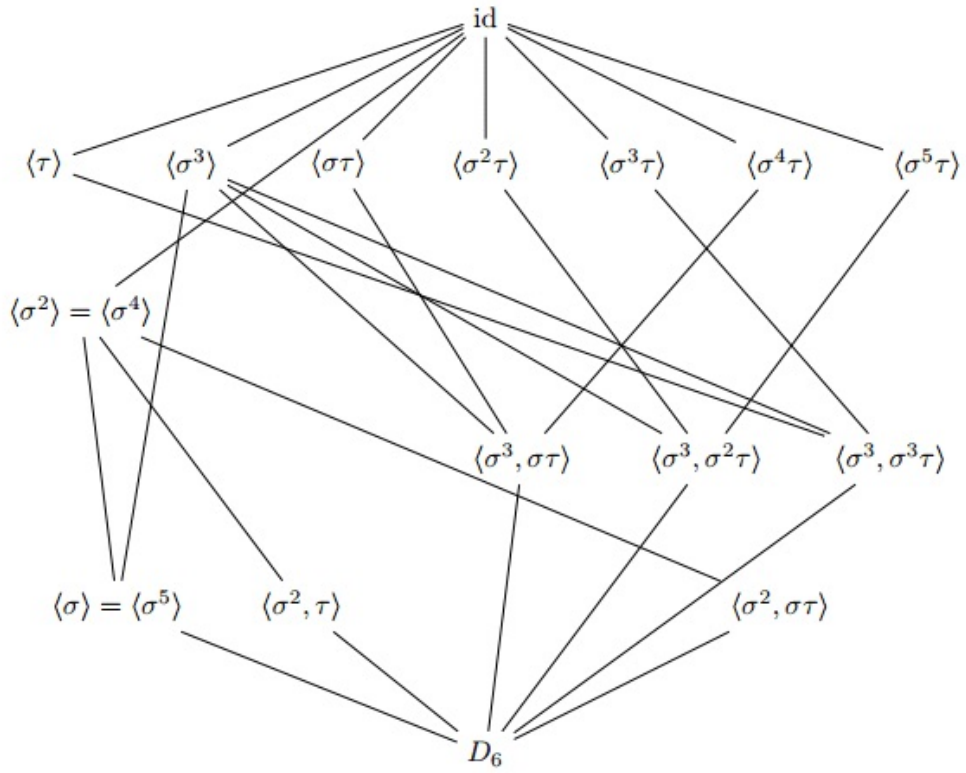

Gruppi risolubili e teoremi di Hall

Marco Damele

5 luglio 2024

Introduzione

Sia G un gruppo finito. In generale è interessante sapere,preso un sottogruppo normale N di G non banale, se si possa ricostruire il gruppo G a partire da N e da G/N.Chiaramente quà il termine "ricostruire" è molto vago, ma ci riferiamo principalmente al fatto se G possa scriversi come prodotto semidiretto di N e G/N. (per informazioni sul prodotto semidiretto potete consultare [3]). Chiaramente la risposta è negativa. Ad esempio se p è un primo e prendiamo $\mathbf{Z}_{p^2}$ abbiamo che l'unico sottogruppo normale non banale è $\mathbf{Z}_p$ e il quoziente ancora $\mathbf{Z}_p$ ma ovviamente $\mathbf{Z}_{p^2}$ non è semidiretto di $\mathbf{Z}_p$ con $\mathbf{Z}_p$.In merito a questo problema abbiamo il seguente teorema (la cui dimostrazione si può trovare in [3]):

Teorema 0.0.1. *(Schur-Zassenhaus Lemma, 1937) Sia G un gruppo finito e $N \trianglelefteq G$: (|N|,|G/N|)=1. Allora $G \simeq N \rtimes_\phi G/N$ per qualche omomorfismo $\phi : G/N \longrightarrow N$.*

quindi, in particolare, se G è un gruppo finito e scriviamo |G|=ab con (a,b)=1 allora se troviamo $N \trianglelefteq G$: |N|=a si avrà che $G \simeq N \rtimes_\phi G/N$ per qualche omomorfismo $\phi : G/N \longrightarrow N$. Da qui la domanda di carattere più generale: Dato un gruppo finito G se scriviamo |G|=ab con (a,b)=1 riusciamo sempre a trovare $H \leq G$: |H|=a ? La risposta sfortunatamente è negativa come vederemo più avanti. Tuttavia ci sono diversi casi in cui la risposta è affermativa:

- Se a=p^m con p primo e (p,b)=1 allora la risposta è affermativa per il primo teorema di Sylow.
- Se G è un gruppo così detto "risolubile", allora indipendentemente da come siano a e b (purchè (a,b)=1), la risposta è affermativa. Nel corso delle dispense dimostreremo questo fatto che và sotto il nome di "Primo teorema di Hall". Esplicitamente:

Teorema 0.0.2. *(P.Hall) Sia G un gruppo finito e risolubile e scriviamo |G|=ab con (a,b)=1. Allora esiste $H \leq G$: |H|=a. Inoltre se $K \leq G$: |K|=a allora H e K sono coniugati in G (cioé esiste $g \in G$: K=gHg^{-1})*

Attenzione però che il teorema appena citato non garantisce che il sottogruppo che troviamo sia anche normale in G. In effetti può capitare che tutti i sottogruppi di ordine a non siano normali. Si pensi ad esempio a $\mathbf{S}_3$. Abbiamo che $| \mathbf{S}_3 | = 6 = 2 \cdot 3$ ma tutti i sottogruppi di ordine 2 devono essere ciclici di ordine 2 quindi generati da elementi di ordine 2 e cioé <(12)>,<(13)> e <(23)> che non sono normali in G. L'obbiettivo di queste note è suscitare il più possibile l'interesse per i gruppi risolubili e arrivare a dimostrare il primo teorema di Hall.La dimostrazione del primo teorema di Hall e gli argomenti che tratteremo in generale usano spesso i teoremi di Sylow. Perciò per completezza ricordiamoli :

Teorema 0.0.3. *(Primo teorema di Sylow) Sia G un gruppo finito e scriviamo |G|=$p^m b$ con p primo : (p,b)=1. Allora esiste $H \leq G$: |H|=p^m.*

Teorema 0.0.4. *(Secondo teorema di Sylow) Sia G un gruppo finito e scriviamo |G|=p^mb con p primo : (p,b)=1. Se H,K sono sottogruppi di G di ordine p^m allora sono coniuigati.*

Teorema 0.0.5. *(Terzo teorema di Sylow) Sia G un gruppo finito e scriviamo |G|=p^mb con p primo : (p,b)=1. Denotiamo con Sylp(G) l'insieme dei sottogruppi di G di ordine p^m (anche detti p-sylow di G). Allora |Sylp(G)|=1 (mod p) e |Sylp(G)| | b.*

Le dimostrazioni di questi tre teoremi si possono trovare in [2].Tuttavia per completezza mettiamo un appendice a fine dispense in cui dimostriamo tali teoremi.

Capitolo 1

Gruppi risolubili

1.1 Definizione di gruppo risolubile

Definizione 1.1.1. *Sia G un gruppo. Una serie normale di G è una sequenza di sottogruppi di G uno normale nell'altro:*

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{r-1} \trianglelefteq N_r = G$$

I fattori della serie normale sono i gruppi quoziente $\frac{N_{i+1}}{N_i}$ $\forall$ *i=0, . . . , r-1.*

Nota 1.1.1. *Stiamo chiedendo che $\forall$ i=0,...,r-1 N_i sia normale in N_{i+1} non che N_i sia normale in G. Può capitare che se G è un gruppo e H,H' sono sottogruppi di G allora $H \triangleleft H'$ ma H non è normale in G. Ad esempio consideriamo il gruppo S_4 e i suoi due sottogruppi $H = <(12)(34)>$, $\mathbf{V} = \{e, (12)(34), (13)(24), (14)(23)\}$ (sottogruppo di Klein). Allora H è normale in $\mathbf{V}$ poiché l'indice di H in $\mathbf{V}$ è 2 tuttavia H non è normale in G (ad esempio perché $(123)(12)(34)(132) \notin H$)*

Esempio 1.1.1. *Una serie normale per il gruppo $\mathbf{Z}_{2n}$ con n>1 è data da:*

$$\{e\} \triangleleft <[2]_n> \triangleleft \mathbf{Z}_{2n}$$

Esempio 1.1.2. *Una serie normale per il gruppo $\mathbf{D}_n = <r,s>$ dove $r^n=1$, $s^2=1$,$srs^{-1}=r^{-1}$ con $n \geq 3$ è data da:*

$$\{e\} \triangleleft <r> \triangleleft \mathbf{D}_n$$

Definizione 1.1.2. *Un gruppo G è detto risolubile se ammette una serie normale :*

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{r-1} \trianglelefteq N_r = G$$

tale che $\forall$ i=0, . . . , r-1 $\frac{N_{i+1}}{N_i}$ *è abeliano. Una tale serie è detta serie abeliana.*

Nota 1.1.2. *L'importanza dei gruppi risolubili nasce nel contesto delle equazioni algebriche. Galois ([1]) nel 1831 ha dimostrato che preso un campo $\mathbf{K}$ di caratteristica 0 e un polinomio $f \in \mathbf{K}[X]$ allora le radici di f sono esprimibili per radicali su $\mathbf{K}$ se e solo se il gruppo di Galois di f su $\mathbf{K}$ è un gruppo risolubile.Quindi preso ad esempio un polinomio $f \in \mathbf{Q}[X]$ se vogliamo capire se le sue radici sono esprimibili per radicali su $\mathbf{Q}$ possiamo*

calcolare il gruppo di Galois di f su $\mathbf{Q}$ *e capire se questo è risolubile. Un altro risultato che mostra l'importanza dello studio dei gruppi risolubili è il teorema di Feit–Thompson del 1963 che afferma che ogni gruppo finito di ordine dispari è risolubile. Una cosa curiosa di questo teorema è che il suo enunciato è facilmente comprensibile sebbene la sua dimostrazione di 255 pagine occupi un volume intero del Pacific Journal of Mathematics.*

Esempio 1.1.3. *Sia A un gruppo abeliano. Allora A è risolubile poichè la serie normale:*

$$\{e\} \trianglelefteq A$$

è abeliana.

Esempio 1.1.4. *Sia n≥3 allora* $\mathbf{D}_n$ *è risoluibile poiché la serie normale*

$$\{e\} \triangleleft <r> \triangleleft \mathbf{D}_n$$

è abeliana avendo come fattori $\mathbf{Z}_2$ *e* $\mathbf{Z}_n$

1.2 Proprietà dei gruppi risolubili

Iniziamo a vedere alcune proprietà dei gruppi risolubili.Prima di iniziare ricordiamo il secondo teorema di isomorfismo per gruppi:

Teorema 1.2.1. *Sia G un gruppo e N,T* $\leq$ *G con N* $\triangleleft$ *G. Allora N* $\cap$ *T* $\triangleleft$ *T e si ha che:*

$$\frac{T}{N \cap T} \simeq \frac{NT}{N}$$

Proposizione 1.2.1. *Sia G un gruppo risolubile e H* $\leq$ *G. Allora H è risolubile.*

Dimostrazione. Poichè G è risolubile ammette una serie normale:

$$\{e\} = \mathrm{N}_0 \trianglelefteq \mathrm{N}_1 \trianglelefteq \ldots \trianglelefteq \mathrm{N}_{r-1} \trianglelefteq \mathrm{N}_r = \mathrm{G}$$

i cui fattori sono abeliani. Adesso per il secondo teorema di isomorfismo ∀ i=0,...,r-1
$N_i \cap \mathrm{H} \trianglelefteq N_{i+1} \cap \mathrm{H}$ (abbiamo usato G=N_{i+1}, N=N_i e T=$N_{i+1} \cap$ H) quindi abbiamo la serie normale per H:

$$\{e\} = N_0 \cap \mathrm{H} \trianglelefteq \mathrm{N}_1 \cap \mathrm{H} \trianglelefteq \ldots \trianglelefteq \mathrm{N}_{r-1} \cap \mathrm{H} \trianglelefteq \mathrm{N}_r \cap \mathrm{H} = \mathrm{H}$$

con fattori (∀ i=0,...,r-1):

$$\frac{N_{i+1} \cap H}{N_i \cap H} \simeq \frac{N_i(N_{i+1} \cap H)}{N_i} \leq \frac{N_{i+1}}{N_i}$$

e quindi abeliani, segue che H è risolubile. □

Proposizione 1.2.2. *Sia G un gruppo risolubile f:G* $\longrightarrow$ *H è un omomorfismo suriettivo allora H è risolubile*

Dimostrazione. Poiché G è risolubile esiste una serie abeliana:

$$\{e\} = \mathrm{N}_0 \trianglelefteq \mathrm{N}_1 \trianglelefteq \ldots \trianglelefteq \mathrm{N}_{r-1} \trianglelefteq \mathrm{N}_r = \mathrm{G}$$

Ora poiché $N_i \trianglelefteq N_{i+1}$ ∀ i=0,...,r-1 si ha immediatamente che ∀ i=0,...,r-1
f(N_i) $\trianglelefteq$ f(N_{i+1}). Abbiamo quindi la serie normale per H:

$$\{e\} = \mathrm{f(N_0)} \trianglelefteq \mathrm{f(N_1)} \trianglelefteq \ldots \trianglelefteq \mathrm{f(N_{r-1})} \trianglelefteq \mathrm{f(N_r)} = \mathrm{f(G)}{=}\mathrm{H}$$

Proviamo che i fattori di questa serie sono abeliani.$\forall$ i=0,...,r-1 è definito l'omomorfismo suriettivo:

$$\phi_i\colon\ N_{i+1} \longrightarrow \frac{f(N_{i+1})}{f(N_i}$$

$$\mathrm{n} \longmapsto \mathrm{f(n)}f(N_{i+1})$$

con N_i contenuto in Ker(ϕ_i). Segue per il primo teorema di isomorfismo che ϕ_i induce un omomorfismo suriettivo:

$$\psi_i\colon\ \frac{N_{i+1}}{N_i} \longrightarrow \frac{f(N_{i+1})}{f(N_i}$$

e quindi $\dfrac{f(N_{i+1})}{f(N_i}$ è quoziente di un gruppo abeliano e quindi è abeliano. □

da cui discende immediatamente:

Corollario 1.2.1. *Sia G un gruppo risolubile ed N $\trianglelefteq$ G. Allora G/N è risolubile.*

Dimostrazione. E' una conseguenza immediata della proposizione anteriore in quanto la proiezione sul quoziente è un omomorfismo suriettivo. □

Prima di andare avanti ricordiamo il terzo teorema di isomorfismo:

Teorema 1.2.2. *Sia G un gruppo e H,K sottogruppi normali di G con K $\leq$ H. Allora:*

$$\frac{G/K}{H/K} \simeq \frac{G}{H}$$

Proposizione 1.2.3. *Sia G un gruppo e H $\triangleleft$ G. Se H e $\dfrac{G}{H}$ sono risolubili allora G è risolubile.*

Dimostrazione. Siccome il quoziente $\dfrac{G}{H}$ è risolubile esiste una serie abeliana:

$$\{e\} = \mathrm{Q_0} \trianglelefteq \mathrm{Q_1} \trianglelefteq \ldots \trianglelefteq \mathrm{Q_{r-1}} \trianglelefteq \mathrm{Q_r} = \frac{G}{H}$$

Ora $\forall$ i=0,...,r-1 $Q_i = \dfrac{N_i}{H}$ dove $N_i \triangleleft N_{i+1}$ e per il terzo teorema di isomorfismo:

$$\frac{N_{i+1}}{N_i} \simeq \frac{Q_{i+1}}{Q_i}.$$

tuttavia anche H è risolubile quindi ammette una serie abeliana:

$$\{e\} = \mathrm{H_0} \trianglelefteq \mathrm{H_1} \trianglelefteq \ldots \trianglelefteq \mathrm{H_{s-1}} \trianglelefteq \mathrm{H_s} = \mathrm{H}$$

segue che la serie:

$$\{e\} = \mathrm{H_0} \trianglelefteq \mathrm{H_1} \trianglelefteq \ldots \trianglelefteq \mathrm{H_{s-1}} \trianglelefteq \mathrm{H_s} = \mathrm{H} \trianglelefteq \mathrm{N_1} \trianglelefteq \ldots \trianglelefteq \mathrm{N_{r-1}} \trianglelefteq \mathrm{N_r} = \mathrm{G}$$

è una serie abeliana per G. □

Proposizione 1.2.4. *Sia G un gruppo e H,K ◁ G. Allora:*

1. *G/H,G/K risolubili ⟶ G/H ∩ K è risolubile.*
2. *H,K risolubili ⟶ HK risolubile.*

Dimostrazione. 1. Definiamo l'applicazione:

$$f: G \longrightarrow G/H \times G/K$$

$$g \longmapsto (gH,gK)$$

f è un omomorfismo il cui nucleo è banalmente H ∩ K da cui G/H ∩ K è un sottogruppo di G/H × G/K che è risolubile e quindi si ha la tesi.

2. Segue dal fatto che HK/H e H sono risolubili.

□

1.3 Alcuni esempi di gruppi risolubili

Esempio 1.3.1. *Sia p un primo ed n un naturale positivo. Allora se G è un gruppo di ordine p^n è risolubile. Per vedere questo fatto ragioniamo per induzione su n. Se n=1 $G \simeq \mathbf{Z}_p$ che è risolubile essendo abeliano. Supposto vero per ogni k<n proviamo che G è risolubile.In effetti Z(G) è un sottogruppo normale di G risolubile il cui quoziente $\frac{G}{Z(G)}$ ha ordine p^k con k<n (poichè i p-gruppi hanno centro non banale [2]) segue, per la proposizione anteriore, che G è risolubile.*

Esempio 1.3.2. *Se H,K sono gruppi risolubili allora G= H × K è risolubile poichè H è normale in G e $\frac{G}{H} \simeq K$ è risolubile. Similmente il prodotto semidiretto di due gruppi risolubili è risolubile.*

Esempio 1.3.3. *Proviamo che $\mathbf{S}_3$ e $\mathbf{S}_4$ sono risolubili mentre per n>4 $\mathbf{S}_n$ non è risolubile. Questo ultimo fatto unito al teorema di risolubilità di Galois e al fatto che esistono polinomi il cui gruppo di Galois è $\mathbf{S}_n$ mostra che non esiste una formula risolutiva per le equazioni algebriche di grado > 4.*

1. *$\mathbf{S}_3$ è risolubile poichè <(123)> è normale in $\mathbf{S}_3$ ed è risolubile poichè abeliano (è isomorfo a $\mathbf{Z}_3$)inoltre il quoziente $\frac{S_3}{<(123)>}$ è risolubile poichè isomorfo a $\mathbf{Z}_2$.*
2. *$\mathbf{S}_4$ è risolubile poichè il suo sottogruppo di Klein $\mathbf{V}$ è risolubile (ha ordine 4) e il quoziente $\frac{\mathbf{S}_4}{V}$ ha ordine 6 e quindi è risolubile.*
3. *∀ n>4 $\mathbf{S}_n$ non è risolubile perchè se lo fosse lo sarebbe $\mathbf{A}_n$ ma questo è semplice e non abeliano. Una dimostrazione alternativa che non usa la semplicità di $\mathbf{A}_n$ per n>4 è la seguente (per una dimostrazione della semplicità di $\mathbf{A}_n$ potete consultare [2]): Consideriamo un generico sottogruppo normale di S_n per n>4 e sia A l'insieme dei tre-cicli di $\mathbf{S}_n$. Se proviamo che $A \subseteq N \longrightarrow A \subseteq N^{(1)}$ abbiamo chiaramente*

concluso (poiché implicherebbe che $\forall\ m \in \mathbf{N}\ A \subseteq N^{(m)}$*).Prendiamo quindi un treciclo* (abc) *e proviamo che* $(abc) \in N^{(1)}$*. Siano* $x,y \in \{1,...,n\}$ *con* $x \neq y$ *e x,y diversi da a,b e c. Un conto immediato mostra che* $[(abx),(acy)]=(abc)$ *e quindi* $(abc) \in N^{(1)}$*.*

Esempio 1.3.4. *Siano p e q primi. Proviamo che ogni gruppo di ordine* p^2q *è risolubile.Chiaramente possiamo assumere che p sia diverso da q poichè in tal caso G è un p-gruppo che è risolubile per quanto già visto. Distinguiamo quindi due casi:* $q < p$ *e* $q > p$*. Se* $q < p$ *allora consideriamo P un p-sylow di G cioè* $P \leq G$ *con* $|P| = p^2$*. Adesso dico che P è normale in G cioè il numero dei p-sylow è 1. Infatti per il secondo teorema di Sylow abbiamo che |Sylp(G)| divide q. Quindi se |Sylp(G)| ≠ 1 allora |Sylp(G)|=q poichè q è primo. Tuttavia per il terzo teorema di Sylow |Sylp(G)|=1+pk con k naturale positivo. Quindi abbiamo che* $q = 1+pk > pk \geq p > q$ *che è assurdo. Segue che P è normale in G. Adesso P è risolubile in quanto abeliano e il quoziente G/P è risolubile sempre poichè abeliano. Dunque G è risolubile. Supponiamo ora che* $q > p$*. Sia Q un q-sylow di G. Se proviamo che Q è normale con un ragionamento simile al primo caso troviamo che G è risolubile. Se Q non è normale in G allora |Sylq(G)| vale p o* p^2*. Tuttavia non può valere p poichè altrimenti esisterebbe un naturale positivo k tale che 1+qk=p da cui l'assurdo p > p. Quindi esiste un naturale positivo k tale che |Sylq(G)|=1+qk=*p^2 *da cui q divide p+1 e cioè q=p+1. Segue che p=2 e q=3 ma allora |G|=12 e per il teorema di classificazione dei gruppi di ordine 12 G è risolubile (per vedere la classificazione dei grupi di ordine 12 rimando a [3]).*

Nota 1.3.1. *Nel capitolo 3 vedremo che l'esempio anteriore risulta immediato con la conoscenza del secondo teorema di Hall.*

1.4 Caratterizzazione dei gruppi risolubili finiti e teorema di Jordan-Holder

Quando G è finito abbiamo la seguente caratterizzazione che risulta cruciale nella dimostrazione del teorema di risolubilità di Galois:

Proposizione 1.4.1. *Sia G un gruppo finito : |G|>1. Allora sono equivalenti:*

1. *G è risolubile*

2. *G ammette una serie normale con fattori di ordine primo.*

Dimostrazione. Il fatto che se G ammette una serie abeliana con fattori di ordine primo implica banalmente che G sia risolubile (poichè i fattori sarebbero gruppi ciclici quindi abeliani). Viceversa se G è risolubile ammette una serie abeliana:

$$\{e\} = \mathrm{N}_0 \trianglelefteq \mathrm{N}_1 \trianglelefteq \ldots \trianglelefteq \mathrm{N}_{r-1} \trianglelefteq \mathrm{N}_r = \mathrm{G}$$

Adesso poichè G è finito e i fattori sono abeliani per ogni i=0,...,r-1 esiste una catena di sottogruppi:

$$\mathrm{N}_i = H_0 \trianglelefteq \mathrm{H}_1 \trianglelefteq \ldots \trianglelefteq \mathrm{H}_{s-1} \trianglelefteq \mathrm{H}_s = N_{i+1}$$

tale che i fattori $\frac{H_{i+1}}{H_i}$ sono semplici e abeliani e quindi ciclici di ordine primo. Segue che possiamo costruire una serie abeliana per G i cui fattori hanno ordine primo.

□

Nota 1.4.1. *(Il teorema di Jordan Holder) Approfittiamo di questo teorema per esibire un altro modo per stabilire se un gruppo finito è risolubile. Sia quindi G un gruppo finito. Viene detta serie di composizione per G una serie normale i cui fattori sono gruppi semplici. Ad esempio:*

$$\{e\} \triangleleft \{(12)(34)\} \triangleleft \mathbf{V} \triangleleft \mathbf{A}_4 \triangleleft \mathbf{S}_4$$

è una serie di composizione per $\mathbf{S}_4$*. Oppure:*

$$\{e\} \triangleleft <r^2> \triangleleft <r> \triangleleft \mathbf{D}_4$$

è una serie di composizione per $\mathbf{D}_4$*. Il teorema di Jordan Holder afferma che ogni gruppo finito G ammette una serie di composizione e che se:*

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{r-1} \trianglelefteq N_r = G$$

$$\{e\} = K_0 \trianglelefteq K_1 \trianglelefteq \ldots \trianglelefteq K_{s-1} \trianglelefteq K_s = G$$

sono serie di composizione per G allora r=s ed esiste $\sigma \in \mathbf{S}_r$ *tale che* $K_i/K_{i-1} \simeq N_{\sigma(i)}/N_{\sigma(i)-1}$ $\forall$ *i=1,...,r.La dimostrazione di questo teorema sebbene non sia particolarmente difficile esula dall'obbiettivo di queste note.Tuttavia ci dà un ulteriore modo di stabilire se un gruppo finito è risolubile. Infatti da questo teorema discende che se un gruppo finito G ammette una serie di composizione con un fattore non ciclico allora non è risolubile.Come esempio di questo corollario c'è il fatto che per n>4* $\mathbf{S}_n$ *non è risolubile. Infatti la serie:*

$$\{e\} \triangleleft \mathbf{A}_n \triangleleft \mathbf{S}_n$$

è di composizione (qua stiamo usando il fatto che $\mathbf{A}_n$ *è semplice per n>4) ma* $\mathbf{A}_n$ *non è ciclico. Si può anche dimostrare il fatto che* $\mathbf{Z}$ *è un dominio a fattorizzazione unica usando il teorema di Jordan Holder e che la buona riuscita dell'extension problem (cioè dati due gruppi H e K trovare tutti i gruppi G tali che esista una sequenza esatta* $1 \longrightarrow H \longrightarrow G \longrightarrow K \longrightarrow 1$*) con il teorema di Jordan Holder permetterebbe di ricostruire tutti i gruppi finiti. Per maggiori informazioni sul teorema di Jordan Holder e le serie normali potete consultare [3] o anche il link* `https://kconrad.math.uconn.edu/blurbs/grouptheory/subgpseries1.pdf`

1.5 Esercizi

1. Provare che esistono gruppi non isomorfi con serie di composizione con fattori isomorfi.
2. Provare che ogmi gruppo abeliano semplice è finito.
3. Provare che un gruppo abeliano ammette una serie di composizione se e solo se è finito.
4. Esibire un gruppo infinito che ammette una serie di composizione.
5. Provare che se un gruppo risolubile ha una serie di composizione allora è finito.
6. Un gruppo G è detto super-risolubile se esiste una serie di sottogruppi

$$\{e\} = H_0 \leq H_1 \leq \ldots \leq H_{r-1} \leq H_r = \mathrm{G}$$

tale che per ogni i=0,...,r $H_i \trianglelefteq$ G e i fattori sono ciclici.Provare che S_4 non è super-risolubile.

7. (Tosto) Provare che se un gruppo finito G è tale che ogni suo sylow è ciclico allora G è risolubile
8. Siano p,q primi con p $<$ q e sia G un gruppo di ordine pq^n.Provare che G è risolubile. Come vedremo la condizione che p $<$ q è comunque superflua (l'ho messa solo per semplificare l'esercizio)
9. Sia $\mathbf{K}$ un campo. Definiamo il gruppo affine su $\mathbf{K}$ come:

$$\mathrm{Aff}(\mathbf{K}) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a, b \in \mathbf{K}, a \neq 0 \right\}$$

con l'operazione di prodotto matriciale usuale. Provare che Aff($\mathbf{K}$) è un gruppo risolubile.

10. Provare che un gruppo di ordine 769 è risolubile.
11. Provare che per n$>$2 $\mathbf{A}_n$ non è risolubile.
12. Sia $\mathbf{K}$ un campo ed Heis($\mathbf{K}$) il gruppo di Heisemberg. Provare che Heis($\mathbf{K}$) è risolubile.
13. Provare che il gruppo dei quaternioni generalizzato $\mathbf{Q}_{2^n}$ con n$>$2 è risolubile.
14. Provare che $\mathbf{GL_2(F_4)}$ non è risolubile.

Capitolo 2

Sottogruppi caratteristici e il problema di Burnside

2.1 Sottogruppi caratteristici e normali minimali

La seguente sezione ci serve per dimostrare alcuni risultati preliminari che permetteranno di dimostrare in maniera più elegante i teoremi di Hall.In particolare data la seguente:

Definizione 2.1.1. *Sia G un gruppo. $H \leq G$ è detto un sottogruppo normale minimale per G se :*

1. $H \neq \{e\}$
2. $H \trianglelefteq G$
3. *Non esiste* $K \trianglelefteq G$ *con* $\{e\} < K < H$.

vogliamo provare che se G è un gruppo finito e risolubile allora i sottogruppi normali minimali sono elementarmente abeliani (cioè p-gruppi abeliani in cui ogni elemento ha ordine p). Per arrivare a ciò ci serve partire con la nozione di sottogruppo caratteristico:

Definizione 2.1.2. *Sia G un gruppo e* $H \leq G$. *H è detto caratteristico in G (e scriviamo H char G) se* $\forall\ \phi \in Aut(G)$ *si ha che* $\phi(H)=H$.

Esempio 2.1.1. *Consideriamo il gruppo* $\mathbf{Z}_{10}$. *Proviamo che il sottogruppo* $<[2]_{10}>$ *è caratteristico in* $\mathbf{Z}_{10}$. *Sia* $\phi \in Aut(\mathbf{Z}_{10})$ *proviamo che* $\phi(<[2]_{10}>) = <[2]_{10}>$. *Poichè* ϕ *è un omomorfismo abbiamo* $\phi(<[2]_{10}>) = <\phi([2]_{10})>$. *Adesso la cardinalità di* $<\phi([2]_{10})>$ *è l'ordine di* $\phi([2]_{10})$ *in* $\mathbf{Z}_{10}$. *Siccome* ϕ *è un isomorfismo l'ordine di* $\phi([2]_{10})$ *in* $\mathbf{Z}_{10}$ *coincide con l'ordine di* $[2]_{10}$ *in* $\mathbf{Z}_{10}$ *cioè 5. Segue , essendo* $\mathbf{Z}_{10}$ *ciclico, che* $\phi(<[2]_{10}>) = <[2]_{10}>$.

vediamo alcune proprietà che risultano spesso utili:

Proposizione 2.1.1. *Sia G un gruppo. Allora valgono le seguenti:*

1. *Se* $\forall\ \phi \in Aut(G)$ *si ha che* $\phi(H) \leq H$ *allora H char G.*
2. *Se H char G allora* $H \trianglelefteq G$.
3. *Se H char K e K char G allora H char G.*

4. *Se H char K e K $\trianglelefteq$ G allora H $\trianglelefteq$ G*

5. *Z(G) char G*

Dimostrazione. 1. Sia $\phi \in$ Aut(G). Allora ϕ(H)$\leq$H e ϕ^{-1}(H)$\leq$H. Segue che H=$\phi(\phi^{-1}(H)) \leq \phi(H)$.

2. Sia g $\in$ H e h $\in$ H. Proviamo che gh$g^{-1} \in$ H. Di fatto se ϕ_g: G $\longrightarrow$ G , a $\longmapsto$ gag^{-1} allora $\phi_g \in$ Aut(G) e quindi ϕ_g(H)=H da cui la tesi.

3. Sia $\phi \in$ Aut(G). Allora $\phi|_K \in$ Aut(K) e quindi ϕ(H)=$\phi|_K$(H)=H.

4. sia h $\in$ H e g $\in$ G. Sia ϕ_g: G $\longrightarrow$ G , a $\longmapsto$ gag^{-1} allora essendo K $\trianglelefteq$ G si ha che $\phi_g|_K \in$ Aut(K) quindi gh$g^{-1} = \phi_g$(h)=$\phi_g|_K$(h) $\in \phi_g|_K$(H) $\leq$ H.

5. Sia $\phi \in$ Aut(G) e g $\in$ Z(G). Proviamo che ϕ(g) $\in$ Z(G). Se h $\in$ G abbiamo che ϕ(g)h=$\phi(g\phi^{-1}(h))=\phi(\phi^{-1}(h)g)$ = hϕ(g).

□

Come visto nella seguente proposizione se un sottogruppo è caratteristico allora è normale. In generale non vale però il viceversa come ci mostra il seguente:

Esempio 2.1.2. *Consideriamo il gruppo* $\mathbf{Z}_2 \times \mathbf{Z}_2 =$ *< (1,0),(0,1)> e il sottogruppo H generato da (1,0). Se ϕ è l'automorfismo che scambia (1,0) con (0,1) chiaramente H non è mandato in se stesso bensì nel sottogruppo generato da (0,1).*

Il secondo ingrediente è la nozione di risolubilità in termine di sottogruppo di commutatori.

Definizione 2.1.3. *Sia G un gruppo.Si pone:*

1. $G^{(0)} = G$

2. $G^{(1)} = < \{[g,h] : g,h \in G\} >$ *(detto sottogruppo dei commutatori di G)*

3. $\forall\ k \in \mathbf{N}\ G^{(k+1)} = (G^{(k)})^{(1)}$

Sono spesso utili le seguenti:

Proposizione 2.1.2. *Sia G un gruppo. Allora valgono le seguenti:*

1. $G^{(1)}$ *char G*

2. $G/G^{(1)}$ *è abeliano*

3. *Se N $\trianglelefteq$ G e G/N è abeliano allora* $G^{(1)} \trianglelefteq N$.

Dimostrazione. 1. Siano g,h $\in$ G. Allora $\forall\ \phi \in$ Aut(G) si ha che ϕ([g,h])=[ϕ(g),ϕ(h)] $\in G^{(1)}$.

2. Siano g,h $\in$ G. Allora g$G^{(1)}$h$G^{(1)}g^{-1}G^{(1)}h^{-1}G^{(1)}$ = [g,h]$G^{(1)}$=$G^{(1)}$ e quindi la tesi.

3. Siano g,h $\in$ G proviamo che [g,h] $\in$ N. Di fatto [g,h]N=N quindi la tesi.

□

Giusto per completezza enunciamo un famoso teorema dovuto a Shur (che comunque non sarà utile ai nostri scopi) la cui dimostrazione non è per nulla immediata:

Teorema 2.1.1. *Sia G un gruppo : [G : Z(G)] è finito. Allora $G^{(1)}$ è finito.*

Dimostrazione. Guardare in [3] □

Siamo ora pronti per la seguente proposizione che ci permetterà di caratterizzare i sottogruppi normali minimali dei gruppi risolubili finiti.

Proposizione 2.1.3. *Sia G un gruppo. Allora G è risolubile se e solo se esiste $n \in \mathbf{N}$: $G^{(n)} = \{e\}$.*

Dimostrazione. Se G è risolubile allora esiste una serie abeliana:

$$\{e\} = \mathrm{N}_0 \trianglelefteq \mathrm{N}_1 \trianglelefteq \ldots \trianglelefteq \mathrm{N}_{r-1} \trianglelefteq \mathrm{N}_r = \mathrm{G}$$

Adesso $\mathrm{N}_{r-1} \trianglelefteq \mathrm{G}$ e $\mathrm{G}/\ \mathrm{N}_{r-1}$ è abeliano quindi $G^{(1)} \trianglelefteq \mathrm{N}_{r-1}$. Similmente $\mathrm{N}_{r-2} \trianglelefteq \mathrm{N}_{r-1}$ e $\mathrm{N}_{r-1}/\mathrm{N}_{r-2}$ è abeliano quindi $G^{(2)} \leq N_{r-1}^{(1)} \leq \mathrm{N}_{r-2}$. Iterando il ragionamento troviamo che $G^{(r)} = \{e\}$. Viceversa se esiste $\mathrm{n} \in \mathbf{N}$: $G^{(n)} = \{e\}$ allora la serie normale:

$$\{e\} = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \ldots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = \mathrm{G}$$

è abeliana e quindi G è risolubile.

□

Siamo pronti per il seguente:

Teorema 2.1.2. *Sia G un gruppo risolubile e finito e H un sottogruppo normale minimale. Allora H è elementarmente abeliano.*

Dimostrazione. Iniziamo a vedere che H è abeliano. Siccome $H^{(1)}$ char H e H è normale in G si ha che $H^{(1)}$ è normale in G. Siccome H è il sottogruppo normale minimale ed è risolubile per la proposizione anteriore l'unica possibilità è che $H^{(1)} = \{e\}$ e quindi H è abeliano.Sia ora p un primo che divide l'ordine di H e sia P un p-sylow di H. Siccome H è abeliano per il secondo teorema di Sylow P è caratteristico in H quindi P=H segue che H è un p gruppo. Inoltre $\{x \in H : x^p = 1\}$ char H quindi H=$\{x \in H : x^p = 1\}$ e cioè ogni elemento di H ha ordine p da cui la tesi. □

Conseguenza immediata del seguente teorema è il:
Corollario

Corollario 2.1.1. *Sia G un gruppo risolubile e finito e H il sottogruppo normale minimale. Allora:*

$$H \simeq \mathbf{Z}_p \times \ldots \times \mathbf{Z}_p$$

per qualche primo p.

Dimostrazione. Poichè H è il sottogruppo normale minimale H è elementarmente abeliano. Quindi esiste un primo p tale che H è un p-gruppo abeliano in cui ogni elemento di H diverso dall'elemento neutro ha ordine p. Allora per il teorema di classificazione dei gruppi abeliani finiti l'unica possibilità è che $\mathrm{H} \simeq \mathbf{Z}_p \times \ldots \times \mathbf{Z}_p$ e quindi la tesi. □

2.2 Il problema di Burnside

Un buon momento per fare una piccola digressione potrebbe essere questo. Partiamo con la seguente definizione:

Definizione 2.2.1. *Un gruppo G è detto di torsione se ogni suo elemento ha ordine finito.*

Chiaramente ogni gruppo finito è di torsione. Il viceversa però non è vero cioè esistono gruppi di torsione che sono infiniti. Uno tra questi è il gruppo di Prüfer
$\mathbf{Z}(\mathbf{p}^{\infty}) := < x_1, x_2, ... | x_1^p = 1, x_2^p = x1, ... >$ con p primo.Tuttavia quest'ultimo gruppo non è finitamente generato.Per questo motivo Burnside propose alla comunità matematica il seguente problema: se tutti gli elementi di un gruppo finitamente generato hanno ordine finito, allora il gruppo è un gruppo finito? In generale la risposta è negativa, cioè esistono gruppi finitamente generati, di torsione che però sono infiniti (Teorema di Golod-Šafarevič). Se chiediamo però che il gruppo G soddisfi qualche proprietà in più allora la risposta è affermativa. Vediamo che la proprietà di essere risolubile e una di quelle.

Lemma 1. *Sia G un gruppo abeliano,finitamente generato e di torsione. Allora G è finito.*

Dimostrazione. Siccome G è finitamente generato esiste un sottoinsieme S = $\{s_1, ..., s_n\}$ di G tale che G = < S >. Inoltre siccome G è di torsione esiste un naturale k tale che per ogni i=1,...,n si ha che s_i^k=1. Allora siccome ogni elemento di G ha la forma $s_1^{k_1}...s_n^{k_n}$ con $0 \leq k_i \leq$ k si ha |G| $\leq$ o(s_1) ... o(s_n) (dove o(x) indica l'ordine di un elemento x). □

Il secondo ingrediente per mostrare che se G è risolubile allora la domanda posta da Burnside è affermativa è il seguente lemma:

Lemma 2. *Sia G un gruppo finitamente generato e H $\leq$ G : [G:H] è finito. Allora H è finitamente generato.*

Dimostrazione. Supponiamo che G=< $g_1, ..., g_m$ >. Senza perdere generalità possiamo assumere che l'inverso di ogni generatore sia un generatore. Siano ora Ht_1,...,Ht_m i laterali di H tali che G = $Ht_1 \cup ... Ht_m$, t_1=1 e $\forall$ i $\neq$ j $Ht_i \cap Ht_j = \emptyset$. Adesso per ogni i,j esiste h(i,j) $\in$ H : $t_i h_j$=$h(i,j)t_{k(i,j)}$ per qualche k(i,j). Non è difficile a questo punto vedere che H è generato dagli elementi h(i,j). □

Teorema 2.2.1. *Sia G un gruppo risolubile,finitamente generato e di torsione. Allora G è finito.*

Dimostrazione. Siccome G è risolubile esiste un naturale n tale che $G^{(n)}$ =$\{e\}$. Facciamo dunque induzione su n. Se n=1 allora G è abeliano quindi dal lemma G è finito. Supponiamo quindi vero per n-1. Il gruppo quoziente G/ $G^{(1)}$ è abeliano, finitamente generato e di torsione quindi è finito. Quindi per il lemma anteriore $G^{(1)}$ è finitamente generato. Ma allora $G^{(1)}$ è risolubile,finitamente generato e di torsione con $(G^{(1)})^{(n-1)} = \{e\}$ quindi per ipotesi induttiva è finito. Ma allora G/ $G^{(1)}$ è finito con $G^{(1)}$ finito segue che G è finito. □

2.3 Esercizi

1. Sia G un gruppo e H $\trianglelefteq$ G : ([G:H] : |H|)=1. Provare che H char G.
2. Sia G un gruppo e H $\leq$ G. Diciamo che H è completamente invariante se per ogni f $\in$ Hom(G,G) si ha f(H) $\leq$ H. Provare che $G^{(1)}$ è completamente invariante.
3. Provare che Z(G) potrebbe non essere completamente invariante.
4. Consideriamo **Z** con l'operazione binaria $\cdot$(m,n)=m+n se m è pari e $\cdot$(m,n)=m-n se m è dispari. Provare che (**Z**, $\cdot$) è un gruppo ed è risolubile.
5. Sia G un gruppo. Viene detto esponente di G il più piccolo naturale positivo n tale che $\forall$ g $\in$ G g^n=e.Provare che un gruppo finitamente generato con esponente 2 è finito (si può mostrare che il gruppo è finito anche se l'esponenente è 3 o 4).

Capitolo 3

I teoremi di Hall

3.1 Il primo teorema di Hall

Sia G un gruppo finito e scriviamo |G|=ab dove (a,b)=1. Come sappiamo dai teoremi di Sylow se a=p^m con p primo allora G ammette un sottogruppo di ordine a e tutti tali sottogruppi sono coniugati. Ma se facciamo la richiesta che a abbia più di un divisore primo non è detto che G ammette tale sottogruppo.Per esibire un esempio esplicito partiamo dimostrando il seguente lemma che generalizza il teorema di rappresentazione di Cayley:

Lemma 3. *Sia G un gruppo e $H \leq G$: [G:H]=n. Allora esiste ϕ: $G \longrightarrow \mathbf{S}_n$ omomorfismo tale che Ker$\phi \leq H$.*

Dimostrazione. Sia X = $\{gX : g \in G\}$. Definiamo l'applicazione:

$$\phi : \mathrm{G} \longrightarrow \mathbf{S}_X \simeq \mathbf{S}_n$$

$$\mathrm{a} \longmapsto \phi_a$$

dove per ogni a ∈ G ϕ_a(gX)=agX. Vediamo che ϕ è ben definita cioè che per ogni a ∈ G ϕ_a è una funzione bigettiva. Se gH=g'H allora agH=agg^{-1}g'H=ag'H quindi ϕ_a è ben definita. Inoltre ϕ_a è iniettiva poiche se agH=ag'H allora gH=g'H. Il fatto che poi ϕ è un omomorfismo è immediato. Vediamo invece che il nucleo è contenuto in H. se a è un elemento del nucleo di ϕ allora agH=gH per ogni g in G quindi aH=H da cui a ∈ H. □

Corollario 3.1.1. *Sia G un gruppo semplice e H<G ; [G:H]=n. Allora G si immerge in* $\mathbf{S}_n$

Dimostrazione. Per il lemma anteriore esiste ϕ: G $\longrightarrow \mathbf{S}_n$ omomorfismo tale che Ker$\phi \leq$ H $<$ G. Poiché G è semplice e ker$\phi \triangleleft$ G l'unica possibilità è che Kerϕ sia banale e cioè ϕ è iniettiva. □

Siamo allora pronti per esibire il controesempio esplicito alla domanda che ci eravamo posti.

Esempio 3.1.1. *Consideriamo il gruppo semplice* $\mathbf{A}_5$*. Abbiamo che* $|\mathbf{A}_5| = 4 \cdot 15$*. Proviamo che non esiste un sottogruppo di* $\mathbf{A}_5$ *di ordine 15. Di fatto se esiste un tale sottogruppo per il corollario anteriore* $\mathbf{A}_5$ *si immergerebbe in* $\mathbf{S}_4$ *ma questo è assurdo poiché 60 non divide 24.*

La cosa che manca è la risolubilità del gruppo di partenza come vedremo nella dimostrazione del primo teorema di Hall. Prima di vedere la dimostrazione del teorema partiamo con un lemma preliminare.Per farlo ricordiamo che dato un gruppo G e H $\leq$ G è detto normalizzante di H in G il più grande sottogruppo di G in cui H è normale ed è denotato con $N_G(H)$. Non è difficile vedere (farlo come esercizio) che g $\in N_G(H) \iff$ gHg^{-1}=H.Siamo allora pronti per il seguente:

Lemma 4. *(L'argomento di Frattini) Sia G un gruppo finito e K $\trianglelefteq$ G. Sia P un p-sylow di K. Allora G=K$N_G(P)$.*

Dimostrazione. Sia g $\in$ G. Allora gP$g^{-1} \leq$ gKg^{-1} = K. Segue che gPg^{-1} è un p-sylow di K e quindi per il secondo teorema di Sylow esiste k $\in$ K tale che gPg^{-1}=kPk^{-1} da cui P=g^{-1}kP$(g^{-1}k)^{-1}$ e quindi g^{-1}k $\in N_G(P)$ segue che g $\in$ K$N_G(P)$.

□

Siamo dunque pronti per il seguente:

Teorema 3.1.1. *(P.Hall 1928) Sia G un gruppo finito risolubile con |G|=ab con (a,b)=1. Allora esiste H $\leq$ G : |H|=a. Inoltre se K $\leq$ G : |K|=a esiste g $\in$ G : K=gHg^{-1}.*

Dimostrazione. Dimostriamo il teorema per induzione su n=|G|. Se n=1 il teorema è ovvio. Supponiamo quindi vero per ogni k $<$ n e dimostriamolo per n. Se b=1 il teorema è ovvio quindi possiamo assumere che b$>$1.

- Iniziamo supponendo che esista H $\triangleleft$ G non banale : $|H| = a'b'$ con a'|a e b'|b con $b'<$b.

  1. ESISTENZA
     Abbiamo che $|G/H| = (a/a')(b/b') <$ ab quindi per ipotesi induttiva esiste A $\leq$ G : A/H $\leq$ G/H e $|A/H| = a/a'$.Allora $|A| = ab' <$ ab ma A è risolubile quindi esiste $A' \leq$ A $\leq$ G : $|A'|$=a (e questo prova l'esistenza).
  2. CONIUGAZIONE
     Proviamo ora che se N,K sono sottogruppi di G di ordine a allora sono coniugati.Come prima cosa osserviamo che |NH|=|KH|=ab'.Infatti abbiamo che essendo H $\triangleleft$ G allora NH $\leq$ G quindi |NH|=cd con c|a e d|b.Tuttavia N $\leq$ NH quindi a | cd ma (a,d)=1 quindi a | c cioè a=c. Similmente H $\leq$ NH quindi $a'b'$ | cd quindi b' | d. Ma cd | $aa'b'$ quindi d | b' cioè d=b'. Segue che |NH|=|KH|=ab'. Proviamo adesso che NH/H e KH/H sono coniugati in G/H. Di fatto NH/H e KH/H sono sottogruppi di G/H di ordine a/a' e quindi per ipotesi induttiva sono coniugati in G/H. Cioè esiste g $\in$ G : (gG)(NH/H)(g^{-1}G)=KH/H da cui N e K sono coniugati in G.

Dunque abbiamo provato il teorema nel caso in cui esista H $\triangleleft$ G non banale : |H|=$a'b'$ con a'|a e b'|b con $b'<$b. Dunque possiamo assumere d'ora in avanti che $\forall$ N $\triangleleft$ G si abbia b | |N|. Ma allora detto H il sottogruppo normale minimale sappiamo che H è un p-gruppo abeliano tale che ogni elemento ha ordine p segue che b=p^m e quindi siamo nel seguente caso:

- |G|=ap^m con (a,p)=1 e H è l'unico p-sylow di G ed è abeliano e normale minimale.

1. ESISTENZA
   Adesso essendo G risolubile si ha che G/H è risolubile di ordine a. Sia K/H il sottogruppo normale minimale di G/H. Allora |K/H|=q^n con q primo diverso da p. Allora |K|=$q^n p^m$. Sia Q un q-sylow di K (esiste per il primo teorema di Sylow) allora K=HQ. Definiamo ora N*=$N_G(Q)$. Proviamo che |N*|=a.Poiché K $\trianglelefteq$ G e Q è un q-sylow di K per l'argomento di Frattini si ha che G=KN*.Definiamo ora N=N* $\cap$ K = $N_K(Q)$. Mostreremo che |N*|=a|H $\cap$ N| e poi che H $\cap$ N è banale.Per il secondo teorema di isomorfismo abbiamo che:

   $$G/K \simeq KN^*/K \simeq N^*/N^* \cap K = N^*/N$$

   da cui, tenendo anche conto che K=HN (poiché K=HQ e Q $\leq$ N $\leq$ K) abbiamo:

   $$|N^*|=|G/K||N|=(|G|/|K|)\ |N| = (|G||N|\ )/\ (|HN|) = a\ |H \cap N|$$

   Proviamo adesso che H $\cap$ N è banale.Mostreremo prima che H $\cap$ N $\leq$ Z(K) e poi che Z(K) è banale.Sia x $\in$ H $\cap$ N e k $\in$ K=HQ. Allora k=hs con h $\in$ H e s $\in$ Q.Proviamo che xk=kx. Sarà sufficiente vedere che xs$x^{-1}s^{-1}$=e ovvero che xs$x^{-1}s^{-1}$ $\in$ H $\cap$ Q.Effettivamente poiché x $\in$ N allora Q=xQx^{-1} quindi xsx^{-1} $\in$ Q da cui xs$x^{-1}s^{-1}$ $\in$ Q. Inoltre H $\trianglelefteq$ G quindi s$x^{-1}s^{-1}$ $\in$ H da cui xs$x^{-1}s^{-1}$ $\in$ H. Proviamo adesso che Z(K) è banale.Supponiamo che Z(K) sia non banale. Allora essendo Z(K) $\trianglelefteq$ G (poiché Z(K) char K e K è normale in G) si deve avere che H $\leq$ Z(K).Ma K=HQ quindi Q char K (stiamo usando il secondo teorema di Sylow) e quindi Q $\trianglelefteq$ G segue che H $\leq$ Q che è assurdo.
2. CONIUGAZIONE
   Infine sia A $\leq$ G : |A|=a. Proviamo che A e N* sono coniugati.Iniziamo a vedere che A $\cap$ K e Q sono coniugati.Basterà provare che |A $\cap$ K|=q^n. Abbiamo che:

   $$a \mid |AK| \text{ e } p^m q^n \mid |AK| \rightarrow |AK|=ab=|G| \rightarrow AK=G$$

   da cui:

   $$G/K = AK/K \simeq A/A \cap K \rightarrow |A \cap K| = q^n$$

   Segue che N* e $N_G(A \cap K)$ sono coniugati (scrivere i dettagli per esercizio). Tuttavia $|N_G(A \cap K)|$=|N*|=a e A $\cap$ K $\trianglelefteq$ A quindi per le proprietà del normalizzante A $\leq$ $N_G(A \cap K)$ da cui A=$N_G(A \cap K)$.

□

3.2 Il secondo teorema di Hall

Sia G un gruppo finito e p un primo che divide l'ordine di G. Allora sarà |G|=ap^m con (a,p)=1. Un sottogruppo di G di ordine a è detto p-complemento di G.Il primo teorema di Hall ci dice che se G è risolubile per ogni primo p che divide l'ordine di G si ha che G ammette un complemento. Ebbene il secondo teorema di Hall ci dice che vale anche il viceversa. Prima di vedere la dimostrazione del teorema vediamo alcuni lemmi preliminari:

Lemma 5. *Sia G un gruppo finito e H,K ≤ G. Allora [G:H ∩ K]=[G:H][H:H ∩ K]*

Dimostrazione. Per il teorema di Lagrange abbiamo che:

$$[G:H \cap K] = |G| \,/\, |H \cap K| = (|G||H|)/(|H||H \cap K) = [G:H][H:H \cap K]$$

□

da cui immediatamente la seguente:

Lemma 6. *Sia G un gruppo finito e H,K ≤ G : ([G:H],[G:K])=1. Allora G=HK.*

Dimostrazione. Poiché [G:H] e [G:K] sono coprimi e dividono [G:H ∩ K] si deve avere che [G:H][G:K] ≤ [G: H ∩ K] quindi |G| ≤ |HK| e quindi la tesi. □

Un altro importante risultato prima di vedere il secondo teorema di Hall è il seguente;

Lemma 7. *Sia G un gruppo finito e H,K,L ≤ G risolubili : [G:H],[G:K],[G:L] sono coprimi due a due. Allora G è risolubile.*

Dimostrazione. Se G è banale è ovvio, quindi procediamo per induzione su |G|.Osserviamo che se H è banale allora G=K per il lemma anteriore e quindi G è risolubile.Possiamo assumere quindi che H non sia banale.Sia quindi N un sottogruppo normale minimale di H. N è un p-gruppo e siccome [G:K] e [G:L] sono coprimi possiamo assumere che p non divida [G:K] quindi K contiene un p-sylow di G e siccome N è un p gruppo $N \leq K^g$ per qualche g ∈ G.Adesso per il lemma anteriore $G=HK^g$. Quindi se x ∈ G allora $N^x \leq K^g$. Segue che il sottogruppo R di G generato da $\cup \{N^g : g \in G\}$ è risolubile. Ma adesso R è normale in G ed è non banale perché contiene N. Inoltre HR/R,KR/R,LR/R sono sottogruppi di G/R risolubili quindi per ipotesi induttiva G/R è risolubile ma quindi G è risolubile. □

Nella dimostrazione del secondo teorema di Hall useremo anche il teorema di Burnside la cui dimostrazione usa tecniche di teoria delle rappresentazioni:

Teorema 3.2.1. *(Burnside) Sia G un gruppo : $|G|=p^m q^n$ con p,q primi. Allora G è risolubile.*

Dimostrazione. La dimostrazione passa per argomenti di teoria dei caratteri reperibile al link: `https://math.uchicago.edu/~may/REU2015/REUPapers/Zimmerman.pdf` □

Teorema 3.2.2. *(Hall, 1937) Sia G un gruppo finito : G ammette un p-complemento per ogni primo p : p | |G|. Allora G è risolubile.*

Dimostrazione. Facciamo induzione sul numero n di divisori primi di G. Se n=1 o n=2 è vero perché se n=1 G è un p-gruppo quindi risolubile come visto nel capitolo 1 mentre se n=2 G è risolubile per il teorema di Burnside. Assumiamo quindi n>2 e supponiamo vero per ogni k<n.Siano p,q ed r primi che dividono l'ordine di G e siano H un p-complemento di G, K un q-complemento di G ed L un r-complemento di G. Se proviamo che H,K ed L sono risolubili per la proposizione anteriore abbiamo finito. Mostriamo che ad esempio H è risolubile.Il numero di divisori di |H| è n-1 quindi se mostriamo che H ammette ad esempio un q-complemento abbiamo finito. Di fatto H ∩ K è un q-complemento di H in quanto G=HK.Segue la tesi. □

3.3 Esercizi

1. Sia G un gruppo semplice infinito.Provare che G non ha sottogruppi di indice finito.
2. Provare che $\mathbf{A}_6$ non ha sottogruppi di indice primo.
3. Sia G un gruppo finito e p il più piccolo primo che divide l'ordine di G. Provare che se H $\leq$ G : [G:H]=p allora H $\triangleleft$ G.
4. Sia G un gruppo abeliano finito. Provare che G è prodotto di p-gruppi.
5. Siano p,q primi con p<q e G un gruppo di ordine pq^2. Provare che G $\simeq \mathbf{Z}_p \rtimes_\phi$ A dove A è un gruppo di ordine q^2 e ϕ : A $\longrightarrow$ Aut($\mathbf{Z}_p$) è un omomorfismo.
6. Provare che un gruppo finito per cui si può invertire il teorema di Lagrange è risolubile.
7. Provare che se p,q,r sono primi allora un gruppo di ordine pqr è risolubile. Classificare quindi tali gruppi a meno di isomorfismo.

Conclusioni

Giusto per completezza mettiamo in luce la potenza del primo teorema di Hall unito al teorema di Shur-Zassenhaus. Consideriamo un gruppo G tale che |G|=$p_1 \dots p_m$ con $p_1, \dots, p_m$ primi dispari e $p_1 < \dots < p_m$.G è un gruppo risolubile per il teorema di Feith-Thompson. Quindi per il primo teorema di Hall esiste un sottogruppo H di G di ordine $p_2 \dots p_m$. Tuttavia, essendo [G:H]=p_1 con p_1 il più piccolo primo che divide l'ordine di G, si ha che H è normale in G. Segue, per il teorema di Shur-Zassenhaus, che
G $\simeq$ H $\rtimes_{\phi_1}$ $\mathbf{Z}_{p_1}$ con H gruppo risolubile di ordine $p_2 \dots p_m$. Adesso, riapplicando il ragionameneto ad H, otteniamo che sarà, G $\simeq$ (K $\rtimes_{\phi_2}$ $\mathbf{Z}_{p_2}$) $\rtimes_{\phi_1}$ $\mathbf{Z}_{p_1}$ con K risolubile di ordine $p_3 \dots p_m$. Iterando il ragionameneto vediamo che alla fine G sarà un semidiretto tra $\mathbf{Z}_{p_1}$,$\mathbf{Z}_{p_2}$, $\dots$ $\mathbf{Z}_{p_m}$. Quindi, in sostanza, il primo teorema di Hall ci permette di classificare tutti i gruppi di ordine $p_1 \dots p_m$ con $p_1, \dots, p_m$ primi dispari e $p_1 < \dots < p_m$ grazie al fatto che ad ogni passo il sottogruppo di Hall che troviamo è normale (qui con sottogruppo di Hall di un gruppo G intendiamo un sottogruppo H di G tale che (|H|,|G/H|)=1) . Ma allora ci poniamo la seguente domanda: Sia G un gruppo finito e scriviamo |G|=ab con (a,b)=1. Sotto quali condizioni esiste in G un sottogruppo normale di ordine a ? Una risposta a questa domanda è stata fornita da Michio SUZUKI e il lettore interessato può trovarla in [4].

Appendice

I teoremi di Sylow

I teoremi di Sylow sono uno degli strumenti più potenti per capire la struttura di un gruppo finito G. Giusto per capire la loro potenza proviamo che ogni gruppo di ordine 15 è isomorfo a $\mathbf{Z}_{15}$. Sia quindi G un gruppo tale che |G|=15=3 · 5. Per il primo teorema di Sylow esiste H ≤ G : |H|=5. Tale sottogruppo è normale per il terzo teorema di Sylow (scrivere i dettagli per esercizio).Inoltre esiste per il primo teorema di Sylow K ≤ G : |K|=3.Tale K è normale in G per il terzo teorema di Sylow (anche qua scrivere i dettagli per esercizio). Segue che G ≃ H × K ≃ $\mathbf{Z}_5 \times \mathbf{Z}_3 \simeq \mathbf{Z}_{15}$. Oltre questo piccola applicazione si possono dimostrare tantissime altre cose. Ad esempio con i teoremi di Sylow si riesce a far vedere che se G è un gruppo di ordine minore stretto di 60 e semplice allora è abeliano. Conseguentemente (scrivere i dettagli) ogni gruppo di ordine < di 60 è risolubile !. L'appendice che segue si limita solamente ha dimostrare tali teoremi ma uno studio accurato e approfondito (con relativi esempi ed esercizi) si può trovare in [2] e in [3]. Per dimostrare i teoremi di Sylow è indispensabile la definizione di azione di gruppo:

Definizione 3.3.1. *Sia G un gruppo e Ω un insieme non vuoto.Se esiste un omomorfismo di gruppi f : G ⟶ S_Ω diciamo che G agisce su Ω tramite f ed f è detta l'azione di G su Ω.*

Quando abbiamo un azione di gruppi possiamo definire alcuni sottoinsiemi particolari:

Definizione 3.3.2. *Sia G un gruppo e Ω un insieme non vuoto e sia f : G ⟶ S_Ω un azione di G su Ω. Allora ∀ x ∈ Ω definiamo:*

- $\Theta_x := \{f(g)(x) : g \in G\}$ *l'orbita di x*
- $G_x = \{g \in G : f(g)(x) = x\}$ *lo stabilizzatore di x*

inoltre definiamo i punti fissi di Ω come :

- $\Omega_G = \{x \in \Omega : f(g)(x) = x \forall g \in G\}$

Sia ora G un gruppo e Ω un insieme non vuoto e sia f : G ⟶ S_Ω un azione di G su Ω.Osserviamo che le orbite indotte dall'azione f possono essere viste come classi di equivalenza.Infatti definiamo su Ω la seguente relazione binaria, ponendo ∀ x,y ∈ Ω:

$$x \sim y \iff \exists\, g \in G : f(g)(x)=y$$

è immediato verificare che ∼ è una relazione di equivalenza su Ω.Inoltre, osserviamo che, fissato x ∈ Ω:

$$[x]_\sim = \{f(g)(x) : g \in G\} = \Theta_x$$

e quindi:

$$\Omega = \sqcup_{x\in\Omega}\Theta_x$$

Osserviamo inoltre che:

$$\mid \Theta_x \mid = 1 \iff \text{x} \in \Omega_G$$

infatti se $\mid \Theta_x \mid = 1$ allora $\Theta_x = \{x\}$ e quindi $\forall$ g $\in$ G : f(g)(x)=x cioe x $\in \Omega_G$, viceversa se x $\in \Omega_G$ allora $\forall$ g $\in$ G : f(g)(x)=x e quindi $\Theta_x = \{x\}$ cioè $\mid \Theta_x \mid = 1$. Mettiamo ora in relazione orbite e stabilizzatori:

Proposizione 3.3.1. *Sia G un gruppo che agisce su insieme non vuoto Ω tramite $f : G \longrightarrow S_\Omega$.Allora:*

- $G_x \leq G \; \forall \; x \in \Omega$.
- $\mid \Theta_x \mid = [G:G_x] \; \forall \; x \in \Omega$.

Dimostrazione. Dimostriamo i due punti.Sia x $\in \Omega$.

- Osserviamo che G_x è non vuoto in quanto 1 vi appartiene (poichè f(1)(x)=Id(x)=x).Siano ora a e b in G_x.Allora

  $$\text{f(ab)(x)=f(a)(f(b)(x))=f(a)(x)=x}$$

  quindi ab $\in G_x$. Inoltre essendo f(a)(x)=x si ha che x = f(a^{-1})(x) e quindi G_x è un sottogruppo di G.

- Osserviamo che [G:G_x]=$\mid \{gG_x : g \in G\} \mid$. Mostriamo quindi che $\{gG_x : g \in G\}$ è in biezione con Θ_x.Definiamo l'applicazione:

  $$\Phi : \{gG_x : g \in G\} \longrightarrow \Theta_x$$

  $$gG_x \longmapsto \text{f(g)(x)}$$

  mostriamo che Φ è bigettiva.Iniziamo a vedere che Φ è ben definita.Se a e b sono due elementi di G tali che aG_x=bG_x allora f($a^{-1}b$)(x)=x e sfruttando il fatto che f è un omomorfismo si ottiene che f(a)(x)=f(b)(x).Quindi Φ è ben definita.Ora Φ è banalmente suriettiva ed è iniettiva perchè se f(a)(x)=f(b)(x) allora f($a^{-1}b$)(x)=x e quindi $a^{-1}b \in G_x$ da cui aG_x=bG_x.Segue l'asserto.

□

Abbiamo ora tutti i prerequisiti per dimostrare il primo teorema di Sylow. Iniziamo prima con qualche nome e poi dimostriamo il teorema.

Definizione 3.3.3. *Sia G un gruppo : $\mid G \mid = p^a m$ con p un primo e (p,m)=1. $H \leq G$: $\mid H \mid = p^a$ è detto p - sottogruppo di Sylow di G (o semplicemente p-sylow di G). L'insieme dei p-sylow di G è denotato con Sylp(G)*

Finalmente possiamo dimostrare il:

Teorema 3.3.1. *(Primo teorema di Sylow) Sia G un gruppo : | G | = $p^a m$ con p un primo e (p,m)=1. Allora* $\exists$ $H \leq G$: | H | = p^a.

Dimostrazione. Consideriamo l'insieme:

$$\Omega = \{X \subseteq G :| X |= p^a\}$$

L'applicazione:

$$\mathrm{f} : \mathrm{G} \longrightarrow S_\Omega$$

$$\mathrm{X} \longmapsto \{gx : x \in X\}$$

è un azione di G su Ω. Denotiamo con $\triangle_1$,...,$\triangle_t$ le orbite indotte dall'azione, allora:

$$| \Omega | = | \triangle_1 | +...+ | \triangle_t |$$

ora siccome:

$$| \Omega | = \binom{p^a}{p^a m}$$

p non divide | Ω | e quindi esiste i $\in \{1, ..., t\}$ tale che p non divide | $\triangle_i$ | allora p^a non divide | $\triangle_i$ |. Adesso $\triangle_i$ avrà la forma:

$$\triangle_i = \Theta_X$$

per qualche X $\in \Omega$. Quindi siccome p^a divide | G | = [G:G_X]| G_X | = | Θ_X | | G_X | si ottiene che p^a divide | G_X | quindi | G_X | = p^ak per qualche naturale positivo k.Se mostriamo che k=1 abbiamo finito.Sia x $\in$ X, consideriamo G_Xx.Abbiamo che G_Xx $\subseteq$ X infatti se y $\in$ G_Xx allora y=gx con g $\in$ G_X. Ma se g $\in$ G_X si ha f(g)(X)=X e allora $\{gx : x \in X\}$ = X da cui y=gx $\in$ X.Allora:

$$| G_X | = | G_X\mathrm{x} | \leq | \mathrm{X} | = p^a$$

consegue che k = 1. □

Passiamo ora a dimostrare il secondo teorema di Sylow.Ci servono dei lemmi preliminari.

Lemma 8. *Sia G un p-gruppo finito (cioè un gruppo di ordine la potenza di un primo) che agisce su insieme finito e non vuoto* Ω *tramite f : G* $\longrightarrow$ S_Ω*.Allora:*

$$| \Omega | \equiv_p | \Omega_G |$$

Dimostrazione. Se | Ω | = | Ω_G | allora il teorema è banalmente vero. Supponiamo quindi che | Ω | > | Ω_G | e denotiamo con $\triangle_1$,...,$\triangle_t$ le orbite di ordine maggiore di 1 indotte dall'azione f, allora essendo:

$$\Omega = \Omega_G \sqcup (\triangle_1 \sqcup ... \sqcup \triangle_t)$$

si ha che:

$$| \Omega | - | \Omega_G | =| \triangle_1 | + ...+ | \triangle_t |$$

Sia ora i $\in \{1, ..., t\}$. Supponiamo che $\triangle_i = \Theta_x$ con x $\in \Omega$ allora:

$$| \triangle_i | = | \Theta_x | = [\mathrm{G}:G_x]$$

quindi | $\triangle_i$ | divide p^n per qualche naturale n $\in \mathbb{N}^+$ da cui | $\triangle_i$ | = p^{r_i} per qualche $r_i \in \mathbb{N}^+$ deduciamo che p divide | Ω | - | Ω_G | e quindi si ha la tesi. □

Ci serve un secondo lemma:

Lemma 9. *Sia G un gruppo :* $\mid G \mid = p^a m$ *con p un primo e (p,m)=1. Siano* $S \leq G :$ $\mid S \mid = p^a$ *e* $P \leq G$ *un p-sottogruppo di G (cioè P ha ordine* p^k *con k≤a). Allora* $\exists\ x \in G$ *:* $P \leq S^x$

Dimostrazione. Sia $\Omega = \{Sx : x \in G\}$. Definiamo l'applicazione:

$$\mathrm{f} : \mathrm{P} \longrightarrow S_\Omega$$

$$\mathrm{g} \longmapsto \mathrm{f(g)}$$

dove f(g)(Sx)=Sxg^{-1} $\forall$ Sx $\in \Omega$.f è un'azione di P su Ω. Osserviamo che $\mid \Omega_P \mid \neq 0$. Infatti se $\mid \Omega_P \mid = 0$ siccome P è un p-gruppo finito:

$$\mid \Omega \mid \equiv_p \mid \Omega_P \mid = 0$$

quindi p divide $\mid \Omega \mid$ = [G:S] e cioè esiste un naturale positivo k, tale che: [G:S]=pk quindi:

$$p^a \mathrm{m} = \mid \mathrm{G} \mid = \mathrm{k}p^a$$

e quindi

$$\mathrm{m} = \mathrm{pk} \text{ da cui } (\mathrm{m,p}) \neq 1.$$

assurdo. Quindi esiste Sx $\in \Omega$ tale che $\forall$ g $\in$ P Sx=Sxg^{-1}. Sia allora g $\in$ P, allora:

$$\mathrm{x}g^{-1}=\mathrm{sx},\ \mathrm{s} \in \mathrm{S}$$

da cui:

$$\mathrm{g} \in S^x$$

allora P $\leq S^x$

□

Nel seguito se G è un gruppo e H $\leq$ G e prendiamo g $\in$ G denotiamo con H^g l'insieme gHg^{-1}.Siamo quindi pronti per dimostrare il secondo teorema di Sylow:

Teorema 3.3.2. *(Secondo teorema di Sylow) Sia G un gruppo :* $\mid G \mid = p^a m$ *con p un primo e (p,m)=1. Siano S,P* $\in$ *Sylp(G). Allora* $\exists\ x \in G : P = S^x$ *. Conseguentemente* $\mid$ *Sylp(G)* $\mid = [G:N_G(S)]$ *e* $\mid$ *Sylp(G)* $\mid$ *divide m.*

Dimostrazione. Poichè P è un p-sottogruppo di G esiste x in G tale che P $\leq S^x$. Ma $\mid$ P $\mid = \mid$ S $\mid = \mid S^x \mid$ quindi P $= S^x$. Allora deduciamo che:

$$\mathrm{Sylp(G)}=\{S^x : x \in G\}$$

consegue:

$$\mid \mathrm{Sylp(G)} \mid = [\mathrm{G}:N_G(S)]$$

Inoltre applicando 3 volte il teorema di Lagrange si ha che:

$$\mid \mathrm{G} \mid = [\mathrm{G}:N_G(S)] \mid N_G(S)$$

$$\mid N_G(S) \mid = [N_G(S):\mathrm{S}] \mid \mathrm{S} \mid$$

$$\mid \mathrm{G} \mid = [\mathrm{G:S}] \mid \mathrm{S} \mid$$

da cui deduciamo che

$$[G:S]=|\ Sylp(G)\ |\ [N_G(S):S]$$

e quindi la tesi. □

Possiamo dimostrare anche il seguente:

Teorema 3.3.3. *(Terzo teorema di Sylow) Sia G un gruppo :* $|\ G\ | = p^a m$ *con p un primo e (p,m)=1. Allora:*

$$|\ Sylp(G)\ | \equiv_p 1$$

Dimostrazione. Sia S ∈ Sylp(G).Per il secondo teorema di Sylow [G:S]=| Sylp(G)| $[N_G(S):S]$. Definiamo

$$\Omega = \{xS : x \in G\}$$

allora:

$$|\ \Omega\ | = [G:S]$$

e dunque:

$$|\ \Omega\ | = |\ Sylp(G)\ |\ [N_G(S):S]$$

Definiamo l'applicazione:

$$f :\ S \longrightarrow S_\Omega$$

$$g \longmapsto f(g)$$

dove f(g)(xS)=gxS ∀ xS ∈ Ω. f è un'azione di S su Ω e si ha che $|\ \Omega_S\ | = [N_G(S):S]$. Per mostrare questo fatto, essendo :

$$[N_G(S):S] =|\ \{xS : x \in N_G(S)\}\ |$$

è sufficiente dimostrare che:

$$\Omega_S = \{xS : x \in N_G(S)\}$$

Sia xS ∈ Ω_S, mostriamo che x ∈ $N_G(S)$ e cioè che S=S^x.Poichè xS ∈ Ω_S si ha che ∀ g ∈ S xS=gxS. Sia quindi g ∈ S allora gx=xs per qualche s ∈ S da cui g ∈ $S^{x^{-1}}$ e quindi S ≤ $S^{x^{-1}}$ e quindi S = $S^{x^{-1}}$.Allora sia g ∈ S. Abbiamo g = x^{-1}(xgx^{-1})x ∈ S^x consegue che S = S^x.Viceversa consideriamo un elemento della forma xS con x ∈ $N_G(S)$ e sia g ∈ S, vogliamo mostrare che xS=gxS. Di fatto:

$$S=S^x \rightarrow xS=Sx \rightarrow gxS=gSx=Sx=xS$$

e quindi $|\ \Omega_S\ | = [N_G(S):S]$.Allora:

$$|\ \Omega\ | = |\ Sylp(G)\ |\ |\ \Omega_S\ |$$

tuttavia S è un p-gruppo e quindi:

$$|\ \Omega\ | \equiv_p |\ \Omega_S\ |$$

allora:

$$|\ Sylp(G)\ |\ |\ \Omega_S\ | \equiv_p |\ \Omega_S\ |$$

ma p non divide Ω_S (altrimenti p divide m e questo è assurdo essendo (p,m)=1).Quindi:

$$| \text{Sylp(G)} | \equiv_p 1$$

□

Nota 3.3.1. *Sia G un gruppo :* $| G | = p^a m$ *con p un primo ,* $a \in \mathbb{N}$, $m \in \mathbb{N}^+$ *, (p,m)=1. Sia* $S \in$ *Sylp(G) allora:*

$$S \triangleleft G \iff | \textit{Sylp(G)} | = 1$$

inoltre nel seguito porremo $| \textit{Sylp(G)} | = n_p(G)$ *o se non ci sarà rischio di ambiguità semplicemente* $| \textit{Sylp(G)} | = n_p$ *.*

Bibliografia

[1] Siegfried Bosch. *Galois Theory*. Springer International Publishing, Cham, 2018.

[2] D.N. Dikranjan and M.S. Lucido. *Aritmetica e algebra*. Liguori Editore, 2007.

[3] J.J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer New York, 2012.

[4] Michio Suzuki. On the existence of a hall normal subgroup. *Journal of the Mathematical Society of Japan*, 15(4):387–391, 1963.