IX Settimana

1. Elementi basilari della teoria dei gruppi

- Una *operazione (binaria)* $*$ su un insieme G è un'applicazione:

$$* : G \times G \to G \, .$$

Per semplicità di notazione, il corrispondente in G di un elemento $(x, y) \in G \times G$, tramite l'operazione $*$, si denota con $x * y$ (invece che $*((x, y))$, usuale notazione della teoria delle applicazioni).

- Un *gruppo* $(G, *)$ è un insieme non vuoto G dotato di un'operazione $*$ che soddisfa alle seguenti proprietà:

(Gr1) L'operazione $*$ verifica *la proprietà associativa:*

$$\forall x, y, z \in G \, , \quad ((x * y) * z) = (x * (y * z)) \, .$$

(Gr2) L'operazione $*$ possiede *un elemento neutro,* cioè un elemento $u \in G$ tale che:

$$\forall x \in G \, , \quad x * u = x * u = x \, .$$

(Gr3) Ogni elemento x di G possiede *un inverso* rispetto a $*$, cioè un elemento $x' \in G$, tale che:

$$x * x' = u = x' * x \, .$$

- Un gruppo $(G, *)$ per il quale, inoltre, si ha che:

(Gr4) L'operazione $*$ verifica *la proprietà commutativa,* cioè:

$$\forall x, y \in G \, , \quad x * y = y * x \, ,$$

viene chiamato un *gruppo abeliano* (o, meno comunemente, un *gruppo commutativo*).

Proposizione 1.1. *Sia $(G, *)$ un gruppo. Allora:*

(1) *L'elemento neutro di $(G, *)$ è unico.*

(2) *Per ogni elemento di G, l'elemento inverso, rispetto a $*$, è unico.*

(3) *Valgono le leggi di cancellazione:*

$$\forall x, y, z \in G \, , \quad x * y = x * z \quad \Rightarrow \quad y = z \quad \textit{(legge di cancellazione a sinistra)} \, ;$$
$$\forall x, y, z \in G \, , \quad y * x = z * x \quad \Rightarrow \quad y = z \quad \textit{(legge di cancellazione a destra)} \, .$$

Dimostrazione. **(1)** Se $u_1, \ u_2$ sono due elementi neutri di $(G, *)$, allora:

$$u_1 \overset{(a)}{=} u_1 * u_2 \overset{(b)}{=} u_2$$

[(a): perché u_2 è un'unità di $(G, *)$; (b): perché u_1 è un'unità di $(G, *)$].

(2) Se $x', \ x''$ sono due inversi di $x \in G$, allora:

$$x'' = u * x'' = (x' * x) * x'' = x' * (x * x'') = x' * u = x' \, .$$

(3) Per la legge di cancellazione a sinistra, "moltiplicando" a sinistra per l'inverso x' di x otteniamo:

$x * y = x * z \quad \Rightarrow \quad x' * (x * y) = x' * (x * z)$ cioè $(x' * x) * y = (x' * x) * z \quad \Rightarrow \quad y = z \, .$

In maniera simile (speculare) si dimostra la validità della legge di cancellazione a destra. □

Semplificazione delle notazioni,
passaggio alla notazione moltiplicativa: $* \rightsquigarrow \cdot$

Per non appesantire le notazioni, invece di usare la notazione " $*$ ", la generica operazione di un gruppo viene indicata con " $\cdot$ " e si dice che si sta utilizzando una *notazione moltiplicativa*. Con tale notazione, si pone semplicemente:

▶ $xy := x \cdot y$ (per denotare *il composto o prodotto di* (x, y) *rispetto alla operazione* $\cdot$ *del gruppo*);

▶ $1 := u$ (per denotare *l'elemento neutro rispetto all'operazione di prodotto*);

▶ $x^{-1} := x'$ (per denotare *l'elemento inverso di* x *rispetto all'operazione di prodotto*).

---

passaggio alla notazione additiva: $* \rightsquigarrow +$

Altre volte (usualmente quando si tratta di gruppi abeliani) si preferisce usare una *notazione additiva* (cioè, invece di usare la notazione " $*$ ", la generica operazione di un gruppo viene indicata con " $+$ "). Con tale notazione, si scrive semplicemente

▶ $x + y$ (per denotare *il composto o somma di* (x, y) *rispetto all'operazione* $+$ *del gruppo*);

▶ $0 := u$ (per denotare *l'elemento neutro rispetto all'operazione di somma*);

▶ $-x := x'$ (per denotare *l'elemento "inverso" di* x *rispetto all'operazione di somma*).

Proposizione 1.2. *Sia* $(G, \cdot)$ *un gruppo. Allora:*

(1) $\forall x, y \in G\,,\ (xy)^{-1} = y^{-1}x^{-1}\,.$

(2) $\forall x \in G\,,\ (x^{-1})^{-1} = x\,.$

Dimostrazione. Entrambe le affermazioni sono conseguenza dell'unicità dell'inverso di un elemento.

Per **(1)** , basta osservare che:

$$\begin{aligned}(y^{-1}x^{-1})(xy) &= y^{-1}(x^{-1}x)y = y^{-1}\cdot 1\cdot y = y^{-1}y = 1\,;\\ (xy)(y^{-1}x^{-1}) &= x(yy^{-1})x^{-1} = x\cdot 1\cdot x^{-1} = xx^{-1} = 1\,.\end{aligned}$$

Per **(2)** , basta osservare che:

$$xx^{-1} = 1 = x^{-1}x\,,$$

quindi x è l'inverso di x^{-1}. □

Osservazione 1.3. La proposizione precedente, in notazione additiva, si traduce nella forma seguente: *Sia* $(G,+)$ *un gruppo. Allora:*

(1) $\forall x,y\in G\,,\ -(x+y)=(-y)+(-x)\,.$
(2) $\forall x\in G\,,\ -(-x)=x\,.$

Esempio 1.4. (1) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, $(\mathbb{Z}[i],+)$ sono gruppi abeliani, dove:

$$\mathbb{Z}[i]:=\{a+ib\mid a,b\in\mathbb{Z}\}\ (\subsetneq\mathbb{C})\,.$$

$(\mathbb{Z}[i],+)$ è chiamato *il gruppo degli interi di Gauss.*

(2) $(\mathbb{N},+)$ *non* è un gruppo (non verifica la proprietà **(Gr3)**).

(3) Sia $\mathbb{Z}^*$ [rispettivamente, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$, $\mathbb{Z}[i]^*$] l'insieme $\mathbb{Z}\setminus\{0\}$ [rispettivamente, $\mathbb{Q}\setminus\{0\},\mathbb{R}\setminus\{0\},\mathbb{C}\setminus\{0\}$, $\mathbb{Z}[i]\setminus\{0\}$]. Allora $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$ sono gruppi abeliani, mentre $(\mathbb{Z}^*,\cdot)$ e $(\mathbb{Z}[i]^*\cdot)$ *non* sono gruppi (non verificano la proprietà **(Gr3)**).

(4) $(\{-1,1\},\cdot\,)$ è un gruppo abeliano.

(5) $(\{-1,1,-i,i\},\cdot\,)$ è un gruppo abeliano.

(6) Per ogni intero $n\geq 2$, consideriamo l'insieme-quoziente di $\mathbb{Z}$ rispetto alla relazione di equivalenza $\equiv_n$ (congruenza modulo n):

$$\frac{\mathbb{Z}}{\equiv_n}:=\{[k]_n\mid k\in\mathbb{Z}\}=\{[0]_n,[1]_n,,\dots,[n-1]_n\}\,.$$

Allora, $(\mathbb{Z}/\equiv_n,+)$ è un gruppo abeliano (dove, $[a]_n+[b]_n:=[a+b]_n$).

(7) Per ogni intero $n\geq 2$, consideriamo l'insieme:

$$\mathbf{U}\left(\frac{\mathbb{Z}}{\equiv_n}\right):=\{[x]_n\mid \mathrm{MCD}(x,n)=1\,,\ 1\leq x\leq n-1\}$$

(avente $\varphi(n)$ elementi) sottoinsieme dell'insieme-quoziente $\mathbb{Z}/\equiv_n$ (avente n elementi). Allora, $(\mathbf{U}(\mathbb{Z}/\equiv_n),\cdot\,)$ è un gruppo abeliano (dove, $[a]_n\cdot[b]_n:=[ab]_n$).
Si noti che se $n=p$ è un numero primo allora:

$$\mathbf{U}\left(\frac{\mathbb{Z}}{\equiv_p}\right)=\left(\frac{\mathbb{Z}}{\equiv_p}\right)^*:=\frac{\mathbb{Z}}{\equiv_p}\setminus\{[0]_p\}\,.$$

(8) Sia $n\geq 1$ un intero fissato e sia $\boldsymbol{C}_n:=\{z\in\mathbb{C}\mid z^n=1\}$. Non è difficile verificare che $(\boldsymbol{C}_n,\cdot\,)$ è un gruppo abeliano (formato da n numeri complessi che giacciono sulla circonferenza unitaria di centro l'origine del piano di Argand-Gauss e che suddividono in n–parti uguali tale circonferenza):

$$\boldsymbol{C}_n=\left\{\zeta_n^k:=\cos\left(\frac{2k\pi}{n}\right)+i\sin\left(\frac{2k\pi}{n}\right)=e^{\frac{2k\pi i}{n}}\mid 0\leq k\leq n-1\right\}\,.$$

Tale gruppo è detto *gruppo delle radici n–esime dell'unità.*
Casi particolari: per $n=2$, $(\boldsymbol{C}_2,\cdot\,)$ è il gruppo dell'esempio **(4)**; per $n=4$, $(\boldsymbol{C}_4,\cdot\,)$ è il gruppo dell'esempio **(5)**.

(9) Siano n,m due interi positivi. Poniamo:

$$\boldsymbol{n}:=\{1,2,\dots,n\}\,,\quad \boldsymbol{m}:=\{1,2,\dots,m\}\,.$$

Sia $R\in\{\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{Z}[i]\}$. L'insieme $R^{\boldsymbol{n}\times\boldsymbol{m}}$ delle applicazioni dall'insieme prodotto cartesiano $\boldsymbol{n}\times\boldsymbol{m}$ all'insieme R, viene chiamato *insieme delle matrici ad n righe ed m colonne ad entrate in R*, e viene denotato con $\boldsymbol{M}_{n,m}(R)$. Il generico

elemento (matrice) A di $\boldsymbol{M}_{n,m}(R)$ viene denotato più o meno esplicitamente in una delle forme seguenti:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,m} \\ a_{2,1} & a_{2,2} & \dots & a_{2,m} \\ \dots & \dots & \dots & \dots \\ a_{n,1} & a_{n,2} & \dots & a_{n,m} \end{pmatrix} = (a_{i,j})_{\substack{1 \le i \le n \\ 1 \le j \le m}} = (a_{i,j}) \, .$$

Dati due elementi in $\boldsymbol{M}_{n,m}(R)$, definiamo la loro somma nella maniera seguente:

$$(a_{i,j}) + (b_{i,j}) := (a_{i,j} + b_{i,j}) \, .$$

Allora, $(\boldsymbol{M}_{n,m}(R), +)$ è un gruppo abeliano.

(10) Sia $K \in \left\{ \mathbb{Q}, \, \mathbb{R}, \, \mathbb{C}, \, \frac{\mathbb{Z}}{\equiv_p} \right\}$ e sia $K^* := K \setminus \{0\}$. Consideriamo:

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \, , \; X := \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \boldsymbol{M}_{2,2}(K) \, .$$

Definiamo un prodotto tra matrici quadrate di $\boldsymbol{M}_{2,2}(K)$ (chiamato *prodotto righe* $\times$ *colonne*), nella maniera seguente:

$$A \cdot X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} := \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix} \, .$$

Non è difficile verificare che $A \cdot X \in \boldsymbol{M}_{2,2}(K)$ e che la matrice:

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

è l'elemento neutro rispetto al prodotto " $\cdot$ " (righe$\times$colonne) di matrici, cioè, per ogni $A \in \boldsymbol{M}_{2,2}(K)$,

$$A \cdot I = A = I \cdot A \, .$$

Si noti anche che il prodotto (righe$\times$colonne) di matrici *non* verifica la proprietà commutativa cioè, in generale, $A \cdot X \neq X \cdot A$. Ad esempio, se:

$$B := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \, , \; C := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in \boldsymbol{M}_{2,2}(K) \, ,$$

$$B \cdot C = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = C \cdot B \, .$$

Da questo esempio si ricava facilmente che non ogni matrice in $\boldsymbol{M}_{2,2}(K)$ possiede un inverso rispetto al prodotto (righe$\times$colonne) di matrici. Infatti, ad esempio, non può esistere un'inversa della matrice B in $\boldsymbol{M}_{2,2}(K)$, perché, per ogni matrice $X \in \boldsymbol{M}_{2,2}(K)$, si ha:

$$B \cdot X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \, .$$

Pertanto, $(\boldsymbol{M}_{2,2}(K), \cdot)$ *non* è un gruppo.

Tuttavia, un importante sottoinsieme $\boldsymbol{M}_{2,2}(K)$ che passiamo a descrivere è un gruppo. Per fare ciò definiamo il *determinante di* $A \in \boldsymbol{M}_{2,2}(K)$ nella maniera seguente:

$$\mathsf{det}(A) := ad - bc \in K \, .$$

Non è difficile verificare che, presi comunque due elementi in $\boldsymbol{M}_{2,2}(K)$:

$$A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{e} \quad X := \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

allora il determinante "preserva" il prodotto, cioè:

$$\mathsf{det}(A \cdot X) = \mathsf{det}(A) \cdot \mathsf{det}(X) \, .$$

Poniamo:

$$\mathrm{GL}_2(K) := \{A \in \boldsymbol{M}_{2,2}(K) \mid \mathsf{det}(A) \neq 0\} \, ,$$

gli elementi di $\mathrm{GL}_2(K)$ sono detti *matrici non singolari di* $\boldsymbol{M}_{2,2}(K)$. Allora, $(\mathrm{GL}_2(K), \cdot\,)$ è un gruppo *non* abeliano.
Innanzitutto, dalla proprietà che il determinante preserva il prodotto si ricava che:

$$A, B \in \mathrm{GL}_2(K) \quad \Rightarrow \quad A \cdot B \in \mathrm{GL}_2(K) \, .$$

Inoltre, la matrice I, elemento neutro del prodotto (righe×colonne) di matrici, appartiene a $\mathrm{GL}_2(K)$. Si calcola , poi, in modo diretto che ogni matrice $A \in \mathrm{GL}_2(K)$ ha un inversa rispetto al prodotto " $\cdot$ " (righe×colonne) di matrici. Precisamente l'inversa della matrice A è la matrice:

$$A^{-1} := \begin{pmatrix} \frac{d}{\mathsf{det}(A)} & \frac{-b}{\mathsf{det}(A)} \\ \frac{-c}{\mathsf{det}(A)} & \frac{a}{\mathsf{det}(A)} \end{pmatrix} \in \mathrm{GL}_2(K) \, .$$

Infatti:

$$A \cdot A^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \frac{d}{\mathsf{det}(A)} & \frac{-b}{\mathsf{det}(A)} \\ \frac{-c}{\mathsf{det}(A)} & \frac{a}{\mathsf{det}(A)} \end{pmatrix} = I = \begin{pmatrix} \frac{d}{\mathsf{det}(A)} & \frac{-b}{\mathsf{det}(A)} \\ \frac{-c}{\mathsf{det}(A)} & \frac{a}{\mathsf{det}(A)} \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A^{-1} \cdot A \, .$$

(Si osservi che $\mathsf{det}(A^{-1}) = (\mathsf{det}(A))^{-1} \in K^*$.)
Si noti infine che abbiamo già osservato che il prodotto di matrici non è commutativo. Pertanto $(\mathrm{GL}_2(K), \cdot)$ è un gruppo non abeliano.

(11) Sia X un insieme non vuoto e sia $\mathrm{Bij}(X) = \{f : X \to X \mid f \text{ è una biiezione}\}$. Allora su $\mathrm{Bij}(X)$ possiamo operare con l'operazione di prodotto operatorio " $\circ$ " tra applicazioni. Non è difficile verificare che $(\mathrm{Bij}(X), \circ\,)$ è un gruppo (non abeliano).

Un caso particolare dell'esempio precedente è il seguente.

(12) Sia $\boldsymbol{n} := \{1, 2, \ldots, n\}$ l'insieme finito formato dai primi n interi positivi. Allora $\mathrm{Bij}(\{\boldsymbol{n}\})$ viene usualmente denotato con $\boldsymbol{S}_n$. Gli elementi di $\boldsymbol{S}_n$ vengono chiamati *permutazioni* oppure *sostituzioni* di $\{1, 2, \ldots, n\}$. Un elemento $\sigma : \boldsymbol{n} \to \boldsymbol{n}$ di $\boldsymbol{S}_n$ che agisce nella maniera seguente $k \mapsto \sigma(k)$, per $1 \leq k \leq n$, viene usualmente descritto da una matrice $2 \times n$ del tipo:

$$\sigma := \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} \, .$$

[Si noti che, σ è una biiezione se e soltanto se l'insieme $\{\sigma(1), \sigma(2), \ldots, \sigma(n)\}$ coincide con l'insieme $\{1, 2, \ldots, n\}$.]

Se $\sigma,\ \tau \in \boldsymbol{S}_n$, allora il prodotto operatorio $\tau \circ \sigma \in \boldsymbol{S}_n$ è descritto da:

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \ldots & \tau(\sigma(n)) \end{pmatrix} \, .$$

Si noti che alcuni autori preferiscono la notazione " $\sigma\tau$ " per denotare il composto " $\tau \circ \sigma$ ".
Non è difficile verificare che $(\boldsymbol{S}_n, \circ)$ è un gruppo non abeliano, avente come elemento neutro la permutazione identica:

$$\mathrm{id}_{\boldsymbol{n}} := \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix} \, .$$

Ad esempio se $n = 3$ allora $\boldsymbol{S}_3$ consiste dei seguenti 6 $(= 3!)$ elementi:

$$\mathrm{id}_{\mathbf{3}} := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \tau := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\alpha := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \beta := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \gamma := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

E' subito visto che:

$$\begin{aligned}
\sigma^2 :=& \quad \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha \,; \\
\sigma^3 :=& \quad \sigma \circ \sigma \circ \sigma = \sigma \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \mathrm{id}_{\mathbf{3}} = \alpha \circ \sigma \,; \\
\tau \circ \sigma =& \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \beta \,; \\
\sigma \circ \tau =& \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \gamma \,; \\
\tau^2 :=& \quad \tau \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id}_{\mathbf{3}} \,; \\
\sigma^2 \circ \tau =& \quad \alpha \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \beta \,. \\
\tau \circ \sigma^2 =& \quad \tau \circ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \gamma \,.
\end{aligned}$$

Da tali relazioni si ricava ad esempio:

$$\begin{aligned}
\beta \circ \sigma =& \quad (\tau \circ \sigma) \circ \sigma = \tau \circ \sigma^2 = \tau \circ \alpha = \gamma \,; \\
\sigma \circ \beta =& \quad \sigma \circ (\sigma^2 \circ \tau) = \sigma^3 \circ \tau = \tau \,; \\
\gamma \circ \sigma =& \quad (\sigma \circ \tau) \circ \sigma = \sigma \circ (\tau \circ \sigma) = \sigma \circ \beta = \tau \,; \\
\sigma \circ \gamma =& \quad \sigma \circ (\sigma \circ \tau) = \sigma^2 \circ \tau = \beta \,; \\
\beta \circ \tau =& \quad (\sigma^2 \circ \tau) \circ \tau = \sigma^2 \circ \tau^2 = \sigma^2 = \alpha \,; \\
\tau \circ \beta =& \quad \tau \circ (\tau \circ \sigma) = \tau^2 \circ \sigma = \sigma \,; \\
\gamma \circ \tau =& \quad (\sigma \circ \tau) \circ \tau = \sigma \circ \tau^2 = \sigma \,; \\
\tau \circ \gamma =& \quad \tau \circ (\tau \circ \sigma^2) = \tau^2 \circ \sigma^2 = \sigma^2 = \alpha \,.
\end{aligned}$$

Dati dei sottoinsiemi X, Y, S di un gruppo $(G, \cdot)$, poniamo:

$$\begin{aligned}
XY :=& \quad \{xy \mid x \in X \,, y \in Y\} \,. \\
S^{-1} :=& \quad \{s^{-1} \mid s \in S\} \,.
\end{aligned}$$

• Un sottoinsieme non vuoto H di un gruppo $(G, \cdot)$ si dice un *sottogruppo* se le proprietà seguenti sono verificate:

(S-Gr1) $HH \subseteq H$ (cioè, H è chiuso rispetto alla operazione di G);

(S-Gr2) $1 \in H$ (cioè, l'elemento neutro del gruppo G appartiene ad H);

(S-Gr3) $H^{-1} \subseteq H$ (cioè, l'inverso di ogni elemento di H appartiene ancora ad H).

Osservazione 1.5. Si noti che un sottoinsieme non vuoto H di un gruppo $(G, \cdot)$ è un sottogruppo di $(G, \cdot)$ se e soltanto se $(H, \cdot)$ è un gruppo (cioè, se H con la stessa operazione $\cdot$ di G, ristretta agli elementi di H, è un gruppo).

Proposizione 1.6. *Sia $(G,\cdot)$ un gruppo ed H un sottoinsieme non vuoto di G.*

$$H \text{ è un sottogruppo di } G \quad \Leftrightarrow \quad HH^{-1} \subseteq H\,.$$

(in altre parole, H è un sottogruppo di G se e soltanto se $xy^{-1} \in H$, presi comunque $x, y \in H$).

Dimostrazione. ($\Rightarrow$) E' ovvio che, se H è un sottogruppo di G e se $x, y \in H$, allora $y^{-1} \in H$, e quindi $xy^{-1} \in H$ ovvero $HH^{-1} \subseteq H$.

($\Leftarrow$) Supponiamo che $xy^{-1} \in H$, presi comunque $x, y \in H$. Allora, per $y = x$, abbiamo che $xx^{-1} = 1 \in H$. Per $x = 1$ e per ogni $y \in H$, abbiamo che $1 \cdot y^{-1} = y^{-1} \in H$. Presi comunque $x, y \in H$, abbiamo visto che $y^{-1} \in H$, allora dall'ipotesi ricaviamo che $x(y^{-1})^{-1} = xy \in H$. □

Se $(G,\cdot)$ è un gruppo ed H è un sottoinsieme non vuoto di G, allora si pone:

$H \leq G$ per indicare che H è un sottogruppo di G.
$H < G$ per indicare che H è un sottogruppo proprio di G.

Osservazione 1.7. In notazione additiva, dati dei sottoinsiemi X, Y, S di un gruppo $(G,+)$, poniamo:

$$\begin{aligned} X + Y &:= \{x + y \mid x \in X\,, y \in Y\}\,. \\ -S &:= \{-s \mid s \in S\}\,. \\ X - Y &:= X + (-Y) = \{x + (-y) =: x - y \mid x \in X\,, y \in Y\}\,. \end{aligned}$$

- Allora, un sottoinsieme H di $(G,+)$ è un sottogruppo se:
  (S-Gr1) $H + H \subseteq H$ (cioè, H è chiuso rispetto alla operazione di G);
  (S-Gr2) $0 \in H$ (cioè, l'elemento neutro del gruppo G appartiene ad H);
  (S-Gr3) $-H \subseteq H$ (cioè, l'inverso additivo di ogni elemento di H appartiene ancora ad H).

Infine, la proposizione precedente, in notazione additiva, si enuncia:

$$H \text{ è un sottogruppo di } G \quad \Leftrightarrow \quad H - H \subseteq H\,.$$

(in altre parole, H è un sottogruppo di G se e soltanto se $x-y \in H$, presi comunque $x, y \in H$).

Esempio 1.8. **(1)** Nel gruppo $(\mathbb{C},+)$ si ha:

$$\mathbb{Z} \lneq \mathbb{Q} \lneq \mathbb{R} \lneq \mathbb{C} \quad \text{e} \quad \mathbb{Z}[i] \lneq \mathbb{C}\,.$$

Notare che, nel gruppo $(\mathbb{Z},+)$, si ha che $\mathbb{N} \subsetneq \mathbb{Z}$, ma $\mathbb{N} \not\leq \mathbb{Z}$.

(2) Nel gruppo $(\mathbb{C}^*,\cdot\,)$ si ha:

$$\mathbb{Q}^* \lneq \mathbb{R}^* \lneq \mathbb{C}^*\,.$$

Notare che, nel gruppo $(\mathbb{Q}^*,\cdot\,)$, si ha che $\mathbb{Z}^* \subsetneq \mathbb{Q}^*$, ma $\mathbb{Z}^* \not\leq \mathbb{Q}^*$. Similmente, nel gruppo $(\mathbb{C}^*,\cdot\,)$, si ha che $\mathbb{Z}[i]^* \subsetneq \mathbb{C}^*$, ma $\mathbb{Z}[i]^* \not\leq \mathbb{C}^*$.

(3) L'insieme $\mathbb{R}^> := \{x \in \mathbb{R} \mid x \gneq 0\}$ dei numeri reali positivi, sottoinsieme dell'insieme di tutti i numeri reali non nulli $\mathbb{R}^*$, è un sottogruppo di $(\mathbb{R}^*,\cdot\,)$.
(Si noti che $0 < x\,,\ 0 < y \ \Rightarrow\ 0 < xy$. Inoltre:

$$0 < x < 1 \quad \Rightarrow \quad 1 < x^{-1}\,; \qquad 1 < x \quad \Rightarrow \quad 0 < x^{-1} < 1\,.)$$

- Dato un gruppo $(G,\cdot)$, si chiama *il centro di* $(G,\cdot)$ il sottoinsieme:

$$\mathbf{Z}(G) := \{x \in G \mid gx = xg\,, \quad \forall g \in G\}\,.$$

Si noti che $(G,\cdot)$ è un gruppo abeliano se e soltanto se $G = \mathbf{Z}(G)$.

Proposizione 1.9. *Sia $(G,\cdot)$ un gruppo. Allora $\mathbf{Z}(G)$ è un sottogruppo di $(G,\cdot)$. Inoltre $(\mathbf{Z}(G),\cdot)$ è un gruppo abeliano.*

Dimostrazione. Innanzitutto, è ovvio (per la definizione stessa di $\mathbf{Z}(G)$) che $gh = hg$, presi comunque $g,h \in \mathbf{Z}(G)$. Siano $g,h \in \mathbf{Z}(G)$, mostriamo che gh^{-1} appartiene ancora a $\mathbf{Z}(G)$. Infatti, preso comunque $x \in G$, poniamo $y := x^{-1}$, allora:

$$\begin{aligned}(gh^{-1})x = &\quad gh^{-1}y^{-1} = g(yh)^{-1} = g(hy)^{-1} = \\ = &\quad (gy^{-1})h^{-1} = (y^{-1}g)h^{-1} = (xg)h^{-1} = x(gh^{-1})\,.\end{aligned}$$ □

Esempio 1.10. Sia $K \in \left\{\mathbb{Q},\mathbb{R},\mathbb{C},\frac{\mathbb{Z}}{\equiv_p}\right\}$ e sia $K^* := K \setminus \{0\}$. Non è difficile verificare che:

$$\mathbf{Z}(\mathrm{GL}_2(K)) = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in K^*\right\}\,.$$

Proposizione 1.11. *Sia $(G,\cdot)$ un gruppo e sia $(H_i \mid i \in I)$ una famiglia non vuota di sottogruppi di $(G,\cdot)$. Allora $\cap_{i\in I} H_i$ è un sottogruppo di $(G,\cdot)$.*

Dimostrazione.

$x,y \in \cap_{i\in I} H_i \;\Rightarrow\; x,y \in H_i,\ \forall i \in I \;\Rightarrow\; xy^{-1} \in H_i,\ \forall i \in I \;\Rightarrow\; xy^{-1} \in \cap_{i\in I} H_i$.□

- Dato un gruppo $(G,\cdot)$, un elemento $g \in G$ ed un intero positivo $n > 0$, si definisce *potenza n–esima di g*, l'elemento:

$$g^n := \underbrace{g \cdot g \cdot \ldots \cdot g}_{n \text{ volte}}\,.$$

Si definisce *potenza $(-n)$–esima di g*, la potenza n–esima di g^{-1}, cioè l'elemento:

$$g^{-n} := \underbrace{g^{-1} \cdot g^{-1} \cdot \ldots \cdot g^{-1}}_{n \text{ volte}}\,.$$

Se $n = 0$, si pone $g^0 := 1$. Si dimostra facilmente che, presi comunque $n,m \in \mathbb{Z}$, valgono le seguenti uguaglianze (tra elementi di G):

$$g^n g^m = g^{n+m}\,, \quad (g^n)^m = g^{nm}\,, \quad (g^n)^{-1} = g^{-n}\,.$$

Osservazione 1.12. Dato un gruppo $(G,+)$, con notazione additiva, un elemento $g \in G$ ed un intero positivo $n > 0$, si definisce *multiplo n–esimo di g*, l'elemento:

$$ng := \underbrace{g + g + \ldots + g}_{n \text{ volte}}\,.$$

Si definisce *multiplo $(-n)$–esimo di g*, il multiplo n–esimo di $-g$, cioè l'elemento:

$$-ng := \underbrace{(-g) + (-g) + \ \ldots\ + (-g)}_{n \text{ volte}}\,.$$

Se $n = 0$, si pone $0g := 0$. Inoltre, presi comunque $n, m \in \mathbb{Z}$, valgono le seguenti uguaglianze (tra elementi di G):

$$ng + mg = (n+m)g\ , \quad m(ng) = (mn)g\ , \quad -(ng) = -ng\ .$$

- Dato un sottoinsieme S di un gruppo $(G, \cdot)$, si dice *sottogruppo di G generato da S* il più piccolo sottogruppo di $(G, \cdot)$, che contiene S. In altre parole, tale sottogruppo, denotato con $\langle S \rangle$, è definito nella maniera seguente:

$$\langle S \rangle := \bigcap_{S \subseteq H \leq G} H\ ,$$

cioè, $\langle S \rangle$ coincide con l'intersezione della famiglia (non vuota) di tutti i sottogruppi di $(G, \cdot)$ che contengono (come sottoinsieme) S.

- Caso particolarmente importante è quello di un sottoinsieme S consistente di un unico elemento g. In tal caso, il sottogruppo $\langle \{g\} \rangle$ viene denotato anche, più semplicemente, con $\langle g \rangle$ e viene chiamato *sottogruppo ciclico di $(G, \cdot)$ generato da g*.

Proposizione 1.13. *Sia $(G, \cdot)$ un gruppo e sia $g \in G$. Allora $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.*

Osservazione 1.14. Si noti che, se $(G, \cdot)$ è un gruppo e se $g \in G$, non è detto che gli elementi di $\{g^n \mid n \in \mathbb{Z}\}$ siano tutti distinti. Ad esempio, quando G è finito, deve accadere necessariamente che, per due interi positivi distinti $n \neq m$, si abbia $g^n = g^m$. Dunque, in particolare, se ad esempio (per fissare le idee) $n > m$ (nota che, comunque, uno dei due interi deve essere maggiore dell'altro), allora $g^{n-m} = 1$, con $n - m > 0$.

- Chiamiamo *ordine* (od anche, *periodo*) di un elemento $g \neq 1$ di un gruppo $(G, \cdot)$ il più piccolo intero positivo s (se esiste) tale che $g^s = 1$; in tal caso, scriveremo $\mathrm{Ord}(g) := s$. Se $g^n \neq 1$ per ogni intero $n > 0$, allora diremo che g ha *ordine* (o, *periodo*) *infinito*; in tal caso scriveremo $\mathrm{Ord}(g) := \infty$. Se $g = 1$, porremo $\mathrm{Ord}(g) := 1$.

- Si chiama *ordine di un gruppo* $(G, \cdot)$ la cardinalità dell'insieme G; precisamente, se G è un insieme finito con m elementi, si pone $\mathrm{Ord}(G) := m$, se invece G è un insieme infinito, si pone $\mathrm{Ord}(G) := \infty$.

Osservazione 1.15. Se il gruppo è assegnato in notazione additiva, allora *ordine* (od anche, *periodo*) di un elemento $g \neq 0$ di un gruppo $(G, +)$ il più piccolo intero positivo s (se esiste) tale che $sg = 0$; in tal caso, scriveremo $\mathrm{Ord}(g) := s$. Se $ng \neq 0$ per ogni intero $n > 0$, allora diremo che g ha *ordine* (o, *periodo*) *infinito*; in tal caso scriveremo $\mathrm{Ord}(g) := \infty$. Se $g = 0$, porremo $\mathrm{Ord}(g) := 1$.

Proposizione 1.16. *Sia $(G, \cdot)$ un gruppo e sia $g \in G$.*

(1) $\mathrm{Ord}(g) = \infty$ *se e soltanto se $g^n \neq g^m$, per $n, m \in \mathbb{Z}$, con $n \neq m$. In tal caso (e soltanto in tal caso) $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ è un sottogruppo infinito di $(G, \cdot)$.*

(2) $\mathrm{Ord}(g) = s$ $(< \infty)$ *se e soltanto se* $\langle g \rangle = \{g^r \mid 0 \leq r \leq s-1\}$. *In tal caso (e soltanto in tal caso)* $\langle g \rangle$ *è un sottogruppo finito di* $(G, \cdot)$, *con esattamente* s *elementi distinti. Inoltre, in tale situazione:*

$$g^n = g^m \quad \Leftrightarrow \quad n \equiv m \pmod{s} .$$

• Un gruppo $(G, \cdot)$ si dice *ciclico generato da un suo elemento* g, se $G = \langle g \rangle$. Un *gruppo ciclico* può essere *finito od infinito*; precisamente se $(G, \cdot)$ è ciclico generato da un suo elemento g, allora $\mathrm{Ord}(G) = \mathrm{Ord}(g)$.
Si noti che un gruppo ciclico è necessariamente un gruppo abeliano.

Esempio 1.17. (1) In $(\mathbb{Z}, +)$ ogni elemento non nullo ha ordine infinito. Inoltre, $(\mathbb{Z}, +)$ è un gruppo ciclico infinito generato dall'elemento 1 (oppure, dall'elemento -1).

(2) In $(\mathbb{Z}/\equiv_4, +)$, si ha $\mathrm{Ord}([0]_4) = 1$, $\mathrm{Ord}([1]_4) = 4$, $\mathrm{Ord}([2]_4) = 2$, $\mathrm{Ord}([3]_4) = 4$. Quindi, $(\mathbb{Z}/\equiv_4, +)$ è un gruppo ciclico finito di ordine 4, generato da $[1]_4$ (oppure da $[3]_4$). Questo esempio (come il precedente) mostra che un gruppo ciclico finito (od infinito) può avere più di un generatore.

(3) In generale, $(\mathbb{Z}/\equiv_n, +)$ è un gruppo ciclico di ordine n generato da $[1]_n$, in quanto $\mathrm{Ord}([1]_n) = n$.

(4) $(\{-1, 1\}, \cdot\,)$ è un sottogruppo di $(\mathbb{Q}^*, \cdot\,)$, detto *gruppo delle radici seconde dell'unità* . Inoltre, $(\{-1, 1\}, \cdot)$ è un gruppo ciclico di ordine 2 generato da -1.

(5) $(\{-1, 1, i, -i\}, \cdot\,)$ è un sottogruppo di $(\mathbb{C}^*, \cdot\,)$, detto *gruppo delle radici quarte dell'unità* . Inoltre, $(\{-1, 1, i, -i\}, \cdot\,)$ è un gruppo ciclico di ordine 4 generato dall'elemento i (oppure, da $-i$). Si noti infatti che $\mathrm{Ord}(1) = 1$, $\mathrm{Ord}(-1) = 2$, $\mathrm{Ord}(-i) = 4$, $\mathrm{Ord}(i) = 4$.

(6) Fissato comunque un intero $n \geq 1$, il gruppo $(\boldsymbol{C}_n, \cdot\,)$ è un gruppo ciclico di ordine n generato dall'elemento $\zeta_n := \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) = e^{\frac{2\pi i}{n}}$, detto *radice primitiva* n*–esima dell'unità.*

Proposizione 1.18. *Sia* $(G, \cdot)$ *un gruppo ciclico con* $G = \langle g \rangle$. *Sia* H *un sottogruppo di* $(G, \cdot)$.

(1) *Se* $(G, \cdot)$ *è un gruppo ciclico infinito, allora anche* H *è un gruppo ciclico infinito.*

(2) *Se* $(G, \cdot)$ *è un gruppo ciclico finito di ordine* s, *allora anche* H *è un gruppo ciclico finito di ordine* s', *con* $s' \mid s$, *generato da* g^t, *dove* t *è il più piccolo intero positivo nell'insieme (non vuoto)* $\{n > 0 \mid g^n \in H\}$.

• Dati due gruppi $(G, *)$ e $(G', \star)$, un'applicazione $f : G \to G'$ si dice *un omomorfismo di gruppi* se:

$$f(x * y) = f(x) \star f(y) , \quad \forall x, y \in G ,$$

cioè, se il corrispondente del composto di due elementi in G coincide con il composto in G' dei corrispondenti dei due elementi. In altre parole, *un omomorfismo di gruppi è un'applicazione che conserva le operazioni.*

• Un omomorfismo di gruppi, *che è anche un'applicazione biiettiva*, viene chiamato un *isomorfismo di gruppi.*

• Dati due gruppi $(G,*)$ e $(G',\star)$, denotiamo con u l'elemento neutro (rispetto a $*$) di G e con u' l'elemento neutro (rispetto a $\star$) di G'. Sia $f : G \to G'$ un omomorfismo di gruppi, poniamo:

$$\begin{aligned} \mathrm{Ker}(f) &:= \{x \in G \mid f(x) = u'\} = f^{-1}(u') \ (\subseteq G)\,, \\ \mathrm{Im}(f) &:= \{x' \in G' \mid f(x) = x',\ \text{per qualche } x \in G\} = f(G) \ (\subseteq G')\,, \end{aligned}$$

dove $\mathrm{Ker}(f)$ è detto *nucleo dell'omomorfismo* f, $\mathrm{Im}(f)$ *è detta immagine dell'omomorfismo* f.

Proposizione 1.19. *Dati due gruppi* $(G,*)$ *e* $(G',\star)$ *ed un omomorfismo di gruppi* $f : G \to G'$, *allora:*

(1) $f(u) = u'$ *(l'immagine dell'elemento neutro di* G *deve coincidere con l'elemento neutro di* G'*).*
(2) $f(x^{-1}) = f(x)^{-1}$ *(l'immagine dell'inverso di un elemento* x *di* G *deve coincidere con l'inverso in* G' *dell'immagine in* G' *dell'elemento* x*).*
(3) $\mathrm{Im}(f)$ *è un sottogruppo di* $(G',\star)$.
(4) $\mathrm{Ker}(f)$ *è un sottogruppo di* $(G,*)$.
(5) $f : G \to G'$ *è un omomorfismo iniettivo se e soltanto se* $\mathrm{Ker}(f) = \{u\}$.

Dimostrazione. (1) Preso comunque $x \in G$, allora:

$$f(x) \star u' = f(x) = f(x * u) = f(x) \star f(u) \quad \overset{(a)}{\Rightarrow} \quad u' = f(u)$$

[(a): per la legge di cancellazione a sinistra in $(G',\star)$].

(2) $u' = f(u) = f(x * x^{-1}) = f(x) \star f(x^{-1})$ e, similmente, $u' = f(u) = f(x^{-1} * x) = f(x^{-1}) \star f(x)$.

(3) $x' = f(x)$, $y' = f(y) \in \mathrm{Im}(f) \ \Rightarrow\ x' \star {y'}^{-1} = f(x) \star f(y)^{-1} = f(x) \star f(y^{-1}) = f(x * y^{-1}) \in \mathrm{Im}(f)$.

(4) $x,\ y \in \mathrm{Ker}(f) \ \Rightarrow\ f(x) = u' = f(y) \ \Rightarrow\ f(x * y^{-1}) = f(x) \star f(y^{-1}) = f(x) \star f(y)^{-1} = u' \star {u'}^{-1} = u' \star u' = u' \ \Rightarrow\ x * y^{-1} \in \mathrm{Ker}(f)$.

(5) ($\Rightarrow$) Se, per assurdo, $\{u\} \subsetneq \mathrm{Ker}(f)$ e se $x \in \mathrm{Ker}(f)$, con $x \neq u$, allora $f(x) = u' = f(u)$. Ciò contraddice l'ipotesi che f è iniettiva.

($\Leftarrow$) Se, per assurdo, $x, y \in G$, con $x \neq y$ e $f(x) = f(y)$, allora $u' = f(x) \star f(y)^{-1} = f(x) \star f(y^{-1}) = f(x * y^{-1})$. Dunque, $x * y^{-1} \in \mathrm{Ker}(f)$, con $x * y^{-1} \neq u$ (perché, $x \neq y$). □

Esempio 1.20. (1) Preso comunque un intero $n \geq 2$, l'applicazione:

$$\pi_n : \mathbb{Z} \to \frac{\mathbb{Z}}{\equiv_n}\,, \qquad k \mapsto [k]_n$$

determina un omomorfismo dal gruppo $(\mathbb{Z},+)$ al gruppo $(\frac{\mathbb{Z}}{\equiv_n},+)$.
Si verifica facilmente che:

$$\mathrm{Ker}(\pi_n) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}\,, \qquad \mathrm{Im}(\pi_n) = \frac{\mathbb{Z}}{\equiv_n}\,.$$

(2) Sia $K \in \left\{\mathbb{Q}, \mathbb{R}, \mathbb{C}, \frac{\mathbb{Z}}{\equiv_p}\right\}$. Allora, l'applicazione:

$$\mathsf{det} : \mathrm{GL}_2(K) \to K^*\,, \qquad A \mapsto \mathsf{det}(A)$$

definisce un omomorfismo dal gruppo $(\mathrm{GL}_2(K),\cdot)$ al gruppo $(K^*,\cdot)$. Si verifica facilmente che:

$$\mathrm{Ker}(\mathsf{det}) = \{A \in \mathrm{GL}_2(K) \mid \mathsf{det}(A) = 1\}\,, \qquad \mathrm{Im}(\mathsf{det}) = K^*\,.$$

(3) L'applicazione "logaritmo" in base 10, denotata "Log" [rispettivamente, in base e, denotata "log"],

$$\begin{array}{rl} & \mathrm{Log} : \mathbb{R}^{>} \to \mathbb{R} \ , \quad x \mapsto \mathrm{Log}(x) \ , \\ [\text{rispettivamente}, & \log : \mathbb{R}^{>} \to \mathbb{R} \ , \quad x \mapsto \log(x) \,] \end{array}$$

definisce un omomorfismo di gruppi da $(\mathbb{R}^{>}, \cdot\,)$ a $(\mathbb{R}, +)$. Infatti, dalla definizione di logaritmo (cioè, $r := \mathrm{Log}(x) :\Leftrightarrow 10^r = x$ [rispettivamente, $r := \log(x) :\Leftrightarrow e^r = x$]) discende che, presi comunque $x, y \in \mathbb{R}^{>}$,

$$\mathrm{Log}(xy) = \mathrm{Log}(x) + \mathrm{Log}(y) \ \ [\text{rispettivamente, } \log(xy) = \log(x) + \log(y) \,] \, .$$

Da tale proprietà si può far discendere che:

$$\begin{array}{rll} & \mathrm{Log}(1) = 0 \, , & \mathrm{Log}(x^{-1}) = -\mathrm{Log}(x) \\ [\text{rispettivamente}, & \log(1) = 0 \, , & \log(x^{-1}) = -\log(x) \,] \, . \end{array}$$

Si noti, infine che:

$$\begin{array}{rll} & \mathrm{Ker}(\mathrm{Log}) = \{1\} \, , & \mathrm{Im}(\mathrm{Log}) = \mathbb{R} \, , \\ [\text{rispettivamente}, & \mathrm{Ker}(\log) = \{1\} \, , & \mathrm{Im}(\log) = \mathbb{R} \, ,] \end{array}$$

pertanto Log e log sono due isomorfismi di gruppi. L'applicazione "esponenziale" in base 10, denotata "Exp" [rispettivamente, in base e , , denotata "exp"],

$$\begin{array}{rl} & \mathrm{Exp} : \mathbb{R} \to \mathbb{R}^{>} \, , \quad r \mapsto \mathrm{Exp}(r) := 10^r \, , \\ [\text{rispettivamente}, & \exp : \mathbb{R} \to \mathbb{R}^{>} \, , \quad r \mapsto \exp(r) := e^r \,] \end{array}$$

è l'applicazione inversa dell'applicazione biiettiva Log [rispettivamente, log], cioè $(\mathrm{Log})^{-1} = \mathrm{Exp}$ [rispettivamente, $(\log)^{-1} = \exp$], ed inoltre essa definisce un omomorfismo biiettivo di gruppi da $(\mathbb{R}, +)$ a $(\mathbb{R}^{>}, \cdot\,)$.

(4) L'applicazione:

$$f : \mathbb{R} \to \mathbb{C}^* \, , \quad r \mapsto \cos(r) + i \cdot \mathrm{sen}(r) \, ,$$

definisce un omomorfismo dal gruppo $(\mathbb{R}, +)$ al gruppo $(\mathbb{C}^*, \cdot\,)$. Si noti che:

$$\begin{array}{rl} \mathrm{Ker}(f) = & \{r \in \mathbb{R} \mid f(r) = 1\} = \{r = 2\pi n \mid n \in \mathbb{Z}\} =: 2\pi\mathbb{Z} \, , \\ \mathrm{Im}(f) = & \{z \in \mathbb{C}^* \mid z = f(r) \, , \, \exists r \in \mathbb{R}\} = \{z = x + iy \in \mathbb{C}^* \mid x^2 + y^2 = 1\} \, . \end{array}$$

• Un sottogruppo H di un gruppo $(G, \cdot)$ determina sempre due relazioni di equivalenza su G, chiamate *relazioni di equivalenza su G associate al suo sottogruppo H,* definite nella mariera seguente: presi $x, y \in G$, allora:

$$\begin{array}{rll} x \ \varepsilon'_{_H} \ y & :\Leftrightarrow & xy^{-1} \in H \, ; \\ x \ \varepsilon''_{_H} \ y & :\Leftrightarrow & x^{-1}y \in H \, . \end{array}$$

Non è difficile mostrare che:

$$\begin{array}{rll} x \ \varepsilon'_{_H} \ y & \Leftrightarrow & Hx = Hy \, ; \\ x \ \varepsilon''_{_H} \ y & \Leftrightarrow & xH = yH \, , \end{array}$$

e, quindi, che le relative classi di equivalenza di un elemento $x \in G$ sono date da:

$$[x]_{\varepsilon'_{_H}} = Hx = \{hx \mid h \in H\} \, , \quad [x]_{\varepsilon''_{_H}} = xH = \{xh \mid h \in H\} \, .$$

• I sottoinsiemi di G del tipo Hx [rispettivamente, xH], che descrivono la partizione di G associata alla relazione di equivalenza $\varepsilon'_{_H}$ [rispettivamente, $\varepsilon''_{_H}$], sono chiamati *classi laterali sinistre [respettivamente, destre] di G modulo il sottogruppo H.*

Lemma 1.21. *Dato un sottogruppo H di un gruppo $(G,\cdot)$, allora:*

$$\varepsilon'_{H} = \varepsilon''_{H} \quad \Leftrightarrow \quad gH = Hg\,,\ \forall g \in G\,.$$

In particolare, se $(G,\cdot)$ è un gruppo abeliano $\varepsilon'_{H} = \varepsilon''_{H}$, per ogni sottogruppo H di G.

- Un sottogruppo N di un gruppo $(G,\cdot)$ si dice *un sottogruppo normale di G* se $gN = Ng$ (o, equivalentemente, $gNg^{-1} = N$), preso comunque $g \in G$.

Esempio 1.22. **(1)** Dato un gruppo $(G,\cdot)$, dalla definizione stessa di centro di un gruppo, discende immediatamente che $\mathbf{Z}(G)$ è un sottogruppo normale di $(G,\cdot)$.

(2) Ogni sottogruppo di un gruppo abeliano è normale.

Se N è un sottogruppo normale, poniamo:

$$\varepsilon_{N} := \varepsilon'_{N} = \varepsilon''_{N}\,,$$

allora l'insieme-quoziente

$$\frac{G}{N} := \frac{G}{\varepsilon'_{N}} = \frac{G}{\varepsilon''_{N}}$$

ha come elementi classi di equivalenza, le quali possono esplicitarsi nella maniera seguente:

$$[g]_{\varepsilon'_{N}} = [g]_{\varepsilon''_{N}} = gN := \{gx \mid x \in N\}\,,$$

al variare di $g \in G$, cioè:

$$\frac{G}{N} = \{gN \mid g \in G\}\,.$$

Proposizione 1.23. *Dato un sottogruppo normale N di un gruppo $(G,\cdot)$, siano $g, g', h, h' \in G$, allora:*

$$g\,\varepsilon_{N}\,h \ \wedge \ g'\,\varepsilon_{N}\,h' \quad \Rightarrow \quad gg'\,\varepsilon_{N}\,hh'\,.$$

Dimostrazione.

$$gg'(hh')^{-1} = gg'h'^{-1}h^{-1} \overset{(a)}{\subseteq} gNh^{-1} \overset{(b)}{=} gh^{-1}N \overset{(c)}{\subseteq} NN \subseteq N\,.$$

[(a): perché $g'\,\varepsilon_{N}\,h'$; (b): perché N è un sottogruppo normale; (c): perché $g\,\varepsilon_{N}\,h$.] □

Nell'insieme-quoziente $\frac{G}{N}$ si può definire un'operazione, dedotta canonicamente dalla operazione $\cdot$ di G, nella maniera seguente:

$$gN \cdot g'N := (g \cdot g')N\,.$$

(Si noti che un'operazione $\cdot$ tra classi laterali di un gruppo modulo un suo sottogruppo, come quella descritta sopra, è ben definita –cioè, è indipendente dalla scelta dei rappresentanti delle classi– se e soltanto se il sottogruppo è normale.)

Proposizione 1.24. *Dato un sottogruppo normale N di un gruppo $(G,\cdot)$, allora $(\frac{G}{N},\cdot)$ è un gruppo, chiamato* il gruppo-quoziente di G rispetto al sottogruppo normale N. Inoltre, se $(G,\cdot)$ è un gruppo abeliano, allora $(\frac{G}{N},\cdot)$ è anch'esso abeliano.

Dimostrazione. Presi comunque $x, y, z \in G$, allora $(xN \cdot yN) \cdot zN = (xyN) \cdot zN = (xy)zN = x(yz)N = xN \cdot yzN = xN \cdot (yN \cdot zN)$.

$1 \cdot N = N$ è l'elemento neutro di $(\frac{G}{N}, \cdot)$.

L'inverso di un elemento xN di $\frac{G}{N}$ è l'elemento $x^{-1}N$.

Infine si noti che, se $(G, \cdot)$ è abeliano allora, presi comunque $x, y \in G$, $xN \cdot yN = xyN = yxN = yN \cdot xN$. □

Esempio 1.25. Sia $n \geq 2$ un intero fissato. Nel gruppo $(\mathbb{Z}, +)$, la relazione di equivalenza ε_N associata al suo sottogruppo (normale) $N := n\mathbb{Z}$, coincide con la relazione di congruenza $\equiv_n$. Pertanto, l'insieme sottogiacente al gruppo-quoziente $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$ coincide con $\frac{\mathbb{Z}}{\equiv_n}$ e, dunque, per ogni $x \in \mathbb{Z}$:

$$x + n\mathbb{Z} \;=\; [x]_{\equiv_n} \;=\; \{y \in \mathbb{Z} \mid\; y \equiv x \pmod{n}\}\,.$$

In particolare:

$$n\mathbb{Z} \;=\; [0]_{\equiv_n}\,.$$

Proposizione 1.26. *Dati due gruppi $(G, *)$ e $(G', \star)$ ed un omomorfismo di gruppi $f : G \to G'$, allora* $\mathrm{Ker}(f)$ *è un sottogruppo normale di $(G, *)$.*

Dimostrazione. Già abbiamo dimostrato che $\mathrm{Ker}(f)$ è un sottogruppo di $(G, *)$ (Proposizione 1.19 (4)). Se poi $g \in G$, allora per ogni $k \in \mathrm{Ker}(f)$, si ha $g * k * g^{-1} \in \mathrm{Ker}(f)$ [perché $f(g * k * g^{-1}) = f(g) \star f(k) \star f(g^{-1}) = f(g) \star u' \star f(g^{-1}) = f(g) \star f(g^{-1}) = f(g * g^{-1}) = f(u) = u'$]. Quindi $g * k \in \mathrm{Ker}(f) * g$, da cui si ricava che $g * \mathrm{Ker}(f) \subseteq \mathrm{Ker}(f) * g$. Similmente si dimostra che $\mathrm{Ker}(f) * g \subseteq g * \mathrm{Ker}(f)$. □

Teorema 1.27. (Teorema Fondamentale dell'Omomorfismo tra gruppi) *Dati due gruppi $(G, *)$ e $(G', \star)$ ed un omomorfismo di gruppi $f : G \to G'$, allora esiste un isomorfismo di gruppi, che denotiamo con $f^{\#}$, canonicamente associato ad f, da $(\frac{G}{\mathrm{Ker}(f)}, *)$ a $(\mathrm{Im}(f), \star)$, (ben)definito nella maniera seguente:*

$$f^{\#}(g * \mathrm{Ker}(f)) := f(g)\,, \quad \forall g \in G\,.$$

Più precisamente, un qualunque omomorfismo $f : G \to G'$ di gruppi si può fattorizzare nel prodotto operatorio di un omomorfismo suriettivo *di gruppi:*

$$\pi_f : G \twoheadrightarrow \frac{G}{\mathrm{Ker}(f)}\,, \qquad g \mapsto g * \mathrm{Ker}(f)\,,$$

un isomorfismo *di gruppi :*

$$f^{\#} : \frac{G}{\mathrm{Ker}(f)} \xrightarrow{\sim} \mathrm{Im}(f)\,, \qquad g * \mathrm{Ker}(f) \mapsto f(g)\,,$$

ed un omomorfismo iniettivo *di gruppi:*

$$j_f : \mathrm{Im}(f) \hookrightarrow G'\,, \qquad y \mapsto y\,,$$

cioè, $f = j_f \circ f^{\#} \circ \pi_f$. In altre parole, il seguente diagramma è commutativo:

$$\begin{array}{ccc} G & \xrightarrow{\;f\;} & G' \\ \downarrow{\scriptstyle \pi_f} & & \uparrow{\scriptstyle j_f} \\ \frac{G}{\mathrm{Ker}(f)} & \xrightarrow{\;f^{\#}\;} & \mathrm{Im}(f) \end{array}$$

Esempio 1.28. **(1)** Sia n un intero fissato e sia $f : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ l'applicazione definita da $f(x) := nx$, per ogni $x \in \mathbb{Z}$. Allora, f è un omomorfismo iniettivo di gruppi, con

$$\mathrm{Ker}(f) = \{0\}\,, \qquad \mathrm{Im}(f) = n\mathbb{Z}\,.$$

Quindi, per il Teorema Fontamentale dell'Omomorfismo tra gruppi abbiamo che:

$$\mathbb{Z} \;\cong\; \frac{\mathbb{Z}}{\{0\}} \;\cong n\mathbb{Z}\,,$$

dove il simbolo $\cong$ indica un isomorfismo tra gruppi.

(2) Sia n un intero fissato e sia $\pi_{_n} : (\mathbb{Z}, +) \to \left(\frac{\mathbb{Z}}{\equiv_{_n}}, +\right)$ l'applicazione definita da $\pi_{_n}(x) := [x]_{\equiv_{_n}}$, per ogni $x \in \mathbb{Z}$. Allora, $\pi_{_n}$ è un omomorfismo suriettivo di gruppi, con

$$\mathrm{Ker}(\pi_{_n}) = n\mathbb{Z}\,, \qquad \mathrm{Im}(\pi_{_n}) = \frac{\mathbb{Z}}{\equiv_{_n}},\,.$$

Quindi, per il Teorema Fontamentale dell'Omomorfismo tra gruppi abbiamo che:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \;\cong\; \frac{\mathbb{Z}}{\equiv_{_n}}\,.$$

(3) Sia n un intero fissato e sia $\varphi : (\mathbb{Z}, +) \to (\boldsymbol{C}_{_n}, \cdot\,)$ l'applicazione definita da $\varphi(x) := \cos(\frac{2\pi x}{n}) + i \cdot \sin(\frac{2\pi x}{n}) = e^{\frac{2\pi x i}{n}}$, per ogni $x \in \mathbb{Z}$. Allora, φ è un omomorfismo suriettivo di gruppi, con

$$\mathrm{Ker}(\varphi) = n\mathbb{Z}\,, \qquad \mathrm{Im}(\varphi) = \boldsymbol{C}_{_n}\,.$$

Quindi, per il Teorema Fontamentale dell'Omomorfismo tra gruppi abbiamo che:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \;\cong\; \boldsymbol{C}_{_n}\,.$$

* * *

Tali argomenti (e le dimostrazioni dei risultati enunciati) si possono trovare nel Capitolo 5 di [PC].

[PC] Giulia Maria Piacentini Cattaneo, *Algebra. Un approccio algoritmico.* Decibel-Zanichelli, 1996.

* * *