Indice

Introduzione

Un gruppo G si dice fattorizzabile se esistono due sottogruppi non-banali A e B, tali che $G = AB := \{ab \mid a \in A, b \in B\}$.

Viene naturale domandarsi se e quando le proprietà possedute dai sottogruppi A e B passano anche al loro prodotto G. Lo studio dei gruppi fattorizzabili risulta non essere affatto banale, infatti fino agli inizi degli anni '50 i risultati riguardanti questo argomento erano pochi e per la maggior parte legati allo studio dei gruppi fattorizzabili finiti, decisamente più facili da studiare rispetto a quelli infiniti. Ma anche riguardo i gruppi finiti, erano diverse le domande che non trovavano risposta. Un esempio è un Teorema di Kegel-Wielandt, che afferma che il prodotto di due gruppi finiti nilpotenti è risolubile. Questa congettura era considerata universalmente vera agli inizi degli anni '50, ma nessuno era ancora riuscito a dimostrarla. In effetti risultava complicato anche solo dimostrare il teorema per il prodotto di due gruppi abeliani.

Nel 1955 il matematico N. Itō riesce però a dimostrare in maniera semplicissima un risultato incredibile, valido anche per gruppi infinti, ovvero che il prodotto di due gruppi abeliani è metabeliano. Il Teorema di Kegel-Wielandt risultò invece ben più complicato da dimostrare e venne risolto da O.H. Kegel e da H. Wielandt agli inizi degli anni '60.

A partire da questi teoremi negli anni si è sviluppata un grande teoria riguardante i gruppi fattorizzabili, e i teoremi di Itō e di Kegel-Wielandt sono stati ampiamente generalizzati. Non possiamo non citare il lavoro del matematico russo S.N. Chernikov, che ha fortemente contribuito a sviluppare la teoria dei gruppi fattorizzabili infiniti.

Quello che faremo in questa tesi sarà dimostrare i teoremi di Itō e di Kegel-Wielandt, e fornire una generalizzazione del Teorema di Itō. Nel primo capitolo cercheremo di raccogliere tutti i prerequisiti necessari per lo studio dei gruppi fattorizzabili. In particolare verrà enunciato e dimostrato il Teorema di Burnside, utile nella dimostrazione del Teorema di Kegel-Wielandt.

Capitolo 1

Il $p^\alpha q^\beta$-Teorema di Burnside

Uno dei maggiori successi della Teoria dei caratteri è il famoso $p^\alpha q^\beta$-Teorema di Burnside: se p e q sono numeri primi, un gruppo di ordine $p^\alpha q^\beta$ è risolubile. In questo capitolo, dopo aver dato la definizione di gruppo risolubile e nilpotente, nonchè una breve introduzione alla Teoria delle rappresentazioni dei gruppi finiti, si fornisce una dimostrazione del succitato risultato seguendo [5].

1.1 Gruppi risolubili e nilpotenti

Introduciamo il concetto di risolubilità di un gruppo partendo dalla definizione di serie subnormale

Definizione 1.1.1. Sia G un gruppo. Una catena di sottogruppi

$$G = G_0 \supset G_1 \supset ... \supset G_{n-1} \supset G_n = \{1\}$$

è detta una serie subnormale di G se G_i è normale in G_{i-1} per ogni $1 \leq i < n$. I quozienti G_{i-1}/G_i sono detti i fattori della serie. Una serie subnormale è detta di composizione se ogni fattore della serie è semplice e non-banale.

Il gruppo G si dice risolubile se ammette una serie subnormale con fattori tutti abeliani.

Posto, per ogni $a, b \in G$

$$[a, b] = a^{-1}b^{-1}ab \quad \text{e} \quad a^b = b^{-1}ab$$

il commutatore di a e b e il coniugato di a secondo b, rispettivamente, e, per ogni $X, Y \subseteq G$

$$[X, Y] := \big\langle [x, y] \mid x \in X, y \in Y \big\rangle,$$

induttivamente definiamo la serie derivata di G, ponendo

$$G^{(0)} := G \quad \text{e} \quad G^{(i+1)} := [G^{(i)}, G^{(i)}] \text{ per ogni } i \geq 0.$$

È facile osservare che un gruppo è risolubile se, e solo se, la sua serie derivata ha lunghezza finita. Nel seguito, porremo $G' = G^{(1)}$ e lo indicheremo come il sottogruppo derivato o il commutatore di G.

Definizione 1.1.2. Un gruppo G si dice metabeliano se G' è abeliano. Equivalentemente, un gruppo metabeliano è un gruppo risolubile che ammette una serie derivata di lunghezza 2.

Denotiamo con $Z(G)$ il centro di G, ovvero

$$Z(G) := \{x \mid x \in G,\ yx = xy \ \ \forall y \in G\} \trianglelefteq G,$$

ed induttivamente definiamo la seguente serie ponendo

$$Z_0(G) = \{1_G\} \quad \text{e} \quad Z_{i+1}(G) = Z(G/Z_i(G)) \text{ per ogni } i \geq 0.$$

Tale successione di sottogruppi

$$Z_0(G) \subseteq Z_1(G) \subseteq \cdots \subseteq Z_m(G) \subseteq \ldots$$

è detta la serie centrale superiore di G.

Definizione 1.1.3. Un gruppo G si dice nilpotente se la sua serie centrale superiore è finita.

Possiamo subito osservare che i fattori della serie centrale sono tutti abeliani, quindi ogni gruppo nilpotente è risolubile. Alcuni esempi banali di gruppi nilpotenti sono i gruppi abeliani e i p-gruppi finiti con p primo.

Un importante fatto sui gruppi nilpotenti che useremo in seguito è il seguente risultato di caratterizzazione:

Teorema 1.1.4. *Un gruppo finito G è nilpotente se, e solo se, è prodotto diretto dei suoi sottogruppi di Sylow.*

1.2 Teorema di Burnside

Il risultato centrale di questo capitolo fu dimostrato da Burnside nel 1904, sfruttando la teoria delle rappresentazioni dei gruppi finiti, ed è probabilmente il maggiore dei successi legati a tale teoria. Per diverso tempo si è cercata una dimostrazione che non coinvolgesse la teoria dei caratteri, ma questa fu trovata solo molto più tardi, agli inizi degli anni '70 da Goldschmidt (1970) per gruppi di ordine dispari e da Bender (1972) per gruppi di ordine pari. Essa risulta però essere parecchio complicata, per cui ci concentreremo sull'originale.

Definizione 1.2.1. Sia G un gruppo e sia V uno spazio vettoriale di dimensione finita sul campo $\mathbb{K}$. Un omomorfismo non-zero $\rho : G \to GL(V)$ si dice una rappresentazione lineare di G su $\mathbb{K}$.

Un sottospazio di V si dice G-invariante o G-stabile se $\rho(g)(W) \subset W$ per ogni $g \in G$. La rappresentazione si dice semplice o irriducibile se V non possiede sottospazi G-stabili, si dice invece completamente irriducibile se ogni sottospazio G-stabile W di V, ammette un complemento G-stabile, ovvero un sottospazio G-stabile W' tale che $V = W \oplus W'$.

Un applicazione lineare α su V si dice invece G-invariante se vale che

$$\alpha(\rho(g)(v)) = \rho(g)(\alpha(v)) \text{ per ogni } g \in G,\ \ v \in V.$$

Per semplicità, da ora in avanti scriveremo

$$\rho(g)(v) = gv.$$

Teorema 1.2.2 (Maschke)**.** *Sia $\rho : G \to GL(V)$ una rappresentazione lineare di un gruppo finito G su di uno spazio vettoriale V di dimensione finita sul campo $\mathbb{K}$. Supponiamo inoltre che la caratteristica di $\mathbb{K}$ non divida l'ordine di G. Allora la rappresentazione è completamente riducibile.*

Dimostrazione. Un endomorfismo π su un $\mathbb{K}$-spazio vettoriale V si dice una proiezione se $\pi^2 = \pi$, ovvero se π è idempotente. Chiaramente possiamo sempre scomporre $V = Ker(\pi) \oplus Im(\pi)$. È vero anche il viceversa, ovvero data una qualsiasi decomposizione di $V = U \oplus W$, possiamo trovare due applicazioni

idempotenti, ovvero le proiezioni sui sottospazi U e W.

Data ora una rappresentazione lineare di G su un $\mathbb{K}$-spazio vettoriale di dimensione finita V, e data una qualsiasi applicazione idempotente π, è chiaro che π è G-invariante se, e solo se, $Ker(\pi)$ e $Im(\pi)$ sono G-stabili.

Quindi per dimostrare il teorema è sufficente mostrare che preso un qualsiasi sottospazio G-stabile W di V, esso è l'immagine di una proiezione G-invariante.

Sia ora π un endomorfismo idempotente qualsiasi con immagine W e $\overline{\pi}$ un endomorfismo così definito:

$$\overline{\pi}(v) = \frac{1}{|G|} \sum_{g \in G} g(\pi(g^{-1}v)).$$

Per ogni $w \in W$ si ha che

$$\overline{\pi}(w) = \frac{1}{|G|} \sum_{g \in G} g(\pi(g^{-1}w)) = \frac{1}{|G|} \sum_{g \in G} g(g^{-1}w) = \frac{1}{|G|} \sum_{g \in G} w = w.$$

Quindi $W \subseteq Im(\overline{\pi})$ ma è anche ovvio che $Im(\overline{\pi}) \subseteq W$ dato che $\overline{\pi}(v)$ è combinazione lineare di elementi di w per ogni $v \in V$.

Quindi $Im(\overline{\pi}) = W$. Inoltre $\overline{\pi}(v)^2 = \overline{\pi}(v)$ dato che per come è definita è ovviamente una proiezione.

Infine per ogni $h \in G$ si ha:

$$\overline{\pi}(hv) = \frac{1}{|G|} \sum_{g \in G} g(\pi(g^{-1}(hv))) = \frac{1}{|G|} \sum_{g \in G} h((h^{-1}g)(\pi(g^{-1}(hv))))$$

$$= h\frac{1}{|G|} \sum_{g \in G} g(\pi(g^{-1}v).$$

Quindi $\overline{\pi}$ è G-invariante. □

Definizione 1.2.3. Sia G un gruppo, V un spazio vettoriale di dimensione finita sul campo $\mathbb{K}$, e $\rho : G \to GL(V)$ una rappresentazione lineare di G. Allora, fissata una base $B := \{v_1, \ldots, v_n\}$, e fissato l'omomorfismo $\rho^* : G \to GL(n, \mathbb{K})$ che associa ad ogni elemento di g la matrice associata a $\rho(g)$ attraverso la base B, chiamiamo il carattere di ρ l'applicazione $\chi_V : G \to \mathbb{K}$ che manda $g \in G$ in $T_R(\rho^*(g))$.

Innanzi tutto osserviamo che χ_V non dipende dalla base scelta, dato che la traccia di una matrice è invariante per matrici simili. Questo implica anche che χ_V è una funzione di classe, ovvero è una funzione che rimane costante sulle classi di coniugio. Diremo che un carattere χ_V è irriducibile/semplice se lo è ρ, e chiameremo il grado di un carattere il grado della sua rappresentazione associata.

Indichiamo ora con $\mathbb{K}[G]$, l'algebra gruppale di G su un campo $\mathbb{K}$, ossia l'algebra sul campo $\mathbb{K}$ generata dagli elementi di G.

Definiamo allora la rappresentazione regolare di G, come la naturale rappresentazione di G su $\mathbb{C}[G]$ visto come $\mathbb{C}[G]$-modulo. Infine il carattere regolare di un gruppo è il carattere della sua rappresentazione regolare, ed è uguale a:

$$\chi_{reg}(g) = \begin{cases} |G| & \text{se } g = 1_G \\ 0 & \text{altrtimenti} \end{cases}$$

Siamo ora pronti a dimostrare il Teorema di Burnside. Procederemo enunciando alcuni lemmi preliminari, a partire dal ben noto Lemma di Shur, che costituiranno i passi fondamentali della dimostrazione.

Lemma 1.2.4 (Shur)**.** *Sia A una $\mathbb{K}$-algebra e sia S un A-modulo semplice. Allora $End_A(S)$ è una $\mathbb{K}$-algebra di divisione.*

Dimostrazione. Sia $\alpha : S \to S$ un omomorfismo non nullo di A-moduli. Il nucleo di questo morfismo è necessariamente un A-sottomodulo di S. Dalla semplicità di S concludiamo che l'applicazione è biettiva, quindi α ha un inverso. □

Dal Lemma di Shur segue anche il seguente fatto

Corollario 1.2.5. *Ogni algebra di divisione su un campo algebricamente chiuso è isomorfa al campo stesso.*

Definizione 1.2.6. Un elemento $x \in \mathbb{C}$ si dice un intero algebrico se è soluzione di un polinomio monico a coefficenti in $\mathbb{Z}$.

Lemma 1.2.7. *Sia G un gruppo finito e sia $\mathbb{K}$ un campo algebricamente chiuso di caratteristica 0. Supponiamo che χ sia il carattere di una rappresentazione irriducibile di G di grado n su un $\mathbb{K}$-spazio vettoriale V. Se $g \in G$ ha l elementi coniugati, allora $l\chi(g)/n$ è un intero algebrico.*

Dimostrazione. Siano $K_1, ..., K_h$ le classi di coniugio di G e sia $k_i = \sum_{x \in K_i} x$. Si può osservare che i k_i formano una base del centro C di $\mathbb{K}[G]$ su $\mathbb{K}$. Dato che $k_i k_j \in C$,

$$k_i k_j = \sum_{r=1}^{h} m_{ij}^{(r)} k_r \tag{1}$$

dove $m_{ij}^{(r)}$ è il numero delle copie (x, y) tali che $x \in K_i$, $y \in K_j$ e xy è uguale ad un elemento z_r fissato in K_r. Possiamo notare che gli $m_{ij}^{(r)}$ non dipendono dalla scelta di z_r.

Sia ora $\rho : G \to GL(V)$ un rappresentazione irriducibile di grado n con carattere χ. Possiamo ovviamente estendere ρ e χ nella maniera ovvia a $\mathbb{K}[G]$. Allora $\rho(k_i) \in End_{\mathbb{K}[G]}(V)$ e quindi, dal Lemma di Shur, $\rho(k_i) = f_i(Id)$ per qualche $f_i \in \mathbb{K}$. Adesso

$$nf_i = \chi(k_i) = l_i \chi^{(i)},$$

con $l_i = |K_i|$ e $\chi^{(i)}$ il valore di χ su K_i. Quindi $f_i = l_i \chi^{(i)}/n$.

Applicando ρ alla (1) otteniamo:

$$f_i f_j = \sum_{r=1}^{h} m_{ij}^{(r)} f_r. \tag{2}$$

Fissando un i nella (2) otteniamo un sistema di h equazioni lineari nelle f_i:

$$\sum_{r=1}^{h} (f_i \delta_{jr} - m_{ij}^{(r)}) f_r = 0 \quad j \in \{1, 2, ..., h\}.$$

Gli f_i non possono essere tutti uguai a 0 dato che, se $K_1 = \{1\}$, allora $f_1 \neq 0$, quindi il sistema lineare ha una soluzione non-banale. Il determinante della matrice $h \times h$ con entrata (j, r) uguale a $f_i \delta_{jr} - m_{ij}^{(r)}$ deve essere uguale a 0, perciò gli f_i sono radici di un polinomio monico in $\mathbb{Z}[t]$, ovvero sono interi algebrici. □

Lemma 1.2.8. *Sia ρ una rappresentazione irriducibile di grado n di un gruppo finito G su un $\mathbb{C}$-spazio vettoriale V, e sia χ il carattere di ρ. Supponiamo inoltre che $g \in G$ sia un elemento con esattamente l coniugati, con $MCD(l,n) = 1$. Allora $\chi(g) = 0$ oppure $\rho(g)$ è scalare.*

Dimostrazione. Dal Lemma 1.2.7, $\chi(g)l/n$ è necessariamente un intero algebrico. Dato che $(l,n) = 1$ allora esistono interi r e s tali che $1 = rl + sn$. Quindi

$$t = \frac{\chi(g)}{n} = \frac{\chi(g)rl}{n} + \chi(g)s$$

è un intero algebrico.

Siano ora $f_1, ..., f_n$ autovalori di $\rho(g)$, in modo tale che $\chi(g) = \sum_{i=1}^{n} f_i$. Dato che l'ordine di g è finito, anche l'ordine di $\rho(g)$ è finito. Ogni f_i è necessariamente una radice dell'unità, quindi $|f_i| = 1$ e $|t| \leq 1$. Supponiamo che gli f_i non siano tutti uguali, in modo tale che $|t| < 1$, e sia α un automorfismo del campo $\mathbb{Q}(f_1, ..., f_n)$. Ovviamente gli $\alpha(f_i)$ non sono tutti uguali, e quindi analogamente $|\alpha(t)| < 1$. Sia u il prodotto degli f_i. Anche $|u| < 1$, ma $\alpha(u) = u$ per ogni automorfismo α. Per cui, dal teorema fondamentale della teoria di Galois, $u \in \mathbb{Q}$. Sappiamo che u è un intero algebrico dato che t lo è, ma è noto che l'insieme degli interi algebrici di $\mathbb{Q}$ è $\mathbb{Z}$. Quindi $u = 0$, $t = 0$, e $\chi(g) = 0$.

Se invece gli f_i sono tutti uguali, allora $\rho(g)$ è scalare. □

Lemma 1.2.9 (Burnside)**.** *Sia G un gruppo finito con una classe di coniugio con esattamente $q^m > 1$ elementi con q primo. Allora G non è semplice.*

Dimostrazione. Sia G un gruppo semplice, $g \in G$ un elemento con esattamente q^m coniugati, ρ una rappresentazione non-banale irriducibile di G sul $\mathbb{C}$-spazio vettoriale di dimensione finita V, e sia χ il carattere di ρ. Supponiamo ora che $\chi(g) \neq 0$ e che q non divida il grado di χ. Allora segue dal Lemma 1.2.8, che $\rho(g)$ è scalare, e quindi centrale in $\rho(G)$. Ma G è semplice e ρ è non-banale, perciò $Ker(\rho) = \{1\}$ e G è isomorfo a $\rho(G)$. Conseguentemente $g = 1$, ma questo va in contraddizione con l'ipotesi per cui $q^m > 1$. Quindi $\chi(g) = 0$ per ogni carattere irriducibile non-banale χ con grado coprimo con q.

Sia ora ψ il carattere della rappresentazione regolare sinistra σ. Si può dimostrare che è possibile scrivere $\psi = \sum_i l_i \chi_i$ con $\chi_1, ..., \chi_n$ $\mathbb{C}$-caratteri irriducibili di G e con l_i grado di χ_i per ogni i. Senza perdità di generalità consideriamo χ_1 il carattere della rappresentazione banale, e quindi consideriamo $l_1 = 1$. Da quanto visto fino ad ora, segue che $\psi(g) \equiv 1 \bmod q$. Ma $\sigma(g)$ non ha punti fissi, il che implica che $\psi(g) = 0$. Questo è chiaramente assurdo, quindi G non è semplice. □

Teorema 1.2.10 (Burnside)**.** *Sia G un gruppo di ordine $p^\alpha q^\beta$ con $p, q \in \mathbb{P}$ e $\alpha, \beta \in \mathbb{N}$. Allora G è risolubile.*

Dimostrazione. Supponiamo che il teorema sia falso e sia G il controesempio di ordine minimo. Se esistesse N sottogruppo normale non-banale di G, allora sia N che G/N sarebbero risolubili, e di conseguenza anche G lo sarebbe. Per cui G è semplice. Sia ora Q un q-sottogruppo di Sylow di G non-banale e $g \in Z(Q)$ non-banale. Allora $[G : C_G(g)]$ è necessariamente uguale ad una potenza di p maggiore di 1, dato che $Q \leq C_G(g) \neq G$. Ma questo è impossibile dal Lemma 1.2.9. □

Capitolo 2

Gruppi fattorizzabili: un Teorema di Kegel-Wielandt

Un gruppo G si dice fattorizzato da due sottogruppi A e B se $G = AB$. Uno dei primi risultati su tali gruppi è un classico Teorema di Itō : se $G = AB$ è il prodotto di due sottogruppi abeliani, allora G è metabeliano. In questo capitolo se ne fornisce la (sorprendentemente facile) dimostrazione insieme a quella (ben più complessa) di un Teorema di Kegel-Wielandt: se $G = AB$ è il prodotto di due sottogruppi nilpotenti finiti, allora G è risolubile. Per la trattazione si fa principalmente riferimento a [1].

2.1 Sottogruppi fattorizzabili e proprietà di gruppi fattorizzabili

Per ogni A, B sottoinsiemi di un gruppo G, definiamo

$$AB := \{ab \mid a \in A, b \in B\}.$$

Definizione 2.1.1. Un gruppo G si dice prodotto dei suoi sottogruppi A e B se $G = AB$. In tal caso, diciamo anche che G è fattorizzato da A e da B. Un gruppo per cui esistono due sottogruppi propri di cui ne è il prodotto si dice fattorizzabile.

Ovviamente non tutti i gruppi sono fattorizzabili, si consideri, per esempio, C_4, il gruppo ciclico di 4 elementi. Però possiamo osservare che se $G = AB$ è un gruppo fattorizzato da A e B e $N \trianglelefteq G$, allora G/N è fattorizzabile. Infatti

$$G/N = (AN/N)(BN/N).$$

Considerazioni diverse riguardano i sottogruppi di un gruppo fattorizzabile. Infatti, se $G = AB$, non è di solito vero che un sottogruppo di G sia il prodotto di un sottogruppo di A ed uno di B.

A tal fine premettiamo la seguente

Proposizione 2.1.2. *Sia $G = AB$ il prodotto di due sottogruppi A e B. Per un sottogruppo S di G, le seguenti condizioni sono equivalenti:*
i) $S = (A \cap S)(B \cap S)$ e $A \cap B \leq S$;
ii) se $ab \in S$, con $a \in A$ e $b \in B$, allora $a \in S$.

Dimostrazione.
(ii)⇒(i): Sia $x = ab$ un elemento di S, con $a \in A$ e $b \in B$. Per ipotesi, $a \in A \cap S$ e $b \in B \cap S$, quindi $S = (A \cap S)(B \cap S)$. Inoltre, se $x \in A \cap B$, allora $xx^{-1} = 1 \in S$, e quindi $x \in S$.
(i)⇒(ii): Sia $x = ab \in S$ con $a \in A$ e $b \in B$. Per ipotesi, esistono $a_1 \in A \cap S$ e $b_1 \in B \cap S$ tali che $x = a_1 b_1$. Ma allora, $a_1^{-1} a = b_1 b^{-1} \in A \cap B \leq S$, quindi $a \in S$. □

Ha senso allora dare la seguente

Definizione 2.1.3. Un sottogruppo di un gruppo fattorizzabile $G = AB$ che soddisfa una delle condizioni della proposizione 2.1.2, è detto un sottogruppo fattorizzabile.

Ovviamente un sottogruppo di $G = AB$ che contiene uno dei fattori A o B è fattorizzabile.

Proposizione 2.1.4. *Sia $G = AB$ il prodotto di due sottogruppi A e B. Allora valgono le seguenti proprietà:*
i) l'intersezione di sottogruppi fattorizzabiliè fattorizzabile;

ii) il sottogruppo generato da dei sottogruppi normali fattorizzabili è fattorizzabile;
iii) se $N \trianglelefteq G$, il sottogruppo S/N del gruppo $G/N = (AN/N)(BN/N)$ è fattorizzabile se, e solo se, S lo è.

Dimostrazione. i) Questo è ovvio dalla definizione di sottogruppo fattorizzabile.

ii) Sia $(S_i)_{i\in I}$ una famiglia di sottogruppi normali fattorizzabili di G e sia $S := \langle S_i \mid i \in I \rangle$. Se x appartiene a S vuol dire che esiste un numero finito di indici $i_1, ..., i_l$ tali che x appartiene a

$$\begin{aligned} &S_{i_1}...S_{i_l} = (A \cap S_{i_1})(B \cap S_{i_1})S_{i_2}...S_{i_l} = (A \cap S_{i_1})S_{i_2}(B \cap S_{i_1})...S_{i_l} \\ &= (A \cap S_{i_1})(A \cap S_{i_2})(B \cap S_{i_2})(B \cap S_{i_1})S_{i_3}...S_{i_l} \\ &= (A \cap S_{i_1})...(A \cap S_{i_l})(B \cap S_{i_1})...(B \cap S_{i_l}) \leq (A \cap S)(B \cap S). \end{aligned}$$

Quindi $S = (A \cap S)(B \cap S)$, ed ovviamente $A \cap B \leq S$.

iii) Sia $S \leq G$ sottogruppo fattorizzabile di G contenente N. Sia ora $xN = abN$ elemento di S/N con $x \in S, a \in A, b \in B$. Allora $x = aby$ con $y \in N \leq S$. Quindi $ab = xy^{-1} \in S$ e quindi $a \in S$. Per cui S/N è un sottogruppo fattorizzabile di G/N.

Viceversa, sia $S/N \leq G/N$ un sottogruppo fattorizzabile e sia $x = ab$ un elemento di S con $a \in A$ e $b \in B$. Dato che $xN = abN$, sappiamo che $aN \in S/N$, e quindi $a \in S$ ed S è fattorizzabile. □

I sottogruppi fattorizzabili godono quindi di eccellenti proprietà. Il problema è che la gran parte dei sottogruppi di un gruppo fattorizzabile, non è a sua volta fattorizzabile. Il prossimo lemma mostra sotto quali ipotesi i normalizzanti di alcuni sottogruppi sono fattorizzabili. Ricordiamo che un gruppo G si dice periodico se per ogni $g \in G$ esiste $n \in \mathbb{N}$ per cui $g^n = e$. Inoltre ricordiamo che se $H \leq G$, il normalizzante di H in G è il sottogruppo $N_G(H) := \{g \mid g \in G, N^g \subset N\}$.

Lemma 2.1.5. *Sia $G = AB$ il prodotto di due sottogruppi A e B e siano A_0, B_0 sottogruppi normali di A e di B rispettivamente, allora, per i normalizzanti dei*

sottogruppi $H := \langle A_0, B_0 \rangle$ *e* $L := A_0 \cap B_0$, *valgono le seguenti proprietà:*

(i) se uno fra A/A_0 *e* B/B_0 *è periodico, allora*

$$N_G(H) = N_A(H)N_B(H).$$

(ii) se un fra A *e* B *è periodico, allora*

$$N_G(L) = N_A(L)N_B(L).$$

Dimostrazione. (i) Sia $g = ab^{-1}$ un elemento di $N_G(H)$, con $a \in A$ e $b \in B$. $H^a = H^{gb} = H^b$, quindi A_0 e B_0 sono entrambi contenuti in $H^a = H^b$. Quindi, per ogni $h \in H$, esiste $\overline{h} \in H$ tale che $a^{-1}ha = b^{-1}\overline{h}b$, ossia, $h = ab^{-1}\overline{h}ba^{-1}$. Ma $b^{-1}\overline{h}b \in H^b = H^a$. Per cui $ab^{-1}\overline{h}ba^{-1} = h \in H^a$, ovvero $H \leq H^a$. Supponiamo ora, senza perdità di generalità, che A/A_0 sia periodico, e quindi che esista $n \in \mathbb{N}$ tale che $a^n \in A_0$. Allora

$$H \leq H^a \leq H^{a^2} \leq ... \leq H^{a^n} = H.$$

Questo vuol dire necessariamente che $a \in N_A(H)$ e $b \in N_B(H)$.

(ii) Sia $g = ab^{-1}$ un elemento di $N_G(L)$, con $a \in A$ e $b \in B$. Allora, $L^a = L^{gb} = L^b$, quindi A_0 e B_0 contengono entrambi $L^a = L^b \leq L$. Supponiamo ora, senza perdità di generalità, che A sia periodico. Allora esiste $n \in \mathbb{N}$ tale che

$$L \geq L^a \geq L^{a^2} \geq ... \geq L^{a^n} = L.$$

Perciò $a \in N_A(L)$ e $b \in N_B(L)$ □

2.2 Un Teorema di Itō e un Teorema di Kegel-Wielandt

Se $G = AB$ è un gruppo fattorizzato, ovviamente la sua struttura è determinata dalle proprietà di A e B. Nel 1955 N. Itō dette una dimostrazione sorprendente (e incredibilmente semplice) di un risultato riguardante la risolubilità di gruppi fattorizzati non necessariamente finiti.

Teorema 2.2.1 (Itō, 1955)**.** *Sia $G = AB$ un gruppo fattorizzabile prodotto di due sottugruppi abeliani A e B. Allora G è metabeliano.*

Dimostrazione. Siano $a, a_1 \in A$ e $b, b_1 \in B$. Siano inoltre $b^{a_1} := a_2 b_2$ e $a^{b_1} := a_3 b_3$. Allora

$$[a,b]^{a_1 b_1} = [a, b^{a_1}]^{b_1} = [a, b_2]^{b_1} = [a^{b_1}, b_2] = [a_3, b_2],$$

e

$$[a,b]^{b_1 a_1} = [a^{b_1}, b]^{a_1} = [a_3, b]^{a_1} = [a_3, b^{a_1}] = [a_3, b_2].$$

Questo prova che $[a,b]^{[a_1,b_1]} = [a,b]$ e quindi che $[a,b]$ e $[a_1,b_1]$ commutano. Pertanto $G/[A,B]$ è abeliano e quindi $G' \leq [A,B]$. Perciò $G' = [A,B]$ è abeliano e G è metabeliano. □

Torniamo ora al teorema di Burnside. Sia G un gruppo di ordine $p^\alpha q^\beta$ e siano P e Q un p-Sylow e un q-Sylow rispettivamente. Allora $G = PQ$ (essendo P e Q permutabili) e G è risolubile. Wielandt nel 1958 e Kegel nel 1961 provarono un risultato sui gruppi fattorizzabili che generalizza il Teorema di Burnside e, in un certo senso, il Teorema di Itō.

Teorema 2.2.2 (Kegel 1961, Wielandt 1958)**.** *Sia $G = AB$ un gruppo finito prodotto di due sottogruppi nilpotenti A e B. Allora G è risolubile.*

La dimostrazione del Teorema 2.2.2, che costituisce probabilmente il più famoso risultato sui gruppi fattorizzabili, è tutt'altro che banale e richiede una serie di risultati preliminari. A tal fine, iniziamo fornendo la definizione di sottogruppo di Hall e una serie di lemmi correlati.

Definizione 2.2.3. Sia G un gruppo finito, $H \leq G$, e π un insieme non-vuoto di numeri primi.

Il sottogruppo H si dice un π-sottogruppo di G se il suo ordine è prodotto di primi contenuti in π, mentre si dice invece un π-sottogruppo di Hall di G se, oltre ad essere un π-sottogruppo, il suo indice e il suo ordine sono coprimi.

Infine G è detto un D_π-gruppo, se ogni suo π-sottogruppo è contenuto in un π-sottogruppo di Hall e se tutti i π-sottogruppi di Hall sono coniugati.

Possiamo notare che la nozione di π-sottogruppo di Hall, generalizza la nozione di sottogruppo di Sylow.

Lemma 2.2.4. *Sia $G = AB$ il prodotto di due sottogruppi A e B, e siano x e y elementi di G. Allora $G = A^x B^y$ ed esiste $z \in G$ tale che $A^x = A^z$ e $B^y = B^z$.*

Dimostrazione. Sia $xy^{-1} = ab$ con $a \in A$ e $b \in B$. Scegliamo $z := a^{-1}x$. Allora $x = az$ e $y = b^{-1}z$ e quindi $A^x = A^z$ e $B^y = B^z$ da cui segue la tesi. □

Lemma 2.2.5. *Sia $G = AB$ un gruppo prodotto dei sottogruppi A e B e π un insieme non-vuoto di primi. Se A,B e G sono D_π-gruppi, allora esistono A_0 e B_0 π-sottogruppi di Hall di A e di B rispettivamente, tali che A_0B_0 è un π-sottogruppo di Hall di G.*

Dimostrazione. Siano A_1,B_1 e G_1 π-sottogruppi di Hall di A,B e G rispetivamente. Per le ipotesi su G, esistono due elementi x e y tali che A_1^x e B_1^y sono entrambi conenuti in G_1. Segue dal Lemma 2.2.4 che $A^x = A^z$ e $B^y = B^z$ per qualche $z \in G$. Siano ora $A_0 := A_1^{xz^{-1}}$ e $B_0 := B_1^{yz^{-1}}$ due sottogruppi di Hall di A e B rispettivamente, entrambi contenuti in $G_0 := G_1^{z^{-1}}$ e n il più grande divisore di $|A \cap B|$ in π. Chiaramente $|A_0 \cap B_0| \leq n$. Dato che

$$|G| = \frac{|A|\,|B|}{|A \cap B|},$$

allora

$$|G_0| = \frac{|A_0|\,|B_0|}{n} \leq \frac{|A_0|\,|B_0|}{|A_0 \cap B_0|} = |A_0B_0|\,.$$

Perciò $A_0B_0 = G_0$ è un π-sottogruppo di Hall di G. □

Lemma 2.2.6. *Sia G un gruppo finito e A e B sottogruppi di G tali che $AB^g = B^gA$ per ogni $g \in G$. Se $G = A^GB = AB^G$ allora $G = AB$.*

Dimostrazione. Possiamo ovviamente suppore che A non sia normale in G, altrimenti la tesi è ovvia. Quindi esiste $b \in B$ e $g \in G$ tali che $A^{b^g} \neq A$.

Procediamo ora per induzione su $[G : A]$. Se $[G : A] = 1$, allora $G = A$ e la tesi è banale.

Supponiamo quindi che $[G : A] > 1$. Ovviamente A è strettamente contenuto in $A_1 := \langle A, A^{b^g} \rangle$. Pertanto $[G : A_1] < [G : A]$. Per l'ipotesi induttiva si ha

$$G = A_1 B^g = \langle A, A^{b^g}, B^g \rangle = AB^g.$$

Dal Lemma 2.2.4, segue la tesi. □

Lemma 2.2.7. *Sia $G = AB$ un gruppo finito e risolubile, prodotto di due sottogruppi A e B, e siano A_0 e B_0 sottogruppi normali di A e di B rispettivamente. Se A_0 e B_0 sono sottogruppi di Hall di G, allora $A_0^x B_0^y = B_0^y A_0^x$ per ogni $x, y \in G$.*

Dimostrazione. Dalla risolubilità di G, esistono $h, k \in G$ tali che A_0^h e B_0^k commutano. Per il Lemma 2.2.4 si ha che $G = A^h B^k$. Quindi possiamo assumere che $A_0 B_0 = B_0 A_0$. Siano ora $x, y \in G$ e sia $xy^{-1} = ab$ con $a \in A$ e $b \in B$. Allora

$$A_0^{xy^{-1}} B_0 = A_0^{b^{-1}} B_0 = (A_0 B_0)^{b^{-1}} = (B_0 A_0)^{b^{-1}} = B_0 A_0^{b^{-1}} = B_0 A_0^{xy^{-1}},$$

da cui segue che $A_0^x B_0^y = B_0^y A_0^x$. □

Lemma 2.2.8 (Wielandt)**.** *Sia G un gruppo, π un insieme non-vuoto di primi, e $H \leq G$ un π-sottogruppo di Hall di G nilpotente. Allora esiste un sottogruppo $N \trianglelefteq G$ tale che $G = NH$ e $N \cap H = \{1\}$.*

Dimostrazione. Per la dimostrazione di questo fatto, rimandiamo a [2]. □

Ora possiamo finalmente dimostrare il Teorema di Kegel-Wielandt:

Dimostrazione. Assumiamo che il teorema sia falso, e sia $G = AB$ un controesempio di ordine minimo.

CASO 1: A e B hanno ordine coprimo.

La prima cosa che osserviamo è che G è semplice. Infatti, sia $N \trianglelefteq G$ con $N \neq \{1\}$. Dalla minimalità di G si ha che G/N è risolubile. Allora N non è risolubile, altrimenti lo sarebbe anche G, e pertanto $AN = A(AN \cap B)$ non è

risolubile. Allora, dalla minimalità di G, si ottiene che $G = AN$ e, analogamente, che $G = BN$. Quindi $|G/N|$ deve necessariamente dividere $|A|$ e $|B|$, e dunque $N = G$, che è quanto che volevamo provare.

Sia ora $1 \neq b \in Z(B)$. Ovviamente $B \subseteq C_G(b)$, quindi $[G : C_G(b)]$ divide $|A|$. Dal Lemma 1.2.9 sappiamo che un gruppo semplice non può avere una classe di coniugio con cardinalità una potenza di un primo. Quindi la cardinalità di A non può essere una potenza di un primo. Analogo risultato vale per B. Siano allora $P_1, ..., P_s, Q_1, ..., Q_t$ i sottogruppi di Sylow di A e di B rispettivamente. Allora $s, t \geq 2$. Per semplicità divideremo la dimostrazione ora in una serie passaggi.

(i) *Siano A_0, B_0 sottogruppi normali di P_i e di Q_j rispettivamente, tali che $H := \langle A_0, B_0 \rangle$ sia un sottogruppo proprio non-banale di G. Allora, esiste $N \trianglelefteq H$ tale che $N \subset P_i$ o $N \subset Q_j$.*

Dato che A_0 e B_0 sono entrambi sottogruppi normali, dal Lemma 2.1.5. si ha che $N_G(H)$ è un sottogruppo fattorizzabile. Dato che P_i è un p_i-sottogruppo di Sylow di G, allora $\widetilde{P_i} := P_i \cap N_G(H)$ è un p_i-sottogruppo di Sylow di $N_G(H)$. Similmente $\widetilde{Q_j} := Q_j \cap N_G(H)$ è un q_j-sottogruppo di Sylow di $N_G(H)$. Notiamo anche che essendo $N_G(H)$ un sottogruppo proprio di G, esso è risolubile. Dal lemma 2.2.7 segue che i sottogruppi $\widetilde{P_i}$ e $\widetilde{Q_j}$ commutano e $\widetilde{P_i}\widetilde{Q}_J \supset H$. In particolare, l'ordine di un sottogruppo normale minimale N di H deve necessariamente essere o una potenza di p_i o una potenza di q_j. Quindi $N \leq P_i$ o $N \leq Q_j$.

(ii) *$G = \langle a, b \rangle$ per ogni elemento non-banale $a \in Z(A)$ e $b \in Z(B)$.*

Innanzi tutto possiamo supporre che a e b abbiano ordini primi, in modo tale che $a \in P_i$ per qualche $i \leq s$ e $b \in Q_j$ per qualche $j \leq t$. Sia allora $H := \langle a, b \rangle$ un sottogruppo proprio di G. Da (i), esiste un sottogruppo $N \trianglelefteq H$ non-banale, contenuto in P_i o in Q_j. Supponiamo, senza perdita di generalità, che sia contenuto in Q_j. Sia ora $k \neq j$ e Q_k un q_k-sottogruppo di Sylow di B. Dato che B è nilpotente, quindi prodotto diretto dei suoi sottogruppi di Sylow, abbiamo che Q_k normalizza N, ovvero che $N \trianglelefteq \langle N, Q_k \rangle$. Ma quindi

anche $K := \langle a, Q_k \rangle$ è contenuto in $N_G(N)$ e quindi è un sottogruppo proprio di G. Riutilizzando (i), esiste un sottogruppo $M \trianglelefteq K$ non-banale contenuto in P_i o in Q_k. Supponiamo che $M \subseteq Q_k$. Questo vorrebbe dire che $M \trianglelefteq B$, e quindi

$$G = a^G = a^B \leq \langle a, B \rangle \leq N_G(M),$$

ovvero $M \trianglelefteq G$. Questa contraddizione forza M a stare in P_i.

Consideriamo allora P_h un p_h-sottogruppo di Sylow di A, con $h \neq i$. Ripetendo quello che abbiamo fatto nella prima parte della dimostrazione di questo passo, $L := \langle P_h, Q_k \rangle \subseteq N_G(M)$ ed è un sottogruppo proprio di G. Quindi da (i) esiste un sottogruppo $E \trianglelefteq L$ non-banale con E contenuto in P_h o in Q_k. Senza perdita di generalità sia $E \leq P_h$. Quindi $E \trianglelefteq A$ e

$$G = Q_k^G = Q_k^A \leq \langle Q_k, A \rangle \leq N_G(E),$$

ma questo contraddice la semplicità di G.

(iii) $C_G(a) = A$ *per ogni elemento non-banale* $a \in Z(A)$.
Dato che $C_G(a)$ contiene A, $C_G(a) = A(B \cap C_G(a))$. Assumiamo che A sia propriamente contenuto in $C_G(a)$. Allora $B \cap C_G(a)$ è non-banale, quindi $B \cap C_G(a) \cap Q_j \neq \emptyset$ per qualche $j \leq t$. Sia b un elemento non-banale in questa intersezione e consideriamo un q_k-sottogruppo di Sylow, Q_k, di B con $k \neq j$. Allora $Q_k \subseteq C_G(b)$ e dunque anche $\langle a, Q_k \rangle \leq C_G(b)$. Poichè da (ii) $G = \langle a, Q_k \rangle$, $C_G(b) = G$ e pertanto $b \in Z(G)$. Ma il centro di un gruppo semplice non abeliano è banale e questa contraddizione mostra che $A = C_G(a)$.

(iv) *Se* $x \in G$ *è tale che* $A \cap Z(A^x) \neq \{1\}$, *allora* $A^x = A$.
Per ipotesi, esiste un p_i-sottogruppo P_i di A, tale che $P_i \cap Z(A^x) \neq \{1\}$. Sia $a \in P_i \cap Z(A^x)$ non-banale. Da (iii) sappiamo che $C_G(a) = A^x$. Inoltre, dalla normalità di P_k in A e dal fatto che $a \in Z(A^x)$, si ha che P_k è contenuto in $C_G(a) = A^x$ per ogni $k \neq i$. Quindi $P_k = P_k^x$, e da (iii) segue che

$$A^x = C_G(Z(P_k))^x = C_G(Z(P_k^x)) = C_G(Z(P_k)) = A.$$

(v) *Sia* H *un sottogruppo di* G *contenente* $Z(A)$. *Allora* $P_i \cap H$ *è un* p_i*-sottogruppo di Sylow di* H *per ogni* $i \leq s$.

Sia P un p_i-sottogruppo di Sylow di H contenente $P_i \cap H$. Allora esiste $x \in G$ tale che $P \leq P_i^x$. Dunque

$$Z(P_i) = P_i \cap Z(A) \leq P_i \cap H \leq P \leq P_i^x \leq A^x.$$

Perciò $\{1\} \neq Z(P_i) \leq A^x \cap Z(A)$ e perciò anche $A \cap Z(A^{x^{-1}})$ è non-banale. Segue ora da (iv) che $A = A^{x^{-1}}$, e dunque $A = A^x$ e $P_i = P_i^x$. Da questo si ottiene che P è contenuto in $P_i \cap H$, e quindi $P = P_i \cap H$ è un p_i-sottogruppo di Sylow di H.

(vi) *Sia $H \leq G$ contenente $Z(A)$ tale che $H \cap N_G(P_i \cap H) = A \cap H$ per ogni $i \leq s$. Allora H è contenuto in A.*
Chiaramente

$$A \cap H = (P_i \cap H) \times ... \times (P_s \cap H)$$

e quindi, da (v), $A \cap H$ è un sottogruppo di Hall di H nilpotente . Inoltre, $\{1\} \neq Z(P_i) \leq Z(A) \leq H$ e $N_H(P_i \cap H) = A \cap H$ per ogni $i \leq s$.

Dal Lemma 2.2.8 esiste $N \trianglelefteq H$ tale che $H = (A \cap H)N$ e $(A \cap H) \cap N = \{1\}$. Ma allora $|N| = [H : A \cap H]$ divide $|B|$. Sia ora π l'insieme dei primi che dividono $|B|$. Allora sappiamo dai teoremi sui π-sottogruppi di Sylow, che B contiene un coniugato N^x di N per qualche $x \in G$. Scrivendo $x := ab$ con $a \in A$ e $b \in B$, N^a è contenuto in B, e perciò $Z(B)$ è contenuto in $N_G(N^a)$. Dato che $H \leq N_G(N)$, abbiamo che

$$Z(A) = Z(A)^a \leq H^a \leq N_G(N^a).$$

Perciò $N_G(N^a)$ contiene $\langle Z(A), Z(B) \rangle$, e quindi da (ii) si ha che $N_G(N^a) = G$. Ma N è propriamente contenuto in G, quindi necessariamente $N = \{1\}$ e $H = A \cap H \leq A$.

(vii) *I sottogruppi $A \cap N_G(B)$ e $B \cap N_G(A)$ contengono al massimo un sottogruppo di ordine p per ogni primo p.*
Sia $A_1 := A \cap N_G(B)$ e $a \in A_1$ ed assumiamo che $b^a = b$ per qualche elemento non-banale $b \in Z(B)$. Dato che da (iii) $C_G(b) = B$, abbiamo che a appartiene a $A \cap B = \{1\}$. Per cui A_1 è isomorfo al gruppo degli automorfismi di $Z(B)$ privi di punti fissi .

È noto che i sottogruppi di un gruppo di automorfismi privi di punti fissi di un gruppo possono essere ciclici, o isomorfi ad un gruppo dei quaternioni generalizzato. Da questo concludiamo che A_1 ha al massimo un sottogruppo di ordine p per ogni primo p.

(viii) *Se x è un elemento di G tale che $A \cap N_G(B) \cap A^x \neq \{1\}$, allora $A^x = A$.* Sia $\overline{a}$ un elemento di ordine primo in $A \cap N_G(B) \cap A^x$ e sia $H := \langle \overline{a} \rangle$. Consideriamo inoltre un elemento $g \in N_G(H)$ e scriviamo $g = ab^{-1}$ con $a \in A$ e $b \in B$. È ovvio che $H^g = H$, e quindi $H^a = H^b$. Dato che H^a è contenuto in A, e H^b è contenuto in $N_G(B)$, abbiamo che $H^a \leq A \cap N_G(B)$. Segue allora da (vii) che $H = H^a = H^b$.
Ma allora, $a \in A \cap N_G(H)$ e $b \in B \cap N_G(H)$ e quindi il normalizzatore

$$N_G(H) = (A \cap N_G(H))(B \cap N_G(H))$$

è un sottogruppo fattorizzabile di G. Inoltre $N_G(H)$ è un sottogruppo proprio di G, dunque è risolubile. Dalla nilpotenza di A e B possiamo anche dire che i sottogruppi

$$\overline{P}_i = P_i \cap N_G(H) \ \ (i = 1, ..., s)$$

e

$$\overline{Q}_j = Q_j \cap N_G(H) \ \ (j = 1, ..., t),$$

sono i sottogruppi di Sylow di $A \cap N_G(H)$ e di $B \cap N_G(H)$, rispettivamente. Supponiamo ora che $\overline{a}$ sia contenuto in P_i. Questo vuol dire che $P_k \subseteq N_G(H)$ per ogni $k \neq i$ e che, per questi k, vale che $\overline{P}_k = P_k$.

Dal Lemma 2.2.6, sappiamo che il prodotto $P_k\overline{Q}_j$ è un sottogruppo per ogni $j \leq t$. Sia ora N un sottogruppo normale minimale di questo prodotto. Allora N è contenuto in P_k o in $\overline{Q}_j$. Supponiamo che sia contenuto in $\overline{Q}_j$. Se questo fosse vero, allora Q_h sarebbe contenuto in $N_G(N)$ per ogni $h \neq j$. Ma questo vorrebbe dire che $N_G(N)$ contiene $\langle P_k, Q_h \rangle$ e quindi, da (ii), $N_G(N) = G$. Questa contraddizione forza N in P_k, e quindi $N \cap Z(P_k) \neq \{1\}$.

Sia ora u un elemento non-banale di $N \cap Z(P_k)$. Per ogni $y \in \overline{Q}_j$ si ha che

$$\langle u \rangle^y \leq \langle u \rangle^{\overline{Q}_j} \leq N^{\overline{Q}_j} = N \leq P_k \leq A,$$

e quindi

$$\langle u\rangle^y \leq A \cap Z(P_k)^y \leq A \cap Z(A)^y = A \cap Z(A^y).$$

Da (iv) si deduce che $A = A^y$ e quindi che $y \in N_G(A)$. Perciò $\overline{Q}_j \subseteq N_G(A)$ per ogni $j \leq t$ e $B \cap N_G(H) \leq N_G(A)$. Allora

$$N_G(H) = (A \cap N_G(H))(B \cap N_G(H)) \leq N_G(A).$$

Dato che $\overline{a}$ appartiene a A^x, otteniamo che

$$Z(A)^x = Z(A^x) \leq N_G(H) \leq N_G(A).$$

D'altra parte, $[N_G(A) : A]$ e $|Z(A)^x|$ sono coprimi e quindi $Z(A)^x \subseteq A$. Da (iv) concludiamo che $A = A^x$.

(ix) *Sia H un sottogruppo di G contenente $Z(A)$ con $B \cap N_G(A) \cap H^a = \{1\}$ per ogni $a \in A$. Allora H è contenuto in A.*
Da (v) l'intersezione $\overline{P}_i := P_i \cap H$ è un p_i-sottogruppo di Sylow di H per ogni $i \leq s$, quindi $A \cap H$ è un sottogruppo di Hall di H. Supponiamo, se possibile, che H non sia contenuto in A. Da (vi) segue che, per qualche $i \leq s$, si ha $A \cap H \leq H \cap N_G(P_i \cap H)$. Perciò deve esistere un primo $q \notin \{p_1, ..., p_s\}$ che divida $\left|H \cap N_G(\overline{P}_i)\right|$. Sia x un elemento di ordine q contenuto in $H \cap N_G(\overline{P}_i)$. Dato che $Z(P_i) \leq Z(A) \leq H$, abbiamo che

$$Z(P_i) \leq P_i \cap H = \overline{P}_i = \overline{P}_i^x \leq A^x.$$

Da (iv) si ottiene che $A = A^x$, e dunque che $x \in N_G(A)$. Dato che x ha ordine q, deve necessariamente esistere un elemento $a \in G$ tale che $x^a \in B$. Poichè $G = AB$, possiamo scelgliere $a \in A$ in modo tale che x^a appartenga a

$$B \cap N_G(A)^a \cap H^a = B \cap N_G(A) \cap H^a,$$

ma questo contraddice le ipotesi.

(x) *Se x è un elemento di G tale che $A^x \neq A$, allora $A \cap A^x = \{1\}$.*
Sia $H := \left\langle Z(A), Z(A)^x \right\rangle$. Ovviamente H è contenuto in $C_G(A \cap A^x)$, e poichè, da (iv), $Z(A)^x = Z(A^x)$ non è contenuto in A, allora H non è contenuto in A. Segue ora da (ix) che $B \cap N_G(A) \cap H^a \neq \{1\}$ per qualche $a \in A$. Inoltre

$$H^a \leq C_G(A \cap A^x)^a = C_G(A \cap A^{xa}),$$

e quindi

$$B \cap N_G(A) \cap C_G(A \cap A^{xa}) \neq \{1\}.$$

Sia ora u un elemento di $A \cap A^{xa}$. Allora

$$B \cap N_G(A) \cap C_G(u) = (B \cap N_G(A) \cap C_G(u))^u \leq B^u.$$

Quindi $B \cap N_G(A) \cap B^u \neq \{1\}$ e, da (viii), $B = B^u$. Perciò u appartiene a $A \cap N_G(B)$ e

$$A \cap A^{xa} = A \cap N_G(B) \cap A^{xa}.$$

Ma dato che $A \neq A^{xa}$ segue da (ix) che $A \cap N_G(B) \cap A^{xa} = \{1\}$. Quindi $A \cap A^{xa} = \{1\}$, e così $A \cap A^x = \{1\}$.

(xi) *Conclusione:*

Assumiamo che $|B| < |A|$. Dato che A non è normale in G, sappiamo che $A \neq A^x$ per qualche $x \in G$. Da (x) concludiamo che $A \cap A^x = \{1\}$. Quindi

$$|AA^x| = |A|\,|A|^x = |A|^2 > |A|\,|B| = |G|.$$

Questa contraddizione prova la tesi che A e B non possono avere ordine coprimo.

CASO 2: A e B non hanno ordine coprimo.

Sia p un primo che divide $|A|$ e $|B|$, e siano A_p e B_p i rispettivi p-sottogruppi di Sylow. Ovviamente B_p^x è un p-sottogruppo di Sylow di B^x per ogni $x \in G$. Quindi possiamo sfruttare il Lemma 2.2.4 e il Lemma 2.2.5, per dire che $A_pB_p^x$ è un p-sottogruppo di Sylow di G per ogni $x \in G$. Chiaramente A_pB_p è un sottogruppo proprio di G, e A_p, B_p sono due sottogruppi che rispettano le ipotesi del Lemma 2.2.6. Quindi possiamo concludere che G non può essere semplice. Scegliamo allora un sottogruppo normale minimale, N, di G. Dalla minimalità di G sappiamo che $G/N = (AN/N)(BN/N)$ è risolubile. Dato che G/N è risolubile, e G non lo è, N deve essere necessariamente un prodotto diretto di sottogruppi semplici non-abeliani. Ma questo vuol dire che $AN = A(B \cap AN)$ non è risolubile. Quindi dalla minimalità di G, $G = AN$.

Analogamente $G = BN$. Perciò $A_pN/N = B_pN/N$ è l'unico p-sottogruppo di Sylow del gruppo nilpotente G/N. Deduciamo quindi che $A_pN = B_pN$ è un sottogruppo normale di G. Ovviamente A_pN non è un p-gruppo, e dunque $A_pB_p \leq A_pN$. Riutilizzando il Lemma 2.2.5, possiamo dire che almeno uno fra A_p e B_p è contenuto in un sottogruppo normale proprio di A_pN. Sia K la chiusura normale di A_p in A_pN e supponiamo, senza perdità di generalità, che K sia un sottogruppo proprio di A_pN. Chiaramente A normalizza K, e quindi K è normale anche in $G = AN$. Dal fatto che

$$K = A_pN \cap K = A_p(N \cap K)$$

segue che $N \cap K$ è propriamente contenuto in N, e quindi, dalla minimalità di N, $N \cap K = \{1\}$. Dunque $A_p = K$ è un sottogruppo normale di G. Ma A_p è risolubile e G/A_p è risolubile, quindi G è risolubile. Questa contraddizione completa la dimostrazione. □

Capitolo 3

Una variazione del Teorema di Itō

In questo capitolo si fornisce una recente generalizzazione del Teorema di Itō data nel 2010 da Shumyatsky e Morigi: se X è un sottoinsieme normale di un gruppo G esistono $A, B \leq G$ abelliani tali che $X \subseteq AB$, allora $\langle X \rangle$ è metabeliano (cfr. [4]).

Definizione 3.0.1. Sia G un gruppo e $X \subseteq G$ un suo sottoinsieme. X si dice normale se $gxg^{-1} \in X$ per ogni $x \in X$ e per ogni $g \in G$.

Teorema 3.0.2. *Sia G un gruppo, X un sottoinsieme normale di G e siano $A, B \leq G$ abeliani tali che $X \subseteq AB$. Allora $\langle X \rangle$ è un sottogruppo metabeliano.*

Ovviamente questo teorema ha come caso particolare il Teorema di Itō, e la sua dimostrazione segue in qualche modo quella originale.

Nelle ipotesi del teorema, sia A^* l'insieme di tutti gli elementi $a \in A$ per cui esiste $b \in B$ tale che $ab \in X$. Definiamo inoltre A^{**} l'insieme di tutti gli elementi $a \in A$ per cui esiste $b \in B$ tale che $ba \in X$. Definiamo analogamente B^* e B^{**}. Ovviamente, dato che X è normale, $A^* = A^{**}$ e $B^* = B^{**}$.

Lemma 3.0.3. *Se $a \in A^*$ e $b \in B$, allora $a^b \in AB$. Similmente, se $a \in A$ e $b \in B^*$, allora $b^a \in AB$.*

Dimostrazione. Sia $b_1 \in B$ tale che $ab_1 \in X$. Allora $(ab_1)^b \in X$ e quindi $(ab_1)^b = a_2b_2$ per qualche $a_2 \in A^*$ e $b_2 \in B^*$. Pertanto $a^b = a_2b_2b_1^{-1} \in AB$. La dimostrazione della seconda parte è analoga. □

Dimostrazione. (Teorema 3.0.2) Siano $x_1, x_2 \in X$, $x_1 = a_1 b_1$ e $x_2 = a_2 b_2$, con $a_1, a_2 \in A^*$ e $b_1, b_2 \in B^*$. Presi $b_3, b_4 \in B^*$ vale che

$$[x_1^{-1}, b_3] = [a_1^{-1}, b_3] \qquad \text{e} \qquad [x_2^{-1}, b_4] = [a_2^{-1}, b_4].$$

Dal Lemma 3.0.3, sappiamo che $b_3^{a_2} = a_5 b_5$ e $a_3^{b_2} = a_6 b_6$ per qualche $a_5, a_6 \in A^*$ e $b_5, b_6 \in B^*$. Perciò è vera l'identità $(a_1^{-1})^{b_4^{-1}} = b_6^{-1} a_6^{-1}$. Ora calcoliamo

$$\begin{aligned}
&[x_1^{-1}, b_3]^{[x_2^{-1}, b_4]} = [a_1^{-1}, b_3]^{[a_2^{-1}, b_4]} = [(a_1^{-1})^{a_2}, b_3^{a_2}]^{b_4^{-1} a_2^{-1} b_4} \\
&= [a_1^{-1}, a_5 b_5]^{b_4^{-1} a_2^{-1} b_4} = [a_1^{-1}, b_5]^{b_4^{-1} a_2^{-1} b_4} = [(a_1^{-1})^{b_4^{-1}}, b_5^{b_4^{-1}}]^{a_2^{-1} b_4} \\
&= [b_6^{-1} a_6^{-1}, b_5]^{a_2^{-1} b_4} = [a_6^{-1}, b_5]^{a_2^{-1} b_4} = [a_6^{-1}, b_5^{a_2^{-1}}]^{b_4} = [a_6^{-1}, a_5^{-1} b_3]^{b_4} \\
&= [(a_6^{-1})^{b_4}, b_3] = [b_6 a_1^{-1}, b_3] = [a_1^{-1}, b_3] = [x_1^{-1}, b_3].
\end{aligned}$$

Questo mostra che $[X^{-1}, B^*]$ è abeliano. Dato che ogni commutatore nella forma $[a^{-1}, b]$ con $a \in A^*$ e $b \in B^*$ si può scrivere in una forma $[x^{-1}, b]$ con $x \in X$, possiamo dire che $D := [A^{-1}, B^*]$ è abeliano. Sia ora $E := \langle A, B \rangle$. Il nostro obbiettivo è dimostrare che D è normale in E. Scegliamo $a_0 \in A^*$, $a \in A$ e $b_7 \in B^*$. Sia inoltre $a_7 \in A^*$ tale che $a_7 b_7 \in X$. Ovviamente $(a_7 b_7)^a \in X$, quindi $(a_7 b_7)^a = a_8 b_8$ con $a_8 \in A^*$ e $b_8 \in B^*$. Ora

$$[a_0^{-1}, b_7]^a = [a_0^{-1}, a_7 b_7]^a = [a_0^{-1}, a_8 b_8] = [a_0^{-1}, b_8] \in D.$$

Analogamente possiamo procedere prendendo $b_0 \in B^*$ e $a_0 \in A^*$ tale che $a_0 b_0 \in X$. Infatti, scegliendo $b \in B^*$, otteniamo $(a_0 b_0)^b = a_9 b_9$ con $a_9 \in A^*$ e $b_9 \in B^*$. Similmente si ottiene

$$[a_0^{-1}, b_7]^b = [a_9^{-1}, b_7] \in D.$$

Questo mostra che sia A che B normalizzano D, quindi D è normale in E. Ovviamente $D = \langle A^*, B^* \rangle'$, e $\langle A^*, B^* \rangle / D$ è abeliano. Quindi $\langle A^*, B^* \rangle$ è un gruppo metabeliano contenente $\langle X \rangle$. Questo conclude la dimostrazione. $\square$

Bibliografia

[1] B. Amberg, S. Franciosi, F. de Giovanni. *Products of Groups*. Oxford Mathematical monographs. The Clarendon Press, Oxford University Press, New York, 1992.

[2] B. Huppert. *Endliche Gruppen I*. Springer, Berlin, 1967.

[3] J.S. Milne. *Group Theory*. Version 4.0. 1996-2021.

[4] M. Morigi, P. Shumyatsky. *A variation of the Ito theorem*. Journal of Algebra. 324(2010), 2052-2057.

[5] D.J.S. Robinson. *A course in the Theory of Groups*. Springer, New York, 1996.

Ringraziamenti

Alla fine di un lungo percorso non possono non esserci dei lunghi ringraziamenti, perché tutti abbiamo bisogno di qualcuno che ci aiuti nei momenti di difficoltà.

Innanzi tutto ringrazio il mio relatore, il professor Ernesto Spinelli.

Poi mi sembra giusto ringraziare la mia famiglia, che sono 20 anni che mi s$\frac{u}{o}$pporta.

Un ringraziamento incredibile ai due pilastri su cui mi sorreggo ogni volta che qualcosa va male, Lorenzo e Masia (quest'ultimo è un pilastro vero).

Un ringraziamento speciale va a Fra, Fra, Camilla, Rick, Carlo, Chiara, William e Chiara Plati. Perché studiare con loro è stato perfetto, e bere con loro è stato ancora meglio.

Un ringraziamento va a Emanuele Caiati, mio mentore, che mi ha insegnato tante cose fra cui il mio valore, il valore del lavoro e soprattutto che fine ha fatto Tranquillo.

Un ringraziamento va a Lorenzo Tomasi e a tutta l'ex squadra del Racing, che, anche se non mi hanno accompagnato fino all'ultimo giorno di triennale, sono stati la più grande e più bella valvola di sfogo che qualcuno possa volere.

Infine voglio ringraziare le due persone senza le quali laurearsi sarebbe stato quasi impossibile per una persona distratta come me: Daniele Tucci e Marta Piperno, due persone che potranno sempre contare su di me, visto quanto io ho fatto affidamento su di loro.