DEFINIZIONE

Sia A un insieme, e $* \; A \times A \longrightarrow A$ una operazione binaria interna che soddisfa le proprietà:

1) associativa: $\forall \, a_1, a_2, a_3 \in A \quad (a_1 * a_2) * a_3 = a_1 * (a_2 * a_3)$

2) $\exists$ elemento neutro "e": $a * e = e * a = a \quad \forall a \in A$

3) $\forall \, a \in A \; \exists$ il suo inverso b tale che: $a * b = b * a = e$

$\Rightarrow (A, *)$ è un GRUPPO

Se vale anche la proprietà commutativa, il gruppo è detto COMMUTATIVO o ABELIANO

Se consideriamo:

$(\mathbb{N}, +)$ non è un gruppo, $(\mathbb{Z}, +)$ è un gruppo abeliano

$(\mathbb{N}, \cdot)$ non è un gruppo, $(\mathbb{Z}, \cdot)$ non è un gruppo (perché non c'è il reciproco)

$(\mathbb{Q}, +)$ è un gruppo abeliano, $(\mathbb{Q}, \cdot)$ non è un gruppo

non è vero che ogni elemento ha il reciproco, perché lo zero non ha un suo inverso

$(\mathbb{R}, +)$ è un gruppo abeliano,

$(\mathbb{R} - \{0\}, \cdot)$ è un gruppo abeliano

$(\mathbb{Q} - \{0\}, \cdot)$ ← Se lo si esclude allora è un gruppo

---

Se su un insieme A mettiamo due operazioni: $* \; A \times A \longrightarrow A$ e $\square : A \times A \to A$ binarie interne tale che siano soddisfatte le proprietà:

- per "$*$":

1) associativa

2) ∃ elemento neutro

3) ∃ dell'inverso $\forall a \in A$

4) commutativa

Inoltre "$\square$" deve essere associativa e deve avere la proprietà distributiva cioè: $a_1 \square (a_2 * a_3) = (a_1 \square a_2) * (a_1 \square a_3)$

$\forall a_1, a_2, a_3 \in A$

⇒ (DEFINIZIONE) = $(A; *, \square)$ è un ANELLO (struttura più complessa rispetto al gruppo, perché gode di più proprietà)

pertanto:

$(\mathbb{N}; +, \cdot)$ non è un anello, $(\mathbb{Z}; +, \cdot)$ è un anello

$(\mathbb{Q}; +, \cdot)$ è un anello, $(\mathbb{R}; +, \cdot)$ è un anello

Se inoltre ∃ elemento neutro per "$\square$" e ogni elemento di A, diverso dall'elemento neutro di "$*$", ∃ un inverso per "$\square$", allora la struttura $(A; *, \square)$ è detta CORPO

Se infine "$\square$" gode della proprietà commutativa, $(A; *, \square)$ è un CAMPO (struttura più complessa delle altre)

Facciamo un esempio:

$(\mathbb{R}; +, \cdot)$ è un gruppo, è un anello, è un corpo, è un campo

poiché valgono tutte le proprietà descritte prima

anche $(\mathbb{Q}, +, \cdot)$ è un campo e $(\mathbb{C}, +, \cdot)$

Una relazione di equivalenza R tra elementi di un insieme A è una applicazione $A \times A \to A$ che soddisfa le proprietà:

$$(a_1, a_2) \longrightarrow a_1 R a_2$$

1) riflessiva : $a R a \quad \forall a \in A$
2) simmetrica : se $a_1 R a_2 \Rightarrow a_2 R a_1 \quad \forall a_1, a_2 \in A$
3) transitiva : se $a_1 R a_2$ e $a_2 R a_3 \Rightarrow a_1 R a_3 \quad \forall a_1, a_2, a_3 \in A$

Esempio: uguaglianza fra numeri reali: $a_1 R a_2 \Leftrightarrow a_1 = a_2$

è riflessiva? $= \quad a = a \quad \forall a \in \mathbb{R}$: VERA

è simmetrica? se $a_1 = a_2 \Rightarrow a_2 = a_1$ VERA $\forall a_1, a_2 \in \mathbb{R}$

è transitiva? se $a_1 = a_2$ e $a_2 = a_3 \Rightarrow a_1 = a_3 \quad \forall a_1, a_2, a_3 \in \mathbb{R}$

soddisfatte le proprietà $\Rightarrow$ l'uguaglianza è una relazione di equivalenza

ESEMPIO:

- $r \parallel r$ vera
- se $r \parallel s \Rightarrow s \parallel r$ vera
- se $r \parallel s$ e $s \parallel t \Rightarrow r \parallel t$ (stessa direzione)

$\Leftarrow$ relazione di parallelismo tra rette del piano è una relazione di equivalenza

Invece la relazione di $\leq$ non è relazione di equivalenza (non è simmetrica) ma è un'altra relazione: UNA RELAZIONE D'ORDINE

ESEMPIO DI RELAZIONE DI EQUIVALENZA:

In $\mathbb{Z}$ diamo la relazione $m R n \Leftrightarrow m - n = 2k, \ \forall k \in \mathbb{Z}$. (FRA NUMERI INTERI m ED n)

è una relazione di equivalenza?

1) riflessiva? $= \quad m R m \quad \forall m \in \mathbb{Z} \quad m - m = 0 \overset{\text{PER}}{=} k = 0$ VERA
2) simmetrica? $=$ so che $m R n$ cioè $m - n = 2k$
   $n R m$? cioè $n - m = 2h$ PER QUALCHE h IN $\mathbb{Z}$?

VEDIAMO: $(n - m) = -(m - n) = -2k = 2(-k)$

$\Rightarrow$ basta prendere $h = -k$! VERA

3) Transitiva? = se $m \mathcal{R} n$ e $n \mathcal{R} p \Rightarrow m \mathcal{R} p$ dimostro così:

$\exists k \in \mathbb{Z} / \; m - n = 2k$ e $\exists h \in \mathbb{Z} / n - p = 2h \Rightarrow$ ~~$\exists$~~ $\exists r \in \mathbb{Z} / m - p = 2r$?

$$m - p = \underbrace{m - n}_{2k} + \underbrace{n - p}_{2h} = 2(k+h) \Rightarrow r = k + h$$

VEDI ⊛ A PAGINA 3

~~[illegible]~~ Riferendosi alla relazione precedente $*$: FORMO LE CLASSI DI EQUIVALENZA! = CIOÈ SOTTOINSIEMI DELL'INSIEME FORMATI DA ELEMENTI TUTTI EQUIVALENTI FRA LORO!

"Scatole" 1) CLASSE DI 1 (CHE È ANCHE LA CLASSE DI 3, DI 5, DI 7, ...) $= \{1, 3, 5, 7, \dots, -1, -3, -5, -7 \dots\}$ dispari

(Scatole 2) CLASSE DI 0 $= \{0, 2, 4, 6, \dots, -2, -4, -6, -8 \dots\}$ pari

INDICO CON $[0]$ o $\bar{0}$: classe di 0 (CHE È ANCHE LA CLASSE DI 2, DI 4, DI 6..)

Prendo 1 come rappresentante $\Rightarrow [1]$ o $\bar{1}$ = classe di 1

Insieme nuovo è formato da due soli elementi: LE DUE CLASSI DI EQUIVALENZA!

IN QUESTO CASO

insieme quoziente (detto) e si indica come $\mathbb{Z}/\mathcal{R} = \{[0], [1]\}$; $\mathbb{Z}_2 = \mathbb{Z}/\mathcal{R}$

Perché usati i multipli di 2

Posso dare due operazioni in $\mathbb{Z}_2$: + e $\cdot$

"+": SOMMO UN RAPPRESENTANTE DI OGNI CLASSE E PRENDO COME SOMMA LA CLASSE DI EQUIVALENZA DELLA SOMMA DEI RAPPRESENTANTI!

$\bar{0} + \bar{0} = \bar{0}$: è la classe di 0

$\bar{0} + \bar{1} = \bar{1}$: " di 1

$\bar{1} + \bar{0} = \bar{1}$: " di 1

$\bar{1} + \bar{1} = \bar{0}$: è la classe di 0 CHE COINCIDE CON LA CLASSE DI 2 $(1+1=2!)$

~~[illegible]~~

Questa operazione di somma è associativa?

Se faccio $(0+0)+1 = 0+(0+1)$ è vero per tutti

$0 + 1 = 0 + 1$

$1 = 1$

esiste l'elemento neutro? Si

esiste l'opposto? Si
di ZERO è ZERO!
e di uno? Sì $(1+1)=0$ ed è così per tutti $\Rightarrow$ L'OPPOSTO DI $\bar{1}$ È $\bar{1}$

è commutativa? Si

$\Rightarrow$ è un gruppo abeliano per la somma : LE OPERAZIONI IN GRUPPI FINITI SI RAPPRESENTANO CON TABELLE :

Prodotto ↘ .	0	1
0	0	0
1	0	1

(IL RISULTATO vedere in $\mathbb{Z}$ — la classe dove sta — POI DARE COME RISULTATO IN $\mathbb{Z}_2$)

risultati

per il prodotto: è associativa, $\exists$ elemento neutro (1), $\exists$ l'inverso ....
tutte proprietà verificate $\Rightarrow$ $\mathbb{Z}_2$ è UN CAMPO finito
L'campo degli interi modulo due"

($\mathbb{Z}_3$ è campo; ma $\mathbb{Z}_4$ no)

Tutti gli $\mathbb{Z}_n$ con n numeri primi sono campi, gli altri no

---

⊛

DATA UNA RELAZIONE DI EQUIVALENZA $\mathcal{R}$ SU UN INSIEME A, POSSIAMO FORMARE DEI SOTTOINSIEMI DI A, COSTITUITI DA ELEMENTI TUTTI EQUIVALENTI FRA LORO: TALI SOTTOINSIEMI SI CHIAMANO CLASSI DI EQUIVALENZA; OGNI CLASSE DI EQUIVALENZA PRENDE IL NOME DA UNO QUALUNQUE DEGLI ELEMENTI CHE SONO IN ESSA: AD ESEMPIO, SE C'È L'ELEMENTO a_0, SI CHIAMERÀ CLASSE DI EQUIVALENZA DI a_0 E SI INDICA CON $[a_0]$ OPPURE $\bar{a}_0$.
L'INSIEME DI TUTTE LE CLASSI DI EQUIVALENZA SI CHIAMA INSIEME QUOZIENTE. SE IN A ABBIAMO UN'OPERAZIONE, AD ESEMPIO, "$*$", POSSIAMO DARE UN'OPERAZIONE ANCHE NELL'INSIEME QUOZIENTE "$\square$", IN QUESTO MODO: $[a_1] \square [a_2] = [a_1 * a_2] \quad \forall\, a_1, a_2 \in A$
COSÌ TRASFORMIAMO ANCHE L'INSIEME QUOZIENTE, CHE SI INDICA CON $A/\mathcal{R}$, IN UNA STRUTTURA ALGEBRICA!