GRUPPI, CORPI, CAMPI

Si dice **gruppo commutativo** un insieme I cui sia associata una applicazione σ che ad ogni coppia ordinata di elementi associ un elemento di $I = x \sigma y$ e che soddisfi le seguenti condizioni

1) $x \sigma y = y \sigma x$ — proprietà commutativa
2) $x \sigma (y \sigma z) = (x \sigma y) \sigma z$ — proprietà associativa
3) $\exists\, e \in I : \forall x \in I,\ x \sigma e = e \sigma x = x$ — esistenza dell'elemento neutro rispetto a σ
4) $\forall x \in I\ \exists x' : x \sigma x' = x' \sigma x = e$ — esistenza dell'elemento inverso o opposto

L'insieme dei numeri interi $\mathbb{Z}$ (o dei numeri razionali $\mathbb{Q}$) costituisce un gruppo commutativo o abeliano rispetto all'addizione con $e = 0$ e $x' = -x$.

L'insieme dei numeri razionali $\mathbb{Q} - \{0\}$ non nulli costituisce un gruppo commutativo o abeliano rispetto alla moltiplicazione.

Si dice che l'insieme I è un **corpo commutativo** o anche un **campo** se date due applicazioni σ e π che ad ogni coppia ordinata x, y di I associno due elementi di I che indichiamo rispettivamente con:

$$x \sigma y = x + y$$
$$x \pi y = x \cdot y$$

tali da soddisfare le seguenti condizioni:

A) I sia un gruppo abeliano rispetto all'applicazione σ

B) l'insieme $I - \{0\}$ dove 0 è l'elemento neutro dell'applicazione σ sia un gruppo abeliano rispetto a π

C) le due applicazioni siano legate dalla seguente proprietà che si dice distributiva di $\cdot$ rispetto a $+$:

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

Abbiamo così che l'insieme dei numeri razionali $\mathbb{Q}$ è un campo rispetto alle operazioni di addizione e moltiplicazione.