Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

GRUPPI PROFINITI E TEORIA DI SYLOW

Tesi di Laurea in Algebra

Relatrice:
Chiar.ma Prof.ssa
MARTA MORIGI

Presentata da:
LUCA PERINI

Sessione Unica
Anno Accademico 2018/2019

Indice

Introduzione

In questo elaborato si propone una presentazione dei gruppi profiniti, con particolare attenzione al loro rapporto con la teoria di Sylow e di Hall. Formalmente i gruppi profiniti sono gruppi topologici definiti come limiti inversi di gruppi finiti e non sono essi stessi finiti, a eccezione di casi banali. Tuttavia moltissime proprietà dei gruppi profiniti possono essere caratterizzate mediante lo studio dei loro quozienti finiti ed è quindi possibile estendere ad essi numerosi risultati validi nei gruppi finiti, come i celebri teoremi di Sylow e di Hall.

Il primo capitolo si concentra sulla definizione dei gruppi profiniti e sul loro studio in quanto gruppi topologici. A tal fine si propone in primo luogo uno studio dei limiti inversi di generici spazi topologici, per poi enunciare e dimostrare alcuni risultati tecnici utili per la comprensione e lo studio dei gruppi topologici e dei limiti inversi di questi. Si presentano inoltre due risultati riguardanti i quozienti di limiti inversi di gruppi topologici, di seguito sfruttati per fornire un'interessante caratterizzazione dei gruppi profiniti: questi sono tutti e soli i gruppi topologici compatti e totalmente disconnessi.

Nel secondo capitolo sono presentati i teoremi di Sylow e di Hall per i gruppi finiti. Ricordando che il teorema di Lagrange afferma che l'ordine di un sottogruppo divide l'ordine di un gruppo, la teoria di Sylow serve a fornire una risposta, seppure parziale, alla domanda inversa, ovvero se, dato un divisore dell'ordine di un gruppo G, esista un sottogruppo di ordine tale divisore. La risposta a questa domanda non

è sempre affermativa, tuttavia lo diventa in alcuni casi speciali. Il primo teorema di Sylow afferma infatti che se il divisore dell'ordine di G è una potenza di un primo, allora esiste sempre un sottogruppo con ordine tale divisore. In particolare, dato un primo p che divide l'ordine di G, un p-sottogruppo di Sylow di G è un sottogruppo il cui ordine è la più grande potenza di p che divide l'ordine di G.
Nel caso di gruppi risolubili è possibile generalizzare questi risultati. Hall ha infatti dimostrato che se G è un gruppo risolubile di ordine mn con m e n coprimi, allora esiste un sottogruppo di G di ordine m, detto π-sottogruppo di Hall, dove π è l'insieme dei primi che dividono m.

Il terzo e ultimo capitolo consiste in una esposizione di come si possono estendere i risultati sui sottogruppi di gruppi finiti anche ai sottogruppi di gruppi profiniti. In primo luogo si generalizza il concetto di indice di un sottogruppo sfruttando i numeri soprannaturali, dopodiché si dimostra un teorema analogo al teorema di Lagrange per i gruppi profiniti. Successivamente, si estendono ai gruppi profiniti anche i teoremi di Sylow e di Hall visti nel secondo capitolo. In conclusione viene presentato il completamento profinito degli interi, si tratta di un importante esempio di gruppo profinito del quale analizziamo la struttura e i sottogruppi di Sylow.

Capitolo 1

Gruppi profiniti

I gruppi profiniti sono gruppi topologici definiti come limiti inversi di gruppi finiti (considerati con la topologia discreta). Iniziamo questo capitolo con lo studio generale dei limiti inversi di spazi topologici, dopodiché vedremo alcuni risultati sui gruppi topologici e per finire studieremo i gruppi profiniti, dei quali vedremo una caratterizzazione di particolare interesse: i gruppi profiniti sono tutti e soli i gruppi topologici compatti e totalmente disconnessi.

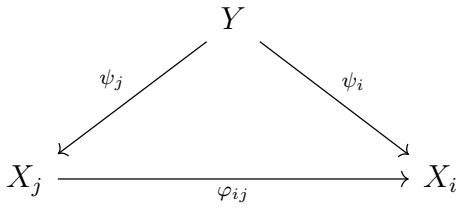
1.1 Limiti inversi

Un *insieme diretto* è un insieme parzialmente ordinato I tale che per ogni $i_1, i_2 \in I$ esiste un elemento $j \in I$ tale che $i_1 \leq j$ e $i_2 \leq j$.

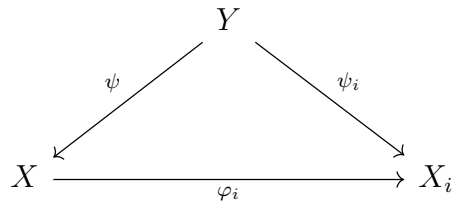
Definizione 1.1. Un *sistema inverso* (X_i, φ_{ij}) di spazi topologici indicizzati da un insieme diretto I consiste in una famiglia $(X_i \mid i \in I)$ di spazi topologici e una famiglia $(\varphi_{ij} : X_j \to X_i \mid i, j \in I,\ i \leq j)$ di mappe continue tali che φ_{ii} è la mappa identica per ogni i e $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$ per ogni $i \leq j \leq k$.

Gli insiemi per cui non specifichiamo la topologia saranno considerati con la topologia discreta. Se ogni X_i è un gruppo topologico e ogni φ_{ij} è un omomorfismo continuo allora (X_i, φ_{ij}) è un sistema inverso di gruppi topologici.

Dati un sistema inverso di spazi topologici (X_i, φ_{ij}) e uno spazio topologico Y, diciamo che una famiglia $(\psi_i : Y \to X_i \mid i \in I)$ di mappe continue è *compatibile* se $\varphi_{ij}\psi_j = \psi_i$ per ogni $i \leq j$. Equivalentemente si può esprimere questa condizione anche con la richiesta che ciascuno dei seguenti diagrammi sia commutativo.



Definizione 1.2. Un *limite inverso* (X, φ_i) di un sistema inverso (X_i, φ_{ij}) di spazi topologici (rispettivamente gruppi topologici) è uno spazio topologico (rispettivamente gruppo topologico) X con una famiglia di mappe continue (rispettivamente omomorfismi continui) compatibili $(\varphi_i : X \to X_i)$ con la seguente proprietà universale: se $(\psi_i : Y \to X_i)$ è una famiglia compatibile di mappe continue da uno spazio Y (rispettivamente omomorfismi continui da un gruppo Y), allora esiste un'unica mappa continua (rispettivamente omomorfismo continuo) $\psi : Y \to X$ tale che $\varphi_i\psi = \psi_i$ per ogni i.
Cioè richiediamo che ci sia un' unica ψ tale che ciascuno dei seguenti diagrammi sia commutativo.



Mostriamo ora l'esistenza e unicità dei limiti inversi.

Teorema 1.3. *Sia (X_i, φ_{ij}) un sistema inverso indicizzato da I.*

1. *Se $(X^{(1)}, \varphi_i^{(1)})$ e $(X^{(2)}, \varphi_i^{(2)})$ sono limiti inversi di un sistema inverso, allora esiste un isomorfismo $\bar{\varphi} : X^{(1)} \to X^{(2)}$ tale che $\varphi_i^{(2)}\bar{\varphi} = \varphi_i^{(1)}$ per ogni i.*

2. *Indichiamo con* $C = Cr(X_i \mid i \in I)$ *il prodotto cartesiano degli* X_i *e con* π_i *le proiezioni naturali da* C *a* X_i *per ogni* i*. Definiamo*

$$X = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c) \text{ per ogni } i, j \in I \text{ con } i \leq j\}$$

e $\varphi_i = \pi_i|_X$ *per ogni* i*. Allora* (X, φ_i) *è un limite inverso di* (X_i, φ_{ij})*.*

3. *Se* (X_i, φ_{ij}) *è un sistema inverso di gruppi topologici e omomorfismi continui, allora* X *è un gruppo topologico e le mappe* φ_i *sono omomorfismi continui.*

Dimostrazione. 1. Per la proprietà universale di $(X^{(1)}, \varphi_i^{(1)})$ applicata alla famiglia di mappe compatibili $(\varphi_i^{(2)})$ esiste una mappa $\varphi^{(1)} : X^{(2)} \to X^{(1)}$ tale che $\varphi_i^{(1)}\varphi^{(1)} = \varphi_i^{(2)}$ per ogni i. Analogamente esiste una mappa $\varphi^{(2)} : X^{(1)} \to X^{(2)}$ tale che $\varphi_i^{(2)}\varphi^{(2)} = \varphi_i^{(1)}$ per ogni i. Sempre per la proprietà universale di $(X^{(1)}, \varphi_i^{(1)})$ esiste solamente una mappa $\psi : X^{(1)} \to X^{(1)}$ tale che $\varphi_i^{(1)}\psi = \varphi_i^{(1)}$. Tuttavia sia $\varphi^{(1)}\varphi^{(2)}$ che la mappa identica hanno questa proprietà, quindi le due coincidono. Analogamente anche $\varphi^{(1)}\varphi^{(2)}$ coincide con la mappa identica. Ne segue che $\varphi^{(2)}$ è un isomorfismo.

2. Poiché consideriamo C con la topologia prodotto e X con la topologia di sottospazio, le mappe φ_i sono continue. Inoltre esse sono compatibili perché per definizione di X si ha $\varphi_{ij}\varphi_j = \varphi_i$ per ogni $i \leq j$.
Sia $(\psi_i : Y \to X_i)$ una famiglia di mappe compatibili. Mostriamo che esiste un'unica mappa (continua) $\psi : Y \to X$ tale che $\varphi_i\psi = \psi_i$ per ogni i. Consideriamo la mappa $\bar{\psi}$ da Y a C che manda un elemento y nel vettore $(\psi_i(y))$. Questa è continua perché $\pi_i\bar{\psi} = \psi_i$ per ogni i. Inoltre l'immagine di $\bar{\psi}$ è contenuta in X perché se $i \leq j$ allora

$$\pi_i\bar{\psi} = \psi_i = \varphi_{ij}\psi_j = \varphi_{ij}\pi_j\bar{\psi}$$

Possiamo allora definire la mappa $\psi : Y \to X$ con $\psi(y) = \bar{\psi}(y)$ per ogni y. Questa è continua e $\varphi_i\psi = \psi_i$ per ogni i. Per dimostrarne l'unicità supponiamo che $\psi' : Y \to X$ sia una mappa tale che $\varphi_i\psi' = \psi_i$ per ogni i. Abbiamo che $\varphi_i(\psi'(y)) = \psi_i(y) = \varphi_i(\psi(y))$ per ogni y e per ogni i, cioè $\psi = \psi'$.

3. Se gli X_i sono gruppi topologici allora lo è anche C. Inoltre se le φ_{ij} sono omomorfismi allora X è un sottogruppo di C e quindi un gruppo topologico con la topologia indotta.

□

Con questo teorema abbiamo verificato che, dato un sistema inverso (X_i, φ_{ij}), un (*il*) suo limite inverso esiste sempre ed è determinato a meno di isomorfismo. Lo indicheremo con $\varprojlim(X_i, \varphi_{ij})$ o più semplicemente con $\varprojlim X_i$. Sarà spesso conveniente lavorare con il particolare limite inverso costruito nella dimostrazione, lo indicheremo con $s\varprojlim X_i$.

Ricordiamo che uno spazio topologico è detto *totalmente disconnesso* quando ogni suo sottospazio connesso ha al più un elemento.

Proposizione 1.4. *Sia (X_i, φ_{ij}) un sistema inverso indicizzato da I. Sia $X = \varprojlim X_i$.*

1. *Se X_i è uno spazio di Hausdorff per ogni i, allora X è uno spazio di Hausdorff.*

2. *Se X_i è totalmente disconnesso per ogni i, allora X è totalmente disconnesso.*

3. *Se X_i è uno spazio di Hausdorff per ogni i, allora $s\varprojlim X_i$ è chiuso in $C = Cr(X_i \mid i \in I)$.*

4. *Se X_i è uno spazio di Hausdorff compatto per ogni i, allora X è uno spazio di Hausdorff compatto.*

5. *Se X_i è uno spazio di Hausdorff compatto non vuoto per ogni i, allora X è non vuoto.*

Dimostrazione. È sufficiente mostrare le tesi per il limite inverso $X = s\varprojlim X_i$. I primi due punti seguono dal fatto che tali proprietà vengono conservate dal passaggio a sottospazi e a prodotti di spazi.

3. Usiamo il seguente fatto: se $f, g : X \to Y$ sono mappe continue e Y è uno spazio di Hausdorff, allora l'insieme $\{x \mid f(x) = g(x)\}$ è chiuso in X. Abbiamo che
$$s\varprojlim X_i = \bigcap_{i \leq j} \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\}$$
dove le mappe π_i e φ_{ij} sono continue. Ne segue che X è un' intersezione di chiusi e quindi è chiuso in C.

4. La tesi è conseguenza diretta dei punti 1 e 3 di questa proposizione, utilizzando il teorema di Tychonoff e il fatto che i sottoinsiemi chiusi di uno spazio compatto sono compatti.

5. Per ogni coppia i, j con $i \leq j$ poniamo $D_{ij} = \{c \in C \mid \varphi_{ij}\pi_j(c) = \pi_i(c)\}$. Notiamo che C è compatto e D_{ij} è chiuso, quindi se per assurdo $s\varprojlim X_i = \emptyset$, allora esistono $i_1, ..., i_n$ e $j_1, ..., j_n$ in I, con $i_r \leq j_r$, per ogni r tali che $\bigcap_{r=1}^{n} D_{i_r j_r} = \emptyset$. Poiché I è un insieme diretto, esiste $k \in I$ tale che $j_r \leq k$ per ogni r. Fissiamo un $x_k \in X_k$, poniamo $x_l = \varphi_{lk}(x_k)$ per ogni $l \leq k$ e x_l arbitrario per ogni altro indice di I. L'elemento (x_i) del prodotto cartesiano C appartiene a $\bigcap_{r=1}^{n} D_{i_r j_r}$, contraddicendo quanto detto in precedenza.

□

Analizziamo ora la topologia dei limiti inversi.

Proposizione 1.5. *Sia (X, φ_i) un limite inverso di un sistema inverso (X_i, φ_{ij}) di spazi di Hausdorff compatti e non vuoti, indicizzato da I. Allora si ha:*

1. *$\varphi_i(X) = \bigcap_{i \leq j} \varphi_{ij}(X_j)$ per ogni $i \in I$.*

2. *Gli insiemi $\varphi_i^{-1}(U)$, con $i \in I$ e U aperto in X_i, formano una base per la topologia di X.*

3. *Se Y è un sottoinsieme di X che soddisfa $\varphi_i(Y) = X_i$ per ogni i, allora Y è denso in X.*

4. *Se θ è una mappa da uno spazio Y a X, allora θ è continua se e solo se $\varphi_i\theta$ è continua per ogni $i \in I$.*

Dimostrazione. È sufficiente mostrare le tesi per il limite inverso $X = s\varprojlim X_i$. Siano $C = Cr(X_i \mid i \in I)$ e π_i la proiezioni naturali da C a X_i per ogni i. Allora per costruzione di $s\varprojlim X_i$ abbiamo $\varphi_i = \pi_i|_X$ per ogni i.

1. Abbiamo che $\varphi_i(X) = \varphi_{ij}\varphi_i(X) \subseteq \varphi_{ij}(X_j)$ per ogni $i \leq j$, perciò $\varphi_i(X) \subseteq \bigcap_{i\leq j} \varphi_{ij}(X_j)$. Mostriamo l'inclusione inversa. Fissiamo $a \in \bigcap_{i\leq j} \varphi_{ij}(X_j)$ e $i \in I$. Per ogni $j \geq i$ poniamo $Y_j = \{y \in X_j \mid \varphi_{ij}(y) = a\}$. Notiamo che Y_j è chiuso in X_j perché è la retroimmagine di un chiuso, quindi Y_j è anche compatto. Se $k \geq j \geq i$ e $y_k \in Y_k$ allora $\varphi_{ij}(\varphi_{jk}(y_k)) = \varphi_{ik}(y_k) = a$, perciò $\varphi_{jk}(y_k) \in Y_k$. Dunque $\{Y_j \mid j \geq i\}$, con le restrizioni delle mappe φ_{ij}, è un sistema inverso di spazi di Hausdorff compatti e non vuoti. Sia allora $(b_j) \in s\varprojlim_{i\leq j} Y_j$. Notiamo che $b_i = a$ e $\varphi_{jk}(b_k) = b_j$ per ogni $k \geq j \geq i$. Se $l \in I$ e $i \not\geq l$ allora prendiamo $j \in I$ tale che $j \geq i, l$ e poniamo $b_l = \varphi_{lj}(b_j)$. Verifichiamo che b_l non dipende dalla scelta di j: prendiamo j' tale che $j' \geq i, l$, esiste k tale che $k \geq j, j'$ e abbiamo

$$\varphi_{lj}(b_j) = \varphi_{lj}\varphi_{jk}(b_k) = \varphi_{lj'}\varphi_{j'k}(b_k) = \varphi_{lj'}(b'_j)$$

Poiché abbiamo costruito $b = (b_j)$ in modo che valga $\varphi_{jk}(b_k) = b_j$ per ogni $k \geq j$, abbiamo che $b \in s\varprojlim_{j\in I} Y_j \subseteq s\varprojlim X_i = X$. Inoltre b è tale che $\varphi_i(b) = \pi_i(b) = a$, cioè $a \in \varphi_i(X)$

2. Gli aperti di X sono unioni di insiemi del tipo

$$P = X \cap \pi_{i_1}^{-1}(U_1) \cap ... \cap \pi_{i_n}^{-1}(U_n)$$

dove $i_1, ..., i_n \in I$ e U_r è aperto in X_{i_r} per ogni r. Mostriamo che per ogni $a = (a_i) \in P$ esiste un insieme $\varphi_k^{-1}(U)$ con U aperto in X_k tale che $a \in \varphi_k^{-1}(U) \subseteq P$. Fissiamo k tale che $k \geq i_1, ..., i_r$. Poiché la mappa φ_{i_rk} è continua, $\varphi_{i_rk}^{-1}(U_r)$ è aperto in X_k, inoltre, per ogni k, $\varphi_{i_rk}^{-1}(U_r)$ contiene a_k perché $\varphi_{ik}(a_k) = a_i$.

Ne segue che l'insieme $U = \bigcap_{r=1}^{n} \varphi_{i_r k}^{-1}(U_r)$ è un intorno aperto di a_k in X_k e dunque che l'insieme $\varphi_k^{-1}(U)$ è un intorno aperto di a in X.
Rimane da verificare che $\varphi_k^{-1}(U) \subseteq P$, cioè che se $b = (b_i) \in \varphi_k^{-1}(U)$, allora $b \in \pi_{i_r}^{-1}(U_r)$ per ogni r. Sia $b \in \varphi_k^{-1}(U)$, allora $b_k \in U$ e quindi $b_{i_r} = \varphi_{i_r k}(b_k) \in U_r$ per ogni r, ovvero $\pi_{i_r}(b) \in U_r$ per ogni r.

3. Per ogni i e per ogni aperto non vuoto U di X_i abbiamo $\varphi_i(Y) \cap U \neq \emptyset$, e quindi $Y \cap \varphi_i^{-1}(U) \neq \emptyset$. Ne segue, usando il secondo punto di questa proposizione, che Y è denso in X.

4. Poiché le mappe φ_i sono continue per ogni i, se θ è continua allora anche le composizioni $\varphi_i\theta$ sono continue per ogni i.
Viceversa se le mappe $\varphi_i\theta$ sono continue per ogni i, allora per ogni i e per ogni aperto U di X_i l'insieme $\theta^{-1}(\varphi_i^{-1}(U)) = (\varphi_i\theta)^{-1}(U)$ è aperto. Ne segue, usando il secondo punto di questa proposizione, che θ è continua.

□

È possibile dimostrare che ogni spazio di Hausdorff compatto e totalmente disconnesso può essere visto come limite inverso dei suoi spazi quoziente discreti. Vedremo e dimostreremo un risultato simile per i gruppi topologici, sui quali ora concentreremo l'attenzione.

1.2 Gruppi topologici

Ricordiamo che un *gruppo topologico* è un gruppo G dotato di una topologia per la quale la mappa $(x, y) \mapsto xy^{-1}$ da $G \times G$ (con la topologia prodotto) a G è continua.

Con il seguente lemma vediamo alcuni risultati sui gruppi topologici che ci saranno utili in seguito. Se G è un gruppo, g è un elemento di G e U, V sono sottoinsiemi di G, allora usiamo le seguenti notazioni: $Ug = \{ug \mid u \in U\}$, $gU = \{gu \mid u \in U\}$, $U^{-1} = \{u^{-1} \mid u \in U\}$ e $UV = \{uv \mid u \in U, v \in V\}$. Indichiamo l'elemento neutro di un gruppo con 1.

Lemma 1.6. *Sia G un gruppo topologico.*

1. *La mappa $(x, y) \mapsto xy$ da $G \times G$ a G è continua e la mappa $x \mapsto x^{-1}$ da G a G è un omeomorfismo. Per ogni $g \in G$ le mappe $x \mapsto xg$ e $x \mapsto gx$ da G a G sono omeomorfismi.*

2. *Se H è un sottogruppo aperto (rispettivamente chiuso) di G, allora ogni classe laterale Hg o gH di H in G è aperta (rispettivamente chiusa).*

3. *Ogni sottogruppo aperto di G è chiuso, ogni sottogruppo chiuso di indice finito è aperto. Se G è compatto allora ogni sottogruppo aperto di G ha indice finito.*

4. *Se H è un sottogruppo che contiene un sottoinsieme aperto non vuoto U di G, allora H è aperto in G.*

5. *Se H è un sottogruppo di G e K è un sottogruppo normale di G, allora H è un gruppo topologico rispetto alla topologia di sottospazio, e G/K è un gruppo topologico rispetto alla topologia quoziente; inoltre la mappa quoziente q da G a G/K manda insiemi aperti in insiemi aperti.*

6. *Il gruppo G è uno spazio di Hausdorff se e solo se $\{1\}$ è un sottoinsieme chiuso di G. Se K è un sottogruppo normale di G, allora G/K è uno spazio di Hausdorff se e solo se K è chiuso in G. Se G è totalmente disconnesso, allora G è uno spazio di Hausdorff.*

7. *Se G è uno spazio di Hausdorff compatto e C, D sono sottoinsiemi chiusi di G, allora l'insieme CD è chiuso.*

8. *Se G è compatto e $(X_\lambda \mid \lambda \in \Lambda)$ è una famiglia di sottoinsiemi chiusi con la proprietà che per ogni $\lambda_1, \lambda_2 \in \Lambda$ esiste un indice $\mu \in \Lambda$ per il quale vale $X_\mu \subseteq X_{\lambda_1} \cap X_{\lambda_2}$, allora, dato un sottoinsieme chiuso Y di G, si ha $(\bigcap_{\lambda\in\Lambda} X_\lambda)Y = \bigcap_{\lambda\in\Lambda} X_\lambda Y$.*

Dimostrazione. 1. Una mappa da uno spazio X a $G \times G$ è continua se e solo se sono continue le sue composizioni con le mappe di proiezione. Quindi se

$\theta : G \to G$ e $\varphi : G \to G$ sono continue, anche la mappa $x \mapsto (\theta(x), \varphi(x))$ da G a $G \times G$ è continua. Prendendo come θ la mappa costante $x \mapsto 1$ e come φ l'identità di G, otteniamo la mappa $x \mapsto (1, x)$; componendo quest'ultima con la mappa continua $c : (x, y) \mapsto xy^{-1}$, otteniamo la mappa $x \mapsto x^{-1}$ che quindi è continua e, in particolare, un omeomorfismo perché coincide con la sua inversa. Ne segue che la mappa $(x, y) \mapsto (x, y^{-1})$ è continua, e quindi lo è anche la sua composizione con c, ovvero la mappa $(x, y) \mapsto xy$.
Prendendo invece come θ l'identità di G e come φ la mappa costante $x \mapsto g^{-1}$, otteniamo la mappa $x \mapsto (x, g^{-1})$; componendo quest'ultima con c, otteniamo la mappa $x \mapsto xg$ che quindi è continua. Lo stesso vale per la mappa inversa $x \mapsto xg^{-1}$. Analogamente si mostra che anche la mappa $x \mapsto gx$ è un omeomorfismo.

2. Segue direttamente dal punto precedente.

3. Abbiamo che $G \setminus H = \bigcup(Hg \mid g \notin H)$, e quindi se H è aperto, allora, per il secondo punto di questo lemma, anche $G \setminus H$ è aperto, cioè H è chiuso. Se H ha indice finito, allora $G \setminus H$ è unione di un numero finito di classi laterali di H, perciò se H è anche chiuso, allora anche $G \setminus H$ è chiuso, cioè H è aperto.
Supponiamo che G sia compatto. Se H è aperto, allora gli insiemi Hg sono aperti e disgiunti e la loro unione è G, cioè costituiscono un ricoprimento aperto di G. Quindi per la compattezza di G, H deve avere indice finito.

4. Per il primo punto di questo lemma, Uh è aperto per ogni $h \in H$. Inoltre si ha $H = \bigcup(Uh \mid h \in H)$, quindi H è aperto.

5. L'affermazione su H è ovvia. Sia V un aperto di G, allora kV è aperto per ogni $k \in K$, e quindi $V_1 = KV$ è aperto. Di conseguenza, poiché $q(V) = q(V_1)$ e $q^{-1}q(v_1) = V_1$, si ha che $q(V)$ è aperto in G/K, cioè q manda aperti in aperti. Rimane da mostrare che G/K è un gruppo topologico, ovvero che la mappa $m : G/K \times G/K \to G/K$ definita da $(\xi, \zeta) \mapsto \xi\zeta^{-1}$ è continua. Sia U un aperto di G/K e sia $(Kw_1, Kw_2) \in m^{-1}(U)$. Poiché q e la mappa $(x, y) \mapsto xy^{-1}$ da

$G \times G$ a G sono continue, esistono intorni aperti W_1, W_2 di w_1, w_2 tali che $W_1 W_2^{-1} \subseteq q^{-1}(U)$, e quindi $q(W_1) \times q(W_2)$ è un intorno aperto di (Kw_1, Kw_2) contenuto in $m^{-1}(U)$.

6. Ricordiamo che i sottoinsiemi di uno spazio di Hausdorff composti da un solo elemento sono chiusi. Mostriamo che se $\{1\}$ è chiuso allora G è uno spazio di Hausdorff. Siano a, b elementi distinti di G, per il primo punto di questo lemma l'insieme $\{ab^{-1}\}$ è chiuso. Di conseguenza esiste un insieme aperto U tale che $1 \in U$ e $ab^{-1} \notin U$. La mappa $(x, y) \mapsto xy^{-1}$ è continua e quindi la retroimmagine di U è aperta. Ne segue che esistono due insiemi aperti V, W contenenti 1 e tali che $VW^{-1} \subseteq U$. Inoltre $ab^{-1} \notin VW^{-1}$, perciò $aV \cap bW = \emptyset$, e quindi G è uno spazio di Hausdorff perché aV e bW sono aperti. L'affermazione su G/K segue direttamente.
   Supponiamo che G sia totalmente disconnesso, mostriamo che $\{x\}$ è chiuso per ogni $x \in G$. Sia C la chiusura di $\{x\}$. Se C è l'unione di due aperti disgiunti A e B con $x \in A$, allora A è chiuso in C e quindi è chiuso anche in X. Ne segue che $A = C$, e quindi C è connesso. Perciò si ha $C = \{x\}$ perché G è totalmente disconnesso.

7. Poiché C e D sono chiusi nel compatto G, C e D sono anche compatti. Quindi è compatta anche l'immagine di $C \times D$ tramite la mappa continua $(x, y) \mapsto xy$, ovvero CD. Poiché G è uno spazio di Hausdorff, i suoi sottoinsiemi compatti sono chiusi; in particolare CD è chiuso.

8. Abbiamo che $(\bigcap X_\lambda)Y \subseteq X_\lambda Y$ per ogni $\lambda \in \Lambda$, e quindi $(\bigcap X_\lambda)Y \subseteq \bigcap (X_\lambda Y)$. Mostriamo il viceversa. Se $g \notin (\bigcap X_\lambda)Y$, allora $gY^{-1} \cap (\bigcap X_\lambda) = \emptyset$, e quindi, poiché G è compatto e poiché gY^{-1} e gli X_λ sono chiusi, si ha che esistono $\lambda_1, ..., \lambda_n \in \Lambda$ tali che $gY^{-1} \cap X_{\lambda_1} \cap ... \cap X_{\lambda_n} = \emptyset$. Per ipotesi esiste $\mu \in \Lambda$ tale che $X_\mu \subseteq X_{\lambda_1} \cap ... \cap X_{\lambda_n}$, e quindi $gY^{-1} \cap X_\mu = \emptyset$, cioè $g \notin X_\mu Y$.

□

Lemma 1.7. *Sia G un gruppo topologico compatto. Se C è un sottoinsieme chiuso e aperto che contiene* 1*, allora C contiene un sottogruppo normale aperto.*

Dimostrazione. Per ogni $x \in C$ l'insieme $W_x = Cx^{-1}$ è un intorno aperto di 1 tale che $W_x x \subseteq C$. Poiché la moltiplicazione è una mappa continua da $G \times G$ a G, esistono due aperti L_x, R_x contenenti 1 tali che l'immagine di $L_x \times R_x$, ovvero $L_x R_x$, è contenuta in W_x. Poniamo $S_x = L_x \cap R_x$, allora S_x è aperto e $S_x S_x \subseteq W_x$. Abbiamo che C è compatto perché è chiuso in G che è compatto. Gli insiemi $C \cap S_x x$ sono un ricoprimento aperto di C, perciò esistono $x_1, ..., x_n$ tali che $C \subseteq \bigcup_{i=1}^{n} S_{x_i} x_i$. Poniamo $S = \bigcap_{i=1}^{n} S_{x_i}$, allora S è aperto, contiene 1 e si ha

$$SC \subseteq \bigcup_{i=1}^{n} S S_{x_i} x_i \subseteq \bigcup_{i=1}^{n} W_{x_i} x_i \subseteq C, \tag{1.1}$$

e quindi $S \subseteq C$.
Poniamo ora $T = S \cap S^{-1}$. Abbiamo che T è aperto, $T = T^{-1}$ e $1 \in T$. Poniamo inoltre $T^1 = T$, $T^n = TT^{n-1}$ per ogni $n > 1$ e $H = \bigcup_{n>0} T^n$. Notiamo che H è il gruppo generato da T e, essendo unione di insiemi del tipo Ty, è aperto. Per induzione e per la formula (1.1) otteniamo che $T^n \subseteq C$ per ogni $n > 0$, e quindi $H \subseteq C$. Per il terzo punto del Lemma 1.6, H ha indice finito in G, perciò ha un numero finito di coniugati (si veda la Proposizione 2.2). L'intersezione di questi coniugati è quindi un sottogruppo normale aperto contenuto in C. □

Concludiamo la sezione con un risultato sui gruppi topologici compatti e totalmente disconnessi. L'importanza di questa classe di gruppi sarà chiara al termine di questo capitolo: mostreremo infatti che un gruppo topologico è profinito se e solo se è compatto e totalmente disconnesso.

Se G è un gruppo topologico, scriveremo $H \leq G$ per indicare che H è un sottogruppo chiuso di G e $N \lhd_O G$ per indicare che N è un sottogruppo normale aperto di G.

Proposizione 1.8. *Sia G un gruppo topologico compatto e totalmente disconnesso.*

1. *Ogni insieme aperto in G è unione di classi laterali di sottogruppi normali aperti.*

2. *Un sottoinsieme di G è sia aperto che chiuso se e solo se è unione di un numero finito di classi laterali di sottogruppi normali aperti.*

3. *Se X è un sottoinsieme di G e $\bar{X}$ è la sua chiusura, allora vale*

$$\bar{X} = \bigcap_{N \lhd_O G} NX.$$

In particolare, per ogni sottoinsieme chiuso C vale

$$C = \bigcap_{N \lhd_O G} NC,$$

e l'intersezione dei sottogruppi normali chiusi di G è 1.

Dimostrazione. 1. Notiamo che G è uno spazio di Hausdorff per il sesto punto del Lemma 1.6.

Sia U un aperto non vuoto di G. Se $x \in U$, allora Ux^{-1} è un aperto che contiene 1. Poiché G è uno spazio di Hausdorff totalmente disconnesso, gli aperti di G sono unioni di insiemi ciascuno dei quali è sia aperto che chiuso, infatti, sia V un aperto di G e sia $a \in V$, allora per ogni $b \in G \setminus \{a\}$ esiste un insieme F_b sia aperto che chiuso e che soddisfa $a \in F_b$ e $b \notin F_b$, e quindi G è l'unione dell'aperto V con gli aperti $G \setminus F_b$; per la compattezza di G esistono $b_1, ..., b_n$ tali che $G = V \cup (G \setminus F_{b_1}) \cup ... \cup (G \setminus F_{b_n})$, e quindi l'insieme $F_{b_1} \cap ... \cap F_{b_n}$ è sia aperto che chiuso e vale $a \in F_{b_1} \cap ... \cap F_{b_n} \subseteq V$, cioè V è unione di insiemi di questo tipo. Da questo segue, usando il Lemma 1.7, che Ux^{-1} contiene un sottogruppo normale aperto K_x. Si ha dunque $U = \bigcup_{x \in U} K_x x$

2. Se P è un insieme sia chiuso che aperto, allora per il primo punto di questa proposizione è unione di classi laterali di sottogruppi normali aperti. Poiché P è chiuso in G che è compatto, P è anche compatto, e quindi è unione di una sottofamiglia finita di queste classi laterali. Viceversa, l'unione di un numero finito di classi laterali di un sottogruppo normale aperto è chiaramente sia aperta che chiusa.

3. Se $y \notin \bar{X}$, allora y ha un intorno aperto disgiunto da X. Per il primo punto di questa proposizione esiste un sottogruppo normale aperto N tale che $Ny \cap X = \emptyset$, e quindi $y \notin NX$. Passando ai complementari si ha la tesi.

□

1.3 Caratterizzazione dei gruppi profiniti

Sia G un gruppo topologico, chiameremo *base filtro* una famiglia I di sottogruppi normali di G quando per ogni $K_1, K_2 \in I$ esiste un sottogruppo $K_3 \in I$ contenuto in $K_1 \cap K_2$. Iniziamo con due risultati tecnici.

Proposizione 1.9. *Sia (G, φ_i) un limite inverso di un sistema inverso (G_i) di gruppi topologici di Hausdorff compatti, sia $L \lhd_O G$. Allora* $\ker\varphi_i \leq L$ *per qualche i. Di conseguenza G/L è isomorfo (come gruppo topologico) ad un quoziente di un sottogruppo di qualche G_i. Inoltre se ognuna delle mappe φ_i è suriettiva, allora G/L è isomorfo ad un quoziente di qualche G_i.*

Dimostrazione. Poiché L è aperto e contiene 1, per la Proposizione 1.5 abbiamo che $\varphi_i^{-1}(U) \subseteq L$ per qualche i e qualche insieme U aperto in G e contenente 1. Ne segue che $\ker\varphi_i \leq L$ per qualche i.
Per i teoremi fondamentali di isomorfismo abbiamo che $G/L \cong (G/\ker\varphi_i)/(L/\ker\varphi_i)$ e anche $G/\ker\varphi_i \cong \mathrm{im}\varphi_i$. Di conseguenza G/L è isomorfo ad un quoziente di $\mathrm{im}\varphi_i$. In particolare se φ_i è suriettiva, G/L è isomorfo ad un quoziente di G_i. □

Proposizione 1.10. *Siano G un gruppo topologico e I una base filtro di sottogruppi normali chiusi. Definiamo in I la relazione d'ordine $\preceq$ in questo modo: se $K, L \in I$ allora $K \preceq L$ se e solo se $L \leq K$. Si ha che I con la relazione d'ordine $\preceq$ è un insieme diretto, inoltre, al variare di $K \in I$, i gruppi G/K con gli omomorfismi suriettivi $q_{KL} : G/L \to G/K$ (definiti per $K \preceq L$) formano un sistema inverso. Poniamo $(\widehat{G}, \varphi_K) = \varprojlim G/K$. Allora esiste un omomorfismo $\theta : G \to \widehat{G}$ il cui nucleo è $\bigcap_{K \in I} K$ e la cui immagine è un sottogruppo denso di $\widehat{G}$. Inoltre $\varphi_K\theta$ è la mappa quoziente da G a G/K per ogni $K \in I$. Se G è compatto allora θ è suriettiva;*

se G è compatto e $\bigcap_{K\in I} K = 1$ allora θ è un isomorfismo di gruppi topologici (cioè è un isomorfismo di gruppi e un omeomorfismo).

Dimostrazione. Il fatto che $(G/K, q_{KL})$ sia un sistema inverso è una semplice verifica. Sia $C = Cr(G/K \mid K \in I)$. Sia $\widehat{G} = s\varprojlim G/K$ ovvero

$$\widehat{G} = \{c \in C \mid q_{UV}\pi_V(c) = \pi_U(c) \text{ per ogni } U, V \in I \text{ con } U \preceq V\}$$

dove le mappe $\pi_U : C \to G/U$ sono le proiezioni naturali. Consideriamo la mappa $\bar{\theta}$ da G a C definita da $\bar{\theta} : g \mapsto (gK)$. Dal quarto punto della Proposizione 1.5 segue che la mappa $\bar{\theta}$ è continua, infatti componendola con le proiezioni naturali si ottengono le mappe quoziente. Mostriamo che l'immagine di $\bar{\theta}$ è contenuta in $\widehat{G}$: siano $g \in G$ e $U \preceq V$, si ha $\pi_U((gK)) = gU$ e $q_{UV}\pi_V((gK)) = q_{UV}(gV) = gU$, quindi $\pi_U((gK)) = q_{UV}\pi_V((gK))$ ovvero $\bar{\theta}(g) = (gK) \in \widehat{G}$.
Sia $\theta : G \to \widehat{G}$ la mappa indotta da $\bar{\theta}$, che è continua perché lo è $\bar{\theta}$. Un elemento $g \in G$ appartiene al nucleo di θ se e solo se $Kg = K$ per ogni K, cioè $\ker\theta = \bigcap_{K\in I} K$. Per ogni $K \in I$ vale $\varphi_K(\theta(G)) = G/K$, perciò dal terzo punto della Proposizione 1.5 segue che l'immagine di θ è densa in $\widehat{G}$.
Per il sesto punto del Lemma 1.6, per ogni $K \in I$ si ha che G/K è un gruppo topologico di Hausdorff, quindi anche C è un gruppo topologico di Hausdorff. Supponiamo che G sia compatto. Poiché θ è continua, anche $\theta(G)$ è compatto e quindi chiuso in C. Ma dal momento che $\theta(G)$ è denso in $\widehat{G}$, si ha che $\theta(G) = G$. Infine se $\bigcap_{K\in I} K = 1$ allora θ è una biezione continua e quindi, essendo il dominio compatto e il codominio di Hausdorff, è un omeomorfismo. □

Per classe di gruppi finiti si intenderà una classe di gruppi finiti chiusa rispetto alle immagini isomorfe, cioè se F_1 appartiene alla classe e F_2 è isomorfo a F_1 allora anche F_2 appartiene alla classe.
Sia $\mathcal{C}$ una classe di gruppi finiti. Un gruppo F è detto *$\mathcal{C}$-gruppo* se $F \in \mathcal{C}$, un gruppo G è detto *gruppo pro-$\mathcal{C}$* se è un limite inverso di $\mathcal{C}$-gruppi. Notiamo che un $\mathcal{C}$-gruppo è anche un gruppo pro-$\mathcal{C}$, infatti lo si può vedere, ad esempio, come limite inverso del sistema inverso composto soltanto dal gruppo stesso e indicizzato dall'insieme

diretto $I = \{i\}$.
Diciamo che $\mathcal{C}$ è chiusa per sottogruppi (rispettivamente quozienti) se ogni sottogruppo (rispettivamente quoziente) di un $\mathcal{C}$-gruppo è ancora un $\mathcal{C}$-gruppo; diciamo che $\mathcal{C}$ è chiusa per prodotti diretti se $F_1 \times F_2 \in \mathcal{C}$ per ogni $F_1, F_2 \in \mathcal{C}$. Alcune importanti classi sono la classe di tutti i gruppi finiti, la classe di tutti i p-gruppi finiti per un primo p fissato e la classe di tutti i gruppi ciclici finiti. Un limite inverso di gruppi finiti si chiama *gruppo profinito*, un limite inverso di p-gruppi si chiama *gruppo pro-p*.

Vediamo ora l'equivalenza di alcune caratterizzazioni dei gruppi pro-$\mathcal{C}$.

Teorema 1.11. *Sia $\mathcal{C}$ una classe di gruppi finiti (considerati con la topologia discreta) chiusa per sottogruppi e prodotti diretti. Sia G un gruppo topologico. Sono equivalenti:*

1. *G è un gruppo pro-$\mathcal{C}$;*
2. *G è isomorfo (come gruppo topologico) ad un sottogruppo chiuso di un prodotto cartesiano di $\mathcal{C}$-gruppi;*
3. *G è compatto e $\bigcap(N \mid N \lhd_O G,\ G/N \in \mathcal{C}) = 1$;*
4. *G è compatto e totalmente disconnesso, inoltre per ogni $L \lhd_O G$ esiste un sottogruppo $N \lhd_O G$ tale che $N \leq L$ e $G/N \in \mathcal{C}$.*

Infine se $\mathcal{C}$ è chiusa per quozienti, allora il quarto punto si può sostituire con:

4'. *G è compatto e totalmente disconnesso, inoltre $G/L \in \mathcal{C}$ per ogni $L \lhd_O G$.*

Dimostrazione. $1 \Rightarrow 2$. Segue dal terzo punto della Proposizione 1.4.

$2 \Rightarrow 3$. Supponiamo che G sia isomorfo ad un sottogruppo chiuso $\widehat{G}$ di $C = Cr(G_i)$, dove G_i è un $\mathcal{C}$-gruppo per ogni i. Sia K_i il nucleo della proiezione naturale da C a G_i per ogni i. Notiamo che, per ogni i, G_i è un gruppo finito, perciò ciascun G_i è compatto e quindi per il teorema di Tychonoff anche C è compatto. Ne segue che $\widehat{G}$, essendo chiuso nel compatto C, è compatto. Poniamo $N_i = K_i \cap \widehat{G}$

per ogni i. Poiché $K_i \lhd_O C$, si ha $N_i \lhd_O \widehat{G}$, inoltre, poiché $\bigcap K_i = 1$, si ha anche $\bigcap N_i = 1$. Per concludere mostriamo che $\bigcap(N \mid N \lhd_O \widehat{G},\ \widehat{G}/N \in \mathcal{C}) \leq \bigcap N_i$, ovvero mostriamo che $\widehat{G}/N_i \in \mathcal{C}$ per ogni i:

$$\widehat{G}/N_i \cong \widehat{G}K_i/K_i \leq C/K_i \cong G_i.$$

$3 \Rightarrow 1$. Sia $I = \{N \lhd_O G \mid G/N \in \mathcal{C}\}$ e siano $N_1, N_2 \in I$. Consideriamo la mappa η da G al $\mathcal{C}$-gruppo $G/N_1 \times G/N_2$ definita da $g \mapsto (N_1 g, N_2 g)$. Si verifica facilmente che η è un omomorfismo continuo, inoltre il suo nucleo è $N_1 \cap N_2 \leq G$. Ma, poiché $\mathcal{C}$ è chiusa per prodotti cartesiani e sottogruppi, si ha che l'immagine di η appartiene a $\mathcal{C}$, quindi $N_1 \cap N_2 \in I$. Osserviamo che i sottogruppi appartenenti ad I sono aperti e quindi anche chiusi perciò, essendo I una base filtro di sottogruppi chiusi, applichiamo la Proposizione 1.10 e otteniamo $G \cong \varprojlim_{N \in I} G/N$.

$1 \Rightarrow 4$. Per la Proposizione 1.4 il gruppo G è compatto e totalmente disconnesso. Il resto della tesi segue dalla Proposizione 1.9, infatti per ogni $L \lhd_O G$ abbiamo che L contiene il nucleo N di un omomorfismo continuo φ da G a un $\mathcal{C}$-gruppo H del sistema inverso di cui G è limite inverso, e quindi $G/N \cong \mathrm{im}\varphi \leq H \in \mathcal{C}$.

$4 \Rightarrow 1$. Segue dalla Proposizione 1.8.

Infine supponiamo che $\mathcal{C}$ sia chiusa per quozienti. Per ogni $L \lhd_O G$ possiamo trovare, nel modo descritto precedentemente in questa dimostrazione, un sottogruppo $N \lhd_O G$ tale che $N \leq L$ e $G/N \in \mathcal{C}$. Poiché $G/L \cong (G/N)/(L/N)$, concludiamo che $G/L \in \mathcal{C}$. □

Se consideriamo come classe $\mathcal{C}$ la classe di tutti i gruppi finiti, che ovviamente è chiusa per quozienti, otteniamo la seguente importante caratterizzazione dei gruppi profiniti.

Corollario 1.12. *Sia G un gruppo topologico. Sono equivalenti:*

1. *G è un gruppo profinito;*

2. *G è isomorfo (come gruppo topologico) ad un sottogruppo chiuso di un prodotto cartesiano di gruppi finiti;*

3. *G è compatto e $\bigcap(N \mid N \lhd_O G) = 1$;*

4. *G è compatto e totalmente disconnesso.*

Il prossimo risultato descrive come un gruppo profinito, i suoi sottogruppi e i suoi quozienti possano essere rappresentati come limiti inversi.

Teorema 1.13. *Sia G un gruppo profinito. Se I è una base filtro di sottogruppi normali chiusi tale che $\bigcap(N \mid N \in I) = 1$ allora*

$$G \cong \varprojlim_{N \in I} G/N.$$

Inoltre per ogni sottogruppo chiuso H si ha

$$H \cong \varprojlim_{N \in I} H/(H \cap N)$$

e per ogni sottogruppo normale chiuso K si ha

$$G/K \cong \varprojlim_{N \in I} G/(KN).$$

Dimostrazione. Le prime due affermazioni seguono dalla Proposizione 1.10.
La famiglia $J = (KN \mid N \in I)$ è una base filtro di sottogruppi normali aperti di G. Per il Lemma 1.6 abbiamo

$$\bigcap_{M \in J} M = K \bigcap_{N \in I} N = K$$

e quindi anche la terza affermazione segue dalla Proposizione 1.10. □

Infine vediamo sotto quali condizioni si conserva la proprietà di essere un gruppo pro-$\mathcal{C}$.

Proposizione 1.14. *Se $\mathcal{C}$ è una classe di gruppi finiti chiusa per sottogruppi e prodotti diretti, allora sottogruppi chiusi, prodotti cartesiani e limiti inversi di gruppi pro-$\mathcal{C}$ sono ancora gruppi pro-$\mathcal{C}$.*
Se inoltre $\mathcal{C}$ è chiusa per quozienti, allora quozienti di gruppi pro-$\mathcal{C}$ rispetto a sottogruppi normali chiusi sono ancora gruppi pro-$\mathcal{C}$.

Dimostrazione. Le affermazioni su sottogruppi chiusi e quozienti sono conseguenza diretta del Teorema 1.13.
L'affermazione sui prodotti cartesiani si dimostra sfruttando la prima equivalenza del Teorema 1.11, osservando che sottogruppi chiusi di sottogruppi chiusi sono ancora chiusi e prodotti cartesiani di prodotti cartesiani sono ancora prodotti cartesiani.
Infine, supponiamo che $\mathcal{C}$ sia chiusa per quozienti. Per la Proposizione 1.4, i gruppi pro-$\mathcal{C}$ sono gruppi topologici di Hausdorff in quanto limiti inversi di gruppi con la topologia discreta, e quindi, per la stessa proposizione, un limite inverso di gruppi pro-$\mathcal{C}$ è isomorfo ad un sottogruppo chiuso del prodotto cartesiano di gruppi pro-$\mathcal{C}$, quindi è a sua volta un gruppo pro-$\mathcal{C}$. □

Capitolo 2

Teoria di Sylow e generalizzazioni nei gruppi finiti

Sappiamo che, per il teorema di Lagrange, l'ordine di un sottogruppo divide l'ordine del gruppo. Ci chiediamo ora se sia vero anche il viceversa, ovvero se, dato un intero m che divide l'ordine di un gruppo, esista un sottogruppo di ordine m. Si può dimostrare che la risposta è affermativa nel caso dei gruppi abeliani ma non in generale. Ricordiamo che il teorema di Cauchy afferma che se m è primo allora esiste un sottogruppo di ordine m; in questo capitolo vedremo dei risultati che generalizzano il teorema di Cauchy.

2.1 Teoremi di Sylow

Ricordiamo che un gruppo in cui ciascun elemento ha ordine una potenza (≥ 0) di un primo p fissato è detto *p-gruppo*. Se H è un sottogruppo di un gruppo G e H è un p-gruppo, allora H è detto *p-sottogruppo* di G. In particolare il sottogruppo banale è un p-sottogruppo di G per ogni primo p perché ha ordine $1 = p^0$.
Usando il teorema di Lagrange e il teorema di Cauchy si può dimostrare facilmente che un gruppo finito è un p-gruppo se e solo se il suo ordine è una potenza di p.
Iniziamo con una breve presentazione delle azioni di gruppo.

Definizione 2.1. Un'*azione* di un gruppo G su un insieme S è una funzione $G \times S \to S$, $(g, x) \mapsto gx$ tale che per ogni $x \in S$ e per ogni $g_1, g_2 \in G$ valgano $1x = x$ e $(g_1 g_2)x = g_1(g_2 x)$.

Quando si ha un'azione di G su S diciamo che G *agisce su* S. Vediamo ora due esempi che ci torneranno utili in seguito.

Esempi:

1. Siano G un gruppo e H un suo sottogruppo. Un'azione del gruppo H sull'insieme G è data da $(h, x) \mapsto hx$, dove hx è il prodotto in G. Questa azione è detta *traslazione sinistra*. Se K è un altro sottogruppo di G e S è l'insieme delle classi laterali sinistre di K in G, allora H agisce su S per traslazione sinistra: $(h, xK) \mapsto hxK$.

2. Siano G un gruppo e H un suo sottogruppo. Un'azione del gruppo H sull'insieme G è data da $(h, x) \mapsto h^{-1}xh$. Questa azione è detta *coniugio* per h e diciamo che l'elemento hxh^{-1} è coniugato a x. Se K è un sottogruppo qualunque di G e $h \in H$, allora $h^{-1}Kh$ è un sottogruppo di G isomorfo a K, e quindi H agisce sull'insieme S dei sottogruppi di G per coniugio: $(h, K) \mapsto h^{-1}Kh$. Diciamo che il gruppo $h^{-1}Kh$ è coniugato a K.

Proposizione 2.2. *Sia G un gruppo che agisce su un insieme S. Dato $x \in S$, poniamo $\bar{x} = \{gx \mid g \in G\}$ e $G_x = \{g \in G \mid gx = x\}$. Allora $|\bar{x}| = [G : G_x]$.*

Dimostrazione. Siano $h, g \in G$, abbiamo che

$$gx = hx \iff g^{-1}hx = x \iff g^{-1}h \in G_x \iff hG_x = gG_x.$$

Ne segue che la mappa definita da $gG_x \mapsto gx$ è biettiva, perciò $|\bar{x}| = [G : G_x]$. □

Gli insiemi $\bar{x}$ e G_x sono detti rispettivamente *orbita di x* e *stabilizzatore di x*.

Lemma 2.3. *Siano p un primo e S un insieme finito. Sia H un gruppo di ordine p^n che agisce su S. Poniamo $S_0 = \{x \in S \mid hx = x$ per ogni $h \in H\}$, allora $|S| \equiv |S_0|$ (mod p).*

Dimostrazione. Un'orbita $\bar{x}$ contiene esattamente un elemento se e solo se $x \in S_0$. Ne segue che S si può vedere come la seguente unione disgiunta: $S = S_0 \cup \bar{x}_1 \cup \bar{x}_2 \cup ... \cup \bar{x}_n$, con $|\bar{x}_i| > 1$ per ogni i. Perciò $|S| = |S_0| + |\bar{x}_1| + |\bar{x}_2| + ... + |\bar{x}_n|$. Notiamo che $p \mid |\bar{x}_i|$ per ogni i perché $|\bar{x}_i| > 1$ e $|\bar{x}_i| = [H : H_{x_i}]$ divide $|H| = p^n$. Quindi si ha $|S| \equiv |S_0| \pmod{p}$. □

Il lemma precedente e la notazione S_0 verranno usate di frequente.
Ricordiamo che il *normalizzante* di un sottogruppo H in un gruppo G è definito come $N_G(H) = \{x \in G \mid xHx^{-1} = H\}$

Lemma 2.4. *Se H è un p-sottogruppo di un gruppo finito G, allora $[N_G(H) : H] \equiv [G : H]$ (mod p).*

Dimostrazione. Sia S l'insieme delle classi laterali sinistre di H in G. Abbiamo che $|S| = [G : H]$. Consideriamo come azione di H su S la traslazione sinistra, allora

$$xH \in S_0 \iff hxH = xH \quad \text{per ogni} \quad h \in H$$
$$\iff x^{-1}hxH = H \quad \text{per ogni} \quad h \in H \iff x^{-1}hx \in H \quad \text{per ogni} \quad h \in H$$
$$\iff x^{-1}Hx = H \iff x \in N_G(H).$$

Quindi $|S_0|$ è il numero di classi laterali xH con $x \in N_G(H)$, ovvero $|S_0| = [N_G(H) : H]$. Per il Lemma 2.3 si ha $[N_G(H) : H] = |S_0| \equiv |S| = [G : H] \pmod{p}$. □

Corollario 2.5. *Se H è un p-sottogruppo di un gruppo finito G e p divide $[G : H]$, allora $N_G(H) \neq H$.*

Dimostrazione. Abbiamo che $0 \equiv [G : H] \equiv [N_G(H) : H] \pmod{p}$, perciò $[N_G(H) : H] > 1$. Ne segue che $N_G(H) \neq H$. □

Vediamo ora il primo teorema di Sylow.

Teorema 2.6. *Sia G un gruppo di ordine $p^n m$, con $n \geq 1$, p primo, e $(p, m) = 1$. Allora G contiene un sottogruppo di ordine p^i per ogni $1 \leq i \leq n$, inoltre ogni sottogruppo di G di ordine p^i, con $i < n$, è normale in qualche sottogruppo di G di ordine p^{i+1}.*

Dimostrazione. Per il teorema di Cauchy, poiché $p \mid |G|$, abbiamo che G contiene un elemento a di ordine p. Di conseguenza il sottogruppo generato da a ha ordine p. Procediamo per induzione. Supponiamo che H sia un sottogruppo di G di ordine p^i, con $1 \leq i < n$, allora $p \mid [G : H]$. Per il Lemma 2.4 e il Corollario 2.5 abbiamo che H è normale in $N_G(H)$, $H \neq N_G(H)$ e $1 < |N_G(H)/H| = |N_G(H) : H] \equiv [G : H] \equiv 0 \pmod{p}$. Perciò $p \mid |N_G(H)/H|$ e quindi per il teorema di Cauchy $N_G(H)/H$ contiene un sottogruppo di ordine p. Questo sottogruppo è della forma H_1/H dove H_1 è un sottogruppo di $N_G(H)$ contenente H. Poiché H è normale in $N_G(H)$ si ha che H è normale anche in H_1. Si ha dunque $|H_1| = |H||H_1/H| = p^i p = p^{i+1}$. □

Un sottogruppo P di un gruppo G è detto *p-sottogruppo di Sylow* quando è un p-sottogruppo massimale di G, cioè se H è un p-gruppo e $P \leq H \leq G$ allora necessariamente $P = H$. Osserviamo che i p-sottogruppi di Sylow esistono sempre, tuttavia potrebbero essere il sottogruppo banale. Ogni p-sottogruppo è contenuto in un p-sottogruppo di Sylow. Per il teorema precedente i gruppi finiti hanno p-sottogruppi di Sylow non banali per ogni primo p che divide l'ordine del gruppo. Abbiamo inoltre il seguente risultato.

Corollario 2.7. *Sia G un gruppo di ordine $p^n m$, con $n \geq 1$, p primo, e $(p, m) = 1$. Sia H un p-sottogruppo di G.*

1. *H è un p-sottogruppo di Sylow di G se e solo se $|H| = p^n$.*

2. *I sottogruppi coniugati a p-sottogruppi di Sylow sono ancora p-sottogruppi di Sylow.*

3. *Se c'è solo un p-sottogruppo di Sylow P, allora P è normale in G.*

Dimostrazione. 1. Abbiamo che H è un p-sottogruppo se e solo se il suo ordine è una potenza di p. Per il Teorema 2.6 esiste un sottogruppo di G di ordine p^n, perciò H è massimale se e solo se ha ordine p^n

2. Segue dal punto precedente e dal fatto che due sottogruppi coniugati hanno lo stesso ordine.

3. Segue direttamente dal punto precedente.

□

Vediamo infine il secondo teorema di Sylow.

Teorema 2.8. *Se H è un p-sottogruppo di G e P è un p-sottogruppo di Sylow di G, allora esiste $x \in G$ tale che $H \leq x^{-1}Px$. In particolare due p-sottogruppi di Sylow di G sono coniugati.*

Dimostrazione. Sia S l'insieme delle classi laterali sinistre di P in G. Abbiamo che $|S| = [G : P]$. Consideriamo come azione di H su S la traslazione sinistra. Per il Lemma 2.3 si ha $|S_0| \equiv |S| \pmod{p}$. Poiché p non divide $[G : P]$ allora necessariamente $|S_0| \neq 0$, quindi esiste una classe laterale $xP \in S_0$.

$$xP \in S_0 \iff hxP = xP \quad \text{per ogni} \quad h \in H$$
$$\iff x^{-1}hxP = P \quad \text{per ogni} \quad h \in H \iff x^{-1}Hx \leq P \iff H \leq xPx^{-1}.$$

In particolare se H è un p-sottogruppo di Sylow, allora si ha $|H| = |P| = |x^{-1}Px|$ e quindi $H = x^{-1}Px$. □

2.2 Sottogruppi di Hall

In questa sezione presentiamo un teorema per i gruppi risolubili finiti che generalizza i teoremi di Sylow. Iniziamo con le definizioni di sottogruppo commutatore e gruppo risolubile.

Definizione 2.9. Sia G un gruppo. Il sottogruppo di G generato dall'insieme $\{a^{-1}b^{-1}ab \mid a, b \in G\}$ è detto *sottogruppo commutatore* di G e viene indicato con G'.

Gli elementi del tipo $a^{-1}b^{-1}ab$ con $a, b \in G$ sono detti *commutatori*. I commutatori generano solamente G', quindi G' potrebbe contenere elementi che non sono commutatori. Notiamo che G è abeliano se e solo se $G' = 1$. In un certo senso, G' fornisce una misura di quanto G differisca da un gruppo abeliano.
Dato un gruppo G, poniamo $G^{(1)} = G'$ e $G^{(i)} = (G^{(i-1)})'$ per $i \geq 1$. Il sottogruppo $G^{(i)}$ è detto *i-esimo sottogruppo derivato* di G. Abbiamo una sequenza di sottogruppi di G: $G \geq G^{(1)} \geq G^{(2)} \geq ....$ Si può verificare che $G^{(i)}$ è un sottogruppo normale di G (e quindi in particolare di $G^{(i-1)}$) per ogni $i \geq 1$.

Definizione 2.10. Un gruppo G è detto *risolubile* se $G^{(n)} = 1$ per qualche n.

Proposizione 2.11. *Valgono le seguenti affermazioni.*

1. *I sottogruppi e le immagini tramite omomorfismi di gruppi risolubili sono ancora risolubili.*

2. *Se N è un sottogruppo normale di un gruppo G tale che N e G/N siano risolubili, allora G è risolubile.*

Dimostrazione. 1. Sia $f : G \to H$ un omomorfismo. Si può verificare che $f(G^{(i)}) \leq H^{(i)}$. Supponiamo che f sia suriettiva e G risolubile, allora si ha che $f(G^{(i)}) = H^{(i)}$ e che, per qualche n, $1 = f(1) = f(G^{(n)}) = H^{(n)}$, cioè H è risolubile. Per i sottogruppi è sufficiente notare che se H è un sottogruppo di G, allora $H^{(n)} \leq G^{(n)} = 1$.

2. Sia $f : G \to G/N$ la mappa quoziente. Poiché G/N è risolubile, per qualche n si ha che $f(G^{(n)}) = (G/N)^{(n)} = 1$. Perciò abbiamo $G^{(n)} \leq \mathrm{Ker} f = N$. Quindi, per il punto precedente di questa proposizione, $G^{(n)}$ è risolubile. Ne segue che, per qualche k, $G^{(n+k)} = (G^{(n)})^{(k)} = 1$, cioè G è risolubile.

□

Per la dimostrazione della generalizzazione dei teoremi di Sylow per i gruppi risolubili finiti abbiamo bisogno delle seguenti definizioni e dei seguenti lemmi.
Un sottogruppo H di un gruppo G è detto *caratteristico* (rispettivamente *pienamente invariante*) se $f(H) \leq H$ per ogni automorfismo (rispettivamente endomorfismo) $f : G \to G$. Notiamo che i sottogruppi pienamente invarianti sono anche caratteristici e che i sottogruppi caratteristici sono anche normali, perché il coniugio è un automorfismo.
Un *sottogruppo normale minimale* di un gruppo G è un sottogruppo normale non banale che non contiene alcun sottogruppo proprio normale in G.

Lemma 2.12. *Sia N un sottogruppo normale di un gruppo finito G e sia H un sottogruppo di G.*

1. *Se H è un sottogruppo caratteristico di N, allora H è normale in G.*

2. *Ogni p-sottogruppo di Sylow normale di G è pienamente invariante.*

3. *Se G è risolubile e N è un sottogruppo normale minimale, allora N è un p-gruppo abeliano per qualche primo p.*

Dimostrazione. 1. Poiché $a^{-1}Na = N$ per ogni $a \in G$, il coniugio per a è un automorfismo di N. Ne segue che $a^{-1}Ha \leq H$ per ogni $a \in G$ perché H è caratteristico in N. Mostriamo che vale anche l'inclusione inversa e quindi che H è normale in G. Per $a^{-1} \in G$ vale $aHa^{-1} \leq H$, perciò, dato $x \in N$, abbiamo che $x = a^{-1}(axa^{-1})a \in a^{-1}Na$, e quindi $N \leq a^{-1}Na$.

2. Sia P un p-sottogruppo di Sylow normale di G e sia f un endomorfismo di G. Per il secondo teorema di Sylow, se ci fosse un altro p-sottogruppo di Sylow di G, questo sarebbe coniugato a P, e quindi coincidente con P perché P è normale. Sia $x \in P$, allora $x^{p^n} = 1$ per qualche numero naturale n. Ne segue che $f(x)^{p^n} = f(x^{p^n}) = 1$, cioè l'ordine di $f(x)$ divide p^n, e quindi il sottogruppo generato da $f(x)$ è un p-sottogruppo. Dal secondo teorema di Sylow segue che $f(x) \in P$, e quindi $f(P) \leq P$.

3. Si può verificare che N' è pienamente invariante in N e quindi, per il primo punto di questa proposizione, N' è normale in G. Poiché N è un sottogruppo normale minimale, o $N' = 1$ oppure $N' = N$. Tuttavia N è risolubile per la Proposizione 2.11, quindi $N' \neq N$. Ne segue che $N' = 1$, cioè N è un sottogruppo abeliano non banale. Sia P un p-sottogruppo di Sylow non banale di N per qualche primo p. Poiché N è abeliano, P è normale in N, quindi, per il secondo punto di questa proposizione, P è pienamente invariante in N. Di conseguenza P è normale in G. Poiché N è minimale e P è non banale, allora necessariamente $P = N$.

□

Lemma 2.13. *Sia G un gruppo e siano H, K, N sottogruppi di G.*

1. *Se K è normale allora $HK = \{hk \mid h \in H, k \in K\}$ è un sottogruppo di G.*

2. *È valida la seguente formula: $|HK| = |H||K|/|H \cap K|$.*

3. *Se N è normale e $K \leq H$ allora si ha $[NH : NK] = [H : (N \cap H)K]$.*

Dimostrazione. 1. Siano $h_1k_1, h_2k_2 \in HK$. Si ha $h_1k_1h_2k_2 = h_1h_2h_2^{-1}k_1h_2k_2$. Poiché K è normale, abbiamo che $h_2^{-1}k_1h_2 = k' \in H$, perciò $h_1k_1h_2k_2 = h_1h_2k'k_2 \in HK$.

2. Sia $n = |H \cap K|$. Mostriamo che per ogni coppia $(h, k) \in H \times K$ esistono esattamente n coppie $(a, b) \in H \times K$ tali che $hk = ab$, da cui segue $n|HK| = |H||K|$. Per ogni $t \in H \cap K$ si ha $hk = (ht)(t^{-1}k)$, perciò si hanno almeno n coppie. Viceversa per ogni coppia (a, b), se $hk = ab$ allora abbiamo un elemento $t = a^{-1}h = bk^{-1} \in H \cap K$, e quindi si hanno al più n coppie.

3. Costruiamo una biezione tra i due insiemi di classi laterali $\{(N\cap H)Kh \mid h \in H\}$ e $\{NKh \mid h \in H\} = \{NKx \mid x \in NH\}$. Osserviamo che se $y \in (N \cap H)K$ allora si ha $NKyx = NKx$ perché $(N \cap H)K \subseteq NK$. Possiamo dunque definire la mappa suriettiva $(N \cap H)Kh \mapsto NKh$. Mostriamo che è anche

iniettiva: se $NKh_1 = NKh_2$ allora $h_1h_2^{-1} \in NK \cap H = (N \cap H)K$, cioè $(N \cap H)Kh_1 = (N \cap H)Kh_2$.

□

Teorema 2.14. *Sia G un gruppo finito risolubile di ordine mn, con $(m, n) = 1$. Allora si ha:*

1. *G contiene un sottogruppo di ordine m.*
2. *Due sottogruppi di G di ordine m sono sempre coniugati.*
3. *Se $k \mid m$ allora ogni sottogruppo di G di ordine k è contenuto in un sottogruppo di G di ordine m.*

Dimostrazione. La dimostrazione procede per induzione su $|G|$. Ci sono due casi.

Caso 1: Esiste un sottogruppo normale proprio H di G il cui ordine non è divisibile per n.

1. Sia m_1n_1 l'ordine di H, dove $m_1 \mid m$, $n_1 \mid n$ e $n_1 < n$. Abbiamo che G/H è un gruppo risolubile di ordine $(m/m_1)(n/n_1)$, con $(m/m_1, n/n_1) = 1$. Quindi per ipotesi induttiva G/H contiene un sottogruppo A/H di ordine (m/m_1), con A sottogruppo di G. Abbiamo che $|A| = |H|[A : H] = (m_1n_1)(m/m_1) = mn_1 < mn$, inoltre per il Teorema 2.11 A è risolubile, perciò per ipotesi induttiva A contiene un sottogruppo di ordine m.

2. Supponiamo che B e C siano sottogruppi di G di ordine m. Poiché H è normale in G, HB è un sottogruppo di G. Sia k l'ordine di HB, allora $k \mid mn$ per il teorema di Lagrange. Si ha che $|HB| = |H||B|/|H \cap B|$, ovvero che $k = m_1n_1m/|H \cap B|$, perciò abbiamo $k|H \cap B| = m_1n_1m$, quindi $k \mid m_1n_1m$. Poiché $(m_1, n) = 1$, esistono due interi x, y tali che $m_1x + ny = 1$, quindi $mn_1m_1x + mn_1ny = mn_1$. Ne segue che $k \mid mn_1$. Per il teorema di Lagrange si ha che $m = |B|$ e $m_1n_1 = |H|$ dividono k, e quindi, poiché $(m, n) = 1$, abbiamo che $mn_1 \mid k$. Di conseguenza $k = |HB| = mn_1$ e, analogamente,

$|HC| = mn_1$. Quindi HB/H e HC/H sono sottogruppi di G/H di ordine m/m_1, e perciò per ipotesi induttiva sono coniugati, ovvero esiste $\bar{x} \in G/H$ tale che $\bar{x}^{-1}(HB/H)\bar{x}$. Ne segue, prendendo le retroimmagini tramite la mappa quoziente, che $x^{-1}HBx = HC$, perciò abbiamo che $x^{-1}Bx$ è un sottogruppo di HC. Poiché $x^{-1}Bx$ e C sono sottogruppi di HC di ordine m, per ipotesi induttiva sono coniugati in HC, e quindi B e C sono coniugati in G.

3. Sia K un sottogruppo di G di ordine k, con $k \mid m$. Per il secondo teorema di isomorfismo si ha che $HK/H \cong K/H \cap K$, e quindi l'ordine di HK/H divide k. Poiché HK/H è un sottogruppo di G/H, il suo ordine divide anche $|G/H| = (m/m_1)(n/n_1)$. Abbiamo che $(k, n) = 1$ perché $k \mid m$, e quindi l'ordine di HK/H divide m/m_1. Per ipotesi induttiva esiste un sottogruppo A/H di G/H di ordine m/m_1 che contiene HK/H. Si ha che K è un sottogruppo di A. Poiché $|A| = |H||A/H| = m_1n_1(m/m_1) = mn_1 < mn$, per ipotesi induttiva K è contenuto in un sottogruppo di A (e quindi di G) di ordine m.

Caso 2: Ogni sottogruppo normale proprio di G ha ordine divisibile per n. Sia H un sottogruppo normale minimale (ne esiste almeno uno perché G è finito), allora per il Lemma 2.12 $|H| = p^r$ per qualche primo p. Poiché $(m, n) = 1$ e $n \mid |H|$, abbiamo che $n = p^r$, e quindi H è un p-sottogruppo di Sylow di G. Inoltre H è l'unico p-sottogruppo di Sylow di G perché è normale. Osserviamo che H è l'unico sottogruppo normale minimale di G, infatti se così non fosse avremmo $n = p^r$ e $n = q^s$ con p, q primi distinti. Ne segue che ogni sottogruppo normale non banale di G contiene necessariamente H.

1. Sia K un sottogruppo normale di G tale che K/H sia un sottogruppo normale minimale di G/H. Per il Lemma 2.12 $|K/H| = q^s$ per qualche primo q diverso da p, e quindi $|K| = p^rq^s$. Sia S un q-sottogruppo di Sylow di K e sia M il normalizzante di S in G. Mostriamo che $|M| = m$. Abbiamo che HS è un sottogruppo di K perché H è normale in K, inoltre $H \cap S = 1$. Ne segue che $|HS| = |H||S|/|H \cap S| = p^rq^s = |K|$, e quindi $K = HS$.

Poiché K è normale in G e $S \leq K$, ogni sottogruppo coniugato a S in G è contenuto in K. Inoltre questi sono coniugati a S anche in K perché S è un sottogruppo di Sylow di K. Sia $N = N_K(S)$, il numero c di sottogruppi coniugati a S in G è $[G : M] = [K : N]$ per la Proposizione 2.2. Poiché $S \leq N \leq K$, abbiamo $K \geq HN \geq HS = K$, e quindi $K = HN$ e $c = [G : M] = [K : N] = [HN : N] = [H : H \cap N]$. Se mostriamo che $H \cap N = 1$, allora abbiamo $c = |H| = p^r$ e quindi $|M| = |G|/[G : M] = mp^r = m$. Per far ciò mostriamo prima che $H \cap N = Z(K)$ e poi che $Z(K) = 1$, dove $Z(K)$ è il centro di K.
Siano $x \in H \cap N$ e $k \in K$. Poiché $K = HS$, abbiamo $k = hs$ per qualche $h \in H$ e $s \in S$. Per il Lemma 2.12 H è abeliano, quindi, dato che $x \in H$, è sufficiente mostrare che $xs = sx$ per avere che $xk = kx$ ovvero $x \in Z(K)$. Abbiamo che $(xsx^{-1})s^{-1} \in S$ perché $x \in N = N_K(S)$. Abbiamo inoltre che $x(sx^{-1}s^{-1}) \in H$ perché $x \in H$ e H è normale in G. Quindi $xsx^{-1}s^{-1} \in H \cap S = 1$, ovvero $xs = sx$.
Si può verificare che $Z(K)$ è un sottogruppo caratteristico di K. Poiché K è normale in G, per il Lemma 2.12 $Z(K)$ è normale in G. Supponiamo per assurdo che $Z(K) \neq 1$. Allora $Z(K)$ contiene necessariamente H. Di conseguenza, poiché $K = HS$, S è normale in K. Per il Lemma 2.12 S è pienamente invariante in K e quindi normale in G, essendo K normale in G. Ne segue che $H \leq S$ e questo porta a una contraddizione. Si ha allora $Z(K) = 1$.

2. Sia M come sopra e sia B un sottogruppo di G di ordine m. Abbiamo che $|BK|$ è divisibile per $|B| = m$ e per $|K| = p^r q^s$. Poiché $(m, p) = 1$, $|BK|$ è divisibile anche per $p^r m = nm = |G|$, e quindi $BK = G$. Di conseguenza $G/K = BK/K \cong B/B \cap K$, perciò $|B \cap K| = |B|/|G/K| = q^s$. Per il secondo teorema di Sylow $B \cap K$ è coniugato a S in K. Inoltre $B \cap K$ è normale in B perché K è normale in G, e quindi B è contenuto in $N_G(B \cap K)$. Si può verificare che sottogruppi coniugati hanno normalizzanti coniugati. Ne segue che $N_G(B \cap K)$ e $N_G(S) = M$ sono coniugati in G, e quindi $|N_G(B \cap K)| = |M| = m$. Poiché $|B| = m$ e $B \leq N_G(B \cap K)$, abbiamo che $B = N_G(B \cap K)$, perciò B e M sono coniugati.

3. Sia $D \leq G$ con $|D| = k$ e $k \mid m$. Siano M e H come sopra. Si ha che $D \cap H = 1$ e $|DH| = |D||H|/|D \cap H| = kp^r$. Abbiamo inoltre che $|G| = mp^r$, $M \cap H = 1$ e $MH = G$ perché $|MH| = |M||H|/|M \cap H| = mp^r = |G|$. Perciò $M(DH) = G$ e quindi $|M \cap DH| = |M||DH|/|MDH| = m(kp^r)/mp^r = k$. Di conseguenza, posto $M^* = M \cap DH$ e applicando il secondo punto di questo teorema al gruppo DH, si ha che M^* e D sono coniugati, ovvero esiste $a \in G$ tale che $aMa^{-1} = D$. Poiché $M^* \leq M$, D è contenuto in $a^{-1}Ma$, ovvero in un sottogruppo di ordine m.

Nelle notazioni del teorema, un sottogruppo di G di ordine m è detto π-*sottogruppo di Hall*, dove π è l'insieme dei primi che dividono m. Nel caso di gruppi non risolubili, i sottogruppi di Hall potrebbero non esistere. Ad esempio mostriamo che in A_5 non esiste un $\{2,5\}$-sottogruppo di Hall. Supponiamo per assurdo che H sia un $\{2,5\}$-sottogruppo di Hall di A_5, poiché $|A_5| = 60$, H deve avere ordine 20, e quindi $[A_5 : H] = 3$. Considerando come azione di A_5 sull'insieme delle classi laterali di H la traslazione sinistra, otteniamo un omomorfismo $\rho : A_5 \to S_3$ il cui nucleo è incluso in H. Si ha perciò $\ker\rho \neq A_5$ e, ovviamente, $\ker\rho \neq 1$, ovvero $\ker\rho$ è un sottogruppo proprio normale e non banale di A_5, che è assurdo perché A_5 è un gruppo semplice. □

Capitolo 3

Estensione della teoria di Sylow ai gruppi profiniti

Riprendiamo ora con lo studio dei gruppi profiniti per mostrare come i risultati visti nel capitolo precedente possano essere estesi anche a questa classe di gruppi. Per prima cosa vediamo le estensioni del concetto di indice di un sottogruppo e del teorema di Lagrange. In questo capitolo sarà sottinteso che i sottogruppi di cui si parla siano chiusi.

3.1 Sottogruppi di Sylow e di Hall

Un *numero soprannaturale* (o *numero di Steinitz*) è un prodotto formale infinito $\prod p^{n(p)}$, su tutti i primi p, nel quale ciascun esponente $n(p)$ è un numero naturale oppure infinito.

Siano $\prod p^{n(p)}$ e $\prod p^{m(p)}$ numeri soprannaturali, diciamo che $\prod p^{m(p)}$ divide $\prod p^{n(p)}$ se $m(p) \leq n(p)$ per ogni p. Possiamo quindi definire il minimo comune multiplo: sia $(a_i \mid i \in I)$ una famiglia di numeri soprannaturali, con $a_i = \prod p^{n(p,i)}$ per ogni i, definiamo

$$\mathrm{mcm}(a_i \mid i \in I) = \prod p^{s(p)}, \qquad \text{con } s(p) = \sup(n(p,i) \mid i \in I).$$

Analogamente definiamo

$$\prod_{i\in I} a_i = \prod p^{t(p)}, \qquad \text{con } t(p) = \sum_{i\in I} n(p,i).$$

Adottiamo le convenzioni standard riguardo ∞: ad esempio, $s(p) = \infty$ se solo se $n(p,i) = \infty$ per qualche i oppure gli $n(p,i)$ sono finiti ma non limitati. Osserviamo che se $(a_i \mid i \in I)$ e $(b_j \mid j \in J)$ sono due famiglie di numeri soprannaturali, allora

$$(\text{mcm}(a_i \mid i \in I))(\text{mcm}(b_j \mid j \in J)) = \text{mcm}(a_i b_j \mid i \in I, j \in J).$$

Definizione 3.1. Sia G un gruppo profinito. L'*indice* $[G : H]$ di un sottogruppo (chiuso) H di G è il minimo comune multiplo degli indici dei sottogruppi aperti di G che contengono H. L'*ordine* $|G|$ di G è $[G : 1]$, e l'ordine di un elemento x di G è l'ordine del sottogruppo generato topologicamente da x, ovvero la chiusura del gruppo astratto generato da x.

Osservazione 3.2. L'indice di un sottogruppo H di G può essere equivalentemente definito come $\text{mcm}([G : NH] \mid N \lhd_O G)$. Infatti $\text{mcm}([G : U] \mid U \text{ aperto}, H \leq U) \geq \text{mcm}([G : NH] \mid N \lhd_O G)$ perché gli NH sono particolari aperti contenenti H (NH è aperto in quanto unione di aperti del tipo Nh), viceversa poiché ciascun sottogruppo aperto U con $H \leq U$ contiene un sottogruppo normale aperto N (segue dal Lemma 1.7), si ha che $|NH|$ divide $|U|$ per il teorema di Lagrange per indici finiti, e quindi $[G : U]$ divide $[G : NH]$.

Come conseguenza della Proposizione 1.9, un gruppo profinito G è un gruppo pro-p se e solo se G/N ha ordine una potenza di p per ogni $N \lhd_O G$. Ne segue che i gruppi pro-p sono esattamente i gruppi profiniti di ordine p^n con $n \leq \infty$.

Vediamo ora il Teorema di Lagrange per i gruppi profiniti.

Teorema 3.3. *Siano H, K sottogruppi di G tali che $K \leq H \leq G$. Allora $[G : K] = [G : H][H : K]$.*

Dimostrazione. Usiamo alcuni risultati riguardanti gli indici finiti. Sia $N \lhd_O G$, allora NK è un sottogruppo aperto di G e quindi ha indice finito. Per il teorema di Lagrange nel caso finito si ha dunque $[G : NK] = [G : NH][NH : NK]$. Inoltre per il Lemma 2.13 abbiamo che $[NH : NK] = [H : (N \cap H)K]$. Di conseguenza si ha

$$[G : NK] = [G : NH][H : (N \cap H)K]. \tag{3.1}$$

Inoltre $N \cap H$ è un aperto normale nella topologia indotta in H, e quindi $\mathrm{mcm}([H : (N \cap H)K] \mid N \lhd_O G) \leq \mathrm{mcm}([H : MK] \mid M \lhd_O H) = [H : K]$. Quindi, facendo variare $N \lhd_O G$ nella formula (3.1) e usando l'Osservazione 3.2, si ottiene che $[G : K]$ divide $[G : H][H : K]$.

Viceversa, siano $N_1 \lhd_O G$ e $N_2 \lhd_O H$, allora N_2 è l'intersezione con H di un insieme aperto in G, perciò esiste $M \lhd_O G$ tale che $M \cap H \leq N_2$. Poniamo $N = M \cap N_1$. Abbiamo che $[G : N_1H][H : N_2K]$ divide $[G : NH][H : (N \cap H)K]$ che, per la formula (3.1), è uguale a $[G : NK]$. Quindi, facendo variare $N_1 \lhd_O G$ e $N_2 \lhd_O H$ e considerando il minimo comune multiplo, si ottiene che $[G : H][H : K]$ divide $[G : K]$. □

Lemma 3.4. *Sia $(H_i \mid i \in I)$ una famiglia di sottogruppi tale che per ogni $i, j \in I$ esiste un indice $k \in I$ con $H_k \leq H_i \cap H_j$, allora vale*

$$[G : \bigcap H_i] = \mathrm{mcm}([G : H_i] \mid i \in I).$$

Dimostrazione. Per il Teorema 3.3 abbiamo $[G : \bigcap H_i] = [G : H_i][H_i : \bigcap H_i]$ per ogni i, quindi $\mathrm{mcm}([G : H_i] \mid i \in I)$ divide $[G : \bigcap H_i]$. Mostriamo che vale anche il viceversa ovvero che $[G : \bigcap H_i] = \mathrm{mcm}([G : U] \mid U \text{ aperto}, \bigcap H_i \leq U)$ divide $\mathrm{mcm}([G : H_i] \mid i \in I)$. Se U è un sottogruppo aperto contenente $\bigcap H_i$, allora $\bigcap(H_i \cap (G \setminus U)) = \emptyset$. Gli insiemi $H_i \cap (G \setminus U)$ sono chiusi per ogni i, quindi per la compattezza si ha

$$\bigcap_{\lambda=1}^{r} (H_{i_\lambda} \cap (G \setminus U)) = \emptyset$$

per qualche insieme finito $\{i_1, ..., i_r\}$. Perciò $\bigcap_{\lambda=1}^{r} H_{i_\lambda} \leq U$. Prendiamo $k \in I$ tale che $H_k \leq H_{i_\lambda}$ per $\lambda = 1, ..., r$. Di conseguenza si ha $H_k \leq U$ e quindi $[G : U]$ divide $[G : H_k]$. □

Vediamo ora il teorema di Sylow per i gruppi profiniti.

Definizione 3.5. Sia G un gruppo profinito e sia p un primo. Un *sottogruppo p-Sylow* di G è un sottogruppo P tale che $|P|$ è una potenza (anche infinita) di p e $[G : P]$ è coprimo con p.

Notiamo che i sottogruppi p-Sylow sono sottogruppi pro-p massimali e, nel caso finito, coincidono con i p-sottogruppi di Sylow.

Teorema 3.6. *Sia G un gruppo profinito e sia p un primo.*

1. *G ha un sottogruppo p-Sylow.*
2. *Se P è un sottogruppo p-Sylow di G e T è un sottogruppo pro-p, allora si ha $g^{-1}Tg \leq P$ per qualche $g \in G$.*
3. *Ogni sottogruppo pro-p di G è contenuto in un sottogruppo p-Sylow.*
4. *Se P_1, P_2 sono sottogruppi p-Sylow di G, allora $g^{-1}P_1g = P_2$ per qualche $g \in G$.*

Dimostrazione. 1. Sia I l'insieme dei sottogruppi chiusi di G di indice coprimo con p. Abbiamo che I è non vuoto perché $G \in I$, inoltre I è parzialmente ordinato rispetto alla relazione d'ordine $\preceq$ così definita: $A \preceq B$ se e solo se $B \leq A$. Sia J una catena in I (cioè per ogni $H_1, H_2 \in J$ si ha $H_1 \leq H_2$ oppure $H_2 \leq H_1$), allora per il Lemma 3.4 si ha $\bigcap(H \mid H \in J) \in I$. Di conseguenza, per il lemma di Zorn, I contiene un elemento minimale P. Si ha che $[G : P]$ è coprimo con p, mostriamo che P è un gruppo pro-p. Supponiamo per assurdo che P non sia un gruppo pro-p, allora per il Teorema 1.11 esiste $M \lhd_O P$ tale che $|P/M|$ non è una potenza di p. Di conseguenza, per il teorema di Sylow sui gruppi finiti, P/M ha un sottogruppo p-Sylow $Q/M \leq P/M$. Poiché M è aperto in P e Q è una unione finita di classi laterali di M, anche Q è aperto in P. Ne segue che Q è chiuso in P e quindi anche in G. Inoltre per il Teorema 3.3 si ha $[G : Q] = [G : P][P : Q]$, perciò $[G : Q]$ è coprimo con p. Questo contraddice la minimalità di P.

2. Sia $N \lhd_O G$, allora $N \cap P \lhd_O P$ e $NP/N \cong P/(N \cap P)$, perciò NP/N è un p-gruppo. Inoltre $[G : NP]$ divide $[G : P]$, e quindi NP/P è un sottogruppo p-Sylow di G/N. Analogamente NT/N è un p-sottogruppo di G/N. Poniamo

$$R(N) = \{g \mid g^{-1}(NT)g \subseteq NP\}.$$

Questo insieme è non vuoto per il secondo teorema di Sylow sui gruppi finiti. Inoltre la condizione $g^{-1}(NT)g \subseteq NP$ implica che per ogni $x \in N$ vale $x^{-1}g^{-1}NTgx \subseteq x^{-1}NPx = NP$, cioè se $g \in R(N)$ allora $gN \subseteq R(N)$. Si ha dunque che $R(N)$ è un'unione di classi laterali di N, e quindi è chiuso. Usando il terzo teorema di isomorfismo si può verificare che se M, N sono sottogruppi normali aperti e $M \leq N$, allora $R(M) \subseteq R(N)$; perciò se $N_1, ..., N_r$ sono sottogruppi normali aperti, si ha

$$R(N_1) \cap ... \cap R(N_r) \supseteq R(N_1 \cap ... \cap N_r) \neq \emptyset.$$

Dunque ogni famiglia finita di insiemi del tipo $R(N)$ ha intersezione non vuota, e quindi per la compattezza esiste un elemento $g \in \bigcap(R(N) \mid N \lhd_O G)$. Per ogni N si ha $g^{-1}Tg \leq NP$, e quindi usando il Lemma 1.8 si ha

$$g^{-1}Tg \leq \bigcap(NP \mid N \lhd_O G) = P.$$

Gli ultimi due punti seguono dai primi due osservando che un sottogruppo coniugato a un sottogruppo p-Sylow è ancora un sottogruppo p-Sylow. □

Concludiamo la sezione con la discussione sui sottogruppi di Hall nel caso profinito. Sia π un insieme di primi. Un gruppo finito F è detto *π-gruppo* se ogni primo che divide $|F|$ appartiene a π; un gruppo profinito è detto *gruppo pro-π* se soddisfa la stessa condizione o, equivalentemente, se è limite inverso di π-gruppi.

Un *sottogruppo di Hall* di un gruppo profinito G è un sottogruppo H tale che $|H|$ e $[G : H]$ sono coprimi. Più precisamente, se π è un insieme di primi, un sottogruppo H di G è detto *sottogruppo π-Hall* se $|H|$ è divisibile solo per primi appartenenti a π e $[G : H]$ è divisibile solo per primi non appartenenti a π.

Osserviamo che i sottogruppi π-Hall di un gruppo profinito sono sottogruppi pro-π massimali, ma i sottogruppi pro-π massimali non sono necessariamente sottogruppi π-Hall, anche nel caso finito. Inoltre se p è primo, un sottogruppo $\{p\}$-Hall di un gruppo profinito è semplicemente un sottogruppo p-Sylow.

Teorema 3.7. *Sia G un gruppo pro-risolubile e sia π un insieme di primi.*

1. *G ha un sottogruppo π-Hall.*
2. *Se P è un sottogruppo π-Hall e T è un sottogruppo pro-π, allora $g^{-1}Tg \in P$ per qualche $g \in G$.*
3. *Ogni sottogruppo pro-π di G è contenuto in un sottogruppo π-Hall.*
4. *Se P_1, P_2 sono sottogruppi π-Hall di G, allora $g^{-1}P_1g = P_2$ per qualche $g \in G$.*

Poiché questi risultati valgono per i gruppi finiti, la dimostrazione nel caso profinito è analoga a quella del Teorema 3.6.

3.2 Un esempio

Consideriamo $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ con la relazione d'ordine $r \leq s \iff r|s$. Notiamo che $(\mathbb{N}, \leq)$ è un insieme diretto perché dati due numeri naturali positivi esiste sempre il massimo comune divisore. Consideriamo ora la famiglia di gruppi topologici $\mathbb{Z}/n\mathbb{Z}$ dotati della topologia discreta, e, per ogni $i, j \in \mathbb{N}$ con $i \leq j$, sia $\varphi_{ij} : \mathbb{Z}/j\mathbb{Z} \to \mathbb{Z}/i\mathbb{Z}$ la mappa definita da $[a]_j \mapsto [a]_i$; poiché vale $\varphi_{ij}\varphi_{jk} = \varphi_{ik}$, abbiamo che $(\mathbb{Z}/n\mathbb{Z}, \varphi_{ij})$ è un sistema inverso indicizzato da $\mathbb{N}^*$. Indichiamo con $\widehat{\mathbb{Z}}$ il limite inverso degli $\mathbb{Z}/n\mathbb{Z}$, ovvero

$$\widehat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{N}^*} (\mathbb{Z}/n\mathbb{Z}) = \{(x_n)_{n \in \mathbb{N}^*} \mid x_n \in \mathbb{Z}/n\mathbb{Z}, x_m = \varphi_{nm}(x_n) \text{ per ogni } n, m \in \mathbb{N}^*\}.$$

$\widehat{\mathbb{Z}}$ è detto *completamento profinito di* $\mathbb{Z}$, ed è un gruppo prociclico.

Analogamente, fissando un primo p e considerando la famiglia dei soli $\mathbb{Z}/p^n\mathbb{Z}$, indichiamo

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}^*} (\mathbb{Z}/p^n\mathbb{Z}) \leq Cr(\mathbb{Z}/p^n\mathbb{Z} \mid n \in \mathbb{N}^*)$$

Mostriamo che $\widehat{\mathbb{Z}} \cong Cr_{p\in\mathcal{P}}(\mathbb{Z}_p)$, dove $\mathcal{P}$ è l'insieme dei numeri primi.
Costruiamo un isomorfismo $\varphi : \widehat{\mathbb{Z}} \to Cr_{p\in\mathcal{P}}(\mathbb{Z}_p)$. Osserviamo che gli elementi di $\widehat{\mathbb{Z}}$ sono successioni di classi resto modulo n con $n \in \mathbb{N}^*$, ovvero sono del tipo $([a_n]_n)_{n\in\mathbb{N}^*} = ([a_1]_1, [a_2]_2, ...)$; invece gli elementi di $\mathbb{Z}_p$ sono successioni di classi resto modulo p^n con $n \in \mathbb{N}^*$. Risulta quindi naturale definire la mappa

$$\varphi_p : \widehat{\mathbb{Z}} \to \mathbb{Z}_p, \quad ([a_n]_n)_{n\in\mathbb{N}^*} \mapsto ([a_{p^k}]_{p^k})_{k\in\mathbb{N}^*} = ([a_p]_p, [a_{p^2}]_{p^2}, ...).$$

Poniamo allora

$$\varphi : \widehat{\mathbb{Z}} \to Cr_{p\in\mathcal{P}}(\mathbb{Z}_p), \quad a = ([a_n]_n)_{n\in\mathbb{N}^*} \mapsto (\varphi_p(a))_{p\in\mathcal{P}}.$$

Mostriamo che φ è iniettiva.
Siano $a, b \in \widehat{\mathbb{Z}}$ tali che $\varphi(a) = \varphi(b)$, cioè $\varphi_p(a) = \varphi_p(b)$ per ogni $p \in \mathcal{P}$. Questo significa che i termini delle successioni a e b in posizioni corrispondenti a potenze di primi coincidono. Fissiamo $j \in \mathbb{N}^*$ e consideriamo la componente j-esima $[a_j]_j$ di a; siano $p_1, ..., p_r \in \mathcal{P}$ e $k_1, ..., k_r \in \mathbb{N}$ tali che $j = p_1^{k_1}...p_r^{k_r}$. Per la compatibilità delle mappe φ_{ij} abbiamo

$$\begin{cases} [a_{p_1^{k_1}}]_{p_1^{k_1}} = \varphi_{p_1^{k_1} j}([a_j]_j) = [a_j]_{p_1^{k_1}} \\ \vdots \\ [a_{p_r^{k_r}}]_{p_r^{k_r}} = \varphi_{p_r^{k_r} j}([a_j]_j) = [a_j]_{p_r^{k_r}}. \end{cases}$$

Per il teorema cinese del resto esiste un'unica classe resto modulo j, diciamo $[c_j]_j$, che soddisfa il sistema, cioè $[c_j]_j = [a_j]_j$. Analogamente si mostra che $[b_j]_j = [c_j]_j = [a_j]_j$.

Mostriamo ora che φ è suriettiva.
Per fare questo, troviamo una funzione $\psi : Cr_{p\in\mathcal{P}}(\mathbb{Z}_p) \to \widehat{\mathbb{Z}}$ che sia un'inversa destra

di φ, cioè tale che $\varphi\psi = id_{Cr_{p\in\mathcal{P}}(\mathbb{Z}_p)}$.
Sia $((\![a_{p^n}]_{p^n})_{n\in\mathbb{N}^*})_{p\in\mathcal{P}} = (([a_2]_2, [a_4]_4, ...), ([a_3]_3, [a_9]_9, ...), ...)$ un elemento di $Cr_{p\in\mathcal{P}}(\mathbb{Z}_p)$, definiamone l'immagine tramite ψ. L'immagine deve essere del tipo $([b_n]_n)_{n\in\mathbb{N}^*} \in \widehat{\mathbb{Z}}$. Notiamo subito che, affinché ψ sia inversa destra di φ, dobbiamo porre $[b_{p^k}]_{p^k} = [a_{p^k}]_{p^k}$ per ogni $p \in \mathcal{P}$ e per ogni $k \in \mathbb{N}^*$. Dobbiamo però anche definire l'immagine in modo che questa sia effettivamente contenuta in $\widehat{\mathbb{Z}}$, ovvero che soddisfi le condizioni di compatibilità. Sia $j = p_1^{k_1}...p_r^{k_r} \in \mathbb{N}^*$, definiamo $[b_j]_j$ come l'unica classe resto modulo j che risolve il sistema

$$\begin{cases} [b_j]_{p_1^{k_1}} = [a_{p_1^{k_1}}]_{p_1^{k_1}} \\ \vdots \\ [b_j]_{p_r^{k_r}} = [a_{p_r^{k_r}}]_{p_r^{k_r}} \end{cases}$$

la cui esistenza è garantita dal teorema cinese del resto. Così facendo si ha che se $l = p_1^{m_1}...p_r^{m_r}$ divide k, allora è verificato anche il seguente sistema

$$\begin{cases} [b_j]_{p_1^{m_1}} = [a_{p_1^{m_1}}]_{p_1^{m_1}} \\ \vdots \\ [b_j]_{p_r^{m_r}} = [a_{p_r^{m_r}}]_{p_r^{m_r}} \end{cases}$$

cioè il sistema è risolto dalla classe resto $[b_j]_l$, ma per come abbiamo definito $[b_l]_l$, anche questa risolve tale sistema, e quindi per unicità della soluzione si ha $[b_j]_l = [b_l]_l$.

Per concludere mostriamo che un sottogruppo p-Sylow di $\widehat{\mathbb{Z}}$ è isomorfo a $\mathbb{Z}_p$.
Osserviamo prima che $\tilde{a} = ([a_n]_n)_{n\in\mathbb{N}^*} \in \widehat{\mathbb{Z}}$ ha ordine divisibile per un primo q se e solo se $\varphi_q(\tilde{a}) \neq 0$. Infatti se $\varphi_q(\tilde{a}) \neq 0$ allora esiste $k \in \mathbb{N}^*$ tale che $[a_{q^k}]_{q^k} \neq [0]_{q^k}$, perciò $[a_{q^k}]_{q^k}$ ha ordine divisibile per q in $\mathbb{Z}/q^k\mathbb{Z}$, e quindi anche a ha ordine divisibile per q. Viceversa se $\tilde{a}$ ha ordine divisibile per q, allora esiste un intero positivo j tale che $[a_j]_j$ ha ordine divisibile per q in $\mathbb{Z}/j\mathbb{Z}$. Sia $j = q^t l$, con $t > 0$ e $(q, l) = 1$. Poiché l'ordine di $[a_j]_j$ è $j/(a_j, j)$, abbiamo che q^t non divide a_j, e quindi $[a_j]_{q^t} \neq [0]_{q^t}$. Per la condizione di compatibilità di $\varphi_{q^t j}$, si ha $[a_{q^t}]_{q^t} = [a_j]_{q^t} \neq [0]_{q^t}$, perciò $\varphi_q[\tilde{a}] \neq 0$.

Ne segue che l'insieme $\{\tilde{a} \in \widehat{\mathbb{Z}} \mid \varphi_q(\tilde{a}) = 0 \text{ per ogni primo } q \neq p\} \cong \mathbb{Z}_p$ contiene tutti e soli gli elementi di ordine una potenza (anche infinita) di p, e quindi è un sottogruppo pro-p massimale, cioè un sottogruppo p-Sylow di $\widehat{\mathbb{Z}}$; inoltre, poiché $\widehat{\mathbb{Z}}$ è abeliano, per il Teorema 3.6 non esistono altri sottogruppi p-Sylow di $\widehat{\mathbb{Z}}$.

Bibliografia

[1] S. Francaviglia, *Topologia*, CreateSpace, Regno Unito, 2018.

[2] T. W. Hungerford, *Algebra*, Springer-Verlag, New York-Berlino, 1980.

[3] L. Ribes, P. Zalesskii, *Profinite Groups*, Springer-Verlag, Berlino, 2000.

[4] D. J. S. Robinson, *A course in the theory of groups*, second edition, Springer-Verlag, New York, 1996.

[5] J. S. Wilson, *Profinite groups*, Oxford University Press, New York, 1998.