

Il teorema di Cauchy

di Gabriel Antonio Videtta

Nota. Nel corso del documento per (G, \cdot) si intenderà un qualsiasi gruppo.

Si dimostra in questo documento, per ben due volte, un inverso parziale del teorema di Lagrange, il celebre teorema di Cauchy. Tale teorema asserisce che se p è un numero primo che divide l'ordine di G , allora esiste un elemento di G di ordine p .

Si mostra innanzitutto che il teorema vale per gruppi abeliani.

Teorema (di Cauchy per gruppi abeliani). Sia G un gruppo abeliano finito. Se un numero primo p divide $|G|$, allora esiste $g \in G$ tale per cui $o(g) = p$.

Dimostrazione. Sia $|G| = pn$ con $n \in \mathbb{N}^+$. Si dimostra per induzione su n la validità della tesi. Se $n = 1$, allora G è ciclico, e quindi ammette un elemento di ordine p , completando il passo base.

Sia allora $n > 1$ e si ipotizzi allora che tutti i gruppi tali che $|G| = pk$ con $k < n$, $k \in \mathbb{N}^+$ ammettano un elemento di ordine p . Sia $h \in G$, $h \neq e$ (questo h sicuramente esiste, dal momento che $p > 1$). Se $p \mid o(h)$, allora $h^{o(h)/p}$ è un elemento di G di ordine p . Altrimenti, si consideri $H = \langle h \rangle$.

Dal momento che G è abeliano, H è normale, e dunque si può considerare il gruppo quoziente G/H . Poiché $p \nmid o(h) = |H|$ e p divide $|G|$, p divide anche $|G/H|$ per il teorema di Lagrange. Inoltre, poiché $o(h) > 1$ (infatti $h \neq e$), $|G/H| < |G|$. Per l'ipotesi induttiva, allora, esiste un elemento tH di ordine p in G/H .

Si mostra adesso che $p \mid o(t)$. Si consideri la proiezione al quoziente $\pi : G \rightarrow G/H$ tale per cui:

$$g \xrightarrow{\pi} gH.$$

Allora $p = o(tH) \mid o(t)$, dal momento che $eH = \pi(t^{o(t)}) = (tH)^{o(t)}$. Pertanto, come prima, $t^{o(t)/p}$ è un elemento di ordine p , concludendo il passo induttivo. \square

Di seguito si dimostra il teorema di Cauchy in generale.

Teorema (di Cauchy). Sia G un gruppo finito. Se un numero primo p divide $|G|$, allora esiste $g \in G$ tale per cui $o(g) = p$.

Dimostrazione. Sia $|G| = pn$ con $n \in \mathbb{N}^+$. Si dimostra la tesi per induzione. Se $n = 1$, G è ciclico e dunque ammette un generatore di ordine p , completando il passo base. Sia ora $n > 1$ e si assuma che ogni gruppo di ordine pk con $k < n$ ammetta un elemento di ordine p .

Sia \mathcal{R} è un insieme dei rappresentanti delle classi di coniugio di G . Se esiste $g \in \mathcal{R}$ tale per cui p divide $|Z_G(g)|$, allora esiste un elemento di ordine p in $Z_G(g)$ per ipotesi induttiva (infatti $Z_G(g) \neq G$, altrimenti g appartenerrebbe al centro di G). Altrimenti si consideri la formula delle classi di coniugio:

$$|G| = |Z(G)| + \sum_{g \in \mathcal{R} \setminus Z(G)} \frac{|G|}{|Z_G(g)|}.$$

Poiché p non divide $|Z_G(g)|$ per ogni $g \in \mathcal{R} \setminus Z(G)$, p divide ancora $|G|/|Z_G(g)|$ (e quindi il secondo termine del secondo membro). Allora, prendendo l'identità modulo p , si deduce che:

$$|Z(G)| \equiv 0 \pmod{p}.$$

Poiché allora p divide $|Z(G)|$ e $Z(G)$ è un gruppo abeliano, il passo induttivo segue dal Teorema di Cauchy per gruppi abeliani, da cui la tesi. \square

Si mostra infine una dimostrazione alternativa del teorema di Cauchy (più immediata e facile da ricordare), basata su una particolare costruzione.

Dimostrazione alternativa. Si¹ consideri l'insieme S , dove:

$$S = \{(a_1, \dots, a_p) \in G^p \mid a_1 \cdots a_p = e\}.$$

Dimostrando che esiste un elemento $h \in G$ diverso dall'identità tale per cui $(h, \dots, h) \in S$, si mostra che $h^p = e$, e dunque che $o(h) = p$ (infatti $h \neq e$), dimostrando la tesi.

Si consideri l'azione φ di $\mathbb{Z}/p\mathbb{Z}$ su S univocamente determinata² dalla relazione:

$$1 \xrightarrow{\varphi} [(a_1, a_2, \dots, a_p) \mapsto (a_2, \dots, a_p, a_1)].$$

In particolare $m \cdot (a_1, \dots, a_p)$ restituisce una p -upla ottenuta "ciclando a sinistra" la p -upla iniziale di m posizioni. Si consideri la somma data dal teorema orbita-stabilizzatore:

$$|S| = \sum_{x \in S} \frac{p}{|\text{Stab}(x)|} = 1 + N + \sum_{x \in S \setminus (\{(e, \dots, e)\} \cup H)} \frac{p}{|\text{Stab}(x)|},$$

dove H è l'insieme degli elementi $h \neq e$ tali per cui $h^p = e$ (ossia le p -uple con coordinate identiche tra loro) e $N = |H|$. Poiché $\text{Stab}(x) \leq \mathbb{Z}/p\mathbb{Z}$, gli unici ordini di $\text{Stab}(x)$ possono essere 1 e p . Se tuttavia, per $x \in S \setminus (\{(e, \dots, e)\} \cup H)$, valesse $\text{Stab}(x) =$

¹Riadattando opportunamente questa dimostrazione, si può fornire un'ulteriore dimostrazione del Teorema di Eulero di teoria dei numeri.

² $\mathbb{Z}/p\mathbb{Z}$ è infatti generato da 1.

$\mathbb{Z}/p\mathbb{Z}$, x avrebbe coordinate tutte uguali, e quindi, per ipotesi, x appartenerrebbe ad H o sarebbe l'identità, \neq . Quindi la somma del secondo membro vale esattamente pk , dove $k = |S \setminus (\{(e, \dots, e)\} \cup H)|$.

Si osserva adesso che $|S| = n^{p-1}$, dove $n = |G|$. Infatti è sufficiente determinare le prime $p-1$ coordinate, per le quali vi sono n scelte, per determinare anche l'ultima coordinata tramite la relazione $a_1 \cdots a_n = e$. Prendendo allora la precedente identità modulo p , si ottiene che³:

$$N \equiv -1 \pmod{p},$$

e quindi in particolare esiste almeno un elemento di ordine p diverso dall'identità. \square

³Questa dimostrazione fornisce quindi anche un risultato sul numero di elementi con ordine primo in G , ossia esso è congruo a -1 in modulo p .