Il gruppo diedrale e i suoi sottogruppi

di Gabriel Antonio Videtta

In questo documento si definisce il gruppo diedrale e si illustrano le sue proprietà principali, a partire da come sono costruiti i suoi sottogruppi.

Sia $n \geq 3$. Si definisce **gruppo diedrale**, denotato[1] come D_n, il gruppo delle isometrie del piano $\mathbb{R}^2$ che mappano i vertici di un poligono regolare centrato nell'origine con n lati in sé stessi.

Si verifica facilmente che D_n è un gruppo:

- Ammette un'identità, che coincide con l'identità delle isometrie,
- La composizione di due isometrie che mappano i vertici del poligono in sé stessi è ancora un'isometria che lascia fissi i vertici del poligono,
- Ogni isometria per cui i vertici del poligono rimangono fissi ammette un'inversa con la stessa proprietà[2][3].

In particolare, se $\sigma \in D_n$, σ permuta i vertici del poligono (pertanto si può visualizzare D_n come un sottogruppo naturale di S_n). Denotando con r la rotazione primitiva del gruppo (ossia una rotazione di $\frac{2\pi}{n}$ gradi in senso antiorario) e con s la simmetria rispetto all'asse y, si osserva che ogni elemento della forma sr^k con $k \in \mathbb{Z}$ è ancora una simmetria, benché non per forza rispetto all'asse y[4]. In particolare, per n pari, le riflessioni di D_n sono esattamente le riflessioni rispetto alle rette passanti per i vertici o per i punti medi del poligono.

Dal momento che $\sigma \in D_n$ è in particolare una isometria, e quindi un'applicazione lineare, σ è completamente determinata da $\sigma(V_1)$ e $\sigma(V_2)$, dove V_i sono i vertici del poligono numerati in senso antiorario. In particolare, se $\sigma(V_1) = V_k$, allora $\sigma(V_2)$, affinché venga preservata la distanza, può valere[5] o V_{k-1} o V_{k+1}. Pertanto vi sono al più $2n$ scelte

[1] Alcuni testi denotano il gruppo diedrale come D_{2n}, dal momento che vale $|D_n| = 2n$.

[2] Si ricorda che ogni isometria è invertibile a prescindere.

[3] Dal momento che D_n ha cardinalità $2n$, come mostrato dopo, questa condizione è automaticamente verificata come conseguenza della finitezza di D_n.

[4] La matrice associata di s nella base canonica è $-1E_{11} + E_{22}$, e quindi deve valere $\det(s) = -1$. Al contrario $r \in \mathrm{SO}(2)$, e quindi $\det(r) = 1$. Si conclude pertanto che $\det(sr^k) = \det(s)\det(r)^k = -1$, e dunque che sr^k deve obbligatoriamente appartenere alla classe laterale $s\,\mathrm{SO}(2)$ delle riflessioni.

[5] Per semplicità si pone $V_0 := V_n$ e $V_{n+1} := V_1$.

possibili di $\sigma(V_1)$ e $\sigma(V_2)$ (e quindi $|D_n| \leq 2n$). D'altra parte si osserva che tutti gli elementi 1, r, ..., r^{n-1}, s, sr, ..., sr^{n-1} sono distinti:

- Gli r^k con $0 \leq k \leq \mathrm{ord}(r) - 1$ sono tutti distinti e $\mathrm{ord}(r)$ vale esattamente[6] n,
- Gli sr^k con $0 \leq k \leq n-1$ sono tutti distinti, altrimenti la precedente osservazione sarebbe contraddetta,
- Nessun r^i coincide con un sr^j, dal momento che i loro determinanti sono diversi ($\det(r^i) = 1$, mentre $\det(sr^j) = -1$). In particolare $r^i \in \mathrm{SO}(2)$, mentre $sr^j \in s\,\mathrm{SO}(2)$.

Pertanto $|D_n| \geq 2n$, e quindi $|D_n| = 2n$. Si conclude inoltre che D_n è generato da r e da s, e quindi che $D_n = \langle r, s \rangle$. Esistono dunque due sottogruppi naturali di D_n:

$$\mathcal{R} := \langle r \rangle \cong \mathbb{Z}/n\mathbb{Z}, \quad \langle s \rangle \cong \mathbb{Z}/2\mathbb{Z}.$$

Proposizione. Vale l'identità $srs^{-1} = r^{-1}$.

Dimostrazione. Si sviluppa srs^{-1} in termini matriciali, considerando $s = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ e $r = \left(\begin{smallmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{smallmatrix}\right)$:

$$srs^{-1} = \begin{pmatrix} \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n}) \\ -\sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix},$$

ottenendo la matrice associata a r^{-1} nella base canonica. $\square$

In generale vale dunque che $sr^ks^{-1} = r^{-k}$. Si deduce allora la presentazione del gruppo D_n:

$$D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs^{-1} = r^{-1} \rangle.$$

Si descrivono adesso tutti i sottogruppi di D_n. Innanzitutto, in $\mathcal{R}$ per ogni $d \mid n$ esiste un unico sottogruppo di ordine d dal momento che $\mathcal{R}$ è ciclico. Pertanto ogni tale sottogruppo assume la forma $\langle r^{\frac{n}{d}} \rangle$. Inoltre, dal momento che[7] $[D_n : \mathcal{R}] = 2$, $\mathcal{R}$ è un sottogruppo normale di D_n. Allora, poiché $\mathcal{R}$ è normale in D_n e ogni sottogruppo $H \leq \mathcal{R}$ è caratteristico[8] in D_n, ogni sottogruppo di $\mathcal{R}$ è normale anche in D_n.

Sia ora H un sottogruppo di D_n con $H \not\subseteq \mathcal{R}$. Si consideri la proiezione al quoziente mediante $\mathcal{R}$, ossia $\pi_{\mathcal{R}} : D_n \to D_n/\mathcal{R}$. Chiaramente deve valere che $\pi_{\mathcal{R}}(H) = D_n/\mathcal{R}$: l'unica altra possibilità è che $\pi_{\mathcal{R}}(H)$ sia $\{\mathcal{R}\}$, e quindi che $H \subseteq \operatorname{Ker} \pi_{\mathcal{R}} = \mathcal{R}$, $\lightning$.

[6] Infatti r è rappresentato in $\mathrm{SO}(2)$ dalla matrice $\left(\begin{smallmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{smallmatrix}\right)$, che ha ordine esattamente n.

[7] Infatti ogni elemento di D_n, come visto prima, è della forma r^k o sr^k.

[8] Per ogni ordine di $\mathcal{R}$ esiste un unico sottogruppo $H \leq \mathcal{R}$, e quindi tale sottogruppo deve essere caratteristico.

Si consideri adesso la restrizione di $\pi_{\mathcal{R}}$ ad H, $\pi_{\mathcal{R}}|_H : H \to D_n/\mathcal{R}$. Vale in particolare che $\operatorname{Ker} \pi_{\mathcal{R}}|_H = H \cap \operatorname{Ker} \pi_{\mathcal{R}} = H \cap \mathcal{R}$ e che $\operatorname{Im} \pi_{\mathcal{R}}|_H = D_n/\mathcal{R}$ (da prima vale infatti che $\pi_{\mathcal{R}}(H) = D_n/\mathcal{R}$). Allora, per il Primo teorema di isomorfismo, vale che:

$$\frac{H}{H \cap \mathcal{R}} \cong D_n/\mathcal{R},$$

da cui si deduce che $|H| = 2\,|H \cap \mathcal{R}|$. In particolare $H \cap \mathcal{R}$ è un sottogruppo di $\mathcal{R}$, e quindi esiste $d \mid n$ tale per cui $H \cap \mathcal{R} = \langle r^d \rangle$, con $|H \cap \mathcal{R}| = \frac{n}{d}$.

Sia ora sr^k una simmetria di H. Innanzitutto si osserva che $\langle r^d \rangle$ è normale in D_n e quindi $\langle r^d \rangle \langle sr^k \rangle$ è effettivamente un sottogruppo di D_n. Dal momento che[9] $\langle r^d \rangle \cap \langle sr^k \rangle = \{e\}$, allora $\left|\langle r^d \rangle \langle sr^k \rangle\right| = \left|\langle r^d \rangle\right| \left|\langle sr^k \rangle\right| = \frac{2n}{d}$. Anche $|H| = \frac{2n}{d}$ e quindi, per questioni di cardinalità, $H = \langle r^d \rangle \langle sr^k \rangle = \langle r^d, sr^k \rangle$.

In conclusione, ogni sottogruppo di D_n è della forma $\langle r^d \rangle$ o della forma $\langle r^d, sr^k \rangle$. Si mostra adesso che per $0 \leq k < d < n$ e $d \mid n$ la classificazione è unica e completa. Chiaramente è completa, dal momento che d si può sempre ridurre in modulo n e che per $k > d$ si può moltiplicare sr^k per riottenere una riflessione con esponente minore di d.

Si verifica adesso che è vi è un solo modo di esprimere un sottogruppo in queste condizioni. Se $H_1 := \langle r^{d_1}, sr^{k_1} \rangle = \langle r^{d_1}, sr^{k_1} \rangle =: H_2$, allora in particolare $H_1 \cap \mathcal{R} = \langle r^{d_1} \rangle = \langle r^{d_2} \rangle = H_2 \cap \mathcal{R}$, da cui si deduce facilmente che $d_1 = d_2$. Sia ora $sr^{k_1} r^{td_1} = sr^{k_2} r^{t'd_2}$ con t, $t' \in \mathbb{Z}$. Allora deve valere che:

$$r^{k_1 + td_1} = r^{k_2 + t'd_2} \iff k_1 + td_1 \equiv k_2 + t'd_2 \quad (n),$$

e quindi, se $d := d_1 = d_2$, questo implica che:

$$k_1 \equiv k_2 \quad (d) \implies k_1 = k_2 \impliedby 0 \leq k_1, k_2 < d.$$

Pertanto esistono esattamente[10] $d(n) + \sigma(n)$ sottogruppi di D_n.

Si studiano adesso i sottogruppi normali di D_n. Come già visto, i sottogruppi di $\mathcal{R}$ sono tutti normali in D_n. Si studiano dunque soltanto i gruppi della forma $\langle r^d, sr^h \rangle$. Si ricorda che il sottogruppo $H = \langle r^d, sr^h \rangle$ è normale se e solo se $N_G(H) = G$, ossia se il suo normalizzatore è tutto G. In particolare questo è vero se i generatori di G appartengono a $N_G(H) = G$ e quindi se $rHr^{-1} = H$ e se $sHs^{-1} = H$. In particolare[11] si deve studiare quando valgono le seguenti identità:

$$\langle r^d, sr^h \rangle = \underbrace{\langle r^d, sr^{h-2} \rangle}_{rHr^{-1}}, \qquad \langle r^d, sr^h \rangle = \underbrace{\langle r^{-d}, r^h s^{-1} \rangle}_{sHs^{-1}} = \langle r^d, sr^{-h} \rangle.$$

[9] Infatti l'unica rotazione che è anche una simmetria è l'identità.

[10] La scrittura $d(n)$ indica il numero di divisori di n, mentre $\sigma(n)$ indica la somma dei divisori di n. Infatti per ogni divisore d di n si conta un sottogruppo ciclico $\langle r^d \rangle$ e un sottogruppo della forma $\langle r^d, sr^h \rangle$ con $0 \leq h < d$ (e quindi d sottogruppi di questo tipo).

[11] Si è utilizzata la relazione $g\langle g_1, \ldots, g_i \rangle g^{-1} = \langle gg_1g^{-1}, \ldots, gg_ig^{-1} \rangle$.

La prima identità è vera se e solo se $h \equiv h-2 \ (d)$, e quindi se e solo se $d \mid 2$. Pertanto d può valere solo 1 o 2: se $d=1$, H è esattamente $\langle r, s \rangle = D_n$; se invece $d=2$, H può essere soltanto $\langle r^2, s \rangle$ o $\langle r^2, sr \rangle$. Ciononostante, nel caso $d=2$, dal momento che $d \mid n$, n deve essere pari (e quindi se n è dispari, D_n non ammette sottogruppi normali non banali, ed è in particolare semplice).

Si consideri dunque n pari. È sufficiente controllare che per $d=2$ valga anche la seconda identità, ossia che valga $h \equiv -h \ (2)$, sempre verificata. Si conclude dunque con la seguente classificazione:

- se n è dispari, D_n ammette come sottogruppi normali soltanto D_n, $\{e\}$ e i sottogruppi di $\mathcal{R}$,
- se n è pari, D_n ammette come sottogruppi normali tutti quelli del caso dispari insieme a $\langle r^2, s \rangle$ e $\langle r^2, sr \rangle$.

Si illustrano adesso le classi di coniugio più importanti in D_n. Si consideri per esempio $\mathrm{Cl}(r)$. Dal momento che $D_n \supseteq Z_{D_n}(r) \subseteq \mathcal{R}$ e che $[D_n : \mathcal{R}] = 2$, allora $Z_{D_n}(r)$ può essere o tutto D_n o soltanto $\mathcal{R}$. Infatti, poiché $\mathcal{R} \leq Z_{D_n}(r)$, $n \mid Z_{D_n}(r)$, e quindi:

$$2 = |D_n/\mathcal{R}| = |D_n/Z_{D_n}(r)| \, |Z_{D_n}/\mathcal{R}| \,,$$

da cui si ricava che un fattore tra $|D_n/Z_{D_n}(r)|$ e $|Z_{D_n}/\mathcal{R}|$ deve valere 1. Se $Z_{D_n}(r)$ fosse uguale a D_n, allora r apparterrebbe a $Z(D_n)$, e quindi deve valere la seguente identità:

$$sr = rs \implies r^{-1} = r,$$

mai verificata in D_n (per $n \geq 3$), $\lightning$. Quindi $Z_{D_n}(r) = \mathcal{R}$, e allora, per il Teorema orbita-stabilizzatore, $|\mathrm{Cl}(r)| = |D_n| / |\mathcal{R}| = 2$. In particolare sia r che $srs^{-1} = r^{-1}$ sono distinti, e quindi:

$$\mathrm{Cl}(r) = \{r, r^{-1}\}.$$