Lezione 2

Prerequisiti: Insiemi numerici. Lezione 1.

Gruppi e sottogruppi

In questa lezione diamo il primo esempio di *struttura algebrica astratta*: un insieme (non necessariamente numerico) dotato di operazioni definite formalmente e soggette a condizioni imposte a priori. L'origine del concetto di *gruppo* risale all'inizio dell'Ottocento, ed è dovuta ad un'idea del giovane matematico francese Evariste Galois (1811-1832). La prima definizione formale di gruppo comparirà però solo nel 1893, in un articolo di Heinrich Weber.

Definizione 2.1 Sia X un insieme non vuoto. Si dice *operazione* (*binaria*) su X ogni applicazione da $X \times X$ ad X.

Esempio 2.2 Sono operazioni su $\mathbb{R}$ l'usuale somma e l'usuale prodotto di numeri reali. Ad esempio, la somma è l'applicazione $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$ definita da $(a,b) \mapsto a+b$ per ogni $a,b \in \mathbb{R}$.

Definizione 2.3 Si dice *gruppo* ogni coppia ordinata $(G,*)$, ove G è un insieme non vuoto, e $*$ un'operazione su G verificante le seguenti condizioni:

(a) per ogni $x,y,z \in G$, $x*(y*z)=(x*y)*z$ ($*$ è *associativa*);
(b) esiste $e \in G$ tale che, per ogni $x \in G$, $x*e=e*x=x$ (esiste un *elemento neutro*);
(c) per ogni $x \in G$ esiste $\overline{x} \in G$ tale che $x*\overline{x}=\overline{x}*x=e$ (ogni elemento ammette un *simmetrico*).

Il gruppo si dice *abeliano* (o *commutativo*) se, inoltre,

(d) per ogni $x,y \in G$, $x*y=y*x$ ($*$ è *commutativa*).

Nota terminologica: Si dice anche, più informalmente, che *un gruppo è un insieme G dotato di un'operazione* $*$. A volte, se non è necessario precisare l'operazione, quest'ultima viene sottintesa e si applica il termine *gruppo* all'insieme G. Si dice anche che *G è un gruppo rispetto all'operazione* $*$.
Se l'operazione è denotata col segno +, la si dice *somma* o *addizione*, il gruppo si dice *additivo*, l'elemento neutro viene detto *zero* ed indicato con 0_G (o, semplicemente, 0, quando non sia necessario specificare il gruppo di appartenenza), ed il simmetrico prende il nome di *opposto*: l'opposto di x è denotato $-x$. Inoltre scriveremo $x-y$ al posto di $x+(-y)$.
Se l'operazione è denotata col segno $\cdot$, la si dice *prodotto* o *moltiplicazione*, il gruppo si dice *moltiplicativo*, l'elemento neutro viene detto *uno* ed indicato con 1_G (o, semplicemente, 1), ed il simmetrico prende il nome di *inverso*: l'inverso di x è denotato x^{-1}.

Esempi 2.4
1.) L'insieme degli interi $\mathbb{Z}$ è un gruppo rispetto alla usuale addizione. Infatti

(a) per ogni $a,b,c \in \mathbb{Z}$, $a+(b+c)=(a+b)+c$ ($+$ è associativa);
(b) per ogni $a \in \mathbb{Z}$, $a+0=0+a=a$ (0 è l'elemento neutro);

(c) per ogni $a \in \mathbb{Z}$, $a+(-a) = -a+a = 0$ ($-a$ è simmetrico di a).

Inoltre è un gruppo abeliano, poiché

(d) per ogni $a, b \in \mathbb{Z}$, $a+b = b+a$ ($+$ è commutativa).

2.) Sono gruppi abeliani, rispetto alle usuali addizioni, anche il campo dei numeri razionali $\mathbb{Q}$, il campo dei numeri reali $\mathbb{R}$ ed il campo dei numeri complessi $\mathbb{C}$ (per quest'ultimo si rimanda alle proprietà (a)-(d) enunciate nella Lezione 1).

Esercizio 2.5 Dire se sono gruppi
a) $(\mathbb{N}, +)$;
b) $(\mathbb{Z}, \cdot)$;
c) $(\mathbb{Q}, \cdot)$.

Svolgimento: La risposta è negativa in tutti e tre i casi.
a) $(\mathbb{N}, +)$ non è gruppo: in esso valgono le proprietà (a) (associatività) e (b) (esistenza dell'elemento neutro, che è 0), ma non vale la proprietà (c) (esistenza degli opposti). Infatti 1 non è dotato di opposto: non esiste alcun $\overline{x} \in \mathbb{N}$ tale che $1+\overline{x} = 0$. Più in generale, nessun numero naturale positivo è dotato, in $\mathbb{N}$, di un opposto. L'unico elemento di $\mathbb{N}$ avente un opposto in $\mathbb{N}$ è 0, che è opposto di se stesso.

b) $(\mathbb{Z}, \cdot)$ non è un gruppo, perché, pur valendo le proprietà (a) (associatività) e (b) (esistenza dell'elemento neutro, che è 1), non vale la proprietà (c) (esistenza degli inversi). Infatti 2 non è dotato di inverso: non esiste alcun $\overline{x} \in \mathbb{Z}$ tale che $2\overline{x} = 1$. Gli unici elementi di $\mathbb{Z}$ dotati di inverso in $\mathbb{Z}$ sono 1 e -1, ciascuno dei quali è inverso di se stesso.

c) $(\mathbb{Q}, \cdot)$ non è un gruppo, perché, pur valendo le proprietà (a) (associatività) e (b) (esistenza dell'elemento neutro, che è 1), non vale la proprietà (c) (esistenza degli inversi). Infatti 0 non è dotato di inverso: non esiste alcun $\overline{x} \in \mathbb{Q}$ tale che $0\overline{x} = 1$. Tutti i numeri razionali non nulli sono, però, dotati di inverso: per ogni $n, m \in \mathbb{Z}$, con $n, m \neq 0$, l'inverso di $\frac{n}{m}$ è $\frac{m}{n}$.

L'Esercizio 2.5 c) suggerisce come ottenere gruppi moltiplicativi dagli insiemi numerici noti.

Esempio 2.6 Sono gruppi moltiplicativi abeliani $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$. Le proprietà (a)-(d) della Definizione 2.3 sono note per i primi due: in particolare, si sa che l'inverso di un numero reale a non nullo è il suo reciproco $\frac{1}{a}$. Per $(\mathbb{C}^*, \cdot)$ si rimanda alla Lezione 1, e, precisamente, alla proprietà (h) per l'associatività, alla proprietà (e) per l'esistenza dell'elemento neutro, alla proprietà (f) per l'esistenza degli inversi, ed alla proprietà (g) per la commutatività.

Considereremo in seguito esempi di gruppi non abeliani.

Vediamo, adesso, alcune proprietà deducibili dalla Definizione 2.2, e quindi valide in ogni gruppo.

Proposizione 2.7 *(Unicità dell'elemento neutro e del simmetrico)* Sia $(G, *)$ un gruppo. Allora

(a) l'elemento neutro è unico;

(b) ogni elemento ha un unico simmetrico.

Dimostrazione: (a) Siano e_1, e_2 elementi neutri di G. Allora si ha

$$e_1 = e_1 * e_2 = e_2.$$

La prima uguaglianza deriva dal fatto che e_2 è un elemento neutro, la seconda dal fatto che e_1 è un elemento neutro.
(b) Sia $x \in G$ e siano x_1 e x_2 suoi simmetrici. Sia e l'elemento neutro di G. Allora si ha

$$x_1 = x_1 * e = x_1 * (x * x_2) = (x_1 * x) * x_2 = e * x_2 = x_2.$$

La prima e l'ultima uguaglianza seguono dal fatto che e è l'elemento neutro, la seconda dal fatto che x_2 è simmetrico di x, la terza dall'associatività di *, la quarta dal fatto che x_1 è simmetrico di x. □

Proposizione 2.8 *(Proprietà del simmetrico)* Sia $(G,*)$ un gruppo. Allora
(a) per ogni $x \in G$, $\overline{\overline{x}} = x$;
(b) per ogni $x, y \in G$, $\overline{x * y} = \overline{y} * \overline{x}$.

Dimostrazione: (a) Ciò è immediata conseguenza della parte (c) della Definizione 2.3.

(b) Siano $x, y \in G$. Sia e l'elemento neutro di G. Allora si ha

$$(x * y) * (\overline{y} * \overline{x}) = x * (y * (\overline{y} * \overline{x})) = x * ((y * \overline{y}) * \overline{x}) = x * (e * \overline{x}) = x * \overline{x} = e. \tag{1}$$

La prima e la seconda uguaglianza derivano dall'associatività, la terza dal fatto che $\overline{y}$ è il simmetrico di y, la quarta dal fatto che e è l'elemento neutro di G, l'ultima dal fatto che $\overline{x}$ è il simmetrico di x. Analogamente si prova che

$$(\overline{y} * \overline{x}) * (x * y) = e. \tag{2}$$

Dalla (1) e dalla (2) segue che $\overline{y} * \overline{x}$ è il simmetrico di $x * y$.□

Proposizione 2.9 *(Cancellabilità in un gruppo)* Sia $(G,*)$ un gruppo. Allora, per ogni $x, y, z \in G$ valgono le seguenti implicazioni:

(i) $x * y = x * z \quad \Rightarrow \quad y = z$ (x è *cancellabile a sinistra*);
(ii) $y * x = z * x \quad \Rightarrow \quad y = z$ (x è *cancellabile a destra*).

Dimostrazione: Proviamo solo (i). Siano $x, y, z \in G$. Allora valgono le seguenti implicazioni:

$$x * y = x * z \quad \Rightarrow \quad \overline{x} * (x * y) = \overline{x} * (x * z) \quad \Rightarrow \quad (\overline{x} * x) * y = (\overline{x} * x) * z \quad \Rightarrow \quad e * y = e * z \quad \Rightarrow \quad y = z.$$

La dimostrazione di (ii) è analoga.

Esercizio 2.10 Sia $(G,*)$ un gruppo. Un elemento x di G si dice *idempotente* se $x*x=x$. Provare che l'elemento neutro è l'unico elemento idempotente di G. In particolare, l'elemento neutro è simmetrico di se stesso.

Svolgimento: Sia e l'elemento neutro di G. Allora si ha $e*e=e$. Ciò prova che e è idempotente, e simmetrico di se stesso. Viceversa sia $x \in G$ idempotente. Allora $x*x=x*e$, da cui, per la cancellabilità a sinistra di x, si deduce che $x=e$. Ciò prova che l'unico elemento idempotente è e.

Il nostro prossimo obiettivo è definire, su un arbitrario insieme X di cardinalità 1, 2 o 3, un'operazione $*$ che lo renda un gruppo.

1.) Sia $X=\{x\}$ un insieme. L'unica operazione su X è quella definita da $x*x=x$. Rispetto a tale operazione, X è un gruppo abeliano. L'associatività e la commutatività sono banalmente verificate. Inoltre x è l'elemento neutro, e quindi inverso di se stesso in base all'Esercizio 2.10.

Un gruppo avente un solo elemento si dice *gruppo banale.*

2.) Sia $X=\{x,y\}$ un insieme di cardinalità 2. Scegliamo y come l'elemento neutro dell'operazione $*$ che vogliamo definire su X. Allora $y*y=y$, $x*y=y*x=x$. Resta da definire $x*x$. Poiché, in base all'Esercizio 2.10, y deve essere l'unico elemento idempotente, non potrà essere $x*x=x$. Quindi, per esclusione, dobbiamo porre $x*x=y$. Scritto ora e al posto di y, avremo così l'operazione $*$ descritta dalla seguente *tavola di composizione:*

$*$	e	x
e	e	x
x	x	e

Quest'operazione è commutativa, dotata di elemento neutro, e tale che ogni elemento abbia un simmetrico (che è poi l'elemento stesso). Si può facilmente provare che $*$ è anche associativa: si tratta di verificare 8 identità (una per ogni possibile terna ordinata di elementi di X).
Quello che abbiamo appena trovato è dunque l'unico modo per dotare un insieme di cardinalità 2 di una struttura di gruppo.

3.) Sia $X=\{x,y,z\}$ un insieme di cardinalità 3. Scegliamo z come elemento neutro dell'operazione $*$ che vogliamo definire su X. Allora $z*z=z$, $x*z=z*x=x$, $y*z=z*y=y$. Restano da definire $x*y$, $y*x$, $x*x$, $y*y$. Ora:

- sapendo che $x*z=x$, e dovendo essere x cancellabile a sinistra, deve essere $x*y \neq x$;
- sapendo che $z*y=y$, e dovendo essere y cancellabile a destra, deve essere $x*y \neq y$.

Dunque $x*y=z$. Analogamente si deduce che $y*x=z$. Si ha così che x e y sono l'uno il simmetrico dell'altro. Allora, data l'unicità del simmetrico stabilita nella Proposizione 2.7 (b), x non è simmetrico di se stesso, cioè $x*x \neq z$. D'altra parte, non essendo x idempotente, si ha anche $x*x \neq x$. Per esclusione si conclude che $x*x=y$. Analogamente si prova che $y*y=x$. (Lo si può dedurre anche nel modo seguente, in cui si tiene conto del fatto che l'operazione * deve essere associativa: $y*y=y*(x*x)=(y*x)*x=z*x=x$.) Abbiamo così ottenuto la seguente tavola di composizione, in cui abbiamo posto $e=z$:

$*$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

(3)

Per costruzione, sono verificate le proprietà (b) e (c) della Definizione 2.3. La proprietà associativa si può provare, come nel caso precedente, attraverso la verifica di un numero finito di identità (ora sono $3^3 = 27$). Quindi l'operazione appena definita è l'unica rispetto alla quale il nostro insieme sia un gruppo. Tutti i gruppi di cardinalità 3 avranno (a meno di ridenominare l'operazione e gli elementi, e di modificare l'ordine delle righe e delle colonne) una tavola di composizione uguale alla (3).
L'operazione è commutativa: ciò risulta, nella tavola di composizione, dalla simmetria rispetto alla diagonale discendente verso destra.

$*$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

La cancellabilità a sinistra equivale invece, graficamente, al fatto che in nessuna riga compaia due volte lo stesso elemento: nella riga relativa ad un elemento a, gli elementi relativi alle colonne dell'elemento b e dell'elemento c sono, rispettivamente $a*b$ ed $a*c$, distinti se lo sono b e c. La cancellabilità a destra, analogamente, equivale al fatto che nessuna colonna contenga elementi ripetuti. A fronte di ciò, avremmo potuto compilare la tavola (3) in maniera più rapida, partendo dalla parte che riguarda l'elemento neutro:

$*$	e	x	y
e	e	x	y
x	x		
y	y		

e riempiendo poi le restanti caselle secondo il principio del Sudoku.

Nota Se $(G,*)$ è un gruppo, e G è un insieme finito, il gruppo si dice *finito*, e la cardinalità di G si dice *ordine* del gruppo. Altrimenti il gruppo G si dice *infinito*.

Osservazione 2.11 Nell'Esempio 2.4, 2.) abbiamo constatato che gli insiemi numerici $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ sono tutti gruppi additivi (abeliani). Tra questi sussistono le inclusioni $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, che esprimono un confronto puramente *insiemistico*, riguardante solo gli elementi in quanto tali. Ci si può domandare se si possa stabilire, tra questi quattro gruppi, una relazione che tenga anche conto delle operazioni. La risposta è racchiusa nella nozione di *sottogruppo*.

Definizione 2.12 Sia $(G,*)$ un gruppo, e sia H un sottoinsieme non vuoto di G. Si dice che H è *chiuso* rispetto all'operazione $*$ se, per ogni $x, y \in H$, $x*y \in H$.

Esempio 2.13 Nel gruppo $(\mathbb{Z},+)$, il sottoinsieme $\mathbb{N}$ è chiuso rispetto all'operazione +: infatti la somma di due numeri naturali è sempre un numero naturale. Invece non è chiuso il sottoinsieme $S = \{0,1\}$, in quanto $1+1 = 2 \notin S$.

Definizione 2.14 Sia $(G,*)$ un gruppo, e sia H un sottoinsieme non vuoto di G**,** chiuso rispetto all'operazione $*$. Si dice *operazione* $*$ *ristretta* ad H (o *restrizione* ad H dell'operazione $*$) l'operazione $*_H$ su H così definita: per ogni $x, y \in H$, si pone $x *_H y = x * y$.

Nota Le Definizioni 2.12 e 2.14 si possono estendere ai sottoinsiemi non vuoti di un qualsiasi insieme dotato di un'operazione. Solitamente, per abuso di notazione, l'operazione e l'operazione ristretta si denotano con lo stesso simbolo. L'uguaglianza della Definizione 2.14 suggerisce di farlo, ed in effetti ciò non solo è naturale, ma anche estremamente pratico nelle applicazioni. Tuttavia è bene ricordare che, formalmente, l'operazione ristretta è altra cosa rispetto all'operazione di partenza. Infatti, se, in base alla Definizione 2.1, $*$ è un'applicazione da $G \times G$ a G, $*_H$ è un'applicazione da $H \times H$ ad H: cambiano quindi, in generale, sia l'insieme di partenza sia quello di arrivo, il che produce un'applicazione diversa.

Esempio 2.15 La restrizione della somma di $\mathbb{Z}$ ad $\mathbb{N}$ è la somma di numeri naturali. Entrambe le operazioni vengono denotate con il simbolo +.

Definizione 2.16 Sia $(G,*)$ un gruppo, e sia H un sottoinsieme non vuoto di G. Allora H si dice un sottogruppo di G se

(a) H è chiuso rispetto all'operazione $*$;
(b) H è un gruppo rispetto all'operazione $*$ ristretta.

In tal caso si scrive anche $H < G$.

Esempio 2.17 (a) Sia G un gruppo. Allora G è sottogruppo di se stesso (*sottogruppo totale*). Inoltre, se e è l'elemento neutro di G, il gruppo $\{e\}$ è un sottogruppo di G (*sottogruppo banale*).
(b) Le restrizioni della somma di $\mathbb{C}$ ad $\mathbb{R}$, a $\mathbb{Q}$ e a $\mathbb{Z}$ coincidono con le somme di numeri reali, numeri razionali e numeri interi rispettivamente. Abbiamo visto nell'Esempio 2.4, 1.) che queste operazioni verificano le proprietà della definizione di gruppo. Dunque

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$$

e questa relazione precisa ed estende quella effettuata nell'Osservazione 2.11.

Osservazione 2.18 Se H è un sottogruppo del gruppo G, e K è un sottogruppo del gruppo H, allora K è un sottogruppo di G. Ciò segue immediatamente dalla Definizione 2.16, dato che la restrizione dell'operazione $*$ di G a K può essere vista come il risultato di una restrizione in due fasi: la prima restringe $*$ ad H, creando $*_H$, la seconda restringe quest'ultima a K, creando $*_K$. Si ha così che $<$ è una relazione transitiva nell'insieme dei sottogruppi di G. Essa è, evidentemente, anche riflessiva ed antisimmetrica, ed è dunque una relazione d'ordine, analoga alla relazione di inclusione tra i sottoinsiemi di un insieme.

Esempio 2.19 Rispetto all'usuale prodotto, $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$.

Esercizio 2.20 Provare che $H = \{-1, 1\}$ è un sottogruppo del gruppo $(\mathbb{Q}^*, \cdot)$.

<u>Svolgimento</u>: H è un sottoinsieme non vuoto di $\mathbb{Q}^*$, ed è evidentemente chiuso rispetto al prodotto $\cdot$ di $\mathbb{Q}^*$, in quanto moltiplicando tra loro due elementi di H si ottiene sempre 1 oppure -1. L'elemento neutro è 1, ed ogni elemento di H è inverso di se stesso. Il prodotto ristretto ad H è associativo, in quanto lo è il prodotto di partenza. Ciò prova che H è un gruppo rispetto al prodotto $\cdot$ di $\mathbb{Q}^*$ ristretto ad H, cioè è un sottogruppo di $\mathbb{Q}^*$.

In particolare, alla luce dell'Esempio 2.19 e dell'Osservazione 2.18, $\{-1,1\}$ è un sottogruppo di $\mathbb{C}^*$. In realtà, come vedremo più avanti, esso appartiene ad una classe infinita di sottogruppi di $\mathbb{C}^*$.

Diamo ora una immediata conseguenza della Definizione 2.16, che precisa il legame tra la struttura di un gruppo e la struttura di gruppo di ogni suo sottogruppo.

Proposizione 2.21 *(Proprietà dei sottogruppi)* Sia $(G,*)$ un gruppo e sia H un suo sottogruppo. Allora

(a) l'elemento neutro di H è l'elemento neutro di G;
(b) il simmetrico in H di ogni elemento di H è il suo simmetrico in G.

<u>Dimostrazione</u>: (a) Sia e_H l'elemento neutro di H. Allora, in base all'Esercizio 2.10, e_H è un elemento idempotente del gruppo H, e dunque $e_H = e_H *_H e_H = e_H * e_H$. Ma, allora, e_H è un elemento idempotente del gruppo G. In base allo stesso esercizio, segue che e_H è l'elemento neutro di G, che denotiamo con e.
(b) Sia x un elemento di H, e sia $\overline{x}^H$ il suo simmetrico in H. Allora $x *_H \overline{x}^H = \overline{x}^H *_H x = e_H$. Possiamo riscrivere queste uguaglianze nella forma $x * \overline{x}^H = \overline{x}^H * x = e$. Ciò prova che $\overline{x}^H$ è il simmetrico di x in G, che denotiamo con $\overline{x}$.

Esempio 2.22 (a) L'elemento neutro del gruppo additivo $(\mathbb{C},+)$ e dei suoi sottogruppi $(\mathbb{R},+)$, $(\mathbb{Q},+)$ e $(\mathbb{Z},+)$ è il numero complesso (reale, razionale, intero) 0. Per ogni numero intero a, il suo opposto in $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ e $(\mathbb{C},+)$ è il numero intero $-a$.
(b) L'elemento neutro del gruppo moltiplicativo $(\mathbb{C}^*,\cdot)$ e dei suoi sottogruppi $(\mathbb{R}^*,\cdot)$, $(\mathbb{Q}^*,\cdot)$ è il numero complesso (reale, razionale) 1. Per ogni numero razionale non nullo a, il suo inverso, in $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$ e $(\mathbb{C}^*,\cdot)$, è il numero razionale $\frac{1}{a}$.

Osservazione 2.23 In base alla Proposizione 2.21, ed alla luce dello svolgimento dell'Esercizio 2.20, per decidere, in base alla Definizione 2.16, se un dato sottoinsieme non vuoto di un gruppo è un sottogruppo, è necessario e sufficiente verificare se:

(1) il sottoinsieme è chiuso rispetto all'operazione del gruppo;
(2) l'elemento neutro del gruppo appartiene al sottoinsieme;
(3) il simmetrico di ogni elemento del sottoinsieme appartiene al sottoinsieme.

Queste tre verifiche, in realtà, possono essere ridotte ad una sola. È quanto stabilito dalla prossima proposizione.

Proposizione 2.24 (*Caratterizzazione dei sottogruppi*) Sia $(G,*)$ un gruppo, e sia H un sottoinsieme non vuoto di G. Allora sono equivalenti le seguenti condizioni:

(i) H è un sottogruppo di G;
(ii) per ogni $x, y \in H$, $x * \overline{y} \in H$.

Dimostrazione: Proviamo prima che (i) $\Rightarrow$ (ii). Sia H un sottogruppo di G, e siano $x, y \in H$. Allora, in base alla Proposizione 2.21 (b), $\overline{y} \in H$. Essendo, per la condizione (a) della Definizione 2.16, H chiuso rispetto all'operazione $*$, segue così che $x * \overline{y} \in H$.
Proviamo ora che (ii) $\Rightarrow$ (i). Supponiamo che H verifichi (ii). Dimostriamo che allora H è un sottogruppo di G in base al procedimento indicato nell'Osservazione 2.23. Effettuiamo prima la verifica (2). Sia e l'elemento neutro di G. Essendo H non vuoto, esiste $x \in H$. Allora, per ipotesi, $e = x * \overline{x} \in H$. Passiamo ora a (3). Sia $x \in H$. Allora, poiché, come abbiamo appena visto, $e \in H$, si ha $\overline{x} = e * \overline{x} \in H$. Effettuiamo, infine, la verifica di (1). Siano $x, y \in H$. Allora, come abbiamo appena verificato, $\overline{y} \in H$, e, pertanto, tenendo conto della Proposizione 2.8 (a), $x * y = x * \overline{\overline{y}} \in H$. □

Nota In un gruppo additivo $(G, +)$ la condizione (ii) della Proposizione 2.24 si scrive nella forma:
(ii) per ogni $x, y \in H$, $x - y \in H$.

In un gruppo moltiplicativo $(G, \cdot)$ la condizione (ii) della Proposizione 2.24 si scrive nella forma:
(ii) per ogni $x, y \in H$, $xy^{-1} \in H$.

Corollario 2.25 Sia $(G, *)$ un gruppo e siano H e K suoi sottogruppi. Allora anche $H \cap K$ è un sottogruppo di G.

Dimostrazione: In base alla Proposizione 2.21 (a), detto e l'elemento neutro di G, si ha che $e \in H, e \in K$, e quindi $e \in H \cap K$. In particolare, $H \cap K$ non è vuoto. Siano ora $x, y \in H \cap K$. Allora, essendo H e K sottogruppi di G, in base alla Proposizione 2.24, si ha che $x * \overline{y} \in H, x * \overline{y} \in K$, e quindi $x * \overline{y} \in H \cap K$. In base alla stessa Proposizione 2.24, ciò basta per concludere che $H \cap K$ è un sottogruppo di G. □

Diamo infine, per concludere, un altro risultato che segue immediatamente dalla Definizione 2.16.

Corollario 2.26 Ogni sottogruppo di un gruppo abeliano è abeliano.

Dimostrazione: Se l'operazione del gruppo è commutativa, tale è anche l'operazione ristretta al sottogruppo. □

Esercizio 2.27*
a) Sia $n \in \mathbb{N}$. Provare che l'insieme H_n dei numeri interi che sono multipli di n è un sottogruppo di $(\mathbb{Z}, +)$.
b) Sia $n \in \mathbb{N}, n \geq 2$. Dimostrare che l'insieme R_n delle radici n-esime di 1 è un sottogruppo di $(\mathbb{C}^*, \cdot)$. (Nota: $R_2 = \{-1, 1\}$, il sottogruppo dell'Esercizio 2.20).
c) Dimostrare che l'insieme $H = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q}\right\}$ è un sottogruppo di $(\mathbb{R}, +)$.
d) Dimostrare che l'insieme $H = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q}, (a, b) \neq (0, 0)\right\}$ è un sottogruppo di $(\mathbb{R}^*, \cdot)$.

Esercizio 2.28* Dire se i seguenti insiemi sono sottogruppi di $(\mathbb{Q},+)$.

a) $F_n = \left\{ \frac{a}{n} \middle| a \in \mathbb{Z} \right\}$, ove n è un numero intero positivo fissato.

b) $S = \left\{ \frac{r}{s} \middle| r, s \in \mathbb{Z}, s \text{ dispari} \right\}$.

c) $D = \left\{ \frac{a}{2^n} \middle| a \in \mathbb{Z}, n \in \mathbb{N} \right\}$.

Esercizio 2.29* Dire se i seguenti insiemi sono sottogruppi di $(\mathbb{Q}^*,\cdot)$.

a) $P = \left\{ \frac{a}{p^n} \middle| a \in \mathbb{Z}, n \in \mathbb{N}, a \neq 0 \right\}$, ove p è un numero primo fissato.

b) $S = \left\{ \frac{r}{s} \middle| r, s \in \mathbb{Z}, r \neq 0, s \text{ dispari} \right\}$.

Nota La proprietà associativa, valida per definizione in ogni gruppo, ci consente di omettere le parentesi intorno agli elementi a cui viene applicata la legge di composizione. Nel gruppo $(G,*)$, dati $x, y, z \in G$, la scrittura $x*y*z$ indicherà dunque l'elemento ottenuto come $x*(y*z)$ oppure $(x*y)*z$. Analogamente, dato $w \in G$, la scrittura $x*y*z*w$ indicherà l'elemento

$$x*(y*(z*w)) = x*((y*z)*w) = (x*(y*z))*w = ((x*y)*z)*w = (x*y)*(z*w).$$