

Legge di composizione interna su un insieme $A \neq \emptyset$ (operazione)

$$\ast : A \times A \longrightarrow A$$
$$(a, b) \longmapsto a \ast b$$
$$a \ast b = \ast(a, b)$$

(A, \ast) si chiama struttura algebrica della quale A è il sostegno

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$+ : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$$

$$+ : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

$$\cdot : \mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$$

$$\cdot : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

(A, \ast) struttura algebrica

* si dice associativa (o può riferirsi anche alla struttura (A, \ast))

$$\forall a, b, c \in A \quad (a \ast b) \ast c = a \ast (b \ast c)$$

* $(\circ (A, \ast))$ ammette elemento neutro

$$\exists e \in A \text{ tale che } \forall a \in A \quad a \ast e = e \ast a = a$$

Abbiamo verificato che l'elemento neutro, quando esiste, è unico.

(A, \ast) si dice monoidre quando è associativa e ammette elemento neutro

$(\mathbb{N}, +)$
 (\mathbb{Z}, \cdot) , (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) } monoidi **commutativi**
 (A^A, \circ) $A^A = \{ f: A \rightarrow A \}$ } monoidi **non commutativi**
 (W, \cdot) monade delle parole

Sia $(A, *)$ una struttura algebrica dotata di elemento neutro e .
 Un elemento $a \in A$ si dice simmetrizzabile se esiste
 $a' \in A$ tale che $a * a' = a' * a = e$; a' si dice
 simmetrico di a e abbiamo visto che nei monoidi
 il simmetrico (eventuale) di un elemento è unico.
 Una struttura algebrica $(A, *)$ si dice gruppo se
 è associativa, è dotata di elemento neutro e se
 ogni elemento di A è simmetrizzabile.

Proprietà commutativa: $(A, *)$ struttura algebrica
 si dice che $*$ (\circ $(A, *)$) è commutativa se
 $\forall a, b \in A \quad a * b = b * a$.

Un gruppo commutativo si dice abeliano.

Esempi di gruppi:

$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$
 (\mathbb{Q}^*, \cdot) , (\mathbb{R}^*, \cdot) } gruppi **abeliani**

Si considera l'insieme $S(A) = \{f : A \rightarrow A : f \text{ è bigettiva}\}$

$$S(A) \subset A^A$$

$(S(A), \circ)$ è un gruppo non abeliano

$$\forall f \in S(A) \quad \exists f^{-1} \in S(A) \text{ tale che } f \cdot f^{-1} = f^{-1} \cdot f = id_A$$

Notazione moltiplicativa: $\cdot, \circ, *$

(G, \cdot) gruppo l'elemento neutro si indica con 1 (1_G)

il simmetrico di un elemento $a \in G$ si dice inverso di a e si indica con a^{-1} .

$$x \in \mathbb{Q}^* \quad x^{-1} = \frac{1}{x}$$

Notazione additiva: $+, \oplus, -$

$(G, +)$ gruppo l'elemento neutro si indica con 0 (0_G)

il simmetrico di un elemento $a \in G$ si dice opposto di a e si indica con $-a$.

(G, \cdot) gruppo si definisce la potenza n-aria ($n \in \mathbb{Z}$) di un elemento $a \in G$

$n > 0$ si definisce ricorsivamente:

$$a^0 = 1$$

$$a^n = a^{m-1} \cdot a$$

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n\text{-volte}}$$

$$n < 0 \Rightarrow -n > 0$$

a^{-n} è noto

$$a^m = (a^{-n})^{-l}$$

$(G, +)$ sia $a \in G$, sia $n \in \mathbb{Z}$. Si definisce il multiplo di a secondo n

$n > 0$ si definisce il multiplo ricorsivamente

$$0 \cdot a = 0$$

$$n \cdot a = (n-1)a + a$$

$$n \cdot a = \underbrace{a + a + \dots + a}_{n\text{-volte}}$$

$$n < 0 \Rightarrow -n > 0 \quad (-n)a \text{ è noto}$$

si pose $n \cdot a = -((-n)a)$

(\mathbb{Q}^+, \cdot)
 $3^4 = 3 \cdot 3 \cdot 3 \cdot 3$

$(\mathbb{Z}, +)$
 $4 \cdot 3 = 3 + 3 + 3 + 3$

Prop. (G, \cdot) gruppo

$$1. \forall a \in G \quad \forall n, m \in \mathbb{Z} \quad (a^n)^m = a^{n \cdot m}$$

$$2. \forall a \in G \quad \forall n, m \in \mathbb{Z} \quad a^n \cdot a^m = a^{n+m}$$

3. Se (G, \cdot) è abeliano

$$\forall a, b \in G \quad \forall n \in \mathbb{Z} \quad (a \cdot b)^n = a^n b^n$$

$(G, +)$ gruppo

$$\forall a \in G \quad \forall n, m \in \mathbb{Z} \quad n(ma) = (n \cdot m)a$$

$$\forall a \in G \quad \forall n, m \in \mathbb{Z} \quad na + ma = (n+m)a$$

Se $(G, +)$ è abeliano

$$\forall a, b \in G \quad \forall n \in \mathbb{Z} \quad n(a+b) = na + nb.$$

Prop. (Leggi di cancellazione nei gruppi)

Sia (G, \cdot) un gruppo.

Allora $\forall a, b, c \in G$ si ha:

$$(1) \quad a \cdot c = b \cdot c \Rightarrow a = b$$

$$(2) \quad c \cdot a = c \cdot b \Rightarrow a = b$$

Dim. (1) $\frac{a \cdot c = b \cdot c}{\text{associatività di } \cdot} \Rightarrow (a \cdot c) \cdot c^{-1} = (b \cdot c) \cdot c^{-1} \Rightarrow$

esistenza dell'inverso di ogni elemento di G

$$\Rightarrow a \cdot (c \cdot c^{-1}) = b \cdot (c \cdot c^{-1}) \Rightarrow a \cdot 1_G = b \cdot 1_G \Rightarrow$$

$$\Rightarrow a = b$$

In modo analogo si prova (2).

Notazione additiva $(G,+)$ gruppo $\forall a, b, c \in G$

$$(1) \quad a + c = b + c \Rightarrow a = b$$

$$(2) \quad c + a = c + b \Rightarrow a = b$$

Def. Sia (A, \ast) una struttura algebrica e sia R una relazione di equivalenza su A . Si dice che R è compatibile con \ast se:

$$\forall a, b, c, d \in A \quad (a, b) \in R \wedge (c, d) \in R \Rightarrow (a \ast c, b \ast d) \in R$$

$$\left. \begin{array}{l} aRb \wedge cRd \Rightarrow a \ast c R b \ast d \end{array} \right\}$$

Esempio 1. $(\mathbb{Z}, +)$ R_n congruenza (mod n)

R_n è compatibile con $+$ se infatti abbiamo verificato che $\forall a, b, c, d \in \mathbb{Z}$

$$a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a+c \equiv b+d \pmod{n}$$

2. (\mathbb{Z}, \cdot) R_n è compatibile con \cdot . Infatti abbiamo verificato che $\forall a, b, c, d \in \mathbb{Z}$

$$a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a \cdot c \equiv b \cdot d \pmod{n}.$$

Terzene sia (A, \ast) una struttura algebrica e sia R una relazione di equivalenza su A compatibile con \ast . Allora si può definire una legge di composizione interna su A/R :

$$\ast_R : A/R \times A/R \longrightarrow A/R$$

tale che $\forall [a]_R, [b]_R \in A/R$

$$[a]_R \ast_R [b]_R = [a \ast b]_R$$

Dim: Siano $[a]_Q, [b]_Q \in A/Q$ e siano $a' \in [a]_Q, b' \in [b]_Q$

$$[a']_Q = [a]_Q, \quad [b']_Q = [b]_Q.$$

perché $a' \in [a]_Q \Rightarrow (a, a') \in Q \Rightarrow [a]_Q = [a']_Q$.

$$[a]_Q * [b]_Q = [a * b]_Q$$

$$[a']_Q * [b']_Q = [a' * b']_Q$$

$$\text{e fosse } [a * b]_Q \neq [a' * b']_Q$$

$$\underbrace{[a]_Q * \underbrace{[b]_Q}_{\equiv}}_{\equiv} = \underbrace{[a']_Q * \underbrace{[b']_Q}_{\equiv}}_{\equiv} \quad \left. \begin{array}{l} \text{contraddiz.} \\ \text{compatib.} \end{array} \right\}$$

$$([a]_Q = [a']_Q \wedge [b]_Q = [b']_Q) \Rightarrow ((a, a') \in Q \wedge (b, b') \in Q) \Rightarrow$$

$$\Rightarrow (a * b, a' * b') \in Q \Rightarrow [a * b]_Q = [a' * b']_Q.$$

Esempi. $(\mathbb{Z}, +)$ (\mathbb{Z}, \cdot)

\mathbb{Z}_n è compatibile sia con $+$ che con \cdot . Allora

possiamo definire (per il Teorema) $\mathbb{Z}_n = \mathbb{Z}/Q_n$

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n$$

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

$$\cdot : \mathcal{N}_n \times \mathcal{N}_n \longrightarrow \mathcal{N}_n$$

$$\forall [a]_n, [b]_n \in \mathcal{L} \quad [a]_n \cdot [b]_n = [a \cdot b]_n .$$

Exempel 1. $\mathcal{L}_1 = \{0\}, \{1\}$

$$[0]_1 + [0]_1 = [0]_1$$

$$[0]_1 \cdot [0]_1 = [0]_1$$

$$2. \quad \mathbb{Z}_2 = \{ [0]_2, [1]_2 \}$$

$$[0]_1 + [0]_2 = [0+0]_2 = [0]_2$$

$$[0]_2 + [1]_2 = [0+1]_2 = [1]_2$$

$$[1]_2 + [0]_2 = [1+0]_2 = [1]_2 + [0]_2$$

$$[1]_2 + [1]_2 = [1+1]_2 = [2]_2 = [0]_2.$$

$[0]_2$	$[1]_2$
$[0]_2$	$[1]_2$
$[1]_2$	$[0]_2$

	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

	+	$[0]_3$	$[1]_3$	$[2]_3$
$\rightarrow [0]_3$		<u>$[0]_3$</u>	<u>$[1]_3$</u>	<u>$[2]_3$</u>
$[1]_3$		$[1]_2$	$[2]_3$	$[0]_3$
$[2]_3$		$[2]_3$	$[0]_3$	$[1]_3$

$$[1]_3 + [2]_3 = [1+2]_3 = [3]_3 = \\ = [0]_3$$

$$[2]_3 \sim [2]_3 = [2+2]_3 = [4]_3 = [1]_3$$

$4 \equiv 1 \pmod{3}$

.	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

4. $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

+	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

*	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[1]_4$

$$q \equiv 1 \pmod{4}$$

$$q-1 = 8 \text{ multipli di } 4.$$

Osserv. Sia $(A, *)$ una struttura algebrica e sia \mathcal{R} una relazione di equivalenza compatibile con $*$. Allora si può considerare la struttura algebrica $(A/\mathcal{R}, *_{\mathcal{R}})$.

Altro: - se (A, \times) è associativa, allora $(A/\alpha, \times_\alpha)$ lo è
 - se $e \in A$ è l'elemento neutro di (A, \times) , allora $[e]_\alpha$ è
 l'elemento neutro di $(A/\alpha, \times_\alpha)$.

Se $a \in A$ e a' è il simmetrico di a , allora
 $[a']_\alpha$ è il simmetrico di $[a]_\alpha$.

Se (A, \times) è commutativa, allora $(A/\alpha, \times_\alpha)$ è commutativa.

Quindi: $(\mathbb{Z}_n, +)$ è un gruppo abeliano, perché
 $(\mathbb{Z}, +)$ è gruppo abeliano. Inoltre

$[0]_\alpha$ è l'elemento neutro di $(\mathbb{Z}_n, +)$

$\forall [a]_n \in \mathbb{Z}_n \quad [-a]_n$ è l'opposto di $[a]_n$.

(\mathbb{Z}_n, \cdot) è un monoido, perché (\mathbb{Z}, \cdot)
 è un monoido e inoltre

$[1]_n$ è l'elemento neutro di (\mathbb{Z}_n, \cdot) .

$\mathbb{Z}_n \neq \mathbb{Z}$!! $\forall [a]_n \in \mathbb{Z}_n \quad [a]_n \notin \mathbb{Z}$

Def. Sia (G, \cdot) (rispettivamente $(G, +)$) un gruppo. Un
 sottogruppo $H \subset G$ si dice chiuso rispetto a \cdot (rispettivamente $+$)

se $a, b \in H$ $a \cdot b \in H$ (rispettivamente $a+b \in H$).

Df. Sia (G, \cdot) un gruppo $((G, +))$ e sia $H \subset G$.
si dice che H è un sottogruppo di (G, \cdot) $((G, +))$ se è
sua volta un gruppo.

Teorema 1. Sia (G, \cdot) $((G, +))$ un gruppo e sia
 $H \subset G$. H è un sottogruppo di (G, \cdot) $((G, +))$ se

$$\left. \begin{array}{l} SG_1) H \neq \emptyset \\ SG_2) \forall a, b \in H \quad a \cdot b \in H \\ SG_3) \forall a \in H \quad a^{-1} \in H \end{array} \right\} \begin{array}{l} H \neq \emptyset \\ \forall a, b \in H \quad a + b \in H \\ \forall a \in H \quad -a \in H \end{array}$$

Teorema 2. Con le stesse notazioni del teorema 1.

H è un sottogruppo se e solo se

$$\left. \begin{array}{l} SG'_1) 1_G \in H \\ SG'_2) \forall a, b \in H \quad a \cdot b^{-1} \in H \end{array} \right\} \begin{array}{l} 0_G \in H \\ \forall a, b \in H \quad a - b \in H \end{array}$$

Esempio $(\mathbb{Z}, +)$ gruppo

$$H = 3\mathbb{Z} = \{n \in \mathbb{Z} : \exists h \in \mathbb{Z} \text{ tale che } n = 3h\} = \\ = \{3h : h \in \mathbb{Z} : \text{insieme dei multipli di } 3\}$$

è un sottogruppo di $(\mathbb{Z}, +)$.

Per il teorema 1

$$\text{SG}_1) H \neq \emptyset \quad \text{per } 0 = 0 \in H$$

$$\text{SG}_2) \text{ siano } n = 3h, m = 3k \in H \text{ allora}$$

$$n + m = 3h + 3k = 3(h + k) \in H$$

$$\text{SG}_3) \text{ ma } n = 3h \in H; \text{ allora } -n = -3h = 3(-h) \in H$$

$3\mathbb{Z}$ è un sottogruppo di $(\mathbb{Z}, +)$.

Osserv. $\forall k \in \mathbb{Z}$ $H = k\mathbb{Z} = \{n \in \mathbb{Z} : \exists h \in \mathbb{Z} \text{ tale che } n = k \cdot h\} =$ insieme dei multipli di k

è un sottogruppo di $(\mathbb{Z}, +)$.

Prop. Sia (G, \cdot) un gruppo e siano H, K sottogruppi di (G, \cdot) . Allora $H \cap K$ è un sottogruppo di (G, \cdot) .

Dinv. (per esercizio).

Osserv. Sia (G, \cdot) un gruppo, e siano H, K sottogruppi di (G, \cdot) . Allora in generale $H \cup K$ non è un sottogruppo di (G, \cdot) .

Esempio $(\mathbb{Z}, +)$ $H = 3\mathbb{Z}$ $K = 4\mathbb{Z}$

$$3 \in H \cap K \quad 4 \in K \subset H \cup K$$

$3+4=7 \notin H \cup K$ e quindi $H \cup K$ non verifica SG₂).

Esempio - $(S(A), \circ)$ è un gruppo non abeliano

In particolare (S_n, \circ) è un gruppo non abeliano.

S_n = insieme delle permutazioni di $\{1, \dots, n\}$.

$$\Delta: S_n \longrightarrow \{-1, 1\}$$

$$\forall f \in S_n \quad \Delta(f) = \begin{cases} 1 & \text{se } f \text{ è di classe pari} \\ -1 & \text{se } f \text{ è di classe dispari} \end{cases}$$

Per esempio

$$\Delta(c_1 c_2) = -1$$

$$\Delta(c_1 c_2 c_3) = 1$$

Prop. Siano $f, g \in S_n$.

Risulta allora $\Delta(f \cdot g) = \Delta f \cdot \Delta g \in \{1, -1\}$

Dim. Sia $f = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_h$ $\sigma_1, \dots, \sigma_h$ scambi

Sia $g = \tau_1 \circ \tau_2 \circ \dots \circ \tau_k$ τ_1, \dots, τ_k scambi

$$f \circ g = \underbrace{\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_h \circ \tau_1 \circ \tau_2 \circ \dots \circ \tau_k}_{h+k \text{ scambi}}$$

h, k pari o dispari entrambi, allora $h+k$ è pari

h, k uno dispari e l'altro pari, allora $h+k$ è dispari

$\Delta(f \circ g) = 1$ se $f \circ g$ sono entrambe di classe pari o dispari

$\Delta f \cdot \Delta g = \overline{1 \cdot 1 = 1}$ se $f \circ g$ sono entrambe di classe pari

$\overline{(-1) \cdot (-1) = 1}$ se $f \circ g$ sono entrambe di classe dispari

Quindi $\Delta(f \circ g) = \Delta f \cdot \Delta g$ perché entrambi uguali a 1

Supponiamo f di classe pari e g di classe dispari (o viceversa). Allora

$\Delta(f \circ g) = -1$ perché $f \circ g$ è composto da $h+k$ scambi

$$\Delta f \cdot \Delta g = 1 \cdot (-1) = -1$$

Anche in questo caso $\Delta(f \cdot g) = \Delta f \cdot \Delta g$.

Sia $\mathcal{A}_n = \{f \in S_n : \Delta f = \pm\}$ = permutazioni di classe pari

\mathcal{A}_n è un sottogruppo di (S_n, \circ) che si dice
gruppo alterno.

SG₁) $\mathcal{A}_n \neq \emptyset$ perché $id_n \in S_n$
 $\Delta id_n = \pm$

SG₂) $f, g \in \mathcal{A}_n \Rightarrow \Delta(f \cdot g) = \Delta f \cdot \Delta g = 1 \cdot 1 = 1 \Rightarrow$
 $\Rightarrow f \cdot g \in \mathcal{A}_n$

SG₃) Sia $f \in \mathcal{A}_n$

$$1 = \Delta id_n = \Delta(f \cdot f^{-1}) \in \Delta f \cdot \Delta(f^{-1}) = 1 \cdot \Delta(f^{-1}) \Rightarrow \Delta(f^{-1}) = 1$$

quindi $f^{-1} \in \mathcal{A}_n$

Abbiamo verificato che \mathcal{A}_n è un sottogruppo di (S_n, \circ)