

# Il gruppo delle permutazioni

di Gabriel Antonio Videtta

**Nota.** Nel corso del documento con  $X_n$  si indicherà l'insieme  $\{1, \dots, n\}$  e con  $G$  un qualsiasi gruppo.

Si definisce brevemente il gruppo delle permutazioni  $S_n$  come il gruppo delle bigezioni su  $G$ , ossia  $S(X_n)$ . Si deduce facilmente che  $|S_n| = n!$  dal momento che vi sono esattamente  $n!$  scelte possibili per costruire una bigezione da  $X_n$  in  $X_n$  stesso.

Come è noto, ogni  $\sigma \in S_n$  può scriversi come prodotto di cicli disgiunti. Di seguito si introduce un modo formale per descrivere questi cicli.

Si consideri l'azione di  $\langle \sigma \rangle$  su  $X_n$  univocamente determinata da  $\sigma \cdot x = \sigma(x)$ . Allora i cicli di  $\sigma$  sono esattamente le orbite di  $\sigma$  ordinate nel seguente modo:

$$\text{Orb}(x) = \{x, \sigma(x), \dots, \sigma^m(x)\}.$$

Si osserva che in effetti tutti gli elementi di  $X$  sono considerati nella scrittura delle orbite dal momento che tali orbite inducono una partizione di  $X$  (infatti sono classi di equivalenza). Si definisce inoltre una permutazione *ciclo* se esiste al più un'unica orbita di cardinalità diversa da 1 e si dice *lunghezza del ciclo* la cardinalità di tale orbita (o se non esiste, si dice che ha lunghezza unitaria). Due cicli si dicono disgiunti se almeno uno dei due è l'identità o se le loro uniche orbite non banali hanno intersezione nulla (e in entrambi i casi, commutano). Per ogni  $k$ -ciclo esistono esattamente  $k$  scritture distinte (in funzione dell'elemento iniziale del ciclo).

Pertanto si deduce facilmente che ogni permutazione  $\sigma$  è prodotto di cicli disgiunti in modo unico (a meno della scelta del primo elemento dell'orbita). Poiché allora ogni  $n$ -ciclo è generato dalla composizione di  $n - 1$  trasposizioni (2-cicli) e ogni permutazione è prodotto di cicli,  $S_n$  è generato dalle trasposizioni. Infatti:

$$(a_1, \dots, a_i) = (a_1, a_i) \circ (a_1, a_{i-1}) \circ \dots \circ (a_1, a_2),$$

o altrimenti:

$$(a_1, \dots, a_i) = (a_1, a_2) \circ (a_2, a_3) \circ \dots \circ (a_{i-1}, a_i),$$

da cui si deduce che la scrittura come prodotto di trasposizioni non è unica. Ciononostante viene sempre mantenuta la parità del numero di trasposizioni impiegate.

Per questo motivo la mappa  $\text{sgn} : S_n \rightarrow \{\pm 1\}$  che vale 1 sulle permutazioni con numero pari di trasposizioni impiegabili e  $-1$  sul resto è ben definita. Inoltre questa mappa è un omomorfismo di gruppi, e si definisce  $\mathcal{A}_n := \text{Ker sgn}$  come il sottogruppo di  $S_n$  delle permutazioni pari, detto anche *gruppo alterno*. La classe laterale  $(1, 2) \mathcal{A}_n$  rappresenta invece le permutazioni dispari.

In particolare, se  $\sigma_k$  è un  $k$ -ciclo,  $\text{sgn}(\sigma_k) = (-1)^{k-1}$  e  $\text{ord}(\sigma_k) = k$ . Si osserva inoltre che vi sono esattamente  $\binom{n}{k} \frac{k!}{k} = \binom{n}{k} (k-1)!$   $k$ -cicli in  $S_n$  e che in generale l'ordine di una permutazione è il minimo comune multiplo degli ordini dei suoi cicli.

Si definisce *tipo* di una permutazione  $\sigma$  la sua decomposizione in cicli disgiunti a meno degli elementi presenti nei cicli. Sia  $\sigma$  tale per cui:

$$\sigma = (a_1, a_2, \dots, a_{k_1})(b_1, \dots, b_{k_2}) \cdots (c_1, \dots, c_{k_i}),$$

allora vale la seguente relazione sul coniugio:

$$\tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \dots, \tau(a_{k_1}))(\tau(b_1), \dots, \tau(b_{k_2})) \cdots (\tau(c_1), \dots, \tau(c_{k_i})).$$

A partire da ciò vale il seguente risultato:

**Proposizione.** Due permutazioni  $\sigma_1, \sigma_2$  sono *coniugabili* (ossia appartengono alla stessa classe di coniugio) se e solo se hanno lo stesso tipo.

*Dimostrazione.* Dalla seguente identità, se  $\sigma_1$  è coniugata rispetto a  $\sigma_2$ , sicuramente le due permutazioni dovranno avere lo stesso tipo. Analogamente, se le due permutazioni hanno lo stesso tipo, si può costruire  $\tau$  che associ ogni elemento di un ciclo di  $\sigma_1$  a un elemento nella stessa posizione in un ciclo di  $\sigma_2$  della stessa lunghezza in modo tale che  $\tau$  rimanga una permutazione di  $S_n$  e che valga  $\sigma_2 = \tau\sigma_1\tau^{-1}$ .  $\square$

Come corollario di questo risultato, se  $m_1$  rappresenta il numero di 1-cicli di  $\sigma$ ,  $m_2$  quello dei suoi 2-cicli, fino a  $m_k$ , vale il seguente risultato:

$$|\text{Cl}(\sigma)| = \frac{n!}{m_1! 1^{m_1} m_2! 2^{m_2} \cdots m_k! k^{m_k}},$$

e in particolare esistono tante classi di coniugio quante partizioni di  $n$ .

Si osserva infine che se  $\tau_1\sigma\tau_1^{-1} = \tau_2\sigma\tau_2^{-1} = \rho$ , allora:

$$\tau_1^{-1}(\tau_2\sigma\tau_2^{-1})\tau_1 = \tau_1^{-1}\rho\tau_1 = \sigma,$$

per cui  $\tau_1^{-1}\tau_2 \in Z_{S_n}(\sigma)$  dacché  $(\tau_1^{-1}\tau_2)\sigma = \sigma(\tau_1^{-1}\tau_2)$ . Allora  $\tau_1 \in \tau_2 Z_{S_n}(\sigma)$ .

Infine, se  $H \leq S_n$ ,  $H$  è normale in  $S_n$  se e solo se per ogni tipo  $H$  contiene tutte le permutazioni di quel tipo o nessuna.