Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

I TEOREMI DI SYLOW

Tesi di Laurea in Algebra

Relatore:
Chiar.ma Prof.ssa
Marta Morigi

Presentata da:
Matteo Gardini

Sessione III
Anno Accademico 2012-2013

A Elisa e Lorenzo

Introduzione

Il teorema di Lagrange per i gruppi finiti fornisce una prima relazione fra l'ordine dei sottogruppi di un gruppo finito dato e l'ordine del gruppo stesso affermando che ogni sottogruppo ha ordine che divide l'ordine del gruppo stesso. È del tutto naturale chiedersi se si possa "invertire" il teorema: cioè chiedersi se, preso un divisore positivo dell'ordine del gruppo, esista un sottogruppo, del gruppo finito dato, che abbia ordine uguale a tale divisore. Sfortunamente ciò vale solo in determinati casi fortunati mentre in generale non è vero; si possono però ottenere alcuni risultati notevoli se si studiano i numeri primi e le loro potenze che dividono l'ordine del gruppo dato. Il primo teorema di Sylow procede proprio in tale direzione. Il secondo e il terzo teorema di Sylow forniscono, invece, risultati sui sottogruppi, che da Sylow prendono il nome, aventi ordine la massima potenza di un primo che divide l'ordine del gruppo.
In questo lavoro sono date più dimostrazioni dei principali teoremi che vengono affrontati. Tale decisione non nasce dal fatto che alcune dimostrazioni siano meno "simpatiche" o convincenti, ma scaturisce dal preciso intento di dare una visione quanto più panoramica possibile dell'argomento. Contrariamente, forse, all'idea iniziale, non sono state date le varie dimostrazioni ai tre teoremi di Sylow in "serie", ma in "parallelo", ponendo in risalto non tanto l'intercambiabilità della strada percorribile, ma alcuni aspetti a volte più canonici e standard di alcune dimostrazioni, e a volte più pirotecnici di altre.

Indice

Capitolo 1

Azioni di Gruppi su Insiemi

Definizione 1.1. Azione sinistra di un gruppo su un insieme.
Siano G un gruppo e X un insieme. Sia e l'identità di G, si definisce azione sinistra (o a sinistra) di G su X una applicazione $G \times X \to X, (g,\mathrm{x}) \mapsto g\mathrm{x}$ per cui valgano

1. $ex = x$ per ogni $x \in X$

2. $g_1(g_2x) = (g_1g_2)x$ per ogni $g_1, g_2 \in G$ e per ogni $x \in X$.

Si dice in tal caso che G agisce a sinistra su X e che X è un G-insieme.

Le condizioni appena date implicano che, per ogni $g \in G$, la traslazione sinistra di ampiezza g

$$\tau_g : X \to X, x \mapsto gx$$

è una biezione la cui applicazione inversa è $\tau_{g^{-1}}$ e che $\tau_{gg'} = \tau_g\tau_{g'}$ (dal punto 2. della definizione). Si ha, quindi, che una azione sinistra induce un omomorfismo di gruppi:

$$\tau : G \to A(X), g \mapsto \tau_g \tag{1.1}$$

dove $A(X)$ è il gruppo delle permutazioni degli elementi di X. Esempi di azioni a sinistra di gruppi su insiemi sono:

Esempio 1.1. L'azione di S_n su $I_n = \{1,2,\ldots,n\}$ definita dalla mappa $(\sigma, i) \mapsto \sigma(i)$.

Esempio 1.2. Dato $H \leqslant G$, l'azione di G su $\{xH \mid x \in G\}$ definita dalla mappa $(g, xH) \mapsto gxH$.

Esempio 1.3. L'azione di coniugio di G su sé stesso, definita dalla mappa $(g, x) \mapsto gxg^{-1}$.

Definizione 1.2. Una azione sinistra si dice **fedele** se l'omomorfismo indotto 1.1 è iniettivo.

Definizione 1.3. Si definisce mappa di G-insiemi una applicazione $\varphi : X \to Y$ tale che $\varphi(gx) = g\varphi(x)$ per ogni $g \in G$.
Se tale mappa è anche una biezione si parla di isomorfismo di G-insiemi.

Osservazione 1. Data una azione di un gruppo G su un insieme X risulta definita la seguente relazione di equivalenza

$$\sim_G: x \sim_G y \Leftrightarrow \text{esiste } g \in G \quad \text{tale che} \quad y = gx. \tag{1.2}$$

Definizione 1.4. Le classi di equivalenza della relazione $\sim_G$ sono chiamate **G-orbite** e vengono indicate con $\bar{x}$ dove x è un elemento dell'orbita.

Osservazione 2. $\bar{x} = \{gx \mid g \in G\}$

Definizione 1.5. Un sottoinsieme S di X si dice **stabile** sotto l'azione di G se per ogni $s \in S$ *e* $g \in G$ si ha $sg \in S$.

Osservazione 3. Se S è un sottoinsieme stabile di X rispetto all'azione di G allora l'azione di G su X induce una azione di G su S.

Osservazione 4. $\bar{x}$ (G-orbita di x) è il più piccolo sottoinsieme stabile di X contenente x.

Definizione 1.6. L'azione di G su X si dice **transitiva** se per ogni $x, y \in X$ esiste $g \in G$ tale che $y = gx$. In tal caso si dice che G agisce transitivamente su X e l'insieme X viene detto **omogeneo**.

Definizione 1.7. Si consideri l'azione di G su X e sia $x_0 \in X$. Si definisce **stabilizzatore** di x_0, e si indica $\mathrm{Stab}(x_0)$, l'insieme $\{g \in G \mid gx_0 = x_0\}$.
Nel caso dell'azione di coniugio di G su sé stesso e dell'azione di coniugio di G sui suoi sottogruppi, gli stabilizzatori di x e H, con $x \in G$ e $H \leqslant G$, prendono i nomi di **centralizzatore** di x in G, che si indica $\mathbf{C_G(x)}$, e **normalizzatore** di H in G, $\mathbf{N_G(H)}$.

Proposizione 1.0.1. *Si ha che:*

1. *Stab(x_0) è un sottogruppo di G (Stab(x_0)$\leqslant G$);*
2. *Stab(gx_0) = gStab(x_0)g^{-1};*
3. *l'omomorfismo indotto τ ha come nucleo $\bigcap_{x\in X}$ Stab(x).*

Dimostrazione. (1) $\mathrm{Stab}(x_0)$ è non vuoto infatti $e \in \mathrm{Stab}(x_0)$. Siano g, g' elementi di $\mathrm{Stab}(x_0)$ allora, poichè $x_0 = ex_0 = g^{-1}gx_0 = g^{-1}x_0$ si ha che $g^{-1} \in \mathrm{Stab}(x_0)$, da cui $g^{-1}g'x_0 = g^{-1}x_0 = x_0$. Da ciò segue che $\mathrm{Stab}(x_0)$ è un sottogruppo di G.
(2) Sia $g' \in \mathrm{Stab}(x_0)$ allora $(gg'g^{-1})gx_0 = gg'x_0 = gx_0$ da cui $gg'g^{-1} \in \mathrm{Stab}(gx_0)$ quindi $\mathrm{Stab}(gx_0) \supseteq g\mathrm{Stab}(x_0)g^{-1}$. Vediamo l'altra inclusione: sia $g' \in \mathrm{Stab}(gx_0)$ allora $g'gx_0 = gx_0$, perciò $(g^{-1}g'g)x_0 = (g^{-1})g'(gx_0) = (g^{-1})gx_0 = x_0$ da cui $(g^{-1}g'g) \in \mathrm{Stab}(x_0)$ cioè $g' \in g\mathrm{Stab}(x_0)g^{-1}$. Abbiamo quindi dimostrato l'uguaglianza dei due insiemi.
(3) $\ker\tau = \{g \in G \mid \tau_g = 1 \text{ (identità in } A(X))\} = \{g \in G \mid \tau_g x = gx = x\ \forall x \in X\}$; allora $\ker\tau = \bigcap_{x\in X} \mathrm{Stab}(x)$. □

Osservazione 5. Il punto 2. della proposizione precedente mette in evidenza che $\mathrm{Stab}(x)$ non è necessariamente normale in G.

Corollario 1.0.2. $C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$.
$C_G(x)$ è quindi il più grande sottogruppo di G in cui x commuta.

Corollario 1.0.3. $N_G(H) = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\}$.
$N_G(H)$ è quindi il più grande sottogruppo di G in cui H è normale.

Proposizione 1.0.4. *Sia G un gruppo che agisce su X e sia $x \in X$ allora esiste una corrispondenza biunivoca tra gli elementi di $\bar{x}$ e i laterali sinistri di Stab(x) in G.*

Vediamo, ora, un'altra proposizione che ci permette di ottenere il risultato della proposizione 1.0.4 senza nessuno sforzo aggiuntivo.

Proposizione 1.0.5. *Sia G un gruppo che agisce transitivamente sull'insieme X allora, per ogni $x_0 \in X$, la mappa $\varphi : G/Stab(x_0) \to X$ [1] definita da $gStab(x_0) \mapsto gx_0$ è un isomorfismo di G-insiemi.*

Dimostrazione. La mappa φ è ben definita e biettiva: il fatto che sia ben definita e iniettiva si vede dal fatto che $g\mathrm{Stab}(x_0) = h\mathrm{Stab}(x_0) \Leftrightarrow g^{-1}h \in \mathrm{Stab}(x_0)$ $\Leftrightarrow g^{-1}hx_0 = x_0 \Leftrightarrow gx_0 = hx_0$, mentre la suriettività è data dalla transitività dell'azione in quanto per ogni $x \in X$ esiste $g \in G$ tale che $x = gx_0$. Abbiamo, inoltre, che $G/\mathrm{Stab}(x_0)$ e X sono G-insiemi e $\varphi(g(h\mathrm{Stab}(x_0))) = \varphi(gh\mathrm{Stab}(x_0)) = ghx_0 = g\varphi(h\mathrm{Stab}(x_0))$ da cui φ è una mappa di G-insiemi, è biettiva e quindi è un isomorfismo di G-insiemi. □

Osservazione 6. La proposizione 1.0.5 mette in evidenza che data una azione **transitiva** di G su X, X è isomorfo a $G/\mathrm{Stab}(x_0)$ per ogni $x_0 \in X$. Tuttavia tale isomorfismo non è canonico, ma dipende dalla scelta di x_0.

Ottenuto il risultato della proposizione 1.0.5, la dimostrazione della proposizione 1.0.4 è immediata:

Dimostrazione della proposizione 1.0.4. $\bar{x}$ è un sottoinsieme stabile di X allora l'azione di G su X induce l'azione di G su $\bar{x}$. Tale azione indotta è transitiva allora per 1.0.5 per ogni $y \in \bar{x}$, $\bar{x} \cong G/\mathrm{Stab}(y)$ quindi, in particolare, esiste una corrispondenza biunivoca tra i due insiemi $\bar{x}$ e $G/\mathrm{Stab}(x)$. □

Corollario 1.0.6. $|\bar{x}| = |G : Stab(x)|$.

[1] $G/\mathrm{Stab}(x_0)$ non è necessariamente un gruppo: $\mathrm{Stab}(x_0)$ non è infatti necessariamente un sottogruppo normale. Con tale scrittura intendiamo perciò il G-insieme $\{g\mathrm{Stab}(x_0) \mid g \in G\}$ delle classi laterali sinistre di $\mathrm{Stab}(x_0)$ in G.

Dimostrazione. Poichè esiste una corrispondenza biunivoca tra $\bar{x}$ e $G/\mathrm{Stab}(x)$ avremo $|\bar{x}| = |G/\mathrm{Stab}(x)| = |G : \mathrm{Stab}(x)|$. □

Corollario 1.0.7. *Data l'azione di coniugio del gruppo G su sé stesso, per ogni $x \in G$ risulta:*

$$|\bar{x}| = |G : C_G(x)|. \tag{1.3}$$

Corollario 1.0.8. *Data l'azione di coniugio del gruppo G sull'insieme dei suoi sottogruppi, per ogni $H \leqslant G$ risulta:*

$$|\bar{H}| = |G : N_G(H)|. \tag{1.4}$$

Vediamo ora un lemma più generale che ci permetterà di dire qualcosa di $\ker\tau$ dove τ è l'omomorfismo 1.1 indotto dall'azione.

Lemma 1.0.9. *Sia G un gruppo e $H \leqslant G$ allora $\bigcap_{g\in G} gHg^{-1}$ è il più grande sottogruppo normale incluso in H*

Dimostrato il lemma 1.0.9, la proposizione che segue è pressoché immediata.

Proposizione 1.0.10. *Se il gruppo G agisce transitivamente su X allora, per ogni $x_0 \in X$, $\ker\tau$ è il più grande sottogruppo normale di G incluso in Stab(x_0).*

Dimostrazione della proposizione 1.0.10.
$\ker\tau =$ (1.0.1) $\bigcap_{x\in X} \mathrm{Stab}(x)$ = (transitività dell'azione) $\bigcap_{g\in G} \mathrm{Stab}(gx_0) =$ (1.0.1) $\bigcap_{g\in G} g\mathrm{Stab}(x_0)g^{-1}$ da cui si ha la tesi per il Lemma 1.0.9. □

Dimostrazione del Lemma 1.0.9.
Sia $M = \bigcap_{g\in G} gHg^{-1}$. M è un sottogruppo di G perchè essendo intersezione di sottogruppi di G è a sua volta un sottogruppo di G, è incluso in H infatti $eHe^{-1} = H$ ed è normale in G perchè, per ogni $\tilde{g} \in G$, $\tilde{g}M\tilde{g}^{-1} = \tilde{g}(\bigcap_{g\in G} gHg^{-1})\tilde{g}^{-1} = \bigcap_{g\in G} \tilde{g}gHg^{-1}\tilde{g}^{-1} = \bigcap_{h\in G} hHh^{-1} = M$. Sia, ora, $N \trianglelefteq G, N \subseteq H$. Per ogni $g \in G$, $N = gNg^{-1} \subseteq$ (perchè $N \subseteq H$) gHg^{-1}, quindi $N \subseteq \bigcap_{g\in G} gHg^{-1}$ da cui segue che $\bigcap_{g\in G} gHg^{-1}$ è il più grande sottogruppo normale di G incluso in H. □

Definizione 1.8. Sia G un gruppo, si definisce centro di G, e si indica $Z(G)$, l'insieme $\{g \in G \mid gh = hg \text{ per ogni } h \in G\}$.

Proposizione 1.0.11 (Equazione delle classi)**.**
Sia G un gruppo finito, allora

$$|G| = |Z(G)| + \sum_{i=1}^{t} |G : C_G(x_i)| \tag{1.5}$$

ove $\{x_1, \ldots, x_t\}$ è un sistema completo di rappresentanti delle classi di coniugio di G non contenute nel centro.

Dimostrazione. L'azione di coniugio di G su di sé induce una relazione di equivalenza in G, si ha perciò una partizione di G data dall'insieme delle classi di equivalenza (orbite). Siano $x_1, \ldots, x_m$ elementi di G le cui orbite siano a due a due distinte e tali che $x_1, \ldots, x_t \notin Z(G)$, $x_{t+1}, \ldots, x_m \in Z(G)$ e $\bigcup_{i=1}^{m} \bar{x}_i = G$, allora $|G| = \sum_{i=1}^{m} |\bar{x}_i|$. D'altra parte se $x_i \in Z(G)$ allora $\bar{x}_i = \{x_i\}$ quindi $|G| = \sum_{i=1}^{m} |\bar{x}_i| = |Z(G)| + \sum_{i=1}^{t} |\bar{x}_i|$ che per 1.3 diventa $|G| = |Z(G)| + \sum_{i=1}^{t} |G : C_G(x_i)|$. □

Proposizione 1.0.12. *Se $H \leqslant G, |G : H| = n$ e H non contiene alcun sottogruppo normale di G diverso da quello banale; allora G è isomorfo a un sottogruppo di S_n.*

Dimostrazione. Sia $X = \{gH | g \in G\}$. Poichè $\ker \tau = \bigcap_{g \in G} \text{Stab}(gH) = \bigcap_{g \in G} g\text{Stab}(H)g^{-1}$ e $\text{Stab}(H) = \{l \in G \mid lH = H\} = H$ (perchè $lH = H$ se e solo se $l \in H$) risulta che $\ker \tau = \bigcap_{g \in G} gHg^{-1}$. $\ker \tau$ è, quindi, il più grande sottogruppo normale incluso in H, ma, dato che l'unico sottogruppo di H normale in G è $\{e\}$, $\ker \tau = \{e\}$ da cui abbiamo che G è isomorfo ad un sottogruppo di $A(X)$. D'altra parte, essendo $|G : H| = n$, $A(X)$ è isomorfo a S_n e da ciò segue immediatamente l'enunciato. □

Corollario 1.0.13. *Sia G un gruppo finito e sia $H \leqslant G$ con $|G : H| = p$, p il più piccolo primo che divide $|G|$; allora $H \trianglelefteq G$*

Dimostrazione. Sia X l'insieme dei laterali sinistri di H in G e sia $K = \ker \tau$. Osserviamo che $K \leqslant H$ quindi $|G : K| > 1$. G/K è isomorfo ad un sottogruppo di $A(X)$ (per il Teorema fondamentale di omomorfismo), ma $A(X) \cong S_p$ perchè $|G : H| = p$, quindi $|G/K|$ divide $p!$. D'altra parte ogni divisore di $|G/K| = |G : K|$ deve dividere $|G|$ di cui p è il suo più piccolo divisore primo. Allora $|G : K| = p = |G : H|$ da cui si ha che H è normale in G essendo $|H : K| = 1$. □

Capitolo 2

Problema "inverso" di Lagrange

Vediamo ora il Teorema di Lagrange[1]:

Teorema 2.0.14 (di Lagrange)**.**
Se G è un gruppo finito e H è un sottogruppo di G, si ha $|G| = |H||G : H|$. In particolare l'ordine di H e l'indice di H in G sono divisori dell'ordine di G.

La domanda che ora giunge del tutto naturale è: dato un gruppo finito G e un suo sottogruppo H, l'ordine di H è un divisore dell'ordine di G, ma cosa si può dire del problema inverso? Cioè risulta naturale chiedersi: dato un intero positivo d che divide l'ordine di G, esiste un sottogruppo H avente ordine d?
In questo capitolo cercheremo di dare una risposta a questo interrogativo.

2.1 Gruppi ciclici finiti e gruppi abeliani

Teorema 2.1.1. *Sia G un gruppo ciclico finito con $|G| = m$ e sia d un intero positivo che divide m allora esiste uno ed un solo $H \leqslant G$ tale che $|H| = d$.*

Dimostrazione. Poichè G è ciclico, esiste un $x \in G$ tale che $G = \langle x \rangle$ quindi, essendo $|G| = m$, m è il periodo di x cioè $m = \min\{n \in \mathbb{Z} |\ n > 0 \text{ e } x^n = e\}$.

[1]Per vederne una dimostrazione si può consultare [1] a pagina 100.

Poichè $d|m$, segue che $m = dn$ con n intero positivo. Consideriamo allora $\langle x^n \rangle$. Si ha che $(x^n)^d = x^{nd} = e$, d'altra parte $d = \min\{h \in \mathbb{Z} |\ h > 0 \text{ e } (x^n)^h = e\}$ perchè, se così non fosse, esisterebbe $h \in \mathbb{Z}, 0 < h < d$ tale che $x^{nh} = e$, ma $0 < nh < nd = m$ allora m non sarebbe il periodo di x. Quindi $\langle x^n \rangle$ è un sottogruppo di G di ordine d e abbiamo provato l'esistenza.
Proviamo ora l'unicità. Sia K un sottogruppo di G di ordine d. Poichè G è ciclico, ogni suo sottogruppo è ciclico, quindi esiste un elemento di G, x^i, tale che $K = \langle x^i \rangle$. Ma allora $(x^i)^d = e = x^0, id \equiv 0\ (mod\ m)$ e quindi $id = mh$ per qualche intero h. Sappiamo però che $m = nd$ da cui $id = ndh$ e, per la legge di cancellazione in $\mathbb{Z}, i = nh$. Si ha quindi $x^i = (x^n)^h$ cioè $K \leqslant \langle x^n \rangle$ cioè $K = \langle x^n \rangle$ dato che hanno lo stesso ordine. Rimane quindi provata l'unicità □

Nel caso di gruppi ciclici finiti è, quindi, possibile "invertire" il teorema di Lagrange.

Lemma 2.1.2. *Sia G un gruppo finito non banale, allora esistono un primo p che divide $|G|$ ed un sottogruppo H di G di ordine p.*

Dimostrazione. Poichè G è un gruppo finito non banale, esiste un elemento $g \in G$ diverso da e e, perchè $\langle g \rangle \leqslant G$, esiste un intero positivo m tale che $|\langle g \rangle| = m$. Sia p un primo che divide m. Dato che $\langle g \rangle$ è ciclico e p divide il suo ordine m, per il teorema 2.1.1, esiste un suo sottogruppo, che chiameremo H, avente ordine p. □

In realtà con questo Lemma non abbiamo guadagnato molto perchè garantisce l'esistenza di un tale primo, ma non fornisce informazioni inerenti agli altri eventuali divisori primi dell'ordine del gruppo dato.

Teorema 2.1.3. *Se G è un gruppo abeliano finito allora, per ogni p primo che divide $|G|$, esiste $x \in G$ tale che $|x| = p$.*

Dimostrazione. È sufficiente mostrare che esiste un elemento y che abbia periodo multiplo di p: infatti se $|y| = pm$ (con $m \geqslant 1$) allora $x = y^m$ ha

necessariamente periodo p. Per induzione su $|G|$. Se $|G| = p$ allora G è ciclico quindi per il teorema 2.1.1 esiste un sottogruppo di G (necessariamente ciclico) di ordine p. L'elemento cercato, x, sarà perciò un suo generatore. Sia ora $m > 1$ e sia $g \in G$. Se $|g| = p$ non c'è più nulla da dimostrare, altrimenti consideriamo $G/\langle g\rangle$ (G abeliano quindi $\langle g\rangle$ è normale in G). $|G/\langle g\rangle|$ è divisibile per p e $|G/\langle g\rangle| < |G| = pm$, usando l'ipotesi induttiva esiste, perciò, un elemento $x\langle g\rangle \in G/\langle g\rangle$ avente periodo multiplo di p, ma allora x ha periodo multiplo di p. □

Corollario 2.1.4. *Sia G un gruppo abeliano finito; allora, per ogni p primo che divide $|G|$, esiste $H \leqslant G$ tale che $|H| = p$.*

Dimostrazione. Sia p un primo che divide $|G|$, per il Teorema 2.1.3 esiste $x \in G$ tale che $|x| = p$, ma allora $\langle x\rangle$ è il sottogruppo cercato. □

Se il lemma 2.1.2 garantisce l'esistenza di un divisore primo dell'ordine del gruppo per cui esiste un sottogruppo avente ordine uguale a tale primo, il corollario 2.1.4 afferma che nei gruppi abeliani si ha tale risultato per ogni divisore primo dell'ordine del gruppo. In realtà questo risultato può essere generalizzato ad ogni gruppo finito.
Vediamo un lemma utile alla generalizzazione di cui si è parlato poco sopra.

Lemma 2.1.5. *Sia H un gruppo di ordine p^n che agisce sull'insieme finito X e sia $X_0 = \{x \in X |\ gx = x \text{ per ogni } g \in G\}$. Allora $|X| \equiv |X_0|$ $(mod\ p)$.*

Dimostrazione. L'azione di H su X induce una relazione di equivalenza su X, perciò l'insieme delle H-orbite, in quanto classi di equivalenza, costituisce una partizione di X. Sia $\{x_1, \dots, x_l\}$ un sistema di rappresentanti delle H-orbite con $x_1, \dots, x_t \notin X_0$ e $x_{t+1}, \dots, x_l \in X_0$, così $X = \bigcup_{i=1}^{l} \bar{x}_i$. Si ha che $x_j \in X_0$ se e solo se $\bar{x}_j = \{x_j\}$, per cui abbiamo $X = X_0 \cup \bigcup_{i=1}^{t} \bar{x}_i$ dove le $\bar{x}_i$ sono orbite aventi più di un elemento. Perciò, considerando gli ordini, $|X| = |X_0| + \sum_{i=1}^{t} |\bar{x}_i|$. Dal corollario 1.0.6 otteniamo, poi, che $|X| = |X_0| + \sum_{i=1}^{t} |H : \mathrm{Stab}(x_i)|$, ma $|H : \mathrm{Stab}(x_i)|$ divide $|H| = p^n$ e $|H : \mathrm{Stab}(x_i)| > 1$ così p deve necessariamente dividere $|H : \mathrm{Stab}(x_i)|$, allora $|X| \equiv |X_0|$ $(mod\ p)$. □

Teorema 2.1.6 (Teorema di Cauchy)**.** *Sia G un gruppo finito e sia p un divisore primo dell'ordine di G; allora esiste $x \in G$ tale che $|x| = p$.*

Ne daremo due dimostrazioni.

Dimostrazione. Per induzione su $|G|$. Se $|G| = p$, G è ciclico per cui esiste un elemento $x \in G$ tale che $|x| = p$ (per il teorema 2.1.3). Sia ora $|G| = pm$ con $(m > 1)$. Se esiste $g \in G$ con $g \notin Z(G)$ tale che p non divide $|G : C_G(g)|$, allora, dal teorema di Lagrange, poichè p divide $|G|$, risulta che p divide $|C_G(g)|$, quindi, per ipotesi induttiva, esiste $x \in C_G(g)$ di periodo p. Supponiamo che p divida tutti i termini del tipo $|G : C_G(y)|$ nella equazione delle classi. p deve, perciò, necessariamente dividere anche $|Z(G)|$ (altrimenti p non dividerebbe G, il che va contro le ipotesi), ma $Z(G)$ è un gruppo abeliano allora per il teorema 2.1.3 esiste un elemento $x \in Z(G) \leqslant G$ tale che $|x| = p$. □

Dimostrazione. (Mc Kay)
Sia $X = \{(g_1, \ldots, g_p) \mid g_i \in G \ \forall i = 1, \ldots, p \text{ e } g_1 \cdots g_p = e\}$. Si ha che g_p è determinato da $g_1, \ldots, g_{p-1}$, infatti si deve necessariamente avere che $g_p = (g_1 \cdots g_{p-1})^{-1}$, perciò $|X| = |G|^{p-1}$ da cui p divide $|X|$. Consideriamo ora l'azione sinistra di $\mathbb{Z}_p$ su X così definita: $(k, (g_1, \ldots, g_p)) \mapsto (g_{k+1}, g_{k+2}, \ldots, g_p, g_1, \ldots, g_k)$. Innanzitutto $(g_{k+1}, g_{k+2}, \ldots, g_p, g_1, \ldots, g_k) \in X$ (per le coppie ordinate: $ab = e \Rightarrow ba = (a^{-1}a)ba = a^{-1}a = e$, e, procedendo nello stesso modo, lo si dimostra anche per le p-tuple). Inoltre $(0, (g_1, \ldots, g_p)) \mapsto (g_1, \ldots, g_p)$ e si ha che le immagini di $(k + k', (g_1, \ldots, g_p))$ e di $(k, (k', (g_1, \ldots, g_p)))$ coincidono. Risulta quindi che $X_0 = \{(g_1, \ldots, g_p) \in X \mid g_1 = g_2 = \ldots = g_p\}$. Per il lemma 2.1.5, $|X| \equiv |X_0| \ (mod\ p)$, allora $|X_0| \equiv 0 \ (mod\ p)$, quindi, poichè X_0 è non vuoto (infatti $(e, \ldots, e) \in X_0$), $|X_0| \geqslant p$ ed esiste $(x, \ldots, x) \in X_0, (x, \ldots, x) \neq (e, \ldots, e)$. Ma, poichè $(x, \ldots, x) \in X_0 \subseteq X$, $x^p = e$ quindi il periodo di x è necessariamente p. □

Segue facilmente dal teorema precedente che, dato un gruppo finito qualsiasi, per ogni divisore primo dell'ordine del gruppo, esiste un sottogruppo

avente tale primo come ordine.
Per i gruppi abeliani, possiamo dire ancora qualcosa in più:

Teorema 2.1.7. *Sia G un gruppo abeliano finito. Allora, per ogni intero positivo d che divide $|G|$, esiste $H \leqslant G$ tale che $|H| = d$.*

Dimostrazione. Per induzione su d. Se $d = 1$ l'asserto è banale. Sia, ora, $d > 1$. Poichè $d > 1$ esiste un p primo che divide d e, per il corollario 2.1.4, esiste $K \leqslant G$ tale che $|K| = p$. D'altra parte G è abeliano quindi $K \trianglelefteq G$ e possiamo allora considerare il gruppo G/K. Posto $|G| = m$ abbiamo che $|G/K| = \frac{m}{p}$. Poichè $\frac{d}{p} \big| \frac{m}{p} = |G/K|$ e $\frac{d}{p} < d$, applicando l'ipotesi induttiva troviamo che esiste $H/K \leqslant G/K$ tale che $|H/K| = \frac{d}{p}$. Ora, essendo $H/K \leqslant G/K$, abbiamo che $H \leqslant G$ e $|H| = |H/K||K| = d$. □

Osservazione 7. Il teorema 2.1.7 mostra che, per i gruppi abeliani finiti, come per i gruppi ciclici finiti, possiamo "invertire" il teorema di Lagrange, anche se, rispetto ai gruppi ciclici finiti abbiamo perso qualcosa perchè, per i gruppi ciclici, per ogni divisore dell'ordine del gruppo, si ha **uno ed un solo** sottogruppo avente tale divisore per ordine mentre nel caso dei gruppi abeliani finiti si è persa l'unicità.

Esempio 2.1. Il gruppo $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ è un gruppo abeliano finito di ordine 4 e ha tre sottogruppi di ordine 2: $\langle (0,1) \rangle$, $\langle (1,0) \rangle$ e $\langle (1,1) \rangle$.

I risultati precedenti potrebbero far sperare riguardo alla fattibilità di poter invertire il Teorema di Lagrange, ma così non è:

Osservazione 8. A_4 è un gruppo di ordine 12 eppure non esiste $H \leqslant A_4$ tale che $|H| = 6$.

Dimostrazione. Osserviamo innanzitutto che A_4 è costituito dall'identità, da tre elementi di ordine 2, $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$, e da otto elementi di ordine 3, $(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$. Osserviamo inoltre che presi due elementi di A_4 di ordine 2, il sottogruppo in S_4 da essi generato è il sottogruppo di Klein $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$,

che, avendo ordine 4 non può essere un sottogruppo di A_4 (per il Teorema di Lagrange). Dalle osservazioni appena fatte risulta quindi che H può contenere al più un elemento di ordine 2. Supponiamo che esista $H \leqslant A_4$ tale che $|H| = 6$. Allora, poichè ogni gruppo di ordine 6 è isomorfo a $\mathbb{Z}_6$ oppure a S_3, $H \cong \mathbb{Z}_6$ oppure $H \cong S_3$. Tuttavia H non può essere ciclico perchè un elemento di ordine 6 può essere decomposto in prodotto di cicli disgiunti solo in due modi e nessuno di questi sta in A_4, allora, non potendo essere ciclico, H non può essere isomorfo a $\mathbb{Z}_6$. L'unica possibilità è quindi che $H \cong S_3$. Ma se così fosse, dovrebbero esistere un elemento, a, di A_4 di ordine 2 e uno, b, di A_4 di ordine 3 che generano H. D'altra parte, dovendo essere H un sottogruppo, si deve avere $bab^{-1} \in H$, ma bab^{-1} è un elemento di ordine 2 diverso da a quindi H avrebbe due elementi di ordine 2, il che non è possibile. Da tutto ciò si ha che non esiste un sottogruppo H di A_4 di ordine 6. □

Tale esempio mostra che il Teorema di Lagrange non è "invertibile".
Si può però ottenere ancora qualcosa lavorando con i p-gruppi e i Teoremi di Sylow che saranno trattati nelle prossime sezioni e nei prossimi capitoli.

2.2 p - gruppi

Definizione 2.1. p - gruppo.
Sia p un primo. Si dice che G è un p-gruppo se e solo se ogni suo elemento ha per periodo una potenza di p.

Definizione 2.2. Siano p un primo e G un gruppo. Si dice che $H \leqslant G$ è un p-sottogruppo se e solo se ogni elemento di H ha per periodo una potenza di p.

Osservazione 9. Tutti i sottogruppi di un p-gruppo sono p-sottogruppi.

Osservazione 10. Ogni gruppo ha un p-sottogruppo banale: $\{e\}$.

Lemma 2.2.1. *Sia p un primo.*

1. *Se G è un p-gruppo e $H \trianglelefteq G$ allora G/H è un p-gruppo.*

2. Se $H \trianglelefteq G$ e H, G/H sono p-gruppi allora G è un p-gruppo.

Dimostrazione.
(1) G è un p-gruppo allora, per ogni $g \in G$, esiste $r > 0$ tale che $g^{p^r} = e$. Consideriamo gH con $g \in G$ e sia p^n il periodo di g. $(gH)^{p^n} = g^{p^n}H = eH = H$, allora gH ha per periodo una potenza di p da cui G/H è un p-gruppo.
(2) Sia $x \in G, xH$ è un elemento di G/H che è un p-gruppo quindi esiste $r > 0$ tale che $H = (xH)^{p^r} = x^{p^r}H$, da ciò risulta $x^{p^r} \in H$ per cui, poichè H è un p-gruppo, esiste $l > 0$ tale che $e = (x^{p^r})^{p^l} = (x^{p^{r+l}})$, così x ha per periodo una potenza di p e G risulta essere un p-gruppo. □

Lemma 2.2.2. *Siano p un primo e G un gruppo finito. G è un p-gruppo se e solo se $|G| = p^r$ con $r \in \mathbb{N}$.*

Dimostrazione. (Necessità) Supponiamo che q primo divida $|G|$ allora (per il Teorema di Cauchy 2.1.6) esiste un elemento $x \in G$ avente periodo q, ma G è un p-gruppo quindi ogni suo elemento ha per periodo una potenza di p, da cui $q = p$. Ciò ci dice che $|G|$ è una potenza di p.
(Sufficienza) Se $|G| = p^r$ con $r \in \mathbb{N}$ allora (per il Teorema di Lagrange) ogni sottogruppo di G ha ordine che divide l'ordine di G. Ciò significa che ogni suo sottogruppo ha come ordine una potenza di p perciò per ogni $g \in G, |g| = |\langle g \rangle|$ è una potenza di p. Da ciò G è un p-gruppo. □

Un primo risultato veramente interessante è il seguente:

Teorema 2.2.3. *Se G è un p-gruppo non banale allora $Z(G)$ è non banale.*

Dimostrazione. Se G è un p-gruppo non banale allora p divide $|G|$. Per l'equazione delle classi si ha $|G| = |Z(G)| + \sum_{i=1}^{t} |G : C_G(x_i)|$ dove $|G : C_G(x_i)| > 1$. Per il Teorema di Lagrange $|G : C_G(x_i)| \big| |G|$. D'altra parte, poichè $|G : C_G(x_i)| > 1$, $p \big| |G : C_G(x_i)|$, ma allora $p \big| (|G| - \sum_{i=1}^{t} |G : C_G(x_i)|) = |Z(G)|$. $p \big| |Z(G)|$, $|Z(G)| \geqslant 1$, perchè $e \in Z(G)$, da cui $|Z(G)| \geqslant p$ quindi $Z(G)$ è non banale. □

Corollario 2.2.4. *Ogni gruppo di ordine p^n ha sottogruppi normali di ordine p^m per ogni $m \in \mathbb{N}, m < n$.*

Dimostrazione. Per induzione sull'esponente n. Sia G un gruppo di ordine p^n. Il caso $n = 0$ è banale: basta considerare $G = \{e\}$ che è anche l'unico sottogruppo di G. Sia $n > 0$. G è un p-gruppo necessariamente non banale perciò $Z(G)$ è un p-sottogruppo di G non banale, $p\big||Z(G)|$ esiste quindi, per il Teorema di Cauchy, un elemento $g \in Z(G)$ tale che $|g| = p$. Osservando che $\langle g\rangle$ è un sottogruppo normale di G, si ha che $G/\langle g\rangle$ è un p-gruppo avente ordine p^{n-1}, così, usando l'ipotesi induttiva, poichè $H/\langle g\rangle \trianglelefteq G/\langle g\rangle$ se e solo se $H \trianglelefteq G$ e $H \geqslant \langle g\rangle$, il corollario rimane dimostrato perchè per ogni $m \in \mathbb{N}, m < n-1$ esiste un sottogruppo $H/\langle g\rangle \trianglelefteq G/\langle g\rangle$ di ordine p^m, ma allora $H \trianglelefteq G$ e $|H| = p^{m+1}$. Rimane da vedere se c'è un sottogruppo normale di ordine 1, ma $\{e\}$ risolve questo problema. □

Lemma 2.2.5. *G è un gruppo abeliano se e solo se esiste un sottogruppo H di $Z(G)$ tale che G/H sia ciclico.*

Dimostrazione. La necessità è banale perchè in tal caso $G = Z(G)$ e se consideriamo $H = Z(G) = G, G/H$ è necessariamente ciclico. Vediamo ora la sufficienza che è il risultato veramente interessante. Per la ciclicità di G/H ogni elemento di G è del tipo $g = x^i h$ con $h \in H$ e x un elemento fissato di G tale che $G/H = \langle xH\rangle$. Siano $g, \tilde{g} \in G$ con $g = x^i h$, $\tilde{g} = x^j k$. Allora $g\tilde{g} = x^i h x^j k = (h \in H \leqslant Z(G))\ x^i x^j hk = (h \in H \leqslant Z(G))\ x^{i+j}kh =$(commutatività in $\mathbb{Z}$) $x^{j+i}kh = x^j x^i kh = (h, k \in H \leqslant Z(G))\ x^j k x^i h = \tilde{g}g$. □

Corollario 2.2.6. *Sia G un gruppo finito di ordine p^2 allora G è ciclico oppure G è isomorfo al prodotto diretto di due sottogruppi ciclici di ordine p. In particolare $G \cong \mathbb{Z}_{p^2}$ oppure $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

Dimostrazione. G è un p-gruppo non banale di ordine p^2 così $Z(G)$ è un sottogruppo non banale di G, da ciò $|Z(G)| = p$ oppure p^2 quindi $|G/Z(G)| = 1$ oppure p. In ogni caso $G/Z(G)$ ciclico e quindi G è abeliano per il lemma 2.2.5. Se G ciclico non c'è più nulla da dimostrare, supponiamo allora G non ciclico. Sia $x \in G, x \neq e$. Poichè $|x|\big||G|$ segue che $|x| = p$ (se infatti $|x| = p^2$ si avrebbe che G è ciclico, contro le l'ipotesi appena fatta). Sia $y \notin \langle x\rangle$ allora

$|y| = p$, $\langle x\rangle \cap \langle y\rangle = \{e\}$ e $G = \langle x, y\rangle$ per cui $G \cong \langle x\rangle \times \langle y\rangle$ da cui G è isomorfo al prodotto diretto di 2 sottogruppi di ordine p. Provato ciò il rimanente è banale: nel caso $G = \langle x\rangle$ l'isomorfismo è $x \mapsto 1_{p^2}$, nel caso $G \cong \langle x\rangle \times \langle y\rangle$ l'isomorfismo è $xy \mapsto (x, y) \mapsto (1_p, 1_p)$. □

2.3 Primo Teorema di Sylow

Lemma 2.3.1. *Siano G un gruppo finito e H un suo p-sottogruppo, allora $|N_G(H) : H| \equiv |G : H| (mod\ p)$.*

Dimostrazione. Sia X l'insieme dei laterali sinistri di H in G, allora $|X| = |G : H|$. Consideriamo l'azione di H su X data dalla traslazione sinistra $(h, gH) \mapsto hgH$ e vediamo chi è X_0. $xH \in X_0 \Leftrightarrow hxH = xH$ per ogni $h \in H \Leftrightarrow x^{-1}hxH = H$ per ogni $h \in H \Leftrightarrow x^{-1}hx \in H$ per ogni $h \in H \Leftrightarrow x^{-1}Hx \subseteq H \overset{(*)}{\Leftrightarrow} x^{-1}Hx = H \Leftrightarrow x \in N_G(H)$. La coimplicazione $\overset{(*)}{\Leftrightarrow}$ è stata ottenuta in questo modo: ($\Leftarrow$) banale, ($\Rightarrow$) $x^{-1}Hx \subseteq H$ e $x^{-1}Hx \leqslant H$, d'altra parte $|x^{-1}Hx| = |H|$ quindi $x^{-1}Hx = H$. Con la catena di coimplicazioni abbiamo visto $xH \in X_0$ se e solo se $x \in N_G(H)$, allora $|X_0| = |N_G(H) : H|$. Perciò partendo dal Lemma 2.1.5 $|X| \equiv |X_0|$ $(mod\ p)$ e riassemblando quanto finora visto abbiamo $|G : H| \equiv |N_G(H) : H|$ $(mod\ p)$. □

Corollario 2.3.2. *Siano G un gruppo finito e H un suo p-sottogruppo tale che p divide $|G : H|$ allora $H \neq N_G(H)$.*

Dimostrazione. Per il lemma 2.3.1, $|N_G(H) : H| \equiv |G : H| (mod\ p)$, ma, poichè $p \big| |G : H|$, $|N_G(H) : H| \equiv 0$ $(mod\ p)$. Poichè $|N_G(H) : H| \geqslant 1$ si ha che $p \big| |N_G(H) : H|$, risulta quindi $N_G(H) \neq H$. □

Dopo queste due ulteriori premesse possiamo vedere il Primo Teorema di Sylow che dice che non solo per ogni primo che divide l'ordine di un gruppo finito esiste un sottogruppo avente ordine uguale a tale primo (Teorema di Cauchy (2.1.6)), ma aggiunge che per ogni potenza del primo considerato che

divide l'ordine del gruppo, esiste un sottogruppo avente tale potenza come ordine.

Teorema 2.3.3 (Primo Teorema di Sylow)**.** *Sia G un gruppo finito e siano p un primo e r un naturale tali che p^r divide $|G|$ allora esiste $H \leqslant G$ tale che $|H| = p^r$.*

Daremo tre dimostrazioni: le prime due direttamente in questo paragrafo, la terza che è un po' più articolata, ma certamente più spettacolare, nella sezione successiva.

Prima dimostrazione.
Sia $|G| = m$ e sia p^n la massima potenza di p che divide m. La dimostrazione è per induzione su m. Se $m = 1$ l'enunciato è banalmente verificato. Sia $m > 1$. Dall'equazione delle classi si ha $|G| = |Z(G)| + \sum_{i=1}^{t} |G : C_G(x_i)|$. Ora, se esiste un indice i per cui p non divide $|G : C_G(x_i)|$, per il Teorema di Lagrange, p^n deve necessariamente dividere $|C_G(x_i)|$. D'altra parte, essendo $|G : C_G(x_i)| > 1$ e $|C_G(x_i)| < |G|$, usando l'ipotesi induttiva si trovano i sottogruppi cercati. Rimane solo da considerare il caso in cui p divida $|G : C_G(x_i)|$ per ogni $i = 1, \ldots, t$. In tal caso p deve necessariamente dividere anche $|Z(G)|$, così, applicando il Teorema di Cauchy a $Z(G)$, si trova un elemento $x \in Z(G)$ di periodo p. Essendo $x \in Z(G)$, si ha che $\langle x \rangle \trianglelefteq G$, ma allora si può considerare il gruppo quoziente $G/\langle x \rangle$ che ha necessariamente ordine $p^{n-1}m$. Applicando l'ipotesi induttiva si vede che per ogni potenza p^j, con $0 \leqslant j < n$, che divide l'ordine di $G/\langle x \rangle$, esiste un sottogruppo $H_{j+1}/\langle x \rangle$ di $G/\langle x \rangle$ avente ordine p^j, da cui $H_{j+1} \leqslant G$ ha ordine p^{j+1}. Ma allora per ogni potenza p^r di p, con $0 < r \leqslant n$, esiste un sottogruppo H_r di G, avente ordine p^r. Inoltre $\{e\}$ è un sottogruppo di ordine $p^0 = 1$, allora l'enunciato è provato. □

Seconda dimostrazione.
Basta mostrare che esiste un sottogruppo di ordine la massima potenza di p che divide $|G|$ perchè il corollario 2.2.4 farà il resto. Sia $|G| = p^n m, (p, m) =$

1. Sia X la famiglia di sottoinsiemi di G aventi p^n elementi, e si consideri la seguente azione di G su X:

$$G \times X \to X, (g, S) \mapsto gS = \{gs \mid s \in S\}.$$

Sia $S \in X$ e sia $H = \text{Stab}(S) = \{g \in G \mid gS = S\}$. Sia $s_0 \in S$; la mappa definita da:

$$H \to S, h \mapsto hs_0$$

è ben definita, perchè $H = \text{Stab}(S)$, ed è iniettiva, perchè, per la legge di cancellazione in G, $hs_0 = ks_0$ implica $h = k$. Da ciò risulta che $|H| \leqslant |S| = p^n$. Se esiste un $S \in X$ tale che p non divide l'ordine dell'orbita di S abbiamo, per il Teorema di Lagrange e ricordando che $|\bar{S}| = |G : H|$, che p^n divide $|H|$, ma allora, essendo $p^n \leqslant |H| \leqslant p^n$, si ha che $|H| = p^n$ e abbiamo concluso. Quindi ciò che si vuole fare è trovare un'orbita di X che non abbia ordine divisibile per p, dopo di che si prenderà un suo elemento e lo stabilizzatore di tale elemento sarà il sottogruppo da cercato.
Usando un po' di combinatoria abbiamo:

$$|X| = \binom{p^n m}{p^n} = \frac{(p^n m)(p^n m - 1) \cdots (p^n m - p^n + 1)}{p^n (p^n - 1) \cdots (p^n - p^n + 1)}$$

Il perchè della scrittura del denominatore della frazione si capirà tra pochissimo. Preso $0 \leqslant i < p^n$, una potenza p^j di p ($j < n$) divide $p^n m - i$ se e solo se divide i e in modo analogo divide $p^n - i$ se e solo se divide i. Perciò tutti i termini al numeratore e al denominatore hanno, come divisori, le stesse potenze di p, da cui $|X|$ non è divisibile per p. $|X| = \sum_{i=1}^{t} |\bar{S}_i|$ dove $\bar{S}_i$ sono orbite a due a due distinte la cui unione è X. Poichè p non divide X, esiste i tale che p non divide $|\bar{S}_i|$. Si è, allora, trovato ciò che si cercava. □

2.4 Terza dimostrazione del Primo Teorema di Sylow

Cominciamo a costruire tutto il necessario per la terza dimostrazione.

Osservazione 11. Si consideri $GL_n(\mathbb{F}_p)$, ove $\mathbb{F}_p$ è il campo con p elementi. L'ordine di $GL_n(\mathbb{F}_p)$ è $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$.

La dimostrazione è banale, poco più che un po' di applicazione del calcolo combinatorio, ma per pignoleria e per completezza, verrà lo stesso fatta.

Dimostrazione. Una matrice $A \in GL_n(\mathbb{F}_p)$ se e solo se le sue colonne costituiscono una base di $(\mathbb{F}_p)^n$ cioè se e solo se le sue colonne sono n vettori di $(\mathbb{F}_p)^n$ linearmente indipendenti. Da ciò abbiamo che la prima colonna può essere un qualsiasi vettore non nullo di $(\mathbb{F}_p)^n$, di cui ne contiamo p^n-1, la seconda colonna può essere un vettore qualsiasi che non si trovi nel sottospazio generato dal vettore nella prima colonna, e ne contiamo p^n-p, la terza colonna può essere in vettore qualsiasi che non sia nel sottospazio generato dai vettori delle prime due colonne, e ce ne sono p^n-p^2, e così via. Abbiamo quindi trovato che l'ordine di $GL_n(\mathbb{F}_p)$, per il principio moltiplicativo, è $(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$. □

Osservazione 12. L'insieme U delle matrici di $GL_n(\mathbb{F}_p)$ della forma

$$\begin{pmatrix} 1 & * & * & \dots & * \\ 0 & 1 & * & \dots & * \\ 0 & 0 & 1 & \dots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

è un sottogruppo di $GL_n(\mathbb{F}_p)$ avente ordine $p^{n-1}p^{n-2}\cdots p$. In particolare $|U|$ è la massima potenza di p che divide $|GL_n(\mathbb{F}_p)|$.

La verifica del fatto che U è un sottogruppo di $GL_n(\mathbb{F}_p)$ è veramente immediata e verrà pertanto omessa, la verifica dell'ordine di U si ottiene ripetendo pedissequamente la dimostrazione della osservazione precedente.

Osservazione 13. Sia G un gruppo finito di ordine n; allora G è isomorfo a un sottogruppo di $GL_n(\mathbb{F}_p)$.

Dimostrazione. Per il Teorema di Cayley, G è isomorfo a un sottogruppo di S_n. La mappa $S_n \to GL_n(\mathbb{F}_p)$ definita da $\sigma \mapsto I(\sigma)$ (dove $I(\sigma)$ è la matrice

identità a cui abbiamo permutato le colonne attraverso la permutazione σ) è un omomorfismo di gruppi, perchè $I(\sigma\sigma') = I(\sigma)I(\sigma')$, ed è iniettiva, perchè σ è una biezione, perciò S_n è isomorfo a un sottogruppo di $GL_n(\mathbb{F}_p)$. Da ciò, riassemblando quanto finora detto, G è isomorfo a un sottogruppo di $GL_n(\mathbb{F}_p)$. □

Definizione 2.3. Sia G un gruppo e siano $H, K \leqslant G$. Si denota con $\sim_{H,K}$ la relazione binaria su G definita in questo modo:

$$x \sim_{H,K} y \Leftrightarrow \ y = hxk \text{ con } h \in H, k \in K.$$

Osservazione 14. La relazione sopra definita è una relazione di equivalenza

Definizione 2.4. La classe di equivalenza di x rispetto alla relazione $\sim_{H,K}$ viene indicata con HxK e viene detto laterale doppio di H e K in G determinato da x.

Osservazione 15. $HxK = \{hxk \mid h \in H, k \in K\}$.

Lemma 2.4.1. *Sia G un gruppo finito e siano H, K sottogruppi di G. Per ogni $x \in G$ risulta:*

$$|HxK| = \frac{|H||K|}{|H^x \cap K|}.$$

In particolare

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Dimostrazione. Si consideri l'applicazione

$$f : H \times K \to HK, (h, k) \mapsto hk$$

che è banalmente suriettiva. Si consideri, poi, la relazione di equivalenza R_f su $H \times K$ determinata da f, cioè $(h, k)R_f(h_0, k_0)$ se e solo se $f(h, k) = f(h_0, k_0)$ cioè se e solo se $hk = h_0k_0$. Sia $(h, k)R_f(h_0, k_0)$ e sia $y = h_0^{-1}h = k_0k^{-1}$. Si ha che $y \in H \cap K$ e $(h_0, k_0) = (hy^{-1}, yk)$, ma ogni coppia del tipo (hy^{-1}, yk) con $y \in H \cap K$ è ovviamente in relazione con la coppia (h, k) e appartengono quindi alla stessa classe di equivalenza che ha perciò ordine pari

all'ordine dell'intersezione di H e K, cioè $|[(h,k)]_{\sim_{H,K}}| = |H \cap K|$. Poichè f è suriettiva risulta che $H \times K/R_f$ è equipotente a HK, così $|HK| = |H \times K/R_f| = \frac{|H \times K|}{|H \cap K|} = \frac{|H||K|}{|H \cap K|}$. Il caso particolare è quindi dimostrato. Rimane ora da vedere il caso generale. L'applicazione

$$\theta : HxK \to H^x K, hxk \mapsto (x^{-1}hx)k$$

è ben definita e biettiva infatti $(x^{-1}hx)k = (x^{-1}h_0x)k_0$ se e solo se, per la legge di cancellazione, $hxk = h_0xk_0$ e la suriettività è immediata. Allora $|HxK| = |H^xK|$ da cui $|HxK| = |H^xK| = \frac{|H^x||K|}{|H^x \cap K|} = \frac{|H||K|}{|H^x \cap K|}$, quindi il teorema è dimostrato. □

Teorema 2.4.2. *Sia G un gruppo finito di ordine $p^n m$, ove $(m,p) = 1$ e sia $P \leqslant G$ con $|P| = p^n$. Allora per ogni sottogruppo H di G esiste un elemento $x \in G$ tale che $H \cap xPx^{-1}$ è un sottogruppo di H tale che $H \cap xPx^{-1}$ ha come ordine la massima potenza di p che divide l'ordine di H.*

Dimostrazione. Essendo $\sim_{P,H}$ una relazione di equivalenza, l'insieme dei laterali doppi di P e H costituisce una partizione di G; allora esistono degli elementi $x_1, \ldots, x_t$ tali che $|G| = \sum_{i=1}^{t} |Px_iH| = \sum_{i=1}^{t} \frac{|P||H|}{|P^{x_i} \cap H|}$ da cui $\frac{|G|}{|P|} = \sum_{i=1}^{t} \frac{|H|}{|P^{x_i} \cap H|}$. Ora p non divide $\frac{|G|}{|P|}$, poichè l'ordine di P è la massima potenza di p che divide l'ordine di G, così esiste un indice i tale che p non divide $\frac{|H|}{|P^{x_i} \cap H|}$. Da ciò si ottiene che l'ordine di $P^{x_i} \cap H$, che è necessariamente 1 oppure una potenza di p (perchè $|P| = p^n$), è la massima potenza di p che divide l'ordine di H. □

Ora abbiamo finalmente tutto il materiale necessario per vedere la terza dimostrazione del Primo Teorema di Sylow.

Terza dimostrazione.
G è isomorfo a un sottogruppo L di $GL_n(\mathbb{F}_p)$; il sottogruppo U di $GL_n(\mathbb{F}_p)$ definito nella osservazione 12 ha ordine pari alla massima potenza di p che divide l'ordine di $GL_n(\mathbb{F}_p)$, perciò per il teorema 2.4.2 esiste un elemento $x \in GL_n(\mathbb{F}_p)$ tale che $L \cap xUx^{-1}$ ha per ordine la massima potenza di p che

divide l'ordine di L. Allora, poichè G è isomorfo a L, esiste un sottogruppo di G il cui ordine è la massima potenza di p che divide $|G|$ così per il corollario 2.2.4, per ogni potenza di p che divide $|G|$ esiste un sottogruppo di G con tale ordine. □

Se non si può trovare un sottogruppo di ordine d per ogni divisore positivo d dell'ordine di un generico gruppo finito, con i p-gruppi le cose funzionano ancora bene infatti, riformulando il corollario 2.2.4 con il linguaggio prima imparato si ha il seguente:

Corollario 2.4.3. *Sia G un p-gruppo. Per ogni divisore positivo d che divide l'ordine di G, esiste un sottogruppo H di G tale che $|H| = d$.*

Capitolo 3

Secondo e Terzo Teorema di Sylow

Nel primo teorema di Sylow si è mostrato che per ogni potenza di un numero primo p che divide l'ordine di un gruppo G esiste un sottogruppo di G di ordine tale potenza, e, con il corollario 2.2.4, si è visto che i sottogruppi di ordine la massima potenza del primo p rivestono un ruolo privilegiato. D'altra parte preso un generico primo p esiste sempre un p-sottogruppo di G che, nel peggiore dei casi è $\{e\}$. Sorgono quindi spontanee due domande:

1. Che cosa possiamo dire dei sottogruppi di ordine la massima potenza di un numero primo che divide l'ordine di un gruppo finito?

2. Che cosa possiamo dire dei p-gruppi massimali per l'inclusione in p-sottogruppi cioè di quei sottogruppi che non sono contenuti propriamente in alcun altro p-sottogruppo del gruppo considerato?

Vedremo che la risposta alle due domande è la stessa perchè, nel caso dei gruppi finiti, i p-sottogruppi massimali e i p-sottogruppi di ordine la massima potenza di p che divide l'ordine del gruppo coincidono.

3.1 p - sottogruppi di Sylow e Secondo Teorema di Sylow

Definizione 3.1 (p-sottogruppi di Sylow)**.** Sia dato un gruppo G e sia p un primo, si dice che un p-sottogruppo H di G è un p-sottogruppo di Sylow se e solo se H è un elemento massimale dell'insieme dei p-sottogruppi di G con l'ordinamento dato dall'inclusione, cioè se e solo se non esistono p-sottogruppi di G che lo contengano propriamente.

Osservazione 16. Se G è un p-gruppo, banalmente è anche l'unico p-sottogruppo di Sylow di G.

Teorema 3.1.1. *Sia G un gruppo, e siano p un primo e H un p-sottogruppo di G. Allora H è incluso in qualche p-sottogruppo di Sylow di G. In particolare, ogni gruppo G è dotato di p-sottogruppi di Sylow.*

Dimostrazione. Sia Γ l'insieme dei p-sottogruppi di G contenenti H. Γ è non vuoto perchè H ne è un elemento per ipotesi, inoltre, dotando Γ dell'inclusione insiemistica, $(\Gamma, \subseteq)$ è un insieme ordinato. Sia Σ un sottoinsieme totalmente ordinato di Γ e sia $S = \bigcup_{K \in \Sigma} K$. Se $x_1, x_2 \in S$, allora esistono in Σ due p-sottogruppi di G, K_1 e K_2, tali che $x_1 \in K_1$ e $x_2 \in K_2$, ma, essendo Σ totalmente ordinato, avremo $K_1 \subseteq K_2$ o $K_2 \subseteq K_1$. Per fissare le idee, supponiamo $K_1 \subseteq K_2$. x_1, x_2 sono allora elementi di K_2 e quindi, poichè K_2 è un sottogruppo di G, anche $x_1^{-1}x_2 \in K_2 \subseteq S$. Abbiamo quindi visto che S è un sottogruppo di G. Ogni elemento di S ha come periodo una potenza di p perchè appartiene a qualche p-sottogruppo di G, perciò S è necessariamente un p-sottogruppo di G. In modo banale si osserva anche che $H \subseteq S$, da cui segue che S è un elemento maggiorante di Σ in Γ. L'insieme ordinato $(\Gamma, \subseteq)$ è, così, un insieme induttivo, e, per il Lemma di Zorn, Γ ammette un elemento massimale, P, che è proprio il p-sottogruppo di Sylow che cercavamo. Infatti, se esistesse un altro p-sottogruppo di G, P_0 contenente H e P, dalla massimalità di P avremmo che $P_0 = P$.

La parte rimanente dell'enunciato deriva, poi, dal fatto che ogni gruppo ha sempre almeno un p-sottogruppo che, nel peggiore dei casi, sarà $\{e\}$. □

Osservazione 17. Si osservi che il teorema precedente vale per gruppi qualsiasi e non solo per gruppi necessariamente finiti.

Teorema 3.1.2 (Secondo Teorema di Sylow)**.** *Siano p un primo e G un gruppo finito. Allora due qualunque p-sottogruppi di Sylow di G sono coniugati.*

Dimostrazione. Il primo teorema di Sylow (teorema 2.3.3) garantisce l'esistenza di un sottogruppo P di G avente per ordine la massima potenza di p che divide $|G|$. Ora, per il Lemma 2.2.2, P è necessariamente un p-sottogruppo e, per il Teorema di Lagrange, è anche un p-sottogruppo di Sylow. Consideriamo un altro p-sottogruppo di Sylow H di G. L'insieme dei laterali doppi di P e H in G costituisce una partizione di G, allora, dal fatto che G è un gruppo finito, esistono $x_1, \ldots, x_r \in G$ tali che $G = \bigcup_{i=1}^{r} Px_iH$ con $Px_iH \cap Px_jH = \varnothing$ per ogni $i \neq j$. Avremo quindi $|G| = \sum_{i=1}^{r} |Px_iH|$ cioè, usando il Lemma 2.4.1,

$$|G| = \sum_{i=1}^{r} \frac{|P||H|}{|P^{x_i} \cap H|}$$

da cui

$$\frac{|G|}{|P|} = \sum_{i=1}^{r} \frac{|H|}{|P^{x_i} \cap H|}.$$

Per l'ipotesi fatta su P, $\frac{|G|}{|P|}$ non è divisibile per p, allora poichè $|H|$ è una potenza di p, essendo un p-sottogruppo, e $|P^{x_i} \cap H|$ è pure una potenza di p, in quanto ordine di un sottogruppo di H, esiste un indice j tale che $\frac{|H|}{|P^{x_j} \cap H|}$ non è divisibile per p, così $H = P^{x_j} \cap H$ che significa $H \leqslant P^{x_j}$. Questo fatto, unitamente al fatto che H è un p-sottogruppo di Sylow, ci dice che $H = P^{x_j}$. L'enunciato segue, poi, dal fatto che la relazione di coniugio è transitiva. □

Il secondo teorema di Sylow non è estendibile al caso di gruppi infiniti come mostra la seguente osservazione.

Osservazione 18. Si considerino i gruppi $G_i = \langle (1\ 3), (1\ 2\ 3)\rangle = S_3$ e i loro sottogruppi $M_i = \langle (1\ 3)\rangle$ e $N_i = \langle (1\ 3)^{(1\ 2\ 3)}\rangle$ per ogni $i \geqslant 1$; allora $M = Dr_{i\geqslant 1}M_i$ e $N = Dr_{i\geqslant 1}N_i$ sono 2-sottogruppi di Sylow non coniugati di $G = Dr_{i\geqslant 1}G_i$.

Dimostrazione. Osserviamo che $(1\ 3)^{(1\ 2\ 3)} = (1\ 2\ 3)(1\ 3)(1\ 2\ 3)^{-1} = (1\ 2)$ da cui $N_i = \langle (1\ 2)\rangle = \{e, (1\ 2)\}$. M e N sono banalmente 2-sottogruppi di G e sono anche massimali per la relazione di inclusione. Vediamo la massimalità di M, la dimostrazione per N è del tutto analoga. Supponiamo per assurdo che M non sia massimale per la relazione di inclusione; allora esistono un 2-sottogruppo H di G ed un indice j tale che la j-esima proiezione, H_j, di H ha tra i suoi elementi almeno un altro ciclo di ordine 2 di $G_j = S_3$ che chiamiamo $(a\ b)$. H_j deve necessariamente avere come suo elemento anche il prodotto $(1\ 3)(a\ b)$, ma tale prodotto è un ciclo di ordine 3 con il risultato che $H_j = S_3$ e quindi H non è più un 2-sottogruppo, il che è assurdo essendo H un 2-sottogruppo per ipotesi. Inoltre M e N non sono coniugati, infatti se fossero coniugati esisterebbe un elemento $g \in G$ tale che $gMg^{-1} = N$ e si avrebbe quindi che $g_iM_ig_i^{-1} = N_i$ per ogni indice i. D'altra parte, per ogni indice j, in M esiste un elemento avente $(1\ 3)$ come proiezione j-esima e l'elemento neutro nelle posizioni relative a tutti gli altri indici con la conseguenza che $g_j(1\ 3)g_j^{-1} \in N_j$. Ma $(1\ 3)$ non sta in N_j così g_j deve essere necessariamente diverso dall'elemento neutro. Allora le proiezioni di g dovrebbero essere tutte diverse dall'elemento neutro, il che non è possibile poichè $g \in G$. □

Le cose, tuttavia, non funzionano male per tutti i gruppi infiniti. Con una dimostrazione analoga alla precedente si prova il seguente enunciato:

Osservazione 19. Tutti i p-sottogruppi di Sylow di $Cr_{i\geqslant 1}G_i$ (con i G_i definiti come sopra) sono coniugati.

Corollario 3.1.3. *Siano p un primo e G un gruppo finito. Allora i p-sottogruppi di Sylow di G sono tutti e soli i p-sottogruppi di G aventi per ordine la massima potenza di p che divide l'ordine di G.*

Dimostrazione. Per il Teorema di Lagrange, tutti i p-sottogruppi di G aventi per ordine la massima potenza di p che divide l'ordine di G sono massimali per l'inclusione nell'insieme dei p-sottogruppi di G, allora sono p-sottogruppi di Sylow di G. Mostriamo ora il viceversa. Sia, ora, H un p-sottogruppo di Sylow di G e sia P come nella dimostrazione al secondo teorema di Sylow. P e H sono coniugati in quanto p-sottogruppi di Sylow, ma essendo coniugati hanno lo stesso ordine così H ha per ordine la massima potenza di p che divide $|G|$. □

Osservazione 20. Sia G un gruppo finito. I coniugati di un p-sottogruppo di Sylow di G sono tutti e soli i p-sottogruppi di Sylow di G.

Dimostrazione. Sia H un p-sottogruppo di Sylow di G. Se K è un altro p-sottogruppo di Sylow di G, allora, per il secondo teorema di Sylow, K e H sono coniugati. D'altra parte, se E è un altro elemento della classe di coniugio di H, si ha che $|E| = |H|$ è la massima potenza di p che divide l'ordine di G, allora, per il corollario 3.1.3, E è un sottogruppo di Sylow. □

Per questioni notazionali indicheremo con $Syl_p(G)$ l'insieme dei p-sottogruppi di Sylow di G. Vediamo ora altri tre corollari del secondo teorema di Sylow.

Corollario 3.1.4. *Siano p un primo e G un gruppo finito. Allora il numero dei p-sottogruppi di Sylow di G divide l'ordine del gruppo G.*

Dimostrazione. L'insieme dei p-sottogruppi di Sylow di G, per l'osservazione 20, è una classe di coniugio. Da ciò risulta, per il corollario 1.0.8, che $|Syl_p(G)| = |G : N_G(P)|$ (con $P \in Syl_p(G)$) così $|Syl_p(G)|$ divide $|G|$. □

Corollario 3.1.5. *Siano p un primo e G un gruppo finito. Allora un p-sottogruppo di Sylow di G è normale in G se e solo se è l'unico p-sottogruppo di Sylow di G.*

Dimostrazione. $H \trianglelefteq G$ se e solo se è l'unico elemento della sua classe di coniugio. Da ciò, essendo $Syl_p(G)$ una classe di coniugio, si ha l'enunciato. □

Corollario 3.1.6. *Siano p un primo, G un gruppo finito e P un p-sottogruppo di Sylow di G. Allora $N_G(N_G(P)) = N_G(P)$.*

Dimostrazione. Indicando $N = N_G(P)$, ciò che dobbiamo dimostrare, nella nuova notazione, è $N_G(N) = N$. Banalmente abbiamo $N \leqslant N_G(N)$ quindi ciò che dobbiamo realmente dimostrare è $N_G(N) \leqslant N$. Sia $g \in N_G(N)$, per definizione $gNg^{-1} = N$, allora, poichè $P \leqslant N$, $gPg^{-1} \leqslant N$, ma $P \trianglelefteq N$ così, per il corollario 3.1.5, $gPg^{-1} = P$ perciò $g \in N$ e l'enunciato è dimostrato. □

3.2 Terzo Teorema di Sylow

Una volta aver osservato che in un gruppo esistono sempre dei p-sottogruppi di Sylow, risulta naturale chiedersi quanti ce ne siano. Il corollario 3.1.4 ci ha già dato una prima informazione per quello che riguarda i gruppi finiti. Vedremo ora il terzo teorema di Sylow che, sempre nel caso di gruppi finiti, ci dà una ulteriore informazione.

Teorema 3.2.1 (Terzo Teorema di Sylow)**.** *Sia p un primo e G un gruppo finito. Allora il numero dei p-sottogruppi di Sylow di G è della forma $1 + kp$ con k numero intero non negativo.*

Ne daremo due dimostrazioni.

Prima dimostrazione. Sia P un p-sottogruppo di Sylow di G. L'unione dei laterali doppi di P e P rappresentati da elementi di $N_G(P)$ è $N_G(P)$ stesso così, essendo G finito, esistono degli elementi di G, $g_1, \ldots, g_t$, che non sono elementi di $N_G(P)$ tali che $\{N_G(P), Pg_1P, \ldots, Pg_tP\}$ costituisce una partizione di G. Da ciò risulta:

$$|G| = |N_G(P)| + \sum_{i=1}^{t} |Pg_iP|$$

e quindi

$$|Syl_p(G)| = |G : N_G(P)| = \frac{|G|}{|N_G(P)|} = 1 + \frac{\sum_{i=1}^{t} |Pg_iP|}{|N_G(P)|}.$$

da cui, essendo $|Syl_p(G)|$ un numero intero positivo, $\sum_{i=1}^{t} |Pg_iP|$ è divisibile per $|N_G(P)|$. P è un p-sottogruppo di Sylow di G, allora ha per ordine la massima potenza di p che divide $|G|$, sia essa p^n. Per il lemma 2.4.1, $|Pg_iP| = \frac{|P||P|}{|P^{g_i} \cap P|}$, ma $P^{g_i} \neq P$ perchè $g_i \notin N_G(P)$, così $P^{g_i} \cap P$ è un sottogruppo proprio di P e, in quanto tale, ha ordine p^{r_i} con $0 \leqslant r_i < n$. Per quanto appena detto risulta che $|Pg_iP| = p^{2n-r_i}$ ed essendo $2n - r_i \geqslant n+1$ (perchè $r_i < n$) risulta anche che p^{n+1} divide $\sum_{i=1}^{t} |Pg_iP|$ dividendone ogni addendo. D'altra parte la massima potenza di p che divide l'ordine di G è p^n perciò, la massima potenza di p che divide $|N_G(P)|$ è p^n, quindi p divide necessariamente

$$\frac{\sum_{i=1}^{t} |Pg_iP|}{|N_G(P)|},$$

allora $|Syl_p(G)| = 1 + kp$. □

Seconda dimostrazione. Si consideri l'azione di coniugio di P su X, con P un p-sottogruppo di Sylow di G e $X = \{p\text{-sottogruppi di Sylow di } G\}$, e sia X_0 definito come nel lemma 2.1.5. Se $Q \in X_0$, per definizione $gQg^{-1} = Q$ per ogni $g \in P$, allora $P \leqslant N_G(Q)$. D'altra parte $Q \trianglelefteq N_G(Q)$ e sia P che Q sono sottogruppi di Sylow in $N_G(Q)$ essendolo in G ed essendo entrambi in $N_G(Q)$, così, per il secondo teorema di Sylow, P e Q sono coniugati da cui $P = Q$. Dal risultato appena mostrato si ha che $|X_0| = 1$, perciò, per il lemma 2.1.5, $|X| \equiv 1 \ (mod\ p)$ da cui $|Syl_p(G)| = |X| = 1 + kp$ con $k \geqslant 0$ essendo $|X|$ un numero intero positivo. □

3.3 Qualche applicazione del Terzo Teorema di Sylow

Combinando quanto visto nel corollario 3.1.4 e nel terzo teorema di Sylow abbiamo otteniamo che il numero dei p-sottogruppi di Sylow di un gruppo finito dato è soggetto a notevoli restrizioni dovendo dividere l'ordine del gruppo e dovendo essere della forma $1 + kp$ con k numero intero non negativo. Questo ci permette di ottenere due altri risultati interessanti.

Corollario 3.3.1. *Siano p e q due numeri primi distinti e sia G un gruppo di ordine pq. Se $p > q$ e $p \not\equiv 1 \ (mod\ q)$, allora G è un gruppo ciclico.*

Prima di dimostrare questo risultato premettiamo due lemmi.

Lemma 3.3.2. *Sia G un gruppo abeliano finito e siano $H, K \trianglelefteq G$ tali che $G = HK$, con H e K gruppi ciclici aventi ordini coprimi; allora G è ciclico.*

Dimostrazione. H e K sono ciclici quindi esistono $h \in H$ e $k \in K$ tali che $H = \langle h \rangle$ e $K = \langle k \rangle$. Siano inoltre m, n, rispettivamente, gli ordini di H e K. $(hk)^m = k^m$ e $(hk)^n = h^n$, ma, dal fatto che $(m, n) = 1$, risulta che $\langle h^n \rangle = \langle h \rangle$ e $\langle k^m \rangle = \langle k \rangle$ da cui $h, k \in \langle hk \rangle$ così $G = \langle hk \rangle$ e risulta essere ciclico. □

Osservazione 21. L'ipotesi che $|H|$ e $|K|$ siano coprimi è indispensabile infatti se il gruppo finito G è tale che $G = HK$ con H e K due sottogruppi ciclici aventi ordini non coprimi, allora G ha sottogruppi distinti dello stesso ordine perciò (per il teorema 2.1.1) G è necessariamente non ciclico.

Lemma 3.3.3. *Sia G un gruppo abeliano finito di ordine pq, con p e q numeri primi distinti; allora G è un gruppo ciclico.*

Dimostrazione. $|G| = pq > 1$, consideriamo allora $g \in G$ tale che $g \neq e$. Se $\langle g \rangle = G$ non abbiamo più nulla da dimostrare, supponiamo quindi che $\langle g \rangle \neq G$ perciò $|\langle g \rangle| = p$ oppure $|\langle g \rangle| = q$, per fissare le idee poniamo $|\langle g \rangle| = p$. Sia $h \in G \setminus \langle g \rangle$. Si ha che $g \in \langle h \rangle$ oppure $g \notin \langle h \rangle$. Se siamo nel primo caso $G = \langle h \rangle$ e non abbiamo più nulla da dimostrare; allora, supponiamo di essere nel secondo caso. Se $g \notin \langle h \rangle$ allora $\langle g \rangle \cap \langle h \rangle = \{e\}$ e $G = \langle g \rangle \langle h \rangle$ quindi, dal lemma precedente, dovendo necessariamente essere $|\langle h \rangle| = q$, risulta che $G = \langle gh \rangle$ perciò è ciclico. □

Affrontiamo ora la dimostrazione del corollario 3.3.1.

Dimostrazione. Siano P e Q rispettivamente un p-sottogruppo di Sylow e un q-sottogruppo di Sylow di G, allora $|P| = p$ e $|Q| = q$. Dal terzo teorema di Sylow sappiamo che il numero dei p-sottogruppi di Sylow di G è della

forma $1 + kp$ e dal corollario 3.1.4 sappiamo che deve essere un divisore di $|G| = pq$ perciò deve essere un elemento dell'insieme $\{1, p, q, pq\}$. Ora, $|Syl_p(G)| \notin \{p, pq\}$ perchè altrimenti p dovrebbe essere un divisore di 1, e $|Syl_p(G)| \neq q$ perchè $p > q$. Se infatti fosse $1 + kp = q$ avremmo $q = 1$, nel caso in cui $k = 0$, il che non è possibile perchè q è un numero primo, oppure, nel caso $k \geqslant 1$, $q > p$, il che non è possibile per ipotesi. L'unica possibilità è che $|Syl_p(G)| = 1$ cioè, per il corollario 3.1.5, P è un p-sottogruppo di Sylow di G normale in G. In modo analogo sappiamo che $|Syl_q(G)| = 1 + kq$ e che $|Syl_q(G)|$ è un divisore di pq, allora deve essere un elemento dell'insieme $\{1, p, q, pq\}$. $|Syl_q(G)| \notin \{q, pq\}$ perchè altrimenti q divide 1 e $|Syl_q(G)| \neq p$ perchè per ipotesi $p \not\equiv 1 \ (mod\ q)$ da cui $|Syl_q(G)| = 1$ e quindi Q è un q-sottogruppo di Sylow di G normale in G. Chiaramente $P \cap Q = \{e\}$, in quanto e è l'unico elemento avente contemporaneamente per periodo una potenza di p e di q, e $\langle P, Q\rangle = G$ perciò $G = PQ$. D'altra parte P e Q, avendo per ordine un primo, sono gruppi ciclici quindi G è necessariamente abeliano, così per il lemma 3.3.3 G è ciclico. □

Definizione 3.2. Sia G un gruppo e siano $H_1, H_2, \ldots, H_r$ sottogruppi di G. G è **prodotto diretto interno** dei sottogruppi $H_1, H_2, \ldots, H_r$ se la mappa

$$H_1 \times H_2 \times \ldots \times H_r \to G, (h_1, h_2, \ldots, h_r) \mapsto h_1 h_2 \cdots h_r$$

è un isomorfismo di gruppi.

Corollario 3.3.4. *Sia G un gruppo finito avente uno ed un solo p-sottogruppo di Sylow per ogni numero primo p che divide il suo ordine. Allora G è prodotto diretto interno dei suoi p-sottogruppi di Sylow.*

Dimostrazione. Sia $|G| = p_1^{r_1} \cdots p_t^{r_t}$ e siano $P_1, \ldots, P_t$ i p-sottogruppi di Sylow di G per ogni primo p che divide $|G|$. Per ogni indice i, $P_i \trianglelefteq G$, essendo l'unico p_i-sottogruppo di Sylow di G, allora $P_1 \cdots P_t \trianglelefteq G$. Mostriamo innanzitutto, per induzione su s, che $P_1 \times P_2 \times \ldots \times P_s \cong P_1 P_2 \cdots P_s$. Se $s = 1$ non c'è nulla da dimostrare. Supponiamo, quindi, che $P_1 \times P_2 \times \ldots \times P_{s-1} \cong P_1 P_2 \cdots P_{s-1}$ e mostriamo che la mappa $(P_1 P_2 \cdots P_{s-1}) \times P_s \to$

$(P_1P_2\cdots P_{s-1})P_s, (u,v) \mapsto uv$ è un isomorfismo di gruppi. Mostrato ciò risulterà immediato che $P_1 \times P_2 \times \ldots \times P_s \cong P_1P_2\cdots P_s$. Tale mappa è banalmente un omomorfismo di gruppi suriettivo ed è anche iniettivo in quanto $(u,v) \mapsto e$ se e solo se $uv = e$ cioè se e solo se $u = v^{-1}$, ma $(P_1P_2\cdots P_{s-1}) \cap P_s = \{e\}$; allora la mappa è un isomorfismo di gruppi.
Abbiamo, ora, che $|P_1P_2\cdots P_t| = |P_1 \times P_2 \times \cdots \times P_t| = |P_1||P_2|\cdots|P_t| = |G|$, quindi $P_1P_2\cdots P_t = G$ e G è prodotto diretto interno dei P_i. □

Conclusioni

Se all'inizio di questo lavoro avremmo ancora potuto sperare di trovare, per ogni divisore positivo dell'ordine di un gruppo finito, un sottogruppo del gruppo dato avente per ordine tale divisore, ora sappiamo che questa cosa non è vera e un controesempio è dato dal gruppo alterno A_4 che, sebbene sia di ordine 12, non ha alcun sottogruppo di ordine 6. Perciò è necessario rinunciare all'idea di "invertire" totalmente il teorema di Lagrange. Tuttavia ci sono casi particolari in cui tale "inversione" è possibile: è il caso dei gruppi ciclici finiti dove, per ogni divisore dell'ordine del gruppo, si ha anche l'unicità del sottogruppo, ed è anche il caso di tutti i gruppi finiti abeliani e di tutti i p-gruppi, anche se, in questi ultimi due casi, si deve rinunciare all'unicità. Si può, però, ottenere ancora tanto: dato un gruppo finito G, il primo teorema di Sylow garantisce che, per ogni potenza, che divide l'ordine di G, dei divisori primi dell'ordine di G, esistono dei sottogruppi di G aventi per ordine tali potenze. Quindi siamo andati ben oltre al risultato del teorema di Cauchy che permette di trovare, scelto un primo che divide l'ordine del gruppo, un elemento del gruppo (quindi un sottogruppo) avente per periodo (e quindi come ordine del sottogruppo) il primo scelto. D'altra parte in alcune dimostrazioni del primo teorema di Sylow viene messa in risalto l'importanza dei sottogruppi aventi per ordine la massima potenza di un primo che divide l'ordine del gruppo; è stato, allora, naturale chiedersi che ruolo giochino tali sottogruppi e che ruolo giochino i p-sottogruppi massimali per l'inclusione (chiamati p-sottogruppi di Sylow) giungendo a scoprire che nel caso dei gruppi finiti tali sottogruppi sono gli stessi. È stato quindi

inevitabile chiedersi se i p-sottogruppi di Sylow siano sempre presenti in ogni gruppo, se abbiano qualche legame tra loro e quanti ne esistano, scoprendo che non solo esistono sempre nei gruppi finiti (il che viene dato dal primo teorema di Sylow), ma esistono in un qualunque gruppo, che nei gruppi finiti tali sottogruppi sono coniugati e che il numero dei p-sottogruppi di Sylow è vincolato dall'essere un divisore dell'ordine del gruppo (per un corollario del secondo teorema di Sylow) e dall'essere della forma $1 + kp$ con k numero intero non negativo (per il terzo teorema di Sylow).

Bibliografia

[1] Franciosi, S. e De Giovanni, F. (1995) Elementi di Algebra, II edizione, Aracne.

[2] Hungerford, T.W. (1980) Algebra, Springer-Verlag.

[3] Milne, J. (2011) Group Theory, disponibile a www.jmilne.org/math/.