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 sottogruppo H 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 p divide $|G|$, allora esiste $H \leq G$ tale per cui $|H| = p$.

Dimostrazione. Sia $|G| = pn$ con $n \in \mathbb{N}^+$. Si dimostra per induzione su n la validità della tesi. Se $n = 1$, allora G stesso è un sottogruppo 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 sottogruppo 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 $\left\langle h^{o(h)/p} \right\rangle$ è un sottogruppo 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 sottogruppo T di ordine p di G/H. Poiché T è di ordine p, T è ciclico, e quindi esiste $t \in G$, $t \neq e$ tale per cui $T = \langle tH \rangle$.

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

$$g \overset{\pi}{\mapsto} gH.$$

Allora $p = o(tH) \mid o(t)$, dal momento che $eH = \pi(t^{o(t)}) = (tH)^{o(t)}$. Pertanto, come prima, si può estrarre da $\langle t \rangle$ un sottogruppo di G 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 $p \mid |G|$, allora esiste $H \leq G$ tale per cui $|H| = p$.

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

Se esiste $H \lneq G$ tale per cui p divide $|H|$, allora H, e quindi anche G, ammette un sottogruppo di ordine p per l'ipotesi induttiva. Si assuma dunque che non esiste alcun sottogruppo proprio $H < G$ tale per cui p divide $|H|$. Si consideri la formula delle classi di coniugio:

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

dove $\mathcal{R}$ è un insieme dei rappresentanti delle classi di coniugio di G. Se $g \in \mathcal{R} \setminus Z(G)$, allora $Z_G(g)$ è un sottogruppo proprio di G, e quindi, per ipotesi, p non divide $|Z_G(g)|$; e quindi p divide ancora ${}^{|G|}/_{|Z_G(g)|}$ (e quindi il secondo termine del secondo membro). Allora, prendendo l'identità modulo p, si deduce che:

$$|Z(G)| \equiv 0 \quad (p).$$

Poiché $Z(G)$ è un sottogruppo di G, se valesse $Z(G) < G$, si violerebbero le ipotesi iniziali. Pertanto deve necessariamente valere $Z(G) = G$, e quindi G è abeliano. Pertanto G ammette un sottogruppo di ordine p per il Teorema di Cauchy per i gruppi abeliani; completando il passo induttivo. □

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

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

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

Dimostrando che esiste un elemento $h \in G$ diverso dall'identità tale per cui $(h, \ldots, h) \in S$, si mostra che $h^p = e$, e dunque che $o(h) = p$ (infatti $h \neq e$). Allora, in tal caso, $\langle h \rangle$ è un sottogruppo di G di ordine p, e si dimostra la tesi.

Si ipotizzi che tale elemento h non esisti. Si consideri l'azione φ di $\mathbb{Z}/p\mathbb{Z}$ su S univocamente determinata[1] dalla relazione:

$$1 \overset{\varphi}{\mapsto} \left[(a_1, a_2, \ldots, a_p) \mapsto (a_2, \ldots, a_p, a_1)\right].$$

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

$$|S| = \sum_{x \in S} \frac{p}{|\mathrm{Stab}(x)|} = 1 + \sum_{x \in S \setminus \{(e, \ldots, e)\}} \frac{p}{|\mathrm{Stab}(x)|}.$$

Poiché $\mathrm{Stab}(x) \leq \mathbb{Z}/p\mathbb{Z}$, gli unici ordini di $\mathrm{Stab}(x)$ possono essere 1 e p. Se tuttavia, per $x \in S \setminus \{(e, \ldots, e)\}$, valesse $\mathrm{Stab}(x) = \mathbb{Z}/p\mathbb{Z}$, x avrebbe coordinate tutte uguali, e

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

quindi, per ipotesi, $x = (e, \ldots, e)$, $\lightning$. Quindi il secondo termine del secondo membro vale esattamente pk, dove $k = |S \setminus \{(e, \ldots, e)\}|$.

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:

$$1 \equiv 0 \quad (p),$$

da cui l'assurdo ricercato, $\lightning$. $\square$