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.

Si definisce l'**azione naturale** di S_n su X_n come l'azione $\varphi : S_n \to S(X_n)$ tale per cui $\sigma \overset{\varphi}{\mapsto} [n \mapsto \sigma(n)]$. In particolare, per $H \leq S_n$, si definisce la sua azione naturale come la restrizione dell'azione naturale di S_n su H. Un sottogruppo H si dice *transitivo* se la sua azione naturale è transitiva. Si osserva che ogni tale azione naturale è fedele (infatti $\sigma \in S_n$ fissa tutto X_n solo se è l'identità di S_n). Si illustra allora subito un risultato sui sottogruppi abeliani transitivi di S_n:

Proposizione. Sia H un sottogruppo abeliano transitivo di S_n. Allora $|H| = n$.

Dimostrazione. Dal Teorema orbita-stabilizzatore, $|H| = |\mathrm{Stab}(i)|\,|\mathrm{Orb}(i)|$. Poiché H è un sottogruppo transitivo, $|\mathrm{Orb}(i)| = n$, e quindi è sufficiente verificare che $\mathrm{Stab}(i)$ sia banale.

Ogni $\mathrm{Stab}(i)$ è coniugato ad ogni altro $\mathrm{Stab}(j)$, sempre per la transitività dell'azione; poiché allora H è abeliano, in particolare $\mathrm{Stab}(i)$ coincide con ogni altro stabilizzatore. Pertanto $\sigma \in \mathrm{Stab}(i)$ se e solo se σ appartiene al nucleo dell'azione naturale di H, ossia a $\cap_{x=1}^{n} \mathrm{Stab}(x)$, e quindi se e solo se $\sigma = e$. Si conclude dunque che $\mathrm{Stab}(i)$ è banale e quindi che $|H| = n$. □

Dimostrazione alternativa. Se H è un sottogruppo transitivo di S_n, allora la sua azione naturale agisce fedelmente e transitivamente su X_n. Poiché però H è anche abeliano, l'azione è anche libera, e dunque ogni stabilizzatore è banale. Pertanto, per il Teorema orbita-stabilizzatore, $|H| = |\mathrm{Stab}(1)|\,|\mathrm{Orb}(1)| = n$. □

Esempio (Il gruppo di Klein V_4)**.** In S_4, e in particolare in A_4, esiste un sottogruppo normale non banale molto particolare[1], il cosiddetto[2] **gruppo di Klein** V_4, dove:

$$V_4 = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

[1] Pertanto A_4 non è semplice.

[2] La lettere V è dovuta al termine *vier*, che in tedesco significa "quattro".

Tale sottogruppo è abeliano e transitivo (e quindi, per il risultato di prima, $|V_4| = 4$, come si osserva facilmente). Poiché ogni suo elemento ha ordine 2 (e in particolare V_4 non è ciclico), V_4 deve necessariamente essere isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Pertanto V_4 è il più piccolo gruppo non ciclico per ordine (a meno di isomorfismo).

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 naturale di $\langle\sigma\rangle$. Allora i cicli di σ sono esattamente le orbite di σ ordinate nel seguente modo:

$$\mathrm{Orb}(x) = \{x, \sigma(x), \ldots, \sigma^m(x)\}.$$

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 σ 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:

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

o altrimenti:

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

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 $\mathrm{sgn} : S_n \to \{\pm 1\}$ 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 $\mathcal{A}_\mathrm{n} := \operatorname{Ker} \mathrm{sgn}$ come il sottogruppo di S_n delle permutazioni pari, detto anche *gruppo alterno*. La classe laterale $(1,2)\,\mathcal{A}_\mathrm{n}$ rappresenta invece le permutazioni dispari.

In particolare, se σ_k è un k-ciclo, $\mathrm{sgn}(\sigma_k) = (-1)^{k-1}$ e $\mathrm{ord}(\sigma_k) = k$. 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. In particolare vale

la seguente identità[3]:

$$\operatorname{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

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

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

allora vale la seguente relazione sul coniugio:

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

A partire da ciò vale il seguente risultato:

Proposizione. Due permutazioni σ_1, σ_2 sono *coniugabili* (ossia appartengono alla stessa classe di coniugio) se e solo se hanno lo stesso tipo.

Dimostrazione. Dalla seguente identità, se σ_1 è coniugata rispetto a σ_2, sicuramente le due permutazioni dovranno avere lo stesso tipo. Analogamente, se le due permutazioni hanno lo stesso tipo, si può costruire τ che associ ogni elemento di un ciclo di σ_1 a un elemento nella stessa posizione in un ciclo di σ_2 della stessa lunghezza in modo tale che τ rimanga una permutazione di S_n e che valga $\sigma_2 = \tau\sigma_1\tau^{-1}$. □

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

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

e in particolare esistono tante classi di coniugio quante partizioni di n. Come conseguenza di questo risultato, per il Teorema orbita-stabilizzatore, vale che:

$$|Z_{S_n}(\sigma)| = m_1!\, 1^{m_1}\, m_2!\, 2^{m_2} \cdots m_k!\, k^{m_k},$$

dove si ricorda[4] che due permutazioni coniugano σ nella stessa permutazione ρ se queste due permutazioni fanno parte della stessa classe in $G/Z_{S_n}(\sigma)$. Infine, sempre come corollario dello stesso risultato, se $H \le S_n$, H è normale in S_n se e solo se per ogni tipo di permutazione H contiene tutte le permutazioni di quel tipo o nessuna.

Per calcolare il centralizzatore di una permutazione $\sigma \in S_n$, la strategia generale si compone di due passi fondamentali: computare il numero di elementi del centralizzatore tramite il Teorema orbita-stabilizzatore (come visto precedentemente) e poi "indovinare" dei sottogruppi con cui σ commuta che, combinati tramite il prodotto di sottogruppi, danno esattamente il numero calcolato inizialmente.

[3] Si verifica facilmente che il prodotto a destra fornisce un omomorfismo. Allora è sufficiente mostrare che è ben definito e che vale -1 sulle trasposizioni. Se si considera $\sigma = (a, b)$, per i e j tali per cui $\{i, j\} \cap \{a, b\} = \varnothing$ il termine della produttoria è unitario; per $\{i, j\} = \{a, b\}$ il termine è -1 e per un'intersezione di un solo termine si osserva che vi sono due termini del prodotto che valgono -1 e che moltiplicati si annullano nell'unità. Poiché sgn vale anch'esso -1 sulle trasposizioni, i due omomorfismi coincidono (infatti le trasposizioni generano S_n).

[4] Infatti $Z_{S_n}(\sigma)$ è lo stabilizzatore di σ nell'azione di coniugio.

Esempio. Sia $\sigma = \overbrace{(1,2,3,4)}^{\sigma_1}\overbrace{(5,6,7)}^{\sigma_2}\overbrace{(8,9)}^{\sigma_3} \in S_9$. Si calcola $Z_{S_9}(\sigma)$. Tramite il Teorema orbita-stabilizzatore, vale che:

$$Z_{S_9}(\sigma) = 1! \cdot 4 \cdot 1! \cdot 3 \cdot 1! \cdot 2 = 4! = 24.$$

Si osserva facilmente che σ commuta con σ_1, σ_2 e σ_3, e quindi $\langle \sigma_i \rangle \leq Z_{S_9}(\sigma)\ \forall\, i \in \{1,2,3\}$. In particolare $\langle \sigma_i \rangle$ commuta sempre con $\langle \sigma_j \rangle$ per $i \neq j$, dal momento che questi cicli sono tutti disgiunti. Si considera[5] il sottogruppo $H = \langle \sigma_1 \rangle \langle \sigma_2 \rangle \langle \sigma_3 \rangle$: ogni suo elemento è esprimibile in modo unico come prodotto di una potenza di σ_1, di σ_2 e di σ_3, e quindi $|H| = |\langle \sigma_1 \rangle|\,|\langle \sigma_2 \rangle|\,|\langle \sigma_3 \rangle| = 4 \cdot 3 \cdot 2 = 24$; poiché allora $H \leq Z_{S_9}(\sigma)$ ha lo stesso numero di elementi del centralizzatore, $Z_{S_9}(\sigma) = H$. Infine, dal momento che $\langle \sigma_i \rangle \cap (\langle \sigma_j \rangle \langle \sigma_k \rangle)$ per ogni i, j, k distinti in $\{1,2,3\}$, $H \cong \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle \times \langle \sigma_3 \rangle$, e dunque:

$$Z_{S_9}(\sigma) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Si osserva adesso che $\mathcal{A}_\mathrm{n}$ può scriversi come il sottogruppo generato dai $2-2$-cicli, infatti ogni permutazione pari è prodotto di un numero pari di trasposizioni, che possono dunque essere ridotte a $2-2$-cicli. Allo stesso tempo allora $\mathcal{A}_\mathrm{n}$ è generato dai 3-cicli se $n \geq 3$. Si consideri infatti $(i,j)(k,l)$. Se $\{i,j\} \cap \{k,l\} = 2$, $(i,j) = (k,l)$, e quindi $(i,j)(k,l) = e$; se $\{i,j\} \cap \{k,l\} = 1$, si può assumere senza perdita di generalità che $k = i$, da cui $(i,j)(i,l) = (i,l,j)$, un 3-ciclo; se invece $\{i,j\} \cap \{k,l\} = 0$, $(i,j)(k,l) = (i,j)(j,k)(j,k)(k,l) = (i,j,k)(j,k,l)$, e quindi $(i,j)(k,l)$ è prodotto di due 3-cicli. Pertanto si è dimostrato che $\mathcal{A}_\mathrm{n} = \langle (i,j)(k,l) \mid i,j,k,l \in X_n \rangle \subseteq \langle (i,j,k) \mid i,j,k \in X_n \rangle$; allo stesso tempo ogni 3-ciclo è una permutazione pari, e quindi vale anche l'inclusione inversa.

Si consideri adesso S_n', il sottogruppo derivato di S_n. Poiché S_n è abeliano per $n \in \{1,2\}$, in tal caso $S_n' = \{e\}$; in tutti gli altri casi S_n' non può essere uguale a $\{e\}$, altrimenti S_n sarebbe abeliano. Si osserva che $[(i,j),(j,k)]$ con i, j e k distinti si scrive come:

$$[(i,j),(j,k)] = (i,j)(j,k)(i,j)^{-1}(j,k)^{-1} = (i,k)(j,k) = (i,k,j),$$

e quindi si deduce che $\langle (i,j,k) \mid |\{i,j,k\}| = 3 \rangle = \mathcal{A}_\mathrm{n}$ è un sottogruppo di S_n'. Inoltre[6] l'omomorfismo sgn ha come codominio un gruppo abeliano isomorfo a $\mathbb{Z}/2\mathbb{Z}$, e quindi $S_n' \subseteq \operatorname{Ker} \operatorname{sgn} = \mathcal{A}_\mathrm{n}$. Si conclude dunque che $S_n' = \mathcal{A}_\mathrm{n}$ e che $S_{n\,ab} = S_n/\mathcal{A}_\mathrm{n} \cong \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ per $n \geq 3$. Pertanto adesso è immediato il seguente risultato:

Proposizione. Sia H un gruppo abeliano. Allora $\mathrm{Hom}(S_n, H) \leftrightarrow \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, H)$.

In particolare, vi sono tanti omomorfismi non banali in $\mathrm{Hom}(S_n, H) \leftrightarrow \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, H)$ quanti elementi di ordine 2 vi sono in H.

[5] Poiché σ_i commuta con σ_j, questo sottogruppo è ben definito.

[6] Alternativamente $[S_n : S_n']$ deve dividere $[S_n : \mathcal{A}_\mathrm{n}] = 2$, e quindi, poiché $S_n \neq S_n'$, è necessario che S_n' sia esattamente $\mathcal{A}_\mathrm{n}$.

Si ricercano adesso le classi di coniugio in $\mathcal{A}_\mathrm{n}$. Si osserva innanzitutto che, se $\sigma \in \mathcal{A}_\mathrm{n}$, $\mathrm{Cl}_{\mathcal{A}_\mathrm{n}}(\sigma) \subseteq \mathrm{Cl}_{S_n}(\sigma)$. Inoltre, per il Teorema orbita-stabilizzatore, vale che:

$$\left|\mathrm{Cl}_{\mathcal{A}_\mathrm{n}}(\sigma)\right|(\sigma) = \frac{|\mathcal{A}_\mathrm{n}|}{|Z_{\mathcal{A}_\mathrm{n}}(\sigma)|} = \frac{|S_n|/2}{|Z_{S_n}(\sigma) \cap \mathcal{A}_\mathrm{n}|}.$$

Poiché[7] $Z_{S_n}(\sigma) \cap \mathcal{A}_\mathrm{n}$ in $Z_{S_n}(\sigma)$ ha indice 1 se $Z_{S_n}(\sigma) \subseteq \mathcal{A}_\mathrm{n}$ e 2 altrimenti, vale che:

- $\left|\mathrm{Cl}_{\mathcal{A}_\mathrm{n}}(\sigma)\right|(\sigma) = \frac{1}{2}\left|\mathrm{Cl}_{S_n}(\sigma)\right|$, se $Z_{S_n}(\sigma) \subseteq \mathcal{A}_\mathrm{n}$,
- $\left|\mathrm{Cl}_{\mathcal{A}_\mathrm{n}}(\sigma)\right|(\sigma) = \left|\mathrm{Cl}_{S_n}(\sigma)\right|$, altrimenti.

[7] È sufficiente osservare che $Z_{S_n}(\sigma) \cap \mathcal{A}_\mathrm{n} = \mathrm{Ker}(\mathrm{sgn}|_{\mathcal{A}_\mathrm{n}})$, e dunque che $Z_{S_n}(\sigma)/(Z_{S_n}(\sigma) \cap \mathcal{A}_\mathrm{n})$ può essere isomorfo tramite il Primo teorema di isomorfismo soltanto a $\{1\}$ o a $\{\pm 1\}$.