Lezione 8

Alessandro Ardizzoni

Operazioni

Sia S un insieme. Definiamo l'insieme S^n per ogni $n \in \mathbb{N}$ ponendo

$$S^0 := \{\emptyset\} = \text{ singoletto}$$

e per $n > 0$

$$S^n := S \times \cdots \times S \ (n \text{ volte}).$$

Un'operazione n-aria su S è una funzione

$$\omega : S^n \to S.$$

Se $n = 0, 1, 2$ si dice anche operazione nullaria, unaria e binaria rispettivamente.

Una struttura algebrica è un insieme S, chiamato insieme soggiacente, munito di una o più operazioni $\omega_1, \omega_2, \ldots, \omega_m$ che soddisfino certe proprietà. Useremo la notazione $(S, \omega_1, \omega_2, \ldots, \omega_m)$ per indicarla.

Osservazione

1) Un'operazione nullaria su S è una funzione $\omega : \{\emptyset\} \to S$ ed è quindi univocamente determinata dall'elemento $\omega(\emptyset) \in S$. Pertanto darsi un'operazione nullaria su S equivale a scegliere un elemento di S.
Pertanto, in luogo della struttura algebrica (S, ω) si scriverà in questo caso semplicemente $(S, \omega(\emptyset))$. Ad es.

- *Se $\omega : \{\emptyset\} \to \mathbb{N}$, $\emptyset \mapsto 1$, invece di $(\mathbb{N}, \omega)$ si scrive $(\mathbb{N}, 1)$.*
- *Se $\omega : \{\emptyset\} \to \mathbb{Z}$, $\emptyset \mapsto 0$, invece di $(\mathbb{Z}, \omega)$ si scrive $(\mathbb{Z}, 0)$.*

2) Un'operazione unaria su S è una funzione $\omega : S \to S$. Ad esempio

- $\mathbb{Z} \to \mathbb{Z}$, $m \mapsto -m$,
- $\mathbb{Q} \setminus \{0\} \to \mathbb{Q} \setminus \{0\}$, $q \mapsto q^{-1}$,
- $\mathbb{N} \to \mathbb{N}$, $n \mapsto n^2$.

In realtà, quando parleremo di operazioni, intenderemo per lo più delle operazioni binarie.

Un'operazione binaria su S (detta anche legge di composizione interna) è una funzione

$$* : S \times S \to S.$$

L'immagine della coppia $(a, b) \in S \times S$ tramite questa funzione è un elemento di S indicato col simbolo $a * b$ che si legge "a composto b" o "composizione di a e b". Scriveremo quindi

$$* : S \times S \to S, \quad (a, b) \mapsto a * b.$$

Un insieme S dotato di un'operazione (binaria) $*$ si chiama magma (oppure gruppoide) e si indica con il simbolo $(S, *)$.
E' dunque un esempio di struttura algebrica.

Le notazioni moltiplicativa e additiva

Si possono usare vari simboli per indicare le operazioni. Ad esempio:

$$* \quad \diamond \quad \square \quad \circ \quad \bullet$$

Ce ne sono però due che sono usati più spesso e sono i seguenti.

1. $\cdot : S \times S \to S, (a, b) \mapsto a \cdot b$. In questo caso l'operazione è detta moltiplicazione mentre $a \cdot b$ è detto il "prodotto di a e b" o anche "a per b". Si dice anche che viene usata la "notazione moltiplicativa".
2. $+ : S \times S \to S, (a, b) \mapsto a + b$. In questo caso l'operazione è detta addizione mentre $a + b$ è detta la "somma di a e b" o anche "a più b". Si dice anche che viene usata la "notazione additiva".

Esempio

Su $\mathbb{N}$ abbiamo sia la moltiplicazione che l'addizione

$$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a \cdot b,$$

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a + b.$$

Abbiamo dunque i due magmi $(\mathbb{N}, \cdot)$ e $(\mathbb{N}, +)$. A volte considereremo entrambe le operazioni cioè la struttura algebrica $(\mathbb{N}, +, \cdot)$.

Notiamo invece che la sottrazione e la divisione

$$- : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a - b$$

$$\div : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (a, b) \mapsto a \div b$$

non sono operazioni su $\mathbb{N}$ perché non sono ben definite.
Ad esempio $1 - 2 \notin \mathbb{N}$ e $1 \div 2 \notin \mathbb{N}$.

Esempio

Poniamo

$$a * b := \frac{ab}{2}.$$

Non è un'operazione su $\mathbb{Z}$ perché in generale $a * b \notin \mathbb{Z}$ se $a, b \in \mathbb{Z}$.
Ad esempio $1 * 1 = \frac{1}{2} \notin \mathbb{Z}$.

Esempio

Ecco altri esempi di magma $(S, *)$:

- Interi, razionali e reali con l'addizione: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$;
- Interi, razionali e reali con la sottrazione: $(\mathbb{Z}, -), (\mathbb{Q}, -), (\mathbb{R}, -)$;
- Interi, razionali e reali con la moltiplicazione: $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$;
- Razionali e reali positivi con la divisione: $(\mathbb{Q}_{>0}, \div), (\mathbb{R}_{>0}, \div)$;
- L'insieme delle parti di S con l'unione: $(P(S), \cup)$;
- L'insieme delle parti di S con l'intersezione: $(P(S), \cap)$.

Definizione

Consideriamo un magma $(S, *)$. Diremo che l'operazione $*$ è

- associativa se $\forall a, b, c \in S,\ (a * b) * c = a * (b * c)$.
- commutativa se $\forall a, b \in S,\ a * b = b * a$.

Un elemento $e \in S$ è detto un elemento neutro (rispetto a $*$) se

$(\mathbb{R}, *)$ con $x * y = \frac{x+y}{2}$ NON associativo ma commutativo

$$\forall a \in S,\ a * e = a = e * a.$$

Dato un elemento neutro e, un elemento $a \in S$ si dice invertibile se

$$\exists b \in S,\ a * b = e = b * a.$$

In tal caso l'elemento b corrispondente è detto un inverso di a.

Osservazione

Se l'operazione $*$ è commutativa, le richieste per l'esistenza di un elemento neutro o di un inverso si dimezzano.

Osservazione

Sia S un insieme dotato di un'operazione. Se la notazione usata è quella moltiplicativa, l'elemento neutro si indica usualmente con il simbolo 1_S o semplicemente 1 e prende il nome di identità oppure di unità di S. Generalmente la notazione additiva è riservata ad operazioni commutative. In tal caso l'elemento neutro si chiamo zero e si indica con il simbolo 0_S o 0. Invece di "inverso" si parla di opposto.

Esempio

Consideriamo $(\mathbb{Z}, -)$.
ASSOCIATIVITA'. Non vale perché $(1-1)-1 \neq 1-(1-1)$.
ELEMENTO NEUTRO. Se in $(\mathbb{Z}, -)$ ci fosse un elemento neutro, diciamo e, allora per ogni $n \in \mathbb{Z}$ si avrebbe $n - e = n$ ed $e - n = n$ da cui $e = 0$ e dunque $-n = n$. Quest'ultima uguaglianza implica $n = 0$ ma n era arbitrario e quindi siamo giunti ad un assurdo.
INVERSO. Se non c'è elemento neutro non c'è inverso.
COMMUTATIVITA'. La commutatività non vale perché $1 - 0 \neq 0 - 1$.

Vediamo nella seguente tabella alcuni esempi:

$(S,*)$	Associatività	Elemento Neutro	Inverso	Commutat.
$(\mathbb{Z},+)$	si	si: è 0 $(n+0=n=0+n)$	si: è l'opposto	si
$(\mathbb{Z},-)$	no	no	no	no
$(\mathbb{Z},\cdot)$	si	si: è 1 $(n\cdot 1=n=1\cdot n)$	no	si
$(\mathbb{Q}\setminus\{0\},\cdot)$	si	si: è 1	si $(\frac{a}{b}\cdot\frac{b}{a}=1=\frac{b}{a}\cdot\frac{a}{b})$	si
$(\mathbb{Q}_{>0},\div)$	no	no	no	no
$(P(S),\cup)$	si	si: è $\emptyset$ $(A\cup\emptyset=A=\emptyset\cup A)$	no (★)	si
$(P(S),\cap)$	si	si: è S $(A\cap S=A=S\cap A)$	no	si

(★) Se in $(P(S),\cup)$, esistesse un inverso di $A\in P(S)$, diciamo B, allora risulterebbe $A\cup B=\emptyset$ da cui $A=B=\emptyset$, assurdo.

Esempio

Poniamo $a*b:=a^b$. E' un'operazione su $\mathbb{N}\setminus\{0\}$ (la potenza) ma non è associativa. Altrimenti $\forall a,b,c\in\mathbb{N}$ si avrebbe $(a*b)*c=a*(b*c)$ cioé $(a^b)^c=a^{b^c}$ ma questo non è vero: $(2^1)^2=4\neq 2=2^{1^2}$. Se ci fosse un elemento neutro e allora, per ogni $a\in\mathbb{N}$, si avrebbe $e*a=a$, cioé $e^a=a$. In particolare, scegliendo $a=1$, si avrebbe $e^1=1$ e dunque $e=1$. Ma allora dovrebbe valere, per ogni $a\in\mathbb{N}$, $1^a=a$ il che è falso.

Proposizione

Un magma può avere un unico elemento neutro

Proof.

Consideriamo un magma $(S, *)$ con elementi neutri e ed e'. Per definizione, $\forall a, b \in S$ abbiamo $a * e = a = e * a$ e $b * e' = b = e' * b$. Scegliendo $a = e'$ e $b = e$ otteniamo $e' * e = e' = e * e'$ ed $e * e' = e = e' * e$. In particolare $e' = e * e' = e$ cioé $e' = e$. □

Per questo diremo che e è l'elemento neutro di S, se esiste.

Esempio

Dato un insieme A consideriamo l'insieme $\mathscr{F}(A)$ delle funzioni $A \to A$ e l'operazione $\circ : \mathscr{F}(A) \times \mathscr{F}(A) \to \mathscr{F}(A), (f, g) \mapsto f \circ g$, che a due funzioni associa la loro funzione composta. Abbiamo già osservato che la composizione di funzioni è associativa. Inoltre Id_A è l'elemento neutro della composizione. Non tutte le funzioni $f : A \to A$ sono invertibili (sappiamo che solo le biiettive lo sono). Inoltre in generale $f \circ g \neq g \circ f$, dunque non vale la commutatività.

Definizione

Sia $(S, *)$ un magma dotato di un elemento neutro $e \in S$. Sia $a \in S$.

- Un inverso sinistro di a è un $s \in S$ tale che $s * a = e$.
- Un inverso destro di a è un $d \in S$ tale che $a * d = e$.
- Un inverso bilatero di a è un $b \in S$ tale che $b * a = e = a * b$ (cioè un suo inverso sinistro e destro).

Osservazione

Se $b \in S$ è un inverso bilatero di a allora $b * a = e = a * b$ e dunque a è invertibile e b è quello che abbiamo chiamato "un inverso di a".

Definizione

Un semigruppo è un magma $(M, *)$ dove $*$ è associativa.
Un monoide è un semigruppo $(M, *)$ in cui esiste l'elemento neutro rispetto a $*$. Diremo anche che $(M, *, e)$ è un monoide, se vogliamo mettere in evidenza l'elemento neutro (si tratta di una struttura algebrica dove e si intende come un'operazione nullaria).
Un monoide $(M, *)$ si dice commutativo o abeliano (tributo al matematico norvegese Niels Henrik Abel) se $*$ è commutativa.

Vediamo ora alcuni esempi di semigruppi e monoidi.

Esempio

- $(\mathbb{N} \setminus \{0\}, +)$ è un semigruppo ma non un monoide;
- $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ sono monoidi commutativi;
- $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(P(S), \cup)$, $(P(S), \cap)$, sono monoidi commutativi;
- dato un insieme A, l'insieme $\mathscr{F}(A)$ delle funzioni $f : A \to A$ è un monoide non commutativo rispetto a $\circ$.

Proposizione

Sia $(M, *, e)$ un monoide. Se $a \in M$ ha un inverso sinistro ed uno destro allora essi coincidono cioé a è invertibile. Inoltre se un elemento ha un inverso, questo è unico.

Proof.

Se $a \in M$ ha un inverso sinistro s ed uno destro d, allora
$s = s * e = s * (a * d) = (s * a) * d = e * d = d$.
Se un elemento $a \in M$ ha due inversi, essi saranno in particolare sia inversi sinistri che destri e quindi dovranno coincidere. □

Abbiamo dimostrato che in un monoide $(M, \cdot, e)$ se un elemento $a \in M$ ha un inverso $b \in M$, allora questo è unico. Diremo allora che b è l'inverso di a e lo indicheremo con a^{-1}. Se il monoide è in notazione additiva, l'inverso si chiama l'opposto di a e lo indicheremo con $-a$.

In notazione moltiplicativa $x \cdot y^{-1}$ si indica anche con x/y se l'operazione è commutativa. Similmente, in notazione additiva in luogo di $x + (-y)$ si scrive più semplicemente $x - y$.

Per alleggerire la notazione, useremo d'ora in poi la notazione moltiplicativa per un operazione binaria non necessariamente associativa.
Sia dunque $(X, \cdot)$ un semigruppo. Allora, per la proprietà associativa, la composizione di n elementi $x_1, \ldots, x_n$ si può denotare semplicemente come $x_1 \cdot x_2 \cdot \cdots \cdot x_n$, omettendo le parentesi.

Osservazione

In particolare per $n \in \mathbb{N} \setminus \{0\}$ è possibile definire la potenza n-esima di un elemento $x \in X$ ponendo $x^1 := x$ e $x^n := x^{n-1} \cdot x$ se $n > 1$. Quindi

$$x^n := \underbrace{x \cdot \cdots \cdot x}_{n \text{ volte}}.$$

Se inoltre $(X, \cdot, 1)$ è un monoide si può includere anche il caso $n = 0$ ponendo

$$x^0 = 1.$$

Risultano quindi definite, per un monoide, tutte le potenze x^n con $n \in \mathbb{N}$.

Proposizione

Sia $(X, \cdot)$ un monoide e $x \in X$. Per ogni $n, m \in \mathbb{N}$ si ha

a) $x^{n+m} = x^n \cdot x^m$;

b) $(x^n)^m = x^{nm}$.

Proof.

Si può fare per induzione su m oppure intuitivamente:

$$x^{n+m} = \underbrace{x \cdot \cdots \cdot x}_{n+m \text{ volte}} = \underbrace{x \cdot \cdots \cdot x}_{n \text{ volte}} \cdot \underbrace{x \cdot \cdots \cdot x}_{m \text{ volte}} = x^n \cdot x^m.$$

$$x^{nm} = \underbrace{x \cdot \cdots \cdot x}_{nm \text{ volte}} = \underbrace{\underbrace{x \cdot \cdots \cdot x}_{n \text{ volte}} \cdot \cdots \cdot \underbrace{x \cdot \cdots \cdot x}_{n \text{ volte}}}_{m \text{ volte}} = \underbrace{x^n \cdot \cdots \cdot x^n}_{m \text{ volte}} = (x^n)^m.$$

Proposizione

Se $(X, \cdot)$ è un monoide commutativo allora per ogni $x, y \in X$ e per ogni $n \in \mathbb{N}$

$$(x \cdot y)^n = x^n \cdot y^n.$$

Proof.

Si ha

$$(x \cdot y)^n = \underbrace{(x \cdot y) \cdot (x \cdot y) \cdot \cdots \cdot (x \cdot y)}_{n \text{ volte}}.$$

Applicando ripetutamente la proprietà commutativa si possono portare tutte le x a sinistra di tutte le y, ottenendo il risultato.
Ad esempio $(x \cdot y)^2 = x \cdot y \cdot x \cdot y = x \cdot x \cdot y \cdot y = x^2 \cdot y^2$. □

Tavola di Cayley

Se $S = \{x_1, x_2, x_3, \ldots, x_n\}$ è un insieme finito, un'operazione $\cdot$ su S può essere rappresentata mediante una Tavola di Cayley, che mostra tutti i possibili prodotti degli elementi di S. Gli elementi di S vengono riportati in riga (rossa in figura) e in colonna (blu) ai margini di una tabella (gialla). Poi all'incrocio tra la i-esima riga e la j-esima colonna scriveremo $x_i \cdot x_j$. Ad esempio, nel caso $S = \{x_1, x_2, x_3\}$ si ha la seguente Tavola di Cayley:

$\cdot$	x_1	x_2	x_3
x_1	$x_1 \cdot x_1$	$x_1 \cdot x_2$	$x_1 \cdot x_3$
x_2	$x_2 \cdot x_1$	$x_2 \cdot x_2$	$x_2 \cdot x_3$
x_3	$x_3 \cdot x_1$	$x_3 \cdot x_2$	$x_3 \cdot x_3$

Questa tavola consente di controllare se $\cdot$ è associativa verificando la condizione caso per caso. Possiamo fare però altre considerazioni.

Discutiamole su un esempio concreto

Sia $S = \{a, b, c\}$ e sia $\cdot$ definita dalla tavola di Cayley

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

- $\cdot$ è commutativa se la matrice gialla è simmetrica rispetto alla diagonale principale. Nell'esempio di sopra lo è.
- Se la colonna blu è uguale ad una certa colonna gialla che sta sotto ad un certo elemento $e \in S$ e lo stesso vale per la riga rossa e per una riga gialla accanto ad e, allora e è un elemento neutro. Nell'esempio a è l'elemento neutro di S (la riga gialla accanto ad a è uguale alla riga rossa e la colonna gialla sotto a è uguale alla colonna blu).
- Se ogni colonna gialla contiene l'elemento neutro almeno una volta allora ogni elemento di S ha un inverso sinistro.
- Se ogni riga gialla contiene l'elemento neutro almeno una volta allora ogni elemento di S ha un inverso destro. Nell'esempio, a, b, c hanno inversi rispettivamente a, c, b.