Definizione 5.2. [1ZF] *(Svolto il 2022-11-15) Un* ***gruppo*** *è un insieme G munito di una operazione binaria $*$, che ad ogni coppia $a, b \in G$ associa un elemento $a * b \in G$, rispettando le seguenti proprietà*

1. *proprietà associativa: dati $a, b, c \in G$ vale $(a * b) * c = a * (b * c)$.*
2. *esistenza dell'elemento neutro: un elemento indicato con e tale che $a * e = e * a = a$.*
3. *Esistenza dell'inverso: ad ogni elemento $a \in G$ è associato un elemento* ***inverso*** *a', tale che $a * a' = a' * a = e$. L'inverso dell'elemento a è spesso indicato con a^{-1} (o $-a$ se il gruppo è commutativo).* [a]

Un gruppo si dice ***commutativo*** *(o abeliano) se vale anche $a * b = b * a$ per ogni coppia $a, b \in G$.*

[a] La notazione a^{-1} è giustificato dal fatto che l'elemento inverso è unico: *cf* [1ZP].