|\, \exists\, M^{-1} \in Mat_{3\times 3}(A) \right\}$$

Si consideri poi in $Mat_{3\times 3}(A)$ il sottoinsieme $U_3^+(A) := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, a, b, c \in A \right\}$.

(a) Dimostrare che $U_3^+(A)$ è sottogruppo di $GL_3(A)$.

(b) Calcolare esplicitamente il centro di $U_3^+(A)$, cioè il sottoinsieme

$$Z\big(U_3^+(A)\big) := \left\{ \zeta \in U_3^+(A) \,\middle|\, \zeta\, g = g\, \zeta \;\forall\, g \in U_3^+(A) \right\}$$

(c) Dimostrare che $Z\big(U_3^+(A)\big) \trianglelefteq U_3^+(A)$.

(d) Dimostrare che il gruppo quoziente $U_3^+(A) \Big/ Z\big(U_3^+(A)\big)$ è isomorfo al gruppo prodotto diretto $\big(A\,;+\big) \times \big(A\,;+\big)$.

(continua...) $\Longrightarrow$

[3] — Determinare l'insieme di tutte le soluzioni in $\mathbb{Z}$ del sistema di congruenze lineari

$$\begin{cases} 361\,x \equiv -78 & (\text{mod } 5) \\ -24\,x \equiv 6285^{930145} & (\text{mod } 7) \end{cases}$$

[4] — Siano G ed H due gruppi finiti con ordini coprimi, cioè $\text{M.C.D.}\big(|G|\,,|H|\big) = 1$. Determinare tutti i morfismi da G ad H e tutti i morfismi da H a G.

[5] — Dato un insieme E, per ogni anello A si consideri la struttura canonica di anello nell'insieme A^E di tutte le funzioni da E ad A. Inoltre, per ogni morfismo di anelli $\phi : A_1 \longrightarrow A_2$ si consideri la funzione $\phi^{(E)} : A_1^E \longrightarrow A_2^E$ data da $\phi^{(E)}(f) := \phi \circ f \ \big(\, f \in A_1^E \,\big)$.
Dimostrare che:

(a) ogni funzione $\phi^{(E)} : A_1^E \longrightarrow A_2^E$ come sopra è un morfismo di anelli;

(b) per ogni anello A si ha $id_A^{(E)} = id_{A^E}$;

(c) per ogni sequenza di morfismi $A_1 \xrightarrow{\phi_1} A_2 \xrightarrow{\phi_2} A_3$ si ha $(\phi_2 \circ \phi_1)^{(E)} = \phi_2^{(E)} \circ \phi_1^{(E)}$;

(d) se $\phi : A_1 \longrightarrow A_2$ è un *iso*morfismo, allora $\phi^{(E)} : A_1^E \longrightarrow A_2^E$ è un *iso*morfismo.

[6] — Sia $\mathbb{Z}\big[\sqrt{-13}\,\big] := \big\{\, \zeta \in \mathbb{C} \;\big|\; \exists\, a, b \in \mathbb{Z} : \zeta = a + b\sqrt{-13} \,\big\}$.

(a) Dimostrare che $\mathbb{Z}\big[\sqrt{-13}\,\big]$ è un sottoanello di $\mathbb{C}$.

(b) Determinare se $\mathbb{Z}\big[\sqrt{-13}\,\big]$ sia un dominio a fattorizzazione.

(c) Determinare se $\mathbb{Z}\big[\sqrt{-13}\,\big]$ sia un dominio a fattorizzazione unica.

(d) Determinare se $\mathbb{Z}\big[\sqrt{-13}\,\big]$ sia un dominio a ideali principali.

(e) Determinare se $\mathbb{Z}\big[\sqrt{-13}\,\big]$ sia un dominio euclideo.

(f) Determinare se esista un elemento di $\mathbb{Z}\big[\sqrt{-13}\,\big]$ che ammetta una fattorizzazione in elementi irriducibili che però *non* siano primi.

ALGEBRA 1 — 1° APPELLO 2023/2024 — 17/06/2024

— ∘ —

1 $V_I := \{\text{parole dell'italiano}\}$

$\Lambda := \{F, E, R, N\}$

$\asymp$ la relazione in V_I data da $(\forall P_1, P_2 \in V_I)$

$P_1 \asymp P_2 \iff P_1$ contiene al più tante lettere di Λ quante ne contiene P_2

Th: (a) $\asymp$ è un preordine in V_I.

(b) $\mathcal{N} := \asymp \cap \asymp^{-1}$ è una equivalenza in V_I

(c) Determinare la cardinalità $|V_I/\mathcal{N}|$

(d) Descrivere ciascuna classe di $\mathcal{N}$-equivalenza.

Svolgimento: (a) definiamo la funzione

$\lambda : V_I \longrightarrow \mathcal{P}(\{F, E, R, N\})$ data da

$\lambda(P) := \{\text{lettere di } P\} \cap \{F, E, R, N\} \quad \forall P \in V_I$

N.B.: tale λ è suriettiva: ad esempio, si ha

$\{F, E, R, N\} = \lambda(\text{FRENO}) = \lambda(\text{ANFORE})$

$\{F, E, R\} = \lambda(\text{FERRO}) = \lambda(\text{FRETTA})$

$\{E, R, N\} = \lambda(\text{ERNIA}) = \lambda(\text{RANE})$

$\{F, R, N\} = \lambda(\text{FORNI}) = \lambda(\text{INFRADITO})$

$\{F, E, N\} = \lambda(\text{FIENO}) = \lambda(\text{GONFIE})$

$\{F, E\} = \lambda(\text{FETTA})$, $\{R, N\} = \lambda(\text{RANA})$, $\{F, R\} = \lambda(\text{FRUTTA})$

$\{E, N\} = \lambda(\text{PIENO})$, $\{F, N\} = \lambda(\text{TONFO})$, $\{E, R\} = \lambda(\text{ERRORE})$

ecc. ecc. ecc.

Poi consideriamo la funzione

$$\ell : V_I \longrightarrow \mathbb{N}, \quad P \longmapsto |\ell(P)|$$

NOTA che $Im(\ell) = \{0, 1, 2, 3, 4\}$

ALLORA la relazione $\asymp$ in $\mathcal{P}V_I$ è descritta da

$$P_1 \asymp P_2 \iff \ell(P_1) \leq \ell(P_2) \quad (\forall P_1, P_2 \in V_I)$$
in $\mathbb{N}$

ORA:

(R) $\forall P \in V_I$ si ha $\ell(P) = \ell(P)$,
quindi è $P \asymp P$ ovvero $\asymp$ è riflessiva

(T) $\forall P_1, P_2, P_3 \in V_I$ tali che
$P_1 \asymp P_2$ e $P_2 \asymp P_3$, si ha
$\ell(P_1) \leq \ell(P_2)$ e $\ell(P_2) \leq \ell(P_3)$
quindi è $\ell(P_1) \leq \ell(P_3)$ in $\mathbb{N}$
perciò $P_1 \asymp P_3$ ovvero $\asymp$ è transitiva

QUINDI $\asymp$ è riflessiva e transitiva
CIOÈ $\asymp$ è un preordine, $\Rightarrow$ (a) è (OK)

NOTA: (1) $\asymp$ NON è una equivalenza, perché
ad esempio
$\ell(\text{FIENO}) = 3$, $\ell(\text{FRENO}) = 4$ $\Rightarrow$
$\Rightarrow$ FIENO $\asymp$ FRENO
ma FRENO $\not\asymp$ FIENO
QUINDI $\asymp$ NON è simmetrica

(2) $\not\asymp$ NON è un ordine, perché ad esempio

$\ell(\text{FRENO}) = 4 = \ell(\text{ANFORE}) \Rightarrow$

$\Rightarrow$ FRENO $\not\asymp$ ANFORE & ANFORE $\not\asymp$ FRENO

e però FRENO $\neq$ ANFORE

Allo stesso modo, è

$\ell(\text{RANE}) = 3 = \ell(\text{FORNI}) \Rightarrow$

$\Rightarrow$ RANE $\not\asymp$ FORNI & FORNI $\not\asymp$ RANE

e però RANE $\neq$ FORNI

QUINDI $\not\asymp$ NON è antisimmetrica.

(R) Da teoria generale segue che

$\not\asymp$ è preordine $\Rightarrow$ $\not\asymp^{-1}$ è preordine

e anche

α, β preordini $\Rightarrow$ $\alpha \cap \beta$ preordine

che per $\alpha := \not\asymp$ e $\beta := \not\asymp^{-1}$ ci dà che

$\not\asymp \cap \not\asymp^{-1}$ è un preordine, q.e.d.

OPPURE, (ri)dimostrandolo a mano...

(R) $\forall P \in V_I$ si ha $\ell(P) = \ell(P)$, $\Rightarrow$

$\Rightarrow P \not\asymp P \Rightarrow P \not\asymp^{-1} P$

$\Downarrow$

$(P \not\asymp P) \wedge (P \not\asymp^{-1} P) \Rightarrow P (\not\asymp \cap \not\asymp^{-1}) P$ (OK)

così $\not\asymp \cap \not\asymp^{-1}$ è riflessiva.

④ $\forall P, P', P'' \in V_I$ ~~n° lati~~

$P'(\mathcal{A} \cap \mathcal{A}^{-1}) P'$

$P'(\mathcal{A} \cap \mathcal{A}^{-1}) P'$

INOLTRE, $\forall$ relazione ϱ si ha sempre che $\varrho \cap \varrho^{-1}$ è simmetrica

perché

$$a(\varrho \cap \varrho^{-1}) b \iff (a \varrho b) \wedge (a \varrho^{-1} b) \iff$$

$$\iff (a \varrho b) \wedge (b \varrho a) \iff (b \varrho a) \wedge (a \varrho b) \iff$$

$$\iff (b \varrho a) \wedge (b \varrho^{-1} a) \iff b(\varrho \cap \varrho^{-1}) a$$

QUINDI per $\varrho := \mathcal{A}$ troviamo che

$\mathcal{A} \cap \mathcal{A}^{-1}$ è simmetrica

MA siccome $\mathcal{A} \cap \mathcal{A}^{-1}$ è anche preordine (vedi sopra), si conclude che è un'equivalenza.

OPPURE

Con approccio diretto, osserviamo che

$\forall P', P'' \in V_I$ si ha

$$P'(\mathcal{A} \cap \mathcal{A}^{-1}) P'' \iff (P' \mathcal{A} P'') \wedge (P' \mathcal{A}^{-1} P'') \iff$$

$$\iff (P' \mathcal{A} P'') \wedge (P'' \mathcal{A} P') \iff$$

$$\iff (\ell(P') \leq \ell(P'')) \wedge (\ell(P'') \leq \ell(P')) \iff$$

$$\iff \ell(P') = \ell(P'')$$

così è $P'(\mathcal{H} \cap \mathcal{H}^{-1}) P'' \iff \ell(P') = \ell(P'')$

$\forall\, P', P'' \in V_I$, perciò

(*) $\mathcal{H} \cap \mathcal{H}^{-1} = \rho_\ell$:= relazione in V_I associata alla funzione ℓ

e sappiamo che ρ_ℓ è una equivalenza, perciò dalla (*) segue che $\mathcal{H} \cap \mathcal{H}^{-1}$ è equivalenza (OK)

(c) da $\mathcal{H} \cap \mathcal{H}^{-1} = \rho_\ell$ segue che

$$V_I / \mathcal{H} \cap \mathcal{H}^{-1} = V_I / \rho_\ell \underset{\ell_*}{\cong} \mathrm{Im}(\ell)$$

↳ TEOR. FONDAMENTALE delle APPLICAZIONI

perciò è

$$\left| V / \mathcal{H} \cap \mathcal{H}^{-1} \right| = \left| V / \rho_\ell \right| = \left| \mathrm{Im}(\ell) \right| =$$

$$= \left| \{0, 1, 2, 3, 4\} \right| = 5$$

cioè $\left| V_I / \mathcal{H} \cap \mathcal{H}^{-1} \right| = 5$ (OK)

(d) Da $\mathcal{H} \cap \mathcal{H}^{-1} = \rho_\ell$ segue che le $\mathcal{H}$-classi di $\mathcal{H}$-equivalenza in V_I sono esattamente le classi di equivalenza per ρ_ℓ, cioè

$$[P]_{\mathcal{H}} = [P]_{\rho_\ell} = \ell^{-1}(\ell(P)) = \{P' \in V_I \mid \ell(P') = \ell(P)\}$$

$\forall\, P \in V_I$

D'altra parte, la biiezione

$$V_I/\varrho_\ell \xrightarrow{\ell^*} \mathrm{Im}(\ell) = \{0,1,2,3,4\}$$

ci dice che le ϱ_ℓ-classi corrispondono biiettivamente ai 5 possibili valori della funzione $\ell : V_I \longrightarrow \mathbb{N}$, così ci sono in tutto 5 classi, cioè

$$V_I/\mathcal{N} = V_I/\varrho_\ell = \{K_0, K_1, K_2, K_3, K_4\}$$

con $K_i = \ell_*^{-1}(i) \quad \forall i \in \{0,1,2,3,4\} = \mathrm{Im}(\ell)$

il che ci dà la descrizione esplicita

$$K_i = \ell_*^{-1}(i) = \{P \in V_I \mid \ell(P) = i\} = \ell^{-1}(i)$$

CIOÈ

$$K_i = \{P \in V_I \mid P \text{ ha esattamente } i \text{ lettere di } \Lambda\}$$

$$\forall\, i = 0,1,2,3,4.$$

Così, ad esempio, possiamo trovare rappresentanti

$$K_0 = [\text{POLLO}]_{\varrho_\ell} = [\text{POLLO}]_{\mathcal{N}} = [\text{GOTA}]_{\mathcal{N}} = \dots$$

$$K_1 = [\text{RAMO}]_{\varrho_\ell} = [\text{RAMO}]_{\mathcal{N}} = [\text{NOCE}]_{\mathcal{N}} = [\text{SETA}]_{\mathcal{N}} = \dots$$

$$K_2 = [\text{RANA}]_{\varrho_\ell} = [\text{RANA}]_{\mathcal{N}} = [\text{FRUTTA}]_{\mathcal{N}} = \dots$$

$$K_3 = [\text{FORNI}]_{\varrho_\ell} = [\text{FORNI}]_{\mathcal{N}} = [\text{ERNIA}]_{\mathcal{N}} = \dots$$

$$K_4 = [\text{ANFORE}]_{\varrho_\ell} = [\text{ANFORE}]_{\mathcal{N}} = [\text{FRENO}]_{\mathcal{N}} = \dots$$

(OK) □

2 **Hp:** A è anello unitario

$$GL_3(A) := \left\{ M \in Mat_{3\times 3}(A) \;\middle|\; \exists\, M^{-1} \in Mat_{3\times 3}(A) \right\}$$

$$U_3^+(A) := \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in A \right\}$$

Th: (a) $U_3^+(A)$ è sottogruppo di $GL_3(A)$

(b) Calcolare il centro di $U_3^+(A)$, cioè

$$Z(U_3^+(A)) := \left\{ \zeta \in U_3^+(A) \;\middle|\; \zeta \cdot_3 g = g \cdot_3 \zeta,\ \forall g \in U_3^+(A) \right\}$$

(c) Dimostrare che $Z(U_3^+(A)) \trianglelefteq U_3^+(A)$

(d) Dimostrare che il gruppo quoziente

$U_3^+(A) / Z(U_3^+(A))$ è isomorfo a $(A;+) \times (A;+)$

Svolgimento:

(a) ① $I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in U_3^+(A)$, con $\begin{cases} a=1 \\ b=1 \\ c=1 \end{cases}$ OK

② $U_3^+(A) \cdot U_3^+(A) \subseteq U_3^+(A)$, cioè

$U_3^+(A)$ è chiuso per il prodotto.

INFATTI $\forall \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & a'' & c'' \\ 0 & 1 & b'' \\ 0 & 0 & 1 \end{pmatrix} \in U_3^+(A)$

mi basa

$$(*) \quad \begin{pmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a'' & c'' \\ 0 & 1 & b'' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a''+a' & c''+a'b''+c' \\ 0 & 1 & b''+b' \\ 0 & 0 & 1 \end{pmatrix} \in U_3^+(A)$$

OK

③ $(U_3^+(A))^{-1} \subseteq U_3^+(A)$, cioè

$U_3^+(A)$ è chiuso per l'inverso

INFATTI, $\forall\ M := \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in U_3^+(A)$

vediamo che si trova $M^{-1} \in U_3^+(A)$ perché si trova una matrice $M' \in U_3^+(A)$ che ha le proprietà di M^{-1}...

Scrivo M' come matrice in $U_3^+(A)$, cioè della forma

$$M' = \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}$$

con $\alpha, \beta, \gamma \in A$ incognite.

Perché sia $M' = M^{-1}$ deve essere in particolare

$M \cdot M' = I_3$, cioè (dalla ⊛)

$$\begin{pmatrix} 1 & \alpha+a & \gamma+a\beta+c \\ 0 & 1 & \beta+b \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} = M \cdot M'$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3$$

$$\begin{cases} \alpha + a = 0 \\ \gamma + a\beta + c = 0 \\ \beta + b = 0 \end{cases} \Leftrightarrow \begin{cases} \alpha = -a \\ \gamma = -c - ab \\ \beta = -b \end{cases}$$

QUINDI deve essere

$$\circledast \quad M' = \begin{pmatrix} 1 & -a & -c-ab \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix}$$

per avere $M \cdot M' = I_3$. INOLTRE, per tale matrice M' si ha anche $M' \cdot M = I_3$

QUINDI M' è proprio l'inversa di M,

CIOÈ

$$\exists \; M^{-1} = M' = \begin{pmatrix} 1 & -a & -c-ab \\ 0 & 1 & -b \\ 0 & 0 & 1 \end{pmatrix} \in U_3^+(A)$$

ORA ① + ② + ③ $\Rightarrow$ $U_3^+(A)$ è sottogruppo di $GL_3(A)$ (OK)

(b) $\forall \; \zeta := \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & \gamma & 1 \end{pmatrix} \in U_3^+(A)$ si ha

$$\zeta \in Z(U_3^+(A)) \iff \zeta \cdot g = g \cdot \zeta \quad \forall\, g \in U_3^+(A) \iff$$

$$\iff \underbrace{\begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}}_{\zeta''} \cdot \underbrace{\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}}_{g''} = \underbrace{\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}}_{\forall a,b,c \in A \; g''} \underbrace{\begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}}_{\zeta''} \iff$$

(stella ⊛ di pag. 7)

$$\iff \begin{pmatrix} 1 & a+\alpha & c+\alpha b+\gamma \\ 0 & 1 & b+\beta \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha+a & \gamma+a\beta+c \\ 0 & 1 & \beta+b \\ 0 & 0 & 1 \end{pmatrix} \iff$$

$$\iff c+\alpha b+\gamma = \gamma+a\beta+c \iff \alpha b = a\beta$$

$\forall a,b,c \in A$ $\qquad$ $\forall a,b,c \in A$

COSÌ si trova

$$\zeta := \begin{pmatrix} 1 & \alpha & \gamma \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix} \in Z\left(U_3^+(A)\right) \iff \begin{array}{l} ab = ab \\ \forall\, a, b, c \in A \end{array}$$

$$\left(\begin{array}{l} \text{scegliendo } b=1,\ a=0 \Rightarrow \alpha = 0 \\ \text{scegliendo } b=0,\ a=1 \Rightarrow \beta = 0 \end{array} \right) \longrightarrow \Uparrow\Downarrow \quad \alpha = 0 \wedge \beta = 0$$

QUINDI è

$$Z\left(U_3^+(A)\right) = \left\{ \begin{pmatrix} 1 & 0 & \gamma \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, \gamma \in A \right\} \Rightarrow \text{(b) è OK}$$

(c)+(d): Sia $\varphi : U_3^+(A) \longrightarrow (A;+) \times (A;+)$

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \longmapsto (a, b)$$

La formula ⊛ a pagina 7 ci dice che la funzione φ è un morfismo di gruppi.
INOLTRE, per definizione e per (b) si ha

$$\ker(\varphi) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \,\middle|\, (a, b) = (0_A, 0_A) \right\} \overset{(b)}{=} Z\left(U_3^+(A)\right)$$

cioè $Z\left(U_3^+(A)\right) = \ker(\varphi) \trianglelefteq U_3^+(A)$

così che $Z\left(U_3^+(A)\right) \trianglelefteq U_3^+(A)$, $\Rightarrow$ (c) OK

INOLTRE, la funzione φ è chiaramente suriettiva, cioè

$$\operatorname{Im}(\varphi) = (A;+) \times (A;+)$$

e allora il TEOREMA FONDAMENTALE DI OMOMORFISMO per gruppi ci dà un isomorfismo di gruppi

$$\begin{array}{ccc} U_3^+(A) & \xrightarrow{\cong} & \mathrm{Im}(\varphi) \\ \hline \ker(\varphi) & \xrightarrow[\varphi_*]{} & \| \\ \| & & (A;+)\times(A;+) \\ U_3^+(A)/Z(U_3^+(A)) & & \end{array}$$

che è descritto esplicitamente da

$$\begin{array}{ccc} U_3^+(A) & \xrightarrow{\varphi_*} & (A;+)\times(A;+) \\ \hline Z(U_3^+(A)) & & \end{array}$$

$$\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \cdot Z(U_3^+(A)) \longmapsto (a,b) \qquad \circledast \qquad \square$$

N.B.: si può anche dimostrare (c) direttamente!

Ad esempio $I_3 \in Z(U_3^+(A))$ con $\gamma = 0$

$Z(U_3^+(A))$ è chiuso per il prodotto, perché

$$\begin{pmatrix} 1 & 0 & \gamma' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & \gamma'' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \gamma''+\gamma' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$ per la ⊛ di pag. 7

e $Z(U_3^+(A))$ è chiuso per l'inverso, per la ⊗ di pag. 3

INOLTRE, $g\cdot\zeta = \zeta\cdot g \quad (\forall g \in U_3^+(A),\ \forall \zeta \in Z(U_3^+(A)))$

implica $g\cdot Z(U_3^+(A)) = Z(U_3^+(A))\cdot g, \quad \forall g \in U_3^+(A)$

[3] Risolvere il sistema $\circledast$ $\begin{cases} 361x \equiv -78 \pmod 5 \\ -24x \equiv 6285^{930145} \pmod 7 \end{cases}$

Svolgimento:

① Semplifichiamo le due equazioni!

(1) $361 \equiv 1 \pmod 5$, $-78 \equiv 2 \pmod 5$

QUINDI $361 \cdot x \equiv -78 \pmod 5 \iff x \equiv 2 \pmod 5$

(2) $-24 \equiv 4 \pmod 7$

$6285 = 897 \cdot 7 + 6 \equiv 6 \equiv -1 \pmod 7$ $\quad -8$

e poi $6285^{930145} \equiv (-1)^{930145} = (-1)^7 = -1 \pmod 7$

QUINDI $-24x \equiv 6285^{930145} \iff 4 \cdot x \equiv -8 \pmod 7$

ALLORA ② + ② dà

$$\circledast \iff \begin{cases} x \equiv 2 \pmod 5 \\ 4x \equiv -8 \pmod 7 \end{cases} \iff \begin{cases} x \equiv 2 \pmod 5 \\ x \equiv -2 \equiv 5 \pmod 7 \end{cases}$$

Procedendo per sostituzione trovo

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv +5 \pmod 7 \end{cases} \iff \begin{cases} x = 2 + 5k \ (k \in \mathbb{Z}) \\ 2 + 5k \equiv +5 \pmod 7 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} x = 2 + 5k \ (k \in \mathbb{Z}) \\ 5k \equiv 3 \pmod 7 \end{cases} \iff \begin{cases} x = 2 + 5k \ (k \in \mathbb{Z}) \\ k \equiv 2 \pmod 7 \end{cases} \Rightarrow$$

$3 \cdot 5 = 15 \equiv_7 1$
$3 \cdot 3 = 9 \equiv_7 2$

$$\Rightarrow \begin{cases} x = 2 + 5(2 + 7z) = 12 + 35z \\ k = 2 + 7z, \ (z \in \mathbb{Z}) \end{cases}$$

QUINDI $S_{\circledast} = 12 + 35\mathbb{Z} = \{ \text{soluzioni di } \circledast \}$

4 **Hp:** G, H gruppi finiti con

$$d := \text{MCD}(|G|, |H|) = 1$$

Th: Determinare tutti i morfismi da G a H e tutti quelli da H a G.

Svolgimento:

Poniamo $g := |G|, \quad h := |H|$

così $d := \text{MCD}(g, h) = 1$

Sia $\varphi : G \longrightarrow H$ un morfismo.

Allora si ha

$$\exists\ \text{Ker}(\varphi) =: K_\varphi \trianglelefteq G, \quad \exists\ I_\varphi := \text{Im}(\varphi) \leq H$$

con $k := |K_\varphi|, \quad i := |I_\varphi|$

e il Teorema di Lagrange ci dà

$$k \mid_N g, \quad i \mid_N h$$

INOLTRE, il Teorema Fondamentale di Omomorfismo per gruppi ci dà un isomorfismo di gruppi

$$G/K_\varphi \underset{gr}{\cong} I_\varphi$$

In particolare,

$$(G : K_\varphi) := |G/K_\varphi| = |I_\varphi| =: i \Leftarrow \text{divisore di } h$$

$$\| \quad g/k \Leftarrow \text{divisore di } g \Big) \longrightarrow \text{divisore di } \text{MCD}(g, h) = 1$$

ALLORA è

$g/k = i$ divide $MCD(g,h) = 1$, $\Rightarrow$

$\Rightarrow$ $g/k = i$ è uguale a 1

MA $i = 1 \Rightarrow |Im(\varphi)| = 1 \Rightarrow Im(\varphi) = \{1_H\}$

$\Uparrow$

$|I_\varphi| = |Im(\varphi)|$

φ è il morfismo banale

$\underline{1}: G \longrightarrow H$

$g \longmapsto 1_H$

CONCLUSIONE:

$$\{\text{morfismi } G \xrightarrow{\varphi} H\} = \left\{ \begin{array}{c} G \xrightarrow{\underline{1}} H \\ g \longmapsto 1_H \end{array} \right\}$$

cioè da G ed H esiste soltanto il morfismo banale!

Invertendo i ruoli di G e H, siccome $MCD(|H|, |G|) = MCD(|G|, |H|) = 1$, troviamo analogamente che

$$\{\text{morfismi } H \xrightarrow{\psi} G\} = \left\{ \begin{array}{c} H \xrightarrow{\underline{1}} G \\ h \longmapsto 1_G \end{array} \right\}$$

5 Hp: $\forall$ insieme E, $\forall$ morfismo di anelli $\phi : A_1 \longrightarrow A_2$ sia

$$\phi^{(E)} : A_1^E \longrightarrow A_2^E, \quad f \longmapsto \phi^{(E)}(f) := \phi \circ f$$

Th: (a) Ogni $\phi^{(E)} : A_1^E \longrightarrow A_2^E$ è morfismo di anelli

(b) $\forall A$ si ha $id_1^{(E)} = id_{A^E}$

(c) $\forall \; A_1 \xrightarrow{\phi_1} A_2 \xrightarrow{\phi_2} A_3$ si ha

$$(\phi_2 \circ \phi_1)^{(E)} = \phi_2^{(E)} \circ \phi_1^{(E)}$$

(d) Se $\phi : A_1 \longrightarrow A_2$ è isomorfismo, allora $\phi^{(E)} : A_1^E \longrightarrow A_2^E$ è isomorfismo.

Svolgimento:

(a) $\forall f_1, f_2 \in A_1^E$ si ha

$$\phi^{(E)}(f_1 + f_2) := \phi \circ (f_1 + f_2)$$

&

$$\phi^{(E)}(f_1) + \phi^{(E)}(f_2) := (\phi \circ f_1) + (\phi \circ f_2)$$

ORA $\forall e \in E$ si ha

$$\left(\phi^{(E)}(f_1 + f_2)\right)(e) = \left(\phi \circ (f_1 + f_2)\right)(e) = \phi\left((f_1 + f_2)(e)\right) =$$

$$= \phi\left(f_1(e) + f_2(e)\right) = \phi(f_1(e)) + \phi(f_2(e)) =$$

$$= (\phi \circ f_1)(e) + (\phi \circ f_2)(e) = \left(\phi^{(E)}(f_1)\right)(e) + \left(\phi^{(E)}(f_2)\right)(e)$$

$$= \left(\phi^{(E)}(f_1) + \phi^{(E)}(f_2)\right)(e)$$

QUINDI ha, $\forall e \in E$,

$$\left(\phi^{(E)}(f_1+f_2)\right)(e) = \left(\phi^{(E)}(f_1) + \phi^{(E)}(f_2)\right)(e)$$

così che

$$\phi^{(E)}(f_1+f_2) = \phi^{(E)}(f_1) + \phi^{(E)}(f_2)$$
$$\forall\, f_1, f_2 \in A_1^E$$

perciò $\phi^{(E)}$ manda la somma di A_1^E nella somma di A_2^E

POI, sostituendo il prodotto alla somma nelle formule precedenti, la stessa identica analisi ci dà

$$\phi^{(E)}(f_1 \cdot f_2) = \phi^{(E)}(f_1) \cdot \phi^{(E)}(f_2)$$

così che $\phi^{(E)}$ manda (anche) il prodotto di A_1^E nel prodotto di A_2^E

QUINDI $\phi^{(E)}$ è morfismo di anelli, q.e.d. (CM)

(b) Per definizione, $\forall f \in A^E$ e $\forall e \in E$ si ha

$$\left(id_A^{(E)}(f)\right)(e) := (id_A \circ f)(e) = f(e)$$

da cui $id_A^{(E)}(f) = f$, $\forall f \in A^E$

e quindi $id_A^{(E)} = id_{A^E}$, q.e.d.

(c) Le definizioni diamo, $\forall f \in A_1^E$,

$$(\phi_2 \circ \phi_1)^{(E)}(f) := (\phi_2 \circ \phi_1) \circ f = \phi_2 \circ (\phi_1 \circ f) =$$

(per associatività di $\circ$)

$$= \phi_2^{(E)}(\phi_1^{(E)}(f)) = (\phi_2^{(E)} \circ \phi_1^{(E)})(f)$$

cioè

$$(\phi_2 \circ \phi_1)^{(E)}(f) = (\phi_2^{(E)} \circ \phi_1^{(E)})(f) \qquad \forall f \in A^E$$

con' che

$$(\phi_2 \circ \phi_1)^{(E)} = \phi_2^{(E)} \circ \phi_1^{(E)}, \text{ q.e.d.}$$ (ok)

(d) Sia $\phi : A_1 \longrightarrow A_2$ un isomorfismo; $\Leftrightarrow$

$\Rightarrow \exists$ morfismo $\psi : A_2 \longrightarrow A_1$ tale che

$$\psi \circ \phi = id_{A_1} \quad \& \quad \phi \circ \psi = id_{A_2}$$

ALLORA da (a) segue che

$\exists$ morfismo $\psi^{(E)} : A_2^E \longrightarrow A_1^E$

e da (c) e (b) segue che

$$\psi^{(E)} \circ \phi^{(E)} = (\psi \circ \phi)^{(E)} = id_{A_1}^{(E)} = id_{A_1^E}$$

$$\phi^{(E)} \circ \psi^{(E)} = (\phi \circ \psi)^{(E)} = id_{A_2}^{(E)} = id_{A_2^E}$$

cioè

$$\psi^{(E)} \circ \phi^{(E)} = id_{A_1^E}$$

$$\& \quad \phi^{(E)} \circ \psi^{(E)} = id_{A_2^E}$$

perciò il morfismo $\psi^{(E)}$ è inverso di $\phi^{(E)}$, con' $\phi^{(E)}$ è invertibile e dunque è un isomorfismo, q.e.d. (ok) □

6 Hp: $\mathbb{Z}[\sqrt{-13}] := \{ z \in \mathbb{C} \mid \exists a, b \in \mathbb{Z} : z = a + b\sqrt{-13} \}$

Th: (a) $\mathbb{Z}[\sqrt{-13}]$ è sottoanello di $\mathbb{C}$.

(b) $\mathbb{Z}[\sqrt{-13}]$ è dominio a fattorizzazione ?

(c) $\mathbb{Z}[\sqrt{-13}]$ è dominio a fattorizzazione unica ?

(d) $\mathbb{Z}[\sqrt{-13}]$ è dominio a ideali principali ?

(e) $\mathbb{Z}[\sqrt{-13}]$ è dominio euclideo ?

(f) $\exists$ in $\mathbb{Z}[\sqrt{-13}]$ un elemento che ha una fattorizzazione in irriducibili che NON siano primi ?

Svolgimento:

(a) ① $0 = (0 + 0 \cdot \sqrt{-13}) \in \mathbb{Z}[\sqrt{-13}]$ ok

② $(a' + b'\sqrt{-13}) + (a'' + b''\sqrt{-13}) =$

$= ((a' + a'') + (b' + b'')\cdot\sqrt{-13}) \in \mathbb{Z}[\sqrt{-13}]$ ok

($a' + a'' \in \mathbb{Z}$, $b' + b'' \in \mathbb{Z}$)

③ $(a + b\sqrt{-13}) \in \mathbb{Z}[\sqrt{-13}]$

($a \in \mathbb{Z}$, $b \in \mathbb{Z}$) ⇓ ok

$-(a + b\sqrt{-13}) = ((-a) + (-b)\sqrt{-13}) \in \mathbb{Z}[\sqrt{-13}]$

④ $(a' + b'\sqrt{-13}) - (a'' + b''\cdot\sqrt{-13}) =$

$= ((\underbrace{a'a'' - 13\cdot b'b''}_{\in \mathbb{Z}}) + (\underbrace{a'b'' + b'a''}_{\in \mathbb{Z}})\sqrt{-13}) \in \mathbb{Z}[\sqrt{-13}]$ ok

Da ① + ② + ③ + ④ segue che

$\mathbb{Z}[\sqrt{-13}]$ è sottoanello di $\mathbb{C}$, q.e.d.

(b) Consideriamo la funzione

$$\nu : \mathbb{Z}[\sqrt{-13}] \longrightarrow \mathbb{N}$$
$$(a + b\sqrt{-13}) \longmapsto \nu(a + b\sqrt{-13}) = a^2 + 13b^2$$

(data dalla restrizione della norma dei numeri complessi $N : \mathbb{C} \longrightarrow \mathbb{R}_{\geq 0}$, $z \longmapsto z \cdot \bar{z}$)

NOTIAMO che ν è moltiplicativa, cioè

$$\nu((a' + b'\sqrt{-13}) \cdot (a'' + b''\cdot\sqrt{-13})) =$$
$$\circledast \quad = \nu(a' + b'\sqrt{-13}) \cdot \nu(a'' + b''\sqrt{-13})$$

((verifica diretta — oppure, segue dalla analoga proprietà della norma))

INOLTRE, si ha

$$\circledast \quad \nu(a + b\sqrt{-13}) = 1 \iff a + b\sqrt{-13} = \begin{cases} +1 \\ -1 \end{cases}$$
$$\Updownarrow$$
$$(a + b\sqrt{-13}) \in U(\mathbb{Z}[\sqrt{-13}])$$
$$\| \{+1, -1\}$$

ALLORA

SE $\zeta \in \mathbb{Z}[\sqrt{-13}]$ si fattorizza in

$\zeta = \alpha \cdot \beta$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-13}]$

la $\circledast$ dà $\nu(\zeta) = \nu(\alpha) \cdot \nu(\beta)$

e dalla ⊛ segue che

la fattorizzazione $\zeta = \alpha \cdot \beta$
è banale (in $\mathbb{Z}[\sqrt{-13}]$)

$\Updownarrow$

la fattorizzazione $\nu(\zeta) = \nu(\alpha) \cdot \nu(\beta)$
è banale (in $\mathbb{N}$)

ALLORA, procedendo per induzione forte su $\nu(\zeta)$
si trova che

ogni $\zeta \in \mathbb{Z}[\sqrt{-13}] \setminus (\{0\} \cup U(\mathbb{Z}[\sqrt{-13}]))$
ha una fattorizzazione in irriducibili

QUINDI $\mathbb{Z}[\sqrt{-13}]$ è un dominio a fattorizzazione (OK)

(f) L'elemento $\zeta := 14$ ammette due fattorizzazioni

$$14 = 2 \cdot 7 \quad \& \quad 14 = (1+\sqrt{-13}) \cdot (1-\sqrt{-13})$$

ORA,

2, 7, $1+\sqrt{-13}$, $1-\sqrt{-13}$ sono irriducibili

INFATTI, ad esempio

$$2 = \alpha \cdot \beta \overset{\circledast}{\Rightarrow} \nu(2) = \nu(\alpha) \cdot \nu(\beta) = \begin{cases} 4 \cdot 1 \\ 2 \cdot 2 \\ 1 \cdot 4 \end{cases} \Rightarrow$$

$\Rightarrow$ può essere soltanto $\begin{cases} 4 \cdot 1 \\ 1 \cdot 4 \end{cases}$ $\Rightarrow$ $2 = \alpha \cdot \beta$ è fattorizzazione banale
(perché $2 \notin \mathrm{Im}(\nu)$)

Analogamente si ha

$7 \notin \mathrm{Im}(\nu) \Rightarrow 7$ è irriducibile

&

$2, 7 \notin \mathrm{Im}(\nu) \Rightarrow (1+\sqrt{-13}),\ (1-\sqrt{-13})$ sono entrambi irriducibili

ORA dalle due decomposizioni in irriducibili

$$2 \cdot 7 = 14 = (1+\sqrt{-13})(1-\sqrt{-13})$$

segue, ad esempio, che

2 divide $(1+\sqrt{-13})(1-\sqrt{-13})$

MA 2 NON divide $(1+\sqrt{-13})$ / $(1-\sqrt{-13})$

perché se $\exists\ (a+b\sqrt{-13}) \in \mathbb{Z}[\sqrt{-13}]$ t.c.

$$2 \cdot (a+b\sqrt{-13}) = (1 \pm \sqrt{-13})$$

sarebbe $\begin{cases} 2a = 1 \\ 2b = \pm 1 \end{cases}$ $a, b \in \mathbb{Z}$, (ASSURDO)

QUINDI 2 NON è primo.

$\rightsquigarrow$ Analogamente, 7 NON è primo.

QUINDI $14 = 2 \cdot 7$ è un esempio di una fattorizzazione in irriducibili che però sono NON primi (OK)

(c) - (d) - (e) Da (f) si ha che

14 ha due fattorizzazioni in irriducibili che non sono equivalenti,

QUINDI $\mathbb{Z}[\sqrt{-13}]$ non è un dominio a fattorizzazione unica $\Rightarrow$ (c) no

POI,

Siccome ogni dominio euclideo e ogni dominio a ideali principali è anche (sempre) un dominio a fattorizzazione unica, si conclude che

$\mathbb{Z}[\sqrt{-13}]$ non è dominio euclideo

e

$\mathbb{Z}[\sqrt{-13}]$ non è dominio a ideali principali

OPPURE

Nell'analisi di (f) abbiamo visto che

2 è irriducibile
MA 2 NON è primo
} in $\mathbb{Z}[\sqrt{-13}]$

(idem per 7, per $(1+\sqrt{-13})$ e per $(1-\sqrt{-13})$)

ma sappiamo che in un dominio a ideali principali - quindi in particolare in un dominio euclideo - si ha che

"ogni irriducibile è primo"

PERCIÒ si conclude che $\mathbb{Z}[\sqrt{-13}]$ NON è / dominio a ideali principali / dominio euclideo