

STRUTTURE ALGEBRICHE CON PIÙ OPERAZIONI. (180)

Per il momento consideriamo ancora solo operazioni interne: $(X, *, \square)$.

Si esaminano in questo caso anche proprietà di "legame tra le varie operazioni". Ad esempio la proprietà "DISTRIBUTIVA DESTRA di \square rispetto a $*$ "

$$\forall x, y, z \in X \quad (x * y) \square z = x \square z * y \square z$$

o "DISTRIBUTIVA SINISTRA di \square rispetto a $*$ "

$$\forall x, y, z \in X \quad x \square (y * z) = x \square y * x \square z$$

Di solito le due operazioni $*$ e \square sono chiamate **Somma (+)** e **prodotto (·)** e quindi si hanno le formule classiche

$$(x+y) \cdot z = x \cdot z + y \cdot z$$

$$x \cdot (y+z) = x \cdot y + x \cdot z$$

ATTENZIONE: se \square non è commutativa (ad es. composizione di funzioni) la validità di una non implica quella dell'altra. Si considerino le funzioni reali di variabile reale con le operazioni di somma

$$(f+g)(x) = f(x) + g(x) \quad \forall x \in \mathbb{R}$$

e composizione: $(f \circ g)(x) = f(g(x))$.

$$\begin{aligned} \text{Si ha } ((f+g) \circ h)(x) &= (f+g)(h(x)) = \underset{DF+}{f(h(x)) + g(h(x))} = \underset{DF \circ}{(f \circ h)(x) + (g \circ h)(x)} \quad \text{vale la distr. ds.} \end{aligned}$$

ma

$$f \circ (g+h)(x) \neq f \circ g(x) + f \circ h(x)$$

Ad es. se $g(x) = x$, $h(x) = x^3 = f(x)$

$$\begin{aligned} f \circ (g+h)(x) &= f(x+x^3) = (x+x^3)^3 \\ f \circ g(x) + f \circ h(x) &= x^3 + (x^3)^3 \end{aligned}$$

E' un MEZZO MIRACOLO che invece valgano entrambe le distributive in $(M_n(\mathbb{R}), +, \cdot)$... dato che il prodotto di matrici rappresenta una composizione di applicazioni: perche' qui si mentre per le funzioni di \mathbb{R} in \mathbb{R} no?

perche' le matrici rappresentano appl. lineari, in particolare omomorfismi di \mathbb{R}^n in \mathbb{R}^n e quindi:
 $(f \circ (g+h))(x) = f \circ (g(x)+h(x)) \stackrel{f \text{ om.}}{=} f(g(x)) + f(h(x))$

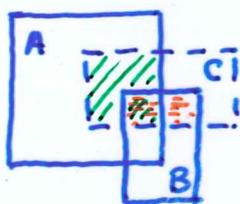
Notizie: c'e' un motivo per non rappresentare subito le due operazioni come SOMMA e PRODOTTO? A parte che gia' il primo esempio dice che il "prodotto" puo' non essere quello usuale, ci sono altre situazioni in cui vale la proprieta' distributiva e le operazioni sono "altre".

ES. In $\mathcal{P}(X)$ - ove X e' un qualunque insieme - posso considerare come \cup l'operazione \cup e come \cap l'operazione \cap ottenendo:

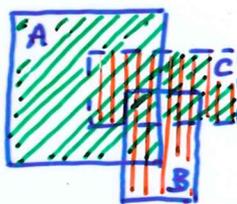
(1) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C) \quad \forall A, B, C \in \mathcal{P}(X)$

ma anche scambiare di ruolo:

(2) $(A \cap B) \cup C = (A \cup C) \cap (B \cup C) \quad \forall A, B, C \in \mathcal{P}(X)$

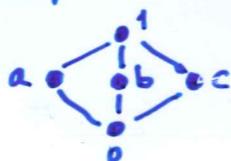


(1)



(2)

ATTENZIONE. Non sempre una relazione d'ordine e relative operazioni \inf (\wedge) e \sup (\vee) provocano questa situazione



$(a \vee b) \wedge c = 1 \wedge c = c$
 $(a \wedge c) \vee (b \wedge c) = 0 \vee 0 = 0$

\rightarrow E' il caso del gruppo TCS_4 con i suoi 4 sgrz propri.

Costituiscono l'esempio più noto di struttura algebrica con 2 operazioni "avvicinate" dall'inserimento di proprietà di legame tra le due operazioni.

DEF. Dico che $(A, +, \cdot)$ è un anello rispetto a $+$ e \cdot se

- 1) $(A, +)$ è un gruppo abeliano
- 2) (A, \cdot) è un semigrupp
- 3) valgono le due propr. distributive destra e sin.:

$$(a+b) \cdot c = a \cdot c + b \cdot c \quad a \cdot (b+c) = a \cdot b + a \cdot c$$
 per ogni $a, b, c \in A$.

l'elemento neutro rispetto a $+$ è denotato con 0_A e l'inverso ^{di $a \in A$} rispetto a $+$ è detto opposto di a e denotato con $-a$.

Le (3) dicono che

- $a \cdot c = (a + 0_A) \cdot c = a \cdot c + 0_A \cdot c$ e sommando $-(a \cdot c)$ a entrambi i membri
 $0_A = 0_A \cdot c \quad \forall c \in A$
- $a \cdot c = a \cdot (0_A + c) = a \cdot 0_A + a \cdot c$ "
 $0_A = a \cdot 0_A \quad \forall a \in A$

cioè 0_A è ZERO rispetto a \cdot .

Dicono anche che $\forall a, c \in A$

- $0_A = 0_A \cdot c = (a + (-a)) \cdot c = a \cdot c + (-a) \cdot c \Rightarrow$
 $- (a \cdot c) = (-a) \cdot c$
- $0_A = a \cdot 0_A = a \cdot ((-c) + c) = a \cdot (-c) + a \cdot c \Rightarrow$
 $- (a \cdot c) = a \cdot (-c)$

La definizione di anello non richiede altro, per cui ad es. sono anelli
 $(\mathbb{Z}, +, \cdot)$ e $(M_2(\mathbb{Z}), +, \cdot)$

DEF. Dico che $(A, +, \cdot)$ è un anello con unità se

- $(A, +, \cdot)$ è un anello e
- (A, \cdot) è un monoid.

Ad esempio sono anelli con unità
 $(\mathbb{Z}_6, +, \cdot)$ e $(M_2(\mathbb{R}), +, \cdot)$

Attenzione: fin qui non si è richiesto che il semigrupp (A, \cdot) sia commutativo (ma si è chiesto dall'inizio che lo sia $(A, +)$). Infatti tra le coppie di esempi fin qui esibite ce n'era sempre uno di quello il cui prodotto non è commutativo.

DEF. Dico che $(A, +, \cdot)$ è un anello commutativo se $(A, +, \cdot)$ è un anello e (A, \cdot) è un semigrupp commutativo.

Si potrebbero indagare strutture non commutative più ricche, ma ci accontentiamo di restare nel commutativo.

DEF. Dico che un anello commutativo con unità $(A, +, \cdot)$ è un dominio di integrità se è privo di divisori dello zero.

Ad es. $(\mathbb{Z}, +, \cdot)$ e $(\mathbb{R}[x], +, \cdot)$ sono domini di integrità
 invece $(\mathbb{Z}_6, +, \cdot)$ non lo è.

Ogni anello con unità ha almeno 2 elem. : $0_A, 1_A$

(183 bis)

C'è un anello con unità che ha esattamente

2 elementi?

$$(\mathbb{Z}_2, +, \cdot)$$

+ interna; ovvio

$[0]_2$ è neutro

$$-[1]_2 = [1]_2$$

gruppo risp + (da propr. in \mathbb{Z}_4)

$$[0]_2 \cdot [1]_2 = [0]_2 \in \mathbb{Z}_2$$

$$[1]_2 \cdot [1]_2 = [1]_2 \in \mathbb{Z}_2$$

$$[0]_2 \cdot [0]_2 \in \mathbb{Z}_2$$

prod è interno

ASS
COMM. da
propr. in \mathbb{Z}_4

$$([a]_2 + [b]_2) [c]_2 = [a+b]_2 [c]_2 = [(a+b) \cdot c]_2 =$$

$$= [ac + bc]_2 = [ac]_2 + [bc]_2 =$$

$$= [a]_2 [c]_2 + [b]_2 [c]_2$$

quindi vale la distributiva destra (e quindi la sinistra poiché il prodotto è commutativo) \Rightarrow

$(\mathbb{Z}_2, +, \cdot)$ è anello commutativo con unità con 2 elementi

È addirittura un campo!

(vedi def. successiva).

È importante che in un anello A non ci siano divisori di zero?

Sì.

Supponiamo di voler risolvere una equazione a coeff nell'anello A della forma

$$a \cdot x = a \cdot b$$



$$a \cdot x - a \cdot b = 0$$



$$a \cdot (x - b) = 0$$

se $a \neq 0$ e A è privo di divisori di zero fanno a:

$$x - b = 0 \iff x = b$$

in $(\mathbb{Z}_6, +, \cdot)$ comun. con unità $[1]_6$

ci sono divisori dello zero:

$$[2]_6 \quad \text{e} \quad [3]_6$$

Sufatti $[2]_6 \cdot [3]_6 = [0]_6$

$\Rightarrow \mathbb{Z}_6$ non è un dom. di integrità

DEF. Dico che $(A, +, \cdot)$ è un campo se

- 1) $(A, +, \cdot)$ è un anello commutativo con unità
- 2) indicato con $A^* = A \setminus \{0_A\}$, sia un gruppo (A^*, \cdot) .

Cio' significa che ogni elemento di A diverso dallo zero è dotato di inverso rispetto a \cdot . Dimosteremo il neutro risp. a \cdot con 1_A e l'inverso di $a \neq 0_A$ con a^{-1} .

Un campo è un dominio di integrità poiché, se $a \neq 0_A$ da $ab = 0_A$ si deduce

$$a^{-1} \cdot (ab) = a^{-1} \cdot 0_A$$

$$1_A \cdot b = 0_A$$

$$b = 0_A$$

Sono esempi di campi $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ ma anche $(\mathbb{Z}_p, +, \cdot)$ se p è un numero primo. Infatti per ogni $[a]_p \neq [0]_p$ è risolvibile (e in modo unico) l'eq.:

$$[a]_p [x]_p = [1]_p$$

corrispondente alla congruenza lineare

$$ax \equiv 1 \pmod{p} \quad (0 < x < p)$$

o all'eq. diofantea

$$ax + py = 1 \quad (0 < x < p).$$

Non sono campi gli anelli citati come esempi in precedenza e in particolare $(\mathbb{Z}_n, +, \cdot)$ con n non primo (che ha divisori dello zero) e $(\mathbb{R}[x], +, \cdot)$ che ha come elementi invertibili solo i polinomi di grado 0.

Se $(A, +, \cdot)$ è un campo, è lecito "fare i conti" (185) usando le ordinarie regole del calcolo letterale; si è già detto che per ogni anello

$$1) \quad \forall a \in A \quad a \cdot 0_A = 0_A \cdot a = 0_A$$

$$2) \quad \forall a, b \in A \quad (-a) \cdot b = a \cdot (-b) = -ab$$

$$\text{e quindi } (-a)(-b) = ab$$

$$3) \quad \forall a, b, c \in A \quad a + b = c \Rightarrow a = c - b$$

e per ogni anello commutativo

$$4) \quad (a+b)(a-b) = a^2 + \underbrace{ba}_{\text{COMM}} + a(-b) + b(-b) = a^2 - b^2 \quad (2)$$

$$5) \quad (a+b)^2 = a^2 + \underbrace{ab + ba}_{\text{COMM}} + b^2 = a^2 + 2ab + b^2$$

e più in generale

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \dots \\ \dots + \binom{n}{n-1} a b^{n-1} + b^n$$

Basta osservare che $(a+b)^n = (a+b)^{n-1} (a+b)$ e lavorare per induzione oppure combinatorialmente.

$$6) \quad (a-b)^n = a^n + (-1)^1 \binom{n}{1} a^{n-1} b + (-1)^2 \binom{n}{2} a^{n-2} b^2 + \dots \\ \dots + (-1)^{n-1} \binom{n}{n-1} a b^{n-1} + (-1)^n b^n$$

ove -1 è l'opposto in A dell'elemento neutro 1_A .

$$7) \quad (a-b)(a^n + a^{n-1} b + \dots + a b^{n-1} + b^n) = a^{n+1} - b^{n+1}$$

$$(a+b)(a^n + a^{n-1}(-b) + \dots + a(-b)^{n-1} + (-b)^n) = a^{n+1} - b^{n+1}$$

Inoltre in un campo, essendo un dominio di integrità, vale la legge di annullamento del prodotto: $a \cdot b = 0$ e $a \neq 0 \Rightarrow b = 0$

e quella di "semplicificazione": $ab = ac$ e $a \neq 0 \Rightarrow b = c$.