UNITELMA SAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA
DIPARTIMENTO DI INFORMATICA

Algebra

Alessandro D'Andrea

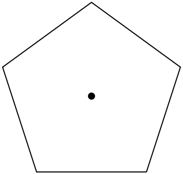
7. Gruppi ciclici, diedrali, simmetrici e alterni

Richiami

- Piccolo teorema di Fermat; teorema di Eulero
- Il teorema di Lagrange per i gruppi ha applicazioni alle congruenze
- Esempi di gruppi: $(A, +), (A^{\times}, \cdot)$, dove A è un anello
- Oggi: **Altri esempi (geometrici, combinatori) di gruppi**
  - Gruppi ciclici e diedrali
  - Gruppi simmetrici e alterni

Gruppo ciclico C_n

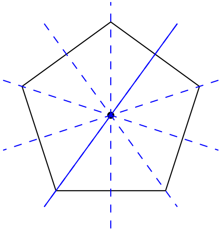
E' il gruppo delle rotazioni del piano che portano il poligono regolare con *n* lati in se stesso.



E' generato dalla rotazione r di angolo $2\pi/n$, che ha ordine n. I suoi unici elementi sono le n potenze di r. Come ogni gruppo ciclico, è abeliano. L'ordine di r^i è $n/\mathrm{MCD}(n,i)$.

Gruppo diedrale D_n - I

E' il gruppo delle isometrie del piano che portano il poligono regolare con *n* lati in se stesso.



Possiede 2*n* elementi: ciascuna isometria è individuata dall'immagine di un vertice (*n* scelte) e dall'immagine di un vertice adiacente (2 scelte). In effetti, D_n contiene le *n* rotazioni di C_n e *n* ribaltamenti (= simmetrie assiali) rispetto agli assi di simmetria del poligono.

Gruppo diedrale D_n - II

Ogni ribaltamento ha ordine 2.

Indichiamo con s uno dei ribaltamenti, $s^2 = 1$. Dal momento che $C_n < D_n$, le due classi laterali (sinistre) sono C_n, sC_n.

Poiché C_n contiene le n rotazioni, sC_n deve contenere tutti e soli gli n ribaltamenti. Ogni sr^i è un ribaltamento, e ha ordine 2.

$$(sr^i)^2 = 1 \implies sr^i = r^{-i}s, \qquad r^i s = sr^{-i}.$$

Possiamo calcolare tutti i prodotti:

$$\begin{aligned} r^i \cdot r^j &= r^{i+j}, & sr^i \cdot r^j &= sr^{i+j} \\ r^i \cdot sr^j = (r^i s)r^j = (sr^{-i})r^j &= sr^{j-i}, & sr^i \cdot sr^j = s(r^i \cdot sr^j) &= r^{j-i}. \end{aligned}$$

All'esponente, $i + j$ va sempre inteso modulo n.

Notazione ciclica in S_n - I

Abbiamo già incontrato il gruppo simmetrico S_n, che contiene tutte le $n!$ permutazioni di n elementi.

Vogliamo introdurre una notazione più compatta per descrivere una permutazione. Ad esempio le permutazioni

$$\sigma : \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 8 \\ 3 \mapsto 4 \\ 4 \mapsto 1 \\ 5 \mapsto 6 \\ 6 \mapsto 3 \\ 7 \mapsto 7 \\ 8 \mapsto 5 \end{cases}, \qquad \tau : \begin{cases} 1 \mapsto 3 \\ 2 \mapsto 2 \\ 3 \mapsto 6 \\ 4 \mapsto 4 \\ 5 \mapsto 8 \\ 6 \mapsto 1 \\ 7 \mapsto 7 \\ 8 \mapsto 5 \end{cases}$$

si indicano con $\sigma = (1\,2\,8\,5\,6\,3\,4)$, $\tau = (1\,3\,6)(5\,8)$.

Notazione ciclica in S_n - II

I cicli di lunghezza uno, cioè i punti fissi della permutazione, non sono indicati:

$$\tau = (1\,3\,6)(2)(4)(5\,8)(7) = (1\,3\,6)(5\,8).$$

Ad una stessa permutazione non corrisponde un'unica espressione ciclica. Ad esempio

$$\sigma = (1\,2\,8\,5\,6\,3\,4) = (8\,5\,6\,3\,4\,1\,2) = (3\,4\,1\,2\,8\,5\,6).$$

Se una permutazione contiene più cicli disgiunti, questi possono comparire in più di un ordine possibile:

$$\tau = (1\,3\,6)(5\,8) = (5\,8)(1\,3\,6) = (8\,5)(3\,6\,1).$$

Si può ovviare a questa ridondanza decidendo che ogni ciclo inizia per il suo elemento minimo, e ordinando cicli disgiunti a seconda del loro primo elemento.
La notazione suggerisce che cicli disgiunti commutano tra loro, il che è vero.

Se

$$\sigma = (1\,2\,8\,5\,6\,3\,4), \qquad \tau = (1\,3\,6)(5\,8),$$

allora

$$\sigma^{-1} = (1\,4\,3\,6\,5\,8\,2), \qquad \tau^{-1} = (1\,6\,3)(5\,8).$$

Inoltre

$$\sigma\tau = (1\,4)(2\,8\,6), \qquad \tau\sigma = (1\,2\,5)(3\,4).$$

La composizione $\sigma\tau$ si legge "σ dopo τ".

Parità di permutazioni

In seguito, avremo bisogno del concetto di parità di una permutazione.

- Le permutazioni sono pari oppure dispari.
- Le parità si sommano per composizione: la parità di $\sigma\tau$ è la somma delle parità di σ e di τ.
  - Pari + pari = pari; pari + dispari = dispari; dispari + dispari = pari.
- Le trasposizioni – cioè gli scambi di due soli elementi – sono tutte dispari.

In pratica, per calcolare la parità di una permutazione σ, la esprimo come composizione di trasposizioni. La parità del numero di trasposizioni necessarie non dipende dall'espressione scelta.

Esempio: $(1\,2\,4) = (1\,4)(1\,2) = (3\,4)(1\,3)(1\,2)(3\,4)$ è una permutazione pari.

Perché funziona? - I

Se $\sigma \in S_n$, considero le due espressioni

$$A = \prod_{1 \leq i < j \leq n} (j - i), \qquad A_\sigma = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)).$$

Entrambe moltiplicano tutte le possibili differenze tra i numeri $1, \ldots, n$.
I fattori nei due prodotti sono gli stessi, e differiscono al più nel segno: nel primo prodotto sono tutti positivi, mentre nel secondo prodotto alcuni sono positivi e altri negativi.
Ad esempio, se $\sigma = (1\,2)(3\,4)$, allora

$$A = (2-1)(3-1)(4-1)(3-2)(4-2)(4-3),$$
$$A_\sigma = (1-2)(4-2)(3-2)(4-1)(3-1)(3-4).$$

I fattori sono gli stessi, ma $(2-1)$ e $(4-3)$ hanno cambiato segno.
Il rapporto $\text{sgn}(\sigma) = A_\sigma / A$ vale ± 1. Se $\text{sgn}(\sigma) = 1$, allora σ si dice pari, altrimenti dispari. $\text{sgn}(1\,2) = -1$.

Perché funziona? - II

Vale la proprietà

$$\operatorname{sgn}(\sigma\tau) = \frac{A_{\sigma\tau}}{A} = \frac{A_{\sigma\tau}}{A_\tau} \cdot \frac{A_\tau}{A} = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

Di conseguenza

$$\begin{aligned}
\operatorname{sgn}(\mathrm{Id}) &= 1 \\
\operatorname{sgn}(\sigma^{-1}) &= \operatorname{sgn}(\sigma)^{-1} = \operatorname{sgn}(\sigma) \\
\operatorname{sgn}(1\,2) &= -1 \\
\operatorname{sgn}(1\,b) = \operatorname{sgn}(2\,b)(1\,2)(2\,b) &= (\operatorname{sgn}(2\,b))^2 \operatorname{sgn}(1\,2) = -1 \\
\operatorname{sgn}(a\,b) = \operatorname{sgn}(1\,a)(1\,b)(1\,a) &= -1.
\end{aligned}$$

Calcolo pratico della parità

- Le trasposizioni sono dispari
- I 3-cicli sono pari:
  - $(1\,2\,3) = (1\,3)(1\,2)$, $(a\,b\,c) = (a\,c)(a\,b)$.
- I 4-cicli sono dispari:
  - $(1\,2\,3\,4) = (1\,4)(1\,3)(1\,2)$.
- Un n-ciclo è pari se n è dispari, e dispari se n è pari.
- Le parità si sommano per composizione.

Ad esempio, $(1\,2\,5)(3\,4\,6\,7)$ è dispari: infatti $(1\,2\,5)$ è pari, mentre $(3\,4\,6\,7)$ è dispari, e pari + dispari = pari.

Il gruppo alterno A_n

L'applicazione $\mathrm{sgn} : S_n \to \{\pm\}$ è un omomorfismo di gruppi.

Il suo nucleo contiene tutte e sole le permutazioni pari, e costituisce un sottogruppo A_n, detto sottogruppo alterno di S_n.

A_n è un sottogruppo normale di S_n e contiene $n!/2$ elementi.

Ad esempio, $A_3 = \{\mathrm{Id}, (1\,2\,3), (1\,3\,2)\}$ ha $3 = 3!/2$ elementi.