Definizione 1. Sia A un insieme non vuoto. Un'applicazione

$$* : A \times A \to A$$

si dice *legge di composizione interna* o *operazione* su A. La coppia ordinata $(A, *)$ si dice *struttura algebrica*, della quale A è il *sostegno*.

Osservazione 1. *Siano $(A, *)$ una struttura algebrica, $(x, y) \in A \times A$. Allora, invece di scrivere $*\big((x, y)\big)$, si scrive $x * y$.*

Definizione 2. Si dice che la legge di composizione $*$ sull'insieme A verifica la proprietà *associativa* oppure che la struttura algebrica $(A, *)$ è associativa se

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

Definizione 3. Sia $(A, *)$ una struttura algebrica. Si dice che $(A, *)$ ammette *elemento neutro* se

$$\exists\ e \in A \ \text{ tale che } \ \forall x \in A \quad x * e = e * x = x.$$

Naturalmente in tal caso e si dice elemento neutro della struttura algebrica $(A, *)$.

Proposizione 1. *Se la struttura algebrica $(A, *)$ ammette elemento neutro, esso è unico.*

Dimostrazione. Siano e_1 ed e_2 elementi neutri della struttura. Allora

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

Definizione 4. Una struttura algebrica associativa e che ammette elemento neutro si dice *monoide*.

Esempio 1. Si può osservare facilmente che $(\mathbb{N}, +)$ e $(\mathbb{Z}, \cdot)$ sono monoidi.

Esempio 2. Sia A un insieme non vuoto. Allora la struttura algebrica $(A^A, \circ)$ avente per sostegno l'insieme A^A delle applicazioni di A in sé, e come operazione la composizione tra applicazioni $\circ$, risulta essere un monoide. Infatti $\circ$ verifica la proprietà associativa e l'elemento neutro è l'applicazione identica id_A.

Esempio 3. Siano A un insieme, $n \in \mathbb{N}$. Se $a_1, a_2, \ldots, a_n \in A$, la successione ordinata

$$w_n = a_1 a_2 \ldots a_n$$

si dice parola di lunghezza n su A. Esiste un'unica parola priva di elementi, la parola vuota, che si indica con w_0 (su qualunque insieme). Per ogni $n \in \mathbb{N}$, si indica con W_n l'insieme di tutte le parole di lunghezza n su A e si pone:

$$\mathcal{W} = \bigcup_{n \in \mathbb{N}} W_n.$$

Si definisce una legge di composizione interna $\cdot$ su $\mathcal{W}$, detta *giustapposizione*, nel modo che segue: se $w, w' \in \mathcal{W}$, allora esistono $n, m \in \mathbb{N}$ tali che $w \in W_n$ e $w' \in W_m$, e quindi esistono $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \in A$ tali che $w = a_1 a_2 \ldots a_n$, $w' = b_1 b_2 \ldots b_m$. Si pone allora

$$w \cdot w' = a_1 a_2 \ldots a_n b_1 b_2 \ldots b_m \in W_{n+m} \subset \mathcal{W}.$$

Si vede facilmente che $\cdot$ verifica la proprietà associativa e che la parola vuota w_0 è l'elemento neutro di $(\mathcal{W}, \cdot)$. Quindi $(\mathcal{W}, \cdot)$ è un monoide, che si dice *monoide delle parole* o *monoide libero* su A.

Definizione 5. Sia $(A, *)$ una struttura algebrica dotata di elemento neutro e, e sia $x \in A$. Si dice che x è *simmetrizzabile* se esiste $x' \in A$ tale che

$$x * x' = x' * x = e;$$

x' si dice *simmetrico di x*.

Proposizione 2. *Sia $(A, *)$ un monoide, con elemento neutro e. Se un elemento $x \in A$ ammette simmetrico, esso è unico.*

Dimostrazione. Siano x' e x'' simmetrici di x: ciò vuo dire, per definizione, che

$$x * x' = x' * x = e \text{ e inoltre } x * x'' = x'' * x = e.$$

Allora si ha:

$$x'' = e * x'' = (x' * x) * x'' = x' * (x * x'') = x' * e = x'$$

e quindi $x'' = x'$.

Definizione 6. Si dice che una struttura algebrica $(A, *)$ è un *gruppo* se è associativa, se ammette elemento neutro e se ogni elemento è simmetrizzabile. In altri termini $(A, *)$ è un gruppo se sono verificate le seguenti proprietà

- $\forall x, y, z \in A, \quad (x * y) * z = x * (y * z).$
- $\exists\ e \in A$ tale che $\forall x \in A \quad x * e = e * x = x.$
- $\forall x \in a \ \ \exists\ x' \in A$ tale che $x * x' = x' * x = e.$

Esempio 4. Esempi di gruppi sono: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$. Si osserva che $(\mathbb{Q}, \cdot)$ è un monoide ma non un gruppo, in quanto esiste $0 \in \mathbb{Q}$ che non ammette simmetrico rispetto a $\cdot$. Analoga argomentazione vale per affermare che $(\mathbb{R}, \cdot)$ non è un gruppo.

Definizione 7. Sia $(G, \cdot)$ un gruppo. Se G è un insieme finito, allora la sua cardinalità si chiama *ordine* di $(G, \cdot)$ e si indica con $|G|$. Se G non è finito si dice che G ha ordine infinito e si pone $|G| = +\infty$.

Esempio 5. Sia A un insieme non vuoto. Allora la struttura algebrica $(\mathcal{S}(A), \circ)$ avente per sostegno l'insieme $\mathcal{S}(A)$ delle applicazioni bigettive di A in sé, e come operazione la composizione tra applicazioni, risulta essere un gruppo. Infatti verifica la proprietà associativa, ha id_A come elemento neutro ed inoltre ogni elemento $f \in \mathcal{S}(A)$ ha elemento simmetrico, che è proprio l'applicazione inversa f^{-1} (che esiste in quanto f è bigettiva). In particolare, se $A = \{1, \dots, n\}$, $n \in \mathbb{N}^*$, allora $\mathcal{S}(A)$ è il gruppo delle permutazioni su n oggetti S_n: il gruppo $(S_n, \circ)$ si chiama *gruppo simmetrico.*

Osservazione 2. Il gruppo simmetrico su n oggetti, $n \in \mathbb{N}^*$, è finito e ha ordine $n!$.

Osservazione 3. La legge di composizione interma di un gruppo di sostegno G viene prevalentemente denotata moltiplicativamente con $\cdot$ o additivamente con $+$ (si possono comunque incontrare altri simboli per indicare la legge di composizione interna). Nel caso della notazione moltiplicativa si usa generalmente la notazione 1_G, o semplicemente 1 per l'elemento neutro e per ogni $x \in G$ si indica con x^{-1} l'elemento simmetrico di x, che dice *inverso di x*. Nel caso della notazione additiva, si usa generalmente la notazione 0_G, o semplicemente 0, per l'elemento neutro e per ogni $x \in G$ si indica con $-x$ l'elemento simmetrico di x, che si dice *opposto di x*.

Definizione 8. Si dice che la legge di composizione $*$ sull'insieme A verifica la proprietà *commutativa* oppure che la struttura algebrica $(A, *)$ è commutativa se

$$\forall x, y \in A, \quad x * y = y * x.$$

Un gruppo commutativo si dice *abeliano.*

Osservazione 4. Il monoide $(A^A, \circ)$ delle applicazioni di un insieme non vuoto A in sé (cf. Esempio 2) e il monoide $(\mathcal{W}, \cdot)$ delle parole su un insieme A (cf. Esempio 3) non sono commutativi. Sono invece commutativi i monoidi $(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$. I gruppi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ sono tutti abeliani, mentre non è abeliano il gruppo $(\mathcal{S}(A), \circ)$ delle applicazioni bigettive di un insieme A in sé, quando $|A| \geq 3$ (cf. Esempio 5).

Definizione 9. Sia $(G, \cdot)$ un gruppo. Fissato $n \in \mathbb{Z}$, definisce la *potenza n-ma* di g nel modo che segue:

- ricorsivamente per $n \in \mathbb{N}$:

$$\begin{cases} g^0 = 1_G \\ g^n = g^{n-1}g, \quad n > 0 \end{cases}$$

- per $n < 0$, si pone $g^n = (g^{-n})^{-1}$.

Osservazione 5. Se $(G, +)$ è un gruppo denotato additivamente, allora fissato $n \in \mathbb{Z}$, si parla non di potenza n-ma di g, ma di *multiplo secondo* n di g, e la definizione si scrive:

- ricorsivamente per $n \in \mathbb{N}$:

$$\begin{cases} 0\ g = 0 \\ n\ g = (n-1)\ g + g, \quad n > 0 \end{cases}$$

- per $n < 0$, $n\ g = -(-n\ g)$.

La dimostrazione del risultato che segue viene omessa.

Proposizione 3. *Sia* $(G, \cdot)$ *un gruppo. Allora si ha*

(1) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad g^m \cdot g^n = g^{m+n}$
(2) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad (g^m)^n = g^{mn}$
(3) *se* $(G, \cdot)$ *è abeliano, allora* $\forall g, h \in G, \quad \forall n \in \mathbb{Z} \quad (g \cdot h)^n = g^n \cdot h^n$.

Osservazione 6. Se il gruppo $(G, +)$ è denotato additivamente, allora le proprietà della Proposizione 3 si riscrivono nel modo seguente:

(1) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad (m+n)\ g = m\ g + n\ g$
(2) $\forall g \in G, \quad \forall m, n \in \mathbb{Z} \quad m\ (n\ g) = (mn)\ g$
(3) se $(G, +)$ è abeliano, allora $\forall g, h \in G, \quad \forall n \in \mathbb{Z} \quad n\ (g + h) = n\ g + n\ h$.

Definizione 10. Sia $(A, *)$ una struttura algebrica, $\mathcal{R}$ una relazione di equivalenza su A. Si dice che $\mathcal{R}$ è *compatibile con* $*$ se

$$\forall a, b, c, d \in A, \quad ((a, b) \in \mathcal{R} \ \wedge \ (c, d) \in \mathcal{R}) \ \Rightarrow \ (a * c, b * d) \in \mathcal{R}.$$

Proposizione 4. *Sia* $(A, *)$ *una struttura algebrica,* $\mathcal{R}$ *una relazione di equivalenza su* A *compatibile con una legge di composizione interna* $*$ *. Allora la legge di composizione interna* $*_\mathcal{R}$ *definita sull'insieme quoziente* $A/\mathcal{R}$ *come segue:*

$$\forall\ [a]_\mathcal{R}, [b]_\mathcal{R} \in A/\mathcal{R}, \quad [a]_\mathcal{R}\ *_\mathcal{R}\ [b]_\mathcal{R} = [a * b]_\mathcal{R}$$

è ben posta.

Dimostrazione. Bisogna provare che se $[a]_\mathcal{R}, [b]_\mathcal{R} \in A/\mathcal{R}$, allora per ogni $a', b' \in A$ tali che $[a']_\mathcal{R} = [a]_\mathcal{R}$ e $[b']_\mathcal{R} = [b]_\mathcal{R}$ deve essere $[a' * b']_\mathcal{R} = [a * b]_\mathcal{R}$. Poichè $[a']_\mathcal{R} = [a]_\mathcal{R}$ e $[b']_\mathcal{R} = [b]_\mathcal{R}$, per le proprietà delle classi di equivalenza, sarà $(a, a') \in \mathcal{R}$ e $(b, b') \in \mathcal{R}$. Quindi, per la compatibilità di $\mathcal{R}$ con $*$, risulta che $(a * b, a' * b') \in \mathcal{R}$ e pertanto $[a' * b']_\mathcal{R} = [a * b]_\mathcal{R}$.

Osservazione 7. Si dimostra che $*_\mathcal{R}$ verifica tutte le proprietà di $*$. Quindi, in particolare, se $(A, *)$ è un monoide o, rispettivamente, un gruppo, allora anche $(A/\mathcal{R}, *_\mathcal{R})$ è monoide o, rispettivamente, un gruppo. Inoltre, se $(A, *)$ è una struttura commutativa, allora anche $(A/\mathcal{R}, *_\mathcal{R})$ è una struttura commutativa.

Esempio 6. Si è dimostrato che congruenza $(\texttt{mod}\ n)$ è compatibile sia con la somma che con il prodotto di $\mathbb{Z}$, ovvero che $\forall a, b.c.d \in \mathbb{Z}$

$$(a \equiv b\ (\texttt{mod}\ n) \quad \wedge \quad c \equiv d\ (\texttt{mod}\ n)) \Rightarrow a + c \ \equiv b + d\ (\texttt{mod}\ n)$$
$$(a \equiv b\ (\texttt{mod}\ n) \quad \wedge \quad c \equiv d\ (\texttt{mod}\ n)) \Rightarrow ac \ \equiv bd\ (\texttt{mod}\ n)$$

e quindi si possono considerare le leggi di composizione interne indotte sull'insieme quoziente $\mathbb{Z}_n$.

$$\forall\ [a]_n,\ [b]_n \in \mathbb{Z}_n \quad [a]_n + [b]_n = [a+b]_n, \qquad [a]_n \cdot [b]_n = [a \cdot b]_n.$$

Risultano, quindi, le due strutture algebriche; $(\mathbb{Z}_n, +)$, che è un gruppo abeliano e $(\mathbb{Z}_n, \cdot)$, che è un monoide commutativo.

Definizione 11. Siano $(A, *)$ una struttura algerica, $H \subset A$. Si dice che H è *chiuso* rispetto a $*$ se $\forall x, y \in H, \quad x * y \in H$.

Definizione 12. Sia $(G, \cdot)$ un gruppo, $H \subseteq G$. Si dice che H è un *sottogruppo* di G se è esso stesso un gruppo.

I seguenti fondamentali teoremi caratterizzano i sottogruppi.

Teorema 1. *Sia $(G, \cdot)$ un gruppo, $H \subseteq G$. Allora H è un sottogruppo di G se e soltanto se sono verificate le seguenti 3 condizioni*

(SG$_1$) $H \neq \emptyset$
(SG$_2$) $\forall x, y \in H, \quad x \cdot y \in H$ *(cioè H è chiuso rispetto a $\cdot$)*
(SG$_3$) $\forall x \in H, \quad x^{-1} \in H$.

Teorema 2. *Sia $(G, \cdot)$ un gruppo, $H \subseteq G$. Allora H è un sottogruppo di G se e soltanto se sono verificate le seguenti 2 condizioni*

(SG'$_1$) $1_G \in H$
(SG'$_2$) $\forall x, y \in H, \quad x \cdot y^{-1} \in H$.

Dimostrazione. Basta provare che le condizioni (SG$_1$), (SG$_2$), (SG$_3$) sono, nel loro insieme, equivalenti alle condizioni (SG'$_1$), (SG'$_2$).
Si suppone che siano verificate (SG$_1$), (SG$_2$), (SG$_3$). Per (SG$_1$), $H \neq \emptyset$, e quindi esiste $x \in H$; allora, per (SG$_3$), $x^{-1} \in H$ e quindi, per (SG$_2$), risulta $1_G = x \cdot x^{-1} \in H$, ovvero (SG'$_1$) è verificata. Siano, ora, $x, y \in H$. Per (SG$_3$) anche $y^{-1} \in H$, pertanto, per (SG$_2$), $x \cdot y^{-1} \in H$, ovvero (SG'$_2$) è verificata.
Si suppone, ora che (SG'$_1$), (SG'$_2$) siano verificate. Poiché $1_G \in H$, certamente $H \neq \emptyset$. Sia $x \in H$: allora, per (SG'$_2$), risulta $x^{-1} = 1 \cdot x^{-1} \in H$, ovvero (SG$_3$) è verificata. Siano, ora, $x, y \in H$: si ha $y^{-1} \in H$ e quindi, per (SG'$_2$), $x \cdot y = x \cdot (y^{-1})^{-1} \in H$, cioè vale (SG$_2$).

Osservazione 8. Nel caso di un gruppo $(G, +)$ denotato additivamente, le condizioni (SG$_2$), (SG$_3$) del Teorema 1 si riscrivono come segue:

(SG$_2$) $\forall x, y \in H, \quad x + y \in H$ (cioè H è chiuso rispetto a $+$)
(SG$_3$) $\forall x \in H, \quad -x \in H$.

Inoltre (SG'$_1$), (SG'$_2$) del Teorema 2 si riscrivono come segue:

(SG'$_2$) $0_G \in H$
(SG'$_3$) $\forall x, y \in H, \quad x - y \in H$.

Esempio 7. L'insieme

$$H = 2\mathbb{Z} = \{n \in \mathbb{Z}\ :\ \exists\ h \in \mathbb{Z} \text{ tale che } n = 2h\}$$

(per ogni $h \in \mathbb{Z}$, $2h = h2$ vuol dire il multiplo di 2 secondo h) è un sottogruppo di $\mathbb{Z}$. Infatti, usando il Teorema 1, risulta:

(SG$_1$) $H \neq \emptyset$ poichè, per esempio, $0 = 2 \cdot 0 \in \mathbb{Z}$
(SG$_2$) Siano $n, m \in H$: allora $\exists\ h, k \in \mathbb{Z}$ tali che $n = 2h,\ m = 2k$ e quindi $n + m = 2h+2k = 2(h+k)$, pertanto $\exists\ t = h+k \in \mathbb{Z}$ tale che $n+m = 2t$, cioè $n+m \in H$
(SG$_3$) Sia $n \in H$: allora $\exists\ h \in \mathbb{Z}$ tale che $n = 2h$ allora $-n = 2(-h)$ e quindi $\exists\ s = -h \in \mathbb{Z}$ tale che $-n = 2s$, cioè $-n \in H$.

Esempio 8. Si prova in maniera analoga all'Esempio 7 che per ogni $a \in \mathbb{Z}$ l'insieme $K = a\mathbb{Z} = \{n \in \mathbb{Z}\ :\ \exists\ h \in \mathbb{Z} \text{ tale che } n = ah\}$ è un sottogruppo di $\mathbb{Z}$.

Il seguente risultato può essere verificato per esercizio.

Proposizione 5. *Sia* $(G, \cdot)$ *un gruppo. Allora l'intersezione di due sottogruppi di* G *è un sottogruppo di* G.

Osservazione 9. In generale l'unione di due sottogruppi di G non è un sottogruppo di G. Ciò si può provare con il seguente controesempio: $H = 3\mathbb{Z}$ e $K = 5\mathbb{Z}$ sono sottogruppi di $\mathbb{Z}$ (cf. Esempio 8), mentre $H \cup K$ non è un sottogruppo di $\mathbb{Z}$. Infatti: $6 \in H \subset H \cup K$, $5 \in K \subset H \cup K$, ma $6 + 5 = 11 \notin H \cup K$.

Al fine di fornire un esempio di un sottogruppo del gruppo simmetrico $(S_n, \circ)$, $n \in \mathbb{N}^*$, detto *gruppo alterno*, si definisce l'applicazione

$$\Delta : S_n \to \{\pm 1\} \ \text{ tale che } \Delta(f) = \begin{cases} 1 & \text{se } f \text{ è di classe pari} \\ -1 & \text{se } f \text{ è di classe dispari.} \end{cases}$$

Proposizione 6. *Per ogni* $f, g \in S_n$ *risulta:*

$$\Delta(f \circ g) = \Delta(f) \cdot \Delta(g). \tag{1}$$

Proof. Siano $f, g \in S_n$. Allora esistono degli scambi $\sigma_1, \ldots, \sigma_h, \tau_1, \ldots, \tau_s$ tali che

$$f = \sigma_1 \circ \cdots \circ \sigma_h, \qquad g = \tau_1 \circ \cdots \circ \tau_s$$

Quindi si può scrivere:

$$f \circ g = \sigma_1 \circ \cdots \circ \sigma_h \circ \tau_1 \circ \cdots \circ \tau_s.$$

Se f e g sono entrambe di classe pari o di classe dispari, allora $f \circ g$ ammette una scomposizione in un numero pari di scambi, perchè $h+s$ è pari, per cui $f \circ g$ è di classe pari e quindi $\Delta(f \circ g) = 1$; d'altra parte se f e g sono entrambe di classe pari (rispettivamente di classe dispari) $\Delta(f) \cdot \Delta(g) = 1 \cdot 1 = 1$ (rispettivamente $\Delta(f) \cdot \Delta(g) = (-1) \cdot (-1) = 1$), pertanto (1) è verificata quando f e g hanno classe della stessa parità. Se invece f e g hanno classe di parità diverse, ad esempio f è di classe pari e g è di classe dispari, allora $f \circ g$ ammette una scomposizione in un numero dispari di scambi, perchè $h + s$ è dispari, per cui $f \circ g$ è di classe dispari. Quindi $\Delta(f \circ g) = -1$; d'altra parte $\Delta(f) = 1$, $\Delta(g) = -1$ per cui $\Delta(f) \cdot \Delta(g) = 1 \cdot (-1) = -1$. Analogo ragionamento vale se f è di classe dispari e g è di classe pari e in conclusione (1) è verificata quando f e g hanno classe di diversa parità. □

Proposizione 7. *Il sottoinsieme* $\mathcal{A}_n$ *formato dalle permutazioni di classe pari costituisce un sottogruppo di* S_n*, che si chiama gruppo alterno.*

Dimostrazione. Si osserva che

$$\mathcal{A}_n = \{f \in S_n \ : \ \Delta(f) = 1\}.$$

Si procede usando il Teorema 1.

SG$_1$) $\mathcal{A}_n \neq \emptyset$ poichè $id \in \mathcal{A}_n$, in quanto si può scrivere, ad esempio $id = (1\ 2) \circ (1\ 2)$.

(SG$_2$) Siano $f, g \in \mathcal{A}_n$: allora $\Delta(f) = 1$ e $\Delta(g) = 1$ quindi $\Delta(f \circ g) = \Delta(f) \cdot \Delta(g) = 1$ e in conclusione $f \circ g \in \mathcal{A}_n$

(SG$_3$) Sia $f \in \mathcal{A}_n$: allora $1 = \Delta(id) = \Delta(f \circ f^{-1}) = \Delta(f) \circ \Delta(f^{-1}) = \Delta(f^{-1})$ cioè $\Delta(f^{-1}) = 1$ e quindi $f^{-1} \in \mathcal{A}_n$..

Il seguente fondamentale Teorema di Lagrange, non verrà dimostrato.

Teorema 3. *Sia* $(G, \cdot)$ *un gruppo finito di ordine* n*,* H *un suo sottogruppo di ordine* h*. Allora* $h \mid n$.

Proposizione 8. *Sia* $(G, \cdot)$ *un gruppo,* $g \in G$*. Allora il sottoinsieme*

$$< g >= \{a \in G \ : \ \exists\ h \in \mathbb{Z} \text{ tale che } a = g^h\} = \{g^h \mid h \in \mathbb{Z}\}$$

è un sottogruppo di G.

Dimostrazione. Si usano il Teorema 1 e la Proposizione 3.

(SG$_1$) $< g > \neq \emptyset$ poichè, per esempio, $g = g^1 \in < g >$.
(SG$_2$) Siano $a, b \in < g >$: allora $\exists\ h, k \in \mathbb{Z}$ tali che $a = g^h,\ b = g^k$ e quindi $a \cdot b = g^h \cdot g^k = g^{h+k}$, pertanto $\exists\ t = h + k \in \mathbb{Z}$ tale che $a \cdot b = g^t$, cioè $a \cdot b \in < g >$.
(SG$_3$) Sia $a \in < g >$: allora $\exists\, h \in \mathbb{Z}$ tale che $a = g^h$ allora $a^{-1} = (g^h)^{-1} = g^{-h}$ e quindi $\exists\ s = -h \in \mathbb{Z}$ tale che $a^{-1} = g^s$, cioè $a^{-1} \in < g >$.

La Proposizione 8 giustifica la Definizione che segue.

Definizione 13. Sia $(G, \cdot)$ un gruppo, $g \in G$. Il sottogruppo $< g >$ si dice *sottogruppo ciclico generato da* g.

Osservazione 10. Se il gruppo $(G, +)$ è denotato additivamente e $g \in G$, allora il sottogruppo ciclico generato da g si scrive

$$< g > = \{hg \mid h \in \mathbb{Z}\}.$$

Osservazione 11. Si osservi che un gruppo infinito può anche ammettere sottogruppi finiti: per esempio il sottogruppo ciclico di $(\mathbb{Q}^*, \cdot)$ generato da -1 è finito, in quanto $< -1 > = \{1, -1\}$.

Proposizione 9. *Sia $(G, \cdot)$ un gruppo, $g \in G$. Allora si ha una delle seguenti possibilità:*
(1) $(\forall\ h, k \in \mathbb{Z})\ (g^h \neq g^k)\ \Leftrightarrow < g >$ *è infinito*
(2) $(\exists\ h, k \in \mathbb{Z})\ (g^h = g^k)\ \Leftrightarrow < g >$ *è finito.*

Definizione 14. Sia $(G, \cdot)$ un gruppo, $g \in G$. Si dice che g *ha ordine infinito*, e si scrive $|g| = +\infty$, se $| < g > | = +\infty$; si dice che g *ha ordine o periodo* $k \in \mathbb{N}^*$, e si scrive $|g| = k$, se $| < g > | = k$.

Si noti che in ogni caso $|g| = | < g > |$.

Proposizione 10. *L'ordine di un ciclo σ di lunghezza r nel gruppo simmetrico $(S_n, \circ)$ è r. Inoltre, se $f \in S_n$, ammette la seguente scomposizione in cicli disgiunti: $f = \sigma_1 \circ \cdots \circ \sigma_h$, allora si ha:*

$$|f| = m.c.m.(|\sigma_1|, \ldots, |\sigma_h|).$$

Definizione 15. Si dice che un gruppo $(G, \cdot)$ è *ciclico* se esiste $g \in G$ tale che $< g > = G$. In tal caso g si dice *generatore* di G.

Esempio 9. Sono gruppi ciclici:
(1) $(\mathbb{Z}, +)$, in quanto 1 ne è un generatore
(2) $(\mathbb{Z}_n, +)$, in quanto $[1]_n$ ne è generatore.

Teorema 4. *Ogni sottogruppo di un gruppo ciclico è ciclico.*

Quindi, per esempio, sono ciclici tutti i sottogruppi di $(\mathbb{Z}, +)$ e tutti i sottogruppi di $(\mathbb{Z}_n, +)$

Teorema 5. *(Inverso del Teorema di Lagrange per i gruppi ciclici) Sia $(G, \cdot)$ un gruppo ciclico di ordine n. Allora per ogni h divisore di n esiste un unico sottogruppo di $(G, \cdot)$ avente ordine h.*

Proposizione 11. *Siano $n \in \mathbb{N}^*$, $(G, \cdot)$ un gruppo ciclico finito di ordine n, g un generatore di $(G, \cdot)$. Allora, per ogni elemento $a \in G$ esiste $h \in \mathbb{Z}$ tale che $a = g^h$. Risulta allora:*

$$|a| = |g^h| = \frac{n}{M.C.D.(h, n)} \tag{4}$$

Osservazione 12. Segue da (4) che per ogni numero intero h primo con n, g^h è un generatore di G. In particolare, i generatori del gruppo $(\mathbb{Z}_n, +)$ sono tutti gli elementi $[h]_n \in \mathbb{Z}_n$ tali che h sia primo con n e quindi i generatori di $(\mathbb{Z}_n, +)$ sono esattamente $\varphi(n)$ (φ funzione di Eulero).

Osservazione 13. Sia $(G, \cdot)$ un gruppo finito di ordine n. Un elemento $a \in G$ è generatore di G se e soltanto se $|a| = n$.

Esercizio 1. Verificare che:

1. un gruppo finito di ordine p primo è ciclico.
2. un gruppo ciclico è abeliano.

Osservazione 14. Per $n > 2$, $(S_n, \circ)$ *non* è abeliano e quindi non può essere ciclico. D'altra parte $(S_2, \circ)$ ha ordine $2! = 2$, che è un numero primo, per cui è ciclico e quindi abeliano (cf. Esercizio 1).

Proposizione 12. *Siano $(G, \cdot)$ un gruppo, $a \in G$, con $|a| = m$. Allora si ha:*

$$m = min\{h \in \mathbb{N}^* : a^h = 1_G\}$$

Proposizione 13. *Sia $n \in \mathbb{N}$, $n > 1$. Allora un elemento $[a]_n \in \mathbb{Z}_n^*$ è invertibile nel monoide $(\mathbb{Z}_n, \cdot)$ se e soltanto se $M.C.D.(a, n) = 1$.*

Dimostrazione. Un elemento $[a]_n \in \mathbb{Z}_n^*$ è invertibile se e solo se esiste $[x]_n \in \mathbb{Z}_n$ tale che

$$[a]_n \cdot [x]_n = [1]_n, \tag{2}$$

ovvero

$$[a \cdot x]_n = [1]_n.$$

Pertanto, per cercare un eventuale x che verifichi (2), bisogna risolvere la congruenza lineare

$$(3) \quad a\, x \equiv 1 \ (\texttt{mod}\ n),$$

che ha soluzioni se e solo se $M.C.D.(a, n) \mid 1$, cioè se e solo se $M.C.D.(a, n) = 1$. Inoltre, nel caso in cui (3) abbia soluzioni, ce nè soltanto una ($\texttt{mod}\ n$): questo a conferma dell'unicità dell'inverso.

Corollario 1. *Se $p \in \mathbb{Z}$ è un numero primo, allora $\mathbb{Z}_p^*$ è chiuso rispetto a $\cdot$.*

Dimostrazione. Per la Proposizione 13, ogni elemento di $\mathbb{Z}_p^*$ ha inverso rispetto a $\cdot$. Siano $[a]_p$, $[b]_p \in \mathbb{Z}_p^*$. Bisogna provare che $[a]_p \cdot [b]_p \in \mathbb{Z}_p^*$. Se fosse

$$[a]_p \cdot [b]_p = 0,$$

moltiplicando a sinistra per l'inverso $[a]_p^{-1}$ di $[a]_p$, si avrebbe

$$[a]_p^{-1} \cdot ([a]_p \cdot [b]_p) = [a]_p^{-1} \cdot 0 = 0. \tag{3}$$

D'altra parte,

$$[a]_p^{-1} \cdot ([a]_p \cdot [b]_p) = ([a]_p^{-1} \cdot [a]_p) \cdot [b]_p = [1]_p \cdot [b]_p = [b]_p \tag{4}$$

Confrontando (3) e (4), si ha $[b]_p = [0]_p$, che contraddice l'ipotesi $[b]_p \in \mathbb{Z}_p^*$. Quindi $[a]_p \cdot [b]_p \neq [0]_p$.

A questo punto è immediata la verifica del seguente risultato:

Corollario 2. *Se $p \in \mathbb{Z}$ è un numero primo, allora la struttura algebrica $(\mathbb{Z}_p^*, \cdot)$ è un gruppo abeliano.*

Siano $(A, *)$, $(B, \cdot)$ due strutture algebriche. Si può allora considerare sul prodotto cartesiano $A \times B$ la legge di composizione interna $\odot$ definita come segue:

$$\forall (a, b),\ (a', b') \in A \times B, \quad (a, b) \odot (a', b') = (a * a', b \cdot b').$$

Si può verificare facilmente che

- se le due strutture $(A, *)$ e $(B, \cdot)$ sono entrambe associative, allora $(A \times B, \odot)$ è associativa

- se la struttura $(A, *)$ ammette elemento neutro e e la struttura $(B, \cdot)$ ammette elemento neutro ε allora $(A \times B, \odot)$ ammette elemento neutro (e, ε)
- se a è un elemento simmetrizzabile di A avente a' come simmetrico e b è un elemento simmetrizzabile di B avente b' come simmetrico, allora la coppia (a, b) ha simmetrico (a', b'), in $(A \times B, \odot)$
- se le due strutture $(A, *)$ e $(B, \cdot)$ sono commutative, allora $(A \times B, \odot)$ è commutativa
- in conclusione, se $(A, *)$ e $(B, \cdot)$ sono monoidi (commutativi), allora $(A \times B, \odot)$ è un monoide (commutativo) e se $(A, *)$ e $(B, \cdot)$ sono gruppi (abeliani), allora $(A \times B, \odot)$ è un gruppo (abeliano), che si dice *gruppo somma diretta* dei gruppi $(A, *)$ e $(B, \cdot)$, che si indica con $A \oplus B$.

Proposizione 14. *Siano $(A, *)$ e $(B, \cdot)$ gruppi, $a \in A$, $b \in B$, entrambi di ordine finito, allora si ha la seguente formula nel gruppo somma diretta $A \oplus B$*

$$|(a, b)| = m.c.m(|a|, |b|).$$

Esempio 10. Fissati $n, m \in \mathbb{N}^*$, $n \neq 1$, si può considerare il gruppo somma diretta $\mathbb{Z}_n \oplus \mathbb{Z}_m$ di $(\mathbb{Z}_n, +)$ e $(\mathbb{Z}_m, +)$, che è un gruppo abeliano finito di ordine $n \cdot m$.

Esercizio 2. In quali ipotesi su n ed m, $\mathbb{Z}_n \oplus \mathbb{Z}_m$ è ciclico?

Esercizio 3. Studiare il gruppo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (gruppo di Klein).