Sia G un gruppo finito di cardinalità n e sia p un divisore primo di n . Scriviamo $n = p^a m$ con m non divisibile per p . Un p -sottogruppo di Sylow di G è un sottogruppo di cardinalità p^a .

Teorema. (Ludwig Sylow 1872) Sia G un gruppo finito come sopra. Allora

- (a) G possiede p -sottogruppi di Sylow;
- (b) Il numero di p -sottogruppi di Sylow divide m ed è congruo ad 1 (mod p).
- (c) I p -sottogruppi di Sylow di G sono coniugati fra loro;

Qua un p -gruppo è un gruppo finito di cardinalità una potenza di un numero primo p .

Lemma 1. Sia H un p -gruppo che agisce su un insieme finito X . Allora si ha che

$$\#X \equiv \#X^H \pmod{p}.$$

Dimostrazione. L'insieme X è unione disgiunta delle orbite di H e quindi $\#X$ è la somma delle cardinalità delle orbite di H . La cardinalità di ogni orbita divide $\#H$ ed è quindi potenza di p . In particolare, un'orbita consiste in un punto fisso oppure la sua cardinalità è divisibile per p . Concludiamo che $\#X \equiv \#X^H \pmod{p}$ dove X^H indica l'insieme dei punti di X fissati da H .

Corollario 2. Sia $H \subset G$ un p -gruppo. Allora si ha che

$$[N_G H : H] \equiv [G : H] \pmod{p}.$$

Dimostrazione. Il gruppo H agisce sull'insieme X delle classi laterali sinistre di H . Abbiamo che $\#X = [G : H]$. Una classe gH in X è fissata da H quando $hgH = gH$ per ogni $h \in H$ ovvero quando $g^{-1}hg \in H$ per ogni $h \in H$. In altre parole, gH è fissata quando g è contenuto nel normalizzante $N_G H$ di H . I punti fissi di X sono quindi le classi laterali gH con $g \in N_G H$. Poiché ce ne sono $[N_G H : H]$, il corollario segue dal Lemma 1.

Lemma 3. Sia G un gruppo finito e siano P e P' due p -sottogruppi di Sylow di G . Se P normalizza P' , allora $P = P'$.

Dimostrazione. Se P normalizza P' , allora si ha che $P \subset N_G P'$. Poiché P' è un sottogruppo normale di PP' , abbiamo l'isomorfismo naturale

$$P/(P' \cap P) \cong PP'/P'.$$

Il gruppo a sinistra è quoziente di P ed è quindi un p -gruppo. Invece, poiché P' è un p -sottogruppo di Sylow, la cardinalità del gruppo a destra non è divisibile per p . Concludiamo che i due gruppi sono banali e quindi $P = P'$, come richiesto.

Dimostrazione del teorema di Sylow. Per la parte (a) è conveniente dimostrare qualcosa più forte: (a') per ogni sottogruppo $H \subset G$ di cardinalità una potenza di p , esiste un p -gruppo di Sylow P che contiene H . Adesso possiamo procedere per induzione rispetto a $\#H$. Però, nel senso inverso! Infatti, se $\#H = p^a$, allora H stesso è un p -gruppo

di Sylow e l'affermazione è banale. Se invece H è il sottogruppo banale $\{e\}$, recuperiamo l'affermazione (a).

Supponiamo che $\#H = p^b$ con $b < a$. Sotto quest'ipotesi p divide $[G : H]$. Per il Corollario 2, anche $[N_G H : H]$ è divisibile per p . Per il Teorema di Cauchy, il gruppo quoziente $N_G H/H$ possiede quindi un elemento x di ordine p .

Sia H' il sottogruppo generato da H e x . Allora H è un sottogruppo normale di H' . Il quoziente H'/H ha cardinalità p ed è generato dall'immagine di x . Ne segue che la cardinalità di H' è p^{b+1} . Per induzione, sappiamo che H' è contenuto in un p -sottogruppo di Sylow e quindi anche H lo è, come richiesto.

(b) Sia X l'insieme dei sottogruppi di Sylow e sia P un sottogruppo di Sylow. Allora P agisce su X via coniugio. Per il lemma 3, P fissa solo se stesso. Le altre orbite di P hanno quindi cardinalità divisibile per p . Concludiamo che $\#X \equiv 1 \pmod{p}$.

(c) Sia P un p -sottogruppo di Sylow e sia Y l'insieme dei sottogruppi di Sylow coniugati con P . In altre parole, G agisce sull'insieme X dei p -sottogruppi di Sylow e Y è la G -orbita di P . Poiché lo stabilizzatore di $P \in Y$ è il normalizzante $N_G P$, la cardinalità di Y è uguale a $[G : N_G P]$. Dal fatto che $[G : N_G P]$ divide $[G : P] = m$, segue che la cardinalità di Y non è divisibile per p .

Ogni altro p -sottogruppo di Sylow P' agisce su Y per coniugio. Poiché $\#Y$ non è divisibile per p , ci sono punti fissi. Per il lemma 3, solo P' stesso può essere un punto fisso. Ne segue che P' sta in Y e quindi P' è coniugato a P , come richiesto.