Capitolo 4

Semigruppi, monoidi e gruppi

Iniziamo ora a studiare una alla volta alcune delle principali strutture algebriche, iniziando dalla struttura di monoide e di gruppo. Enunceremo e dimostreremo alcune delle loro principali proprietà e soprattutto impareremo a conoscere alcuni gruppi particolarmente significativi.

§ 4.1 Generalità sulle operazioni

Ricordiamo che una operazione binaria (ne esistono anche di più complicate) in un insieme A è una funzione $f\colon A \times A \to A$. Di solito non indicheremo una operazione con una lettera, come fatto ora, ma con un simbolo (ad esempio $+$, $\cdot$, $\circ$ o più in astratto $*$). Inoltre, se $*$ indica l'operazione, per l'immagine di una coppia (a, b) useremo la scrittura $a * b$ (come siamo abituati a fare con le operazioni tra numeri), invece della notazione tipica delle funzioni, ossia $*((a, b))$. Chiameremo tale immagine **risultato** dell'operazione tra a e b. Questa definizione di operazione racchiude una classe molto vasta di funzioni, alcune delle quali decisamente poco interessanti e altre ben note fino dai tempi della scuola elementare.

Esempio 4.1. La funzione costante $c_{14}\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ è una operazione in $\mathbb{R}$. Il risultato dell'operazione tra due qualsiasi numeri reali è sempre 14.

Esempio 4.2. L'addizione tra numeri naturali è una operazione in $f\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ è una operazione in $\mathbb{N}$. Per ogni coppia di numeri naturali (n, m) l'immagine $f((n, m))$ è il numero naturale $n + m$.

Esempio 4.3. La funzione $\star : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\star(a, b) = a \star b = ab - a - b + 2$ è un'operazione su $\mathbb{Z}$.

Elenchiamo ora alcune proprietà interessanti relative alle operazioni (che possono essere soddisfatte oppure anche **non** soddisfatte) da una certa operazione). Sia $*$ una operazione nell'insieme A:

- Proprietà associativa: per ogni $a, b, c \in A$, $(a * b) * c = a * (b * c)$.
- Proprietà commutativa: per ogni $a, b \in A$, $a * b = b * a$.

- Esistenza dell'elemento neutro: esiste $e \in A$ tale che $e * a = a * e = a$ per ogni $a \in A$.
- Esistenza dell'inverso (o opposto): per ogni $a \in A$, esiste $a^{-1} \in A$ (o $-a \in A$) tale che $a * a^{-1} = a^{-1} * a = e$ (o $a * (-a) = -a * a = e$).

§ 4.2 Semigruppi e monoidi

Definizione 4.4. *Sia A un insieme e $*$ un'operazione su A. $(A, *)$ è* **semigruppo** *se $*$ è associativa.*

Esempio 4.5. Gli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con l'usuale operazione somma sono tutti semigruppi. Analogamente se invece della somma consideriamo il prodotto.

Esempio 4.6. Sia A un insieme, sia A^A l'insieme delle funzioni $f : A \to A$ e sia $\circ$ la composizione di funzioni. Possiamo considerare $\circ$ come un'operazione su A^A:

$$\circ : A^A \times A^A \to A^A, \quad \circ(f, g) = f \circ g : A \to A$$

L'operazione $\circ$ è associativa:

$$\forall f, g, h \in A^A, f \circ (g \circ h) = (f \circ g) \circ h.$$

Si verifica osservando come agiscono $f \circ (g \circ h)$ e $(f \circ g) \circ h$ su un qualsiasi elemento di A:

$$\forall a \in A, (f \circ (g \circ h))(a) = f((g \circ h)(a)) = f(g(h(a)) = (f \circ g)(h(a)) = ((f \circ g) \circ h)(a).$$

Quindi $(A^A, \circ)$ è un semigruppo.

Esempio 4.7. Consideriamo $\mathbb{Z}$ e la funzione $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$: $(a, b) \mapsto a - b$. La funzione $-$ è un'operazione, ma non è associativa: infatti, è possibile trovare almeno una terna $a, b, c, \in \mathbb{Z}$ per cui $a-(b-c) \neq (a-b)-c$. Per esempio $a = 4, b = -2, c = 8$: $(4 - (-2)) - 8 = -2 \neq 10 = 4 - (-2 - 8)$. Quindi l'operazione $-$ non dà su $\mathbb{Z}$ la struttura di semigruppo.

Esempio 4.8. su $\mathbb{R} \times \mathbb{R}$ definiamo $(a, b) * (a', b') = (aa', ab' + b)$. Otteniamo un semigruppo.

Definizione 4.9. *Se $(A, *)$ è un semigruppo, possiamo definire le potenze di un elemento $a \in A$ mediante l'induzione:*

$$\begin{cases} a^1 = a \\ \forall n \geq 1 \quad a^{n+1} := a^n * a. \end{cases}$$

Proposizione 4.10. *Sia $(A, *)$ un semigruppo. Se $a \in A$ e m, n sono interi positivi, allora $a^n * a^m = a^{n+m}$ e $(a^n)^m = a^{nm}$.*

Dimostrazione. Dimostriamo per induzione su m che $a^n a^m = a^{n+m}$. Se $m = 1$, si ha $a^n * a^1 = a^n a = a^{n+1}$ per come abbiamo definito a^n. Supponiamo la proprietà sia vera per un certo m, ossia che valga $a^n * a^m = a^{n+m}$, e dimostriamo che allora vale la proprietà anche per l'intero successivo $m+1$, ossia che si ha $a^n * a^{m+1} = a^{n+m+1}$. Si hanno le uguaglianze:

$$a^n * a^{m+1} = a^n * (a^m * a) = (a^n * a^m) * a = a^{n+m} * a = a^{n+m+1}$$

dove

- la prima e la quarta uguaglianza valgono per la definizione di potenza
- la seconda uguaglianza vale perché l'operazione $*$ è associativa
- la terza uguaglianza vale per l'ipotesi induttiva fatta.

Dimostriamo ora per induzione su m che $(a^n)^m = a^{nm}$. Per $m = 1$, $(a^n)^1 = a^n = a^{n \cdot 1}$. Supponiamo ora che sia vero che $(a^n)^m = a^{nm}$ e otteniamo la catena di uguaglianze

$$(a^n)^{m+1} = (a^n)^m * (a^n)^1 = (a^n)^m * a^n = a^{nm} * a^n = a^{nm+n} = a^{n(m+1)}$$

dove

- la prima e la seconda uguaglianza valgono per la definizione di potenza
- la seconda uguaglianza vale per l'ipotesi induttiva
- la terza uguaglianza si ottiene applicando la prima proprietà delle potenze (che abbiamo già dimostrato).

□

Quando l'operazione che si considera è l'addizione tra numeri, oppure più in generale se usiamo il simbolo $+$ per indicare una operazione, le potenze di un elemento si denotano in modo diverso: l'operazione $\underbrace{a * a * \cdots * a}_{n \text{ volte}}$ con notazione additiva diventa $\underbrace{a + a + \cdots + a}_{n \text{ volte}}$ ed è quindi naturale indicarla con na dove $n \in \mathbb{N}$.

Esempio 4.11. Se sommiamo la matrice $M = \begin{pmatrix} 1 & 4 \\ -3 & 0 \end{pmatrix}$ con se stessa per 5 volte otteniamo la matrice $5M = M + M + M + M + M = \begin{pmatrix} 5 & 20 \\ -15 & 0 \end{pmatrix}$.

Proposizione 4.12. *Sia $(A, *)$ un semigruppo. Se esiste in A l'elemento neutro per $*$, allora esso è unico.*

Dimostrazione. Supponiamo che in A vi siano due elementi e, e' che soddisfano la proprietà che definisce l'elemento neutro. Eseguendo l'operazione $e * e'$ troviamo come risultato e', poichè e composto con ogni altro elemento di A lo lascia invariato; d'altra parte abbiamo anche $e * e' = e$, poichè la stessa proprietà vale per e'. Quindi $e = e * e' = e'$. □

Definizione 4.13. *Sia A un insieme e $*$ un'operazione su A. Si dice che $(A, *)$ è un* **monoide** *se $*$ è associativa ed esiste l'elemento neutro. In altre parole $(A, *)$ è un semigruppo dotato di elemento neutro.*

Esempio 4.14. Gli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ con l'usuale operazione somma sono tutti monoidi, l'elemento neutro è sempre 0. Analogamente se invece della somma consideriamo il prodotto, abbiamo struttura di monoide per tutti gli insiemi sopra citati, con elemento neutro 1.

Esempio 4.15. Consideriamo $\mathbb{Z}$ e l'operazione $a * b := ab - a - b + 2$. Verifichiamo se $\mathbb{Z}, *$ è un semigruppo. Prendo a, b, c in $\mathbb{Z}$.

$$a*(b*c) = a*(bc-b-c+2) = (abc-ab-ac+2a)-a-(bc-b-c+2)+2 = abc-ab-ac-bc+a+b+c.$$

$$(a*b)*c = (ab-a-b+2)*c = (abc-ac-bc+2c)-(ab-a-b+2)-c+2 = abc-ab-ac-bc+a+b+c.$$

Quindi $(\mathbb{Z}, *)$ è un semigruppo. Verifichiamo se esiste un elemento neutro e rispetto all'operazione $*$. Cerchiamo $e \in \mathbb{Z}$ tale che $a * e = e * a = a$ per ogni $a \in \mathbb{Z}$.

$$a * e = ae - a - e + 2 = a \Rightarrow (e-2)a + (e-2) = 0 \Rightarrow e = 2.$$

L'elemento neutro esiste ed è 2. Quindi $(\mathbb{Z}, *)$ è un monoide.

Esempio 4.16. Definiamo su $\mathbb{R} \times \mathbb{R}$ l'operazione $(a, b) * (a', b') = (aa', ab' + b)$. L'operazione $*$ è associativa (si veda esercizio 5.1). $(\mathbb{R} \times \mathbb{R}, *)$ è un monoide perché esiste l'elemento neutro, $e = (1, 0)$.

Il monoide delle parole

Sia A un insieme, che chiamiamo **alfabeto**. Chiamiamo **parola nell'alfabeto** A una qualsiasi sequenza $a_1 a_2 \ldots a_n$ di elementi $a_i \in A$ (ed anche la parola vuota, sequenza di 0 simboli).

Esempio 4.17. Sia $A = \{0, 1, 2, \ldots, 15\}$. Alcune parole nell'alfabeto A sono ad esempio

$$1\ 5\ 15, \quad 4\ 4\ 4\ 3\ 4\ 5, \quad 6.$$

Per ogni $n \geq 0$, definiamo W_n come l'insieme delle parole w nell'alfabeto A formate da esattamente n elementi di A:

$$W_n := \{w = a_1 \dots a_n | a_i \in A\}.$$

Per $n = 0$, W_0 contiene un solo elemento, la **parola vuota** w_0 che non contiene nessun elemento di A. Invece $W_1 = A$.

Definizione 4.18. *L'insieme $W_A = \bigcup_{n\in\mathbb{N}} W_n$ è l'***insieme della parole** *nell'alfabeto A.*

Definiamo un'operazione su W_A: siano $w_1 = a_1a_2 \dots a_n$ e $w_2 = b_1b_2 \dots b_m$ due parole di W_A,

$$w_1 \circ w_2 = a_1a_2 \dots a_nb_1b_2 \dots b_m.$$

$w_1 \circ w_2$ è una parola di W_A e $\circ$ è un'operazione, quindi $(W_A, \circ)$ è una struttura algebrica. Chiamiamo $\circ$ la **concatenazione**.

Proposizione 4.19. *$(W_A, \circ)$ è un monoide.*

Dimostrazione. Dobbiamo verificare che la concatenazione sia un'operazione associativa e che esista l'elemento neutro. Per l'associatività è sufficiente osservare che se $w_1 = a_1a_2 \dots a_n, w_2 = b_1b_2 \dots b_m$ e $w_3 = c_1c_2 \dots c_l$ allora

$$(w_1 \circ w_2) \circ w_3 = (a_1a_2 \dots a_nb_1b_2 \dots b_m) \circ w_3 = a_1a_2 \dots a_nb_1b_2 \dots b_mc_1c_2 \dots c_l,$$

$$w_1 \circ (w_2 \circ w_3) = w_1 \circ (b_1b_2 \dots b_mc_1c_2 \dots c_l) = a_1a_2 \dots a_nb_1b_2 \dots b_mc_1c_2 \dots c_l.$$

Inoltre l'elemento neutro rispetto a $\circ$ esiste, ed è la parola vuota w_0. □

§ 4.3 Gruppi

Definizione 4.20. *Siano G un insieme e $*$ un'operazione in G. Diremo che $(G, *)$ è un* **gruppo** *se:*

i) l'operazione $*$ è associativa;

ii) esiste un elemento $e \in G$, detto **identità** *o* **elemento neutro** *tale che $\forall a \in G$ si ha $a * e = e * a = a$;*

iii) ogni elemento ha l'inverso, ossia $\forall a \in G$ $\exists b \in A$ tale che $a * b = b * a = e$.

Esempio 4.21. $\mathbb{Z}$ con la somma è un gruppo, mentre $\mathbb{N}$ con la somma non lo è (manca l'inverso degli elementi rispetto a $+$). Se consideriamo l'operazione prodotto usuale, nessun insieme tra $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ è un gruppo: infatti l'elemento 0 non possiede inverso rispetto al prodotto. Otteniamo invece un gruppo se consideriamo l'operazione prodotto negli insiemi $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$, dove il simbolo di insieme numerico con stellina ad esponente indica l'insieme stesso privato dello zero. Quindi ad esempio $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Esempio 4.22. Sia A un insieme e sia A^A l'insieme di tutte le funzioni $f : A \to A$. Come già visto nell'Esempio 4.6, A^A con la composizione di funzioni $\circ$ è un semigruppo. Inoltre A^A è anche dotato di elemento neutro rispetto a $\circ$: la **funzione identità** Id_A e costituisce quindi un monomide.

$$\begin{aligned} id_A : A &\to A \\ a &\mapsto a. \end{aligned}$$

Però, se $|A| \geq 2$, A^A non è un gruppo, poichè ad esempio le funzioni costanti non hanno inverso. Se infatti $a, b \in A$ sono due elementi diversi e indichiamo con c_a la funzione costante data da $c_a(x) = a\ \forall x \in A$, allora la composizione $c_a \circ g$ di una qualsiasi funzione $g \in A^A$ con c_a, coincide con c_a ed è quindi diversa da Id_A: si ha ad esempio $c_a(b) = a \neq Id_A(b) = b$.

Definizione 4.23. *Un gruppo $(G, *)$ si dice* **gruppo abeliano** *se l'operazione $*$ è anche commutativa, ossia $\forall a, b \in A$ si ha $a * b = b * a$.*

Da ora in poi indicheremo abitualmente l'operazione di un generico gruppo G mediante il simbolo $\cdot$ e chiameremo "prodotto" tale operazione, ossia adotteremo la **notazione moltiplicativa**. Per coerenza, l'unica identità di G sarà denotata con 1_G e l'unico inverso di un elemento $a \in G$ sarà denotato a^{-1}. Spesso il simbolo $\cdot$ di prodotto si sott'intende. Nel caso dei soli gruppi abeliani potremo indicare l'operazione di gruppo col simbolo $+$ e chiamarla somma, ossia useremo la **notazione additiva**; in tal caso indicheremo con 0_G l'identità del gruppo e con $-a$ l'inverso di un elemento $a \in G$ (che chiameremo opposto di a).

Proposizione 4.24. *Sia $(G, *)$ un gruppo. Allora:*

i) l'identità di G è unica;

ii) per ogni $a \in G$, l'inverso di a è unico.

iii) per ogni $a, b \in G$, l'inverso di ab è unico ed è dato da $b^{-1} * a^{-1}$ **prodotto degli inversi in ordine invertito**.

Dimostrazione. i) Abbiamo già dimostrato l'unicità dell'identità parlando dei semigruppi. *ii)* Supponiamo che per un dato elemento $a \in G$ esistano due elementi b e b' che si comportano come suoi inversi, ossia tali che $a * b = b * a = e$ ed anche $a * b' = b' * a = 1_G$. Eseguendo il prodotto a tre $b * a * b'$ ed utilizzando la proprietà associativa otteniamo:

$$b = b * 1_G = b * (a * b') = (b * a) * b' = 1_G * b' = b'.$$

Dal confronto del primo e dell'ultimo membro otteniamo allora $b = b'$ e quindi i due inversi sono in realtà lo stesso elemento. *ii)* Verifichiamo che quello scritto è proprio l'inverso di $a * b$ applicando la definizione (tralasciamo ora il simbolo di operazione) :

$$(ab)(b^{-1}a^{-1}) = a(b\, b^{-1})a^{-1} = a\ 1_G\ a^{-1} = a\ a^{-1} = 1_G$$

ed anche

$$(b^{-1}a^{-1})(ab) = (a^{-1}a)b = b^{-1}1_G\ b = b^{-1}b = 1_G.$$

□

Proposizione 4.25. *Sia $(G, \cdot)$ un gruppo ed a, b, c tre suoi elementi. Allora:*

i) $ab = 1_G \iff ba = 1_G \iff b = a^{-1}$

ii) $ab = b \iff ba = b \iff a = 1_G$

iii) vale la cancellazione ossia: $ab = ac \iff ba = ca \iff b = c.$

Dimostrazione. *i*) Se $b = a^{-1}$ le altre due uguaglianze valgono per definizione. Supponiamo allora che $ab = 1_G$ e moltiplichiamo i due membri a sinistra per a^{-1} (che esiste poichè siamo in un gruppo). Otteniamo allora: $a^{-1}(ab) = a^{-1}1_G$. Per definizione di identità il secondo membro è a^{-1}, mentre per la proprietà associativa il primo membro diventa $(a^{-1}a)b = 1_Gb = b$. Pertanto $b = a^{-1}$. La dimostrazione dell'altra implicazione è analoga: basterà moltiplicare a destra per a^{-1}. *ii)* Se $a = 1_G$, allora le altre due uguaglianze si ottengono per definizione di identit'a. Supponiamo allora $ab = b$ e moltiplichiamo i due membri a destra per b^{-1} (che esiste poichè siamo in un gruppo). Otteniamo cosı: $abb^{-1} = bb^{-1}$ ossia $a = 1_G$. L'altra implicazione si ottiene in modo analogo moltiplicando a sinistra per b^{-1}. *iii)* Anche la verifica della proprietà di cancellazione si ottiene come le precedenti, moltiplicando opportunamente (ossia a sinistra oppure a destra) per l'inverso di a, l'elemento che vogliamo "cancellare ". □

Esempio 4.26. Gli insiemi $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ con l'operazione $\cdot$ sono gruppi

Esempio 4.27. Sia A un insieme e sia A^A l'insieme di tutte le funzioni $f : A \to A$. Come già visto negli Esempi 4.6 e 4.22, A^A con la composizione di funzioni $\circ$ è un monoide. $(A^A, \circ)$ non è in generale un gruppo: infatti le funzioni biunivoche da A in A sono tutte e sole quelle che possiedono inverso rispetto a $\circ$. Le funzioni non biunivoche invece non hanno inverso. Inoltre, per A^A non possono in generale valere le proprietà dei gruppi quali ad esempio la cancellazione. Per vederlo esplicitamente, possiamo pensare a $A = \mathbb{Z}$, e considerare la funzione $f : \mathbb{Z} \to \mathbb{Z}$, $f(a) = a^2$. Questa funzione non ha inversa rispetto a $\circ$. Per quel che riguarda la cancellazione, sia $h : \mathbb{Z} \to \mathbb{Z}$ la funzione definita come $h(a) = -a$. Allora

$$f \circ h = f \circ id_{\mathbb{Z}}, \quad \text{ma } h \neq id_{\mathbb{Z}}.$$

Esempio 4.28. Sia A un insieme e consideriamo $\widetilde{A^A} = \{f : A \to A | f \text{ è biunivoca}\}$. Osserviamo che possiamo considerare l'operazione di composizione di funzioni $\circ$ come un'operazione su $\widetilde{A^A}$: infatti, componendo funzioni biunivoche, otteniamo ancora una funzione biunivoca. $(\widetilde{A^A}, \circ)$ è un gruppo. Infatti

1. la composizione di funzioni $\circ$ è associativa in generale, in particolare in $\widetilde{A^A}$;
2. l'identità di A appartiene a $\widetilde{A^A}$, ed è l'elemento neutro rispetto a $\circ$;
3. se $f \in \widetilde{A^A}$, allora esiste l'inversa di f rispetto a $\circ$ (vedi Proposizione 2.20).

Definizione 4.29. *Sia $(G, \cdot)$ un gruppo e sia a un suo elemento. Definiamo le potenze di a con esponente intero (positivo, nullo o negativo) n nel modo seguente:*

- *se $n > 0$, a^n è la potenza di a che abbiamo già definito nei semigruppi*
- *se $n = 0$, poniamo $a^0 := 1_G$*
- *se $n < 0$ ossia se $n = -m$ con $m > 0$, poniamo $a^n := (a^{-1})^m$*

Le proprità delle potenze che abbiamo dimostrato nei semigruppi relativamente al caso degli esponenti positivi valgono nel caso dei gruppi anche per gli esponenti minori o uguali a 0 e si estendono a proprietà che riguardano gli inversi.

Corollario 4.30. *Se $(G, \cdot)$ è un gruppo e $a \in G$, allora valgono le proprietà seguenti per ogni $n, m \in \mathbb{Z}$:*

- $a^n \cdot a^m = a^{n+m}$
- $(a^n)^m = a^{nm}$
- $(a^n)^{-1} = a^{-n}$

§ 4.4 Esercizi

4.1 Consideriamo su $\mathbb{R} \times \mathbb{R}$ l'operazione $(a, b) * (a', b') = (aa', ab' + b)$. Verificare che $*$ è associativa.

4.2 Sia A un insieme, $\mathcal{P}(A)$ il suo insieme delle parti e sia $\triangle$ la differenza simmetrica:

$$\triangle : \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A), \quad (A, B) \mapsto (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

$\triangle$ è un'operazione? 'E commutativa? Esiste elemento neutro? Esiste inverso per ogni elemento di $\mathcal{P}(A)$?

4.3 Consideriamo su $\mathbb{R}$ l'operazione quoziente: per ogni $a, b \in \mathbb{R}$, $a : b$ è un numero reale. Verificare se l'operazione quoziente è commutativa, associativa, se esiste elemento neutro in $\mathbb{R}$ rispetto a tale operazione e eventualmente se esiste inverso di ogni elemento in $\mathbb{R}$ rispetto all'operazione quoziente.

4.4 Si consideri su $\mathbb{N} \times \mathbb{N}$ l'operazione $(n,m) * (n',m') = (nn' + mm', nm' + n'm)$. Stabilire se $(\mathbb{N} \times \mathbb{N}, *)$ è un monoide.

4.5 Sia $A = \{a, b, c\}$ e consideriamo il monoide delle parole W_A. Quante sono le parole di W_4 che contengono solo a e b?

4.6 Si pone $G = \mathbb{R}^* \times \mathbb{R}$ e si definisce la seguente legge di composizione interna:

$$(a,b) * (c,d) = (ac, bc + d), \forall (a,b), (c,d) \in G.$$

1. Eseguire: $(1,2) * (3,5)$, $(1,0) * (-1,3)$;
2. verificare che $*$ è associativa;
3. trovare l'elemento neutro di $(G, *)$;
4. trovare l'inverso di $(1,2)$, $(3,5)$, $(-1,4)$;
5. dimostrare che $(G, *)$ è un gruppo non abeliano.
6. Calcolare le potenze n-esime di $(1,2)$ per ogni $n \in \mathbb{Z}$.

4.7 Considerati gli insiemi $G = \{a, b, c, d\}$ e $G' = \{1, 2, 3, 4\}$ con le operazioni definite dalle tabelle seguenti

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	d	d	a	b
d	d	c	b	a

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

1. Trovare gli elementi neutri per cascuna delle strutture $(G, *)$ e $(G', \circ)$;
2. trovare l'inverso di cascun elmento di $(G, *)$ e $(G', \circ)$;
3. tralasciando l'associatività, dimostrare che $(G, *)$ e $(G', \circ)$ sono gruppi;
4. stabilire se $(G, *)$ e $(G', \circ)$ sono gruppi abeliani.

4.8 Si consideri la struttura algebrica $(\mathbb{Z}, *)$, dove l'operazione interna $*$ è definita come segue:

$$\forall x, y \in \mathbb{Z}, \quad x * y = x + y - 3.$$

1. Stabilire se $*$ è una legge associativa e/o commutativa;
2. determinare l'eventuale elemento neutro della struttura algebrica $(\mathbb{Z}, *)$
3. se la struttura algebrica $(\mathbb{Z}, *)$ ammette elemento neutro, determinare gli (eventuali) elementi di $\mathbb{Z}$ che hanno inverso rispetto all'operazione $*$;
4. concludere se la struttura algebrica $(Z, *)$ è un monoide o un gruppo (abeliano?).

4.9 Si consideri la struttura algebrica $(\mathbb{Z}, \circ)$, dove l'operazione $\circ$ è definita come segue:

$$\forall x, y \in \mathbb{Z}, \quad x \circ y = xy + x + y.$$

1. Stabilire se $\circ$ è un'operazione associativa e/o commutativa;
2. determinare l'eventuale elemento neutro della struttura algebrica $(\mathbb{Z}, \circ)$;
3. se la struttura algebrica $(\mathbb{Z}, \circ)$ ammette elemento neutro, determinare gli (eventuali) elementi di $\mathbb{Z}$ che hanno inverso rispetto alla legge $\circ$;
4. concludere se la struttura algebrica $(Z, \circ)$ è un monoide o un gruppo (abeliano?).