GRUPPI, CORPI, CAMPI

Struttura algebrica

Definizione
Sia G un insieme non vuoto totalmente ordinato. Indichiamo con $\perp$ una legge di composizione fra gli elementi di G. Se accade che il composto fra due elementi di G è ancora un elemento di G allora la $\perp$ dicesi legge di composizione *interna* a G. La coppia ordinata (G, $\perp$) dicesi ***struttura algebrica***.

In simboli: $\forall\, x, y \in G: x \perp y \in G$.

Esempio: Nell'insieme dei numeri naturali $\mathbb{N}$ la + è legge di composizione interna. Infatti, considerati due numeri a piacere a e b di $\mathbb{N}$ si ha a+b=c che appartiene ad $\mathbb{N}$.

Elemento neutro

Definizione
Una struttura algebrica (G, $\perp$) è dotata di elemento neutro se esiste un elemento $e \in G$ tale che

$$\forall\, x \in G: x \perp e = e \perp x = x$$

Elemento inverso

Definizione
Data una struttura algebrica (G, $\perp$) dotata di elemento neutro *e,* un elemento $x \in G$ è invertibile quando esiste un elemento $x' \in G$ tale che

$$x \perp x' = x' \perp x = e$$

L'elemento x' è detto **inverso** o **reciproco** di x.

Proprietà associativa

Definizione
Una struttura (G, $\perp$) si dice **associativa**, o che l'operazione $\perp$ gode della **proprietà associativa**, quando

$$\forall\, x, y, z \in G: x \perp (y \perp z) = (x \perp y) \perp z.$$

Proprietà commutativa

Definizione
Una struttura (G, $\perp$) si dice **commutativa**, o che l'operazione $\perp$ gode della **proprietà commutativa**, quando

$$\forall\, x, y \in G: x \perp y = y \perp x$$

GRUPPO

Definizione
Una struttura (G, $\perp$) si dice che è un **gruppo** quando valgono le seguenti proprietà:

1. La $\perp$ è associativa;
2. Ha elemento neutro;
3. Esiste l'inverso.

Gruppo commutativo

Definizione
Se poi la $\perp$ è anche commutativa allora il **gruppo** si dice **commutativo** o **abeliano.**

CORPO

Definizione
Un **corpo** è un insieme G, dotato di due operazioni binarie interne $+$ e $*$, dette *somma* e *prodotto*, per le quali valgono le seguenti proprietà:

A) (G, +) è un gruppo abeliano con elemento neutro 0:

1. $x + (y + z) = (x + y) + z$ (associativa)
2. $x + y = y + x$ (commutativa)
3. $x + 0 = 0 + x = x$ (0 elemento neutro)
4. $\forall\, x \in G\ \exists\, x' \in G \text{ tale che } x + x' = x' + x = 0$,

l'elemento x' viene indicato con $-x$, che si dice opposto di x, per cui $x + (-x) = (-x) + x = 0$.

B) (G, *) è un gruppo con elemento neutro 1:

1. $x * (y * z) = (x * y) * z$ (associativa)
2. $1 * x = x * 1 = x$ (1 è elemento neutro)
3. $\forall\, x \in G\ \exists\, x' \in G \text{ tale che } x * x' = x' * x = 1$,

l'elemento x' viene indicato con $x^{-1} = \frac{1}{x}$, che si dice inverso di x, per cui $x * \frac{1}{x} = 1$.

La moltiplicazione è distributiva rispetto alla somma:
$\forall\, x, y, z \in G$:

1. $x * (y + z) = (x * y) + (x * z)$ (distributiva a sinistra)
2. $(y + z) * x = (y * x) + (z * x)$ (distributiva a destra)

CAMPO

Definizione
Un corpo la cui seconda operazione, la $*$, è anche commutativa si dice **campo.**