CdL in Matematica

ALGEBRA 1

prof. Fabio GAVARINI

a.a. 2023–2024

Esame scritto del 17 Luglio 2024 — Sessione Estiva, II appello

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

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

[1] — Dati due insiemi A e B, si indichi B^A l'insieme delle funzioni da A a B. Sia poi "$\sim$" l'usuale relazione di equipotenza tra insiemi, e siano infine X, Y, Z tre insiemi arbitrari.

(a) Dimostrare che $\big(X \times Y\big)^Z \sim X^Z \times Y^Z$.

(b) Dimostrare che se $X \sim Y$, allora si ha anche $X^Z \sim Y^Z$.

[2] — Sia E un insieme non vuoto, e sia $\rho : E \dashrightarrow E$ una relazione qualsiasi in E. Si definiscano iterativamente le *potenze* di ρ come le relazioni

$$\rho^1 := \rho \quad , \qquad \rho^{n+1} := \rho \circ \rho^n \qquad \forall\ n \in \mathbb{N}_+$$

Allora:

(a) Se ρ è transitiva, dimostrare che $\rho^n \subseteq \rho^k$ per ogni $n, k \in \mathbb{N}_+$ con $n \geq k$.

(b) Se ρ è transitiva e riflessiva, dimostrare che $\rho^n = \rho^k$ per ogni $n, k \in \mathbb{N}_+ : n \geq k$.

(c) Per l'insieme $E := \mathbb{Z}$, fornire un esempio di una relazione ρ che sia transitiva ma non riflessiva e tale che $\rho^2 \subsetneqq \rho$.

[3] — Sia G un gruppo *privo di torsione*, cioè tale che valga la seguente proprietà: per ogni $g \in G$ e per ogni $n \in \mathbb{N}_+$, si ha $g^n = 1_G \iff g = 1_G$.

(a) Se $g \in G \setminus \big\{1_G\big\}$ è tale che $g^r = g^s$ per qualche $r, s \in \mathbb{Z}$, dimostrare che allora è $r = s$;

(b) Se G è *commutativo* e $g, \gamma \in G$ sono tali che $g^n = \gamma^n$ per un certo $n \in \mathbb{Z} \setminus \{0\}$, dimostrare che allora è $g = \gamma$;

(c) Dare un esempio di un gruppo commutativo G privo di torsione, di due elementi $g, \gamma \in G$ con $g \neq \gamma$ e di due interi positivi $n, m \in \mathbb{N}$ tali che $g^n = \gamma^m$.

(continua...) $\Longrightarrow$

[4] — Sia G un gruppo, siano $H \leqslant G$, $K \leqslant G$, e siano G/H e G/K i corrispondenti spazi di classi laterali sinistre (modulo H e modulo K, rispettivamente).

(a) Dimostrare che esiste una funzione iniettiva $G\big/(H \cap K) \hookrightarrow \big(G/H\big) \times \big(G/K\big)$.

(b) Dimostrare che se $H \trianglelefteq G$, $K \trianglelefteq G$, allora è anche $(H \cap K) \trianglelefteq G$.

(c) Dimostrare che se $H \trianglelefteq G$, $K \trianglelefteq G$, allora si può trovare una funzione come in *(a)* che è un morfismo di gruppi, dove $\big(G/H\big) \times \big(G/K\big)$ ha la struttura canonica di prodotto diretto di gruppi.

(d) Dimostrare che se $H \trianglelefteq G$, $K \trianglelefteq G$, e i gruppi quoziente G/H e G/K sono abeliani, allora anche il gruppo quoziente $G\big/(H \cap K)$ è abeliano.

[5] — Sia S un insieme di irriducibili in $\mathbb{Z}$, con $S \subseteq \mathbb{Z}_+$, e per tale S definiamo $\mathbb{Z}_S := \big\{\, n/d \in \mathbb{Q} \,\big|\, \text{i fattori irriducibili di } d \text{ appartengono a } S \,\big\}$. Dimostrare che:

(a) $\mathbb{Z}_S$ è sottoanello di $\mathbb{Q}$;

(b) Se S' e S'' sono due insiemi di irriducibili in $\mathbb{Z} \setminus \{0\}$, come sopra, allora si ha

$$S' \text{ è sottoinsieme di } S'' \iff \mathbb{Z}_{S'} \text{ è sottoanello di } \mathbb{Z}_{S''} \quad ;$$

[6] — Nell'anello degli interi di Gauss $\mathbb{Z}[\,i\,]$ si considerino i quattro elementi

$$A := 7 + 4\,i \quad , \qquad B := 3 + i \quad , \qquad C' := 1 + 3\,i \quad , \qquad C'' := 5$$

(a) Determinare se l'equazione diofantea $A\,X + B\,Y = C'$ in $\mathbb{Z}[\,i\,]$ abbia soluzioni: in caso negativo, si spieghi perché non esistano soluzioni, in caso positivo si calcoli almeno una soluzione esplicita (X, Y).

(b) Determinare se l'equazione diofantea $A\,X + B\,Y = C''$ in $\mathbb{Z}[\,i\,]$ abbia soluzioni: in caso negativo, si spieghi perché non esistano soluzioni, in caso positivo si calcoli almeno una soluzione esplicita (X, Y).

(c) Calcolare il *M.C.D.*$\big(A\,,B\big)$.

ALGEBRA 1

ESAME SCRITTO del 17 LUGLIO 2024

---

1 Dati insiemi A e B, si indichi

$$B^A := \{ \text{funzioni } A \longrightarrow B \}$$

e sia $\sim$ la relazione di equipotenza tra insiemi. Siano X, Y, Z tre insiemi. Dimostrare che:

(a) $(X \times Y)^Z \sim X^Z \times Y^Z$

(b) se $X \sim Y$, allora $X^Z \sim Y^Z$

Svolgimento:

(a) Per definizione si ha

$$(X \times Y)^Z := \{ \text{funzioni } l : Z \longrightarrow X \times Y \}$$

$$X^Z \times Y^Z := \{ h : Z \to X \} \times \{ k : Z \longrightarrow Y \}$$

Consideriamo le due "proiezioni canoniche" da $X \times Y$ ai due "fattori" X e Y, cioè

$$\pi_X : X \times Y \longrightarrow X, \quad (x,y) \longmapsto x$$

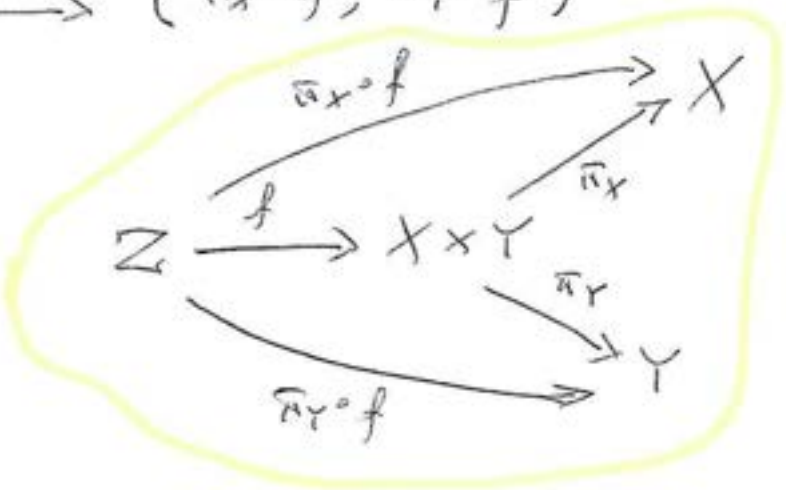
&

$$\pi_Y : X \times Y \longrightarrow Y, \quad (x,y) \longmapsto y$$

Ora definiamo la funzione

$$\mathcal{D} : (X \times Y)^Z \longrightarrow X^Z \times Y^Z$$
$$f \longmapsto (\pi_X \circ f, \pi_Y \circ f)$$

Così definiamo la funzione (a rovescio!)



$$\mathcal{U} : X^Z \times Y^Z \longrightarrow (X \times Y)^Z$$
$$(h,k) \longmapsto h \times k$$

dove $h \times k$ è la funzione da Z a $X \times Y$ definita così

$$\therefore \quad Z \xrightarrow{h \times k} X \times Y \qquad (\forall z \in Z)$$
$$z \longmapsto (h \times k)(z) := (h(z), k(z))$$

Adesso, direttamente dalle definizioni

si verifica facilmente (!) che

$$\mathcal{U} \circ \mathcal{D} = id_{(X\times Y)^Z}$$

&

$$\mathcal{D} \circ \mathcal{U} = id_{X^Z \times Y^Z}$$

cioè le funzioni $\mathcal{U}$ e $\mathcal{D}$ sono inverse l'una dell'altra, $\Rightarrow$

$\Rightarrow$ in particolare, $\mathcal{U}$ e $\mathcal{D}$ sono biiezioni $(X\times Y)^Z \rightleftarrows X^Z \times Y^Z$ (con $\mathcal{D}$ e $\mathcal{U}$)

QUINDI si conclude che

$$(X\times Y)^Z \sim X^Z \times Y^Z, \quad \text{q.e.d.}$$

(b) Per ipotesi $X \sim Y$, cioè

$\exists\, f: X \twoheadrightarrow Y$ funzione biiettiva con inversa $f^{-1}: Y \twoheadrightarrow X$.

Ora costruiamo tra X^Z e Y^Z le

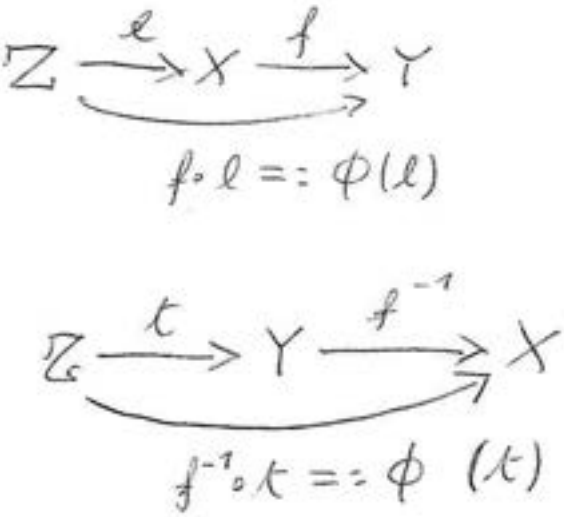
due funzioni $(\forall\, \ell \in X^Z)$

$$X^Z \xrightarrow{\Phi} Y^Z, \qquad \ell \longmapsto \Phi(\ell) := f \circ \ell$$

e $(\forall\, t \in Y^Z)$

$$Y^Z \xrightarrow{\Phi'} X^Z$$

$$t \longmapsto \Phi'(t) := f^{-1} \circ t$$



Ora osserviamo che

$\forall\, \ell \in X^Z$ si ha

$$(\Phi' \circ \Phi)(\ell) = \Phi'(\Phi(\ell)) = \Phi'(f \circ \ell) = f^{-1} \circ (f \circ \ell) =$$
$$= (f^{-1} \circ f) \circ \ell = id_X \circ \ell = \ell$$

cioè $(\Phi' \circ \Phi)(\ell) = \ell \quad \forall\, \ell \in X^Z$

quindi $\Phi' \circ \Phi = id_{X^Z}$

e analogamente $\forall\, t \in Y^Z$ si ha

$$(\Phi \circ \Phi')(t) = \Phi(\Phi'(t)) = \Phi(f^{-1} \circ t) = f \circ (f^{-1} \circ t) =$$
$$= (f \circ f^{-1}) \circ t = id_Y \circ t = t$$

cioè $(\Phi \circ \Phi')(t) = t \quad \forall\, t \in Y^Z$

quindi $\Phi \circ \Phi' = id_{Y^Z}$

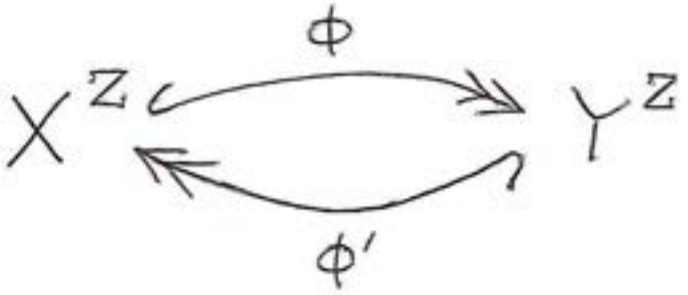
Allora da

$$\phi' \circ \phi = id_{X^Z} \,, \quad \phi \circ \phi' = id_{Y^Z}$$

concludiamo che

ϕ e ϕ' sono invertibili

(e inverse l'una dell'altra)



QUINDI

si conclude che

$$X^Z \sim Y^Z \,, \quad \text{q.e.d.} \qquad \square$$

CONTINUA

2 Sia E un insieme, $E \neq \emptyset$, e sia $\rho : E \dashrightarrow E$ una relazione in E. Si definiscono le potenze di ρ così:

$$\rho^1 := \rho \,, \quad \rho^{n+1} := \rho \circ \rho^n \,, \quad \forall n \in \mathbb{N}_+$$

(a) Dimostrare che

$$\rho \text{ transitiva} \Rightarrow \rho^n \subseteq \rho^k, \quad \forall n, k \in \mathbb{N}_+ : n \geq k$$

(b) Dimostrare che

$$\left.\begin{array}{l}\rho \text{ transitiva} \\ \& \\ \text{riflessiva}\end{array}\right\} \Rightarrow \begin{array}{l}\rho^n = \rho^k \\ \forall n, k \in \mathbb{N}_+ : n \geq k\end{array}$$

(c) Per $E := \mathbb{Z}_4$, dare un esempio di una ρ che sia transitiva ma non riflessiva e tale che $\rho^2 \subsetneq \rho$.

Svolgimento:

(a) Per definizione di "transitiva" si ha

ρ è transitiva $\Leftrightarrow$ $\forall a, b, c \in E$ si ha $(a \rho b) \,\&\, (b \rho c) \Rightarrow a \rho c$

MA $(a \rho b) \,\&\, (b \rho c) \Rightarrow a \rho^2 c$ (sempre!), per definizione di ρ^2

QUINDI abbiamo che

ρ è transitiva $\iff$ $\supset$ a ρ c

cioè

$\rho^2 \subseteq \rho$

Ora, osserviamo che

$\forall\ \sigma, \varphi, \psi$ relazioni in E si ha

$$\varphi \subseteq \psi \supset \sigma \circ \varphi \subseteq \sigma \circ \psi \qquad (\bullet)$$

(per come è definita la composizione "$\circ$")

Allora abbiamo anche che

$$\rho^2 \subseteq \rho \Rightarrow \rho \circ \rho^2 \subseteq \rho \circ \rho$$
$$\rho^3 \qquad\quad \rho^2$$

cioè $\rho^2 \subseteq \rho \Rightarrow \rho^3 \subseteq \rho^2$

e poi, per ogni $n \in \mathbb{N}_+$, abbiamo

Hp Ind: $\rho^{n+1} \subseteq \rho^n \Rightarrow$ Th Ind: $\rho^{n+2} \subseteq \rho^{n+1}$

INFATTI

(Hp) $\rho^{n+1} \subseteq \rho^n \Rightarrow \rho^{n+2} := \rho \circ \rho^{n+1} \subseteq \rho \circ \rho^n =: \rho^{n+1}$

cioè $\rho^{n+2} \subseteq \rho^{n+1}$, q.e.d.

Così abbiamo dimostrato per induzione che

$$\circledast \quad \rho^{l+1} \leq \rho^{l} \quad , \quad \forall\, l \in \mathbb{N}_+$$

Complessivamente, questo ci dà

$$\rho = \rho^1 \geq \rho^2 \geq \rho^3 \geq \dots \geq \rho^{l-1} \geq \rho^{l} \geq \rho^{l+1} \geq \dots$$

da cui si vede subito che

$$\rho^{k} \geq \rho^{n} \quad \forall \quad k \leq n$$

cioè

$$\circledast \quad \rho^{n} \leq \rho^{k} \quad , \quad \forall\, k, n \in \mathbb{N}_+ : n \geq k$$

OPPURE, più formalmente, si dimostra la proprietà $\circledast$ facendo induzione (semplice) su $t := n - k$, come segue:

BASE: $t = 0 \Rightarrow n = k \Rightarrow$

$\Rightarrow \rho^{n} = \rho^{k} \Rightarrow$ (OK) la tesi è provata!

PASSO INDUTTIVO: $(\forall t \in \mathbb{N}_+)$ **Hp Ind.:** $\varrho^{t+k} \subseteq \varrho^k$

Th Ind.: $\varrho^{(1+t)+k} \subseteq \varrho^k$

Dim.: il calcolo ci dà

$$\varrho^{(1+t)+k} = \varrho^{1+(t+k)} := \varrho \circ \varrho^{(t+k)}$$

MA $\varrho^{t+k} \subseteq \varrho^k \Rightarrow \varrho \circ \varrho^{t+k} \subseteq \varrho \circ \varrho^k$

($\Rightarrow$ per (•) di pag. 7; $\varrho^{t+k} \subseteq \varrho^k$ per Hp Ind)

$\varrho \circ \varrho^{t+k} \subseteq \varrho \circ \varrho^k$!! $\varrho^{1+k} = \varrho^{k+1} \subseteq \varrho^k$ (per ⊛ di pag. 8)

QUINDI in sintesi

$$\varrho^{(1+t)+k} \subseteq \varrho^{k+1} \subseteq \varrho^k$$

da cui

$$\varrho^{(1+t)+k} \subseteq \varrho^k, \quad \text{q.e.d.}$$

(b) Sia ϱ transitiva & riflessiva.

Siccome ϱ è transitiva, $\forall k, n \in \mathbb{N}_+$ t.c. $n \geq k$ è $\varrho^n \subseteq \varrho^k$, e quindi dobbiamo provare $\varrho^k \subseteq \varrho^n$.

Siano $a, b \in E$ t.c. $\exists \rho$

Allora è anche $b \rho b$, perché

ρ è riflessiva; quindi

$$\left.\begin{array}{l} a \rho b \\ \& \\ b \rho b \end{array}\right\} \Rightarrow a \rho^2 b$$

cosi $\forall a, b \in E$, $a \rho b \Rightarrow a \rho^2 b$

cioè $\forall a, b \in E$, $(a,b) \in \rho \Rightarrow (a,b) \in \rho^2$

QUINDI è $\rho \subseteq \rho^2$

Ma allora, sfruttando più volte la proprietà (•) di pag. 7 e iterando (cioè facendo induzione!) si ha

$$\rho \subseteq \rho^2 \Rightarrow \rho \cdot \rho \subseteq \rho \cdot \rho^2 \Rightarrow \rho^2 \subseteq \rho^3$$

$$\rho^2 \subseteq \rho^3 \Rightarrow \rho \cdot \rho^2 \subseteq \rho \cdot \rho^3 \Rightarrow \rho^3 \subseteq \rho^4$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$\rho^l \subseteq \rho^{l+1} \Rightarrow \rho \cdot \rho^l \subseteq \rho \cdot \rho^{l+1} \Rightarrow \rho^{l+1} \subseteq \rho^{l+2}$$

$$\vdots \qquad \vdots \qquad \vdots$$

cioè $\rho^k \subseteq \rho^{k+1}$, $\forall k \in \mathbb{N}_+$

e QUINDI, globalmente

$$\rho \subseteq \rho^2 \subseteq \rho^3 \subseteq \cdots \subseteq \rho^{k-1} \subseteq \rho^k \subseteq \rho^{k+1} \subseteq \cdots$$

da cui "estraiamo" che

$$\rho^k \subseteq \rho^n \,, \quad \forall k, n \in \mathbb{N}_+ : n \geq k$$

q.e.d.

((OPPURE, analogamente a prima, si dimostra che $\rho^k \subseteq \rho^n$ $(\forall n \geq k)$ per induzione semplice su $t := n - k$))

(c) In $E := \mathbb{Z}$, consideriamo la relazione, transitiva ma NON riflessiva,

$\rho := <$:= "strettamente minore di"

(dove "$\leq$" è la relazione d'ordine standard in $\mathbb{Z}$, così che $< = \leq \setminus =$); così ad esempio si ha $5 < 7$, $-3 < 2$, ma $6 \not< 1$, $4 \not< 4$

Allora abbiamo, ad esempio

$$\left.\begin{array}{l} 3 < 5 \\ \& \\ 5 < 9 \end{array}\right\} \Rightarrow \left.\begin{array}{l} 3 \,\rho\, 5 \\ \& \\ 5 \,\rho\, 9 \end{array}\right\} \Rightarrow 3 \,\rho^2\, 9$$

come anche $3 < 5$, cioè $3 \,\rho\, 9$

così che $\begin{array}{l} 3 \,\rho^2\, 9 \\ \& \\ 3 \,\rho\, 9 \end{array}$, che è coerente

col fatto che $\rho^2 \subseteq \rho$ perché

ρ è transitiva.

D'altra parte abbiamo anche

$7 < 8$, cioè $7 \,\rho\, 8$

MA $7 \not\rho^2 8$, perché

$\nexists\, z \in \mathbb{Z} : (7 < z) \,\&\, (z < 8)$

CIOÈ $(7 \,\rho\, z) \,\&\, (z \,\rho\, 8)$

QUINDI è $(7 \,\rho\, 8) \,\&\, (7 \not\rho^2 8)$

CIOÈ $(7,8) \in \rho \quad \& \quad (7,8) \notin \rho^2$

PERCIÒ si ha $\rho^2 \subseteq \rho$ (per la (a))

MA $\rho \notin \rho^2$, COSÌ È $\rho^2 \subsetneq \rho$, q.e.d. □

3 Sia G un gruppo tale che

(*) $\forall g \in G$, $\forall n \in \mathbb{N}_+$ $\quad g^2 = 1_G \iff g = 1_G$

Th: (a) $\forall g \in G \setminus \{1_G\}$, $\forall r, s \in \mathbb{Z}$,

$g^r = g^s \Rightarrow r = s$

(b) Se G è commutativo, $\forall n \in \mathbb{Z} \setminus \{0\}$

$g, \gamma \in G$, $\quad g^n = \gamma^n \Rightarrow g = \gamma$

(c) Dare un esempio di gruppo commutativo G in cui valga (*) e di due elementi $g, \gamma \in G$ con $g \neq \gamma$ per cui $\exists\, n, m \in \mathbb{N} : g^n = \gamma^m$

Svolgimento:

(a) Siano $g \in G \setminus \{1_G\}$, $r, s \in \mathbb{Z}$ t.c. $g^r = g^s$. Allora

$$g^{r-s} = g^r \cdot g^{-s} = g^r \cdot (g^s)^{-1} \overset{\text{per } g^r = g^s}{=} g^r \cdot (g^r)^{-1} = 1_G$$

cioè $g^{r-s} = 1_G$; $\Rightarrow$ $g^{-(r-s)} = (g^{r-s})^{-1} = 1_G$

QUINDI è $g^{|r-s|} = 1_G$ con $|r-s| \in \mathbb{N}$

ORA, se $|r-s| \neq 0$ allora la (*) ci dà $g = 1_G$, ↯ (per Hp, è $g \neq 1_G$);

QUINDI deve essere $|r-s| = 0$,

cioè $r = s$, q.e.d.

(b) Sia G commutativo, $n \in \mathbb{Z} \setminus \{0\}$ e $g, \gamma \in G$ t.c. $g^n = \gamma^n$.

Allora $g^n = \gamma^n \Rightarrow g^n \cdot (\gamma^n)^{-1} = 1_G \Rightarrow$

$\Rightarrow g^n \cdot \gamma^{-n} = 1_G \Rightarrow g^n \cdot (\gamma^{-1})^n = 1_G$

ORA, siccome G è commutativo si ha

$$g^n \cdot (\gamma^{-1})^n = (g \cdot \gamma^{-1})^n$$

QUINDI da $g^n = \gamma^n$ ricaviamo che

$(g \cdot \gamma^{-1})^n = 1_G$, da cui

(come prima) $(g \cdot \gamma^{-1})^{|n|} = 1_G$

con $|n| \in \mathbb{N}_+$

$\Longrightarrow$ la condizione (*) implica

$g \cdot \gamma^{-1} = 1_G$, da cui

$g = \gamma$, q.e.d.

(c) Si consideri $G := (\mathbb{Q}_+ ; \cdot)$,

il gruppo dei numeri razionali positivi con l'operazione di moltiplicazione.

In tale gruppo si ha

$$q^n = 1 \iff q = 1$$

$\forall\, q \in \mathbb{Q}_+$ e $\forall\, n \in \mathbb{N} \setminus \{0\} =: \mathbb{N}_+$

cioè vale la condizione (*) in $(\mathbb{Q}_+ ; \cdot)$;

inoltre, tale gruppo è commutativo.

Possiamo allora scegliere

$g := 2$, $\gamma := 8$ in $\mathbb{Q}_+$, con $g \neq \gamma$

e troviamo $n = 3$, $m = 1$ in $\mathbb{N}$

tali che $g^n = 2^3 = 8$, $\gamma^m = 8^1 = 8$

così che $g^n = \gamma^m$, q.e.d. $\square$

4 Sia G un gruppo, H e K due sottogruppi di G, e G/H, G/K i corrispondenti insiemi di classi laterali sinistre. Dimostrare che:

(a) $\exists$ funzione iniettiva

$$G/(H \cap K) \hookrightarrow G/H \times G/K$$

(b) Se $H \leq G$, $K \leq G$, allora $H \cap K \leq G$

(c) Se $H \leq G$, $K \leq G$, allora si può trovare una funzione come in (a) che è un morfismo di gruppi, dove $G/H \times G/K$ è prodotto diretto dei gruppi quoziente G/H e G/K.

(d) Se $H \leq G$, $K \leq G$, e i gruppi G/H e G/K sono abeliani, allora anche $G/(H \cap K)$ è abeliano.

Svolgimento:

(a) Consideriamo la funzione

$$\phi : G \longrightarrow G/H \times G/K$$
$$g \longmapsto \phi(g) := (gH, gK)$$

Sia poi ρ_ϕ la relazione di equivalenza in G associata a ϕ, che è data da $(\forall g_1, g_2 \in G)$

$$g_1 \rho_\phi g_2 \iff \phi(g_1) = \phi(g_2)$$

Sappiamo allora, dal Teorema Fondamentale delle Applicazioni, che esiste una (unica) funzione iniettiva a ϕ (e a ρ_ϕ) data da

$$\phi_* : G/\rho_\phi \hookrightarrow G/H \times G/K \qquad (1)$$
$$[g]_{\rho_\phi} \longmapsto \phi(g) := (gH, gK)$$

dove G/ρ_ϕ è l'insieme quoziente di G modulo l'equivalenza ρ_ϕ.

Adesso proviamo che $G/\rho_\phi = G/H \cap K$

così che la ϕ_* in (1) è una funzione del tipo richiesto per (a).

Calcoliamo ρ_ϕ. Per ogni $g_1, g_2 \in G$,

$$g_1 \rho_\phi g_2 \iff \phi(g_1) = \phi(g_2) \iff$$

$$\iff (g_1 H, g_1 K) = (g_2 H, g_2 K) \iff$$

$$\iff (g_1 H = g_2 H) \;\&\; (g_1 K = g_2 K) \iff$$

$$\iff (g_2^{-1} g_1 \in H) \;\&\; (g_2^{-1} g_1 \in K) \iff$$

$$\iff g_2^{-1} g_1 \in (H \cap K) \iff g_1 \rho^s_{H\cap K} g_2$$

dove $\rho^s_{H\cap K}$ è la relazione (di equivalenza!) sinistra in G associata al sottogruppo $H \cap K$. Dunque è

$$g_1 \rho_\phi g_2 \iff g_1 \rho^s_{H\cap K} g_2 \quad (\forall g_1, g_2 \in G)$$

QUINDI è $\rho_\phi = \rho^s_{H\cap K}$

da cui segue che $G/\rho_\phi = G/\rho^s_{H\cap K}$

Ora ricordiamo anche che (per un fatto generale) si ha

$$[g]_{\mathcal{C}^s_{H\wedge K}} = g\,(H\wedge K) \qquad \forall g \in G$$

e quindi $\boxed{G/\mathcal{C}^s_{H\wedge K} = G/(H\wedge K)}$

Pertanto, da $[g]_{\mathcal{C}_\phi} = [g]_{\mathcal{C}^s_{H\wedge K}} = g\,(H\wedge K)$ e

$$G/\mathcal{C}_\phi = G/\mathcal{C}^s_{H\wedge K} = G/H\wedge K$$

concludiamo che la (1) è in effetti una funzione iniettiva

$$\varphi := \phi_* : G/H\wedge K \longrightarrow G/H \times G/K$$
$$g\,(H\wedge K) \longmapsto (gH, gK)$$

del tipo richiesto, q.e.d.

(b) Supponiamo che $H \trianglelefteq G$ e $K \trianglelefteq G$, cioè i sottogruppi H e K sono normali. Allora è $gHg^{-1} \subseteq H$ e $gKg^{-1} \subseteq K$, $\forall g \in G$; $\Rightarrow$

$$\Rightarrow g(H\wedge K)g^{-1} \subseteq (gHg^{-1}) \wedge (gKg^{-1}) \subseteq H\wedge K$$
$$\forall g \in G$$

cioè $g(H \cap K)g^{-1} \subseteq H \cap K \qquad \forall g \in G$

QUINDI $H \cap K$ (che già sappiamo essere un sottogruppo) è normale, q.e.d.

(c) Se $H \trianglelefteq G$ e $K \trianglelefteq G$ allora G/H e G/K hanno le strutture canoniche di gruppo quoziente.

Inoltre, per (b) è anche $H \cap K \trianglelefteq G$, quindi anche $G/H \cap K$ ha la struttura canonica di gruppo quoziente.

Infine, il prodotto cartesiano $G/H \times G/K$ ha la struttura naturale di gruppo prodotto diretto, per il quale l'operazione è

$$(g_1 H, g_2 K) \cdot (g_1' H, g_2' K) :=$$
$$:= (g_1 H \cdot g_1' H, g_2 K \cdot g_2' K)$$
$$\left(= (g_1 g_1' H, g_2 g_2' K) \right)$$

Ora, con riferimento alla costruzione fatta per dimostrare (a), la funzione

$$\phi : G \longrightarrow G/H \times G/K$$
$$g \longmapsto \phi(g) := (gH, gK)$$

è chiaramente un morfismo di gruppi

(in breve, perché lo sono le proiezioni canoniche $G \xrightarrow{\pi_H} G/H$ e $G \xrightarrow{\pi_K} G/K$, $g \longmapsto gH$, $g \longmapsto gK$)

e allora anche la funzione iniettiva

$$\varphi := \phi_* : G/_{H\cap K} = G/_{\mathcal{C}\phi} \hookrightarrow G/H \times G/K$$
$$g(H\cap K) \longmapsto (gH, gK)$$

associata a ϕ dal Teorema Fondamentale è a sua volta un morfismo di gruppi, q.e.d.

(d) Se $H \trianglelefteq G$ e $K \trianglelefteq G$ e i gruppi quoziente G/H e G/K sono abeliani, allora anche il prodotto diretto $G/H \times G/K$ è abeliano. Ne segue che è abeliano anche il suo sottogruppo $\mathrm{Im}(\varphi)$, con $\varphi : G/_{H\cap K} \hookrightarrow G/H \times G/K$ morfismo (di gruppi) iniettivo come in (c).

Siccome $\varphi : G/_{H \cap K} \hookrightarrow G/_H \times G/_K$ è iniettiva, la sua corestrizione a $Im(\varphi)$ ci dà un isomorfismo

$$\varphi' : G/_{H \cap K} \xrightarrow{\cong} Im(\varphi)$$
$$g(H \cap K) \longmapsto \varphi'(g) := \varphi(g)$$

così che $\boxed{G/_{H \cap K} \cong Im(\varphi)}$.

Infine, dato che abbiamo visto che $Im(\varphi)$ è abeliano, concludiamo che anche $G/_{H \cap K}$ è abeliano, q.e.d. □

CONTINUA

5 Sia S un insieme di irriducibili in $\mathbb{Z}$, con $S \subseteq \mathbb{Z}_+$. Per tale S definiamo il sottoinsieme di $\mathbb{Q}$

$$\mathbb{Z}_S := \left\{ n/d \in \mathbb{Q} \;\middle|\; \begin{array}{l} \text{i fattori irriducibili} \\ \text{di } d \text{ appartengono a } S \end{array} \right\}$$

dimostrare che:

(a) $\mathbb{Z}_S$ è sottoanello di $\mathbb{Q}$;

(b) se S' e S'' sono due insiemi di irriducibili come sopra, allora

$$S' \subseteq S'' \iff \mathbb{Z}_{S'} \leq \mathbb{Z}_{S''}$$

dove "$\leq$" significa "è sottoanello di".

Svolgimento:

(a) (I) $0_{\mathbb{Q}} = 0/1 \in \mathbb{Z}_S$ perché i fattori irriducibili di 1 (nessuno!) stanno in S

(II) $\forall\ n'/d', n''/d'' \in \mathbb{Z}_S$, si ha

$$\left(\frac{n'}{d'} - \frac{n''}{d''} \right) \in \mathbb{Z}_S$$

Infatti, siano $d' = s'_1 \cdots s'_{k'}$, $d'' = s''_1 \cdots s''_{k''}$

fattorizzazioni di d' e d'' in irriducibili,
con $s'_1, \dots, s'_{k'}, s''_1, \dots, s''_{k''} \in S$ per ipotesi.

Allora $$\frac{n'}{d'} - \frac{n''}{d''} = \frac{n'd'' - n''d'}{d'd''} \qquad (*)$$

con $d'd'' = \underbrace{s'_1 \cdots s'_{k'} \cdot s''_1 \cdots s''_{k''}}$
fattori irriducibili in S

quindi $(*)$ ci dà $\left(\frac{n'}{d'} - \frac{n''}{d''}\right) \in \mathbb{Z}_S$, q.e.d.

(III) Con la stessa notazione di (II) si ha

$\forall\ n'/d', n''/d'' \in \mathbb{Z}_S$, si ha

$\frac{n'}{d'} \cdot \frac{n''}{d''} \in \mathbb{Z}_S$, perché

$$\frac{n'}{d'} \cdot \frac{n''}{d''} = \frac{n'n''}{d'd''} \quad \text{con}$$

$d'd'' = \underbrace{s'_1 \cdots s'_{k'} \cdot s''_1 \cdots s''_{k''}}$
irriducibili in S

Le proprietà (I), (II) e (III) ci dicono che
$\mathbb{Z}_S$ è sottoanello di $\mathbb{Q}$, q.e.d.

(b-) $S' \subseteq S'' \Rightarrow \mathbb{Z}_{S'} \subseteq \mathbb{Z}_{S''}$

è ovvio per definizione! Poi, siccome $\mathbb{Z}_{S'}$ e $\mathbb{Z}_{S''}$ sono entrambi sottoanelli di $\mathbb{Q}$, da $\mathbb{Z}_{S'} \subseteq \mathbb{Z}_{S''}$ segue subito che $\mathbb{Z}_{S'} \leq \mathbb{Z}_{S''}$, q-e-d.

VICEVERSA

supponiamo che $\mathbb{Z}_{S'} \leq \mathbb{Z}_{S''}$ (che è equivalente a $\mathbb{Z}_{S'} \subseteq \mathbb{Z}_{S''}$) e dimostriamo che allora $S' \subseteq S''$.

Per ogni $s' \in S'$ si ha

$$\frac{1}{s'} \in \mathbb{Z}_{S'} \quad \& \quad \mathbb{Z}_{S'} \leq \mathbb{Z}_{S''}$$

$$\frac{1}{s'} \in \mathbb{Z}_{S''} \Rightarrow \frac{1}{s'} = \frac{n''}{d''} \text{ con}$$

$n'', d'' \in \mathbb{Z}$, $d'' = s''_1 \cdots s''_k$ per certi elementi $s''_1, \dots, s''_k \in S''$

ORA $\frac{1}{s'} = \frac{n''}{d''} \Rightarrow d'' = s' n'' \Rightarrow$

$\Rightarrow \quad s_1'' \cdots s_k'' = d'' = s' n'' \quad \Rightarrow$

$\Rightarrow$ per la fattorizzazione unica in $\mathbb{Z}_s$,

$\exists \; l \in \{1, \ldots, k''\} : \quad s_l'' = s' \; , \quad \Rightarrow$

$\Rightarrow \quad s' = s_l'' \in S'' \quad \Rightarrow \quad s' \in S''$

DUNQUE abbiamo

$s' \in S'', \quad \forall \, s' \in S',$

CIOÈ $\quad S' \subseteq S'', \quad$ q.e.d. $\square$

CONTINUA

6 Nell'anello $\mathbb{Z}[i]$ degli interi di Gauss si considerino

$$A := 7+4i, \quad B := 3+i, \quad C' := 1+3i, \quad C'' := 5$$

(a) Determinare se l'equazione diofantea

$$A \cdot X + B \cdot Y = C' \qquad \text{in } \mathbb{Z}[i]$$

abbia soluzioni; se sì, se ne calcoli una.

(b) Idem – di (a) – per

$$A \cdot X + B \cdot Y = C''$$

(c) Calcolare $MCD(A, B)$.

Svolgimento:

Dalla teoria generale delle equazioni diofantee in un dominio a ideali principali $\mathcal{D}$, sappiamo che

$$\tilde{A} \cdot X + \tilde{B} \cdot Y = \tilde{C} \qquad (\tilde{A}, \tilde{B}, \tilde{C} \in \mathcal{D})$$

ha soluzioni se e soltanto se

$MCD(\tilde{A}, \tilde{B})$ divide $\tilde{C}$

QUINDI cominciamo da (c), calcolando $MCD(A, B)$, e poi affrontiamo (a) e (b).

(c) Siccome $\mathbb{Z}[i]$ è un dominio euclideo, possiamo calcolare $MCD(A,B)$ tramite l'algoritmo euclideo delle divisioni successive. I calcoli danno

$$\underset{\text{ii}}{A} = \underset{\text{ii}}{B} \cdot q_1 + r_1$$

$$7+4i = (3+i)\cdot q_1 + r_1$$

con q_1 e r_1 calcolati così:

$$\kappa := \frac{7+4i}{3+i} = \frac{(7+4i)\cdot(3-i)}{(3+i)(3-i)} = \frac{5}{2} + \frac{1}{2}i$$

Tale κ è in $\mathbb{Q}[i]$, dobbiamo approssimarlo in modo ottimale con un $q_1 \in \mathbb{Z}[i]$: ponendo $q_1 = z_0 + z_1 i$ con $z_0, z_1 \in \mathbb{Z}$, dev'essere

$$\left|z_0 - \tfrac{5}{2}\right| \leq \tfrac{1}{2}, \quad \left|z_1 - \tfrac{1}{2}\right| \leq 1$$

$\rightsquigarrow$ le possibilità sono

$$z_0 \in \{3, 2\} \quad \& \quad z_1 \in \{1, 0\}$$

QUINDI per q_1 ci sono quattro opzioni

$$q_1 \in \{3+i,\ 3,\ 2+i,\ 2\}$$

A seguire, r_1 si calcola poi come

$$r_1 := A - B \cdot q_1 = (7+4i) - (3+i) \cdot q_1$$

Secondo la scelta fatta per q_1, si trova

① $q_1 = 3+i \Rightarrow r_1 = (7+4i) - (3+i)(3+i) = -1-2i$

② $q_1 = 3 \Rightarrow r_1 = (7+4i) - (3+i) \cdot 3 = -2+i$

③ $q_1 = 2+i \Rightarrow r_1 = (7+4i) - (3+i)(2+i) = 2-i$

④ $q_1 = 2 \Rightarrow r_1 = (7+4i) - (3+i) \cdot 2 = 1+2i$

Come secondo passo, dopo (1) operiamo una seconda divisione, di B per r_1

$$B = r_1 \cdot q_2 + r_2 \qquad (2)$$

$\Rightarrow$ secondo la scelta di (q_1, r_1) - come in ① $\rightarrow$ ④ qui sopra - la (2) diventa

① $B = (-1-2i) \cdot (-1+i) + 0$

② $B = (-2+i) \cdot (-1-i) + 0$

③ $B = (2-i) \cdot (1+i) + 0$

④ $B = (1+2i) \cdot (1-i) + 0$

$\rightarrow$ RESTO $= 0$

In ciascun caso, il resto r_2 in questa seconda divisione è 0, QUINDI l'algoritmo si arresta e ci dice che

$$MCD(A,B) = r_1 = \begin{cases} -1-2i \\ -2+i \\ 2-i \\ 1+2i \end{cases} \Rightarrow (5\text{pt})$$

N.B.: com'è giusto che sia, i quattro valori trovati per $MCD(A,B)$ sono a due a due associati, cioè si trovano l'uno dall'altro moltiplicando per un invertibile in $\mathbb{Z}[i]$, cioè per $+1, -1, +i$ o $-i$. Ad esempio, è $(-2+i) = (-1-2i)\cdot(-i)$.

(a) Controlliamo se c'è divisibilità

$$MCD(A,B) \;\delta_{\mathbb{Z}[i]}\; C' \quad ???$$

Prendendo $MCD(A,B) = -1-2i$ si ha

$$\mathbb{Q}[i] \ni \frac{C'}{MCD(A,B)} = \frac{1+3i}{-1-2i} =$$

$$= \frac{(1+3i)(-1+2i)}{(-1-2i)(-1+2i)} = \frac{(-1-6)+(-3+2)i}{5} = -\frac{7}{5} - \frac{1}{2}i$$

così $\dfrac{C'}{MCD(A,B)} = -\frac{7}{5} - \frac{1}{2}i \in \mathbb{Q}[i] \setminus \mathbb{Z}[i]$

e quindi, siccome $\dfrac{C'}{MCD(A,B)} \notin \mathbb{Z}[i]$, si ha

$MCD(A,B) \not\delta_{\mathbb{Z}[i]} C'$, $\Rightarrow$

$\Rightarrow \nexists$ soluzioni di $AX+BY=C'$ in $\mathbb{Z}[i]$

Siccome esprimendo $MCD(A,B)$ tramite il valore in ①, ②, ③ o ④ si altera soltanto per un fattore in $\mathbb{Z}[i]$ invertibile, la condizione $MCD(A,B)\ \delta_{\mathbb{Z}[i]}\ C'$ è sempre vera o falsa indipendentemente dalla espressione di $MCD(A,B)$ come r_1, r_2, r_3 o r_4.

(b) Calcoliamo se c'è divisibilità (in $\mathbb{Z}[i]$)

$MCD(A,B)\ \delta_{\mathbb{Z}[i]}\ C''$???

Prendendo $MCD(A,B) = -1-2i$ si ha

$$\mathbb{Q}[i] = \frac{C''}{MCD(A,B)} = \frac{5}{-1-2i} = \frac{5\cdot(-1+2i)}{(-1-2i)(-1+2i)} =$$

$$= \frac{-5+10i}{5} = -1+2i \in \mathbb{Z}[i], \Rightarrow$$

$\Rightarrow$ QUINDI $MCD(A,B) \;\delta_{\mathbb{Z}[i]}\; C''$

e perciò $\exists$ soluzioni dell'equazione diofantea $A \cdot X + B \cdot Y = C''$ (*)

Per calcolare esplicitamente una soluzione di (*), ci serve una identità di Bézout per $MCD(A,B)$: questa la ricaviamo dalle divisioni con resto fatte per trovare $MCD(A,B)$ tramite l'algoritmo euclideo. In questo caso, poiché tale $MCD(A,B)$ è semplicemente il primo resto r_1 calcolato nella prima divisione, come identità di Bézout abbiamo semplicemente

$MCD(A,B) = r_1 = A \cdot 1 + B \cdot (-q_1)$, cioè

① $MCD(A,B) = A \cdot 1 + B \cdot (-3-i)$

② $MCD(A,B) = A \cdot 1 + B \cdot (-3)$

③ $MCD(A,B) = A \cdot 1 + B \cdot (-2-i)$

④ $MCD(A,B) = A \cdot 1 + B \cdot (-2)$

Da queste, si ottiene una soluzione di (*)

moltiplicando i coefficienti di A e B per $t := \frac{c''}{MCD(A,B)}$, così che si ha

$$A \cdot t + B \cdot (-q_1 t) = c''$$

di modo che la coppia $(t, -q_1 t)$ è soluzione di ⊛. Esplicitamente, nei quattro casi troviamo

① $(t, -q_1 t) = (-1+2i,\ 5-5i)$

② $(t, -q_1 t) = (-2-i,\ 6+3i)$

③ $(t, -q_1 t) = (2+i,\ -3-4i)$

④ $(t, -q_1 t) = (1-2i,\ -2+4i)$

che sono tutte soluzioni di ⊛, q.e.d. □