DEFINIZIONI

Si dirà operazione su di un insieme A una qualsiasi funzione "$*$" che sia definita da $A \times A$ in A. $\quad * : A \times A \to A$
La coppia $(A, *)$ si dirà struttura algebrica.

Es. $(\mathbb{N}, +)$ è una struttura algebrica.
$(\mathbb{N}, -)$ NON è una struttura algebrica. $5 - 10$ non ha senso in $\mathbb{N}$
$(\mathbb{Q}^*, \div)$ è una struttura algebrica, perché ho escluso lo zero $(\mathbb{Q}^* = \mathbb{Q} - \{0\})$.

DEFINIZIONE

Una struttura algebrica del tipo $(A, *)$ si dirà gruppo se verifica le seguenti proprietà:

① L'operazione $*$ è ASSOCIATIVA: $\forall a, b, c \in A \quad a * (b * c) = b * (a * c)$
② Esiste l'ELEMENTO NEUTRO rispetto a $*$: $\forall a \in A \ \exists u_a \in A \ / \ a * u_a = a$ (e viceversa per la proprietà precedente)
③ Esiste l'INVERSO rispetto a $*$: $\forall a \in A \ \exists \bar{a} \in A \ / \ a * \bar{a} = u_a$ (cioè all'elemento neutro per $*$) (e viceversa ☆)

Se poi verifica anche la COMMUTATIVITÀ, cioè $\forall a, b \in A \quad a * b = b * a$ diremo che $(A, *)$ è un gruppo commutativo (o abeliano)

Es. $(\mathbb{R}, +)$ è un gruppo commutativo
$(\mathbb{N}, +)$ NON è un gruppo. Manca l'inverso rispetto alla somma in $\mathbb{N}$.
$(\mathbb{Z}, +)$ è un gruppo commutativo.

DEFINIZIONE

Una struttura algebrica $(A, \oplus, \otimes)$ si dirà anello se verifica le seguenti proprietà:

① $(A, \oplus)$ è un GRUPPO ABELIANO.
② In A esiste l'ELEMENTO NEUTRO rispetto a $\otimes$.
③ L'operazione $\otimes$ è ASSOCIATIVA.
④ L'operazione $\otimes$ è DISTRIBUTIVA rispetto a $\oplus$: $\forall a, b, c \in A \quad a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Se poi vale anche la COMMUTATIVITÀ rispetto a $\otimes$, $(A, \oplus, \otimes)$ si dirà anello commutativo.
Se poi esiste l'INVERSO rispetto a $\otimes$, cioè se $(A, \oplus)$ e $(A, \otimes)$ sono due gruppi abeliani e vale anche la distributiva rispetto a $\oplus$, allora parliamo di campo.

Es. $(\mathbb{R}, +, \times)$ è un campo
$(M^{n \times n}, +, \cdot)$ è un anello NON commutativo.
$(M^{n \times n}(n \geq 2 = 0), +, \cdot)$ è un anello NON commutativo e NON unitario, ovvero $\nexists \lambda \in \mathbb{R} : \lambda \cdot M^{n,n} = M^{n,n}$

*Un anello in cui esistono divisori dello zero NON può essere un campo. Se non vi esistono esso è detto dominio di integrità.

DIMOSTRAZIONE

Supponiamo $ab=0$, con $a, b \neq 0$. Allora: $\bar{a}^{-1}(ab) = \bar{a}^{-1}\cdot 0 \to (\bar{a}^{-1}a)b = \bar{a}^{-1}\cdot 0 \to 1\cdot b = \bar{a}^{-1}\cdot 0 \to b=0$, che va contro le ipotesi iniziali.

Le classi di resto (indicate con $\mathbb{Z}_n$) sono degli insiemi formati dal resto di un $c \in \mathbb{R}$ con n.

Es. $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

Infatti ogni $c \in \mathbb{R}/4$ da come resto 0 oppure 1 V 2 V 3.

La terna $(\mathbb{Z}_n, +, \cdot)$, dove $+, \cdot$ sono rispettivamente le usuali operazioni di somma e prodotto è un anello.

Se e solo se n è un numero primo allora $(\mathbb{Z}_n, +, \cdot)$ è un campo. Se infatti $n \neq$ numero primo, esisteranno un $a, b \in \mathbb{R}$, tali che $a<n$, $b<n$, $ab=n$. che diventa $0=ab$

ESEMPIO

$(\mathbb{Z}_6, +, \cdot)$ $\quad \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$a = 14$

$b = 15$

$14 \cdot 15 = 210$

Ma $14 \% 6 = 2$, $15 \% 6 = 3$, $210 \% 6 = 0$

Quindi $[2] \cdot [3] = [0]$

$(\mathbb{Z}_3, +, \cdot)$ $\quad \mathbb{Z}_3 = \{0, 1, 2\}$

$[2] \cdot [1] \neq [0]$