31-10-2018 STRUTTURE ALGEBRICHE

Definizione: Se in un insieme V viene messa un'operazione binaria interna "$*$" $V \times V \to V$, $(v_1, v_2) \to v_1 * v_2$, tale che tale operazione soddisfa le proprietà

1) associativa,
2) $\exists$ elemento neutro
3) $\exists$ reciproco per ogni $v \in V$

$\Rightarrow$ Allora la struttura algebrica $(V; *)$ è detta **GRUPPO**

Se "$*$" gode anche della proprietà commutativa $\Rightarrow$ si parla di Gruppo Commutativo o Abeliano (Matematico Abel). Il Premio Abel è il "premio Nobel" della matematica

~~Strutture algebriche~~:

- Gruppo: ESEMPI

1) Es $(\mathbb{Z}, +)$ è un gruppo?
   1) è Associativa ✓
   2) $\exists$ elemento neutro: 0 ✓
   3) $\forall m \in \mathbb{Z}$ $\exists$ il suo reciproco che in questo caso è detto opposto: $-m$

   ⇓

   È un gruppo $\Rightarrow$ Se l'operazione è la somma, il gruppo è detto Additivo

   ⇓

   Inoltre vale anche la proprietà commutativa $\Rightarrow$ Il gruppo è Abeliano

2) Es $(\mathbb{Z}; \cdot)$
   1) è Associativa perché $m(u \cdot k) = (m \cdot u) \cdot k \quad \forall m, u, k \in \mathbb{Z}$
   2) $\exists$ elemento neutro: $m = 1$
   3) $\forall m \in \mathbb{Z}$ $\exists$ il suo reciproco che in questo caso è l'inverso? No, perché ad esempio preso in $\mathbb{Z}$ $m = 2 \Rightarrow 2 \cdot x = 1$ se $x = \frac{1}{2} \Rightarrow$ Non vive in $\mathbb{Z}$!

   ⇓

   Per il punto 3) $(\mathbb{Z}, \cdot)$ NON è un gruppo

3) Es $(\mathbb{Q}; \cdot)$ ~~è un gruppo~~ ~~perché è associativa~~
   ↳ Non è un gruppo perché $m = 0$ non ha l'inverso!

(2)

Se dall'insieme $\mathbb{Q}$ togliamo lo 0 $\Rightarrow (\mathbb{Q}-\{0\};\cdot)$ è un gruppo moltiplicativo $\Rightarrow$ Inoltre vale anche la proprietà commutativa $\Rightarrow$ Gruppo Abeliano

Definizione: Se in un insieme V, metto 2 operazioni binarie interne "$*$": $V\times V \to V$ e "$\square$": $V\times V \to V$ che soddisfano le seguenti proprietà:

$(v_1, v_2) \to v_1 * v_2$ $\quad$ $(v_1, v_2) \to v_1 \square v_2$

1) $(V, *)$ sia un gruppo Abeliano

2) "$\square$" deve essere Associativa, deve esistere l'elemento neutro, e deve valere la proprietà distributiva di "$\square$" rispetto al "$*$" cioè $v_1 \square (v_2 * v_3) = (v_1 \square v_2) * (v_1 \square v_3) \quad \forall\, v_1, v_2, v_3 \in V$

$\Rightarrow$ la struttura algebrica $(V; *, \square)$ è detta **ANELLO**

Inoltre se "$\square$" soddisfa la proprietà commutativa, allora $(V; *, \square)$ è **anello commutativo**

1) Esempio: $V = \mathbb{Z}$ con le operazioni di somma e moltiplicazione

$+: V\times V \to V$, $(v_1, v_2) \to v_1 + v_2$ $\quad$ $\cdot: V\times V \to V$, $(v_1, v_2) \to v_1 \cdot v_2$

$(\mathbb{Z}, +, \cdot)$ è un anello?

- $(\mathbb{Z}, +)$ è un gruppo commutativo ✓
- "$\cdot$" è associativa? Sì ✓ esiste l'elemento neutro? sì: 1 ✓
- vale la proprietà distributiva di "$\cdot$" rispetto "$+$" cioè $v_1 \cdot (v_2 + v_3) = v_1 v_2 + v_1 v_3$ $\Rightarrow$ Si vede ✓ $\forall\, v_1, v_2, v_3 \in \mathbb{Z}$

$\Downarrow$

Quindi $(\mathbb{Z}; +, \cdot)$ è un Anello, $\Rightarrow$ Anello degli Interi

- È inoltre commutativo

2) Esempio: $V = \mathbb{R}[x] = \left\{ \sum_{i=0}^{N} a_i x^i,\ \forall N \in \mathbb{N} \text{ e } \forall a_i \in \mathbb{R} \right\}$

$(\mathbb{R}[x], +, \cdot)$ è un Anello? $\Rightarrow$ DA FARE

Definizione: Se in un insieme V metto due operazioni binarie interne $* \; V\times V \to V$ e $\square \; V\times V \to V$ che soddisfano:

1) $(V;*)$ è un gruppo Abeliano
2) $(V - \{\text{elemento neutro di } *\}; \square)$ è un gruppo
3) Vale la proprietà distributiva di "$\square$" rispetto "$*$", allora la struttura $(V;*,\square)$ è detta [redacted] **CORPO**

Inoltre se l'operazione $\square$ gode della commutatività, la struttura $(V;*,\square)$ è detta **CAMPO**

ESERCIZI DA SVOLGERE

$(\mathbb{R};+,\cdot)$ è un Campo

$(\mathbb{Q};+,\cdot)$ è un Campo

$(\mathbb{C};+,\cdot)$ è un Campo

Definizione: Dato un campo K si dice CARATTERISTICA del campo K, char K, il più piccolo intero n per cui $\forall x \in K$ $\underbrace{x+x+\ldots x}_{n \text{ volte}} = 0$

↓

Per $\mathbb{Q}$, $\mathbb{C}$ ed $\mathbb{R}$ è 0

Costruisco un campo il cui insieme è dato da 2 elementi (soggiacente):

Considero $\mathbb{Z}$ e una relazione di equivalenza fra i suoi elementi:

$p \sim q$ se e solo se $p = q + 2K$ con $K \in \mathbb{Z}$ (operazione detta resto modulo 2)

es: $4 - 26 = -22 = 2\cdot(-11)$ ⇒ ABBIAMO TROVATO $K=-11$ ⇒ 4 e 26 sono nella stessa classe di equivalenza.

⇓

In questo modo si costruiscono solo 2 classi di equivalenza: $[0]$ $[1]$ $(= \bar{0}, \bar{1})$ (DOVE METTIAMO IN EVIDENZA I RAPPRESENTANTI 0 E 1)

$[0]$ → Classe di interi Pari; $[1]$ → Classe degli interi dispari

l'insieme $\{\bar{0}, \bar{1}\} = \mathbb{Z}_2$ è detto insieme Quoziente

Definiamo due operazioni in $\mathbb{Z}_2$ "$+$" $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$ E "$\cdot$" $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2$

4)

Costruiamo la tabella dell'operazione Somma ($\bar{0}$ e $\bar{1}$ rappresentano rispettivamente i numeri pari e i numeri dispari)

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

VOGLIO $\bar{0}+\bar{0}$ ⇒ PRENDO UN RAPPRESENTANTE DI $\bar{0}$ (AD ESEMPIO 26), UN RAPPRESENTANTE DEL SECONDO ADDENDO $\bar{0}$ (AD ES. −18), FACCIO 26 − 18 = 8 ; STA NELLA CLASSE $\bar{0}$ ⇒ $\bar{0}+\bar{0}=\bar{0}$

↳ Perché 1+1=2 che è un numero pari E QUINDI STA NELLA CLASSE $\bar{0}$ ⇒ $\bar{1}+\bar{1}=\bar{0}$ E COSÌ VIA...

·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

Dimostrare che $(\mathbb{Z}_2, +, \cdot)$ è un Campo (DA FARE)

COSTRUIRE $\mathbb{Z}_5$ E DIMOSTRARE CHE $(\mathbb{Z}_5, +, \cdot)$ È UN CAMPO. $\forall p$ NUMERO PRIMO, $(\mathbb{Z}_p, +, \cdot)$ È CAMPO.

ORA Consideriamo $(V, +, \cdot\alpha)$, SPAZIO VETTORIALE SU UN CAMPO K (ABBIAMO GIÀ DEFINITO QUESTA STRUTTURA ALGEBRICA DEFINITA SU V)

Alcuni sottoinsiemi di V mantengono la struttura algebrica definita su V

Tali sottoinsiemi W verificano queste proprietà:

1) $0 \in W$

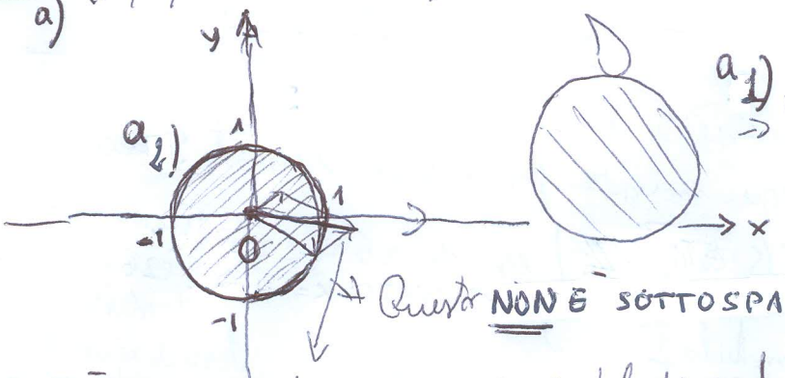
2) Se $w_1 e w_2 \in W \Rightarrow w_1 + w_2 \in W$ $\forall w_1, w_2 \in W$

3) Se $w \in W \Rightarrow \alpha w \in W$ $\forall \alpha \in K$, $\forall w \in W$.

↳ Si dice che W deve essere CHIUSO rispetto alle operazioni definite su V e W è detto SOTTOSPAZIO VETTORIALE.

ESEMPI: $(\mathbb{R}^2, +, \cdot\alpha)$ è uno spazio vettoriale ⇒ IN $\mathbb{R}^2$:

a)



a_1) ↳ D non è un sottospazio vettoriale AD ESEMPIO PERCHÉ $0 \notin D$!

a_2) ↳ Questo NON È SOTTOSPAZIO VETTORIALE DI $\mathbb{R}^2$ PERCHÉ AD ESEMPIO, la somma esce dal disco!

a_3) SE $w \in W \Rightarrow \alpha w$ DEVE $\in W$, $\forall \alpha \in \mathbb{R}$ ⇒ DA UN PUNTO DI VISTA GEOMETRICO la retta per l'origine r È sottospazio vettoriale, DOVE $r = \langle\langle w \rangle\rangle$!

Il sottospazio vettoriale più piccolo di ogni spazio vettoriale è il sottoinsieme definito DAL SOLO VETTORE NULLO!

(5)

I sottospazi (VETTORIALI) di $\mathbb{R}^2$ sono

- l'origine;
- le rette passanti per l'origine;
- il piano stesso.

IL SOTTOSPAZIO DEFINITO DAL SOLO $\vec{v}=0$ E IL SOTTOSPAZIO DEFINITO DA TUTTO L'INSIEME, SONO DETTI Sottospazi BANALI" E SONO SOTTOSPAZI DI OGNI SPAZIO VETTORIALE

I sottospazi di $\mathbb{R}_3$ sono

- l'origine
- le rette passanti per O
- lo spazio stesso
- i piani passanti per O.

Lo spazio dell'insieme delle soluzioni del sistema omogeneo di p EQUAZIONI ED n VARIABILI è un sottospazio (VETTORIALE) di $\mathbb{R}^n$, in cui n è il numero di variabili. (COME ABBIAMO PRECEDENTEMENTE DIMOSTRATO)

Quando il rango corrisponde ad n, lo spazio delle soluzioni corrisponde all'origine, SOTTOSPAZIO BANALE DI $\mathbb{R}^n$