Gruppi e campi

Stefano Capparelli

November 26, 2012

Abstract

Diamo alcuni esempi di gruppi e campi

1 Gruppi e campi

La nozione di gruppo rappresenta il tentativo dei matematici di formalizzare e studiare la nozione di simmetria. Il concetto di simmetria è importante sia nella matematica che nelle scienze e nelle arti. Nella fisica ad esempio le leggi di conservazione sono legate a delle simmetrie delle leggi fisiche. È quindi comprensibile l'importanza attribuita al concetto di gruppo.

Prendiamo ad esempio un triangolo equilatero ABC: un oggetto di cui possiamo senz'altro dire che sia dotato di "simmetria". Per essere più concreti le simmetrie del triangolo equilatero sono 6: l'identità I, la simmetria S_A rispetto all'asse passante pr A, e analogamente S_B e S_C e infine le rotazioni di 120 e di 240 gradi. Usando la nozione di composizione di esse (cioè fare una simmetria seguita da un'altra) si definisce un'operazione su questo insieme e si può verificare che esso è un gruppo, denotato D_3. Esso risulta "isomorfo" al gruppo S_3 delle permutazioni su tre oggetti. In modo analogo si potrebbe definire D_4 come il gruppo delle simmetrie di un quadrato. Esso ha 8 oggetti e pertanto non è isomorfo al gruppo S_4 che ha $4! = 24$ elementi. La circonferenza ha infinite simmetrie: le rotazioni formano un gruppo che può essere identificato con il gruppo $SO(2, \mathbb{R})$ (gruppo speciale ortogonale) di tutte le matrici (ortogonali di determinante 1) oppure $O(2, \mathbb{R})$ di tutte le matrici ortogonali di ordine 2 (le isometrie).

Il gruppo di tutte le matrici invertibili di ordine n si indica con $GL(n, \mathbb{R})$ (gruppo lineare generale).

Un altro tipo di gruppi è quello dei gruppi delle classi resto modulo n. Nell'insieme degli interi relativi $\mathbb{Z}$ introduciamo una relazione di equivalenza dicendo che $a \equiv b$(modulo n) se $a - b = kn$ per qualche intero k. Ad esempio $7 \equiv 19 \bmod 12$, $8 \equiv 26 \bmod 2$ etc.

Per un fissato n, indichiamo con $\mathbb{Z}_n$ l'insieme delle classi di equivalenza di $\mathbb{Z}$ rispetto a questa relazione di equivalenza che chiameremo relazione di congruenza.

Si può verificare che $\mathbb{Z}_n$ è un gruppo rispetto alla somma definita da $[a]+[b] = [a + b]$.

Si può inoltre verificare che è anche possibile definire una moltiplicazione in maniera analoga $[a] \cdot [b] = [ab]$. Tuttavia, rispetto alla moltiplicazione così definita in generale Z_n non è un gruppo. Se però, $n = p$ è un numero primo allora $\mathbb{Z}_p^{\times} = \mathbb{Z}_p - \{[0]\}$ con la moltiplicazione è anch'esso un gruppo abeliano

(cioè commutativo). In tal caso parleremo allora di **campo**. In altre parole, un campo è un insieme K dotato di due operazioni, indichiamole con $+, \cdot$, ripetto alle quali $K, +$ è un gruppo abeliano, $K^\times, \cdot$ è un gruppo abeliano e le due operazioni sono legate dalla distributività: $a \cdot (b + c) = a \cdot b + a \cdot c$ per ogni $a, b, c \in K$.

Esempi di campi sono: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \mathbb{Z}_{11}, ...$ Non sono campi invece, ad esempio: $\mathbb{Z}, \mathbb{Z}_4, \mathbb{Z}_9$.