Appunti di Istituzioni di Algebra superiore

De Donato Paolo

Indice

Capitolo 1

Concetti preliminari

1.1 Concetti base della teoria dei gruppi

In questo capitolo elencheremo alcuni risultati della teoria dei gruppi che utilizzeremo. La gran parte di essi non verrà dimostrata in quanto si presume facciano già parte del bagaglio culturale dello studente.

Indici

Teorema 1.1.1 (Lagrange)**.** *Se G è un gruppo finito e $H \leq G$ allora*

$$|G| = |H| \, |G : H|$$

Proposizione 1.1.2. *Sia G gruppo e $H \leq K \leq G$ allora $|G : K| \leq |G : H|$. Se $H < K$ e $|G : K|$ è finito allora $|G : K| < |G : H|$. Se ancora $H, K \lhd G$ allora esiste un epimorfismo da G/K in G/H.*

Dimostrazione. L'applicazione

$$\phi : gH \in G/R'_H \to gK \in G/R'_K$$

è ben definita in quanto

$$gH = hH \Rightarrow h^{-1}g \in H \leq K \Rightarrow gK = hK$$

L'applicazione è banalmente suriettiva e quindi $|G : H| \leq |G : K|$. La funzione ϕ non è iniettiva se $H < K$ in quanto esisterà certamente un $l \in K \setminus H$ quindi $H \neq lH$ ma

$$\phi(lH) = lK = K = \phi(H)$$

quindi se $|G : K| < \infty$ o $|G : H|$ è infinito e quindi vale banalmente l'inclusione stretta oppure sarà anch'esso finito. In quest'ultimo caso ϕ è una applicazione suriettiva ma non iniettiva tra due insiemi finiti quindi $|G : K| < |G : H|$. ■

Proposizione 1.1.3. *Siano $M, N \leq G$ allora*

$$|G : (M \cap N)| \leq |G : M|\,|G : N|$$

Dimostrazione. Consideriamo l'applicazione

$$f : x\,(M \cap N) \in \frac{G}{R'_{M\cap N}} \to (xM, xN) \in \frac{G}{R'_M} \times \frac{G}{R'_N}$$

essa è ben definita ed iniettiva poiché

$$\begin{aligned} x(M \cap N) = y(M \cap N) \Leftrightarrow y^{-1}x \in M \cap N &\Leftrightarrow y^{-1}x \in M, y^{-1}x \in N \\ &\Leftrightarrow (xM, xN) = (yM, yN) \end{aligned}$$

e quindi $|G : (M \cap N)| \leq |G : M|\,|G : N|$. ∎

Lemma 1.1.4. *Sia $G = \langle g \rangle$ gruppo ciclico infinito e $H \leq G$, allora per ogni $n \in \mathbb{N}$ avremo che*

$$|\langle g \rangle : \langle g^n \rangle| = n$$

Lemma 1.1.5. *Sia $G = \langle g \rangle$ gruppo ciclico finito con $m = |G|$. Per ogni $n \in \mathbb{N}$ avremo che*

$$|\langle g \rangle : \langle g^n \rangle| = \gcd(m, n)$$

Teorema 1.1.6 (Identità di Dedekind)**.** *Sia G gruppo ed $H, K, L \leq G$ suoi sottogruppi con $L \leq H$. Allora*

$$L\,(K \cap H) = LK \cap H \qquad (1.1.1)$$
$$(K \cap H)\,L = H \cap KL \qquad (1.1.2)$$

Dimostrazione. Dimostriamo solo la (1.1.1), l'altra si dimostra con un procedimento analogo.

Innanzitutto $K \cap H \leq K$ e quindi $L\,(K \cap H) \subseteq LK \cap H$ poiché $L \leq H$. Viceversa presi $k \in K, l \in L$ tali che $lk \in H$ segue immediatamente che $k \in H$ e quindi $lk \in L\,(K \cap H)$. ∎

Proposizione 1.1.7. *Presi $A, B \leq G$ tali che $B \lhd \langle A, B \rangle$ allora $\langle A, B \rangle = AB$ e*

$$\frac{AB}{B} \cong \frac{A}{A \cap B} \qquad (1.1.3)$$

Se B non fosse un sottogruppo normale non potremmo costruire il gruppo quoziente, ciononostante vale un risultato simile anche se più debole.

Proposizione 1.1.8. *Siano $A, B \leq G$ tali che $\langle A, B \rangle = AB$. Allora*

$$|AB : B| = |A : A \cap B|$$

Dimostrazione. Chiaramente dalle ipotesi segue che AB è un sottogruppo di G e quindi

$$AB/R'_B = \{aB \mid a \in A\}$$

Ora per ogni $a, a' \in A$

$$aB = a'B \Leftrightarrow a^{-1}a' \in B \Leftrightarrow a^{-1}a' \in A \cap B \Leftrightarrow a\,(A \cap B) = a'\,(A \cap B)$$

e quindi l'applicazione

$$f : aB \in AB/R'_B \to a\,(A \cap B) \in A/R'_{A\cap B}$$

è ben definita e biettiva, quindi i due insiemi hanno la stessa cardinalità. ■

Corollario 1.1.9. *Presi $A, B, C \leq G$ tali che*

- $\langle A, B\rangle = AB$ *e* $\langle A, C\rangle = AC$*;*
- $C \leq B$*;*
- $A \cap B \leq C$*.*

allora

$$|AB : AC| = |B : C|$$

Dimostrazione. Chiaramente $(AC)\,B = AB \leq G$ per cui dalla proposizione precedente e dall'identità di Dedekind

$$|AB : AC| = |(AC)\,B : AC| = |B : B \cap AC| = |B : (B \cap A)\,C| = |B : C|$$

■

Teorema 1.1.10 (Inverso forte di Lagrange)**.** *Se $G = \langle g\rangle$ ciclico e $H \leq G$ allora esiste $n \in \mathbb{N}_0$ tale che $H = \langle g^n\rangle$. Inoltre $|G : H| < \infty$ e non esistono altri sottogruppi di G distinti da H con il medesimo indice.*

Teorema 1.1.11 (Inverso debole del teorema di Lagrange)**.** *Se G è un gruppo abeliano finito allora per ogni $n \in \mathbb{N}$ tale che $n \mid |G|$ esiste $H \leq G$ tale che $|H| = n$.*

Periodicità

Un elemento g di G è detto *periodico* se e solo se esiste $n \in \mathbb{N}$ tale che $g^n = 1$. Un gruppo G è detto *periodico* se tutti i suoi elementi sono periodici mentre è *aperiodico* o *senza torsione* se e solo se il suo unico elemento periodico è l'elemento neutro.

Chiaramente si ha

$$g \text{ periodico} \Leftrightarrow \langle g\rangle \text{ finito}$$

e $|\langle g\rangle|$ coincide con l'ordine di g.

Se G è gruppo generico, allora per ogni $n \in \mathbb{N}$ definiamo

$$G^n = \langle g^n \mid g \in G \rangle$$

che in notazione additiva diventa nG. Se G è un gruppo abeliano poiché $(xy)^n = x^n y^n$ dunque G^n è composto interamente di potenze n-esime di G.

Il gruppo G ha *esponente finito* $n \in \mathbb{N}$ se e solo se $G^n = \{1\}$ e il più piccolo di tali $n \in \mathbb{N}$ è detto *esponente* di G.

Proposizione 1.1.12. *Sia $g \in G$ periodico allora se $g^n = 1$ per un certo $n \in \mathbb{Z}$ l'ordine di g deve dividere n.*

Proposizione 1.1.13. *Se G ha esponente 2 allora è abeliano.*

Dimostrazione. Presi $x, y \in G$ avremo che $x^2 = y^2 = (xy)^2 = 1$ e quindi

$$yx = (xy)^2 yx = xyxyyx = xyxx = xy$$

e quindi G è abeliano. ∎

Nocciolo e chiusura normale

Consideriamo un generico gruppo G, $H \leq G$ un suo sottogruppo e $X \subseteq G$ sottoinsieme non vuoto, la *chiusura normale* di H in X è il sottogruppo

$$H^X = \langle H^x \mid x \in X \rangle$$

mentre il *nocciolo* di H in X vale

$$H_X = \bigcap_{x \in X} H^x$$

Vale il seguente risultato

Teorema 1.1.14. *Sia $H, K \leq G$ allora*

$$H^K = \bigcap \{N \leq G \mid N \lhd \langle H, K \rangle, H \leq N\}$$
$$H_K = \langle N \leq G \mid N \lhd \langle H, K \rangle \wedge N \leq H \rangle$$

Chiaramente H^G, $H_G \lhd G$ e sono rispettivamente il più piccolo sottogruppo normale contenete H e il più grande sottogruppo normale contenuto in H.

Proposizione 1.1.15. *Sia G gruppo e $H \leq G$ tale che $|G : H| = n \in \mathbb{N}$. Allora $|G : H_G|$ divide $n!$.*

Dimostrazione. Poniamo $X = G/R''_H = \{Hg \mid g \in G\}$, osserviamo che X non è un gruppo non essendo H normale. Ciononostante l'insieme delle permutazioni su X, che indichiamo con S_X, è un gruppo rispetto all'operazione di composizione ovvero per ogni $\phi_1, \phi_2 \in S_X$ e $x \in X$

$$(\phi_1\phi_2)(x) = \phi_2[\phi_1(x)]$$

Non è difficile dimostrare che se $|X| = n$ allora $|S_X| = n!$. Per ogni $g \in G$ consideriamo l'applicazione

$$\psi_g : Hx \in X \to Hxg \in X$$

è chiaramente una permutazione poiché $\psi_g^{-1} = \psi_{g^{-1}}$ e quindi $\psi_g \in S_X$.

Definiamo adesso

$$f : g \in G \to \psi_g \in S_X$$

la funzione f è in realtà un omomorfismo in quanto per ogni $g, g' \in G$ e $Hx \in X$

$$\psi_{gg'}(Hx) = Hxgg' = [\psi_g(Hx)]\, g' = \psi_{g'}[\psi_g(Hx)] = \left(\psi_g\psi_{g'}\right)(Hx)$$

determiniamo il kernel di f. L'elemento neutro di S_X è chiaramente l'applicazione identica id_X su X, quindi preso $g \in G$ tale che per ogni $Hx \in X$

$$f(g) = \mathrm{id}_X \Leftrightarrow Hxg = \psi_g(Hx) = Hx \Leftrightarrow xgx^{-1} \in H \Leftrightarrow g \in H^x$$

e perciò

$$g \in \ker f \Leftrightarrow g \in \bigcap_{x \in G} x^{-1}Hx = H_G$$

Dalla proprietà universale il quoziente G/H_G è isomorfo ad un sottogruppo di S_X e quindi $|G : H_G|$ divide $|S_X| = n!$ ottenendo così la tesi. ∎

Centralizzante e normalizzante

Siano ora $H, K \leq G$ sottogruppi, il *normalizzante* di H rispetto a K è il sottogruppo

$$N_K(H) = \{k \in K \mid kH = Hk\}$$

Inoltre per ogni $X, Y \subseteq G$ sottoinsiemi non vuoti di G definiamo il *centralizzante* di X rispetto ad Y il sottoinsieme

$$C_Y(X) = \{y \in Y \mid xy = yx\, \forall x \in X\}$$

se $Y \leq G$ allora $C_Y(X) \leq G$ anche se X non è un sottogruppo.

Se $H, K \leq G$ allora $C_K(H) \leq N_K(H)$ chiaramente.

Proposizione 1.1.16. *Se $N \lhd G$ allora $C_G(N) \lhd G$*

Dimostrazione. Sia $x \in N$, $g \in G$ e $y \in C_G(N)$ allora

$$y^g x = \left(yx^{g^{-1}}\right)^g = \left(x^{g^{-1}}y\right)^g = xy^g$$

∎

1.2 Prodotto diretto e semidiretto

Prodotto diretto

Definizione 1.2.1. Presa una generica famiglia di gruppi $\mathcal{F} = \{G_i\}_{i\in I}$ definiamo il *prodotto diretto esterno* di $\mathcal{F}$ il gruppo

$$\operatorname*{Dr}_{i\in I} G_i$$

composto interamente dalle applicazioni $x : I \to \bigcup_i G_i$ tali che $x(i) \in G_i$ per ogni indice $i \in I$ e inoltre $x(i) \neq 1_i$, dove 1_i è l'elemento neutro di G_i, soltanto per un *numero finito* di indici $i \in I$.

Se $\{H_i\}_{i\in I} = \{H_1, H_2, \ldots, H_t\}$ allora utilizzeremo anche la notazione

$$G_1 \times G_2 \times \cdots \times G_t$$

Per ogni $x \in \mathrm{Dr}_{i\in I} G_i$ porremo $x_i = x(i)$ e x_i sarà chiamata la *componente* di x su G_i. Il prodotto diretto esterno risulta essere un gruppo rispetto all'operazione

$$(x \cdot y)_i = x_i y_i \text{ per ogni } i \in I$$

con elemento neutro $(1)_i = 1_i$ e $\left(x_i^{-1}\right) = (x_i)^{-1}$.

Quindi per ogni elemento x del prodotto diretto esterno di $\{G_i\}_{i\in I}$ se $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ sono le uniche componenti di x non identiche allora avremo che

$$x = x_{i_1} x_{i_k} \cdots x_{i_k}$$

dove abbiamo identificato $x_i \in G_i$ con quell'unico elemento nel prodotto diretto esterno la cui componente i-esima vale x_i e tutte le altre sono identiche. Con questa identificazione G_i è isomorfo ad un sottogruppo di $\mathrm{Dr}_{i\in I} G_i$.

Definizione 1.2.2. Se G è un gruppo generico e $\mathcal{F} = \{H_i\}_{i\in I}$ è una famiglia di sottogruppi di G diciamo che G è *prodotto diretto interno* di $\mathcal{F}$ se e solo se valgono le seguenti asserzioni

1. $H_i \lhd G$ per ogni $i \in I$;
2. $G = \langle H_i \mid i \in I\rangle$;
3. $H_i \cap \langle H_j \mid j \neq i\rangle = \{1\}$ per ogni $i \in I$.

Teorema 1.2.3. *Sia G un gruppo generico e $\mathcal{F} = \{H_i\}_{i\in I}$ famiglia di sottogruppi di G. Dunque G è prodotto diretto interno di $\mathcal{F}$ se e solo se valgono le seguenti asserzioni:*

1. *Per ogni $x \in H_i$ e per ogni $y \in H_j$ con $i \neq j$ si ha $xy = yx$;*
2. *Gli elementi di G si esprimono in maniera univoca (a meno del prodotto di un numero arbitrario di copie dell'elemento neutro) come prodotto di un numero finito di elementi appartenenti ciascuno ad un diverso H_i.*

Teorema 1.2.4. *Se G è prodotto diretto interno della famiglia di sottogruppi $\{H_i\}_{i\in I}$ allora il prodotto diretto esterno della medesima famiglia è isomorfo a G.*

Ancora presa una famiglia generica di gruppi $\{G_i\}_{i\in I}$ e sia $G = \mathrm{Dr}_{i\in I} G_i$ allora ogni G_i è isomorfo ad un opportuno $H_i \leq G$ e G è prodotto diretto interno della famiglia $\{H_i\}_{i\in I}$.

Per questo motivo parleremo da ora in poi solamente di *prodotto diretto* identificando le due definizioni e utilizzando la medesima simbologia. In notazione additiva indicheremo il prodotto diretto come

$$\bigoplus_{i\in I} G_i$$

mentre per una famiglia finita useremo anche la notazione

$$G_1 \oplus G_2 \oplus \cdots \oplus G_t$$

Proposizione 1.2.5. *Sia $G = \mathrm{Dr}_{i\in I} G_i$ e per ogni $i \in I$ prendiamo H_i sottogruppo normale di G_i. Allora $H = \mathrm{Dr}_{i\in I} H_i$ è un sottogruppo di G e*

$$\frac{G}{H} \cong \operatorname*{Dr}_{i\in I} \frac{G_i}{H_i}$$

Prodotto semidiretto

Definizione 1.2.6. Presi due qualunque gruppi K, A e un monomorfismo $F : K \to \mathrm{Aut}(A)$ definiamo *prodotto semidiretto esterno* di K per A tramite F il gruppo

$$K \ltimes_F A$$

composto dalle coppie (k, a) con $k \in K$, $a \in A$ e dotato dell'operazione di prodotto

$$(k, a)\left(k', a'\right) = \left(kk'\right) a^{F(k')} a'$$

dove per ogni $f \in \mathrm{Aut}(A)$ si pone per definizione $a^f = f(a) \in A$.

Si ricorda che $\mathrm{Aut}(A)$ è un gruppo rispetto al prodotto $(fg)(a) = g\left[f(a)\right]$ per ogni $f, g \in \mathrm{Aut}(A)$ e $a \in A$. Quindi valgono i seguenti risultati:

$$\begin{gathered}\left(a^f\right)^g = a^{fg} \\ (ab)^f = a^f b^f \\ 1^f = 1 \\ a^{\mathrm{id}} = a \\ \left(a^f\right)^{-1} = \left(a^{-1}\right)^f\end{gathered}$$

Con questa definizione di prodotto il prodotto semidiretto esterno è un gruppo con elemento neutro $(1_K, 1_A)$, in quanto $F(1_K) = \mathrm{id}_A$ essendo F omomorfismo, e inverso

$$(k,a)^{-1} = \left(k^{-1}, \left(a^{-1}\right)^{F\left(k^{-1}\right)}\right)$$

Notiamo inoltre che per ogni $k \in K$ e $a, b \in A$

$$(1,b)^{(k,a)} = \left(1, a^{-1} b^{F(k)} a\right)$$

Definizione 1.2.7. Se G è un gruppo generico e $K, H \leq G$ diciamo che G è *prodotto semidiretto interno* di K per H se e solo se valgono le seguenti asserzioni

1. $H \lhd G$;
2. $G = \langle H, K \rangle$;
3. $H \cap K = \{1\}$.

Se G è prodotto semidiretto interno di K per H allora scriveremo $G = K \ltimes H$.

Teorema 1.2.8. *Sia G un gruppo generico e $K, H \leq G$ famiglia di sottogruppi di G. Dunque G è prodotto diretto interno di $\mathcal{F}$ se e solo se valgono le seguenti asserzioni:*

1. *$H \lhd G$*
2. *Per ogni $g \in G$ esistono e sono univocamente determinati $h \in H$ e $k \in K$ tali che $g = kh$.*

Osservazione. Se G è un gruppo generico e $H \lhd G$ allora per ogni $g \in G$ l'applicazione

$$g^* : h \in H \to h^g \in H$$

è un automorfismo di H.

Teorema 1.2.9. *Se $G = K \ltimes H$ allora posto $\theta : k \in K \to k^* \in \mathrm{Aut}(G)$ avremo che $G \cong K \ltimes_\theta H$.*

Ancora presi H e K gruppi generici e $F : K \to \mathrm{Aut}(G)$ definiamo $G = K \ltimes_F H$. Allora esiste $K' \leq G$ isomorfo a K e $H' \leq G$ isomorfo a H tali che $G = K' \ltimes H'$.

Per questo motivo parleremo da ora in poi solamente di *prodotto semidiretto*.

Gruppi diedrali

Prendiamo A un generico gruppo abeliano tale che $A^2 \neq \{1\}$, quindi esisterà in A almeno un elemento distinto dal proprio inverso.

Per questo motivo l'applicazione

$$x : a \in A \to a^{-1} \in A$$

non solo è biiettiva ma è un automorfismo distinto dall'automorfismo identico id_A. Inoltre $x^2 = \mathrm{id}_A$ e quindi $\langle x \rangle = \{\mathrm{id}_A, x\} \leq \mathrm{Aut}(G)$ e possiamo definire il *gruppo diedrale* su A il gruppo

$$D_A = \langle x \rangle \ltimes A$$

Per comodità di notazione supponiamo che A e $\langle x \rangle$ siano sottogruppi di D_A.

Proposizione 1.2.10. *Per ogni $a \in A$ avremo che $a^x = xax = a^{-1}$.*

Proposizione 1.2.11. *I sottogruppi di A sono normali propri in D_A.*

Dimostrazione. Se $H \leq A$ allora dalla proposizione di prima $x \in N_{D_A}(H)$ mentre $A \leq N_{D_A}(H)$ essendo abeliano quindi $D_A = N_{D_A}(H)$ e $H \lhd D_A$. ∎

Se $A = \langle a \rangle$ è ciclico di ordine n allora poniamo $D_A = D_{2n}$ mentre se A è ciclico infinito $D_A = D_\infty$.

Proposizione 1.2.12. *Se A è un gruppo ciclico generato da a allora $(xa)^2 = 1$ e*

$$D_A = \langle x, xa \rangle$$

Osservazione. Gli elementi x e xa che generano D_A hanno entrambi ordine 2 mentre D_A possiede sempre elementi di ordine diverso da 2. Questo esempio mostra che in un gruppo non abeliano il quadrato di un prodotto è in generale diverso dal prodotto dei quadrati.

Proposizione 1.2.13. *Sia A gruppo abeliano con $A^2 \neq \{1\}$ allora $Z(D_A) = A[2]$.*

Dimostrazione. Sia $D_A = \langle x \rangle \ltimes A$ chiaramente per ogni $a \in A$ $a^x = a^{-1}$. Quindi se $a^2 = 1$ allora $a^x = a^{-1} = a \Rightarrow xa = ax$ e quindi $A[2] \leq Z(D_A)$. Ora prendiamo $b \in Z(D_A)$, se esistesse $a \in A$ tale che $b = xa$ allora per ogni $a' \in A$

$$a'b = ba' \Leftrightarrow a'xa = xaa' = x\left(a'\right)^{-1}a \Leftrightarrow a' = \left(a'\right)^{-1} \Leftrightarrow \left(a'\right)^2 = 1$$

e quindi $A^2 = \{1\}$ il che è assurdo. Perciò $b \in A$ e quindi $xb = bx = xb^{-1} \Rightarrow b^2 = 1$ ovvero $b \in A[2]$- ∎

1.3 I teoremi di Sylow

Definizione 1.3.1. Sia p un numero primo, un gruppo G è un *p-gruppo* se e solo se è periodico e i suoi elementi hanno tutti periodo una potenza di p. Un elemento g di un generico gruppo G è un *p-elemento* se e solo se ha ordine una potenza di p.

Un sottogruppo $H \leq G$ è un *p-sottogruppo di Sylow* se e solo se è un p-sottogruppo ed è massimale nella classe dei p-sottogruppi di G. Denotiamo con $Syl_p(G)$ l'insieme di tutti i p-sottogruppi di Sylow di G.

Proposizione 1.3.2. *Un gruppo G finito è un p-gruppo se e solo se $|G|$ è una potenza di p.*

Primo teorema di Sylow. Sia G gruppo finito e p primo tale che $p^n \mid |G|$ per un opportuno $n \in \mathbb{N}$, allora esiste $H \leq G$ tale che $|H| = p^n$.

Corollario. Se G è un gruppo finito con $|G| = n$ allora per ogni primo p tale che $p \mid n$ esiste un p-sottogruppo di Sylow P di G. Inoltre un generico sottogruppo S di G con $|S| = p^k$ è un p-sottogruppo di Sylow di G se e solo se $p^k \mid n$ e $p^{k+1} \nmid n$.

Secondo teorema di Sylow. Sia G finito e P, Q due p-sottogruppi di Sylow di G. Esisterà allora un elemento $x \in G$ tale che $Q = P^x$.

Corollario. Se p divide l'ordine del gruppo G allora ogni p-sottogruppo di Sylow di G è normale se e solo se è l'unico p-sottogruppo di Sylow di G.

Preso un generico $P \in Syl_p(G)$ vale l'uguaglianza degli indici

$$\left|Syl_p(G)\right| = |G : N_G(P)|$$

e quindi la cardinalità di $Syl_p(G)$ deve dividere $|G|$.

Osservazione. Se G è un gruppo infinito non vale più il secondo teorema di Sylow. Ciononostante possiamo sempre dire che se P è l'*unico* p-sottogruppo di Sylow di G generico allora P è caratteristico in G e quindi normale, in quanto gli automorfismi di G mandano p-sottogruppi massimali in altri p-sottogruppi massimali.

Terzo teorema di Sylow. Se G è un gruppo finito e p numero primo allora esiste $k \in \mathbb{N}_0$ tale che

$$\left|Syl_p(G)\right| = 1 + kp$$

Proposizione 1.3.3. *Sia G gruppo periodico allora*

$$G = \langle P \leq G \mid P \textit{ sottogruppo di Sylow} \rangle$$

Dimostrazione. Poiché G è periodico per ogni $g \in G$ esisterà $n \in \mathbb{N}$ tale che $g^n = 1$. Se $g \neq 1$ allora $n > 1$ e $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ è la sua scomposizione in fattori primi, definiamo allora per ogni i intero tra 1 e k l'intero l_i in modo tale che $n = p_i^{m_i} l_i$.

Poiché $\gcd(l_1, l_2, \ldots, l_k) = 1$ sono a due a due coprimi dal teorema di Bezout esistono $j_1, j_2, \ldots, j_k \in \mathbb{Z}$ tali che

$$l_1 j_1 + l_2 j_2 + \cdots + l_k j_k = 1$$

Se definiamo adesso $h_i = g^{l_i j_i}$ allora

$$h_i^{p_i^{m_i}} = g^{p_i^{m_i} l_i j_i} = g^{n j_i} = 1$$

quindi h_i è un p_i-elemento e sarà dunque contenuto in qualche p_i-sottogruppo di Sylow e

$$g = g^{l_1 j_1 + l_2 j_2 + \cdots + l_k j_k} = g^{l_1 j_1} g^{l_2 j_2} \cdots g^{l_k j_k} = h_1 h_2 \cdots h_k$$

dunque $g \in \langle P \leq G \mid P \text{ sottogruppo di Sylow} \rangle$. ■

1.4 Classi di gruppi

Per comodità di notazione identifichiamo una generica proprietà dei gruppi con una *classe* e diciamo che un certo gruppo G appartiene alla classe $\mathcal{X}$ se e solo se G soddisfa la relativa proprietà. Le proprietà basilari che richiediamo implicitamente in ogni classe di gruppi $\mathcal{X}$ sono le seguenti:

- $\{1\} \in \mathcal{X}$;
- Se $G \in \mathcal{X}$ e $G \cong G'$ allora $G' \in \mathcal{X}$.

Per esempio sia $\mathcal{F}$ la classe dei gruppi finiti, poniamo allora

$$G \in \mathcal{F} \Leftrightarrow G \text{ finito}$$

Definizione 1.4.1. Una classe $\mathcal{X}$ si dice *chiusa per sottogruppi* se e solo se per ogni $G \in \mathcal{X}$ ed $H \leq G$ si ha $H \in \mathcal{X}$.

Una classe $\mathcal{X}$ si dice *chiusa per quozienti* se e solo se per ogni $G \in \mathcal{X}$ ed $H \lhd G$ si ha $G/H \in \mathcal{X}$.

Una classe $\mathcal{X}$ si dice *chiusa per estensioni* se e solo se per ogni gruppo G ed $H \lhd G$ tali che $H, G/H \in \mathcal{X}$ si ha $G \in \mathcal{X}$.

Proposizione 1.4.2. *Sia $\mathcal{X}$ una classe di gruppi chiusa per quozienti ed estensioni. Allora per ogni $M, N \lhd G$ tali che $M, N \in \mathcal{X}$ si avrà*

$$MN \in \mathcal{X}$$

Dimostrazione. Chiaramente $MN, M \cap N \lhd G$ e perciò dalla chiusura per sottogruppi

$$MN/N \cong M/(M \cap N) \in \mathcal{X}$$

poiché $N \in \mathcal{X}$ la tesi segue dalla chiusura per estensioni. ■

Esempio 1. Queste caratteristiche delle classi di gruppi sono tutte indipendenti tra loro, come dimostrano i seguenti esempi.

- La classe dei gruppi finiti è chiusa per sottogruppi, quozienti ed estensioni;
- La classe dei gruppi finitamente generati è chiusa per quozienti ed estensioni ma non per sottogruppi;
- La classe dei gruppi abeliani è chiusa per sottogruppi e quozienti ma non per estensioni;
- La classe dei gruppi policiclici infiniti (pag. 92) è chiusa per sottogruppi ed estensioni ma non per quozienti.

Definizione 1.4.3. Presa una qualunque classe di gruppi $\mathcal{X}$ definiamo la classe *localmente* $\mathcal{X}$ la nuova classe $L\mathcal{X}$ definita nel seguente modo

$$G \in L\mathcal{X} \Leftrightarrow \forall X \subseteq G \text{ finito } \exists H \leq G \text{ tale che } X \subseteq H \wedge H \in \mathcal{X} \tag{1.4.1}$$

Chiaramente $\mathcal{X} \subseteq L\mathcal{X}$ ed $LL\mathcal{X} = L\mathcal{X}$. Nel caso particolare in cui $\mathcal{X}$ sia chiusa per sottogruppi la (1.4.1) può essere riscritta come

$$G \in L\mathcal{X} \Leftrightarrow H \in \mathcal{X} \ \forall H \leq G \text{ finitamente generato} \tag{1.4.2}$$

Si ricorda che la (1.4.2) vale se e solo se $\mathcal{X}$ è chiuso per sottogruppi e non altrimenti.

Proposizione 1.4.4. *Presa una generica classe di gruppi $\mathcal{X}$ allora*

1. *Se $\mathcal{X}$ è chiusa per sottogruppi allora anche $L\mathcal{X}$ è chiusa per sottogruppi;*
2. *Se $\mathcal{X}$ è chiusa per quozienti allora anche $L\mathcal{X}$ è chiusa per quozienti.*

Dimostrazione. Dimostriamo innanzitutto il primo punto, prendiamo allora $G \in L\mathcal{X}$ ed $H \leq G$. Prendiamo dunque $X \subseteq H$ finito, per quanto detto prima allora $\langle X \rangle \in \mathcal{X}$ e $\langle \mathcal{X} \rangle \leq H$ dunque $H \in L\mathcal{X}$.

Sia ora $\mathcal{X}$ chiusa per quozienti, prendiamo $G \in L\mathcal{X}$ e $N \lhd G$. Preso $X \subseteq G$ finito e $X' = \{xN \mid x \in X\} \subseteq G/N$ esisterà $X \subseteq H \leq G$ per cui $H \in \mathcal{X}$. Dalla chiusura per quozienti allora $HN/N \cong H/(H \cap N) \in \mathcal{X}$ e $X' \subseteq HN/N$ quindi $L\mathcal{X}$ è chiusa per quozienti. ■

Definizione 1.4.5. Sia $\mathcal{X}$ una generica classe di gruppi e G gruppo generico, allora il *$\mathcal{X}$-radicale* di G è il sottogruppo

$$\rho_{\mathcal{X}}(G) = \langle N \lhd G \mid N \in \mathcal{X} \rangle$$

Teorema 1.4.6. *Se G è un gruppo generico allora $\rho_{\mathcal{X}}(G)$ è caratteristico in G.*

Dimostrazione. Gli automorfismi mandano sempre sottogruppi normali in sottogruppi normali e gruppi in $\mathcal{X}$ in altri gruppi sempre in $\mathcal{X}$, quindi il radicale è sempre caratteristico. ■

Lemma 1.4.7. *Sia G gruppo generico e $\mathcal{X}$ una classe di gruppi generici tale che per ogni $M, N \lhd G$ tali che $M, N \in \mathcal{X}$ si ha $MN \in \mathcal{X}$. Allora $\rho_{\mathcal{X}}(G) \in L\mathcal{X}$.*

Dimostrazione. Consideriamo $X \subseteq \rho_{\mathcal{X}}(G)$ finito, allora X sarà contenuto nel sottogruppo generato da $N_1, N_2, \ldots, N_l$ con $N_i \lhd G$ e $N_i \in \mathcal{X}$. Essendo normali allora $X \subseteq N_1 N_2 \cdots N_l \in \mathcal{X}$ e quindi la tesi. ■

1.5 Prodotti intrecciati

Presi H, K gruppi generici, supponiamo che per ogni $k \in K$ esista un gruppo H_k isomorfo a H ed $\varphi_k : H \to H_k$ il relativo isomorfismo. Poniamo per comodità $H_1 = H$ ed $\varphi_1 = id_H$ allora per ogni $k, y \in K$ definiamo

$$\theta_k^y : h \in H_y \to (\varphi_{ky} \circ \varphi_y^{-1})(h) \in H_{ky} \tag{1.5.1}$$

la quale effettua una sorta di moltiplicazione a sinistra di y per k tra questi gruppi.

Posto $B = \mathrm{Dr}_{k \in K} H_k$ non è difficile dimostrare che esiste un unico automorfismo $\theta_k : B \to B$ tale che $\theta_k(h_y) = \theta_k^y(h_y)$ per ogni $h_y \in H_y$. Dimostriamo ora che l'applicazione

$$F : k \in K \to \theta_k \in \mathrm{Aut}\, B$$

è un omomorfismo di gruppi, difatti per ogni $y \in K$ e $h \in H_y$

$$\begin{aligned}\theta_{k'k}(h) = \theta_{k'k}^y(h) = (\varphi_{k'ky} \circ \varphi_y^{-1})(h) &= (\varphi_{k'ky} \circ \varphi_{ky}^{-1} \circ \varphi_{ky} \circ \varphi_y^{-1})(h) \\ &= (\theta_{k'}^{ky} \circ \theta_k^y)(h) = (\theta_{k'} \circ \theta_k)(h)\end{aligned}$$

e quindi è un omomorfismo tra gruppi.

Definiamo allora il *prodotto intrecciato standard* tra H e K il gruppo

$$H \sim K = K \ltimes_F B$$

il sottogruppo B è detto *gruppo base* di $H \sim K$.

Proposizione 1.5.1. *Fissato $G = H \sim K$ allora*

$$H^G = B$$

Dimostrazione. Innanzitutto $B \lhd G \Rightarrow H^G \leq B$, dalla definizione di prodotto semidiretto si ha $H^k = \theta_k(H) = H_k$ per ogni $k \in K$ e quindi

$$H^G \geq \left\langle H^k \;\middle|\; k \in K \right\rangle = B$$

■

Teorema 1.5.2. *Definito $G = H \sim K$ allora*

1. *Se K è infinito allora $Z(G) = \{1\}$;*
2. *Se $K = \{1, k_1, k_2, \ldots, k_t\}$ allora $Z(G) = \left\{ hh^{k_1}h^{k_2} \cdots h^{k_t} \;\middle|\; h \in Z(H) \right\}$.*

Dimostrazione. Per comodità di notazione poniamo $H_{k_i} = H_i$ nel caso in cui K sia finito, allora $h \in H \Leftrightarrow h^{k_i} \in H_i$.

Supponiamo K finito e dimostriamo che $Z(G) \supseteq U = \left\{ hh^{k_1}h^{k_2} \cdots h^{k_t} \;\middle|\; h \in Z(H) \right\}$, chiaramente $h \in Z(H) \Rightarrow h^{k_i} \in Z(H_i)$ e quindi $u = hh^{k_1}h^{k_2} \cdots h^{k_t} \in Z(B) \Rightarrow B \leq C_G(U)$. Se ora prendiamo $k \in K$ allora l'applicazione $k_i \in K \to k_i k \in K$ è in realtà una permutazione e perciò $u^k = u$ e quindi

$$K \leq C_G(U) \Rightarrow G = C_G(U) \Rightarrow U \leq Z(G)$$

Viceversa prendiamo $bk \in Z(G)$ dove $b \in B$ e $k \in K$, con K finito o infinito, allora per ogni $h \in H$

$$h = h^{bk} = \left(h^b\right)^k \in H \cap H_k \Rightarrow H = H_k \Rightarrow k = 1$$

e quindi $Z(G) \leq B$. Esisteranno inoltre $b_k \in H_k$ tali che $b = \prod_{k \in K} b_k$, ricordiamo che dalla definizione di prodotto diretto $b_k \neq 1$ solamente per un numero finito di $k \in K$. Allora per ogni $k \in K$

$$b = b^k = \prod_{i \in K} b_i^k \Leftrightarrow b_i = b_{k^{-1}i}^k \Rightarrow b_i = b_1^i \ \forall i \in K$$

Posto $h = b_i \in H$ se K è infinito e $h \neq 1$ allora $b_i \neq 1$ per ogni i il che è assurdo perciò $Z(G) = \{1\}$ mentre se K fosse finito allora segue immediatamente che $Z(G) \leq U$. ■

Capitolo 2

Gruppi abeliani

2.1 Definizioni e risultati preliminari

Dimostriamo prima di tutto il seguente teorema che risulta fondamentale in molti dei risultati che seguiranno.

Teorema 2.1.1. *Sia A gruppo abeliano, allora A è finito se e solo se è finitamente generato e periodico.*

Dimostrazione. Supponiamo $A = \langle a_1, a_2, \ldots, a_n \rangle$ finitamente generato e periodico, dimostriamone la finitezza lavorando per induzione su n.

Se $n = 1$ allora G è ciclico e periodico quindi è necessariamente finito, altrimenti supponiamo l'asserto vero per $n - 1$ e $B = \langle a_1, \ldots, a_{n-1} \rangle$. Il sottogruppo B è quindi finito e inoltre $A = B + \langle a_n \rangle$ essendo gruppi abeliani. L'elemento a_n è periodico per cui $\langle a_n \rangle$ è finito e quindi anche A risulta finito. ■

In un gruppo abeliano A per ogni $n \in \mathbb{Z}$ definiamo

$$A[n] = \{a \in A \mid na = 0\}$$

il quale è ancora un sottogruppo di A per via della proprietà commutativa della somma. Inoltre vale l'uguaglianza

$$|A : A[n]| = |nA|$$

In un gruppo abeliano anche l'insieme $\{a \in A \mid a \text{ periodico } \}$ è un sottogruppo chiamato *sottogruppo di torsione* di A.

Scelto p numero primo definiamo

$$A_p = \{a \in A \mid \exists m \in \mathbb{N} \text{ tale che } p^m a = 0\}$$

chiaramente A_p è un sottogruppo del gruppo abeliano A e quindi è anche l'unico p sottogruppo di Sylow di A.

Definizione 2.1.2. Un gruppo abeliano A è detto *libero* se e solo se $A = \{1\}$ oppure esiste $X \subseteq A$ non vuoto composto interamente da elementi aperiodici tale che

$$A = \operatorname*{Dr}_{a \in X} \langle a \rangle$$

È invece un p-gruppo abeliano elementare se e solo se gli elementi dell'insieme X sono periodici di periodo p primo.

Un risultato immediato da verificare ma molto utile nel seguito è il seguente

Proposizione 2.1.3. *Se A è un gruppo abeliano libero allora per ogni p primo*

$$\bigcap_{n=1}^{+\infty} p^n A = \{0\}$$

Dimostrazione. Possiamo supporre che A sia ciclico, dato che è prodotto diretto di gruppi ciclici. Sia allora $a \in A$ il suo generatore allora per ogni $g \in A$ si avrà $g = ma$ per un certo $m \in \mathbb{N}$. Se fosse $g \in \bigcap_{n=1}^{+\infty} p^n A$ allora $ma = i_n p^n a$ per ogni $n \in \mathbb{N}$ ovvero, essendo ciclico infinito, $m = i_n p^n$ e questo è vero se e solo se $m = i_n = 0$ per n grande e quindi $g = 0$. ■

Proposizione 2.1.4. *Sia A un gruppo abeliano e $f : X \to A$ una funzione definita su un insieme X. Allora esiste F abeliano libero contenente X tale che $F = \bigoplus_{x \in X} \langle x \rangle$ ed esiste un unico omomorfismo $\varphi : F \to A$ tale che $\varphi(x) = f(x)$ per ogni $x \in X$.*

Dimostrazione. A partire da ogni $x \in X$ definiamo il gruppo $G_x = \mathbb{Z}$ e ne facciamo il prodotto esterno $F = \bigoplus_{x \in X} G_x$. Quindi possiamo considerare $x \in X$ anche come elemento di F e quindi $G_x = \langle x \rangle$ ciclico infinito. Quindi possiamo definire, presi qualunque $x_i \in X$ distinti e $n_i \in \mathbb{Z}$.

$$\varphi : n_1 x_1 + n_2 x_2 + \cdots + n_t x_t \in F \to n_1 f(x_1) + n_2 f(x_2) + \cdots + n_t f(x_t) \in A$$

la quale è ben definita per l'unicità della scrittura degli elementi di F tramite somme finite di elementi di X a meno di eventuali termini nella forma $0x_j$ che non influiscono in quanto $0f(x_j) = 0$.

Dimostriamo che φ è un omomorfismo, presi allora $x_1, x_2, \ldots, x_t \in X$ distinti e $m_i, n_i \in \mathbb{Z}$ avremo che

$$\begin{aligned} \varphi\left(\sum_{i=1}^{t} n_i x_i\right) + \varphi\left(\sum_{i=1}^{t} m_i x_i\right) &= \sum_{i=1}^{t} n_i f(x_i) + \sum_{i=1}^{t} m_i f(x_i) \\ &= \sum_{i=1}^{t} (n_i + m_i) f(x_i) = \varphi\left(\sum_{i=1}^{t} (n_i + m_i) x_i\right) \end{aligned}$$

sfruttando l'abelianità di A. ■

Teorema 2.1.5 (decomposizione gruppi abeliani)**.** *Consideriamo un gruppo abeliano A e indichiamo con T il suo sottogruppo di torsione. Allora*

1. *A/T è senza torsione ovvero non ha elementi periodici non identici;*
2. *$T = \mathrm{Dr}_{p\ primo} A_p$.*

Dimostrazione. Dimostriamo i vari punti

1. Sia $a + T \in A/T$ tale che esista $n \in \mathbb{N}$ tale che $n(g + T) = T$ allora $ng \in T$ ed esisterà $m \in \mathbb{N}$ tale che $nmg = 0$, quindi $g \in T$ e $g + T = T$.
2. Chiaramente $A_p \lhd A$, dimostriamo che per ogni numero intero primo p vale $A_p \cap \langle A_q \mid q \neq p \text{ primo}\rangle$.

   Se un elemento u appartenesse all'intersezione allora avrebbe ordine p^n e sarebbe la somma di un numero finito di elementi $u_1, u_2, \ldots, u_t$ dove l'ordine di u_i è $q_i^{n_i}$ con q_i primo diverso da p.

   Definiamo $m = q_1^{n_1} \cdots q_t^{n_t}$ allora sfruttando la commutatività della somma osserviamo che

   $$mu = m\,(u_1 + \cdots + u_t) = mu_1 + mu_2 + \cdots + mu_t = 0 = p^n u$$

   e quindi $u = 0$ in quanto $\gcd(p^n, m) = 1$.

   Dalla proposizione 1.3.3 T è generato dai suoi sottogruppi di Sylow e quindi $T = \langle A_p \mid p \text{ primo}\rangle$ concludendo in tal modo la dimostrazione.

∎

Il p-gruppo di Prüfer

Consideriamo il gruppo quoziente $\mathbb{Q}/\mathbb{Z} = \{a/b + \mathbb{Z} \mid a \in \mathbb{Z} \wedge b \in \mathbb{N}\}$. Tutti gli elementi di $\mathbb{Q}/\mathbb{Z}$ sono periodici quindi dal teorema 2.1.5 possiamo scrivere

$$\mathbb{Q}/\mathbb{Z} = \underset{p \text{ primo}}{\mathrm{Dr}} (\mathbb{Q}/\mathbb{Z})_p$$

Fissiamo un qualunque numero primo p definiamo allora il *p-gruppo di Prüfer* if fattore diretto

$$\mathbb{Z}(p^\infty) = (\mathbb{Q}/\mathbb{Z})_p = \left\{ \frac{r}{p^n} + \mathbb{Z} \;\middle|\; r \in \mathbb{Z} \wedge n \in \mathbb{N}_0 \right\}$$

sempre dal teorema 2.1.5, ogni p-gruppo di Prüfer è isomorfo ad un quoziente di $\mathbb{Q}/\mathbb{Z}$.

Fissiamo un generico p primo e per ogni $i \in \mathbb{N}_0$ definiamo

$$a_i = \frac{1}{p^i} + \mathbb{Z} \in \mathbb{Z}(p^\infty)$$

chiaramente $|\langle a_i\rangle| = p^i$ e $pa_{i+1} = a_i$, perciò dalle proprietà dei gruppi ciclici $\langle a_i\rangle < \langle a_{i+1}\rangle$ e non vi sono altri sottogruppi tra di loro. Se indichiamo con A_i il sottogruppo $\langle a_i\rangle$ allora vale il seguente risultato

Lemma 2.1.6. *Gli unici sottogruppi propri di $\mathbb{Z}(p^\infty)$ sono gli A_i con $i \in \mathbb{N}_0$.*

Dimostrazione. Prendiamo un sottogruppo proprio generico $H < \mathbb{Z}(p^\infty)$, poiché $A_0 = \{\mathbb{Z}\}$ e $\bigcup_{i\in\mathbb{N}_0} A_i = \mathbb{Z}(p^\infty)$ esisterà sicuramente l'indice $j = \min\{i \in \mathbb{N} \mid A_i \nleq H\}$ e $A_{j-1} \leq H$.

Per ogni indice $n \geq j$ avremo perciò $A_{j-1} \leq H \cap A_n \leq A_n$, dall'inverso forte del teorema di Lagrange A_j è l'unico sottogruppo di ordine p^j di A_n, quindi se $H \cap A_n$ avesse sottogruppi di ordine p^j esso sarebbe necessariamente A_j. Ciò andrebbe in contrasto con la definizione di j e perciò, essendo $H \cap A_n$ ciclico, $|H \cap A_n| = p^{j-1}$.

Questo significa che $A_j = H \cap A_n$ per ogni $n \geq j$ ma allora

$$H = H \cap \bigcup_{n=j}^{+\infty} A_n = \bigcup_{n=j}^{+\infty} (H \cap A_n) = A_j$$

■

2.2 Prodotto tensoriale

Adesso consideriamo due gruppi abeliani $(A, +)$ e $(B, +)$, definiamo a partire da essi l'insieme U i cui elementi sono nella forma $\{n_{ab}(a,b)\}_{a\in A, b\in B}$ dove $n_{ab} \in \mathbb{Z}$ ed è diverso da 0 solo per un numero finito di indici $a \in A$ e $b \in B$ altrimenti vale 0.

Possiamo dotare U dell'operazione somma definita in modo tale che

$$\{m_{ab}(a,b)\}_{a\in A,b\in B} + \{n_{ab}(a,b)\}_{a\in A,b\in B} = \{(m_{ab} + n_{ab})(a,b)\}_{a\in A,b\in B}$$

come conseguenza possiamo scrivere

$$\{n_{ab}(a,b)\}_{a\in A,b\in B} = \sum_{i=1}^{t} n_i(a_i, b_i)$$

Questa operazione rende U un gruppo abeliano ma non possiamo ancora definirlo prodotto tensoriale, dobbiamo prendere il seguente sottogruppo di U

$$V = \left\langle (a + a', b) - (a, b) - (a', b), (a, b + b') - (a, b) - (a, b') \right\rangle$$

allora il *prodotto tensoriale* di A e B è il gruppo quoziente

$$A \otimes B = U/V$$

e per ogni $a \in A$ e $b \in B$ poniamo

$$a \otimes b = (a, b) + V \tag{2.2.1}$$

Si noti che la (2.2.1) non esaurisce tutti gli elementi di $A \otimes B$, cioè esisteranno elementi di $A \otimes B$ che non saranno esprimibili nella forma precedente. Tra le proprietà elementari dei prodotti tensoriali figurano le seguenti

Proposizione 2.2.1. *Presi A e B gruppi abeliani allora valgono le seguenti affermazioni*

- $A \otimes B = \langle a \otimes b \mid a \in A, b \in B \rangle$;
- $(a + a') \otimes b = a \otimes b + a' \otimes b$;
- $a \otimes (b + b') = a \otimes b + a \otimes b'$;
- $0 \otimes b = a \otimes 0 = 0$;
- $(na) \otimes b = a \otimes (nb) = n(a \otimes b)$ *per ogni* $n \in \mathbb{Z}$.

Una qualunque funzione $f : A \times B \to C$ con C gruppo abeliano è detta *bilineare* se e solo se $f(a + a', b) = f(a, b) + f(a', b)$ e $f(a, b + b') = f(a, b) + f(a, b')$.

Teorema 2.2.2. *Se A, B e C sono gruppi abeliani e $f : A \times B \to C$ è bilineare allora esiste un unico omomorfismo $g : A \otimes B \to C$ tale che $f(a, b) = g(a \otimes b)$.*

Dimostrazione. Innanzitutto sappiamo che $U = \mathrm{Dr}_{(a,b) \in A \times B} \langle (a, b) \rangle$ e quindi esiste un unico omomorfismo $h : U \to C$ tale che $f(a, b) = h(a, b)$. Dalla bilinearità di f segue quella di h e quindi $V \leq \ker h$.

Allora dal teorema fondamentale degli omomorfismi esiste un unico omomorfismo $g : A \otimes B \to C$ tale che $f(a, b) = g(a \otimes b)$. ∎

Corollario 2.2.3. $A \otimes B \cong B \otimes A$.

Dimostrazione. Basta applicare il teorema precedente alle due applicazioni bilineari

$$f : (a, b) \in A \times B \to b \otimes a \in B \otimes A$$
$$f' : (b, a) \in B \times A \to a \otimes b \in A \otimes B$$

∎

Un altro risultato quasi immediato è il seguente

Proposizione 2.2.4. *Scelti A e B gruppi abeliani allora*

1. *Se A è periodico allora anche $A \otimes B$ è periodico;*
2. *Se A e B sono finitamente generati allora anche $A \otimes B$ è finitamente generato;*
3. *Se A e B sono finiti allora anche $A \otimes B$ è finito.*

Dimostrazione. Dimostriamo i vari punti.

1. Per ogni elemento $a \in A$ esiste $n_a \in \mathbb{N}$ tale che $n_a a = 0$. Quindi consideriamo un generico elemento $\sum_{i=1}^{t} m_i(a_i \otimes b_i)$ di $A \otimes B$ e poniamo $n = \prod_{i=1}^{t} n_{a_i}$ allora

$$n \sum_{i=1}^{t} m_i(a_i \otimes b_i) = \sum_{i=1}^{t} m_i \frac{n}{n_{a_i}} n_{a_i}(a_i \otimes b_i) = 0$$

2. Se $A = \langle a_1, a_2, \ldots, a_m \rangle$ e $B = \langle b_1, b_2, \ldots, b_n \rangle$ allora per ogni $a \in A$ esistono $s_1, s_2, \ldots, s_m \in \mathbb{Z}$ tali che $a = \sum_{i=1}^{m} s_i a_i$, analogamente mostriamo che $b = \sum_{i=1}^{n} t_i b_i$ per $t_i \in \mathbb{Z}$. Ma allora
$$a \otimes b = \sum_{i,j} s_i t_j (a_i \otimes b_j)$$
e quindi $A \otimes B$ è finitamente generato.

3. Segue banalmente dalle due ipotesi precedenti e dal teorema 2.1.1.

■

2.3 Gruppi divisibili

Definizione 2.3.1. Sia A gruppo abeliano, un elemento $a \in A$ è detto *m-divisibile*, con $m \in \mathbb{N}$ oppure $m \in \mathbb{Z} \setminus \{0\}$, se e solo se esiste $a' \in a$ tale che $a = ma'$, il gruppo A è detto *m-divisibile* se e solo se è composto interamente da elementi m-divisibili, in altre parole $A = mA$ per ogni $m \in \mathbb{N}$.

A è *divisibile* se $A = mA$ per ogni $m \in \mathbb{N}$.

È immediato constatare che il gruppo dei numeri razionali $(\mathbb{Q}, +)$ è un gruppo divisibile.

Osservazione. L'unico gruppo divisibile e periodico è il gruppo banale $\{0\}$.

Proposizione 2.3.2. *A è divisibile se e solo se è p-divisibile per ogni p primo.*

Dimostrazione. Sia A sia p-divisibile per ogni p primo, dimostriamo che $A = mA$ per ogni $m \in \mathbb{N}$. Se $m = 1$ è chiaramente verificato altrimenti supponiamo $A = nA$ per ogni $n < m$. Se m è primo allora segue dalle ipotesi altrimenti esisteranno un intero n ed un primo p tali che $m = np$ e quindi
$$mA = n(pA) = nA = A$$
■

Proposizione 2.3.3. *Se A è divisibile allora A/B è divisibile per ogni $B \leq A$. La divisibilità è quindi chiusa per quozienti.*

Dimostrazione. Per ogni $m \in \mathbb{N}$ e $a + B \in A/B$ esisterà $a' \in A$ tale che $a = ma'$ e quindi $a + B = ma' + B = m(a' + B)$. ■

Corollario 2.3.4. *I p-gruppi di Prüfer $\mathbb{Z}(p^\infty)$ sono sempre divisibili.*

Dimostrazione. Per la proposizione precedente $\mathbb{Q}/\mathbb{Z}$ è divisibile e periodico, quindi dal teorema di decomposizione dei gruppi abeliani anche $\mathbb{Z}(p^\infty) = (\mathbb{Q}/\mathbb{Z})_p$ è ancora un quoziente di $\mathbb{Q}/\mathbb{Z}$ e quindi è divisibile. ■

Proposizione 2.3.5. *Sia G gruppo abeliano ed $N \leq G$, supponiamo che sia N che G/N siano divisibili allora anche G è divisibile*

Dimostrazione. Prendiamo $g \in G$ ed $n \in \mathbb{N}$, esisterà allora $g' \in G$ tale che $g + N = n\,(g' + N) = ng' + N$. Allora $ng = ng' + u$ con $u \in N$ il quale essendo divisibile garantisce l'esistenza di $v \in N$ tale che $u = nv$ e quindi

$$ng = ng' + u = ng' + nv = n(g + v)$$

■

Osservazione. In generale i sottogruppi di un gruppo divisibile non è chiuso per sottogruppi. Basta prendere $\mathbb{Q}$ che è chiaramente divisibile mentre $\mathbb{Z} \leq \mathbb{Q}$ non lo è.

Definizione 2.3.6. Un gruppo abeliano G è detto *iniettivo* se e solo se per ogni coppia di gruppi abeliani H, K se esistono $\phi : H \to G$ omomorfismo e $i : H \to K$ monomorfismo allora esiste un omomorfismo $\varphi : K \to G$ tale che $\phi = \varphi \circ i$.

Il seguente grafico permette di visualizzare bene la definizione di gruppo iniettivo

$$\begin{tikzcd} H \arrow[r, "i"] \arrow[d, "\phi"] & K \arrow[dl, dashed, "\varphi"] \\ G & \end{tikzcd}$$

Proposizione 2.3.7. *Un gruppo abeliano G è iniettivo se e solo se per ogni K gruppo abeliano e $H \leq K$ e per ogni $\phi : H \to G$ allora esiste $\varphi : H \to G$ tale che $\varphi(x) = \phi(x)$ per ogni $x \in H$.*

Dimostrazione. Esercizio. ■

Teorema 2.3.8. *Un gruppo abeliano G è iniettivo se e solo se è divisibile.*

Dimostrazione. Supponiamo G iniettivo, allora per ogni $m \in \mathbb{Z}$ possiamo costruire l'applicazione

$$\psi_m : mk \in m\mathbb{Z} \to kg \in G$$

Ora $m\mathbb{Z} \leq \mathbb{Q}$ e per la proposizione precedente esiste $\eta_m : \mathbb{Q} \to G$ tale che $\eta_m(mk) = kg$ per ogni $k \in \mathbb{Z}$. Sia $h = \eta_m(1)$ allora $mh = \eta_m(m) = g$ e perciò G è divisibile.

L'implicazione opposta è più complessa da dimostrare, per questo procederemo per gradi. Prendiamo G gruppo divisibile, K gruppo abeliano generico con $H \leq K$ un suo sottogruppo. Consideriamo anche un omomorfismo $\alpha : H \to G$, dimostrare il teorema equivale a trovare un omomorfismo $\beta : K \to G$ che estende α.

Definiamo allora la classe di omomorfismi

$$\mathcal{L} = \{\phi : L \to G \mid \phi \text{ omomorfismo } \wedge H \leq L \leq K \wedge \phi|_H = \alpha\}$$

chiaramente $\alpha \in \mathcal{L}$ e quindi non è vuoto. Definiamo su $\mathcal{L}$ la relazione d'ordine: Se $\phi, \varphi \in \mathcal{L}$ allora

$$\phi \precsim \varphi \Leftrightarrow \operatorname{dom}\phi \leq \operatorname{dom}\varphi \wedge \varphi|_{\operatorname{dom}\phi} = \phi$$

dove $\operatorname{dom}\phi$ è il dominio della funzione ϕ.

- Dimostriamo che $\mathcal{L}$ è induttivo. Preso infatti un sottoinsieme $\mathcal{U}$ di $\mathcal{L}$ totalmente ordinato vogliamo dimostrare che $\mathcal{U}$ abbia un maggiorante.

  Innanzitutto dimostriamo che l'insieme

  $$U = \bigcup_{\phi \in \mathcal{U}} \operatorname{dom}\phi$$

  è effettivamente un sottogruppo di K. Difatti per ogni $x, y \in U$ esistono $\phi, \varphi \in \mathcal{U}$ tali che $x \in \operatorname{dom}\phi$ e $y \in \operatorname{dom}\varphi$, poiché $\mathcal{U}$ è totalmente ordinato possiamo supporre che $\operatorname{dom}\phi \leq \operatorname{dom}\varphi$ e perciò $x^{-1}y \in \operatorname{dom}\varphi \subseteq U$.

  Osserviamo inoltre che $\phi(x) = \varphi(y)$ e quindi la funzione $\epsilon : U \to G$ tale che $\epsilon(x) = \phi(x)$ se $x \in \operatorname{dom}\phi$ è ben definita ed è anche un omomorfismo. Dimostriamo che $\epsilon \in \mathcal{L}$, chiaramente $H \leq U$ e per ogni $x \in H$ abbiamo $\epsilon(x) = \phi(x) = \alpha(x)$. Quindi $\epsilon \in \mathcal{L}$ ed è un maggiorante di $\mathcal{U}$ ed $\mathcal{L}$ è induttivo.

- Dal lemma di Zorn $\mathcal{L}$ possiede un elemento massimale $\eta : L \to G$ dove $H \leq L \leq K$ e $\eta|_H = \alpha$. Possiamo supporre per assurdo che $L < K$ e quindi esisterà un $x \in K \backslash L$ generico, vogliamo sfruttarlo per costruire un'estensione di η su $\langle L, x\rangle$.

  Se $L \cap \langle x\rangle = \{0\}$ allora $\langle L, x\rangle = L \oplus \langle x\rangle$ e quindi possiamo costruire l'estensione nel seguente modo

  $$\tilde{\eta} : y + nx \in L \oplus \langle x\rangle \to \eta(y) \in G$$

  contraddicendo la massimalità di η.

- Supponiamo ora che $L \cap \langle x\rangle \neq \{0\}$, poniamo perciò $m = \min\{n \in \mathbb{N} \mid nx \in L\} > 0$, osserviamo che per ogni $g \in \langle L, x\rangle$ esistono e sono determinati univocamente $y \in L$ e $n \in \{0, 1, \ldots, m-1\}$ tali che $g = y + nx$. Difatti se non fossero univoci esisterebbero $y' \in L$ ed $0 \leq n' \leq n < m$ tali che $y + nx = y' + n'x$.

  Ma allora $y' - y = (n - n')x \in L \cap \langle x\rangle$ ma $n - n' < m \Rightarrow n = n'$ e quindi $y = y'$ garantendone l'unicità. Grazie alla divisibilità di G esiste $z \in G$ tale che

  $$\eta(mx) = mz$$

  Siamo ora in grado di costruire la nostra estensione di η, se $0 \leq n < m$ definiamo

  $$\tilde{\eta} : y + nx \in \langle L, x\rangle \to \eta(y) + nz \in G$$

  dobbiamo dimostrare solamente che $\tilde{\eta}$ sia un omomorfismo. Ricordiamo dall'aritmetica che per ogni $n, n' \in \mathbb{Z}$ esistono e sono unici $l \in \mathbb{Z}$ ed $r_{x+y} \in \{0, 1, \ldots, m-1\}$ tali che

  $$n + n' = lm + r_{x+y}$$

Perciò per ogni $y, y' \in L$ ed n, n' interi non negativi minori di m

$$\begin{aligned}\tilde{\eta}(y+nx)+\tilde{\eta}(y'+n'x) &= \eta(y)+\eta(y')+(n+n')z \\ &= \eta(y)+\eta(y')+lmz+r_{n+n'}z \\ &= \eta(y+y'+lmx)+r_{n+n'}z \\ &= \tilde{\eta}\left(y+y'+lmx+r_{n+n'}x\right) \\ &= \tilde{\eta}\left(y+nx+y'+n'x\right)\end{aligned}$$

quindi $\tilde{\eta}$ è un omomorfismo e quindi è una estensione di η il che è assurdo.

■

Osservazione. Un gruppo iniettivo/divisibile permette di *estendere il domonio di un omomorfismo tramite una funzione iniettiva.*

Da questo teorema discende immediatamente il seguente notevole risultato.

Teorema 2.3.9 (Baer). *Sia G gruppo abeliano e $D \leq G$ divisibile, allora esiste $L \leq G$ tale che*

$$G = D \oplus L$$

In altre parole ogni sottogruppo divisibile di un gruppo abeliano possiede il complementare algebrico.

Dimostrazione. Sappiamo già che D è iniettivo, esisterà allora un epimorfismo $f : G \to D$ tale che $f(x) = x$ per ogni $x \in D$. Poniamo $L = \ker f$ e osserviamo che per ogni $g \in G$

$$f\left(g - f(g)\right) = f(g) - f(g) = 0$$

e quindi $g = f(g) + g - f(g) \in D \oplus L$ per ogni $g \in G$ in quanto se $g \in D \cap L$ allora $g = f(g) = 0$. ■

Corollario 2.3.10. *Se G è abeliano e $D \leq G$ divisibile allora esiste $L \leq G$ tale che $D \cong G/L$.*

Definizione 2.3.11. Un gruppo R è *ridotto* se e solo se l'unico suo sottogruppo divisibile è il sottogruppo banale $\{0\}$.

Proposizione 2.3.12. *Per ogni G gruppo abeliano esistono $D \leq G$ divisibile e $R \leq G$ ridotto tali che $G = D \oplus R$.*

Dimostrazione. Basta porre

$$D = \langle D_i \leq G \mid D_i \text{ divisibile}\rangle$$

difatti D è ancora divisibile: per ogni $g \in D$ esistono e sono unici $g_i \in D_i$, di cui solo un numero finito di essi è diverso da 0, tali che $g = \sum_i g_i$. Per ogni $m \in \mathbb{N}$ esisteranno $h_i \in D_i$ tali che $g_i = mh_i$ e per l'abelianità di G

$$g = \sum_i (mh_i) = m \sum_i h_i = mh$$

con $h \in D$. La tesi segue allora dal teorema di Baer. ■

Prima di enunciare il teorema di struttura dei gruppi divisibili dimostriamo il seguente lemma

Lemma 2.3.13. *Se G è un gruppo abeliano di esponente p allora $G = \bigoplus_{i\in I} G_i$ dove G_i è un gruppo ciclico di ordine p.*

Dimostrazione. Basta osservare che l'applicazione

$$f : ([r]_p, g) \in \mathbb{Z}_p \times G \to rg \in G$$

è ben definita e funge da prodotto esterno su G che quindi può essere visto come uno spazio vettoriale e perciò esiste una base $\Lambda \subseteq G$ ovvero $G = \bigoplus_{x\in\Lambda} \langle x\rangle$ con $|\langle x\rangle| = p$. ■

Teorema 2.3.14 (Struttura dei gruppi divisibili)**.** *Sia G gruppo abeliano divisibile, allora esistono $\{G_i\}_{i\in I}$, dove $G_i \cong \mathbb{Q}$ oppure $G_i \cong \mathbb{Z}(p_i{}^\infty)$ per un opportuno p_i primo, tali che*

$$G = \bigoplus_{i\in I} G_i$$

Dimostrazione. Prendiamo il sottogruppo di torsione T di G, dobbiamo dimostrare che T è divisibile. Difatti preso $g \in T$ chiaramente esisterà $n \in \mathbb{N}$ affinché $ng = 0$, per la divisibilità di G per ogni $m \in \mathbb{N}$ avremo $h \in G$ tale che $g = mh$. Quindi $nmh = ng = 0$ e $h \in T$ quindi T è divisibile.

Dal teorema 2.3.9 esisterà $L \leq G$ tale che $G = L \oplus T$ e quindi L è senza torsione e divisibile in quanto $L \cong G/T$. Ancora $T = \bigoplus_{p \text{ primo}} G_p$ e tutti i p-sottogruppi di Sylow G_p sono dunque divisibili, ci basterà perciò dimostrare il teorema nel caso in cui G sia senza torsione oppure un p-gruppo.

- Supponiamo che G sia senza torsione, prendiamo $x, y \in G$ e $n \in \mathbb{N}$ tali che $nx = ny$, allora $n(x - y) = 0 \Rightarrow x = y$.

  Possiamo perciò definire per ogni $n \in \mathbb{N}$ e $g \in G$ l'elemento $\frac{1}{n}g$ di G come l'unico elemento tale che $n\frac{1}{n}g = g$. Vogliamo definire su G un prodotto esterno rispetto a $\mathbb{Q}$ da cui seguirebbe immediatamente l'asserto. Per questo motivo prendiamo $m, m' \in \mathbb{Z}$ e $n, n' \in \mathbb{N}$ tali che $mn' = m'n$ allora

  $$nn'm\left(\frac{1}{n}g\right) = mn'g = m'ng = nn'm'\left(\frac{1}{n'}g\right)$$

  e quindi sfruttando ancora una volta l'aperiodicità di G

  $$m\left(\frac{1}{n}g\right) = m'\left(\frac{1}{n'}g\right) \tag{2.3.1}$$

  Dalla (2.3.1) possiamo dedurre facilmente che l'applicazione

  $$k : \left(\frac{m}{n}, g\right) \in \mathbb{Q} \times G \to m\left(\frac{1}{n}g\right) \in G$$

  è ben definita e induce un prodotto esterno rispetto a $\mathbb{Q}$, quindi esisterà $\Lambda \subseteq G$ tale che $G = \bigoplus_{x\in\Lambda} \langle x\rangle$ e $\langle x\rangle \cong \mathbb{Q}$.

- Supponiamo adesso che G è un p-gruppo, dal lemma 2.3.13 esistono $x_i \in G[p]$ per ogni $i \in I$ tali che $|\langle x_i \rangle| = p$ e $G[p] = \bigoplus_{i\in I} \langle x_i \rangle$.

  Ricordiamo che per ogni p gruppo di Prüfer il sottogruppo $(\mathbb{Z}(p^\infty))$ è un gruppo ciclico di ordine p. Possiamo perciò porre per ogni $i \in I$ $P_i \cong \mathbb{Z}(p^\infty)$ e $P = \bigoplus_{i\in I} P_i$, quindi anche $P[p]$ sarà prodotto diretto di I gruppi ciclici di ordine p, avremo perciò un isomorfismo ψ tra $G[p]$ e $P[p]$. Dobbiamo costruire un isomorfismo tra G e P per concludere la dimostrazione.

  Per maggiore chiarezza riportiamo tutti questi omomorfismi su di un grafico

$$
\begin{tikzcd}
G[p] \arrow[r, hook, "i_1"] & G \\
P[p] \arrow[u, "\psi"] \arrow[ur, "\alpha"] \arrow[r, hook, "i_2"] & P \arrow[u, dashed, "\beta"']
\end{tikzcd}
$$

  Poiché $\psi : P[p] \to G[p]$ è un isomorfismo allora $\alpha = i_1 \circ \psi$ è un omomorfismo da $P[p]$ in $G[p]$ e per la divisibilità di G esisterà un omomorfismo $\beta : P \to G$ tale che $\beta(g) = \psi(g)$ per ogni $g \in P[p]$. Dimostriamo che P è un isomorfismo.

  Supponiamo che esista un $x \in \ker\beta \setminus \{0\}$ allora esisterà $k \in \mathbb{N}$ tale che $|\langle x \rangle| = p^k$ e perciò $p^{k-1}x \in P[p]$. Allora

$$0 = \beta\left(p^{k-1}x\right) = \phi\left(p^{k-1}\right) \Rightarrow 0 = p^{k-1}x$$

  il che è assurdo quindi β è iniettiva in P.

  Chiaramente $\beta(P) \cong P$ è un sottogruppo divisibile e dal teorema di Baer esiste $L \leq G$ tale che $G = \beta(P) \oplus L$. Ora $G[p] = \beta(P[p])$ e quindi $L \cap G[p] = \{0\}$, se esistesse $x \in L \setminus \{0\}$ allora $|\langle x \rangle| = p^k$ e $p^{k-1}x \in G[p] \cap L$ e quindi $p^{k-1}x = 0$ assurdo.

  Quindi G è isomorfo a P e il teorema è così dimostrato.

■

2.4 Sottogruppi puri

Definizione 2.4.1. Sia G un gruppo abeliano e $H \leq G$, diciamo che H è *puro* in G se e solo se per ogni $n \in \mathbb{N}$ vale l'uguaglianza

$$nH = nG \cap H$$

Dato che l'inclusione $\subseteq$ è banale allora H è puro se e solo se per ogni $n \in \mathbb{N}$ e $g \in G$ allora se l'elemento ng appartiene ad H deve esistere un $h \in H$ tale che $ng = nh$.

I fattori diretti di G sono sempre sottogruppi puri, infatti se $G = L \oplus H$ sfruttando l'identità di Dedekind

$$nG \cap H = (nL \oplus nH) \cap H = (nL \cap H) \oplus nH = nH$$

Proposizione 2.4.2. *Il gruppo di torsione di un gruppo abeliano è puro.*

Dimostrazione. Se T è il sottogruppo di torsione allora G/T è senza torsione. Sia allora $g \in G$ tale che $ng \in T$ allora

$$T = ng + T = n\,(g + T) \Rightarrow T = g + T \Rightarrow g \in T$$

■

Abbiamo già visto che i sottogruppi di gruppi divisibili possono non essere divisibili. Se però il sottogruppo è anche puro allora sarà esso stesso divisibile. Difatti vale il seguente risultato

Proposizione 2.4.3. *Se G è divisibile e $H \leq G$ è puro allora anche H è divisibile.*

Dimostrazione. La tesi segue immediatamente dalla definizione di purezza, difatti per ogni $n \in \mathbb{N}$

$$nH = nG \cap H = G \cap H = H$$

■

Proposizione 2.4.4. *Sia G abeliano ed $N \leq H \leq G$. Allora*

1. *Se H è puro in G allora H/N è puro in G/N;*

2. *Se N è puro in G e H/N è puro in G/N allora anche H è puro in G.*

Dimostrazione. Dimostriamo i vari punti

1. Fissiamo $n \in N$ e $g \in G$ tale che $ng + N \in H/N$. Allora $ng \in H$ e $ng = nh$ per un opportuno $h \in H$ e quindi $ng + N = nh + N$.

2. Sia $g \in G$ tale che $ng \in H$ allora $ng + N \in H/N$ ed avremo un $h \in H$ tale che $ng + N = nh + N$ ovvero $n(g - h) \in N$. Per la purezza di N esisterà $u \in N$ tale che $n(g - h) = nu \Rightarrow ng = n(h + u) \in nH$.

■

Lemma 2.4.5. *Sia G un p-gruppo e $H \leq G$ allora H è puro in G se e solo se per ogni $m \in \mathbb{N}_0$*

$$p^m H = p^m G \cap H$$

Dimostrazione. Sia $n \in \mathbb{N}$ generico, supponiamo inizialmente che p non divide n. Questo significa che $\langle nx \rangle = \langle x \rangle$ per ogni $x \in G$ e quindi $G = nG$ e $H = nH$.

Se invece p divide n allora esisterà un $k \in \mathbb{N}$ ed un $m \in \mathbb{N}$ tali che $n = p^k m$ ed m non è divisibile per p. Quindi per quanto detto prima

$$nH = p^k (mH) = p^k H = p^k G \cap H = nG \cap H$$

■

Definizione 2.4.6. Sia G un gruppo abeliano e $g \in G$. Diciamo che g ha *p-altezza infinita* se e solo se $g \in p^k G$ per ogni $k \in \mathbb{N}_0$, altrimenti la quantità

$$\max \{n \in \mathbb{N} \mid g \in p^n G\}$$

è detta *p-altezza* di g.

Osservazione. Se G è un p-gruppo e $q \neq p$ è primo allora $qG = G$ ed ogni suo elemento ha q-altezza infinita. Per questo in un p-gruppo ha senso considerare solamente la p-altezza e non le altre, quindi verrà indicata semplicemente come altezza di un elemento.

Chiaramente un gruppo è divisibile se e solo se ogni suo elemento ha p altezza infinita per ogni primo p. Per i p-gruppi vale un risultato più forte

Proposizione 2.4.7. *Se G è un p-gruppo abeliano allora è divisibile se e solo se ogni elemento di $G[p]$ ha altezza infinita.*

Dimostrazione. Per assurdo G non è divisibile, allora $pG < G$ ed esiste $g \in G \setminus pG$ di ordine *minimo*. Se $|\langle g \rangle| = p^k$ allora $p^{k-1} g \in G[p]$ e quindi ha altezza infinita, in particolare $p^{k-1} g \in p^k G$ ed esisterà $h \in G$ tale che $p^{k-1}(g - ph) = 0$.

Ora il periodo di g era il minimo possibile e quindi $g - ph \in pG$ da cui seguirebbe che $g \in pG$ assurdo. ■

Proposizione 2.4.8. *Sia G un p-gruppo abeliano non divisibile, allora esiste un sottogruppo non banale $H \leq G$ puro e ciclico.*

Dimostrazione. Poiché G non è divisibile dalla proposizione precedente possiederà un elemento in $G[p]$ di altezza finita. Esistono allora $g \in G[p]$ e $i \in \mathbb{N}$ tali che $g \in p^i G \setminus p^{i+1} G$, e sia $h \in G$ tale che $g = p^i h$. Definiamo

$$H = \langle h \rangle$$

vogliamo dimostrare che H è puro, se non lo fosse possiamo rendere $n \in \mathbb{N}$ il più piccolo intero tale che $p^n G \cap H > p^n H$. Quindi $p^{n-1} G \cap \langle h \rangle = \langle p^{n-1} h \rangle$ e perciò

$$\langle p^n h \rangle < p^n G \cap \langle h \rangle \leq p^{n-1} G \cap \langle h \rangle = \langle p^{n-1} h \rangle$$

dall'inverso forte del teorema di Lagrange per i gruppi cilici si ha $p^n G \cap \langle h \rangle = \langle p^{n-1} h \rangle$.

Ora $0 = pg = p^{i+1}h$ e poiché $p^{n-1}h \neq 0$ (altrimenti non varrebbe l'inclusione stretta) allora $n-1 < i+1$ ovvero $i \geq n-1$. Possiamo quindi scrivere

$$g = p^i h = p^{i-n+1}p^{n-1}h \in \langle p^{n-1}h \rangle$$

ma allora $p^{n-1}h \notin p^n G$ altrimenti g apparterrebbe a $p^{i+1}G$, quindi $p^n G \cap \langle h \rangle$ non coinciderebbe con $\langle p^{n-1}h \rangle$ raggiungendo una contraddizione. ■

Definizione 2.4.9. Se G è abeliano periodico un suo sottogruppo B è *basico* se e solo se

- B è puro in G;
- B è somma diretta di gruppi ciclici;
- G/B è divisibile.

Teorema 2.4.10 (Mulikov). *Ogni gruppo abeliano periodico possiede sottogruppi basici.*

Dimostrazione. Sappiamo già dal teorema 2.1.5 che $G = \bigoplus_{p \text{ primo}} G_p$, supponiamo inizialmente di aver dimostrato il teorema per i p-gruppi. Esisteranno allora $H_p \leq G_p$ basici rispetto a G_p, poniamo allora $H = \bigoplus_{p \text{ primo}} H_p$ innanzitutto H è ancora prodotto diretto di gruppi ciclici e inoltre

$$\frac{G}{\bigoplus_{p \text{ primo}} H_p} \cong \bigoplus_{p \text{ primo}} G_p/H_p$$

il secondo e il terzo punto sono così verificati. Per dimostrare che H è anche puro osserviamo che per ogni $n \in \mathbb{N}$

$$nG \cap H = \bigoplus_{p \text{ primo}} (nG_g \cap H_p) = nH$$

Possiamo quindi porre senza perdere in generalità che G sia un p-gruppo. Se G fosse divisibile allora $B = \{0\}$ ne è un sottogruppo basico altrimenti dalla proposizione 2.4.8 esisterà un sottogruppo $H \leq G$ puro e ciclico. Perciò la classe

$$\mathcal{F} = \left\{ \Lambda \subseteq G \;\middle|\; \langle \Lambda \rangle = \bigoplus_{x \in \Lambda} \langle x \rangle \wedge \langle \Lambda \rangle \text{ è puro in } G \right\}$$

è non vuota. Con un procedimento analogo utilizzato nella dimostrazione del teorema 2.3.8 si fa vedere che $\mathcal{F}$ è induttivo e quindi dal lemma di Zorn possiede un elemento massimale $Y \in \mathcal{F}$ e $B = \langle Y \rangle$.

Verifichiamo che G/B è divisibile. Se non lo fosse sempre dalla proposizione 2.4.8 esisterà $g \in G \setminus B$ tale che $\langle g + B \rangle$ è puro. Posto $|\langle g + B \rangle| = p^i$ avremo che $|\langle g \rangle| \geq p^i$ e $p^i g \in B$ il quale, essendo puro, garantisce l'esistenza di $b \in B$ tale che $p^i g = p^i b$. Posto

$$g' = g - b$$

avremo $g + B = g' + B$ e $\langle g' \rangle = p^i$. Ma allora

$$ng' \in B \Rightarrow n\left(g' + B\right) = n\left(g + B\right) = B \Rightarrow ng' = mp^i g' = 0 \Rightarrow B \cap \left\langle g' \right\rangle = \{0\}$$

e quindi $\langle Y, g' \rangle = B \oplus \langle g' \rangle$. Infine poiché $\langle Y, g' \rangle / B = \langle g + B \rangle$ è puro in G/B dalla proposizione 2.4.4 segue che $\langle Y, g' \rangle$ è puro in contraddizione con la massimalità di Y dato che $g' \notin Y$.

Quindi G/B è basico e il teorema è dimostrato. ∎

Teorema 2.4.11 (Prüfer-Baer). *Se G è un gruppo abeliano di esponente finito allora è somma diretta di gruppi ciclici con ordine una potenza di primi.*

L'ordine di questi sottogruppi sarà sempre minore o uguale all'esponente del gruppo.

Si ricordi che G ha esponente finito se e solo se esiste $n \in \mathbb{N}$ tale che $nG = \{0\}$. Il più piccolo di tali n è detto esponente di G.

Dimostrazione. Sia $m \in \mathbb{N}$ l'esponente di G, dal teorema di Mulikov esiste $B \leq G$ basico ma allora

$$\{B\} = mG/B = G/B$$

e quindi $G = B$ ed esiste $\Lambda \subseteq G$ tale che $G = \bigoplus_{x \in \Lambda} \langle x \rangle$.

Dalla dimostrazione del teorema di Mulikov ogni $x \in \Lambda$ appartiene ad un opportuno p-sottogruppo di G per cui il suo ordine è necessariamente nella forma p^n con p primo e $n \in \mathbb{N}$. Osserviamo che $mx = 0$ e perciò $p^n = \langle x \rangle$ deve dividere m da cui segue che $p^n \leq m$. ∎

Da questo risultato segue immediatamente il teorema

Teorema 2.4.12 (Frobenus-Stickelburger). *Se G è un gruppo abeliano finito allora è somma diretta di un numero finito di gruppi ciclici di ordine potenza di primo.*

2.5 Gruppi proiettivi

Teorema 2.5.1. *Se G è un gruppo abeliano allora esiste un gruppo abeliano libero F e un suo sottogruppo H tali che*

$$G \cong F/H$$

Dimostrazione. Se prendiamo un generico insieme Λ equipotente a G possiamo sempre costruire un gruppo abeliano libero F generato da Λ ovvero

$$F = \bigoplus_{x \in \Lambda} \langle x \rangle$$

Se $\psi : \Lambda \to G$ è biiettiva allora possiamo costruire un epimorfismo $f : F \to G$ in modo tale che $f(x) = \psi(x)$ per ogni $x \in \Lambda$ e quindi $G \cong F/\ker f$. ∎

Teorema 2.5.2. *Per ogni G abeliano esiste un gruppo D divisibile ed $H \leq D$ tale che $G \cong H$.*

Dimostrazione. Da teorema precedente sappiamo che esiste F abeliano libero e $N \leq F$ tali che $G \cong F/N$. Ora $F = \bigoplus_{x\in\Lambda} \langle x \rangle$ con $\Lambda \subseteq F$ e poniamo per ogni $x \in \Lambda$ $Q_x \cong \mathbb{Q}$ ed $A = \bigoplus_{x\in\Lambda} Q_x$.

Ora sappiamo che A è divisibile, prendiamo perciò $a_x \in Q_x \setminus \{0\}$ e $B = \bigoplus_{x\in\Lambda} \langle a_x \rangle \leq A$, poiché $|\langle a_x \rangle| = +\infty$ possiamo sempre trovare un isomorfismo $\psi : F \to B$ tale che $\psi(x) = a_x$ se $x \in \Lambda$ e quindi

$$G \cong F/N \cong B/\psi(N) \leq A/\psi(N)$$

Il teorema è così dimostrato per $D = A/\psi(N)$ e $H = B/\psi(N)$. ■

Teorema 2.5.3. *Se F è abeliano libero sul sottoinsieme X e $H \leq F$ allora Y è abeliano libero su un suo sottoinsieme Y tale che $|Y| \leq |X|$.*

Dimostrazione. Omessa. ■

Definizione 2.5.4. Un gruppo abeliano G è *proiettivo* se e solo se per ogni coppia di gruppi abeliani H, K se esistono $\phi : G \to K$ omomorfismo e $s : H \to K$ epimorfismo allora esiste un omomorfismo $\varphi : G \to H$ tale che $\phi = s \circ \varphi$.

Il seguente grafico permette di visualizzare bene la definizione di gruppo proiettivo

$$\begin{tikzcd}
G \arrow[d, "\phi"] \arrow[dr, dashed, "\varphi"] & \\
K & H \arrow[l, "s"]
\end{tikzcd}$$

Come per i gruppi iniettivi dimostriamo anche per i gruppi proiettivi un risultato di equivalenza

Teorema 2.5.5. *Un gruppo è proiettivo se e solo se è abeliano libero.*

Dimostrazione. Supponiamo inizialmente che G sia proiettivo. Dal teorema 2.5.1 esistono F abeliano libero, $H \leq F$ tali che $G \cong F/H$ che induce un epimorfismo $s : F \to G$.

Poiché G è proiettivo esisterà un omomorfismo $f : G \to F$ tale che per ogni $g \in G$ si avrà

$$g = s[f(g)]$$

e in particolare f è un monomorfismo. Quindi $G \cong f(G) \leq F$ e dal teorema 2.5.3 segue che anche G è abeliano libero.

Viceversa se G è abeliano libero siano H, K gruppi generici ed $\phi : G \to K$ omomorfismo e $s : H \to K$ epimorfismo. Allora $G = \bigoplus_{x\in\Lambda} \langle x \rangle$ e per la suriettività di s per ogni $x \in \Lambda$ esisterà $h_x \in H$ tale che

$$\phi(x) = s(h_x)$$

Quindi possiamo sempre costruire un omomorfismo $\varphi : G \to H$ tale che per ogni $x \in \Lambda$

$$\varphi(x) = h_x$$

e quindi G è proiettivo. ■

Proposizione 2.5.6. *Sia G gruppo abeliano e $H \leq G$ tale che G/H è abeliano libero, allora G/H è addendo diretto di G ovvero esiste $L \leq G$ tale che $G = L \oplus H$ e $L \cong G/H$.*

Dimostrazione. Consideriamo l'epimorfismo canonico $\pi : G \to G/H$, esisterà un monomorfismo $\alpha : G/H \to G$ tale che per ogni $g \in G$

$$\alpha(g+H) + H = g + H \Leftrightarrow \alpha(g+H) - g \in H$$

e quindi $G = \alpha(G/H) + H$, dimostriamo ora che $H \cap \alpha(G/H) = \{0\}$.

Preso $h \in H \cap \alpha(G/H)$ esisterà un elemento $g \in G$ tale che $h = \alpha(g+H)$ e perciò

$$H = h + H = \alpha(g+H) + H = g + H \Rightarrow g \in H \Rightarrow h = \alpha(H) = 0$$

e allora $G = \alpha(G/H) \oplus H$. ∎

I gruppi divisibili e proiettivi soddisfano proprietà speculari, che qui elencheremo brevemente per maggior chiarezza.

1. I gruppi divisibili permettono di estendere il dominio di un omomorfismo mediante un monomorfismo, mentre quelli proiettivi estendono il codominio tramite un epimorfismo;

2. I sottogruppi divisibili e i quozienti proiettivi sono sempre addendi diretti del gruppo principale;

3. Un gruppo divisibile è somma diretta di gruppi isomorfi a $\mathbb{Q}$ o $\mathbb{Z}(p^\infty)$, mentre un gruppo divisibile è somma diretta di gruppi ciclici infiniti;

4. La classe dei gruppi divisibili è chiusa per quozienti ma non per sottogruppi, quella dei gruppi proiettivi è chiusa per sottogruppi ma non per quozienti;

5. Ogni gruppo è isomorfo ad un sottogruppo di un gruppo divisibile e ad un quoziente di un gruppo proiettivo.

Capitolo 3

Serie di gruppi

3.1 Condizione minimale e massimale

Innanzitutto dimostriamo il seguente risultato di teoria degli insiemi:

Proposizione 3.1.1. *Consideriamo un insieme ordinato* $(S, \preceq)$ *e le seguenti affermazioni*

1. *Ogni* $T \subseteq S$ *non vuoto possiede elementi massimali;*
2. *Per ogni successione crescente* $x_n \in S$ *esiste* $N \in \mathbb{N}$ *tale che per ogni* $n > N$ *si ha* $x_n = x_N$*;*
3. *Ogni* $T \subseteq S$ *non vuoto possiede elementi minimali;*
4. *Per ogni successione decrescente* $x_n \in S$ *esiste* $N \in \mathbb{N}$ *tale che per ogni* $n > N$ *si ha* $x_n = x_N$*.*

allora la 1 e la 2 sono equivalenti, come lo sono anche la 3 e la 4.

Dimostrazione. Diamo per buona la 1, quindi l'insieme $T = \{x_n \mid n \in \mathbb{N}\}$ possiederà un elemento massimale x_N. Dato che $x_N \leq x_n$ per ogni $n \geq N$ segue immediatamente l'ipotesi 2 per via della massimalità.

Per assurdo ora supponiamo che valga la 2 ma non la 1 per un particolare insieme $T \subseteq S$. Poiché T è non vuoto possiamo sempre prendere $x_1 \in T$ generico, il quale non è un elemento massimale per T, ciò significa che esisterà $x_2 \in T$ tale che $x_1 < x_2$.

Ma nemmeno x_2 è massimale per cui avremo un $x_3 \in T$ tale che $x_1 < x_2 < x_3$. Continuando così possiamo costruire una successione strettamente crescente in S violando in tal modo la 2. L'equivalenza tra 3 e 4 si dimostra con un procedimento del tutto analogo. ∎

Definizione 3.1.2. Il gruppo G soddisfa l'*ipotesi massimale* se e solo se la famiglia ordinata $(\{H \leq G\}, \subseteq)$ soddisfa l'ipotesi 1 (od 2).

G soddisfa invece l'*ipotesi minimale* se e solo se la famiglia ordinata di sopra soddisfa la 3 o la 4.

La classe dei gruppi massimali si indica con Max mentre quella dei gruppi minimali con Min. Chiaramente i gruppi finiti appartengono sia a Max che a Min mentre esistono gruppi soddisfacenti le condizione minimale e massimali pur non essendo finiti. Un esempio di tali gruppi sono i *gruppi di Tarski* che, pur essendo infiniti, soddisfano entrambe le ipotesi. Ciò è dovuto alla loro particolare struttura

$$
\begin{tikzcd}[column sep=small]
 & & G \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\ldots \arrow[drr, dash] & H \arrow[dr, dash] & K \arrow[d, dash] & L \arrow[dl, dash] & \ldots \arrow[dll, dash] \\
 & & \{1\} & &
\end{tikzcd}
$$

Esempio 2. I gruppi ciclici finiti appartengono sia a Max che a Min, mentre quelli infiniti soddisfano solamente la condizione massimale.

Difatti ogni sottogruppo non banale H di $\langle a \rangle$ è necessariamente ciclico e in particolare $|\langle a \rangle : H| = n < +\infty$. Una proprietà dei gruppi ciclici afferma che se H, K sono sottogruppi di $\langle a \rangle$ tali che $|\langle a \rangle : H| = |\langle a \rangle : K|$ allora $H = K$ e perciò vi sono solo un numero finito di sottogruppi contenenti H.

I gruppi ciclici infiniti non possono essere mai Min, difatti la successione decrescente $H_n = \left\langle a^{2^n} \right\rangle$ non termina.

Esempio 3. I gruppi di Prüfer soddisfano la condizione minimale ma non quella massimale. Ciò deriva automaticamente dalla struttura del gruppo, data dal lemma 2.1.6.

Proposizione 3.1.3. *Un gruppo G soddisfa la condizione massimale se e solo se ogni suo sottogruppo è finitamente generato.*

Dimostrazione. Supponiamo per assurdo che $G \in$ Max ed abbia un sottogruppo $H \neq \{1\}$ non finitamente generato. Preso $x_1 \in H$ avremo $H \setminus \langle x_1 \rangle \neq \emptyset$ e quindi esisterà $x_2 \in H \setminus \langle x_1 \rangle$. Ancora $H \setminus \langle x_1, x_2 \rangle$ altrimenti sarebbe generato da questi due elementi e quindi esisterà necessariamente $x_3 \in H \setminus \langle x_1, x_2 \rangle$.

Abbiamo costruito in tal modo una successione $x_n \in H$, poniamo per ogni $n \in \mathbb{N}$

$$H_n = \langle x_1, x_2, \ldots, x_n \rangle$$

allora $H_n < H_{n+1}$ e la successione è strettamente crescente, in contrasto con l'ipotesi 2. Quindi H deve essere finitamente generato.

Viceversa prendiamo una qualunque successione crescente $H_n \leq G$ e calcoliamone l'unione $H = \bigcup_{n \in \mathbb{N}} H_n$. Chiaramente $H \leq G$ e quindi esisteranno $h_1, h_2, \ldots h_m$ tali che $H = \langle h_1, \ldots h_m \rangle$, per la crescenza esisterà dunque $N \in \mathbb{N}$ tale che $h_1, h_2, \ldots h_m \in H_N$ e quindi $H = H_N = H_n$ per ogni $n \geq N$ e perciò $G \in$ Max. ■

Se solo G è finitamente generato non è detto in generale che G soddisfi anche la condizione massimale. Però se G è anche abeliano oltre che finitamente generato allora più avanti dimostreremo che $g \in$ Max.

Proposizione 3.1.4. *Se $G \in \mathrm{Min}$ allora G è periodico.*

Dimostrazione. Se G non periodico, allora possiederà un sottogruppo ciclico infinito tramite il quale possiamo costruire una successione strettamente decrescente, perciò $G \notin \mathrm{Min}$. ■

Lemma 3.1.5. *Le classi* Max *e* Min *sono chiuse per sottogruppi, quozienti ed estensioni.*

Dimostrazione. Che siano chiuse per sottogruppi e quozienti è banale da verificare. Dimostriamo che Min è chiusa per estensioni, per Max il procedimento è del tutto analogo.

Prendiamo perciò una successione decrescente $H_n \leq G$ e sia $N \lhd G$ tale che $N, G/N \in \mathrm{Min}$. Esisterà allora $m \in \mathbb{N}$ tale che per ogni $n \geq m$

$$H_n \cap N = H_m \cap N \tag{3.1.1}$$

$$H_n N/N = H_m N/N \tag{3.1.2}$$

dalla (3.1.2) deduciamo immediatamente che $H_n N = H_m N$, poiché $H_n \leq H_m$ dall'identità di Dedekind osserviamo che

$$H_m = H_m \cap H_m N = H_m \cap H_n N = H_n (H_m \cap N) = H_n (H_n \cap N) = H_n$$

■

Proposizione 3.1.6. *Se $G \in \mathrm{Max} \cup \mathrm{Min}$ e $G = \mathrm{Dr}_{i \in \mathbb{N}} H_i$ con $H_i \neq \{1\}$ per ogni $i \in I$ allora $|I| < \infty$.*

Dimostrazione. Se I fosse infinito allora potremmo scegliere un suo sottoinsieme numerabile $\{i_1, i_2, \ldots\}$e quindi costruire le successioni

$$K_n = \mathop{\mathrm{Dr}}_{k=1}^{n} H_{i_k}$$

$$L_n = \mathop{\mathrm{Dr}}_{k=n}^{+\infty} H_{i_k}$$

che sono rispettivamente strettamente crescente e strettamente decrescente. ■

Proposizione 3.1.7. *Se G è un gruppo tale che ogni suo sottogruppo non banale H ha indice finito allora $G \in \mathrm{Max}$.*

Dimostrazione. Dalla proposizione 1.1.2 se $\{1\} < K < H \leq G$ avremo immediatamente che $|G : H| < |G : K|$. Ogni successione crescente deve necessariamente terminare per via della finitezza degli indici. ■

Gruppi abeliani

Se il gruppo G fosse abeliano allora è possibile dimostrare altre proprietà di regolarità dei gruppi Max e Min.

Proposizione 3.1.8. *Gli unici gruppi abeliani a soddisfare sia la condizione massimale che quella minimale sono finiti.*

Dimostrazione. Essendo $G \in \mathrm{Max}$ esisteranno $g_1, \ldots, g_n \in G$ tali che

$$G = \langle g_1, \ldots, g_n \rangle = \langle g_1 \rangle + \langle g_2 \rangle + \cdots + \langle g_n \rangle$$

essendo G abeliano. Inoltre G è periodico quindi gli $\langle g_i \rangle$ hanno ordine finito per cui anche G è finito. ∎

Proposizione 3.1.9. *Se G è abeliano e finitamente generato allora $G \in \mathrm{Max}$.*

Dimostrazione. Sia $G = \langle g_1, g_2, \ldots, g_n \rangle$ se $n = 1$ allora G è ciclico quindi Max altrimenti supponiamo il risultato valido per $n - 1$.

Essendo G abeliano tutti i suoi sottogruppi sono normali e quindi

$$G/\langle g_1 \rangle = \langle g_2 \langle g_1 \rangle, g_3 \langle g_1 \rangle, \ldots, g_n \langle g_1 \rangle \rangle \in \mathrm{Max}$$

e la tesi segue dalla chiusura per estensioni di Max. ∎

Teorema 3.1.10 (struttura per gruppi abeliani Max). *Sia G gruppo abeliano, allora $G \in \mathrm{Max}$ se e solo se $G = H_1 \otimes H_2 \otimes \cdots \otimes H_n$ con H_i ciclico infinito o di ordine potenze di qualche numero primo.*

Dimostrazione. Dalla proposizione 1.4.2 segue immediatamente l'implicazione da destra a sinistra. Dimostriamo l'implicazione opposta, supponendo inizialmente che G sia aperiodico.

Sappiamo che G è finitamente generato, quindi lavoriamo per induzione su n con $G = \langle g_1, \ldots, g_n \rangle$. Se $n = 1$ il teorema è banalmente verificato, supponiamo allora che sia valido per $n - 1$, indichiamo allora con $H/\langle g_1 \rangle$ il sottogruppo di torsione di $G/\langle g_1 \rangle$. Ma allora

$$G/H \cong \frac{G/\langle g_1 \rangle}{H/\langle g_1 \rangle}$$

che è senza torsione e finitamente generato. Per la proposizione precedente è anche Max e quindi possiamo applicare l'ipotesi induttiva e quindi G/H è abeliano libero.

Dalla proposizione 2.5.6 esisterà $L \leq G$ tale che $G/H \cong L$ e $G = H \otimes L$, quindi L è prodotto diretto di un numero finito di gruppi ciclici infiniti. Ma anche $H/\langle g_1 \rangle$ è finitamente generato, abeliano e periodico e perciò finito di ordine $m \in M$, ovvero $H^m \leq \langle g_1 \rangle$. Quindi possiamo costruire l'omomorfismo

$$f : h \in H \to h^m \in \langle g_1 \rangle$$

Ora poiché G è aperiodico l'applicazione f è iniettiva e quindi H è isomorfo ad un sottogruppo di un gruppo ciclico, quindi o $H = \{1\}$ oppure H è ciclico infinito. In ogni caso G è prodotto diretto di un numero finito di gruppi ciclici.

Consideriamo adesso un gruppo abeliano $G \in \mathrm{Max}$ generico con T il suo sottogruppo di torsione, G/T è abeliano libero e con un numero finito di fattori diretti per quanto detto sopra, sempre dalla proposizione 2.5.6 esisterà $L \leq G$ isomorfo a G/L tale che $G = L \otimes T$. Il sottogruppo T è abeliano, finitamente generato e periodico e quindi finito, dal teorema 2.4.12 anche T è prodotto diretto di un numero finito di sottogruppi ciclici di ordine primo. ■

Corollario 3.1.11. *Se G è un gruppo abeliano finitamente generato e T è il suo sottogruppo di torsione allora esiste $F \leq G$ abeliano libero di rango finito tale che $G = T \times F$.*

Dimostrazione. Dal teorema di struttura esistono $H_1, H_2, \ldots, H_s \leq G$ ciclici di ordine primo e $H_{s+1}, \ldots, H_t \leq G$ ciclici infiniti tali che $G = H_1 \times H_2 \times \cdots \times H_t$.

Osserviamo che $T = H_1 \times H_2 \times \cdots \times H_s$ in quanto, per via della scomposizione unica degli elementi di un prodotto diretto, tutti e soli questi elementi hanno periodo finito, quindi ponendo $F = H_{s+1} \times H_{s+2} \times \cdots \times H_t$ otteniamo la tesi. ■

Teorema 3.1.12 (struttura per gruppi abeliani Min)**.** *Sia G gruppo abeliano, allora $G \in \mathrm{Min}$ se e solo se $G = H_1 \otimes H_2 \otimes \cdots \otimes H_n$ con H_i ciclico di ordine potenza di primo o isomorfo a $\mathbb{Z}(p_i{}^{\infty})$ per un opportuno p_i primo.*

Dimostrazione. L'implicazione da destra a sinistra è banale, supponiamo allora $G \in \mathrm{Min}$. Allora G è periodico e dal teorema 2.1.5 possiamo scrivere

$$G = \underset{p \text{ primo}}{\mathrm{Dr}} G_p = G_{p_1} \otimes G_{p_2} \otimes \cdots \otimes G_{p_n}$$

Possiamo quindi supporre che G sia un p-gruppo, dalla proposizione 2.3.12 esistono $D \leq G$ divisibile e $R \leq G$ ridotto tali che $G = D \otimes R$. Dal teorema di struttura dei gruppi divisibili, poiché $\mathbb{Q}$ non è Min essendo aperiodico, D è prodotto diretto di gruppi di Prüfer $\mathbb{Z}(p^{\infty})$. Possiamo quindi restringere ancora la nostra analisi nel caso in cui G sia un p-gruppo ridotto.

Supponiamo per assurdo che G sia infinito, poniamo

$$\mathcal{F} = \{H \leq G \mid H \text{ infinito}\}$$

essendo $G \in \mathrm{Min}$ esisterà $K \leq G$ elemento minimale di $\mathcal{F}$, il quale è infinito e non divisibile. Poiché G è anche un p-gruppo esisterà $h \in K \setminus K^p$ ovvero $K^p < K$ e quindi K^p è finito.

Definiamo adesso l'omomorfismo

$$f : h \in K \to h^p \in K^p$$

chiaramente $K/\ker f \cong f(K)$ è finito e perciò $\ker f \leq K$ deve essere necessariamente infinito, ma allora $\ker f = K$ ovvero $K^p = \{1\}$ e dal teorema di Prüfer-Baer

$$K = K[p] = \langle h_1 \rangle \otimes \langle h_2 \rangle \otimes \cdots \otimes \langle h_m \rangle$$

in quanto $K \in \mathrm{Min}$. Ma allora K è finito pur avendo supposto che fosse infinito, ottenendo in tal modo un assurdo. ■

3.2 Serie di gruppi

Definizione 3.2.1. Sia G un gruppo generico e $\mathcal{F}$ una classe composta da sottogruppi di G. Diciamo che $\mathcal{F}$ è un *sistema seriale* se e solo se

1. $\mathcal{F}$ è totalmente ordinata rispetto all'operazione di inclusione;
2. Preso un qualunque sottoinsieme $\{H_i\}_{i\in I} \subseteq \mathcal{F}$ allora $\bigcup_i H_i, \bigcap_i H_i \in \mathcal{F}$;
3. Se $H, K \in \mathcal{F}$ sono consecutivi, ovvero $K < H$ e non vi sono altri elementi di $\mathcal{F}$ tra H e K, allora $K \lhd H$.

Gli elementi di $\mathcal{F}$ sono detti *termini* del sistema seriale, mentre se $H < K$ sono consecutivi la quantità H/K è un *fattore*.

Definizione 3.2.2. Un sistema seriale $\mathcal{F}$ su G è una *serie* di G se e solo se $G \in \mathcal{F}$.
(Alcuni dicono se e solo se $\mathcal{F} \cup \{G\}$ è contenuto in un qualche sistema seriale).

Definizione 3.2.3. Una serie $\mathcal{F}$ di G è

- *ascendente* se e solo se ogni sottoinsieme di $\mathcal{F}$ ha minimo;
- *discendente* se e solo se ogni sottoinsieme di $\mathcal{F}$ ha massimo;
- *normale* se e solo se $\mathcal{F}$ è finito;
- *normale* se e solo se per ogni $H \in \mathcal{F}$ si ha $H \lhd G$;
- *abeliana* se e solo se ogni suo fattore H/K è abeliano;
- *centrale* se e solo se è normale e per ogni coppia di termini consecutivi $H < K$ si ha $K/H \leq Z(G/H)$.

Se $\mathcal{F}$ è una serie finita diciamo che ha *lunghezza* $n \in \mathbb{N}$ se e solo se $|\mathcal{F}| = n + 1$. Una serie $\mathcal{G}$ è un *raffinamento* di $\mathcal{F}$ se e solo se $\mathcal{F} \subseteq \mathcal{G}$, mentre $\mathcal{F}$ è una *serie di composizione* se e solo se non possiede raffinamenti propri, i suoi fattori sono detti *fattori di composizione*. Una serie $\mathcal{F}$ è *principale* se e solo se è normale e non possiede raffinamenti propri normali. Se $H \lhd K$ allora diciamo che K/H è principale se e solo se è un fattore di una serie principale.

Definizione 3.2.4. Sia G gruppo e $\{1\} < N \leq G$, allora N è *normale minimale*, e lo indichiamo con $N \underset{\min}{\lhd} G$, se e solo se $N \lhd G$ e per ogni $L < N$ tale che $L \lhd G$ si ha $L = \{1\}$.

Proposizione 3.2.5. *Sia G gruppo ed $K \lhd H \leq G$. Allora*

1. *H/K è un fattore di composizione se e solo se H/K è semplice, ovvero non possiede sottogruppi normali non banali;*
2. *H/K è un fattore principale se e solo se $H, K \lhd G$ e $H/K \underset{min}{\lhd} G/K$.*

Dimostrazione. Seguono immediatamente dall'equivalenza

$$L/K \lhd H/K \Leftrightarrow K \lhd L \lhd H$$

∎

Definizione 3.2.6. Sia G gruppo e $H \leq G$.

- Diciamo che H è *ascendente* in G, e lo indichiamo con $H \operatorname{asc} G$, se e solo se esiste una serie ascendente contenente H e G.
- Diciamo che H è *discendente* in G, e lo indichiamo con $H \operatorname{dis} G$, se e solo se esiste una serie discendente contenente H e G.
- Diciamo che H è *subnormale* in G, e lo indichiamo con $H \operatorname{sn} G$, se e solo se esiste una serie finita contenente H e G. In tal caso definiamo il *difetto* di H in G come la più piccola lunghezza di una tale serie.

Proposizione 3.2.7. *Se G è un gruppo e $H < G$ allora*

1. *$H \operatorname{asc} G \Rightarrow H < N_G(H)$;*
2. *$H \operatorname{dis} G \Rightarrow H^G < G$.*

Dimostrazione. Dimostriamo i vari punti

1. Se $\mathcal{F}$ è una serie ascendente contenente G ed H allora esiste il minimo della classe

   $$\{L \in \mathcal{F} \mid H < L\}$$

   che indichiamo con K. Poiché sono consecutivi $H \lhd K$ e quindi $H < K \leq N_G(H)$.
2. Se $\mathcal{F}$ è una serie discendente contenente G ed H allora esiste il massimo della classe

   $$\{L \in \mathcal{F} \mid H \leq L < G\}$$

   che indichiamo con K. Poiché sono consecutivi $H \leq K \lhd G$ e $L < G$ quindi $H^G \leq K < G$.

■

Esempio 4 (Sottogruppo ascendente non discendente)**.** Consideriamo $G = \langle x \rangle \ltimes \mathbb{Z}(2^\infty)$ il 2-gruppo localmente diedrale con $a^x = a^{-1}$ per ogni $a \in \mathbb{Z}(2^\infty) = A$. Dimostriamo che $H = \langle x \rangle$ è ascendente ma non discendente e per mostrarlo consideriamo la serie

$$H_i = \langle x \rangle \ltimes A_i$$

per ogni $i \in \mathbb{N}_0$ e A_i ciclico definito come nella dimostrazione del lemma 2.1.6. Poiché $|H_{i+1} : H_i| = |A_{i+1} : A_i| = 2$ avremo che $H_i \lhd H_{i+1}$ e $\bigcup_{i=0}^{+\infty} H_i = G$ dunque $H \operatorname{asc} G$.

Prendiamo ora un qualunque $H \lhd G$ tale che $x \in H$ quindi per ogni $a \in A$ avremo $x^a \in H \Rightarrow a^{-1}xa = xa^2 \in H \Rightarrow a^2 \in H$ ed essendo A divisibile avremmo $H = G$ quindi per la proposizione 3.2.7 $\langle x \rangle$ non è un sottogruppo discendente.

Esempio 5 (Sottogruppo discendente non ascendente)**.** Consideriamo stavolta $G = \langle x \rangle \ltimes \mathbb{Z}$ gruppo diedrale infinito e prendiamo sempre $H = \langle x \rangle$, dimostriamo che H è ascendente ma non discendente. Per dimostrare che il sottogruppo H è discendente basta considerare la serie decrescente

$$H_i = \langle x \rangle \ltimes \left\langle 2^i \right\rangle$$

allora $H_0 = G$ e $|H_i : H_{i+1}| = \left|\left\langle 2^i \right\rangle : \left\langle 2 \cdot 2^i \right\rangle\right| = 2$ e quindi $H_{i+1} \lhd H_i$ e $\bigcap_{i=0}^{+\infty} H_i = \langle x \rangle$.

Per far vedere che H non è ascendente osserviamo prima di tutto che $\langle x \rangle \leq N_G(H)$, se per assurdo esistesse $n \in A = \mathbb{Z}$ tale che $(-n)xn = x(2n) \in x$ allora dovrebbe essere $2n = 0$ e quindi $n = 0$. Perciò $N_G(H) = H$ e sempre per la proposizione 2.1.6 H non è ascendente.

Gruppi risolubili e nilpotenti

Definizione 3.2.8. Un gruppo G è detto *risolubile* se e solo se esiste una serie abeliana finita contenente sia G che $\{1\}$. In tal caso denotiamo con $\operatorname{der}(G)$ la più piccola lunghezza di tale serie.

Il gruppo G è *nilpotente* se e solo se esiste una serie centrale finita contenente sia G che $\{1\}$. In tal caso denotiamo con $\operatorname{cl}(G)$ la più piccola lunghezza di tale serie.

Chiaramente si ha

$$G \text{ abeliano } \Leftrightarrow \operatorname{der}(G) = 1 \Leftrightarrow \operatorname{cl}(G) = 1$$

diciamo che G è *metabeliano* se e solo se $\operatorname{der}(G) \leq 2$. Inoltre vale il seguente risultato

Proposizione 3.2.9. *Sia G gruppo allora*

$$\operatorname{cl}(G) \leq 2 \Leftrightarrow G/Z(G) \text{ abeliano}$$

Dimostrazione. Possiamo supporre che $\operatorname{cl}(G) = 2$, in tal caso esiste $\{1\} < H < G$ tale che la serie $\{1\} \lhd H \lhd G$ è centrale. Ciò significa che

$$H \leq Z(G)$$
$$G/H \leq Z(G/H)$$

perciò G/H è abeliano e quindi

$$G/Z(G) \cong \frac{G/H}{Z(G)/H}$$

è abeliano.

Viceversa la serie $\{1\} \lhd Z(G) \lhd G$ è chiaramente centrale. ■

Proposizione 3.2.10. *La classe dei gruppi risolubili, indicata con $\mathcal{S}$, è chiusa per sottogruppi, quozienti ed estensioni.*

Dimostrazione. Dimostriamo le varie asserzioni.

- Sia G risolubile e $H \leq G$, dimostriamo che $H \in \mathcal{S}$. Sia $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ serie abeliana, allora non è difficile verificare che

$$G_i \lhd G_{i+1} \Rightarrow H \cap G_i \lhd H \cap G_{i+1}$$

  e quindi $H_i = H \cap G_i$ è una serie finita di H. Allora

$$\frac{H \cap G_{i+1}}{H \cap G_i} = \frac{H \cap G_{i+1}}{(H \cap G_{i+1}) \cap G_i} \cong \frac{(H \cap G_{i+1})\, G_i}{G_i} \leq G_{i+1}/G_i$$

  e quindi la serie è abeliana e $\mathrm{der}(H) \leq \mathrm{der}(G)$.

- Usando la stessa notazione del punto precedente sia $N \lhd G$, allora $G_iN \lhd G_{i+1}N$ poiché $G_{i+1} \leq N_G(G_iN)$ e quindi $N \leq G_iN \leq N_G(G_iN)$. Perciò G_iN/N è una serie finita di G/N e inoltre

$$\frac{G_{i+1}N/N}{G_iN/N} \cong \frac{G_{i+1}N}{G_iN} \cong \frac{G_{i+1}}{G_{i+1} \cap G_iN} \cong \frac{G_{i+1}/G_i}{(G_{i+1} \cap G_iN)/G_i}$$

  che è abeliano e perciò $\mathrm{der}(G/N) \leq \mathrm{der}(G)$.

- Siano G e $N \lhd G$ tali che $N, G/N \in \mathcal{S}$ e consideriamo le seguenti serie abeliane

$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_n = N$$
$$\{N\} = H_0/N \lhd H_1/N \lhd \cdots \lhd H_m/N = G/N$$

  Quindi $H_0 = N$ e $H_{i+1}/H_i \cong \frac{H_{i+1}/N}{H_i/N}$ è abeliano, perciò la serie

$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_n = N = H_0 \lhd H_1 \lhd \cdots \lhd H_m = G$$

  è abeliana e quindi G è risolubile con $\mathrm{der}(G) \leq \mathrm{der}(N) + \mathrm{der}(G/N)$.

■

Corollario 3.2.11. *Se $M, N \lhd G$ e $M, N \in \mathcal{S}$ allora $MN \in \mathcal{S}$.*

Dimostrazione. Segue immediatamente dalla proposizione 1.4.2. ∎

Prima di dimostrare un risultato analogo per i gruppi nilpotenti osserviamo che, preso G gruppo e $L \lhd G$ allora

$$\begin{aligned}&L = L_0 \lhd L_1 \lhd \cdots \lhd L_n = G \text{ è centrale}\\ &\qquad\Leftrightarrow \{L\} = L_0/L \lhd L_1/L \lhd \cdots \lhd L_n/L = G/L \text{ è centrale}\end{aligned}$$

Difatti se $\varphi : G/L_i \to (G/L)/(L_i/L)$ è un isomorfismo allora si dimostra facilmente che

$$\begin{aligned}L_{i+1}/L_i \leq Z\left(G/L_i\right) \Leftrightarrow \frac{L_{i+1}/L}{L_i/L} &= \varphi\left(L_{i+1}/L_i\right)\\ &\leq \varphi\left(Z\left(G/L_i\right)\right) = Z\left(\varphi\left(G/L_i\right)\right) = Z\left(\frac{G/L}{L_i/L}\right)\end{aligned}$$

Proposizione 3.2.12. *La classe dei gruppi nilpotenti è chiusa per sottogruppi e quozienti*

Dimostrazione. Per ogni $x, y \in G$ definiamo

$$[x; y] = x^{-1}y^{-1}xy \in G$$

allora

$$K/H \leq Z\left(G/H\right) \Leftrightarrow [g; k] \in H \text{ per ogni } g \in G \text{ e } k \in K$$

- Sia G nilpotente e $H \leq G$, dimostriamo che $H \in \mathfrak{N}$. Sia $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ serie centrale, allora non è difficile verificare che

  $$G_i \lhd G \Rightarrow H \cap G_i \lhd H$$

  e quindi $H_i = H \cap G_i$ è una serie finita e normale di H. Allora per ogni $g \in G \cap H$ e $g' \in G_{i+1} \cap H$ si ha $[g; g'] \in G_i \cap H$ e quindi la serie è centrale e $\mathrm{cl}(H) \leq \mathrm{cl}(G)$.

- Usando la stessa notazione del punto precedente sia $N \lhd G$, allora $G_iN \lhd G$ essendo prodotto di sottogruppi normali. Perciò G_iN/N è una serie finita e normale di G/N, per dimostrare l'asseto basta verificare che

  $$\frac{NG_{i+1}}{NG_i} \leq Z\left(\frac{G}{NG_i}\right)$$

  Presi $g \in G$, $g' \in G_{i+1}$ e $n \in N$ allora

  $$\left[g; ng'\right] = g^{-1}g'^{-1}n^{-1}gng' = g^{-1}g'^{-1}gg'g'^{-1}g^{-1}n^{-1}gng' = \left[g; g'\right][g; n]^{g'} \in G_iN$$

  in quanto $N \lhd G \Rightarrow [g; n] = \left(n^{-1}\right)^g n \in N \Rightarrow [g; n]^{g'} \in N$. La serie è perciò centrale con $\mathrm{cl}\left(G/N\right) \leq \mathrm{cl}(G)$.

■

Esempio 6. La classe $\mathcal{N}$ non è chiusa per estensioni, basta per esempio prendere $G = S_3$ il gruppo delle permutazioni di 3 elementi, difatti $A_3 \lhd S_3$ è abeliano e $|S_3 : A_3| = 2$. Ma S_3 non è nilpotente poiché $Z(S_3) = \{1\}$.

Ciononostante vale ancora il corollario 3.2.11 anche per i gruppi risolubili, ma la dimostrazione è più lunga e verrà dimostrata più avanti nel teorema di Fitting.

3.3 Commutatori e interderivati

Nella sezione precedente abbiamo visto la quantità

$$[x; y] = x^{-1}y^{-1}xy$$

essa è il *commutatore* di x e y, ed è stata introdotta per dare una misura di quanto due elementi "non commutano", difatti $[x; y] = 1 \Leftrightarrow xy = yx$.

Tra le proprietà più immediate del commutatore osserviamo le seguenti

Proposizione 3.3.1. *Sia G gruppo e $x, y, z \in G$. Allora*

1. $[x; 1] = 1$;
2. $[x; y] = \left(y^{-1}\right)^x y = x^{-1}x^y$;
3. *Se $f : G \to G'$ è un omomorfismo tra gruppi allora* $f([x; y]) = [f(x); f(y)]$;
4. $[x; y]^{-1} = [y; x]$;
5. *Se $N \lhd G$ allora* $[xN; yN] = [x; y]\, N$;
6. $[xz; y] = [x; y]^z [z; y]$ *e* $[x; yz] = [x; z] [x; y]^z$;
7. $\left[x^{-1}; y\right] = \left([x; y]^{-1}\right)^{x^{-1}}$ *e* $\left[x; y^{-1}\right] = \left([x; y]^{-1}\right)^{y^{-1}}$;
8. $[x; y]\, z = z^x [x; yz]$.

Dimostrazione. Dimostriamo i vari punti

1. Banale.
2. Banale.
3. Banale poiché $f\left(x^{-1}\right) = f(x)^{-1}$.
4. Banale.
5. Segue dal punto 3.

6. Svolgendo i conti

$$\begin{aligned}[xz;y] &= z^{-1}x^{-1}y^{-1}xzy = z^{-1}x^{-1}y^{-1}xyy^{-1}zy \\ &= z^{-1}x^{-1}y^{-1}xyzz^{-1}y^{-1}zy = [x;y]^z\,[z;y]\end{aligned}$$

mentre la seconda formula segue dalla prima

$$[x;yz] = [yz;x]^{-1} = \left([y;x]^z\,[z;x]\right)^{-1} = [x;z]\,[x;y]^z$$

7. $1 = [1;y] = \left[xx^{-1};y\right] = [x;y]^{x^{-1}}\left[x^{-1};y\right]$. L'altro punto si mostra con un ragionamento analogo.

8. $[x;yz] = [x;z]\,z^{-1}\,[x;y]\,z = \left(z^{-1}\right)^x zz^{-1}\,[x;y]\,z = (z^x)^{-1}\,[x;y]\,z.$

■

Generalizziamo i commutatori in modo tale da possedere un numero arbitrario di elementi:

$$\begin{cases} [x_1] = x_1 \\ [x_1;x_2;\ldots;x_{n-1};x_n] = [[x_1;x_2;\ldots;x_{n-1}];x_n]\end{cases}$$

Lemma 3.3.2 (Identità di Hall-Witt)**.** *Siano $x,y,z \in G$ allora*

$$\left[x;y^{-1};z\right]^y\left[y;z^{-1};x\right]^z\left[z;x^{-1};y\right]^x = 1 \tag{3.3.1}$$

Dimostrazione. Innanzitutto osserviamo che $[x;y;z] = [y;x]\,z^{-1}\,[x;y]\,z = y^{-1}x^{-1}yx$ $\cdot z^{-1}x^{-1}y^{-1}xyz$ e quindi

$$\left[x;y^{-1};z\right]^y = y^{-1}yx^{-1}y^{-1}xz^{-1}x^{-1}yxy^{-1}zy = \left(y^{-1}\right)^x z^{-1}\,(y)^x\,(z)^y$$

Possiamo riscrivere la (3.3.1) in modo più agevole

$$\begin{aligned}\left[x;y^{-1};z\right]^y\left[y;z^{-1};x\right]^z\left[z;x^{-1};y\right]^x &= \left(y^{-1}\right)^x z^{-1}\,(y)^x\,(z)^y \\ &\cdot \left(z^{-1}\right)^y x^{-1}\,(z)^y\,(x)^z \\ &\cdot \left(x^{-1}\right)^z y^{-1}\,(x)^z\,(y)^x \\ &= \left(y^{-1}\right)^x z^{-1}\,(y)^x\,x^{-1}\,(z)^y\,y^{-1}\,(x)^z\,(y)^x \\ &= \left(y^{-1}\right)^x z^{-1}x^{-1}yy^{-1}z\,(x)^z\,(y)^x \\ &= x^{-1}y^{-1}xz^{-1}x^{-1}zz^{-1}xzx^{-1}yx \\ &= 1\end{aligned}$$

■

Definizione 3.3.3. Siano G gruppo e $X, Y \subseteq G$ sottoinsiemi non vuoti. Allora definiamo l'*interderivato* tra X e Y il sottoinsieme

$$[X; Y] = \langle [x; y] \mid x \in X \ y \in Y \rangle$$

Inoltre se $X_1, X_2 \dots X_n \subseteq G$ sono tutti non vuoti allora poniamo

$$[X_1; X_2; \dots ; X_n] = [[X_1; X_2; \dots ; X_{n-1}]; X_n]$$

e per ogni $n \in \mathbb{N}$

$$[X;_n Y] = [X; \overbrace{Y; Y; \dots ; Y}^{n \text{ volte}}]$$

Lemma 3.3.4. *Sia G un gruppo generico, $x, y \in G$ ed $H \leq G$ tali che*

$$[x; y; H] = \{1\} \Leftrightarrow [x; y] \leq C_G(H)$$

allora per ogni $m \in \mathbb{N}_0$ se $x \in H$ avremo

$$[x^m; y] = [x; y]^m$$

mentre se $y \in H$ allora

$$[x; y^m] = [x; y]^m$$

Dimostrazione. Supponiamo che $x \in H$ allora $x^m \in H$ per ogni $m \in \mathbb{N}_0$. L'ipotesi è verificata per $m = 0, 1$ altrimenti supponiamola verificata per un certo $m \geq 1$ allora

$$\left[x^{m+1}; y\right] = [xx^m; y] = [x; y]^{x^m} [x^m; y] = [x; y] [x; y; x^m] [x; y]^m = [x; y]^{m+1}$$

poiché $[x; y; x^m] \in [x; y; H] = \{1\}$.

Se invece $y \in H$ allora supponiamo l'ipotesi verificata per un certo $m \geq 1$ allora

$$\left[x; y^{m+1}\right] = [x; yy^m] = [x; y^m] [x; y]^{y^m} = [x; y]^m [x; y] [x; y; y^m] = [x; y]^{m+1}$$

poiché $[x; y; y^m] \in [x; y; H] = \{1\}$. ■

Proposizione 3.3.5. *Presi $x, y \in G$ ed $A \lhd G$ abeliano, allora se $x \in A$ avremo $[x^m; y] = [x; y]^m$ mentre se $y \in A$ allora $[x; y^m] = [x; y]^m$.*

Se invece per certi $x, y \in G$ abbiamo $[x; y] \in Z(G)$ allora valgono gli stessi risultati.

Dimostrazione. Supponiamo che $x \in A$ allora $[x; y] \in A$ per ogni $y \in G$ per normalità. Inoltre $A \leq C_G(A)$ essendo A abeliano e quindi possiamo applicare il lemma precedente.

Il secondo asserto è banale in quanto $Z(G) = C_G(G)$. ■

Sia G gruppo, diciamo che $H \leq G$ è *pienamente invariante* se e solo se $\varphi(H) \leq H$ per ogni $\varphi : G \to G$ *endomorfismo*. La piena invarianza è una ipotesi molto più forte di quella di sottogruppo caratteristico che considera solamente gli *automorfismi* di G.

Il centro di un gruppo è sempre caratteristico, mentre può non essere pienamente invariante come dimostra questo esempio

Esempio 7. Consideriamo S_3 gruppo delle permutazioni su $\{1, 2, 3\}$, poniamo

$$G = \mathbb{Z}_2 \otimes S_3$$

Non è difficile mostrare che $Z(S_3) = \{\mathrm{id}\}$ e quindi $Z(G) = \mathbb{Z}_2$. L'applicazione $f : \mathbb{Z}_2 \to S_3$ tale che $f(0) = \mathrm{id}$ e $f(1) = (1, 2)$ è un omomorfismo tra gruppi, quindi anche

$$\varphi : (t, s) \in \mathbb{Z}_2 \otimes S_3 \to (0, f(t)) \in \mathbb{Z}_2 \otimes S_3$$

è un endomorfismo e $\varphi(Z(G)) = \{0\} \otimes \langle(1, 2)\rangle \nleq Z(G)$.

Proposizione 3.3.6. *Se $M, N \leq G$ e $X \subseteq G$ allora*

- *Se $M, N \lhd G$ allora $[M; N] \lhd G$;*
- *Se M, N sono caratteristici in G allora $[M; N]$ è caratteristico in G;*
- *Se M, N sono pienamente invarianti in G allora $[M; N]$ è pienamente invariante in G.*

Dimostrazione. Sono tutte una diretta conseguenza del punto 3 della proposizione 3.3.1. ■

Proposizione 3.3.7. *Siano $X_1, X_2, \ldots, X_m \subseteq G$, se esiste $l \leq m$ tale che $X_l \lhd G$ allora*

$$[X_1; X_2; \ldots ; X_m] \leq X_l$$

Dimostrazione. Utilizzeremo l'induzione su m, se $m = 1$ è banale mentre se $m = 2$ allora segue velocemente dal punto 2 della proposizione 3.3.1.

Supponiamo l'asserto verificato per $m \geq 2$ e siano $X_1, \ldots, X_m, X_{m+1} \subseteq G$, se $l = m+1$ allora $[X_1; X_2; \ldots ; X_{m+1}] = [[X_1; X_2; \ldots ; X_m] ; X_{m+1}] \leq X_{m+1}$ altrimenti per ipotesi induttiva $[X_1; X_2; \ldots ; X_{m+1}] = [[X_1; X_2; \ldots ; X_m] ; X_{m+1}] \leq [X_l; X_{m+1}] \leq X_l$. ■

Proposizione 3.3.8. *Sia G gruppo e $K \leq G$ e $X \subseteq G$ insieme generico. Allora*

1. *$X^K = \langle X, [X; K]\rangle$;*
2. *$[X; K]^K = [X; K]$ e quindi $K \leq N_G([X; K])$.*

Dimostrazione. Dimostriamo i vari punti

1. Ricordiamo che $X^K = \left\langle k^{-1}Xk \;\middle|\; k \in K\right\rangle$ e quindi per ogni $x \in X$ e $k \in K$ abbiamo $[x; k] = x^{-1}x^k \in X^K$ e quindi $\langle X, [X; K]\rangle \leq X^K$. Viceversa abbiamo $x^k = x\,[x; k] \in \langle X, [X; K]\rangle$.
2. Chiaramente $[X; K] \leq [X; K]^K$ viceversa per ogni $x \in X$ e $k, k' \in K$ dalla proposizione 3.3.1
$$[x; k]^{k'} = \left[x; k'\right]^{-1} \left[x; kk'\right] \in [X; K]$$

■

Corollario 3.3.9. *Per ogni $X \subseteq G$ segue immediatamente che $[X;G] \lhd G$ e quindi*

$$X^G = \langle X, [X;G] \rangle = \langle X \rangle [X;G]$$

Proposizione 3.3.10. *Presi $H, K, L \lhd G$ allora $[HK;L] = [H;L][K;L]$.*

Dimostrazione. Chiaramente $[H;L][K;L] \leq [HK;L]$, però essendo tutti questi sottogruppi normali dalla proposizione 3.3.1 segue che per ogni $h \in H$ $k \in K$ e $l \in L$

$$[hk;l] = [h;l]^k [k;l] \in [H;L][K;L]$$

∎

Lemma 3.3.11. *Sia G gruppo e $X, Y \subseteq G$ due suoi sottoinsiemi. Posto $K = \langle Y \rangle$ allora*

$$[X;K] = [X;Y]^K$$

Dimostrazione. Se $Y = K$ allora discenderebbe immediatamente dalla proposizione 3.3.8 quindi $[X;Y]^K \leq [X;K]^K = [X;K]$.

Viceversa per ogni $k \in K$ esistono $y_1, y_2, \dots, y_n \in Y$ ed $\epsilon_1, \dots \epsilon_n \in \{1, -1\}$ tali che $k = y_1^{\epsilon_1} y_2^{\epsilon_2} \cdots y_n^{\epsilon_n}$ utilizziamo l'induzione su $n \in \mathbb{N}$ per mostrare che $[x;k] \in [X;Y]^K$ per ogni $x \in X$. Se $n = 1$ allora

$$[x;y_1^{\epsilon_1}] = \begin{cases} [x;y_1] & \text{se } \epsilon_1 = 1 \\ \left([x;y_1]^{-1}\right)^{y_1^{-1}} & \text{se } \epsilon_1 = -1 \end{cases} \in [X;Y]^K$$

Supponiamo di aver già dimostrato l'asserto per $n-1$ e sia $k' = y_1^{\epsilon_1} y_2^{\epsilon_2} \cdots y_{n-1}^{\epsilon_{n-1}}$ allora

$$\left[x; k' y_n^{\epsilon_n}\right] = [x; y_n^{\epsilon_n}] \left[x;k'\right]^{y_n^{\epsilon_n}} \in [X;Y]^K$$

e quindi $[X;K] \leq [X;Y]^K$. ∎

Corollario 3.3.12. *Presi $X, Y \subseteq G$ e $H = \langle X \rangle$, $K = \langle Y \rangle$ allora*

$$[H;K] = [X;Y]^{HK}$$

si ricorda che non è necessario che HK sia un sottogruppo.

Dimostrazione. Dalla proposizione precedente $[H;K] = \left([X;Y]^H\right)^K$ e la tesi segue osservando che $\left(g^h\right)^k = g^{hk}$. ∎

Lemma 3.3.13 (Tre sottogruppi). *Siano $H, K, L \leq G$ e $N \lhd G$. Se N contiene due dei seguenti sottogruppi*

$$[H;K;L], [K;L;H], [L;H;K]$$

allora contiene anche il terzo.

Dimostrazione. Non possiamo applicare direttamente l'identità di Hall-Witt poiché in generale

$$[H;K;L] \neq \langle [h;k;l] \mid h \in H, k \in K, l \in L \rangle$$

Se però poniamo $X = \{[h;k] \mid h \in H, k \in K\} \subseteq G$ allora $\langle X \rangle = [H;K]$ e dalla proposizione 3.3.8 abbiamo $[H;K;L] = [X;L]^{[H;K]}$ e $[X;L] = \langle [h;k;l] \mid h \in H, k \in K, l \in L \rangle$.

Per la normalità di N si ha allora

$$[H;K;L] \leq N \Leftrightarrow [X;L] \leq N$$

e possiamo dunque applicare Hall-Witt. ■

Definizione 3.3.14. Sia G gruppo, il *derivato* di G è il sottogruppo

$$G' = [G;G]$$

Per quanto detto sopra G' è caratteristico in G e $G' = \{1\}$ se e solo se G è abeliano.

Lemma 3.3.15. *Siano $A, B \lhd G$ tali che $G = AB$ allora*

$$G' = A'B' [A;B]$$

Dimostrazione. Applicando la proposizione 3.3.10 e per la normalità dei sottogruppi abbiamo

$$G' = [AB;AB] = [A;A] [A;B] [B;A] [B;B] = A'B' [A;B]$$

■

Proposizione 3.3.16. *Sia G gruppo generico*

1. *Presi $H, K \leq G$ allora $K \leq N_G(H)$ se e solo se $[K;H] \leq H$;*
2. *Se ora $H \leq K \leq G$ allora*

$$[K;G] \leq H \Leftrightarrow H \lhd G \text{ e } K/H \leq Z(G/H)$$

Dimostrazione. Il primo punto è immediato in quanto $K \leq N_G(H) \Leftrightarrow h^k = h[h;k] \in H$ per ogni $h \in H$ e $k \in K \Leftrightarrow [K;H] \leq H$.

Supponiamo inizialmente che $H \lhd G$ e $K/H \leq Z(G/H)$, quindi per ogni $k \in K$ e $g \in G$ abbiamo $kgH = gkH \Rightarrow k^{-1}g^{-1}kgH = H \Rightarrow [k;g] \in H$. Viceversa dobbiamo solo mostrare che $H \lhd G$, ma $[H;G] \leq [K;G] \leq H$ e dal punto precedente si ha $G = N_G(H)$ e quindi $H \lhd G$. ■

Corollario 3.3.17. *G/G' è abeliano e inoltre per ogni $H \leq G$*

$$G' \leq H \Leftrightarrow H \lhd G \wedge G/H \text{ abeliano}$$

3.4 Esempi notevoli di serie

Richiamiamo inizialmente alcuni concetti di teoria degli insiemi. Un *ordinale* α non è nient'altro che che un insieme che può o coincidere con l'insieme vuoto oppure soddisfare i seguenti assiomi

- Se $x \in \alpha$ allora $x \subseteq \alpha$, ovvero se $x \in \alpha$ e $y \in x$ allora $y \in \alpha$;
- La relazione d'ordine tra gli elementi di α definita come $x \preceq y \Leftrightarrow x = y \vee x \in y$ è di buon ordine, ovvero ogni suo sottoinsieme possiede minimo.

Per ogni ordinale α definiamo l'*ordinale successore* l'insieme

$$\alpha + 1 = \alpha \cup \{\alpha\}$$

l'ordinale successore è esso stesso un ordinale, inoltre avendo posto $0 = \emptyset$ allora possiamo definire i seguenti ordinali

$$\begin{aligned}
1 &= 0 + 1 = \{\emptyset\} \\
2 &= 1 + 1 = \{\emptyset, \{\emptyset\}\} \\
3 &= 2 + 1 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
4 &= 3 + 1 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\} \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}
\end{aligned}$$

e così via. Gli ordinali di questo genere sono detti *ordinali finiti* mentre tutti gli altri sono detti *ordinali infiniti*. Un ordinale α è detto *limite* se e solo se non esiste alcun ordinale β tale che $\beta + 1 = \alpha$.

Non è difficile vedere che $\mathbb{N} = \omega$ è un ordinale infinito contenente tutti gli ordinali finiti, e quindi è anche un ordinale limite. Enunciamo i seguenti risultati fondamentali sugli ordinali

Teorema 3.4.1. *Se S è un insieme ben ordinato rispetto alla relazione $\leq$ allora esiste un unico ordinale α e un'unica funzione biiettiva $\psi : \alpha \to S$ tale che per ogni $\beta, \gamma \in \alpha$*

$$\beta \preceq \gamma \Leftrightarrow \psi(\beta) \leq \psi(\gamma)$$

Teorema 3.4.2. *Se Λ è un insieme non vuoto composta da ordinali e $\Theta \subseteq \Lambda$ tale che*

1. $\min \Lambda \in \Theta$;
2. *Per ogni $\alpha \in \Lambda$ tale che*

$$\alpha \cap \Lambda = \{\beta \in \Lambda \mid \beta \prec \alpha\} \subseteq \Theta$$

si abbia $\alpha \in \Theta$

Se valgono entrambe queste asserzioni allora $\Lambda = \Theta$.

Osservazione. Possiamo riscrivere il secondo punto nel caso in cui $\alpha = \beta + 1$ per un opportuno $\beta \in \Lambda$ come

$$\beta \in \Theta \Rightarrow \alpha = \beta + 1 \in \Theta$$

riottenendo il principio di induzione usuale.

Da questo risultato possiamo perciò definire funzioni sugli ordinali per ricorrenza come nel caso usuale per gli ordinali che possiedono un elemento precedente, con la sola accortezza di specificare il caso di un ordinale limite.

Applichiamo la teoria degli ordinali nello studio delle serie ascendenti e discendenti. Se Σ fosse una serie ascendente (o anche discendente invertendo l'ordine) allora sarebbe bene ordinata e dal teorema precedente esiste un unico ordinale μ e un'unica applicazione biiettiva

$$: \alpha \in \mu \to H_\alpha \in \Sigma$$

tale che per ogni $\alpha \preceq \beta \in \mu$ si abbia $H_\alpha \leq H_\beta$ per le serie ascendenti, $H_\alpha \geq H_\beta$ per quelle discendenti.

Dalla definizione di serie allora abbiamo per le serie ascendenti

- $H_\alpha \lhd H_{\alpha+1}$ e i due termini sono consecutivi in Σ;
- $H_\lambda = \bigcup_{\alpha \prec \lambda} H_\alpha$ se $\lambda \in \mu$ fosse un ordinale limite.

e per le serie discendenti

- $H_{\alpha+1} \lhd H_\alpha$ e i due termini sono consecutivi in Σ;
- $H_\lambda = \bigcap_{\alpha \prec \lambda} H_\alpha$ se $\lambda \in \mu$ fosse un ordinale limite.

Per le serie ascendenti dovrà necessariamente esistere $\eta \in \mu$ tale che $\bigcup_{H \in \Sigma} H = H_\eta$, tale elemento sarà necessariamente il più grande dell'intera serie e quindi possiamo porre senza perdere in generalità che $\mu = \eta + 1$ e quindi la nostra serie ascendente avrà la seguente forma

$$H_0 \lhd H_1 \lhd H_2 \lhd \cdots H_\omega \lhd H_{\omega+1} \lhd \cdots H_\eta$$

Stesso ragionamento per le serie discendenti, solo che qui i versi saranno invertiti

$$H_0 \rhd H_1 \rhd H_2 \rhd \cdots H_\omega \rhd H_{\omega+1} \rhd \cdots H_\eta$$

Il principio di induzione transfinita permette di definire una serie ascendente o discendente semplicemente a partire dall'ordinale minimo e sugli ordinali successori, dato che per gli ordinali limiti saranno unione/intersezioni degli elementi precedenti all'interno della serie.

Possiamo adesso definire alcune serie di gruppi che saranno molto utili più avanti. Innanzitutto sia G gruppo e $H \leq G$, definiamo per ogni ordinale α le quantità

$$\begin{cases} H^{G,0} = G \\ H^{G,\alpha+1} = H^{H^{G,\alpha}} \\ H^{G,\alpha} = \bigcap_{\beta \prec \alpha} H^{G,\beta} & \text{se } \alpha \text{ è ordinale limite} \end{cases}$$

Se ci fermiamo ad un ordinale prefissato otteniamo una serie discendente detta *serie delle chiusure normali* di H in G in quanto $H \leq H^{G,\alpha}$ e $H^{G,\alpha+1} = H^{H^{G,\alpha}} \lhd H^{G,\alpha}$ per ogni α ordinale.

Proposizione 3.4.3. *Se $H \operatorname{sn} G$ e $G = H_0 \rhd H_1 \rhd \cdots \rhd H_n = H$ allora per ogni $i \in \mathbb{N}$*

$$H \leq H^{G,i} \leq H_i$$

e quindi la serie delle chiusure normali è la più corta serie congiungente G ad H. Perciò la sua lunghezza coincide con il difetto di H in G.

Dimostrazione. Useremo l'induzione classica, dato che la serie H_i termina dopo un numero finito di addendi. Chiaramente $H_0 = G = H^{G,0}$ e supponiamo che valga $H^{G,i} \leq H_i$ per un certo $i \in \mathbb{N}$. Poiché $H \leq H_{i+1} \lhd H_i$

$$H^{G,i+1} = \left\langle H^x \;\middle|\; x \in H^{G,i} \right\rangle \leq \langle H^x \mid x \in H_i \rangle = H^{H_i} \leq H_{i+1}$$

e quindi per induzione vale l'asserto. ∎

Definizione 3.4.4. Sia G gruppo, definiamo la *serie derivata* di G per induzione come

$$\begin{cases} G^{(0)} = G \\ G^{(\alpha+1)} = \left[G^{(\alpha)}; G^{(\alpha)}\right] \\ G^{(\alpha)} = \bigcap_{\beta \prec \alpha} G^{(\beta)} & \text{se } \alpha \text{ è ordinale limite} \end{cases}$$

Proposizione 3.4.5. *Per ogni α ordinale $G^{(\alpha)}$ è pienamente invariante in G.*
In particolare è una serie normale.

Dimostrazione. Se $\alpha = 0$ allora l'asserto è vero. Se $G^{(\alpha)}$ è pienamente invariante allora anche $G^{(\alpha+1)}$ lo è per via della proposizione 3.3.6 mentre se α è un ordinale limite e $G^{(\lambda)}$ è pienamente invariante per ogni $\lambda \prec \alpha$ allora per ogni endomorfismo $f : G \to G$

$$f\left(G^{(\alpha)}\right) = f\left(\bigcap_{\lambda \prec \alpha} G^{(\lambda)}\right) \leq \bigcap_{\lambda \prec \alpha} f\left(G^{(\lambda)}\right) \leq \bigcap_{\lambda \prec \alpha} G^{(\lambda)} = G^{(\alpha)}$$

per ipotesi induttiva. ∎

La serie derivata inoltre ha i fattori abeliani per quanto visto prima.

Proposizione 3.4.6. *Sia $G = G_0 \rhd G_1 \rhd G_2 \rhd \cdots G_\eta$ una serie abeliana discendente, allora per ogni ordinale α*

$$G^{(\alpha)} \leq G_\alpha$$

Quindi G è risolubile se e solo se esiste $n \in \mathbb{N}$ tale che $G^{(n)} = \{1\}$.

Dimostrazione. Usiamo l'induzione transfinita, ci sta da verificare solo il caso di ordinali successori. Supponiamo allora che $G^{(\alpha)} \leq G_\alpha$ per un opportuno α allora $G_{\alpha+1} \lhd G_\alpha$ e $G_\alpha/G_{\alpha+1}$ è abeliano.

Applicando la proposizione 3.3.16 segue immediatamente che

$$G^{(\alpha+1)} = \left[G^{(\alpha)}; G^{(\alpha)}\right] \leq [G_\alpha; G_\alpha] \leq G_{\alpha+1}$$

concludendo la dimostrazione. ■

Definizione 3.4.7. Sia G gruppo, definiamo la *serie centrale inferiore* di G per induzione come

$$\begin{cases} \gamma_1(G) = G \\ \gamma_{\alpha+1}(G) = [\gamma_\alpha(G); G] \\ \gamma_\alpha(G) = \bigcap_{\beta\prec\alpha} \gamma_\beta(G) & \text{se } \alpha \text{ è ordinale limite} \end{cases}$$

Definizione 3.4.8. Sia G gruppo, definiamo la *serie centrale superiore* di G per induzione come

$$\begin{cases} Z_0(G) = \{1\} \\ \frac{Z_{\alpha+1}(G)}{Z_\alpha(G)} = Z\left(\frac{G}{Z_\alpha(G)}\right) \\ Z_\alpha(G) = \bigcup_{\beta\prec\alpha} Z_\beta(G) & \text{se } \alpha \text{ è ordinale limite} \end{cases}$$

La serie centrale superiore è una serie ascendente (può essere sempre completata ad una serie) mentre quella inferiore è discendente. Entrambe sono serie centrali e quella inferiore è anche pienamente invariante.

Se esiste il massimo della serie centrale superiore $\overline{Z}(G)$ esso sarà l'*ipercentro* di G e varrà

$$Z\left(\frac{G}{\overline{Z}(G)}\right) = \{\overline{Z}(G)\}$$

Proposizione 3.4.9. *Sia $G = G_1 \rhd G_2 \rhd \cdots G_\eta$ una serie centrale discendente, allora per ogni ordinale α*

$$\gamma_\alpha(G) \leq G_\alpha$$

Dimostrazione. Usiamo l'induzione transfinita, ci sta da verificare solo il caso di ordinali successori. Supponiamo allora che $\gamma_\alpha(G) \leq G_\alpha$ per un opportuno α allora $G_{\alpha+1} \lhd G$ e $G_\alpha/G_{\alpha+1} \leq Z\left(G/G_{\alpha+1}\right)$.

Applicando la proposizione 3.3.16 segue immediatamente che

$$\gamma_{\alpha+1}(G) = [\gamma_\alpha(G); G] \leq [G_\alpha; G] \leq G_{\alpha+1}$$

concludendo la dimostrazione. ■

Proposizione 3.4.10. *Sia $\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots G_\eta$ una serie centrale ascendente, allora per ogni ordinale α*

$$G_\alpha \leq Z_\alpha(G)$$

Dimostrazione. Usiamo l'induzione transfinita, ci sta da verificare solo il caso di ordinali successori. Supponiamo allora che $G_\alpha \leq Z_\alpha(G)$ per un opportuno α allora $G_\alpha \lhd G$ e $G_{\alpha+1}/G_\alpha \leq Z\left(G/G_\alpha\right)$.

Applicando la proposizione 3.3.16 e la 3.3.10

$$[G; G_{\alpha+1}Z_{\alpha+1}(G)] = [G; G_{\alpha+1}]\,[G; Z_{\alpha+1}(G)] \leq G_\alpha Z_\alpha(G) \leq Z_\alpha(G)$$

e quindi

$$\frac{G_{\alpha+1}Z_{\alpha+1}(G)}{Z_\alpha(G)} \leq Z\left(\frac{G}{Z_\alpha(G)}\right) = \frac{Z_{\alpha+1}(G)}{Z_\alpha(G)} \Rightarrow G_{\alpha+1} \leq Z_{\alpha+1}$$

concludendo la dimostrazione. ■

Osserviamo che per ogni $i \in \mathbb{N}$ si ha $\gamma_i(G) = [G; G; \dots; G]$ dove la G compare n volte. Vale inoltre il seguente risultato

Proposizione 3.4.11. *Per ogni $i \in \mathbb{N}$ si ha*

$$\gamma_i(G) = \langle [g_1; g_2; \dots; g_i] \mid g_j \in G \textit{ per ogni } 1 \leq j \leq i \rangle$$

Dimostrazione. Per $i = 1$ o 2 è banale, supponiamolo valido per un certo n allora posto $X = \{[g_1; g_2; \dots; g_i] \mid g_j \in G \text{ per ogni } 1 \leq j \leq i\}$ dal lemma 3.3.11 segue che

$$\gamma_{i+1}(G) = [\gamma_i(G); G] = [X; G]^{\gamma_i(G)}$$

Inoltre osserviamo che

$$[x_1; \dots; x_{i+1}]^g = \left[x_1^g; \dots; x_{i+1}^g\right] \in [X; G]$$

quindi il sottogruppo è normale e la tesi dimostrata. ■

per questo motivo si chiamano rispettivamente serie centrale inferiore e superiore.

Dimostriamo ora altre proprietà della serie derivata e della centrale e superiore

Teorema 3.4.12. *Sia G gruppo allora per ogni i, j interi*

1. $[\gamma_i(G); \gamma_j(G)] \leq \gamma_{i+j}(G)$;
2. $\gamma_i\left(\gamma_j(G)\right) \leq \gamma_{ij}(G)$;
3. *Se $i \leq j$ allora* $[\gamma_i(G); Z_j(G)] \leq Z_{j-i}(G)$;
4. $Z_i\left(G/Z_j(G)\right) = Z_{i+j}(G)/Z_j(G)$;
5. $G^{(i)} \leq \gamma_{2^i}(G)$.

Dimostrazione. Dimostriamo i vari punti tramite l'induzione.

1. È chiaramente verificato per $i = 1$ e per ogni $j \in \mathbb{N}$, supponiamola vera per un certo $i \in \mathbb{N}$ allora $[\gamma_{i+1}(G); \gamma_j(G)] = [\gamma_i(G); G; \gamma_j(G)]$. Ora
$$[\gamma_j(G); \gamma_i(G); G] \leq [\gamma_{i+j}; G] = \gamma_{i+j+1}(G)$$
$$[G; \gamma_j(G); \gamma_i(G)] \leq [\gamma_{j+1}; \gamma_i(G)] \leq \gamma_{i+j+1}(G)$$
poiché $\gamma_{i+j+1}(G) \lhd G$ dal lemma dei tre sottogruppi segue la tesi.

2. Anche qui per $i = 1$ e j generico è banale, quindi supponiamolo vero per un certo i allora dal punto precedente
$$\gamma_{i+1}(\gamma_j(G)) = [\gamma_i(\gamma_j(G)); \gamma_j(G)] \leq [\gamma_{ij}(G); \gamma_j(G)] \leq \gamma_{(i+1)j}(G)$$

3. L'inclusione è verificata per $i = 1$ difatti essendo $Z_j(G)$ centrale abbiamo chiaramente $[G; Z_j(G)] \leq Z_{j-1}(G)$. Supponendola valida per un certo i e per ogni $j' \geq i$ allora preso $j \geq i + 1$ abbiamo
$$[G; Z_j(G); \gamma_i(G)] \leq [Z_{j-1}(G); \gamma_i(G)] \leq Z_{j-i-1}(G)$$
$$[Z_j(G); \gamma_i(G); G] \leq [Z_{j-i}(G); G] \leq Z_{j-i-1}(G)$$
e quindi dal lemma dei tre sottogruppi abbiamo
$$[\gamma_{i+1}(G); Z_j(G)] = [\gamma_i(G); G; Z_j(G)] \leq Z_{j-i-1}(G)$$

4. Per $i = 0, 1$ è banale, supponiamolo verificato allora per un certo $i \geq 1$ allora posto $Z_{i+1}(G/Z_j(G)) = K/Z_j(G)$ abbiamo
$$\frac{K/Z_j(G)}{Z_{i+j}(G)/Z_j(G)} = \frac{K/Z_j(G)}{Z_i(G/Z_j(G))} = Z\left(\frac{G/Z_j(G)}{Z_i(G/Z_j(G))}\right) = Z\left(\frac{G/Z_j(G)}{Z_{i+j}(G)/Z_j(G)}\right)$$
e quindi applicando l'isomorfismo canonico
$$\frac{K}{Z_{i+j}(G)} = Z\left(\frac{G}{Z_{i+j}(G)}\right)$$
e quindi $K = Z_{i+j+1}(G)$.

5. Se $i = 0$ è banale, altrimenti
$$G^{(i+1)} = \left[G^{(i)}; G^{(i)}\right] \leq [\gamma_{2^i}(G); \gamma_{2^i}(G)] \leq \gamma_{2^{i+1}}(G)$$

■

Proposizione 3.4.13. *Sia G gruppo generico ed $N \lhd G$ allora per ogni $i \in \mathbb{N}_0$*
$$\gamma_{i+1}\left(\frac{G}{N}\right) = \frac{\gamma_{i+1}(G)N}{N}$$

Dimostrazione. È banale per $i = 0$, supponendolo vero per $i - 1$ allora
$$\gamma_{i+1}\left(\frac{G}{N}\right) = \left[\gamma_i\left(\frac{G}{N}\right); \frac{G}{N}\right] = \left[\frac{\gamma_i(G)N}{N}; \frac{G}{N}\right] = \frac{[\gamma_i(G); G]\, N}{N} = \frac{\gamma_{i+1}(G)N}{N}$$
dove abbiamo usato la proposizione 3.3.1 per portare il quoziente fuori. ■

Capitolo 4

Gruppi nilpotenti

4.1 Il teorema di Fitting

In questa sezione ci dedicheremo interamente allo studio dei gruppi nilpotenti e delle loro proprietà.

Sappiamo già che non tutti i gruppi finiti sono nilpotenti (per esempio S_3) quindi per stabilire se un gruppo finito sia nilpotente o meno bisogna procedere con molta cautela.

Proposizione 4.1.1. *I p-gruppi finiti sono nilpotenti.*

Dimostrazione. Sia G un p-gruppo, allora $|G| = p^n$ per in certo $n \in \mathbb{N}$, dimostreremo il teorema tramite l'induzione su n. Se $n = 1$ allora G è ciclico e quindi nilpotente, altrimenti supponiamolo verificato per ogni intero $m < n$, possiamo supporre anche che $Z(G) < G$. In questo caso ogni elemento di $C = G \setminus Z(G)$ possiederà un elemento coniugato distinto. Esisteranno perciò $a_1, a_2, \ldots, a_n \in C$ tali che $|C_i| = \{a_i^g \mid g \in G\}$ formano una partizione di $G \setminus Z(G)$ e $|C_i| \geq 2$.

Perciò

$$|G| = |Z(G)| + \sum_{i=1}^{n} |C_i|$$

Ricordiamo che $C_G(a_i) = \{g \in G \mid a_i^g = a_i\}$ allora per ogni $x, y \in G$

$$a_i^x = a_i^y \Leftrightarrow a_i = a_i^{yx^{-1}} \Leftrightarrow yx^{-1} \in C_G(a_i) \Leftrightarrow C_G(a_i)\, y = C_G(a_i)\, x$$

allora l'applicazione

$$\eta : a_i^x \in C_i \to C_G(a_i)\, x \in G/R''_{C_G(a_i)}$$

è ben definita e iniettiva. Essendo chiaramente suriettiva allora si ha

$$2 \leq |C_i| = |G : C_G(a_i)| = p^m$$

con $m \in \mathbb{N}$. Ma allora p divide $|Z(G)|$ e quindi $|G/Z(G)| < |G|$ e quindi per induzione avremo una serie centrale

$$\{Z(G)\} = H_0/Z(G) \lhd H_1/Z(G) \lhd \cdots \lhd H_l/Z(G) = G/Z(G)$$

Per una osservazione fatta nel capitolo precedente anche la serie

$$\{1\} \lhd Z(G) = H_0 \lhd H_1 \lhd \cdots \lhd H_l = G$$

è centrale e perciò $G \in \mathcal{N}$. ■

Prima di dimostrare risultati più avanzati sui gruppi nilpotenti abbiamo bisogno di questi risultati

Teorema 4.1.2. *Se G è finitamente generato e sia $H \leq G$ tale che $|G : H| < \infty$ allora anche H è finitamente generato.*

Dimostrazione. Poniamo $G/R'_H = \{t_1H, t_2H, \ldots, t_nH\}$ e $X \subseteq G$ finito tale che $G = \langle X \rangle$. Per comodità poniamo $t_1 = 1$ e definiamo l'applicazione $f : I_n \times G \to I_n$, dove $I_n = \{1, 2, \ldots, n\}$, tale che

$$t_{f(i,g)}H = gt_iH$$

che è ben definita in quanto formano una partizione.

Chiaramente $f(i, 1) = i$ per ogni $i \in I_n$ e per ogni $g, g' \in G$

$$t_{f(i,gg')}H = gg't_iH = gt_{f(i,g')}H = t_{f(f(i,g'),g)}H \Leftrightarrow f(i, gg') = f\left(f(i, g'), g\right)$$

e quindi, fissato g, è biiettiva con $f^{-1}(x, g) = f\left(i, g^{-1}\right)$.

Possiamo definire un'altra applicazione $h : I_n \times G \to H$ tale che

$$gt_i = t_{f(i,g)}h(i, g) \Leftrightarrow h(i, g) = t^{-1}{}_{f(i,g)}gt_i$$

Vogliamo dimostrare che

$$H = \left\langle h(i, g) \;\middle|\; i \in I_n \text{ e } g \in X \cup X^{-1} \right\rangle$$

Osserviamo che se $a \in H$ allora $f(1, a) = 1$ e perciò $h(1, a) = a$ quindi possiamo scrivere $H = \langle h(1, g) \mid g \in G\rangle$, ma la dimostrazione non può dirsi ancora conclusa, difatti bisogna ancora mostrare che per ogni $i \in I_n$ e $g, g' \in G$

$$\begin{aligned} h(i, gg') &= t^{-1}{}_{f(i,gg')}gg't_i = t^{-1}{}_{f(i,gg')}gt_{f(i,g')}t^{-1}{}_{f(i,g')}g't_i \\ &= t^{-1}{}_{f(f(i,g'),g')}gt_{f(i,g')}h(i, g') = h\left(f(i, g'), g\right)h(i, g') \end{aligned}$$

e quindi se $h = g_1g_2 \cdots g_m \in H$ con $g_i \in X \cup X^{-1}$ allora

$$h = h(1, h) = h(t_1, g_1) \cdots h(t_m, g_m)$$

per opportuni $t_i \in I_n$ e $h(t_i, g_i) \in H$. ■

Enunciamo il seguente teorema senza però dimostrarlo

Teorema 4.1.3 (Schur-Zassenhaus)**.** *Se G è un gruppo finito e $N \lhd G$ tale che*

$$\gcd(|N|, |G : N|) = 1$$

allora esiste $K \leq G$ tale che $G = K \ltimes N$.

Teorema 4.1.4 (Schur)**.** *Se $G/Z(G)$ è finito allora anche G' è finito.*

Dimostrazione. Sia $G/Z(G) = \{x_1 Z(G), \ldots, x_n Z(G)\}$ e poniamo $K = \langle x_1, \ldots, x_n \rangle$ quindi $G = KZ(G)$. Ora poiché $K \leq N_G(K)$ e $Z(G) \leq N_G(K)$ allora $K \lhd G$ e dal lemma 3.3.15 si ha $G' = K'Z(G)'[K; Z(G)] = K'$. Ancora il quoziente $G/Z(G) \cong K/(K \cap Z(G))$ è finito e tramite l'epimorfismo

$$: x(Z(G) \cap K) \to xZ(K)$$

segue che anche $K/Z(K)$ è finito.

Quindi se riusciamo a dimostrare il teorema nel caso in cui G sia *finitamente generato* allora seguirà immediatamente anche il caso generale. Supponiamo perciò che G sia finitamente generato, dal teorema 4.1.2 anche $Z(G)$ è finitamente generato e abeliano, quindi dal teorema di struttura dei gruppi abeliano Max abbiamo $Z(G) = A \otimes T$ con A prodotto diretto di un numero finito di ciclici infiniti e T finito.

Il centro è caratteristico in G per cui $A \leq Z(G) \Rightarrow A \lhd G$ e

$$|G : A| = |G : Z(G)|\,|Z(G) : A| = |G : Z(G)|\,|T| = m \in \mathbb{N}$$

e scegliamo allora $p > m$ numero primo e $n \in \mathbb{N}$ generico. Se $A = \langle a_1 \rangle \otimes \cdots \otimes \langle a_i \rangle$ allora ragionando sui fattori $\left|A : A^{p^n}\right| = p^{ni}$ e ancora

$$G/A \cong \frac{G/A^{p^n}}{A/A^{p^n}}$$

Ora concentriamoci sugli ordini. Chiaramente p non può dividere l'intero $|G : A| = \left|G/A^{p^n} : A/A^{p^n}\right|$ e allora possiamo applicare Schur-Zassenhaus ottenendo

$$G/A^{p^n} = K_n/A^{p^n} \ltimes A/A^{p^n} \Rightarrow G = K_n A = K_n Z(G)$$

Sempre per quanto detto sopra $K_n \lhd G$ e inoltre $K_n \cap A = A^{p^n}$ per ogni $n \in \mathbb{N}$ e quindi il prodotto semidiretto in realtà è diretto. Perciò

$$G/K_n \cong \frac{G/A^{p^n}}{K_n/A^{p^n}} \cong A/A^{p^n} \text{ abeliano}$$

applicando il corollario 3.3.17 $G' \leq K_n$ per ogni $n \in \mathbb{N}$ e quindi $G' \cap A \leq \bigcap_{n=1}^{+\infty} A^{p^n} = \{1\}$ e infine

$$G' \cong G'A/A \leq G/A$$

che è finito. ∎

Il nostro scopo in questa sezione è la dimostrazione del teorema di Fitting ovvero una versione del corollario 3.2.11 per i gruppi nilpotenti. Dimostriamo ancora qualche risultato sui gruppi nilpotenti.

Proposizione 4.1.5. *Se $G \in \mathfrak{N}$ e $\{1\} \neq N \lhd G$ allora $N \cap Z(G) \neq \{1\}$.*

Dimostrazione. Sappiamo che esisterà $n \in \mathbb{N}$ tale che $Z_n(G) = G$ e quindi $N \cap Z_n(G) \neq \{1\}$. Possiamo allora definire

$$m = \min \{n \in \mathbb{N} \mid N \cap Z_n(G) \neq \{1\}\} > 0$$

Quindi $Z_{m-1}(G) \cap N = \{1\}$ ma $[G; N \cap Z_m(G)] \leq Z_{m-1}(G) \cap N = \{1\}$ e perciò $Z_m(G) \cap N \leq Z(G)$ e quindi $N \cap Z(G) \neq \{1\}$. ∎

Corollario 4.1.6. *Se G è nilpotente e $N \underset{min}{\lhd} G$ allora $N \leq Z(G)$.*

Dimostrazione. Segue dalla proposizione di prima e da $N \cap Z(G) \lhd G$. ∎

Corollario 4.1.7. *Se G è nilpotente e $N \underset{min}{\lhd} G$ allora N è abeliano e non possiede sottogruppi non banali, ovvero è ciclico di ordine primo.*

Proposizione 4.1.8. *Se $G \in \mathcal{N}$ e A è un elemento massimale della classe*

$$\{H \leq G \mid H \textit{ abeliano e } H \lhd G\}$$

allora $A = C_G(A)$.

Dimostrazione. Sia A elemento massimale allora A è abeliano e perciò $A \leq C_G(A)$, poi $A \lhd G$ implica che $C_G(A) \lhd G$.

Se per assurdo $A < C_G(A)$ allora $A \lhd C_G(A)$ e $\{1\} \neq C_G(A)/A \lhd G/A$ e quindi dalla proposizione precedente $C_G(A)/A \cap Z(G/A) \neq \{A\}$. Quindi esisterà un $c \in C_G(A) \setminus A$ tale che per ogni $g \in G$ $[c; g] \in A$ e consideriamo il sottogruppo $\langle A, c\rangle$, per la definizione di centralizzante questo gruppo è abeliano e quindi $\langle A, c\rangle = A\langle c\rangle$ e

$$\langle A, c\rangle/A = A\langle c\rangle/A = \langle cA\rangle \leq Z(G/A)$$

e quindi $A\langle c\rangle \lhd G$ raggiungendo così un assurdo. ∎

Proposizione 4.1.9. *Se $M, N \lhd G$ allora per ogni $i \in \mathbb{N}$*

$$\gamma_i(MN) = \langle [X_1; X_2; \ldots ; X_i] \mid X_j \textit{ coincide con } M \textit{ o } N \textit{ per ogni } j\rangle$$

Dimostrazione. Se $i = 1$ allora $\gamma_1(MN) = MN = [M][N]$ mentre se $i = 2$ segue dal lemma 3.3.15. Supponiamo l'asserto valido per $i \geq 2$ allora

$$\begin{aligned}\gamma_{i+1}(MN) = [\langle [X_1; X_2; \ldots ; X_i]\rangle; MN] &= \left[\prod [X_1; X_2; \ldots ; X_i]; MN\right] \\ &= \prod [[X_1; X_2; \ldots ; X_i]; M] \prod [[X_1; X_2; \ldots ; X_i]; N]\end{aligned}$$

per la proposizione 3.3.10. ∎

Teorema 4.1.10 (Fitting)**.** *Sia G generico e $M, N \lhd G$ tali che $M, N \in \mathcal{N}$. Allora $MN \in \mathcal{N}$ e*

$$\mathrm{cl}(MN) \leq \mathrm{cl}(M) + \mathrm{cl}(N)$$

Dimostrazione. Sia $c = \mathrm{cl}(M)$ e $d = \mathrm{cl}(N)$ allora $\{1\} = [M; M; \dots; M]$ che compare $c+1$ volte e $\{1\} = [N; N; \dots; N]$ che stavolta la N compare $d+1$ volte.

Dalla proposizione precedente $\gamma_{c+d+1}(MN)$ è generato da $[X_1; X_2; \dots; X_{c+d+1}]$ dove X_i coincide con M o N a seconda dei casi. Per il principio della piccionaia o la M compare almeno $c+1$ volte oppure N compare almeno $d+1$ volte in uno di questi interderivati.

Supponiamo di trovarci nel primo caso, dimostriamo che $[X_1; X_2; \dots; X_{c+d+1}] = \{1\}$ e per farlo ne riduciamo la lunghezza in modo da togliere tutti gli N che compaiono. Se per esempio abbiamo $[N; N; M; \dots]$ possiamo applicare la proposizione 3.3.7 per mostrare che $[N; N; M] \leq M$ e

$$[N; N; M; \dots] = [[N; N; M]; \dots] \leq [M; \dots]$$

eliminando così le due N iniziali. Se ora invece ci troviamo nel caso $[M; M; M; N \dots]$ allora sappiamo già che $[M; M; M] \lhd G$ e quindi

$$[M; M; M; N \dots] = [[[M; M; M]; N] \dots] \leq [M; M; M \dots]$$

eliminando così la N.

Procedendo in tal modo avremo che $\gamma_{c+d+1}(MN) \leq [M; M; M; \dots; M] = \{1\}$. Procedimento del tutto analogo anche nel secondo caso. ■

Corollario 4.1.11. *Nelle stesse ipotesi del teorema di fitting con la condizione aggiuntiva che $M \cap N = \{1\}$, ovvero $\langle M, N\rangle = M \otimes N$, allora*

$$\mathrm{cl}(MN) \leq \max\{\mathrm{cl}(M), \mathrm{cl}(N)\}$$

Dimostrazione. Discende immediatamente che se un interderivato $[X_1; X_2; \dots; X_n]$ compaiono all'interno sia M che N allora sarebbe contenuto sia in M che in N e quindi anche nella loro intersezione. Per questo motivo nella dimostrazione precedente possiamo fermarci all'indice $\max\{\mathrm{cl}(M), \mathrm{cl}(N)\}$ come il lettore può verificare. ■

Il teorema di Fitting può essere generalizzato nella seguente maniera

Teorema 4.1.12 (Fitting generalizzato)**.** *Sia G gruppo generico e $H, K \leq G$ nilpotenti con $H \operatorname{sn} G$ e $K \lhd G$. Allora HK è nilpotente.*

Dimostrazione. Essendo K normale allora HK è un sottogruppo di G e $H \operatorname{sn} HK$, utilizziamo allora l'induzione sulla lunghezza minima d della serie da H a HK. Se $d = 0$ allora $H = HK$ mentre se $d = 1$ allora $H \lhd HK$ e quindi dal teorema di Fitting classico HK è nilpotente.

Supponiamo l'asserto vero per ogni $1 \leq d' < d$ allora per i risultati sulla serie delle chiusure normali il difetto di H in H^{HK} vale esattamente $d-1$ e inoltre $H^{HK} = H^{HK} \cap HK = H\left(H^{HK} \cap K\right)$ e chiaramente $H^{HK} \cap K \lhd H^{HK}$.

Per ipotesi induttiva H^{HK} è nilpotente, osserviamo che poiché $H \leq H^{HK} \leq HK$ possiamo scrivere $HK = H^{HK}K$. Poiché $H^{HK} \lhd HK$ e $K \lhd HK$ sono entrambi nilpotenti dal teorema di Fitting anche HK lo è concludendo la dimostrazione. ■

4.2 Caratterizzazione gruppi nilpotenti

Utilizzeremo la notazione $M \lessdot G$ per indicare che M è un sottogruppo massimale ovvero $M < G$ e non esiste alcun L tale che $M < L < G$.

Lemma 4.2.1. *Sia G un gruppo generico e consideriamo le seguenti asserzioni:*

1. *$G \in \mathfrak{N}$;*
2. *Per ogni $H \leq G$ $H \operatorname{sn} G$;*
3. *G verifica la condizione dei normalizzanti ovvero*

$$H < G \Rightarrow H < N_G(H)$$

4. *Se $M \lessdot G$ allora $M \lhd G$.*

allora $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4$.

Dimostrazione. Sia G nilpotente allora la serie centrale superiore è finita. Poniamo $H_n = Z_n(G)H$ allora $H_0 = H$ ed esiste $n \in \mathbb{N}$ tale che $H_n = G$, dimostriamo che $H_i \lhd H_{i+1}$. Chiaramente $Z_i(G)H/Z_i(G) \leq G/Z_i(G)$ e $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ e quindi

$$\frac{Z_{i+1}(G)}{Z_i(G)} \leq N_{G/Z_i(G)}\left(\frac{Z_i(G)H}{Z_i(G)}\right)$$

questo implica che

$$\frac{Z_i(G)H}{Z_i(G)} \lhd \frac{Z_i(G)H}{Z_i(G)}\frac{Z_{i+1}(G)}{Z_i(G)} = \frac{Z_{i+1}(G)H}{Z_i(G)}$$

e quindi $Z_i(G)H \lhd Z_{i+1}(G)H$.

Se $H \operatorname{sn} G$ allora chiaramente $H \operatorname{asc} G$ e quindi $H < N_G(H)$ per quanto detto nel capitolo precedente, mentre se $M \lessdot G$ allora $N_G(M) = G$ e quindi $M \lhd G$. ■

Corollario 4.2.2. *Se G fosse nilpotente e $M \lessdot G$ allora $|G : M|$ è un numero primo*

Dimostrazione. Altrimenti G/M avrebbe un sottogruppo non banale K/M e quindi $M < K < G$. ■

si confronti questo risultato con il corollario 4.1.7.

In generale non è possibile passare dalla 4 alla 1 quindi non è un vero e proprio teorema di caratterizzazione. Nel caso di gruppi *finiti* è invece possibile invertire le implicazioni. Per dimostrarlo abbiamo bisogno di un risultato sui sottogruppi di Sylow

Lemma 4.2.3. *Sia G finito e P un sup p-sottogruppo di Sylow. Se esiste $H \leq G$ tale che $N_G(P) \leq H$ allora*

$$N_G(H) = H$$

Dimostrazione. Dimostriamo che $N_G(H) \leq H$, per farlo prendiamo $x \in N_G(H)$ e quindi $P^x \leq H^x \leq H$. Sia P che P^x sono p-sottogruppi di Sylow di H e dal secondo teorema di Sylow (che vale solo per i gruppi finiti) esiste $h \in H$ tale che $P = P^{xh}$ e quindi $xh \in N_G(P) \leq H \Rightarrow x \in H$. ■

Teorema 4.2.4 (caratterizzazione gruppi nilpotenti finiti)**.** *Sia G gruppo finito, allora le seguenti asserzioni*

1. *$G \in \mathcal{N}$;*
2. *Per ogni $H \leq G$ $H \operatorname{sn} G$;*
3. *G verifica la condizione dei normalizzanti;*
4. *Se $M \lessdot G$ allora $M \lhd G$.*
5. *G è prodotto diretto dei suoi p-sottogruppi di Sylow.*

sono tutte equivalenti.

Dimostrazione. Supponiamo che vale il punto 4. Sia P un p-sottogruppo di Sylow di G, se non fosse normale allora $N_G(P) < G$ ed esisterà $M \lessdot G$ tale che $N_G(P) \leq M$. Dal lemma precedente avremmo che $N_G(M) = M$ ma dal punto 4 $N_G(M) = G$ generando così una contraddizione.

Quindi ogni p-sottogruppo di Sylow di G è normale. Se $|G| = p_1^{m_1} \cdots p_t^{m_t}$ allora dal secondo teorema di Sylow esiste un unico p_i-sottogruppo di Sylow P_i per ogni i e $|P_i| = p_i^{m_i}$ dal primo teorema di Sylow. Quindi sono tutti disgiunti tra loro e perciò

$$|\langle P_1, \dots P_t \rangle| = |P_1 P_2 \cdots P_t| = |P_1| \, |P_2| \cdots |P_t| = |G|$$

e quindi $G = P_1 \otimes \cdots \otimes P_t$.

Viceversa i p gruppi finiti sono sempre nilpotenti come abbiamo visto a inizio capitolo, mentre dal teorema di Fitting segue che se G è prodotto diretto di p-gruppi di Sylow allora anche G è nipotente. ■

Lemma 4.2.5. *Sia G gruppo generico, allora per ogni $i \in \mathbb{N}$ l'applicazione*

$$f_i : \left(a\gamma_{i+1}(G), gG'\right) \in \frac{\gamma_i(G)}{\gamma_{i+1}(G)} \times \frac{G}{G'} \to [a; g] \, \gamma_{i+2}(G) \in \frac{\gamma_{i+1}(G)}{\gamma_{i+2}(G)}$$

è bilineare.

Dimostrazione. Innanzitutto $[\gamma_i(G); G] = \gamma_{i+1}(G)$ e dal teorema 3.4.12 segue immediatamente che $[\gamma_{i+1}(G); G]$, $[\gamma_i(G); G'] \leq \gamma_{i+2}(G)$.

Prendiamo ora $a, a' \in \gamma_i(G)$ e $g, g' \in G$ allora

$$\begin{aligned}\left[aa'; g\right] = [a; g]^{a'} \left[a'; g\right] = [a; g] \left[a; g; a'\right] \left[a'; g\right] \\ = [a; g] \left[a'; g\right] \left[a; g; a'\right]^{[a'; g]} \in [a; g] \left[a'; g\right] \gamma_{i+2}(G)\end{aligned}$$

e

$$\begin{aligned}\left[a;gg'\right] = \left[a;g'\right][a;g]^{g'} = \left[a;g'\right][a;g]\left[a;g;g'\right] \in \left[a;g'\right][a;g][\gamma_i(G);G;G] \\ = \left[a;g'\right][a;g]\,\gamma_{i+2}(G)\end{aligned}$$

quindi l'applicazione è bilineare e inoltre è anche ben definita come è facile da verificare. ■

Questi quozienti sono in realtà abeliani, quindi possiamo applicare il teorema 2.2.2 ed esisterà un unico omomorfismo

$$g_i : \frac{\gamma_i(G)}{\gamma_{i+1}(G)} \otimes \frac{G}{G'} \to \frac{\gamma_{i+1}(G)}{\gamma_{i+2}(G)}$$

dove il prodotto al dominio è il *prodotto tensoriale*, tale che

$$f_i\left(a\gamma_{i+1}(G), gG'\right) = g_i\left(a\gamma_{i+1}(G) \otimes gG'\right)$$

La funzione g_i è anche suriettiva in quanto

$$[a_1;b_1][a_2;b_2]\cdots[a_l;b_l] = g_i\left(a_1 \otimes b_1 + a_2 \otimes b_2 + \cdots + a_l \otimes b_l\right)$$

Dimostreremo ora il seguente risultato sulle classi di gruppi

Teorema 4.2.6 (Robinson)**.** *Sia $\mathcal{X}$ una classe di gruppi chiusa per estensioni e per quozienti di prodotti tensoriali di $\mathcal{X}$-gruppi abeliani.*
Se $G \in \mathfrak{N}$ e $G/G' \in \mathcal{X}$ allora $G \in \mathcal{X}$.

Dimostrazione. Poiché G è nilpotente esisterà $n \in \mathbb{N}$ tale che $\gamma_{n+1}(G) = \{1\}$. Da quanto detto sopra per ogni $i \in \mathbb{N}$ si avrà

$$\frac{\gamma_i(G)/\gamma_{i+1}(G) \otimes G/G'}{\ker g_i} \cong \gamma_{i+1}(G)/\gamma_{i+2}(G)$$

Quindi se $G/G' \in \mathcal{X}$ allora anche $\gamma_2(G)/\gamma_3(G)$ sta in $\mathcal{X}$, e quindi applicando tale concetto una seconda volta avremo $\gamma_3(G)/\gamma_4(G) \in \mathcal{X}$. Procediamo così fino ad arrivare a $\gamma_n(G)/\gamma_{n+1}(G) \cong \gamma_n(G) \in \mathcal{X}$, poiché $\gamma_{n-1}(G)/\gamma_n(G) \in \mathcal{X}$ per la chiusura per estensioni avremo $\gamma_{n-1}(G) \in \mathcal{X}$.

Procedendo a ritroso abbiamo perciò $G \in \mathcal{X}$. ■

Ritorniamo un attimo ai gruppi Max, sappiamo già che un gruppo soddisfa la condizione massimale se e solo se ogni suo sottogruppo è finitamente generato. Se il gruppo è anche abeliano allora basta sapere solamente se l'intero gruppo sia finitamente generato o meno per poter stabilire se si trovi in Max o meno.

Utilizzeremo il teorema di Robinson per dimostrare lo stesso risultato per i gruppi nilpotenti.

Lemma 4.2.7. *Se G è nilpotente e finitamente generato allora è anche* Max*.*

Dimostrazione. Dalla proposizione 2.2.4 il prodotto tensoriale di gruppi abeliani finitamente generati è ancora finitamente generato e abeliano e quindi Max. La classe Max è allora chiusa per quozienti di prodotti tensoriali ed estensioni e quindi possiamo applicare il teorema di Robinson in quanto $G/G' \in \mathrm{Max}$ essendo abeliano. ∎

Sempre applicando la proposizione 2.2.4 al teorema di Robinson abbiamo i seguenti risultati

- Se $G \in \mathcal{N}$ e G/G' è periodico allora G è periodico;
- Se $G \in \mathcal{N}$ e G/G' è finito allora G è finito.

Definizione 4.2.8. Fissato un insieme π contenente numeri primi. Diciamo che $g \in G$ è un π-*elemento* se e solo se $|\langle q \rangle| \in \mathbb{N}$ e tutti i suoi divisori primi stanno in π, mentre G è un π-*gruppo* se e solo se è composto esclusivamente da π-elementi.

Il concetto di π-gruppo generalizza quello di p-gruppo chiaramente. Vogliamo dimostrare che la classe di tutti i π-gruppi, con π fissato, soddisfi le ipotesi richieste dal teorema di Robinson.

Proposizione 4.2.9. *Fissato $\pi \subseteq \mathbb{P}$ la classe dei π-gruppi è chiusa per estensioni e quozienti di prodotti tensoriali.*

Dimostrazione. Sia G gruppo con $N \lhd G$ tale che $N, G/N$ siano π-gruppi. Allora per ogni $g \in G$ esiste $n \in \mathbb{N}$ i cui fattori primi stanno tutti in π tale che $g^n \in N$. Non è importante sapere se n coincida o meno con il suo periodo dato che quest'ultimo ne è un divisore.

Esisterà allora un $m \in \mathbb{N}$ con fattori primi sempre in π tale che $g^{mn} = (g^n)^m = 1$ e quindi g è un π-elemento e G π-gruppo.

Prendiamo ora due π-gruppi abeliani A, B e $K \leq A \otimes B$ dimostriamo che anche $(A \otimes B)/K$ è un π-gruppo. Essendo quest'ultimo abeliano possiamo limitarci allo studio dei suoi generatori $a \otimes b + K$, ma allora esisterà $n \in \mathbb{N}$ con fattori primi in π tale che

$$n\,(a \otimes b + K) = n\,(a \otimes b) + K = (na) \otimes b + K = 0 \otimes b + K = K$$

e quindi i generatori sono π-elementi. ∎

Teorema 4.2.10 (decomposizione gruppi nilpotenti)**.** *Sia $G \in \mathcal{N}$ e consideriamo $T = \{g \in G \mid g \text{ periodico}\}$, allora T è un sottogruppo normale di G.*

Inoltre G/T è senza torsione e $T = \mathrm{Dr}_{p\ primo}\, T_p$ dove T_p è composto da tutti gli elementi di T aventi ordine potenza di p.

Dimostrazione. Dimostriamo innanzitutto che T è un sottogruppo, la normalità poi è immediata da verificare. Per ogni π contenente numeri primi definiamo

$$T_\pi = \langle g \in G \mid g \text{ è un } \pi\text{-elemento} \rangle$$

dalla chiusura per sottogruppi abbiamo $T_\pi \in \mathcal{N}$ mentre T_π/T'_π è un gruppo abeliano generato da π-elementi e quindi un π-gruppo. Dal risultato precedente e dal teorema di Robinson T_π è un π-gruppo e quindi $T_\pi = \{g \in G \mid g \text{ è un } \pi\text{-elemento}\}$. La tesi segue osservando che $T = T_{\mathbb{P}}$.

Dimostriamo ora che T è prodotto diretto delle componenti T_p, sappiamo già che $T_p \lhd T$ e quindi dobbiamo solo dimostrare le altre asserzioni. Per ogni primo p sappiamo già che T_p è l'unico p-sottogruppo di Sylow di G quindi dalla proposizione 1.3.3 $G = \langle T_p \mid p \in \mathbb{P}\rangle$ con $\mathbb{P}$ l'insieme di tutti i numeri primi.

Per dimostrare che $T_p \cap \langle T_q \mid q \neq p \text{ primo}\rangle = \{1\}$ basta osservare che

$$\langle T_q \mid q \neq p \text{ primo}\rangle \leq T_{\mathbb{P}\setminus\{p\}}$$

e che gli elementi in $T_p \cap T_{\mathbb{P}\setminus\{p\}}$ avrebbero due ordini coprimi. ■

Si confronti questo risultato con il teorema di decomposizione per i gruppi abeliani.

4.3 Sottogruppo di fitting e frattini

Definizione 4.3.1. Sia G un gruppo generico, definiamo il suo *sottogruppo di fitting* il sottogruppo

$$\mathrm{FIT}(G) = \langle N \lhd G \mid N \in \mathcal{N}\rangle = \rho_{\mathcal{N}}(G)$$

Segue immediatamente dalle considerazioni iniziali sui radicali che $\mathrm{FIT}(G)$ è caratteristico in G.

Proposizione 4.3.2. *I gruppi risolubili non identici hanno un sottogruppo di fitting non identico*

Dimostrazione. Esiste $n \in \mathbb{N}$ tale che $G^{(n+1)} = \{1\}$ e $G^{(n)} \neq \{1\}$. Il lettore può verificare che $G^{(n)} \leq \mathrm{FIT}(G)$. ■

Proposizione 4.3.3. $x \in \mathrm{FIT}(G) \Leftrightarrow \langle x\rangle^G \in \mathcal{N}$

Dimostrazione. Sia $x \in \mathrm{FIT}(G)$ allora esistono $G_1, G_2, \ldots, G_n \lhd G$ nilpotenti tali che $x \in G_1G_2\cdots G_n$. Ma $G_1G_2\cdots G_n \lhd G$ e dal teorema di Fitting $G_1G_2\cdots G_n \in \mathcal{N}$ quindi $H = G_1G_2\cdots G_n$ è nilpotente. Allora $\langle x\rangle^G \leq H$ e dalla chiusura per sottogruppi si ha la tesi. ■

Corollario 4.3.4. *Se G è un gruppo generico allora* $\mathrm{FIT}(G) \in L\mathcal{N}$.

Dimostrazione. Sia $H = \langle x_1, x_2, \ldots, x_n\rangle \leq \mathrm{FIT}(G)$ allora per quanto detto sopra $H \leq {x_1}^G {x_2}^G \cdots {x_n}^G \in \mathcal{N}$ e la tesi segue per la chiusura per sottogruppi. ■

Definizione 4.3.5. Sia G gruppo, diciamo che $G \in$ Max-n se e solo se la classe $\{H \lhd G\}$ soddisfa la condizione massimale, analogamente definiamo Min-n.

Chiaramente Max $\subseteq$ Max-n e Min $\subseteq$ Min-n.

Proposizione 4.3.6. *Le classi* Max-n *e* Min-n *sono chiuse per quozienti ed estensioni.*

Dimostrazione. Il procedimento è lo stesso per i casi Max e Min. ■

Le classi Max-n e Min-n non sono però chiuse per sottogruppi come vedremo più avanti.

Proposizione 4.3.7. *Se* $G \in$ Max-n *allora* $\text{FIT}(G) \in \mathcal{N}$.

Dimostrazione. La classe di sottogruppi $\{N \lhd G \mid N \in \mathcal{N}\}$ possiede un elemento massimale L e quindi $L \leq \text{FIT}(G)$.

Se per assurdo fosse $L < \text{FIT}(G)$ esisterebbe un $x \in \text{FIT}(G) \setminus L$ e dal teorema di Fitting $L\langle x\rangle^G \in \mathcal{N}$. Ancora $L\langle x\rangle^G \lhd G$ e quindi per la massimalità di L dovremmo avere $L = L\langle x\rangle^G$ ovvero $x \in L$ raggiungendo un assurdo. ■

Vogliamo conoscere di più sulla struttura del sottogruppo di fitting, e per farlo dobbiamo dimostrare alcuni risultati preliminari

Proposizione 4.3.8. *Se G è un gruppo finito e $K/H \underset{min}{\lhd} G/H$ allora esiste una serie principale Σ che possiede K/H come fattore (principale).*

Dimostrazione. Innanzitutto osserviamo che $\{H, K, G\}$ è una serie normale e quindi la classe

$$\{\mathcal{L} \text{ contenente sottogruppi di } G \mid \mathcal{L} \text{ è una serie normale contenente } H \text{ e } K\}$$

è non vuota.

Poiché G è finito anche questa classe è finita per cui possiederà certamente un elemento massimale Σ, dato che questa serie non possiede dei raffinamenti normali Σ è una serie principale.

Se esistesse $H \lhd K' \lhd K$ con $K' \in \Sigma$ allora $K'/H < K/H$ e $K'/H \lhd G/H$ assurdo. ■

Definizione 4.3.9. Sia G gruppo, $K \lhd G$ e $K \leq H \leq G$, definiamo il sottoinsieme $C_G(H/K)$ in modo tale che

$$\frac{C_G(H/K)}{K} = C_{G/K}\left(\frac{H}{K}\right)$$

Osservazione. Utilizzando la stessa notazione della definizione

$$C_G(H/K) = \{g \in G \mid [g; h] \in K \text{ per ogni } h \in H\} \supseteq C_G(H)$$

Teorema 4.3.10. *Se G è un gruppo finito e $K \leq H \leq G$ con $K \lhd G$ allora*

$$\text{FIT}(G) = \bigcap_{\substack{H/K \\ \textit{fattore principale}}} C_G(H/K)$$

Dimostrazione. Poniamo per comodità $F = \mathrm{FIT}(G)$. Supponiamo inizialmente che $K = \{1\}$ e $H \underset{\min}{\lhd} G$, se per assurdo fosse $[F; H] \neq \{1\}$ allora $[F; H] \lhd G$ e $\leq H$. Quindi $[F; H] = H \leq F$. Essendo i gruppi finiti Max-n allora $F \in \mathcal{N}$ ed esiste $c \in \mathbb{N}$ per cui $\gamma_{c+1}(F) = [F;_c F] = \{1\}$ e inoltre

$$[H;_c F] = H \leq \gamma_{c+1}(G) = \{1\}$$

assurdo. Perciò $[F; H] = \{1\}$ ovvero $F \leq C_G(H)$.

Prendiamo adesso K generico e $H/K \underset{\min}{\lhd} G/K$ applicando il punto precedente abbiamo

$$\mathrm{FIT}\left(\frac{G}{K}\right) \leq \frac{C_G(H/K)}{K}$$

poiché $FK/K \cong F/(F \cap K)$ allora FK/K è nilpotente e normale in G quindi $F \leq C_G(H/K)$.

Prendiamo adesso una serie principale $\{1\} = C_0 \lhd C_1 \lhd \cdots \lhd C_t = G$ (il gruppo è finito quindi anche la serie è finita) allora $C_{i+1}/C_i \underset{\min}{\lhd} G/C_i$ e poniamo

$$I = \bigcap_{i=1}^{t} C_G(C_i/C_{i-1}) \lhd G$$

Allora la serie $C_i \cap I$ è ancora normale. Ora osserviamo che

$$[C_{i+1} \cap I; I] \leq [C_{i+1} \cap I; C_G(C_{i+1}/C_i)] \leq C_i$$

e quindi è anche una serie centrale. Perciò $I \in \mathcal{N}$ e $I \leq F$. ■

Definizione 4.3.11. Prendiamo un gruppo G, definiamo il suo *sottogruppo di frattini* il sottogruppo $\mathrm{Frat}(G)$ definito nella maniera seguente: se G non possiede sottogruppi massimali allora $\mathrm{Frat}(G) = G$ altrimenti

$$\mathrm{Frat}(G) = \bigcap_{M \lessdot G} M$$

Proposizione 4.3.12. *Se G è un gruppo ciclico infinito allora* $\mathrm{Frat}(G) = \{1\}$.

Dimostrazione. Se $G = \langle g \rangle$ è un gruppo ciclico infinito allora un suo sottogruppo M è massimale se e solo se $M = \langle g^p \rangle$ per un qualche p primo. Se $g^m \in \mathrm{Frat}(G)$ allora m deve essere divisibile per ogni primo p ovvero $m = 0$ e $\mathrm{Frat}(G) = \{1\}$. ■

Teorema 4.3.13 (Wielandt)**.** *Se G è un gruppo generico allora*

$$G \in \mathcal{N} \Rightarrow G' \leq \mathrm{Frat}(G)$$

mentre se G fosse anche finito allora avremmo

$$G \in \mathcal{N} \Leftrightarrow G' \leq \mathrm{Frat}(G)$$

Dimostrazione. Basta dimostrare la seguente asserzione per un gruppo generico

$$M \lessdot G \to M \lhd G \Leftrightarrow G' \leq \mathrm{Frat}(G) \tag{4.3.1}$$

così l'implicazione da sinistra a destra segue dal lemma 4.2.1 mentre supponendo G finito possiamo utilizzare il teorema di caratterizzazione dei gruppi nilpotenti finiti.

Dimostriamo prima l'implicazione da sinistra a destra della (4.3.1). Per il corollario 4.2.2 $|G : M|$ è un numero primo quindi G/M è un gruppo abeliano e perciò dal corollario 3.3.17 si ha $G' \leq M$ per ogni $M \lessdot G$.

Viceversa per ogni $M \lessdot G$ abbiamo $G' = [G; G] \leq M$ applicando sempre il corollario 3.3.17 abbiamo $G = N_G(M)$ ovvero $M \lhd G$. ∎

Proposizione 4.3.14. *Se G è un gruppo finitamente generato non identico allora possiede un sottogruppo massimale proprio, ovvero* $\mathrm{Frat}(G) \neq G$.

Dimostrazione. Prendiamo la classe di sottogruppi $\{H < G\}$ con $G = \langle g_1, g_2, \dots g_l\rangle$. Vogliamo dimostrare che possiede elementi massimali e per questo consideriamo un qualunque suo sottoinsieme Υ totalmente ordinato rispetto all'inclusione e consideriamo $K = \bigcup_{H \in \Upsilon} H$. Se per assurdo fosse $K = G$ allora per ogni i esisterebbe $H_i \in \Upsilon$ tale che $g_i \in H_i$, quindi essendo totalmente ordinato avremmo un $H \in \Upsilon$ per cui $g_i \in H$ per ogni i e quindi $G = H$ assurdo.

Quindi $K < G$ ed è perciò un maggiorante. Per il lemma di Zorn esiste $M \lessdot G$ e l'asserto dimostrato. ∎

Definizione 4.3.15. Un elemento $g \in G$ è un *non generatore* se e solo se per ogni $X \subseteq G$ tale che $G = \langle X, g\rangle$ si ha $G = \langle X\rangle$.

Possiamo estendere questo concetto anche per un numero finito di non generatori.

Lemma 4.3.16.

$$\mathrm{Frat}(G) = \{g \in G \mid g \textit{ non generatore}\}$$

Dimostrazione. Sia g un non generatore di G ed $M \lessdot G$. Allora $M \leq \langle M, g\rangle \leq G$ e quindi o $M = \langle M, g\rangle$ oppure $G = \langle M, g\rangle$, nel primo caso $g \in M$ mentre nel secondo per definizione di non generatore avremmo che $M = G$ il che è assurdo.

Viceversa sia $g \in \mathrm{Frat}(G)$ e per assurdo esiste $X \subseteq G$ tale che $G = \langle X, g\rangle$ ma $\langle X\rangle < G$. Per il lemma di Zorn la classe

$$\{H \leq G \mid X \subseteq H \wedge g \notin H\}$$

è non vuota e possiede un elemento massimale M. Per ogni $M < K \leq G$ deve essere $g \in K$ e $X \subseteq M \leq K$ e quindi $K = G$, allora $M \lessdot G$ e G possiede sottogruppi massimali. Però essendo g un elemento del Frattini otterremo un assurdo, quindi g deve necessariamente essere un non generatore. ∎

Proposizione 4.3.17. *Se $N \lhd G$ allora*

$$\frac{\mathrm{Frat}(G)N}{N} \leq \mathrm{Frat}\left(\frac{G}{N}\right)$$

se inoltre $N \lhd \mathrm{Frat}(G)$ allora

$$\frac{\mathrm{Frat}(G)}{N} = \mathrm{Frat}\left(\frac{G}{N}\right)$$

Dimostrazione. Possiamo supporre tranquillamente che G/N possieda un qualche sottogruppo massimale M/N, ma allora $N \leq M \lessdot G$ e quindi

$$\frac{\mathrm{Frat}(G)N}{N} \leq \bigcap_{M \lessdot G} \frac{MN}{N} \leq \bigcap_{\substack{N \leq M \\ M/N \lessdot G/N}} \frac{M}{N} = \mathrm{Frat}\left(\frac{G}{N}\right)$$

Supponiamo adesso che $N \leq \mathrm{Frat}(G)$ e sia $gN \in \mathrm{Frat}\,(G/N)$. Poiché ora $M \lessdot G \Leftrightarrow M/N \lessdot G/N$ abbiamo $g \in M$ per ogni M sottogruppo massimale di G e quindi la tesi. ■

Teorema 4.3.18. *Se G è un gruppo finito allora*

1. *Per ogni $H \leq G$ si ha $\mathrm{Frat}(H)_G \leq \mathrm{Frat}(G)$;*

2. *Se $H \lhd G$ allora $\mathrm{Frat}(H) \leq \mathrm{Frat}(G)$.*

Dimostrazione. Dimostriamo i vari punti

1. Posto $N = \mathrm{Frat}(H)_G \lhd G$ se per assurdo $N \nleq \mathrm{Frat}(G)$ vuol dire che esiste $M \lessdot G$ tale che $N \nleq M$ e quindi per massimalità $MN = G$. Applicando l'identità di Dedekind abbiamo

$$H = H \cap MN = (H \cap M)\,N = \langle H \cap M, N \rangle \Rightarrow H = H \cap M$$

   dato che N è finito e composto interamente da non generatori di H. Quindi $N \leq H \leq M$ assurdo.

2. Il sottogruppo di Frattini è *caratteristico* in quanto un automorfismo manda sempre sottogruppi massimali in sottogruppi massimali. Quindi poiché $H \lhd G$ e $\mathrm{Frat}(H)$ caratteristico in H allora $\mathrm{Frat}(H) \lhd G$ e quindi la tesi.

■

Teorema 4.3.19. *Se G è un gruppo finito e $A \lhd G$ abeliano tale che $A \cap \mathrm{Frat}(G) = \{1\}$ allora esiste $K \leq G$ tale che $G = K \ltimes A$.*

Dimostrazione. Consideriamo la classe finita

$$\{L \leq G \mid LA = G\}$$

esisterà chiaramente un elemento minimale K.

Chiaramente abbiamo $K \cap A \lhd K$ e $K \cap A \lhd A$ per cui $K \cap A \lhd G$, questo ci permette di affermare che se per assurdo $K \cap A \nleq \mathrm{Frat}(G)$ allora per il punto 1 del teorema precedente esiste $M \lessdot K$ tale che $K \cap A \nleq M$. Quindi

$$K = M(K \cap A) \Rightarrow G = M(K \cap A)A = MA$$

e perciò M è un elemento della classe iniziale. Incorriamo così in una contraddizione poiché M è un elemento minimale della stessa.

Quindi

$$K \cap A \leq \mathrm{Frat}(G) \cap A = \{1\}$$

e il prodotto è semidiretto. ∎

Riprendiamo la dimostrazione del teorema di caratterizzazione dei gruppi nilpotenti finiti, osserviamo che se sapessimo già che tutti i p-sottogruppi di Sylow del gruppo finito G fossero normali allora potremmo dimostrare automaticamente che G ne è il prodotto diretto. L'ipotesi di nilpotenza di G serve proprio a dimostrare la normalità di tali sottogruppi.

Proposizione 4.3.20. *Se G è un gruppo finito e P ne è un p-sottogruppo di Sylow allora per ogni $N \lhd G$ anche PN/N è un p-sottogruppo di Sylow di G/N.*

Dimostrazione. Che fosse un p-sottogruppo è immediato da constatare. Per il primo teorema di Sylow $|P| \mid |G|$ e $p\,|P| \nmid |G|$ quindi $|G : P|$ non è divisibile per p.

Inoltre $|PN/N| = |P/(N \cap P)|$ ed è perciò una potenza di p, inoltre

$$|G : P| = |G : PN|\,|PN : P| = |G/N : PN/N|\,|PN : P|$$

Quindi $|G : PN|$ non è divisibile per p e ciò è possibile se e solo se $|PN/N|$ è la più grande potenza di p che divide $|G/N|$ ovvero PN/N è un suo p-sottogruppo di Sylow. ∎

Teorema 4.3.21 (Argomento di Frattini)**.** *Se G è un gruppo generico e $H \lhd G$ un suo sottogruppo finito. Preso un p-sottogruppo di Sylow P di H abbiamo*

$$G = N_G(P)\,H$$

Dimostrazione. Per ogni $g \in G$ P^g è un p-sottogruppo di Sylow di $H^g = H$ e perciò dal secondo teorema di Sylow esiste $h \in H$ tale che $P = P^{gh}$ e quindi $gh \in N_G(P)$. Quindi per ogni $g \in G$ esiste $h \in H$ per cui

$$g = ghh^{-1} \in N_G(P)\,H$$

∎

Teorema 4.3.22 (Goschutz). *Sia G un gruppo finito e $H \lhd G$ per cui* $\mathrm{Frat}(G) \leq H$ *e* $H/\mathrm{Frat}(G) \in \mathcal{N}$ *(abbiamo già dimostrato che il frattini è caratteristico). Allora $H \in \mathcal{N}$.*

Dimostrazione. Poniamo per comodità $F = \mathrm{Frat}(G)$ dimostriamo che i p-sottogruppi di Sylow P di H sono normali, così dal teorema di caratterizzazione segue immediatamente che $H \in \mathcal{N}$.

Dalla proposizione 4.3.20 PF/F è un p-sottogruppo di Sylow di $H/F \in \mathcal{N}$ e dal teorema di caratterizzazione dei gruppi nilpotenti finiti PF/F è caratteristico in H/F (gli automorfismi mandano p-sottogruppi di Sylow in p sottogruppi di Sylow, dal secondo teorema di Sylow e dal teorema di caratterizzazione ve ne sta uno solo).

Allora $PF \lhd G$ e dall'argomento di Frattini $G = N_G(P)\, PF = N_G(P)\, F = N_G(P)$ essendo F finito e composto da non generatori. Quindi $P \lhd G$ per ogni p-sottogruppo di Sylow di H e perciò dal teorema di caratterizzazione $H \in \mathcal{N}$. ■

Corollario 4.3.23. *Se G è un gruppo finito allora* $\mathrm{Frat}(G) \in \mathcal{N}$ *e perciò*

$$\mathrm{Frat}(G) \leq \mathrm{FIT}(G)$$

4.4 G-moduli

Definizione 4.4.1. Sia A un gruppo *abeliano* e G generico. Prediamo anche un'applicazione $* : A \times G \to A$ allora $(A, \cdot, *)$ è un *G-modulo* se e solo se

- $(a * g_1) * g_2 = a * (g_1 g_2)$ per ogni $a \in A$ e $g_1, g_2 \in G$;
- $(a * g)(b * g) = (ab) * g$ per ogni $a, b \in A$ e $g \in G$;
- $a * 1 = a$ per ogni $a \in A$.

Un G-modulo è molto simile ad uno spazio vettoriale. Osserviamo che per ogni $H, K \lhd G$ tali che $H \leq K$ e K/H abeliano allora possiamo renderlo un G-modulo definendo

$$(kH) * g = k^g H$$

Il concetto di G-modulo serve in particolare a poter parlare di coniugio anche quando sarebbe improprio usarli, come nell'esempio mostrato sopra.

Definizione 4.4.2. Preso un G-modulo A

- A è *triviale* se e solo se $a * g = a$ per ogni $a \in A$ e $g \in G$;
- diciamo che $B \leq A$ è un *sottomodulo* di A, e lo indichiamo con $B \leq_G A$, se e solo se per ogni $b \in B \leq A$ e $g \in G$ abbiamo $b * g \in B$;
- A è un G-modulo *politriviale* se e solo se esiste una catena finita di sottogruppi

$$\{0\} = A_0 \leq A_1 \leq \cdots \leq A_t = A$$

tali che $A_i \leq_G A$ e A_{i+1}/A_i (sono tutti abeliani) è un G-modulo triviale rispetto al prodotto esterno

$$p : (aA_i, g) \in \frac{A_{i+1}}{A_i} \times G \to (a * g)\, A_i \in \frac{A_{i+1}}{A_i}$$

ovvero

$$a^{-1}\,(a * g) \in A_i \text{ per ogni } a \in A_{i+1}, g \in G$$

Osservazione. Nell'ultimo punto se $A \lhd G$ abeliano e poniamo $a * g = a^g$ diventa

$$[a; g] \in A_i \text{ per ogni } a \in A_{i+1}, g \in G$$

ovvero $[A_{i+1}; G] \leq A_i$ e perciò $A_{i+1}/A_i \leq Z\,(G/A_i)$ e abbiamo così ottenuto una specie di serie centrale. Difatti non è detto che G/A sia anch'esso abeliano però da una idea dello scopo di questa sezione, ovvero ovviare in qualche misura alla non chiusura per estensioni dei gruppi nilpotenti.

Proposizione 4.4.3. *Prendiamo $H, K \lhd G$ tali che $H \leq K$ e K/H sia abeliano. Dotiamolo della struttura di G-modulo del coniugio allora*

1. *K/H è triviale se e solo se $K/H \leq Z\,(G/H)$;*
2. *$L/H \leq_G K/H$ se e solo se $L \lhd G$ e $H \leq L \leq K$;*
3. *se $L/H \leq_G K/H$ allora anche*
$$\frac{K/H}{L/H}$$
è un G-modulo rispetto al coniugio e quindi anche K/L lo è;
4. *se K/H è un G-modulo politriviale allora $[K_{i+1}/H; G/H] \leq K_i/H$.*

Enunciamo il seguente risultato senza però dimostrarlo

Lemma 4.4.4. *Se A e B sono G-moduli allora anche $A \otimes B$ è un G-modulo tale che per ogni $a \in A$, $b \in B$ e $g \in G$*

$$(a \otimes b) * g = (a * g) \otimes (b * g)$$

Proposizione 4.4.5. *Se A e B sono G-moduli politriviali allora anche $A \otimes B$ è un G-modulo politriviale.*

Dimostrazione. Siano A_i e B_j le relative serie di lunghezza s e t rispettivamente. Definiamo allora

$$T_k = \langle a \otimes b \mid a \in A_i, b \in B_j, i + j \leq k \rangle$$

Chiaramente $T_{s+t} = A \otimes B$, $T_0 = T_1 = \{0\}$ ed è crescente, ed essendo i quozienti dei moduli triviali per ogni $a \in A_{i+1}$, $b \in B_{j+1}$ e $g \in G$ esistono $a' \in A_i$ e $b' \in B$ tali che

$$a * g = a + a' \qquad\qquad b * g = b + b'$$

e quindi per ogni $a \otimes b \in T_{k+1}$

$$(a \otimes b) * g = a \otimes b + a' \otimes b + a \otimes b' + a' \otimes b' \Rightarrow (a \otimes b + T_k) * g = a \otimes b + T_k$$

e quindi anche T_{s+t} è un modulo politriviale. ■

Ancora un ultimo risultato prima di passare al teorema principale

Proposizione 4.4.6. *Se A è un G-modulo politriviale e $B \leq_G A$ allora A/B è un G-modulo politriviale.*

Dimostrazione. Sia A_i la serie politriviale, osserviamo che

$$\frac{A_i B}{B} = \{aB \mid a \in A_i\}$$

quindi $A_i B/B \leq_G A/B$. Inoltre per ogni $a \in A_{i+1}$ esiste $a' \in A_i$ tale che $a * g = aa'$ e quindi

$$(a * gB) \frac{A_i B}{B} = (aB) \left(a'B\right) \frac{A_i B}{B} = (aB) \frac{A_i B}{B}$$

per cui $A_i B/B$ è una serie politriviale di A/B. ■

Teorema 4.4.7 (Philip-Hall)**.** *Sia G gruppo generico, se esiste $N \lhd G$ per cui $N \in \mathcal{N}$ e $G/N' \in \mathcal{N}$ allora $G \in \mathcal{N}$.*

Dimostrazione. Sia $c = \mathrm{cl}(N)$ e quindi $\{1\} = \gamma_{c+1}(N) \leq N'$. Poiché $G/N' \in \mathcal{N}$ esisterà una serie centrale finita $N' = K_0 \lhd K_1 \lhd \cdots \lhd K_n = G$ ovvero

$$[K_{i+1}; G] \leq K_i$$

Posto $N' = K_0 \cap N \lhd \cdots \lhd K_n \cap N = N$ per la normalità di N abbiamo

$$[K_{i+1} \cap N; G] \leq [K_{i+1}; G] \cap [N; G] \leq K_i \cap N$$

in particolare N/N' è un G-modulo politriviale rispetto al coniugio.

Dimostriamo per induzione che $\gamma_i(N)/\gamma_{i+1}(N)$ è un G-modulo politriviale per ogni i. Se $i = 1$ è banale poiché $\gamma_2(N) = N'$, dal lemma 4.2.5 abbiamo dimostrato che

$$\frac{\gamma_i(N)/\gamma_{i+1}(N) \otimes N/N'}{\ker g_i} \cong \gamma_{i+1}(N)/\gamma_{i+2}(N) \tag{4.4.1}$$

dalla proposizione 4.4.5 il prodotto tensoriale di G moduli politriviali è politriviale, mentre da come abbiamo definito la g_i nel lemma 4.2.5 abbiamo

$$g_i\left((a \otimes b)^g\right) = g_i\left(a^g \otimes b^g\right) = [a^g; b^g] = [a; b]^g = (g_i(a \otimes b))^g$$

quindi la g è stabile rispetto al prodotto esterno, per cui sia $\ker g_i$ è un sottomodulo che l'isomorfismo che compare in (4.4.1) è stabile rispetto al prodotto esterno. Quindi dalla proposizione 4.4.6 anche $\gamma_{i+1}(N)/\gamma_{i+2}(N)$ è un G-modulo politriviale.

Da quanto abbiamo detto esisteranno allora per ogni i una serie politriviale

$$\gamma_{i+1}(G) \leq L_0^i \leq L_1^i \leq \cdots \leq L_{n_i}^i = \gamma_i(G)$$

tale che $L_j^i \lhd G$ e $\left[G; L_{j+1}^i\right] \leq L_j^i$.

Dimostriamo ora che G/N è nilpotente, e per farlo riprendiamo la serie K_n definita sopra ma stavolta consideriamo $N = K_0N \lhd K_1N \lhd \cdots \lhd K_nN = G$ e osserviamo che dalla proposizione 3.3.10 poiché $K_i \lhd G$

$$[G; K_{i+1}N] = [G; K_{i+1}]\,[G; N] \leq K_iN$$

e quindi la serie è centrale.

Poiché tutte queste serie sono centrali in G le possiamo incollare tra loro nella seguente maniera

$$G \to N \to N' = \gamma_2(N) \to \gamma_3(G) \to \cdots \to \gamma_{c+1}(N) = \{1\}$$

e perciò $G \in \mathcal{N}$. ■

4.5 Ulteriori risultati sui gruppi nilpotenti

Dimostriamo i seguenti risultati che ci saranno utile nel seguito

Proposizione 4.5.1. *I raffinamenti finiti di una serie centrale finita sono ancora centrali.*

Dimostrazione. Se $H \lhd K$ sono due termini consecutivi di una serie centrale in G allora $[G; K] \leq H$. Se ora prendiamo L tale che $H \leq L \leq K$ allora

$$[G; L] \leq [G; K] \leq H \Rightarrow L/H \leq Z\,(G/H)$$
$$[G; K] \leq H \leq L \Rightarrow K/L \leq Z\,(G/L)$$

e quindi è centrale. ■

Proposizione 4.5.2. *I gruppi risolubili (e quindi anche i nilpotenti) periodici e finitamente generati sono finiti.*

Dimostrazione. Utilizzeremo l'induzione su $d = \mathrm{der}(G)$. Se $d = 1$ allora G è abeliano e quindi la tesi è immediata da verificare altrimenti supponiamola verificata per ogni d' tale che $d \geq d' \geq 1$.

Se $\mathrm{der}(G) = d+1$ allora $A = G^{(d)}$ è abeliano non identico, quindi G/A è finitamente generato, periodico e $\mathrm{der}\,(G/A) \leq d$ per cui G/A è finito. Dal teorema 4.1.2 A è finitamente generato oltre ad essere periodico quindi A è finito. La finitezza è chiaramente chiusa per estensioni e perciò G è finito. ■

Teorema 4.5.3 (Mal'Cev)**.** *Se $Z\,(G)$ è senza torsione allora $Z_{i+1}(G)/Z_i(G)$ è senza torsione per ogni $n \in \mathbb{N}$.*

Dimostrazione. Se $i = 0$ è banale, dimostriamo prima il caso $i = 1$. Sia $xZ(G) \in Z_2(G)/Z(G)$ per cui esiste $m \in \mathbb{N}$ tale che $x^m \in Z(G)$, sapendo che per ogni $g \in G$ abbiamo $[x;g] \in Z(G)$ dalla proposizione 3.3.5 $[x;g]^m = [x^m;g] = 1$ e quindi $x \in Z(G)$.

Supponiamo l'asserto vero per $i \geq 1$ e quindi $Z_{i+1}(G)/Z_i(G)$ è senza torsione, ma allora

$$\frac{Z_{i+2}(G)}{Z_{i+1}(G)} \cong \frac{Z_{i+2}(G)/Z_i(G)}{Z_{i+1}(G)/Z_i(G)} = \frac{Z_2(G/Z_i(G))}{Z(G/Z_i(G))}$$

per ipotesi induttiva $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ è senza torsione per cui applicando il caso $i = 1$ otteniamo la tesi. ■

Proposizione 4.5.4. *Sia G un gruppo nilpotente e finitamente generato, allora G possiede una serie centrale i cui fattori sono o ciclici infiniti o ciclici di ordine primo.*

Se G è anche aperiodico allora tutti i suoi fattori sono ciclici infiniti.

Dimostrazione. Consideriamo una qualunque sua serie centrale $\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$, dal lemma 4.2.7 $G \in \mathrm{Max}$ e quindi dalla proposizione 3.1.3 ogni suo sottogruppo è finitamente generato.

Quindi G_{i+1}/G_i è abeliano e finitamente generato e possiamo perciò applicare il teorema di struttura dei gruppi Max abeliani ovvero

$$\frac{G_{i+1}}{G_i} = \frac{A_1}{G_i} \times \frac{A_2}{G_i} \times \cdots \frac{A_r}{G_i} \times \frac{A_{r+1}}{G_i} \times \cdots \times \frac{A_l}{G_i}$$

dove $\frac{A_j}{G_i}$ è ciclico infinito se $1 \leq j \leq r$ mentre ha ordine primo se $r < j \leq l$. Quindi $G_i \lhd A_j \lhd G_{i+1}$ e possiamo raffinare la nostra serie nella seguente maniera

$$G_i \lhd A_1 \lhd A_1A_2 \lhd \cdots \lhd A_1A_2A_3\cdots A_l = G_{i+1}$$

Per quanto detto sopra anche questo raffinamento è centrale mentre

$$\begin{aligned} \frac{A_1A_2\cdots A_jA_{j+1}}{A_1A_2\cdots A_j} \cong \frac{A_1A_2\cdots A_j/G_i \times A_{j+1}/A_j}{A_1A_2\cdots A_j/G_i} &\cong \frac{A_{j+1}/G_i}{A_{j+1}/G_i \cap A_1A_2\cdots A_j/G_i} \\ &\cong \frac{A_{j+1}}{G_i} \end{aligned}$$

e quindi è ciclico infinito per $0 \leq j < r$ e ciclico di ordine primo per $r \leq j < l$.

Se ora G è senza torsione anche $Z(G)$ è senza torsione, da Mal'Cev i fattori della serie $G_i = Z_i(G)$ sono senza torsione e quindi la fattorizzazione precedente non possiederà fattori ciclici finiti. ■

Teorema 4.5.5 (Dixmer). *Se G è un gruppo nilpotente con $\mathrm{cl}(G) = c$. Supponiamo che $Z(G)$ abbia esponente e finito allora anche G ha esponente finito e per ogni $g \in G$*

$$g^{e^c} = 1$$

e quindi il suo esponente è minore o uguale a e^c.

Dimostrazione. Utilizzeremo l'induzione su $c \in \mathbb{N}$. Se $c = 1$ allora G è abeliano e $G = Z(G)$ altrimenti supponiamo l'asserto vero per $c \geq 1$.

Preso un gruppo G con $\mathrm{cl}(G) = c + 1$ allora $\mathrm{cl}(G/Z(G)) = c$, dobbiamo solo stimare l'esponente di $Z(G/Z(G)) = Z_2(G)/Z(G)$ per poter usare il passo induttivo. Per ogni $x \in Z_2(G)$ e $g \in G$ abbiamo $[x; g] \in Z(G)$ e quindi

$$[x; g]^e = [x^e; g] = 1$$

per l'arbitrarietà di g allora $x^e \in Z(G)$ e quindi l'esponente e' di $Z(G/Z(G))$ è un divisore di e.

Applicando l'ipotesi induttiva per ogni $g \in G$

$$g^{e^c} \in Z(G) \Rightarrow \left(g^{e^c}\right)^e = 1 = g^{e^{c+1}}$$

e quindi la tesi. ■

Se $Z(G)$ fosse semplicemente periodico non potremmo dire che anche G lo è. Esistono difatti gruppi nilpotenti con centro periodico pur non essendolo. Se però G fosse anche finitamente generato allora possiamo mostrare un risultato ben più forte.

Proposizione 4.5.6. *Se G è nilpotente, finitamente generato e $Z(G)$ periodico allora G è finito.*

Dimostrazione. Sempre per il lemma 4.2.7 $G \in \mathrm{Max}$ e quindi il suo centro è finitamente generato, abeliano e periodico. Perciò è finito e per la proposizione precedente G è periodico.

Ora G è un gruppo nilpotente finitamente generato e periodico, per la proposizione 4.5.2 è finito concludendo così la dimostrazione. ■

Capitolo 5

Gruppi risolubili

Nel capitolo precedente ci siamo concentrati nello studio delle proprietà dei gruppi nilpotenti. In particolare abbiamo osservato che per questi gruppi valgono molti dei risultati precedentemente dimostrati per i gruppi abeliani.

In questo capitolo invece ci concentreremo sui gruppi risolubili, ovvero quei gruppi che possiedono una serie abeliana finita. A differenza dei gruppi nilpotenti per i gruppi risolubili non valgono molte proprietà dei gruppi abeliani e quindi il loro studio sarà diverso.

L'unico risultato non banale visto finora sui gruppi risolubili è la proposizione 4.5.2 la quale afferma che ogni gruppo risolubile finitamente generato e periodico è necessariamente finito, come per i gruppi abeliani.

5.1 Gruppi risolubili

Proposizione 5.1.1. *Se $|G| = p^2$ con p primo allora G è abeliano.*

Dimostrazione. Chiaramente G è nilpotente essendo un p-gruppo quindi $Z(G) \neq \{1\}$. Se per assurdo fosse $|Z(G)| = p$ allora $G/Z(G)$ è ciclico. Per un ben noto risultato di teoria dei gruppi G è abeliano raggiungendo un assurdo. ∎

Proposizione 5.1.2. *Se G è risolubile e $N \underset{min}{\lhd} G$ allora N è abeliano.*

Dimostrazione. Chiaramente N è risolubile quindi $N' = [N;N] < N$. Inoltre $N' \lhd G$ e quindi $N' = \{1\}$ ovvero N è abeliano. ∎

Nel capitolo precedente abbiamo dimostrato che ogni p-gruppo finito è nilpotente, e quindi anche risolubile. Il seguente teorema dimostra la risolubilità di una classe piuttosto ampia di gruppi risolubili finiti.

Teorema 5.1.3. *Sia G un gruppo finito, siano inoltre p, q, r primi distinti e $n \in \mathbb{N}$. Se*

$$|G| \in \left\{p^n q, p^2 q^2, pqr\right\}$$

allora G è risolubile.

Dimostrazione. Analizziamo le tre diverse possibilità una alla volta.

Caso $|G| = p^n q$.

Per assurdo G non risolubile e $|G|$ sia il minimo possibile. Allora per ogni $N \lhd G$ avremmo $N, G/N \in \mathcal{S}$, dato che sarebbero o p o q gruppi oppure ricadrebbero nella forma $p^m q$, e quindi $G \in \mathcal{S}$ essendo la risolubilità chiusa per estensioni. Perciò G è semplice ovvero non possiede sottogruppi normali non banali.

Indichiamo con $Syl_p(G)$ l'insieme dei p-sottogruppi di Sylow di G allora, preso un qualunque $P \in Syl_p(G)$, abbiamo dal secondo teorema di Sylow

$$n_p = \left|Syl_p(G)\right| = |G : N_G(P)| = \frac{|G : P|}{|N_G(P) : P|}$$

e quindi $n_p \mid |G : P| = q$, se fosse $n_p = 1$ allora $P \lhd G$ il che è assurdo, perciò $n_p = q$.

Consideriamo ora due casi

- Esistono $P_1, P_2 \in Syl_p(G)$ distinti tali che $P_1 \cap P_2 \neq \{1\}$. Definiamo allora $\mathcal{L} = \left\{P_1 \cap P_2 \mid P_1, P_2 \in Syl_p(G) \text{ e } P_1 \neq P_2\right\}$ e prendiamo $I \in \mathcal{L}$ di ordine massimo e quindi non banale. Esisteranno allora $P_1, P_2 \in Syl_P(G)$ per cui $I = P_1 \cap P_2$ e per ogni $i \in \{1, 2\}$

  $$N_i = N_{P_i}(I)$$

  Sappiamo già che P_i è nilpotente per cui dalla condizione dei normalizzanti $N_i > I$ e quindi

  $$I < J = \langle N_1, N_2 \rangle$$

  Se per assurdo J fosse un p-sottogruppo esisterebbe $P_3 \in Syl_p(G)$ per cui $J \leq P_3$, (se fosse $P_3 = P_1$ allora $N_2 \leq P_1$ e quindi $N_2 \leq I$ assurdo). Quindi

  $$P_1 \cap P_3 \geq N_1 \Rightarrow |P_1 \cap P_3| \geq |N_1| > |I|$$

  andando in contraddizione con la massimalità di I.

  Quindi J non è un p-sottogruppo e dal primo teorema di Sylow esiste $Q \leq J$ tale che $|Q| = q$. Allora

  $$|P_1 Q| = \frac{|P_1|\,|Q|}{|P_1 \cap Q|} = |P_1|\,|Q| = p^n q \Rightarrow P_1 Q = G$$

  inoltre poiché $N_i = N_{P_i}(I) \leq N_G(I) \Rightarrow J \leq N_G(I)$ abbiamo $I \lhd J$ e quindi $I^g = I$ per ogni $g \in Q \leq J$. Da quanto detto sopra $I^G = I^{P_1} \leq P_1$ e quindi $I^G < G$ che va in contrasto con l'ipotesi che G non abbia sottogruppi normali propri.

- Per ogni $P_1, P_2 \in Syl_p(G)$ si ha $P_1 \cap P_2 = \{1\}$. Consideriamo il seguente insieme

  $$S = \{g \in G \setminus \{1\} \mid g \text{ ha ordine potenza di } p\}$$

  ogni elemento di S genera un p-sottogruppo di G per cui sarà contenuto certamente in un p-sottogruppo di Sylow. Poiché $S = \bigcup_i P_i \setminus \{1\}$ e sono disgiunti abbiamo

  $$|S| = q(p^n - 1) \Rightarrow |G \setminus S| = q$$

e quindi esiste un unico q-sottogruppo di Sylow di G il quale sarebbe perciò normale, assurdo.

Caso $|G| = p^2q^2$.

Procediamo per assurdo come nel punto precedente prendendo G di ordina minimo. Allora G deve essere semplice in quanto i suoi possibili sottogruppi normali e quozienti avrebbero ordine $p, q, p^2, pq, q^2, p^2q, pq^2$ che come abbiamo visto prima sono tutti risolubili.

Per comodità sia $p > q$ e $n_p = \left|Syl_p(G)\right|$ dal terzo teorema di Sylow esiste $k \in \mathbb{N}_0$ per cui $n_p = 1 + kp$ e quindi $n_p > p$. Come dicemmo nel punto precedente n_p divide $|G : P| = q^2$ e quindi $n_p = q^2$.

Consideriamo come prima due casi

- Esistono $P_1, P_2 \in Syl_p(G)$ distinti tali che $P_1 \cap P_2 = I \neq \{1\}$. Stavolta poniamo

$$J = \langle P_1, P_2 \rangle$$

  stavolta possiamo applicare la proposizione 5.1.1 e quindi P_i è abeliano. Perciò $I \lhd P_i$ e quindi $I \lhd J$ con $J \neq I$, per ipotesi allora $J < G$. Ora P_1 e P_2 sono distinti e $P_i < J$, da queste due condizioni segue immediatamente $|J| = p^2q$ e $|G : J| = q$.

  Possiamo allora applicare la proposizione 1.1.15 e quindi $|G : J_G|$ deve dividere $q!$. Ma essendo $J_G \lhd G$ e $J_G \leq J$ allora per ipotesi $J_G = \{1\}$ e quindi $|G| = p^2q^2$ divide $q!$. All'inizio abbiamo supposto che $p > q$ e quindi nella fattorizzazione di $q!$ non ci sarà alcuna occorrenza del fattore primo p e quindi p non dividerà $q!$ generando così un assurdo.

- Per ogni $P_1, P_2 \in Syl_p(G)$ si ha $P_1 \cap P_2 = \{1\}$. Con un procedimento analogo al precedente abbiamo $|S| = q^2\left(p^2 - 1\right)$ e $|G \setminus S| = q^2$ quindi vi è un unico q-sottogruppo di Sylow il quale è normale, assurdo.

Caso $|G| = pqr$.

Supponiamo G non risolubile di ordine minimo e $p > q > r$, allora sempre per quanto detto sopra G deve essere semplice. Poiché i sottogruppi di Sylow hanno ordine primo la loro intersezione è necessariamente banale, inoltre dal terzo teorema di Sylow $n_p = qr$ e quindi $|S| = (p-1)qr$ e $|G \setminus S| = qr$.

Ora sia $n_q = \left|Syl_q(G)\right|$ allora dat terzo teorema di Sylow $n_q > q$ e $n_q \in \{p, r, pr\}$, e quindi $n_q \geq p$. Indicando con T l'insieme degli elementi non identici di ordine q abbiamo $|T| = n_q(q-1) \geq p(q-1)$ e quindi

$$|G \setminus (S \cup U)| \leq qr - p(q-1) < qr - r(q-1) = r$$

ma ciò è assurdo dato che dal primo teorema di Sylow $G \setminus (S \cup U)$ dovrebbe contenere un r-sottogruppo.

Quindi il gruppo G possiede necessariamente un sottogruppo normale contraddicendo l'ipotesi di minimalità, quindi ogni gruppo in questa forma deve essere risolubile. ■

In realtà vale un risultato molto più generale, che non dimostreremo in questa sede

Teorema 5.1.4 (Burnside). *Se G è un gruppo finito con $|G| = p^m q^n$, dove p, q sono primi distinti e $m, n \in \mathbb{N}_0$, allora G è risolubile.*

Esempio 8. Consideriamo il gruppo alterno A_4 delle permutazioni pari su di un insieme di cardinalità 5. Chiaramente $|A_4| = |S_4|/2 = 3 \cdot 2^2$ e quindi è un gruppo risolubile ma non nilpotente in quanto $Z(A_4) = \{1\}$ come tra l'altro S_3.

Invece si può dimostrare che A_5 non è risolubile, tra l'altro $|A_5| = 5 \cdot 3 \cdot 2^2$ e non ricade dunque nelle ipotesi del teorema.

Proposizione 5.1.5. *Preso $H < G$ e $A \lhd G$ abeliano per cui $G = HA$ allora*

1. $|G : H| = \frac{|A|}{|A \cap H|}$;
2. $H \lessdot G \Leftrightarrow A/(A \cap H)$ *è un fattore principale, ovvero in ogni serie normale contenente sia A che $A \cap H$ questi due termini sono sempre consecutivi.*

Dimostrazione. Il primo punto è banale, dimostriamo solo il secondo. Preso $H \lessdot G$ ora $H \cap A \lhd H$ e quindi $H \leq N_G(H \cap A)$ e poiché A è abeliano segue che $H \cap A \lhd G$.

Se $H \cap A = A$ seguirebbe che $G = H$ assurdo per ipotesi, dunque $\{H \cap A\} \neq A/H \cap A \lhd G/H \cap A$, supponiamo ancora per assurdo che esiste L per cui $H \cap A < L < A$ per cui $L \lhd G$. In questo caso avremmo $H \leq HL \leq G$ e per la massimalità di H sono possibili due sole possibilità:

- Se $H = HL$ allora $L \leq H \cap A$ assurdo;
- Se $HL = G$ allora per l'identità di Dedekind $A = A \cap HL = (A \cap H) L = L$ il che è impossibile.

Perciò $A/(H \cap A) \underset{\min}{\lhd} G/(H \cap A)$ e quindi dalla proposizione 3.2.5 è un fattore principale.

Viceversa sia $A/(H \cap A)$ normale minimale e $H \leq K \leq G$ allora $H \cap A < A$ e quindi $H \neq G$. Passando alle intersezioni $H \cap A \leq K \cap A \leq A$ mentre $G = KA$, possiamo mostrare in maniera analoga che $K \cap A \lhd G$ e quindi dobbiamo considerare due casi

- Se $K \cap A = H \cap A$ allora per l'identità di Dedekind $K = K \cap HA = H(K \cap A) = H$;
- Se $K \cap A = A$ allora $K \leq A$ e quindi $G = KA = K$.

e quindi $H \lessdot G$. ■

Dimostriamo adesso il seguente risultato sui gruppi risolubili.

Proposizione 5.1.6. *Se G è un gruppo risolubile allora*

1. *I fattori di composizione hanno ordine primo;*
2. *Se X è un fattore principale di G allora X è un p-gruppo abeliano elementare per un qualche primo p oppure è prodotto diretto di gruppi isomorfi a $\mathbb{Q}$;*

3. *Se $M \lessdot G$ e $|G:M| < \infty$ allora $|G:M|$ è una potenza di primo.*

Dimostrazione. Dimostriamo i vari punti.

1. Se X è un fattore di composizione allora è semplice e non identico oltre ad essere risolubile. Quindi il derivato X' non può coincidere con X e quindi si ha $X' = \{1\}$ ovvero X è abeliano. Gli unici gruppi abeliani semplici hanno ordine primo.

2. Per comodità non usiamo i quozienti, quindi prendiamo $N \underset{\min}{\lhd} G$, quindi N è abeliano e $N[p]$ è caratteristico in N per ogni p primo e dunque $N[p] \lhd G$.

   Se $N[p] = N$ per un certo primo allora N è un p-gruppo abeliano elementare per il teorema di Prüfer-Baer, mentre se $N[p] = \{1\}$ per ogni primo p allora N è abeliano e aperiodico e quindi $N^p \neq \{1\}$ per ogni primo p. Essendo anche questo sottogruppo caratteristico allora $N^p = N$ e quindi N è divisibile e aperiodico.

   Dal teorema di struttura dei gruppi divisibili N è prodotto diretto di sottogruppi isomorfi a $\mathbb{Q}$.

3. Prendiamo $M \lessdot G$ con $|G:M| < \infty$ esisterà allora $j \in \mathbb{N}$ per cui $G^{(j+1)} \leq M$ ma $G^{(j)} \nleq M$. Per la massimalità allora $G = MG^{(j)}$ e perciò

$$\frac{G}{G^{(j+1)}} = \frac{M}{G^{(j+1)}} \cdot \frac{G^{(j)}}{G^{(j+1)}}$$

   che possiamo riscrivere come $\overline{G} = \overline{M}A$ con A abeliano. Abbiamo ancora $\overline{M} \lessdot \overline{G}$ e dunque dalla proposizione precedente $\left|\overline{G} : \overline{M}\right| = |G:M| = \left|A/\left(A \cap \overline{M}\right)\right| < \infty$ ed $A/\left(A \cap \overline{M}\right)$ è un fattore principale. Per il secondo punto di questa proposizione questo quoziente è un p-gruppo abeliano elementare.

■

Da adesso in poi ci dedicheremo al sottogruppo di fitting di un gruppo risolubile

Proposizione 5.1.7. *Se G è risolubile con $d = \mathrm{der}(G) \geq 1$ allora*

1. $G^{(d-1)} \leq \mathrm{FIT}(G)$*;*

2. *se $N \underset{min}{\lhd} G$ allora $N \leq \mathrm{FIT}(G)$;*

3. *più in generale se $\{1\} \neq N \lhd G$ allora $N \cap \mathrm{FIT}(G) \geq A$ dove $\{1\} \neq A \lhd G$ ed A è abeliano.*

Dimostrazione. Il primo punto è banale essendo $G^{(d-1)}$ abeliano, mentre il secondo punto è conseguenza diretta della proposizione 5.1.2.

Concentriamoci nel dimostrare la terza affermazione, $N \in \mathcal{S}$ e $d = \mathrm{der}(N)$. Per induzione si dimostra facilmente che $N^{(d-1)}$ è caratteristico in N e quindi $A = N^{(d-1)} \leq \mathrm{FIT}(G)$ essendo abeliano e normale in G. ■

Lemma 5.1.8. *Se $G \in \mathcal{S}$ allora $C_G(\mathrm{FIT}(G)) \le \mathrm{FIT}(G)$. Questo significa in particolare che $C_G(\mathrm{FIT}(G)) = Z(\mathrm{FIT}(G))$.*

Dimostrazione. Per assurdo $C = C_G(\mathrm{FIT}(G))$ non è contenuto in $F = \mathrm{FIT}(G)$, dalla definizione di sottogruppo di fitting abbiamo $F \lhd G$ e quindi $CF/F \neq \{F\}$. Ancora per la proposizione 1.1.16 anche C è normale in G e quindi $CF/F \lhd G/F$.

Per la proposizione precedente esiste $F < B \le CF$ tale che B/F è abeliano e $B/F \lhd G/F$, per l'identità di Dedekind $B = B \cap CF = (B \cap C) F$.

Dimostriamo che $B \cap C \le F$, chiaramente è normale in G quindi dobbiamo mostrarne la nilpotenza. Innanzitutto $(B \cap C)' \le B' \le F$ per via del corollario 3.3.17 mentre

$$\left[(B \cap C)'; B \cap C\right] \le [F; C] = [F; C_G(F)] = \{1\}$$

quindi è nilpotente con $\mathrm{cl}(B \cap C) \le 2$. Ma allora $B = F$ raggiungendo così una contraddizione. ■

Prima di dimostrare l'ultimo risultato sui gruppi risolubili abbiamo bisogno di questa proposizine

Proposizione 5.1.9. *Per ogni $N \lhd G$ abbiamo*

$$\frac{G}{C_G(N)} \preceq \mathrm{Aut}(N)$$

Dimostrazione. Per ogni $g \in G$ l'applicazione

$$\theta_g : x \in N \to x^g \in N$$

è un automorfismo di N, inoltre $f : g \in G \to \theta_g \in \mathrm{Aut}(N)$ è un omomorfismo tra gruppi. Inoltre $g \in \ker F \Leftrightarrow gx = xg$ per ogni $x \in \mathbb{N} \Leftrightarrow g \in C_G(N)$. ■

Proposizione 5.1.10. *Sia G gruppo risolubile tale che* $\mathrm{FIT}(G)$ *sia finito, allora anche G è finito.*

Dimostrazione. Posto come prima $F = \mathrm{FIT}(G)$ allora $\mathrm{Aut}(F)$ è ancora finito e quindi anche il quoziente $G/C_G(F)$ lo è. Dal lemma precedente $C_G(F)$ è finito e quindi G deve essere necessariamente un gruppo finito. ■

5.2 Gruppi supersolubili

Definizione 5.2.1. Un gruppo G si dice *supersolubile* se e solo se possiede una serie finita da G a $\{1\}$ che sia normale e a fattori ciclici.

La classe dei gruppi supersolubili la indicheremo con PnC

Dalla proposizione 4.5.4 i gruppi nilpotenti e finitamente generati sono supersolubili. Inoltre tanto il gruppo diedrale finito D_{2n} che quello infinito D_∞ sono supersolubili dato che hanno la forma $D = \langle x \rangle \ltimes \langle a \rangle$ con $|\langle x \rangle| = 2$ e $\langle a \rangle$ è un gruppo ciclico finito o infinito.

Una serie supersolubile è la seguente

$$\{1\} \lhd \langle a \rangle \lhd D$$

che è valida per ogni gruppo diedrale.

Proposizione 5.2.2. *La classe dei gruppi supersolubili è chiusa per sottogruppi e quozienti.*

La dimostrazione è la stessa utilizzata per dimostrare la medesima proprietà nei gruppi risolubili, si veda la proposizione 3.2.10, l'unico aspetto da verificare è la normalità delle nuove serie. Difatti

$$G_i \lhd G \Rightarrow H \cap G_i \lhd H$$
$$G_i, N \lhd G \Rightarrow G_iN \lhd G \Leftrightarrow \frac{G_iN}{N} \lhd \frac{G}{N}$$

ed è questo il motivo per cui la classe dei gruppi supersolubili non è chiusa per estensioni, come si può vedere nella dimostrazione dato che la serie in N non è necessariamente normale in G.

Proposizione 5.2.3. $\mathrm{PnC} \subseteq \mathcal{S} \cap \mathrm{Max}$

Dimostrazione. I gruppi supersolubili sono chiaramente risolubili. Ora i gruppi ciclici (finiti o infiniti) sono sempre Max la quale classe è chiusa per estensioni. Perciò ripercorrendo la serie otteniamo che ogni gruppi supersolubile è necessariamente Max. ∎

Proposizione 5.2.4. *Sia* $G \in \mathrm{PnC}$ *allora*

1. *I sottogruppi normali minimali sono ciclici di ordine primo;*

2. *I sottogruppi massimali hanno indice primo.*

Dimostrazione. Preso $N \underset{\min}{\lhd} G$ e $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$ serie supersolubile. Esiste chiaramente $j \in \mathbb{N}_0$ tale che $N \cap G_j = \{1\}$ e $N \cap G_{j+1} \neq \{1\}$. Poiché la serie è normale in G per minimalità abbiamo $N \cap G_{j+1} = N$ ovvero $N \leq G_{j+1}$ e quindi

$$N \cong \frac{N}{N \cap G_j} \cong \frac{NG_j}{G_j} \leq \frac{G_{j+1}}{G_j}$$

che è ciclico.

Per l'inverso forte del teorema di Lagrange tutti i suoi sottogruppi sono caratteristici e quindi sarebbero normali in G, ma essendo N minimale allora deve avere ordine primo.

Per la dimostrazione del secondo punto ripercorriamo quella della proposizione 5.1.6. Prendiamo $M \lessdot G$ con $|G : M| < \infty$ esisterà allora $j \in \mathbb{N}$ per cui $G^{(j+1)} \leq M$ ma $G^{(j)} \not\leq M$. Per massimalità allora $G = MG^{(j)}$ e perciò

$$\frac{G}{G^{(j+1)}} = \frac{M}{G^{(j+1)}} \cdot \frac{G^{(j)}}{G^{(j+1)}}$$

che possiamo riscrivere come $\overline{G} = \overline{M}A$ con A abeliano. Abbiamo ancora $\overline{M} \lessdot \overline{G}$ e dunque dalla proposizione 5.1.5 $\left|\overline{G} : \overline{M}\right| = |G : M| = \left|A/\left(A \cap \overline{M}\right)\right|$.

Ma $A/\left(A \cap \overline{M}\right)$ è normale e minimale di $\overline{G}/\left(\overline{M} \cap A\right)$ che è quoziente di un gruppo supersolubile e perciò è ciclico finito di ordine primo. ∎

Il secondo punto è una versione più forte della proposizione 5.1.6 in quanto non richiede come ipotesi la finitezza dell'indice. Quindi i sottogruppi massimali di gruppi supersolubili devono a forza di cose avere indice finito.

Come per i gruppi risolubili studiamo il sottogruppi di fitting anche in quelli supersolubili. Innanzitutto abbiamo bisogno di un risultato preliminare

Proposizione 5.2.5. *Se G è un gruppo ciclico allora* $\mathrm{Aut}(G)$ *è finito e abeliano*

Dimostrazione. Poniamo $G = \langle g \rangle$ allora per ogni $\phi \in \mathrm{Aut}(G)$ esistono $m, n \in \mathbb{Z}$ tali che $\phi(g) = g^m$ e $\phi^{-1}(g) = g^n$ in particolare $\phi\left(g^k\right) = g^{mk}$ e quindi $g = g^{mn}$.

Se G fosse ciclico infinito allora $g^{mn} = g \Leftrightarrow mn = 1$ ed essendo entrambi interi o $m = n = 1$ oppure $m = n = -1$ quindi $|\mathrm{Aut}(G)| = 2$. Se invece G fosse ciclico di ordine k allora m può sempre essere preso sempre tra 0 e $k - 1$, stessa cosa per n e quindi sono in numero finito. ∎

Proposizione 5.2.6. *Sia G supersolubile allora*

- $\mathrm{FIT}(G) \in \mathfrak{N}$*;*
- $G/\mathrm{FIT}(G)$ *è abeliano e finito.*

Dimostrazione. I gruppi supersolubili sono Max e quindi Max-n, applicando la proposizione 4.3.7 il sottogruppo di fitting è necessariamente nilpotente.

Per dimostrare il secondo punto prendiamo una serie supersolubile $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$. Per ogni $i \in \mathbb{N}_0$ poniamo

$$C_i = C_G\left(\frac{G_{i+1}}{G_i}\right)$$

essendo $G_i \lhd G$ e quindi poiché $G_{i+1}/G_i \lhd G/G_i$

$$\frac{G}{C_i} \cong \frac{G/G_i}{C_i/G_i} \preceq \mathrm{Aut}\left(\frac{G_{i+1}}{G_i}\right)$$

per quanto detto sopra G/C_i è abeliano finito.

Questo significa anche che $G' \leq C_i$ per ogni $0 \leq i < n$. Posto

$$C = \bigcap_{i=0}^{n-1} C_i \geq G'$$

allora G/C è abeliano e finito per la proposizione 1.1.3.

Chiaramente $[C_i; G_{i+1}] \leq G_i$ per come abbiamo definito C_i e dunque

$$[G_{i+1} \cap C; C] \leq [G_{i+1}; C_i] \leq G_i$$

e perciò la serie $G_i \cap C$ è centrale in C. Questo vuol dire che $C \in \mathcal{N}$ ed essendo $C \lhd G$ in quanto intersezione di sottogruppi normali abbiamo $C \leq F$ e allora

$$\frac{G}{F} \cong \frac{G/C}{F/C}$$

abeliano e finito. ■

Teorema 5.2.7 (Zappa). *Se G è un gruppo supersolubile allora esiste una serie normale finita $\{1\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$ a fattori ciclici infiniti o ciclici di ordine primo.*

Esistono inoltre $0 \leq s \leq t < n$ tali che

- *Per ogni $0 \leq i < s$ G_{i+1}/G_i ha come ordine un primo dispari in ordine decrescente rispetto ad i;*
- *Per ogni $s \leq i < t$ G_{i+1}/G_i ha ordine infinito;*
- *Per ogni $t \leq i < n$ G_{i+1}/G_i ha ordine 2.*

Dimostrazione. Innanzitutto prendiamo $\{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_l = G$ serie normale a fattori ciclici.

Supponiamo che K_{i+1}/K_i sia un ciclico finito, per la proposizione 4.5.4 esiste una serie centrale

$$\{K_i\} = \frac{C_0^i}{K_i} \lhd \frac{C_1^i}{K_i} \lhd \cdots \lhd \frac{C_u^i}{K_i} = \frac{K_{i+1}}{K_i}$$

a fattori ciclici di ordine primo. Poiché $C_{j+1}^i/C_j^i \cong \left(C_{j+1}^i/K_i\right)/\left(C_j^i/K_i\right)$ la serie $K_i = C_0^i \lhd C_1^i \lhd C_2^i \lhd \cdots \lhd C_u^i = K_{i+1}$ è ancora a fattori ciclici di ordine primo. Ancora, per l'inverso forte del teorema di Lagrange $\frac{C_0^i}{K_i}$ è caratteristico in $\frac{K_{i+1}}{K_i} \lhd G/K_i$ e quindi la serie ottenuta incollandole è normale e a fattori ciclici infiniti o di ordine primo.

Adesso dobbiamo "riordinare" questi fattori in modo da portare tutti i fattori secondo lo schema nell'enunciato, e per farlo concentriamoci su tre termini consecutivi di questa serie $H \lhd K \lhd L$ in particolare sostituendo K con un certo $X \lhd G$ per cui $H \lhd X \lhd L$ abbia i fattori invertiti.

Quindi posto $C = C_L(K/H) \lhd G$ in quanto $H, K, L \lhd G$ abbiamo $K \leq C \leq L$ essendo K/H ciclico e quindi sempre per la proposizione 5.1.9

$$\frac{L}{C} \cong \frac{L/H}{C/H} = \frac{L/H}{C_{L/H}(K/H)} \preceq \operatorname{Aut}\left(\frac{K}{H}\right)$$

e quindi è finito. Abbiamo così dedotto questi risultati che utilizzeremo nel corso della dimostrazione

- L/C è isomorfo ad un quoziente di L/K essendo $C \leq K$;
- $|L : C|$ divide $|\mathrm{Aut}\,(K/H)|$

Caso $|K : H| = p$ e $|L : K| = q$ con $p < q$.

Innanzitutto per quanto detto prima $|L : C|$ o vale 1 o vale q, ma $|\mathrm{Aut}\,(K/H)| = \varphi(p) = p - 1 < q$ (φ è la funzione di Eulero) e perciò $L = C$. Questo significa che $L/H = C_{L/H}\,(K/H)$ ovvero $K/H \leq Z\,(L/H)$.

Allora $(L/H)/Z\,(L/H)$ è ciclico con lo "stesso generatore" di $L/K \cong (L/H)/(K/H)$ e per un noto teorema L/H è abeliano. Applicando il teorema 2.1.5 è prodotto diretto dei suoi sottogruppi di Sylow in quanto $|L : H| = pq$ è finito. Ora poiché $|K/H| = p$ ed è un suo sottogruppo esiste $H \leq X \lhd L$ tale che

$$\frac{L}{H} = \frac{K}{H} \times \frac{X}{H}$$

e $|X/H| = q$.

Sostituiamo K con X e verifichiamo che in tal modo gli indici vengono scambiati. Poiché X/H è l'unico q-sottogruppo di Sylow di L/H (contiene tutti gli elementi di periodo potenza di q) allora è caratteristico e quindi $X \lhd G$. Infine

$$|L/X| = \frac{|L/H|}{|X/H|} = p$$

e quindi i due primi vengono scambiati di posizione.

Caso $|K : H| = \infty$ e $|L : K| = p$ con $p > 2$.

In questo caso $|\mathrm{Aut}\,(K/H)| = 2$ e quindi possiamo tranquillamente procedere come sopra dimostrando che L/H è abeliano. Ora il quoziente L/H è infinito, quindi non possiamo applicare ancora il teorema di prima e bisogna procedere con maggior cautela. Posto $A = L/H$ e $B = K/H$ allora A è finitamente generato oltre che abeliano essendo la classe dei gruppi finitamente generati chiusa per estensioni.

Quindi ogni suo sottogruppo è necessariamente finitamente generato tra cui il suo sottogruppo di torsione T che sarà allora finito. Per il teorema di struttura dei gruppi abeliani Max possiamo scrivere $A = T \times F$ con F abeliano libero di rango finito, poiché B è ciclico infinito si ha $T \cap B = \{1\}$ e $T \cong TB/B \leq A/B$. Ma $|A : B| = |L : K| = p$ e questo significa che o $|T| = 1$ oppure $|T| = p$.

Passiamo ad F, esso è prodotto diretto di un numero finito di ciclici infiniti ma

$$\left|\frac{F}{F \cap B}\right| = \left|\frac{FB}{B}\right| \leq \left|\frac{A}{B}\right| = p$$

con p numero primo.

Sia $F = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_t \rangle$, poiché $F \cap B$ è ciclico infinito esistono $n_i \in \mathbb{Z}$ tali che $T \cap B = \langle n_1x_1 + n_2x_2 + \cdots + n_tx_t \rangle$. Per comodità supponiamo che $n_1 \neq 0$ allora $px_1 \in F \cap B$ e quindi esiste un k intero non nullo tale che $px_1 = kn_1x_1 + kn_2x_2 + \cdots + kn_tx_t$ e per l'unicità della scrittura avremo per ogni $i > 1$ $kn_ix_i = 0 \Rightarrow kn_i = 0 \Rightarrow n_i = 0$ e quindi $F \cap B \leq \langle x_1 \rangle$.

Ma allora $F = \langle x_1 \rangle$ altrimenti $F/(F \cap B)$ non sarebbe finito quindi $F \cong A/T$ è ciclico infinito.

Alla fine il sottogruppo $T = X/H$ è caratteristico in $A = L/H$ in quanto di torsione e dunque $X \lhd G$. Sostituiamo K con X, possono succedere due fatti

1. Se $T = \{H\}$ allora $X = H$ e quindi rimane solo il fattore $L/H \cong A/T$ che è ciclico infinito.

2. Se $|T| = p$ allora $|X : H| = p$ ed è ciclico mentre $L/X \cong A/T$ è ciclico infinito e quindi i posti sono scambiati.

Caso $|K : H| = 2$ e $|L : K| = \infty$.

In questo caso il procedimento da seguire è diverso, poiché $K/H \lhd G/H$ ha ordine 2 allora $k^g H = kH$ per ogni $k \in K$ e $g \in G$ e in particolare $K/H \leq Z(L/H)$ e quindi con un procedimento analogo sfruttando l'ipotesi che L/K sia ciclico verifichiamo che $A = L/H$ è comunque abeliano e finitamente generato.

Posto sempre $B = K/H$ finito allora $A/B \cong L/K$ ciclico infinito e dunque il sottogruppo di torsione di A deve coincidere con B e non contenerlo semplicemente. Ancora dal teorema di struttura dei gruppi Max $A = B \times F$ con F abeliano libero di rango finito ma in questo caso si vede velocemente che

$$F \cong \frac{A}{B} \cong \frac{L}{K}$$

e allora è ciclico infinito.

Ancora $A^2 = B^2 \times F^2 = F^2$ il quale è caratteristico in A mentre B è caratteristico in A come è facile da constatare dunque $F^2 \times B$ è caratteristico in A. Ma per le proprietà dei prodotti diretti

$$\frac{A}{F^2} = \frac{B \times F}{B^2 \times F^2} \cong B \times \frac{F}{F^2} \Rightarrow \left|A : F^2\right| = 4$$

Ordinando i vari sottogruppi otteniamo

$$\{1\} \leq F^2 < F^2 \times B \leq F \times B = A$$

e poniamo $F^2 = \frac{X}{H}$ mentre $F^2 \times B = Y/H$. Entrambi essendo caratteristici sono normali in G e stavolta sostituiamo K non solo con X ma con $H \lhd X \lhd Y \lhd L$. Chiaramente X/H è ciclico infinito mentre $Y/X \cong B$ ha ordine 2 e

$$L/Y \cong (B \times F)/\big(B \times F^2\big) \cong F/F^2$$

che ha ancora ordine 2.

Per riordinare globalmente la serie si può procedere così: prima si portano tutti i fattori di indice 2 a destra tramite sia la prima (che non distingue tra primi dispari e 2) che la terza regola, poi i fattori infiniti tramite la seconda regola e infine i fattori di ordine primi dispari vengono riordinati in ordine decrescente tramite la prima regola. ■

Questo risultato che a prima vista può sembrare del tutto inutile ha delle conseguenze piuttosto interessanti, come la seguente

Corollario 5.2.8. *Se G è supersolubile allora il sottoinsieme*

$$\{g \in G \mid g \text{ ha periodo dispari}\}$$

è un sottogruppo di G.

Dimostrazione. Se prendiamo una successione G_i ottenuta riordinandola come nel teorema di Zappa allora possiamo prendere $s \in \mathbb{N}_0$ il massimo indice per cui H_{i+1}/H_i abbia ordine finito e dispari mentre $t \in \mathbb{N}_0$ il massimo indice per cui H_{i+1}/H_i abbia ordine infinito. Quindi posto $X = H_s$ e $Y = H_{t+1}$ allora $X \leq Y$ e $|G : Y| = 2^u$ chiaramente.

Ancora Y/X è senza torsione e X è finito. Se prendiamo adesso un $x \in G$ che abbia ordine dispari allora anche $xY \in G/Y$ ($Y \lhd G$ essendo supersolubile) ha ordine dispari, ma questo gruppo ha ordine 2^u e perciò $x \in Y$. Ma allora $xX \in Y/X$ e stavolta il gruppo è senza torsione e quindi $x \in X$.

Supponiamo ora che $x \in X$ chiaramente $|X| = c$ è un numero dispari e $x^c = 1$ indi anche l'ordine di x deve essere dispari. ■

5.3 Gruppi policiclici

Definizione 5.3.1. Un gruppo G si dice *policiclico* se e solo se possiede una serie finita da G a $\{1\}$ a fattori ciclici. Un gruppo G è *policicliclo infinito* se e solo se coincide con $\{1\}$ oppure è policiclico e possiede una serie finita a fattori ciclici infiniti.

La classe dei gruppi supersolubili la indicheremo con PC.

La differenza rispetto ai gruppi supersolubili è che la serie a fattori ciclici può non essere normale. Infatti a differenza dei gruppi risolubili che possiedono sempre una serie normale e abeliana per le serie a fattori ciclici questo non è sempre vero.

Chiaramente ogni gruppo supersolubile è policiclico e ogni gruppo policiclico è risolubile.

Proposizione 5.3.2. $\mathrm{PC} = \mathcal{S} \cap \mathrm{Max}$

Dimostrazione. Come per i gruppi supersolubili si mostra l'inclusione $\subseteq$. Prendiamo ora $G \in \mathcal{S} \cap Max$ allora ogni suo sottoinsieme è finitamente generato, perciò presa una serie abeliana H_i dal teorema di struttura per i gruppi abeliani Max possiamo scrivere

$$\frac{H_{i+1}}{H_i} = \frac{A_0}{H_i} \times \frac{A_1}{H_i} \times \cdots \times \frac{A_l}{H_i}$$

e inoltre

$$\frac{A_0 A_1 \cdots A_i A_{i+1}}{A_0 A_1 \cdots A_i} \cong \frac{A_0 A_1 \cdots A_i / H_j \times A_{i+1}/H_j}{A_0 A_1 \cdots A_i / H_j} \cong \frac{A_{i+1}/H_j}{A_{i+1}/H_j \cap A_0 A_1 \cdots A_i / H_j} \cong \frac{A_{i+1}}{H_j}$$

che è ciclico. ■

Abbiamo visto nel capitolo precedente che i gruppi risolubili, Max e periodici sono necessariamente finiti. Per quanto detto sopra i gruppi risolubili e Max sono tutti e soli i gruppi policiclici. Da questa osservazione possiamo dimostrare immediatamente la proposizione 4.5.2 in quanto per i gruppi policiclici periodici la relativa serie policiclica può essere formata solamente da fattori ciclici finiti, e quindi il gruppo stesso deve essere ciclico.

Corollario 5.3.3. *La classe dei gruppi policiclici è chiusa per sottogruppi, quozienti ed estensioni.*

Dimostrazione. Lo sono sia la classe dei gruppi risolubili che Max. ■

Proposizione 5.3.4. *La classe dei policiclici infiniti è chiusa per sottogruppi ed estensioni.*

Dimostrazione. Si veda la dimostrazione della proposizione della 3.2.10, dato che sottogruppi di gruppi ciclici infiniti o sono banali o sono ancora ciclici infiniti. ■

Corollario 5.3.5. *I gruppi policiclici infiniti non hanno sottogruppi finiti non banali.*

Proposizione 5.3.6. *Sia G un gruppo policiclico. Allora*

1. *esiste $N \lhd G$ tale che G/N è finito e N policiclico infinito;*
2. *Se G non è finito allora esiste $A \lhd G$ abeliano e aperiodico. Inoltre poiché $G \in \mathrm{Max}$ allora A è prodotto diretto di un numero finito di gruppi ciclici infiniti*

Dimostrazione. Per dimostrare il primo punto lavoreremo per induzione sulla lunghezza della serie di G. Se è 1 allora G è ciclico e possiamo scegliere N pari a $\{1\}$ o G a seconda dei casi.

Supponiamo il teorema valido per i gruppi la cui serie ha lunghezza $t-1$, sia $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_t = G$ e prendiamo $K = G_{t-1} \lhd G$. Per ipotesi induttiva esiste $H \lhd K$ tale che H/K è finito e K policiclico infinito, quindi anche $H_G \lhd G$ è policiclico infinito.

Chiaramente K/H_G è risolubile e Max, dimostriamo che è periodico. Posto $|K : H| = n$ dunque $x^n \in H$ per ogni $x \in K$, inoltre osserviamo che $|K^g : H^g| = n$ per ogni $g \in G$ dato che l'operazione di coniugio è un automorfismo. Ma $K \lhd G$ e quindi $K^g = K$ e quindi $x^n \in H^g$ per ogni $x \in K$ e $g \in G$ e

$$x^n \in \bigcap_{g \in G} H^g = H_G$$

Quindi K/H_G è risolubile, Max e periodico, dalla proposizione 4.5.2 segue che è finito.

Se G/K è finito allora $G/K \cong (G/H_G)/(K/H_G)$ e dunque G/H_G è anch'esso finito. Altrimenti $G/K = \langle yK \rangle$ ciclico infinito ovvero $\langle y \rangle \cap K = \{1\}$ e dunque

$$G = \langle y \rangle \ltimes K$$

dato che $K \lhd G$. Se prendiamo ora $\overline{H} = \langle y \rangle \ltimes H_G$ esso è ancora policiclico infinito essendo $\overline{H}/H_G \cong \langle y \rangle$ ed applicando il corollario 1.1.9

$$\left|G : \overline{H}\right| = |\langle y \rangle K : \langle y \rangle H_G| = |K : H_G| < \infty$$

Per la proposizione 1.1.15 $G/\overline{H}_G$ è finito mentre $\overline{H}_G \leq \overline{H}$ è policiclico infinito.

Dimostriamo il secondo punto ora. Per quanto detto sopra esiste $N \lhd G$ policiclico infinito tale che G/N è finito, in particolare N è aperiodico e risolubile. Quindi se $d = \mathrm{der}(N)$ allora $A = N^{(d-1)}$ è abeliano, aperiodico e caratteristico in N e perciò $A \lhd G$. ■

Per dimostrare il prossimo risultato abbiamo bisogno del seguente teorema, di cui non daremo una dimostrazione completa.

Teorema 5.3.7 (raffinamento)**.** *Preso un gruppo G e due sue serie finite Σ_1, Σ_2 allora esistono $\Sigma_1' \supseteq \Sigma_1$ e $\Sigma_2' \supseteq \Sigma_2$ serie finite di G e un isomorfismo f che manda i fattori di Σ_1' nei fattori di Σ_2' e viceversa.*

Dimostrazione. (cenni) Posto $\Sigma_1 : \{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_l = G$ e $\Sigma_2 : \{1\} = K_0 \lhd K_1 \lhd \cdots \lhd K_m = G$ allora i raffinamenti vengono ottenuti nella seguente maniera

$$\Sigma_1' : H_i \lhd H_i (H_{i+1} \cap K_1) \lhd H_i (H_{i+1} \cap K_2) \lhd \cdots \lhd H_i (H_{i+1} \cap K_m) = H_{i+1} \quad (5.3.1)$$
$$\Sigma_2' : K_i \lhd K_i (K_{i+1} \cap H_1) \lhd K_i (K_{i+1} \cap H_2) \lhd \cdots \lhd K_i (K_{i+1} \cap H_l) = K_{i+1} \quad (5.3.2)$$

■

Proposizione 5.3.8. *Se $G \in \mathrm{PC}$ allora il numero di fattori ciclici infiniti di una sua qualunque serie policiclica è invariante ovvero non dipende dalla particolare serie scelta.*

Dimostrazione. Se prendiamo H_i e K_j due serie policicliche di G, alla luce del teorema di raffinamento dobbiamo solo verificare che i raffinamenti finiti di una serie policiclica è ancora una serie policiclica con lo stesso numero di fattori ciclici infiniti.

Consideriamo perciò due termini consecutivi $H_i \lhd H_{i+1}$ tali che $|H_{i+1} : H_i| = \infty$ ed $H_i < X \leq H_{i+1}$ un termine del raffinamento finito tale che $X \lhd H_{i+1}$. Allora $H_i \lhd X$ e $X/H_i \lhd H_{i+1}/H_i$. Ora poiché $X \neq H_i$ il quoziente X/H_i è necessariamente un gruppo ciclico infinito mentre

$$\frac{H_{i+1}}{X} \cong \frac{H_{i+1}/H_i}{X/H_i}$$

e quindi per le proprietà dei gruppi ciclici esso è un gruppo ciclico finito. Infine iterando il procedimento la nuova serie è policiclica con lo stesso numero di fattori ciclici infiniti. ■

Definizione 5.3.9. Sia G gruppo policiclico, il numero dei fattori ciclici infiniti di una qualunque serie policiclica di G è detta *lunghezza di Hirsch* di G la quale non dipende dalla particolare serie scelta.

La lunghezza di Hirsch di G si indica con il simbolo $h(G)$

Proposizione 5.3.10. *Se $G \in \mathrm{PC}$ e $N \lhd G$ allora*

$$h(G) = h(N) + h\left(\frac{G}{N}\right)$$

Dimostrazione. Segue immediatamente dalla proposizione 3.2.10 e dall'invarianza della lunghezza di Hirsch. ■

5.4 Il residuale finito

Definizione 5.4.1. Preso un gruppo G generico definiamo il suo *residuale finito* il sottogruppo

$$f^*_{\mathcal{F}}(G) = \bigcap_{\substack{H \leq G \\ |G:H| < \infty}} H$$

Un gruppo G è *residualmente finito* se e solo se $f^*_{\mathcal{F}}(F) = \{1\}$.

Proposizione 5.4.2. *Per ogni gruppo G*

$$f^*_{\mathcal{F}}(G) = \bigcap_{\substack{N \lhd G \\ |G:N| < \infty}} N$$

Dimostrazione. Sicuramente vale l'inclusione $\subseteq$, viceversa se $|G : H| < \infty$ allora dalla proposizione 1.1.15 segue che $|G : H_G| < \infty$. Inoltre poiché $H_G \leq H$

$$f^*_{\mathcal{F}}(G) \supseteq \bigcap_{\substack{H \leq G \\ |G:H| < \infty}} H_G \supseteq \bigcap_{\substack{N \lhd G \\ |G:N| < \infty}} N$$

■

Corollario 5.4.3. *Se G è un gruppo generico allora $f^*_{\mathcal{F}}(G) \lhd G$.*

Osservazione. Se G è un gruppo residualmente finito allora per ogni $H \leq G$ finito esiste $N \lhd G$ tale che $|G : N| < \infty$ e $H \cap N = \{1\}$. Questo vuol dire che

$$H \cong \frac{HN}{N} \leq \frac{G}{N}$$

ovvero ogni sottogruppo finito è isomorfo ad un sottogruppo di un quoziente finito di G.

Lemma 5.4.4. *I gruppo abeliani finitamente generati sono residualmente finiti.*

Dimostrazione. Da teorema di struttura possiamo scrivere un qualunque gruppo abeliano finitamente generato A nella forma $A = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle \times F$ con F finito e x_i aperiodico.

Supponiamo anche che A sia infinito e definiamo $E = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$ il quale è abeliano libero, quindi dalla proposizione 2.1.3 segue che $\bigcap_{n \in \mathbb{N}} E^{p^n} = \{1\}$ mentre $\left| E : E^{p^n} \right|$ è sempre finito.

Questo significa allora che

$$\left| A : E^{p^n} \right| = |A : E| \left| E : E^{p^n} \right| = |F| \left| E : E^{p^n} \right| < \infty$$

possiamo perciò esprimere il sottogruppo banale come intersezione di sottogruppi con indice finito. ■

Corollario 5.4.5. *Se A è abeliano e finitamente generato allora ogni suo sottogruppo è intersezione di sottogruppi di A con indice finito.*

Dimostrazione. Applicando il lemma precedente al gruppo A/H otteniamo l'uguaglianza $f^*_{\mathcal{F}}(A/H) = \{H\}$ ovvero esistono $\{K_i\}_{i \in I} \leq A$ contenenti H tali che

$$|A : K_i| = \left| \frac{A/H}{K_i/H} \right| < \infty$$
$$\bigcap_{i \in I} \frac{K_i}{H} = \{H\} \Leftrightarrow \bigcap_{i \in I} K_i = H$$

e quindi la tesi. ■

Teorema 5.4.6 (Mal'Cev)**.** *In un gruppo policiclico tutti i suoi sottogruppi sono intersezione di sottogruppi con indice finito.*

Dimostrazione. Supponiamo per assurdo che l'asserto sia falso, quindi esisterà $H \leq G$ tale che

$$\overline{H} = \bigcap_{\substack{H \leq K \\ |G:K| < \infty}} K > H$$

e supponiamo che la lunghezza di Hirsch di G sia la più piccola per cui vale questa affermazione. Chiaramente $h(G) \geq 1$ e quindi G infinito dato che per i gruppi finiti il teorema è sempre verificato.

Dalla proposizione 5.3.6 esisterà $A \lhd G$ non identico, abeliano e senza torsione e quindi $h(A) \geq 1$ e dalla proposizione 5.3.10 $h(G) > h(G/A)$ e quindi HA/A è intersezione di sottogruppi con indice finito di G/A. Esisterà dunque un $x \in \overline{H} \setminus H$, ma allora per ogni $L/A \geq HA/A$ con $|G : L| = |G/A : L/A| < \infty$ dovremmo avere $x \in L$ e quindi $xA \in L/A$, quindi per ipotesi induttiva $xA \in HA/A$. Questo significa che esistono $h \in H$ ed $a \in A$ tali che $x = ha$ ma essendo $x \notin H$ allora $a \notin H \cap A$.

Ora poiché i gruppi policiclici sono anche Max segue che A è finitamente generato e possiamo applicare il corollario 5.4.5 ottenendo

$$A \cap H = \bigcap_{\substack{A \cap H \leq C \\ |A:C| < \infty}} C$$

e dunque esiste $B \leq A$ tale che $m = |A : B| < \infty$, $A \cap H \leq B$ ma $a \notin B$. Inoltre $A^m \leq B$ e A^m è chiaramente caratteristico in A abeliano aperiodico, dunque $A^m \lhd G$ e non identico e senza torsione. Ciò significa che $h(A^m) > 0$ e quindi per ipotesi induttiva

$$\frac{HA^m}{A^m} = \bigcap_{\substack{L \geq HA^m \\ |G:L|<\infty}} \frac{L}{A^m} \Rightarrow x \in HA^m$$

Dunque esistono $k \in H$ e $b \in A^m$ per cui $x = kb$. Ora da quanto detto sopra

$$ha = kb \Rightarrow k^{-1}h = ba^{-1} \in H \cap A \leq B \Rightarrow a \in B$$

assurdo. ∎

Corollario 5.4.7 (Hirsch)**.** *I gruppi policiclici sono residualmente finiti.*

Corollario 5.4.8. *I gruppi nilpotenti finitamente generati sono residualmente finiti.*

Dimostrazione. I gruppi nilpotenti finitamente generati sono supersolubili e quindi policiclici. ∎

Concentriamoci ora sul residuale finito di gruppi nilpotenti.

Proposizione 5.4.9. *Se G è residualmente finito, allora valgono le seguenti asserzioni*

1. *Se tutti i quozienti finiti sono abeliani allora anche G è abeliano;*

2. *Se tutti i quozienti finiti sono nilpotenti con classe di nilpotenza $\leq k$ allora anche G è nilpotente.*

Dimostrazione. Innanzitutto prendiamo un qualunque quoziente finito G/N con $N \lhd G$, per ipotesi sappiamo che è abeliano e dunque $G' \leq N$. Poiché G è residualmente finito allora $G' = \{1\}$ e quindi G è abeliano.

Per quanto riguarda il secondo punto per ogni $N \lhd G$ tale che $|G : N| < \infty$ per ipotesi $\gamma_{k+1}(G/N) = \{1\}$, per la proposizione 3.4.13 abbiamo

$$\gamma_{k+1}\left(\frac{G}{N}\right) = \frac{\gamma_{k+1}(G)N}{N}$$

quindi $\gamma_{k+1}(G) \leq N$ per ogni $N \lhd G$ tale che $|G : N| < \infty$ e dunque G è nilpotente di classe al più k. ∎

Dimostriamo alcuni risultati preliminari

Proposizione 5.4.10. *Sia G gruppo, $r \in \mathbb{N}_0$ e $H \leq G$, allora*

$$H \leq Z_r(G) \Leftrightarrow [H;_r G] = \{1\}$$

Dimostrazione. Se $r = 0$ allora $Z_0(G) = \{1\}$ e quindi è banale. Supponiamo l'asserto vero per un certo $r \geq 0$ allora dal teorema 3.4.12

$$\begin{aligned} H \leq Z_{r+1}(G) \Leftrightarrow \frac{HZ(G)}{Z(G)} \leq \frac{Z_{r+1}(G)}{Z(G)} = Z_r\left(\frac{G}{Z(G)}\right) \Leftrightarrow \left[\frac{HZ(G)}{Z(G)};_r \frac{G}{Z(G)}\right] = \{Z(G)\} \\ \Leftrightarrow [HZ(G);_r G]\, Z(G) = Z(G) \Leftrightarrow [HZ(G);_r G] \leq Z(G) \\ \Leftrightarrow [H;_r G] \leq Z(G) \Leftrightarrow [H;_{r+1} G] = \{1\} \end{aligned}$$

ottenendo il risultato cercato. ■

Proposizione 5.4.11. *Se G è un gruppo nilpotente e $N \lhd G$ finito con $|N| = p^r$ per un primo p e $r \in \mathbb{N}_0$ allora $N \leq Z_r(G)$.*

Dimostrazione. Utilizzeremo l'induzione su r, se $r = 0$ è chiaramente banale altrimenti supponiamolo verificato per ogni $0 \leq t < r$. Poiché $G \in \mathcal{N}$ e $|N| = p^r$ per la proposizione 4.1.5 $N \cap Z(G) \neq \{1\}$ e quindi

$$\left|\frac{NZ(G)}{Z(G)}\right| = \left|\frac{N}{N \cap Z(G)}\right| \leq p^{r-1}$$

per ipotesi induttiva

$$\frac{NZ(G)}{Z(G)} \leq Z_{r-1}\left(\frac{G}{Z(G)}\right) = \frac{Z_r(G)}{Z(G)}$$

e quindi $N \leq Z_r(G)$. ■

Siamo ora in grado di dimostrare il

Teorema 5.4.12 (Hirsch)**.** *Preso $G \in$ PC tale che per ogni $N \lhd G$ con $|G : N| < \infty$ si ha $G/N \in \mathcal{N}$. Allora G è nilpotente.*

Dimostrazione. Utilizzeremo sempre l'induzione sulla lunghezza di Hirsch h. Se $h = 0$ allora G è finito, altrimenti supponiamolo verificato per ogni $0 \leq t < h$ e quindi esiste $A \lhd G$ non identico, aperiodico abeliano e finitamente generato, quindi dal teorema di struttura $A = \langle a_1 \rangle \times \cdots \times \langle a_l \rangle$ e dunque $h(G/A) < h(G)$.

Ora prendiamo $A \leq K \lhd G$ tale che $|G : K| < \infty$, allora G/K è nilpotente e inoltre

$$\frac{G/A}{K/A} \cong \frac{G}{K}$$

e quindi per ipotesi induttiva G/A è nilpotente. Per le proprietà dei gruppi ciclici per ogni p primo abbiamo $|A : A^p| = p^l$ e $A^p \lhd G$ chiaramente, dunque possiamo far vedere che $G/A^p \in \mathcal{N}$.

Per le proposizioni precedenti allora

$$\frac{A}{A^p} \leq \mathbb{Z}_l\,(G/A^p) \Leftrightarrow \left[\frac{A}{A^p};_l \frac{G}{A^p}\right] = \{A^p\} = \frac{[A;_l G]\, A^p}{A^p} \Leftrightarrow [A;_l G] \leq A^p$$

e dunque

$$[A;_l G] \leq \bigcap_{p \text{ primo}} A^p = \{1\} \Leftrightarrow A \leq Z_l(G) \Rightarrow \frac{G}{Z_l(G)} \cong \frac{G/A}{Z_l(G)/A} \in \mathcal{N}$$

Concludendo allora esisterà $k \in \mathbb{N}_0$ per cui

$$\frac{Z_{t+k}(G)}{Z_l(G)} = Z_k\left(\frac{G}{Z_l(G)}\right) = \frac{G}{Z_l(G)} \Rightarrow Z_{t+k}(G) = G$$

e quindi G è nilpotente. ■

5.5 Condizioni Max-n e Min-n

Proposizione 5.5.1. *Se G è un gruppo abeliano e* Min *allora per ogni $m \in \mathbb{N}$ $G[m]$ è finito.*

Dimostrazione. Il gruppo $G[m]$ è ancora abeliano e Min, oltre ad avere esponente finito. Per il teorema di Prüfer-Baer $G[m]$ è prodotto diretto di sottogruppi ciclici, ma essendo $G[m] \in$ Min allora è periodico e il prodotto diretto è composto da un numero finito di fattori e quindi è finito. ■

Proposizione 5.5.2. *Se $G \in$* Min-n *allora $|G : f^*_{\mathcal{F}}(G)| < \infty$ ed è il più piccolo sottogruppo di G ad avere indice finito.*

Dimostrazione. La classe $\{N \lhd G \mid |G : N| < \infty\}$ ha un qualche elemento minimale M e quindi $f^*_{\mathcal{F}}(G) \leq M$. Utilizzando la proposizione 1.1.3 M deve essere contenuto in ogni altro elemento di questa classe da cui segue che $M \leq f^*_{\mathcal{F}}(G)$. ■

Corollario 5.5.3. *I gruppi* Min-n *residualmente finiti sono finiti.*

Per comodità di notazione utilizzeremo il simbolo J per indicare il residuale finito di G.

Proposizione 5.5.4. *Per ogni $N \lhd G$*

- *$f^*_{\mathcal{F}}(G/N) \geq JN/N$;*
- *Se $N \leq J$ allora $f^*_{\mathcal{F}}(G/N) = J/N$.*

Dimostrazione. Poiché $|G : K| = |G/N : K/N|$ per ogni $N \leq K \leq G$ allora

$$f^*_{\mathcal{F}}(G/N) = \bigcap_{\substack{N \leq K \leq G \\ |G:K|<\infty}} \frac{K}{N} \geq \bigcap_{\substack{K \leq G \\ |G:K|<\infty}} \frac{KN}{N} = \frac{JN}{N}$$

Se inoltre $N \leq J$ significa che per ogni $K \leq G$ tale che $|G : K| < \infty$ allora $N \leq K \leq G$ e quindi possiamo effettuare il procedimento opposto e ritrovare la tesi. ■

Definizione 5.5.5. Un gruppo G è un *gruppo di Chernikov* se e solo se esiste $N \lhd G$ tale che G/N è finito ed N è prodotto diretto di un numero finito di gruppi di Prüfer.

La classe dei gruppi di Chernikov si indica con $\mathcal{C}$.

Chiaramente i gruppi abeliani Min sono gruppi di Chernikov per via del teorema di struttura.

Proposizione 5.5.6. *Se $G \in \mathcal{C}$ allora $G \in \mathrm{Min}$ e $N = J$.*

Dimostrazione. Che G sia Min è immediato da constatare, inoltre essendo $\mathrm{Min} \subseteq \text{Min-n}$ per la proposizione precedente $|G : J| < \infty$. Poiché $J \leq N$ allora $|N : J| < \infty$, poiché N è divisibile allora anche N/J è divisibile e finito, dunque $|N : J| = 1$ e $N = J$. ∎

Teorema 5.5.7. *Per ogni $G \in \mathcal{S} \cap \mathrm{Min}$ si ha $G \in \mathcal{C}$ e il suo residuale finito J è abeliano.*

Dimostrazione. Sia G infinito risolubile e Min, allora G è periodico e per la proposizione 5.5.2 $J \neq \{1\}$. Inoltre $J \in \mathcal{S}$ e quindi esiste $d \in \mathbb{N}_0$ tale che $A = J^{(d)} \neq \{1\}$ e $J^{(d+1)} = \{1\}$, quindi A è abeliano e caratteristico in J quindi $A \lhd G$.

Essendo $A \in \mathrm{Min}$ e abeliano allora $A[n]$ è finito per ogni $n \in \mathbb{N}$, quindi per ogni $a \in A \setminus \{1\}$ vale

$$|\{b \in A \mid \operatorname{ord} b = \operatorname{ord} a\}| < \infty$$

e quindi essendo $\operatorname{ord} a^g = \operatorname{ord} a$ per ogni $g \in G$

$$|J : C_J(a)| = |\{a^x \mid x \in J\}| < \infty$$

Adesso chiaramente $C_J(a) \leq J$ e $|G : C_J(a)| = |G : J|\,|J : C_J(a)| < \infty$ quindi $J = C_J(a) \Rightarrow a \in Z(J)$. Dunque $A \leq Z(J)$ e in particolare $Z(J) \neq \{1\}$. Dimostriamo che J è abeliano, se non lo fosse allora $J/Z(J) \neq \{1\}$ e inoltre $J/Z(J) = f^*_{\mathcal{F}}(G/Z(J))$.

Poiché sia la classe dei gruppi risolubili che quella dei gruppi Min è chiusa per quozienti possiamo ripetere tutto il ragionamento precedente in modo da ottenere

$$Z\left(\frac{J}{Z(J)}\right) = \frac{Z_2(J)}{Z(J)} \neq \{1\}$$

Poiché G è periodico esiste $z \in Z_2(J) \setminus Z(G)$ di periodo n, inoltre per ogni $x \in J$ abbiamo $[z;x] \in Z(G)$ e dunque per la proposizione 3.3.5 $[z;x]^n = [z^n;x] = 1$ e quindi

$$\left\{z^{-1}z^x \mid x \in J\right\} = \{[z;x] \mid x \in J\} \subseteq Z(G)[n]$$

che è finito, dunque $|J : C_J(z)| < \infty$ e perciò $J = C_J(z) \Rightarrow z \in Z(J)$ assurdo.

Quindi J è abeliano e possiamo dimostrare il teorema, dal teorema di struttura dei gruppi abeliani Min abbiamo che $J = P_1 \times P_2 \times \cdots \times P_n \times E = U \times E$ con P_i gruppo di Prüfer ed E finito. Ora sappiamo già che $|G : J| < \infty$ mentre $|J : U| = |E| < \infty$ e quindi $J = U$, perciò G è un gruppo di Chernikov. ∎

Teorema 5.5.8 (struttura dei gruppi risolubili Max e Min)**.** *Se G è risolubile allora*

$$G \in \mathrm{PC} \Leftrightarrow G \in \mathrm{Max}$$
$$G \in \mathcal{C} \Leftrightarrow G \in \mathrm{Min}$$

Dimostrazione. La prima equivalenza è stata dimostrata nella proposizione 5.3.2 mentre la seconda deriva dalla proposizione 5.5.6 e dal teorema 5.5.7. ■

Definizione 5.5.9. Preso un generico gruppo G ed $K \leq G$ diciamo che $K \in \text{Max} - G$ se e solo se la famiglia di insiemi $\{N \leq K \mid N \lhd G\}$ soddisfa la condizione massimale. Analogo con $\text{Min} - G$.

Se un gruppo è Max-n allora è necessariamente $\text{Max} - G$, difatti se $N \leq\!< K$ e $N \lhd G$ allora $N \lhd K$ e quindi

$$\begin{aligned} \text{Max} &\subseteq \text{Max-n} \subseteq \text{Max} - G \\ \text{Min} &\subseteq \text{Min-n} \subseteq \text{Min} - G \end{aligned}$$

Vale un risultato più generale della chiusura per estensioni di Max-n e Min-n. Qui lo dimostreremo solo per Max-n anche se vale un risultato analogo per Min-n.

Proposizione 5.5.10. *Sia $N \lhd G$ tale che $G/N \in$ Min-n e $N \in \text{Max} - G$ allora $G \in$ Max-n.*

Dimostrazione. Consideriamo una successione di sottogruppi di G H_i tali che $H_i \leq H_{i+1}$ ed $H_i \lhd G$, allora $H_i \cap N \leq N$ ed $H_i \cap N \lhd G$ per la normalità di N, ancora $H_iN/N \lhd G/N$ e suindi esiste un $n \in \mathbb{N}$ tale che per ogni $m \geq n$ abbiamo $H_m \cap N = H_n \cap N$ e $H_mN = H_nN$.

Utilizzando l'identità di Dedekind abbiamo

$$H_m = H_m \cap H_mN = H_m \cap H_nN = H_n\left(H_m \cap N\right) = H_n\left(H_n \cap N\right) = H_n$$

■

Osservazione. Mostriamo che Max e Min sono contenuti strettamente in Max-n e Min-n rispettivamente. Esiste un teorema (che non dimostreremo) il quale afferma che per ogni gruppo G esiste un gruppo S semplice ed un monomorfismo $G \to S$.

Se prendiamo $G = \mathbb{Z}\left(p^\infty\right)$ allora esisterebbe S semplice con un sottogruppo isomorfo a G, dunque $S \in$ Max-n ma $S \notin$ Max. Vale un risultato analogo con Min prendendo invece G ciclico infinito. Da questa osservazione deduciamo che Max-n e Min-n *non sono chiusi per sottogruppi*, quindi se $G \in$ Max-n ed $H \leq G$ allora possiamo dire solamente che $H \in \text{Max} - G$.

Se G è abeliano chiaramente Max-n e Max coincidono, ciò è vero anche se G è solamente nilpotente difatti

Proposizione 5.5.11. *Se $G \in \mathfrak{N}$ e Max-n allora $G \in Max$. Valo lo stesso risultato con* Min.

Dimostrazione. Essendo G nilpotente esiste $t \in \mathbb{N}$ tale che $G = Z_t(G)$. Ora per ogni $i \in \mathbb{N}_0$ $G/Z_i(G)$ è chiaramente Max-n essendo chiuso per quozienti, inoltre $Z_{i+1}(G)/Z_i(G) = Z\left(G/Z_i(G)\right)$ è Max in quanto tutti i sottogruppi del centro sono normali.

Dato che Max è chiuso per estensioni allora proseguendo per la serie centrale deduciamo che $G \in$ Max. ■

Esempio 9 (gruppi metabeliani)**.** All'inizio abbiamo visto che $\mathbb{Q}/\mathbb{Z}$ è un gruppo abeliano periodico ed è somma diretta di gruppi di Prüfer. Consideriamo invece il suo 2-sottogruppo di Sylow $\mathbb{Q}_2$ ovvero

$$\mathbb{Q}_2 = \left\{ \frac{m}{2^n} \;\middle|\; m \in \mathbb{Z}, n \in \mathbb{N}_0 \right\}$$

Consideriamo l'applicazione $h : a \in \mathbb{Q}_2 \to 2a \in \mathbb{Q}_2$, non è difficile verificare che h è un automorfismo di $\mathbb{Q}_2$ in sé con inversa $h^{-1}(a) = a/2$.

Quindi per ogni $i \in \mathbb{Z}$ le applicazione $h_i(a) = 2^i a$ sono tutti automorfismi di $\mathbb{Q}_2$ e $h_i = (h)^i \in \langle h \rangle$ e quindi possiamo effettuarne il prodotto semidiretto nella seguente maniera

$$G = \langle h \rangle \ltimes \mathbb{Q}_2$$

ricordiamo che per ogni $a, b \in \mathbb{Q}_2$ e $h_i, h_j \in \langle h \rangle$

$$(h_i, a)(h_j, b) = (h_i h_j, h_j(a) b) = \left(h_{i+j}, 2^j a + b\right)$$

Se ora prendiamo $A = \{(\mathrm{id}, a) \in G \mid a \in \mathbb{Q}_2\}$ allora $A \cong \mathbb{Q}_2$, dimostriamo che $A \in \mathrm{Max}-G$.

Fissato $N \leq A$ con $N \lhd G$ non identico poniamo $Z = \{(\mathrm{id}, n) \in G \mid n \in \mathbb{Z}\} \leq A$ allora $N \cap Z \neq \{u\}$ dove $u = (\mathrm{id}, 0)$, supponiamo che $N/N \cap Z$ sia finito di ordine t quindi per ogni $(\mathrm{id}, a) \in N$ avremo $(\mathrm{id}, ta) \in Z$. Ma per la normalità di N in G per ogni $i \in \mathbb{Z}$ avremo

$$(\mathrm{id}, a)^{(h_i, 0)} = \left(\mathrm{id}, 2^i a\right) \in N \to t2^i a \in \mathbb{Z}$$

e questo è possibile se e solo se $a = 0$ e quindi $N = \{u\}$ assurdo. Dunque $|N : N \cap Z| = \infty$.

Allora NZ/Z è un sottogruppo infinito di A/Z il quale è isomorfo a $\mathbb{Z}(2^\infty)$. Quindi per quanto detto all'inizio sui gruppi di Prüfer $NZ = A$ e quindi $A/N \cong Z/(Z \cap N)$ finito essendo $Z \cong \mathbb{Z}$ e $N \cap Z$ non identico.

Adesso presa una qualunque successione crescente di sottogruppi $N_i \leq A$ con $N_i \lhd G$ allora $|A : N_{i+1}| \leq |A : N_i| < \infty$ e quindi questa serie deve terminare prima o poi. Dunque $A \in \mathrm{Max}-G$ e $G/A \in \mathrm{Max}$ essendo ciclico, quindi dalla proposizione 5.5.10 $G \in$ Max-n.

Osserviamo infine che $A \notin \mathrm{Max} \cup$ Max-n in quanto $A/Z \cong \mathbb{Z}(2^\infty)$ che non è Max.

Esempio 10 (metabeliano bis)**.** Consideriamo il campo $\mathbb{Z}_p$ con p primo e la sua chiusura algebrica K. Da un teorema di teoria dei campi si può dimostrare che K ha caratteristica p e $(K, +)$ è un p-gruppo abeliano elementare con

$$(K \setminus \{0\}, \cdot) = \mathop{\mathrm{Dr}}_{q \neq p} X_q \text{ con } X_q \cong \mathbb{Z}(q^\infty)$$

gli X_q sono le *componenti primarie* di K.

Indichiamo per comodità $K^* = K \setminus \{0\}$ con l'operazione di prodotto e fissiamo una sua qualunque componente primaria $(X, \cdot)$. Indichiamo con F il sottocampo di K generato da X, ovvero

$$F = \left\{ \sum_{i=1}^{n} \lambda_i x_i \;\middle|\; n \in \mathbb{N}, \lambda_i \in \mathbb{Z}, x_i \in X \right\}$$

Posto $A = (F, +)$ gruppo per quanto detto sopra è un p-gruppo abeliano elementare infinito e per ogni $x \in X$ l'applicazione

$$f_x : a \in A \to a \cdot x \in A$$

è un isomorfismo di A e quindi possiamo definire l'omomorfismo tra gruppi $v : x \in X \to f_x \in \mathrm{Aut}(A)$ e il relativo prodotto semidiretto

$$G = X \ltimes_v A$$

In questo caso per ogni $a, b \in A$ e $x, y \in X$ abbiamo

$$(x, a)(y, b) = (xy, ay + b)$$

Adesso per ogni $N \leq \overline{A} \cong A$ con $N \lhd G$ non identico, prendiamo allora $a \neq 0$ tale che $(1, a) \in N$. Allora possiamo sempre prenderne l'inverso rispetto al prodotto $a^{-1} = \sum_{i=1}^{n} \lambda_i x_i$. Per normalità allora $(1, ax_i) \in N$ per ogni i e dunque

$$N \ni \prod_{i=1}^{n} (1, ax_i)^{\lambda_i} = \left(1, \sum_{i=1}^{n} \lambda_i a x_i\right) = (1, 1) \Rightarrow (1, 1)^{(x,0)} = (1, x) \in N$$

per ogni $x \in X$ e quindi $N = \overline{A}$ dato che X genera A.

Abbiamo appena dimostrato che $\overline{A} \underset{\min}{\lhd} G$ e quindi $\overline{A} \in \mathrm{Min}-G$, inoltre $G/\overline{A}$ è isomorfo ad un gruppo di Prüfer e quindi $G \in$ Min-n.

Poiché A è un p-gruppo abeliano elementare infinito allora $A \notin \mathrm{Min} \cup$ Min-n e quindi $G \notin$ Min.

Questi esempi mostrano che le inclusioni di queste classi sono tutte disgiunte.

Proposizione 5.5.12. *Sia G gruppo allora $G \in$ Max-n $\Leftrightarrow$ per ogni $H \lhd G$ esiste $E \leq H$ finitamente generato tale che $H = E^G$.*

Dimostrazione. Per assurdo supponiamo che $G \in$ Min-n ma esiste $H \lhd G$ tale che per ogni $E \leq H$ finitamente generato si ha $E^G < H$.

Prendiamo allora $x_1 \in H \setminus \{1\}$ e $N_1 = \langle x_1 \rangle^G \leq H$, ma allora $H \setminus N_1$ non è vuoto e possiamo prendere $x_2 \in H \setminus N_1$ e $N_2 = \langle x_1, x_2 \rangle^G > N_1$. Abbiamo costruito una successione strettamente crescente di sottogruppi normali in G, il che è assurdo in quanto $G \in$ Min-n.

Viceversa prendiamo una qualunque successione crescente di sottogruppi H_i normali in G e definiamo $H = \bigcup_{i=1}^{+\infty} H_i \lhd G$, esisterà allora $E \leq H$ tale che $E = \langle x_1, x_2, \ldots, x_m \rangle$ e $E^G = H$.

Poiché gli H_i sono crescenti ne esisterà uno che conterrà tutti gli x_j, che indicheremo con H_k, quindi $E \leq H_k$ ed essendo $H_k \lhd G$

$$H = E^G \leq H_k \leq H$$

e la serie H_i diventa definitivamente costante. ■

Proposizione 5.5.13. *Se G generico ed $H \lhd G$ con $H \in \mathrm{Min}-G$, allora esiste una serie* ascendente $\{1\} = N_0 \lhd N_1 \lhd \cdots N_\omega = \bigcup_{n\in\mathbb{N}} N_n \lhd \cdots N_\tau = H$ *tale che $N_i \lhd G$ e*

$$\frac{N_{i+1}}{N_i} \underset{min}{\lhd} \frac{G}{N_i}$$

Dimostrazione. La costruiremo tramite l'induzione transfinita. Sia λ ordinale e supponiamo di aver definito N_α per ogni $\alpha < \lambda$, se λ è un ordinale limite allora $N_\lambda = \bigcup_{\alpha<\lambda} H_\alpha$ necessariamente. Supponiamo allora che $\lambda = \alpha + 1$ per un opportuno α e inoltre $N_\alpha < H$ altrimenti possiamo terminare tranquillamente la serie. Allora la classe

$$\{N_\alpha < K \leq H \mid K \lhd G\}$$

possiederà un elemento minimale $N_{\alpha+1} = N_\lambda$. L'induzione transfinita garantisce che questo procedimento porta effettivamente ad una serie, inoltre la serie deve prima o poi arrestarsi in quanto un ordinale λ potrebbe superare la cardinalità di G che ci farebbe esaurire gli elementi. ■

Osservazione. Se $G \in$ Min-n allora per ogni $H \lhd G$ avremo $H \in \mathrm{Min}-G$ e quindi il risultato precedente vale per ogni sottogruppo normale di G.

Proposizione 5.5.14. *Se G è risolubile e* Max-n *allora G è finitamente generato*

Dimostrazione. Utilizzeremo l'induzione sulla lunghezza d della serie derivata. Se $d = 1$ allora G è abeliano, viceversa supponiamolo verificato per $d - 1 \geq 1$ allora $A = G^{(d-1)}$ è abeliano mentre $\mathrm{der}(G/A) = d - 1$ e quindi per la chiusura di Max-n per quozienti $G/A = \langle x_1A, x_2A \ldots, x_tA\rangle = EA$ dove $E = \langle x_1, x_2 \ldots, x_t\rangle$.

Per la proposizione 5.5.12 esiste $K \leq A$ non identico abeliano e finitamente generato per cui $A = K^G$ (si ricorda che Max-n non è chiusa per sottogruppi). Ma allora per ogni $g \in G$ esistono $a \in A \lhd G$ ed $y \in E$ per cui $g = ay$ e dunque

$$K^g = (K^a)^y = K^y \in \langle K, E\rangle \Rightarrow G = \langle K, E\rangle$$

e quindi G è finitamente generato. ■

Vogliamo dimostrare un risultato analogo per Min-n con la periodicità, però la dimostrazione non è elementare come per quella di Max-n e dobbiamo introdurre alcuni concetti preliminari.

Definizione 5.5.15. Sia G gruppo generico, $H \leq G$ e $\Gamma \leq \mathrm{Aut}(G)$. Diciamo che H è Γ-*invariante* se e solo se per ogni $\gamma \in \Gamma$ abbiamo $\gamma(H) \leq H$ ovvero $\gamma(H) = H$.

Se $\Gamma = \mathrm{Aut}(G)$ otteniamo la definizione di sottogruppo caratteristico mentre ogni gruppo caratteristico è Γ-invariante per ogni Γ.

Teorema 5.5.16. *Sia A gruppo abeliano e $\Gamma \leq \mathrm{Aut}(A)$ tale che $\Gamma \neq \{\mathrm{id}\}$ e $\Gamma \in L\mathfrak{F}$. Supponiamo inoltre che A non contenga sottogruppi Γ-invarianti non banali, allora A è un p-gruppo abeliano elementare per un certo primo p.*

Dimostrazione. Per assurdo supponiamo che A non sia un p-gruppo abeliano elementare per nessun primo p, dal teorema di Prüfer-Baer $A \neq A[p]$ per ogni primo p. Chiaramente $A[p]$ è Γ-invariante e dunque $A[p] = \{1\}$ per ogni primo, allora A è aperiodico. Dunque $A^n \neq \{1\}$ per ogni $n \in \mathbb{N}$ e perciò $A^n = A$ essendo anch'esso caratteristico, quindi A è divisibile e senza torsione.

Ora per le nostre ipotesi su Γ deve esistere $b \in A$ e $\gamma \in \Gamma$ per cui $\gamma(b) \neq b$, definiamo inoltre

$$G = \Gamma \ltimes A$$

osserviamo ancora che per ogni $a \in A$, $\gamma \in \Gamma$ visti come elementi di G abbiamo $[a; \gamma] = a^{-1}a^{\gamma} = a^{-1}\gamma(a) \in A$. Questo significa che per ogni $K \leq \Gamma$ utilizzando la proposizione 3.3.11

$$[\langle a \rangle; K] = [a; K]^{\langle a \rangle} \leq A$$

Chiaramente $[b; \Gamma] \lhd A$ mentre per la proposizione 3.3.8 si ha $\Gamma \leq N_G\left([b; \Gamma]\right)$ e quindi $[b; \Gamma] \lhd G$.

Preso adesso $H \leq A$ con $H \lhd G$ allora per ogni $\gamma \in \Gamma$ abbiamo $\gamma\left(H\right) = H^{\gamma} = H$ e quindi per ipotesi $A \underset{\min}{\lhd} G$, ciò implica che $[b; \Gamma] = A$ in quanto $\gamma(b) \neq b$ per un certo $\gamma \in \Gamma$ e quindi non può essere identico.

Ancora $A = [b; \Gamma]$ è divisibile e quindi esiste $x \in [b; \Gamma]$ tale che $b = x^2$ e quindi

$$x \in [b; \langle \gamma_1, \gamma_2, \ldots, \gamma_n \rangle] = [b; E]$$

per opportuni $\gamma_1 \in \Gamma$ ed E è dunque finitamente generato e quindi finito in quanto Γ è localmente finito. Osserviamo che $E \leq N_G\left([b; E]\right)$ e dunque

$$[x; E] \leq [[b; E]; E] \leq [b; E] = \left[x^2; E\right] = [x; E]^2 \tag{5.5.1}$$

L'ultimo passaggio è giustificato tramite la proposizione 3.3.5 con $H = A$. Difatti $A \lhd G$ mentre $[x; \gamma] \leq A \leq C_G\left(A\right)$ per ogni $\gamma \in E$. Dunque essendo A abeliano

$$\left[x^2; E\right] = \left\langle \left[x^2; \gamma_1\right] \cdots \left[x^2; \gamma_i\right] \right\rangle = \left\langle \left([x; \gamma_1] \cdots [x; \gamma_i]\right)^2 \right\rangle = [x; E]^2$$

e $[x; E] = [x; E]^2$.

Ora E è finito e quindi $[x; E]$ è finitamente generato e abeliano, quindi è prodotto diretto di un numero finito di gruppi ciclici. Ma abbiamo detto che A è aperiodico quindi i fattori ciclici sono infiniti, però $[x; E]$ coincide con il suo quadrato e quindi $[x; E] = \{1\}$. Quindi per la 5.5.1 anche $[b; E] = \{1\} \Rightarrow x = 1 \Rightarrow b = 1$ il che è assurdo. ∎

Teorema 5.5.17. *Se G è un gruppo risolubile e* Min-n *allora è periodico.*

Dimostrazione. Utilizzeremo l'induzione su $d = \operatorname{der}(G)$. Se $d = 1$ allora G è abeliano e Min dunque periodico, supponiamo l'asserto vero per $d - 1 \geq 1$ e prendiamo $A = G^{(d-1)}$ dunque G/A è per induzione periodico e risolubile, quindi per la proposizione 4.5.2 $G/A \in L\mathfrak{F}$.

Per la proposizione 5.5.13 esisterà una serie ascendente N_α con $1 \leq \alpha \leq \tau$ con fattori normali minimali in G e $N_\tau = A$. Perso $\alpha < \tau$ poniamo $C = C_G\left(N_{\alpha+1}/N_\alpha\right)$ allora

$$\frac{G}{C} \cong \frac{G/N_\alpha}{C_{G/N_\alpha}\left(N_{\alpha+1}/N_\alpha\right)} \cong \Gamma \leq \operatorname{Aut}\left(\frac{N_{\alpha+1}}{N_\alpha}\right)$$

ricordiamo che gli elementi di Γ sono nella forma

$$\gamma_g : xN_\alpha \to x^g N_\alpha$$

Dunque i sottogruppi Γ-invarianti di $N_{\alpha+1}/N_\alpha$ sono normali in G/N_α e per ipotesi di minimalità di $N_{\alpha+1}/N_\alpha$ devono essere i sottogruppi banali. Quindi non contiene sottogruppi Γ-invarianti non banali.

Ora $A \leq C$ e quindi anche $G/C \in L\mathfrak{F}$, difatti sia $E \leq G$ finitamente generato allora $EA/A \cong E/E \cap A$ è finito. L'applicazione $x\left(E \cap A\right) \to x\left(E \cap C\right)$ è chiaramente suriettiva per ogni $x \in E$ e quindi anche $EC/C \cong E/E \cap C$ deve essere finito.

Se $\Gamma = \{1\}$ allora $G = C$ e questo è possibile se e solo se $N_{\alpha+1}/N_\alpha \leq Z\left(G/N_\alpha\right)$ e quindi $N_{\alpha+1}/N_\alpha$ è caratteristico in G/N_α e non può dunque possedere sottogruppi non banali, quindi o $N_{\alpha+1} = N_\alpha$ oppure $|N_{\alpha+1} : N_\alpha|$ è primo.

Invece se Γ è non identico allora per il teorema 5.5.16 $N_{\alpha+1}/N_\alpha$ è un p-gruppo abeliano elementare, in tutti i casi $N_{\alpha+1}/N_\alpha$ è periodico per ogni $\alpha < \tau$. Se per assurdo $A = N_\tau$ non è periodico allora esiste necessariamente il minimo ordinale $\mu \leq \tau$ per cui N_μ non sia periodico. Se $\mu = \beta + 1$ allora N_β e N_μ/N_β sono periodici e quindi anche N_μ lo deve essere, mentre se μ è limite allora $N_\mu = \bigcup_{\alpha<\mu} N_\alpha$ che sono tutti periodici.

Quindi A è periodico come G/A e dunque G è periodico. ■

Capitolo 6

Classi intermedie

6.1 Locale nilpotenza

Ricordiamo che un gruppo G è localmente nilpotente se e solo se ogni suo sottogruppo finitamente generato è nilpotente, in quanto sappiamo già che i gruppi nilpotenti sono chiusi per sottogruppi.

Innanzitutto mostriamo che non tutti i gruppi localmente nilpotenti sono nilpotenti, l'esempio che utilizzeremo è piuttosto semplice. Per ogni $n \in \mathbb{N}$ scegliamo $G_n \in \mathfrak{N}$ tal che $\mathrm{cl}\,(G_n) = n$ e definiamo

$$G = \operatorname*{Dr}_{n \in \mathbb{N}} G_n$$

Ogni suo sottoinsieme finito può essere generato chiaramente da un numero finito di G_n, per il teorema di Fitting anche il loro prodotto finito è nilpotente.

Se per assurdo G fosse nilpotente con $\mathrm{cl}(G) = c$ allora $n = \mathrm{cl}\,(G_n) < leqc$ per ogni n il che è assurdo. Quindi G è localmente nilpotente ma non nilpotente.

Una delle proprietà più interessanti dei gruppi nilpotenti è quella di possedere un sottogruppo di torsione il quale è prodotto diretto degli elementi di periodo potenza di primo. Possiamo generalizzarlo anche ai gruppi localmente nilpotenti nella seguente maniera

Proposizione 6.1.1. *Se $G \in L\mathfrak{N}$ allora $T = \{g \in G \mid g \text{ periodico}\}$ è un sottogruppo di G con $T = \mathrm{Dr}_{p \text{ primo}} T_p$.*

Dimostrazione. Se π è un insieme di primi prendiamo x, y π-elementi di G, allora $\langle x, y\rangle$ è nilpotente e dal teorema 4.2.10 è un π-gruppo, quindi anche $\{x \in G \mid x\pi\text{-elemento}\}$ è un π-sottogruppo di G.

Da questo punto si procede come nella dimostrazione del teorema 4.2.10. ■

Proposizione 6.1.2. *Se G è localmente nilpotente allora per ogni $N \lessdot G$ si ha $N \lhd G$.*

Dimostrazione. Se per assurdo N non fosse normale in G allora $G' \not\leq N$ e quindi avremmo $c \in G' \setminus N$ e quindi $G = \langle N, c\rangle$.

Inoltre esistono $x_1, y_1, x_2, y_2, \ldots, x_u, y_u \in G$ tali che $c = [x_1; y_1] \cdots [x_u; y_u] \in E'$ con $E = \langle x_1, y_1, \ldots, x_u, y_u \rangle$, inoltre per quanto detto prima per ogni $g \in G$ esiste $F_g \leq N$ finitamente generato per cui $g \in \langle F_g, c \rangle$ e quindi poniamo

$$F = \langle F_{x_i}, F_{y_i} \mid 1 \leq i \leq u \rangle$$

Il sottogruppo F è finitamente generato come anche $H = \langle F, c \rangle$, quindi H è nilpotente contenente E e dal teorema di Wielandt $c \in E' \leq H' \leq \mathrm{Frat}(H)$ ovvero c è un non generatore di H.

Questo porta all'uguaglianza $H = F \leq N$ dunque $c \in N$ il che è assurdo. ■

Proposizione 6.1.3. *Se $G \in L\mathcal{N}$ allora per ogni $N \underset{min}{\lhd} G$ avremo $N \leq Z(G)$.*

Dimostrazione. Se per assurdo esiste $a \in N \setminus Z(G)$ allora esisterebbe un $g \in G$ per cui $h = [a; g] \neq 1$. Ora dalla proposizione 3.3.7 $h \in N$ e dunque $\langle h \rangle^G = N$. Dunque $a \in \langle h^g \mid g \in G \rangle$ e quindi $a \in \langle h^{g_1}, h^{g_2}, \ldots, h^{g_u} \rangle$ per opportuni $g_i \in G$.

Definiamo

$$H = \langle a, g, g_1, g_2, \ldots, g_u \rangle \in \mathcal{N}$$

e anche $A = \langle a \rangle^H \lhd H$. Chiaramente $h \in [A; H]$ e $[A; H] \lhd H$ quindi $h^{g_i} \in [A; H]$ per ogni i dunque $a \in [A; H] \Rightarrow A \leq [A; H]$ e quindi $A = [A; H]$. Perciò per ogni $r \geq 0$ $[A;_r H] = A \leq \gamma_{r+1}(H)$ e poiché H è nilpotente $a = 1$ assurdo, dunque $N \leq Z(G)$. ■

Grazie alla proposizione 1.4.4 la classe dei gruppi localmente nilpotente è chiusa per sottogruppi e quozienti, e come per i gruppi nilpotenti non possiamo stabilire immediatamente che il prodotto di sottogruppi normali sia localmente nilpotente.

Teorema 6.1.4 (Hirish-Plotkin)**.** *Sia G gruppo e $H, K \lhd G$ tali che $H, K \in L\mathcal{N}$, allora $HK \in \mathcal{N}$.*

Dimostrazione. Prendiamo un generico sottogruppo $L \leq HK$ finitamente generato allora $L = \langle h_i k_i \mid 1 \leq i \leq m \rangle$. Poniamo $X = \langle h_i \mid 1 \leq i \leq n \rangle$ e $X = \langle k_i \mid 1 \leq i \leq n \rangle$ dunque $L \leq \langle X, Y \rangle$ e inoltre $X, Y \in \mathcal{N}$. Poiché $X \leq X^Y \lhd \langle X, Y \rangle$ e analogamente con Y segue immediatamente che

$$\langle X, Y \rangle = X^Y Y^X$$

Definiamo ancora $C = \{[h_i; k_j] \mid 1 \leq i, j \leq n\}$ finito allora $C \subseteq [H; K] \leq H \cap K$ essendo normali in G e dunque $C^G \leq H \cap K$. Ora $\langle X, C \rangle$ è finitamente generato e quindi anche nilpotente, per il lemma 4.2.7 soddisfa la condizione massimale e quindi ogni suo sottogruppo è finitamente generato, in particolare C^X. Sempre per normalità $C^X \leq K$ e perciò $\left\langle Y, C^X \right\rangle \leq K$ e finitamente generato quindi è anche nilpotente.

Sempre per il ragionamento di sopra $\left(C^X\right)^Y = C^{XY}$ è finitamente generato, dal corollario 3.3.12 $C^{XY} = [X; Y]$ mentre sappiamo già che $X^Y = \langle X, [X; Y] \rangle$ e $Y^X = \langle Y, [Y; X] \rangle$ che sono finitamente generati. Dal teorema di Fitting $X^Y Y^X \in \mathcal{N}$ e per la chiusura per sottogruppi anche L è nilpotente. ■

Nel primo capitolo abbiamo definito il radicale di un gruppo G, abbiamo anche osservato che il sottogruppo di fitting di G non è nient'altro che in $\mathcal{N}$-radicale di G. Il radicale $\rho_{L\mathcal{N}}(G)$ è detto anche radicale di Hirich-Plotkin.

Come per il sottogruppo di fitting vale il seguente risultato, anche se G non è Max-n

Teorema 6.1.5. *Se G è un gruppo generico allora $\rho_{L\mathcal{N}}(G)$ è localmente nilpotente.*

Dimostrazione. Prendiamo $H \leq \rho_{L\mathcal{N}}(G)$ con $H = \langle h_1, \ldots, h_n \rangle$, esisteranno allora $N_i \lhd G$ e localmente nilpotenti tali che $h_i \in N_1 N_2 \cdots N_m$, per il teorema di Hirish-Plotkin segue immediatamente che $H \in \mathcal{N}$. ■

Il seguente risultato non verrà dimostrato

Teorema 6.1.6.

$$\rho_{L\mathcal{N}}(G) \geq \langle N \leq G \mid N \operatorname{asc} G \text{ e } N \in L\mathcal{N} \rangle$$

invece ne dimostreremo una versione più debole con $H \operatorname{sn} G$. Abbiamo già dimostrato che H è subnormale se e solo se la serie delle chiusure normali $H^{G,i}$ termina in H e la sua lunghezza è la minima possibile.

Utilizzeremo l'induzione sulla lunghezza della serie delle chiusure normali d. Se $d = 1$ allora $H \lhd G$ e localmente nilpotente e quindi $H \leq \rho_{L\mathcal{N}}(G)$ per definizione, altrimenti supponiamolo verificato per $d-1 \geq 1$. In questo caso $H \operatorname{sn} H^G$ e ha lunghezza $d-1$ dunque $H \leq \rho_{L\mathcal{N}}\left(H^G\right) = K$ che per il teorema precedente è ancora localmente nilpotente. Ma K è caratteristico in $H^G \lhd G$ e quindi $K \leq \rho_{L\mathcal{N}}(G)$.

In generale Max-n non è chiuso per sottogruppi come abbiamo detto, sotto condizioni aggiuntive è invece possibile come afferma il seguente risultato

Teorema 6.1.7 (Wilson)**.** *Preso $H \leq G$ tale che $|G : H| < \infty$ allora se $G \in$ Min-n segue che $H \in$ Min-n.*

Dimostrazione. Omessa. ■

Dimostriamo come per i gruppi risolubili le proprietà Max-n e Min-n dei gruppi localmente nilpotenti.

Teorema 6.1.8. *Se $G \in$ Max-n$\cap L\mathcal{N}$ allora G è nilpotente e finitamente generato, in particolare è Max.*

Dimostrazione. Innanzitutto G/G' è Max quindi finitamente generato ovvero $G/G' = \langle x_1 G', x_2 G', \ldots, x_t G' \rangle$. Poniamo $X = \langle x_1, x_2, \ldots, x_t \rangle$ allora $XG' = G$ e X è nilpotente e finitamente generato, quindi esiste $c = \operatorname{cl}(X)$ ed $L = \gamma_{c+2}(G) \neq \{1\}$ e poniamo $\overline{G} = G/L \in$ Max-n.

Ora $\overline{G}/\overline{G}'$ è finitamente generato, inoltre per la proposizione 3.4.13 $\gamma_{c+2}\left(\overline{G}\right) = \{1\}$ e quindi $\overline{G} \in \mathcal{N}$. Possiamo applicare il teorema di Robinson per affermare che $\overline{G}$ è Max dunque $\overline{G}' = \langle g_1, g_2, \ldots g_r \rangle$. Applicando ora il teorema di Wielandt $\overline{G}' \leq \operatorname{Frat}\left(\overline{G}\right)$ e quindi tutti gli g_i sono non generatori di $\overline{G}$.

Forniamo una stima più accurata della classe di nilpotenza di $\overline{G}$, difatti

$$\overline{G} = \frac{XG'}{L} = \frac{XL}{L}\frac{G'L}{L} = \frac{XL}{L}\left(\frac{G}{L}\right)' = \left\langle \frac{XL}{L}, g_1, g_2, \ldots, g_r \right\rangle = \frac{XL}{L}$$

e quindi

$$\gamma_{c+1}\left(\overline{G}\right) = \gamma_{c+1}\left(\frac{X}{X \cap L}\right) = \{1\} = \frac{\gamma_{c+1}(G)}{L} \Rightarrow \gamma_{c+1}(G) = L = \gamma_{c+2}(G) \Rightarrow [L; G] = L$$

La serie centrale inferiore allora si arresta da un certo punto in poi. Se si arresta in $\{1\}$ allora è nilpotente altrimenti non lo è. Se per assurdo $L \neq \{1\}$ allora la classe $\{K \lhd G \mid K < L\}$ è non vuota e possiede un elemento massimale N. Perciò $L/N \underset{\min}{\lhd} G/N$ ma essendo $G/N \in L\mathcal{N}$ per la proposizione 6.1.3 $L/N \leq Z\left(G/N\right)$ dunque $L = [L; G] \leq N$ e dunque $L = N$ ottenendo una contraddizione. Quindi $L = \{1\}$ e G è nilpotente e $G = \overline{G}$ e quindi per la chiusura per estensioni anche G è finitamente generato. ■

Teorema 6.1.9. *Se $G \in$ Min-n $\cap L\mathcal{N}$ allora G è un gruppo di Chernikov.*

Dimostrazione. Posto $J = f^*_{\mathcal{F}}\left(G\right)$ allora $|G : J| < \infty$ e non esiste alcun $H < J$ tale che $|G : H| < \infty$. Per il teorema di Wilson $J \in$ Min-n, dimostriamo che J è abeliano.

Se J fosse non identico allora la classe $\{N \lhd J \mid N \neq \{1\}\}$ ha un elemento minimale A, sempre per la proposizione 6.1.3 $A \leq Z\left(J\right)$ e quindi il centro non è identico. Se per assurdo $Z\left(J\right) < J$ allora $J/Z\left(J\right) \neq \{1\}$ il quale sarebbe ancora Min-n e localmente nilpotente, dunque ripetendo il medesimo ragionamento $Z\left(J/Z\left(J\right)\right) \neq \{1\}$ quindi esisterà quindi $x \in Z_2(G) \setminus Z(G)$.

Sappiamo che Min-n non è chiusa per sottogruppi, ma sappiamo che tutti i sottogruppi del centro sono normali e quindi $Z\left(J\right)$ e $Z\left(J/Z\left(J\right)\right)$ sono Min-n ovvero Min essendo abeliani, dunque $Z_2(G) \in$ Min in particolare è periodico. Sia n il periodo di x, allora per ogni $y \in J$ avremmo $[x; y] \in Z\left(J\right)$ e dunque dalla proposizione 3.3.5 $[x; y] = 1$ dunque $[x; y] \in Z\left(J\right)[n]$, il quale per il teorema di struttura dei gruppi Min è finito.

Ciò significa che $\{x^y \mid y \in J\}$ è finito ovvero $|J : C_J\left(x\right)| < \infty$ e dunque $J = C_J\left(x\right)$ ovvero $x \in Z\left(J\right)$ assurdo, quindi J è abeliano e dunque Min. Dal teorema di struttura per gruppi Min $J = P \times E$ con E finito e P prodotto diretto di un numero finito di gruppi di Prüfer. Infine

$$|G : P| = |G : J|\,|J : P| = |G : J|\,|E| < \infty$$

quindi $C \in \mathcal{C}$. ■

Esempio 11. In generale gruppi localmente nilpotenti e di Chernikov non sono anche nilpotenti. Difatti se prendiamo $A \cong \mathbb{Z}\left(2^\infty\right)$ e $G = D_A = \langle x \rangle \ltimes A$, chiamato anche 2-*gruppo localmente diedrale*. Banalmente $G \in \mathcal{C}$ e tutti i suoi sottogruppi diversi da G e A, che non sono finitamente generati, sono finiti con ordine 2^k quindi G è localmente nilpotente.

Dimostriamo che G non è nilpotente, per ogni $n \in \mathbb{N}_0$ prendiamo A_n l'unico sottogruppo di A con ordine 2^n, mostriamo per induzione che $Z_n(D_A) = A_n$. Se $n = 0$ è banale mentre $Z(G) = A[2] = A_1$, supponiamo per induzione che $Z_n(G) = A_n$ con $n \geq 1$ allora

$$\frac{D_A}{Z_n(D_A)} = \frac{\langle x \rangle A}{A_n} = \langle x A_n \rangle \ltimes \frac{A}{A_n} = D_{A/A_n}$$

dunque

$$Z\left(\frac{D_A}{Z_n(D_A)}\right) = \frac{A}{A_n}[2] = \left\{ aA \mid a \in A, a^2 \in A_n \right\} = \frac{A_{n+1}}{A_n}$$

perciò $Z_{n+1}(G) = A_{n+1}$. Per questo motivo la serie centrale superiore è infinita e G non è nilpotente.

Un ultima osservazione prima di passare oltre. Ricordiamo che la serie centrale superiore è una serie ascendente e quindi può essere definita anche per ordinali infiniti. Posto $\omega = \mathbb{N}$ il primo cardinale limite abbiamo $Z_\omega(G) = A$ e $Z_{\omega+1}(G) = G$. Il gruppo 2-localmente diedrale, come vedremo ora, è un buon esempio di gruppo *ipercentrale* ma non nilpotente.

6.2 Altre classi

In questa sezione introdurremo varie classi di gruppi che si interpongono tra la classe $L\mathcal{N}$ e quella $\mathcal{N}$.

Innanzitutto la proposizione 3.2.7 afferma che preso un $H \operatorname{asc} G$ con $H < G$ allora $H < N_G(H)$. Quindi se in un gruppo G ogni suo sottogruppo è ascendente (per esempio se G è nilpotente) allora i sottogruppi propri soddisfano la cosiddetta *condizione dei normalizzanti* ovvero sono propriamente contenuti nel proprio normalizzante.

In questa versione più debole vale anche l'inverso, cioè

Proposizione 6.2.1. *Se per ogni $H < G$ si ha $H < N_G(H)$ allora $H \operatorname{asc} G$ per ogni $H \leq G$.*

Dimostrazione. Costruiamo una serie ascendente nella seguente maniera

$$\begin{cases} H_0 = H \\ H_{\alpha+1} = N_G(H_\alpha) \\ H_\lambda = \bigcup_{\alpha<\lambda} H_\alpha & \text{se } \lambda \text{ limite} \end{cases}$$

Questa serie non può crescere indefinitamente, esisterà dunque un ordinale β per cui $H_\beta = N_G(H_\beta)$ e questo implica che $H_\beta = G$ per la condizione dei normalizzanti e quindi $H \operatorname{asc} G$. ∎

Se la condizione dei normalizzanti non vale per tutti i sottogruppi allora il risultato non è più valido.

Elenchiamo le varie classi che analizzeremo all'interno della sezione

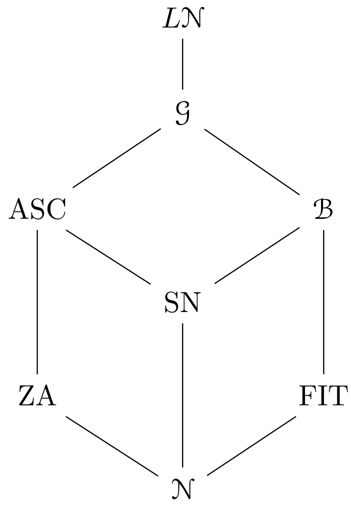

Figura 6.1: Classi intermedie tra $\mathcal{N}$ e $L\mathcal{N}$

Definizione 6.2.2. Un gruppo G tale che $H \operatorname{asc} G$ per ogni $H \leq G$ è detto *ascendente*. La classe dei gruppi ascendenti si indica con ASC.

Definizione 6.2.3. Un gruppo G è di *Gruemberg* se e solo se per ogni $g \in G$ si ha $\langle g \rangle \operatorname{asc} G$. La classe dei di Gruemberg si indica con $\mathcal{G}$.

Definizione 6.2.4. Un gruppo G è di *Baer* se e solo se $\langle g \rangle \operatorname{sn} G$ per ogni $g \in G$. La classe dei gruppi di Baer si indica con $\mathcal{B}$.

Definizione 6.2.5. Un gruppo G tale che $G = \mathrm{FIT}(G)$ è detto di *fitting*.

Definizione 6.2.6. Un gruppo G tale che esiste un ordinale β per cui $G = Z_\beta(G)$ è detto *ipercentrale*. La classe dei gruppi ipercentrali si indica con ZA.

Definizione 6.2.7. Diciamo che un gruppo G soddisfa la condizione dei subnormali se e solo se per ogni $H \leq G$ si ha $H \operatorname{sn} G$.

I gruppi nilpotenti appartengono a tutte queste classi, che difatti sono tutte ottenute a partire dalle proprietà dei gruppi nilpotenti dimostrate precedentemente. Da adesso in poi dimostreremo le eventuali inclusioni tra queste classi, che sono state riassunte nel seguente grafico in figura 6.1 dove le classi più in alto contengono quelle più in basso

Dimostriamo ora le varie inclusioni. Innanzitutto è banale verificare che i gruppi ascendenti ed i gruppi di Baer sono anche di Gruemberg.

Proposizione 6.2.8. *I gruppi di Gruemberg sono localmente nilpotenti.*

Dimostrazione. Preso $G \in \mathcal{G}$ allora per ogni $g \in G$ abbiamo $\langle g \rangle \operatorname{asc} G$ e $\langle g \rangle$ nilpotente essendo abeliano. Per il teorema 6.1.6 $\langle g \rangle \leq \rho_{L\mathcal{N}}(G)$ e quindi $G = \rho_{L\mathcal{N}}(G) \in L\mathcal{N}$ per il teorema 6.1.5. ∎

Proposizione 6.2.9. *Se $G \in L\mathfrak{N}$ e G è numerabile allora $G \in \mathfrak{G}$.*

Dimostrazione. Prendiamo $g \in G = \{y_n \mid n \in \mathbb{N}\}$ e poniamo $H_0 = \langle g \rangle$. Allora per ogni $k \in \mathbb{N}$ definiamo per ricorrenza

$$H_k = \langle H_{k-1}, y_k \rangle$$

tutti gli H_k saranno finitamente generati e perciò nilpotenti quindi $H_{k-1} \operatorname{sn} H_k$ per ogni $k \in \mathbb{N}$.

Se esistesse un $k \in \mathbb{N}$ tale che $H_k = G$ allora possiamo comporre tranquillamente le varie serie ottenendo $\langle g \rangle = H_0 \operatorname{sn} H_k = G$, altrimenti $H_\omega = \bigcup_{k=0}^{+\infty} H_k = G$ in quanto $y_k \in H_k$ e dunque $\langle g \rangle \operatorname{asc} G$. ■

Proposizione 6.2.10. *I gruppi di fitting sono di Baer.*

Dimostrazione. Sia G un gruppo di fitting, allora per ogni $x \in G$ avremo $\langle x \rangle^G \in \mathfrak{N}$ e quindi $\langle x \rangle \operatorname{sn} \langle x \rangle^G \lhd G$ e quindi G è di Baer. ■

Proposizione 6.2.11. ZA $\subseteq$ ASC

Dimostrazione. Esiste un ordinale β tale che $Z_\beta(G) = G$, consideriamo allora la serie ascendente $HZ_\alpha(G)$, allora possiamo procedere come nella dimostrazione del lemma 4.2.1 per dimostrare che $HZ_\alpha(G) \lhd HZ_{\alpha+1}(G)$.

Inoltre se λ è un ordinale limite allora $\bigcup_{\alpha<\lambda} HZ_\alpha(G) \leq HZ_\lambda(G)$, viceversa per ogni $x \in HZ_\lambda(G)$ esiste $h \in H$ tale che $h^{-1}x \in Z_\lambda(G)$. Per definizione allora esisterà $\alpha < \lambda$ tale che $h^{-1}x \in Z_\alpha(G)$ e quindi $\bigcup_{\alpha<\lambda} HZ_\alpha(G) = HZ_\lambda(G)$ e quindi abbiamo ottenuto una serie ascendente da H a G. ■

Proposizione 6.2.12. *Un gruppo G è ipercentrale se e solo se esiste una serie ascendente e centrale da $\{1\}$ a G.*

Dimostrazione. Sia $\{1\} = G_0 \lhd G_1 \lhd \cdots G_\beta = G$ tale che $G_\alpha \lhd G$ e $G_{\alpha+1}/G_\alpha \leq Z(G/G_\alpha)$ dimostriamo per induzione che $G_\alpha \leq Z_\alpha(G)$ per ogni ordinale $\alpha \leq \beta$.

Se esiste $\gamma < \beta$ tale che $\alpha = \gamma + 1$ e $G_\gamma \leq Z_\gamma(G)$ allora

$$\begin{aligned}\frac{G_{\gamma+1}}{G_\gamma} \leq Z\left(\frac{G}{G_\gamma}\right) \Leftrightarrow [G; G_{\gamma+1}] \leq G_\gamma \leq Z_\gamma(G) \Rightarrow \frac{G_{\gamma+1}Z_\gamma(G)}{Z_\gamma(G)} &\leq Z\left(\frac{G}{Z_\gamma(G)}\right)\\ = \frac{Z_{\gamma+1}(G)}{Z_\gamma(G)} \Rightarrow G_{\gamma+1}Z_\gamma(G) \leq Z_{\gamma+1}(G) &\Rightarrow G_{\gamma+1} \leq Z_{\gamma+1}(G)\end{aligned}$$

Sia ora $\lambda \leq \beta$ ordinale limite tale che $G_\alpha \leq Z_\alpha(G)$ per ogni $\alpha < \lambda$ allora dalla definizione di serie

$$G_\lambda = \bigcup_{\alpha<\lambda} G_\alpha \leq \bigcup_{\alpha<\lambda} Z_\alpha(G) = Z_\lambda(G)$$

e quindi otteniamo la tesi poiché $G = G_\beta \leq Z_\beta(G)$ ■

Teorema 6.2.13. *Se G è localmente nilpotente e* Min-n *allora è ipercentrale.*

Dimostrazione. Dalla proposizione 5.5.13 esiste una serie ascendente G_α fino a G tale che $G_{\alpha+1}/G_\alpha \underset{\min}{\lhd} G/G_\alpha$, dalla proposizione 6.1.3 $G_{\alpha+1}/G_\alpha \leq Z(G/G_\alpha)$ ed è quindi una serie centrale e ascendente. ■

Osservazione. Sappiamo già che se $G \in L\mathfrak{N} \cap$ Min-n allora G è un gruppo di Chernikov, quindi posto $J = f^*_{\mathcal{F}}(G)$ avremo dalla proposizione 5.5.6 che G/J è finito mentre $J = P_1 \times P_2 \times \cdots \times P_t$ con $P_t \cong \mathbb{Z}(p_t{}^\infty)$ con p_i non necessariamente distinti. Quindi J è abeliano e possiamo definire per ogni $n \in \mathbb{N}$

$$S_n = J\left[(p_1 p_2 \cdots p_t)^n\right]$$

Ora S_n è caratteristico in J ed è finito con $\bigcup_{n\in\mathbb{N}} S_n = J$ quindi $S_n \lhd G$. Prendiamo ora un generico $N \lhd G$ finito allora per le proposizioni 5.5.13 e 6.1.3 esisterà una serie finita $\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_u = N$ tale che $N_i \lhd G$ e $N_{i+1}/N_i \leq Z(G/N_i)$ ovvero $N_i \leq Z_i(G)$.

Dunque $N \leq Z_\omega(G)$ per ogni $N \lhd G$ finito e quindi $J \leq Z_\omega(G)$. Quindi anche $G/Z_\omega(G)$ è finito ed essendo $G \in L\mathfrak{N}$ allora guel quoziente è nilpotente. Non possiamo dire che anche G sia nilpotente, basta considerare ad esempio il 2-gruppo localmente diedrale il quale è localmente nilpotente e Min ma non nilpotente.

Teorema 6.2.14. *Se G è un gruppo di Baer* Min-n *allora $G/Z(G)$ è finito e $G \in \mathfrak{N}$.*

Dimostrazione. Il gruppo G è un gruppo di Chernikov e perciò $|G : J| < \infty$. Dimostriamo per induzione che $[J;_m \langle x\rangle]$ è abeliano e divisibile per ogni $x \in G$ e $m \in \mathbb{N}_0$.

Per $m = 0$ sappiamo già che J è abeliano e divisibile, supponiamo l'asserto vero per $m \geq 0$. Sia $n \in \mathbb{N}$ generico allora poiché $J \lhd G$ $[J;_{m+1} \langle x\rangle]^n = [[J;_m \langle x\rangle]; \langle x\rangle]^n \leq J$ e possiamo quindi applicare la proposizione 3.3.5

$$[J;_{m+1} \langle x\rangle]^n = [[J;_m \langle x\rangle]; \langle x\rangle]^n = [[J;_m \langle x\rangle]^n; \langle x\rangle] = [[J;_m \langle x\rangle]; \langle x\rangle] = [J;_{m+1} \langle x\rangle]$$

Per assurdo supponiamo che $J \nleq Z(G)$ allora esiste $g \in G$ per cui $[g; J] \neq \{1\}$, ricordiamoci che $G \in bae$ e perciò esiste una serie finita $\langle g\rangle = H_0 \lhd H_1 \lhd \cdots \lhd H_d = G$ con d la minima lunghezza possibile di tale serie. Dimostriamo per induzione che

$$[G;_i \langle g\rangle] \leq H_{d-i}$$

Se $i = 0$ è banale, altrimenti supponiamolo verificato per un certo $i \geq 0$ allora

$$[G;_{i+1} \langle g\rangle] = [[G;_i \langle g\rangle]; \langle g\rangle] \leq [H_{d-i}; \langle g\rangle] \leq [H_{d-i}; H_{d-i-1}] \leq H_{d-i-1}$$

dove l'ultima disuguaglianza deriva dalla relazione $H_{d-i-1} \lhd H_{d-i}$. Quindi $[G;_d \langle g\rangle] \leq \langle g\rangle$ abeliano e perciò $[G;_{d+1} \langle g\rangle] = \{1\} \Rightarrow [J;_{d+1} \langle g\rangle] = \{1\}$.

Prendiamo $r \leq d$ il più piccolo possibile affinché $[J;_{d+1} \langle g\rangle] = \{1\}$ allora $[J;_r \langle g\rangle] \neq \{1\}$, per ipotesi allora $r \geq 1$. Posto $M = [J;_{r-1} \langle g\rangle]$ allora $[M; \langle g\rangle] \neq \{1\}$ e $[M;_2 \langle g\rangle] = \{1\}$, ancora i gruppi di Chernikov sono sempre periodici dunque esisterà $n \in \mathbb{N}$ tale che $\langle g\rangle = n$.

Chiaramente $[M;\langle g\rangle] \leq C_G(\langle g\rangle)$ e inoltre $[M;\langle g\rangle]^n = [M^n;\langle g\rangle]$, quindi applicando il lemma 3.3.4

$$[M;\langle g\rangle] = [M^n;\langle g\rangle] = [M;\langle g\rangle]^n = [M;\langle g\rangle^n] = \{1\}$$

per la divisibilità di M, generando così un assurdo.

Perciò $J \leq Z(G)$ e $G/Z(G)$ è finito dunque nilpotente poiché $G \in L\mathfrak{N}$ ovvero $G \in \mathfrak{N}$. ■

Lemma 6.2.15. *Se G è un gruppo metabeliano ed esiste un p primo tale che $(G')^p = \{1\}$ allora per ogni $n \in \mathbb{N}_0$ ed $x, y \in G$*

$$[x;_{p^n} y] = \left[x; y^{p^n}\right]$$

Dimostrazione. Omessa. ■

Proposizione 6.2.16. *Se $G = A\langle g\rangle$ con $A \lhd G$ abeliano. Se esiste $r \in \mathbb{N}_0$ tale che $[A;_r \langle g\rangle] = \{1\}$ allora $\langle g\rangle \operatorname{sn} G$.*

Dimostrazione. Se $r = 0$ allora $G = \langle g\rangle$ altrimenti supponiamolo vero per $r - 1 \geq 0$. In questo caso $[A;_r \langle g\rangle] = \{1\} \Rightarrow [A;_{r-1} \langle g\rangle] \leq C_G(\langle g\rangle)$ e per le ipotesi su A allora $[A;_{r-1} \langle g\rangle] \leq Z(G)$.

Posto $\overline{G} = G/Z(G) = \overline{A}\langle\overline{g}\rangle$ allora $\overline{A} \lhd \overline{G}$ abeliano e per un risultato precedente

$$\left[\overline{A};_{r-1} \langle\overline{g}\rangle\right] = \frac{[A;_{r-1}\langle g\rangle] Z(G)}{Z(G)} = \{1\} \Rightarrow \langle\overline{g}\rangle \operatorname{sn} \overline{G} \Rightarrow \langle g\rangle Z(G) \operatorname{sn} G$$

la tesi segue osservando che $Z(G) \leq N_G(\langle g\rangle)$ e quindi $\langle g\rangle \lhd \langle g\rangle Z(G)$. ■

Teorema 6.2.17. *Ogni p-gruppo risolubile con esponente finito è un gruppo di Baer.*

Dimostrazione. Prendiamo un gruppo G risolubile di esponente finito, allora per ogni $i \in \mathbb{N}$ $A = G^{(i)}/G^{(i+1)}$ è un p-gruppo abeliano di esponente finito, dunque esisterà $t \in \mathbb{N}$ tale che $A\left[p^t\right] = A$. Costruiamo così la serie finita

$$\{1\} \leq A[p] \leq A\left[p^2\right] \leq \cdots \leq A\left[p^t\right] = A$$

Scelto $0 \leq j < t$ e $a \in A\left[p^{j+1}\right]$ allora $a^p \in A\left[p^j\right]$ e quindi per il teorema di Prüfer-Baer $A\left[p^{j+1}\right]/A\left[p^j\right]$ è un p-gruppo abeliano elementare. Adesso poiché $A \lhd G/G^{(i+1)}$ poniamo $H_j \lhd G$ tale che

$$A\left[p^j\right] = \frac{H_j}{G^{(i+1)}}$$

allora H_j è una serie normale in G da $G^{(i+1)}$ a $G^{(j)}$ quindi le possiamo comporre in modo tale da ottenere una serie normale finita di G di lunghezza $s \in \mathbb{N}$ i cui fattori sono p-gruppo abeliano elementare.

Se $s = 1$ allora G è abeliano e quindi un gruppo di Baer, altrimenti supponiamo l'asserto vero per ogni serie di lunghezza $s - 1$, indichiamo con G_t questa serie crescente allora per passo induttivo $G/G_1 \in \mathcal{B}$ allora per ogni $g \in G$ avremo $\langle gG_1 \rangle \operatorname{sn} G/G_1$. Questo significa che $\langle g \rangle G_1 \operatorname{sn} G$ e dobbiamo solamente dimostrare che $\langle g \rangle \operatorname{sn} \langle g \rangle G_1$.

Scelto $a \in G_1$ e $x \in \langle g \rangle$ allora $[a; x] \in G_1 \Rightarrow [a; x]^p = 1$. Per il lemma 6.2.15, scelto $l \in \mathbb{N}$ in modo tale che $|\langle g \rangle| = p^l$

$$[a;_{p^l} x] = \left[a; x^{p^l}\right] = 1 \Rightarrow [G_1;_{p^l} \langle g \rangle] = \{1\}$$

e dunque per la proposizione precedente (G_1 è un p-gruppo abeliano elementare) abbiamo $\langle g \rangle \operatorname{sn} \langle g \rangle G_1$ e il teorema è così dimostrato. ■

6.3 Casi notevoli

In questa sezione mostreremo alcuni esempi di gruppi con i quali dimostreremo che le varie classi introdotte nella precedente sezione sono tutte disgiunte tra loro.

Esempio 12 (FIT non ascendente)**.** Prendiamo A gruppo ciclico di ordine p e X un p-gruppo abeliano elementare equipotente ad $\mathbb{N}$. Definiamo

$$G = A \sim X = X \ltimes B$$

il prodotto intrecciato tra X e A con $B = \mathrm{Dr}_{x \in X} A_x$. Ricordiamo che da come abbiamo definito il prodotto intrecciato $A^x = A_x$ per ogni $x \in X \leq G$, dimostriamo che $G = \mathrm{FIT}(G)$.

Innanzitutto G/B è abeliano e perciò $\langle x \rangle B \lhd G$ per ogni $x \in X$ mentre $G' \leq B$, ma B è abeliano dunque G è risolubile. Il gruppo G ha esponente minore o uguale a p^2, difatti per ogni $x \in X, b \in B$

$$(xb)^{p^2} \in (xB)^{p^2} = (x^p B)^p = B^p = \{1\}$$

dunque per il teorema 6.2.17 G è un gruppo di Baer.

Quindi per ogni $x \in X$ avremo che $\langle x \rangle \operatorname{sn} G$ e in particolare $\langle x \rangle \operatorname{sn} \langle x \rangle B$. Ora abbiamo $\langle x \rangle$ ciclico di ordine p e B un p-gruppo abeliano elementare e quindi sono entrambi nilpotenti. Esisterà allora $H \leq G$ tale che $\langle x \rangle \lhd H$ e perciò $\langle x \rangle B \lhd HB$ e possiamo perciò applicare il teorema di Fitting e $\langle x \rangle B \in \mathcal{N}$. Dimostriamo adesso che $\langle x \rangle B \lhd G$, per ogni $y \in X$ abeliano avremo $xy = yx$ e $yB = By$ dunque $X \leq N_G(\langle x \rangle B)$ e quindi $\langle x \rangle B \lhd G$ e

$$G = \langle \langle x \rangle B \mid x \in X \rangle \,\mathrm{FIT}(G)$$

Dimostriamo ora che G non soddisfa la condizione dei normalizzanti. Dall'identità di Dedekind $N_G(X) = N_G(X) \cap XB = X(N_G(X) \cap B)$ mentre per la normalità di B

$$[N_G(X) \cap B; X] \leq X \cap B = \{1\} \Rightarrow N_G(X) \cap B \leq C_G(X)$$

inoltre B è abeliano e quindi $N_G(X) \cap B \leq C_G(B)$ e dunque $N_G(X) \cap B \leq Z(G) = \{1\}$ per il teorema 1.5.2 essendo X infinito. Ma $N_G(X)$ è un sottogruppo di G contenente X e perciò $X = N_G(X)$ quindi G non soddisfa la condizione dei normalizzanti e in particolare non è ascendente.

Esempio 13 ($\mathfrak{B}$ non FIT)**.** Stavolta prendiamo H un p-gruppo infinito, risolubile ma *non nilpotente* e con esponente finito (per esempio quello dell'esempio precedente). Prendiamo anche $C = \langle g \rangle$ gruppo ciclico di ordine p e definiamo

$$G = H \sim C = C \ltimes B$$

con $B = H_0 \times H_1 \times \cdots \times H_{p-1}$ con $H^{g^i} = H_i$. Dal corollario 3.2.11 B è risolubile oltre ad essere un p-gruppo di esponente finito e $|G : B| = p$, dunque per la chiusura per estensioni $G \in \mathfrak{S}$ ed è ancora un p-gruppo di esponente finito ovvero di Baer.

Dimostriamo che non è un gruppo di fitting. Poiché H non è nilpotente allora $\gamma_n(H) \neq \{1\}$ per ogni $n \in \mathbb{N}$ ovvero per la proposizione 3.4.11 esisteranno $a_1, a_2, \ldots, a_n \in H$ tali che $[a_1, a_2, \ldots, a_n] \neq 1$.

Ora per ogni i abbiamo $a_i^g \in H_1$ e dunque $c_i\,[g; a_i] \in H \times H_1$ da cui segue immediatamente che $[c_1, c_2, \ldots, c_n] \in H \times H_1$ e la sua componente su H è esattamente $[a_1, a_2, \ldots, a_n]$. Ora $c_i = g^{-1} g^{a_i} \in C^G$ e dunque

$$1 \neq [c_1, c_2, \ldots, c_n] \in \gamma_n \left(C^G\right)$$

Abbiamo appena mostrato che $\langle g \rangle^G \notin \mathfrak{N}$ e quindi $g \notin \mathrm{FIT}(G)$.

Prima di enunciare il prossimo esempio dimostriamo la seguente proposizione

Proposizione 6.3.1. *Sia A gruppo ciclico con $|A| = 2^n > 2$ e $G = D_A = \langle x \rangle \ltimes A$ gruppo diedrale allora il difetto di $\langle x \rangle$ in G è pari ad n e* $\mathrm{cl}(G) = n$.

Dimostrazione. Dimostriamo le due asserzioni, ponendo per comodità $A_i = A\left[2^i\right]$ crescente.

- Dimostriamo innanzitutto per induzione che $\langle x \rangle^{G,i} = \langle x \rangle \ltimes A\left[2^{n-i}\right]$ per ogni $0 \leq i \leq n$. Se $i = 0$ allora è banale, altrimenti supponiamolo verificato per un certo $i \geq 0$ allora $\langle x \rangle^{G,i} = \langle x \rangle \ltimes A\left[2^{n-i}\right]$.

  Sappiamo già che $\langle x \rangle^{G,i+1} = \langle x \rangle^{\langle x \rangle \ltimes A\left[2^{n-i}\right]}$, inoltre per ogni $a \in A$ si ha $x^a = a^{-1}xa = xa^2$ e quindi
  $$\langle x \rangle^{G,i+1} \leq \langle x \rangle \ltimes A\left[2^{n-i-1}\right]$$
  ma essendo $\left|A\left[2^{n-i}\right] : A\left[2^{n-i-1}\right]\right| = 2$ allora è normale e vale l'uguaglianza.

- Dimostriamo per induzione che $Z_i(G) = A\left[2^i\right]$ per ogni $0 \leq i < n-1$, se $i = 0$ è banale altrimenti supponiamo che $A_i = Z_i(G)$ per un certo $0 \leq i < n-2$.

  Innanzitutto si ha
  $$\frac{Z_{i+1}(G)}{Z_i(G)} = Z\left(\langle xA_i \rangle \ltimes \frac{A_n}{A_i}\right)$$
  con $|A_n : A_i| = 2^{n-i}$ e quindi $i < n-2 \Rightarrow n-i > 2$ e il gruppo è *diedrale* (altrimenti otterremo un gruppo di Klein abeliano) e possiamo così applicare la proposizione 1.2.13
  $$\frac{Z_{i+1}(G)}{Z_i(G)} = \frac{A_n}{A_i}[2] = \frac{A_{i+1}}{A_i}$$

e dunque $Z_{i+1}(G) = A_{i+1}$.

Se invece $i = n-1$ allora G/A_{n-1} è il gruppo di Klein che è abeliano e perciò $Z_{n-1}(G) = G$.

$\blacksquare$

Esempio 14 (Ipercentrale non nilpotente né Baer)**.** Prendiamo qui $G = \langle x \rangle \ltimes \mathbb{Z}(2^\infty)$ il 2-gruppo localmente diedrale.

Dimostriamo prima di tutto che $\langle x \rangle^G = G$, difatti con un ragionamento analogo fatto nella dimostrazione della proposizione precedente avremo $\langle x \rangle^G \geq \langle x \rangle \ltimes A_n$ per ogni $n \in \mathbb{N}$, quindi $G \notin \mathcal{B}$.

Ancora, sempre come nella proposizione precedente $Z_i(G) = A_i \Rightarrow Z_\omega(G) = A \Rightarrow Z_{\omega+1}(G) = G$ e quindi G è ipercentrale ma non nilpotente.

Esempio 15 (FIT e ipercentrale ma non subnormale)**.** Per ogni $n \in \mathbb{N}$ prendiamo un gruppo ciclico B_n di cardinalità 2^n e poniamo $G_n = D_{B_n} = \langle x_n \rangle \ltimes B_n$ prodotto diedrale. Definiamo allora

$$G = \operatorname*{Dr}_{n \in \mathbb{N}} G_n$$

Chiaramente $G_n \in \mathcal{N}$ per ogni $n \in \mathbb{N}$ e dal teorema di Fitting anche il prodotto di un numero finito di essi è nilpotente oltre ad essere normale, dunque $G = \mathrm{FIT}(G)$, dimostriamo che $G = Z_\omega(G)$.

Per ogni $N \lhd G$ finito chiaramente $N \in \mathrm{Min}-G$ e per la proposizione 5.5.13 esiste una serie finita $\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_t = N$ normale in G tale che $N_{i+1}/N_i \underset{\min}{\lhd} G/N_i$. Per quanto detto prima $G \in L\mathcal{N}$ e dunque per la proposizione 6.1.3 $N_{i+1}/N_i \leq Z(G/N_i)$, ora essendo $N_0 = \{1\} = Z_0(G)$ possiamo dimostrare per induzione che $N_i \leq Z_i(G)$ per ogni i e dunque $N \leq Z_\omega(G)$ per ogni $N \lhd G$ finito.

Ma allora $G_n \leq \mathbb{Z}_\omega(G)$ essendo finiti e quindi G è ipercentrale. Dimostriamo ora che esiste un sottogruppo H di G non subnormale. Prendiamo $H = \mathrm{Dr}_{n\in\mathbb{N}} \langle x_n \rangle$ se per assurdo fosse subnormale con difetto d in G allora $H \cap G_n = \langle x_n \rangle$ deve avere difetto minore o uguale a d in G_n, il che è assurdo per la proposizione di prima.

Capitolo 7

Rango di un gruppo

7.1 Rango di gruppi abeliani

Definizione 7.1.1. Consideriamo un gruppo abeliano $(A, +)$ ed $S \subseteq A$ non vuoto, diciamo che S è *linearmente indipendente* se e solo se $0 \notin S$ e per ogni $x_1, x_2, \dots, x_r \in S$ distinti tali che esistono $n_1, n_2, \dots, n_r \in \mathbb{Z}$ per cui

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0$$

allora $n_ix_i = 0$ per ogni i.

Un insieme indipendente $S \subseteq A$ si dice *aperiodico* se e solo se è composto interamente da elementi aperiodici, invece si dice *p-indipendente* per un certo p primo se e solo se è composto da elementi di periodo potenza di p.

Non chiediamo che $x_i = 0$ per ogni i, altrimenti nessun gruppo abeliano periodico possiederebbe sottoinsiemi linearmente indipendenti. Inoltre sottoinsiemi non vuoti di insiemi indipendenti sono ancora indipendenti.

Osservazione. Sia $S \subseteq A$ linearmente indipendente e siano $s_1, \dots, s_r \in S$ ed $n_1, \dots, n_r \in \mathbb{Z}$.

- Se S è aperiodico allora

$$n_1s_1 + n_2s_2 + \cdots + n_ks_k = 0 \Rightarrow n_i = 0 \, \forall i$$

- Se S è p indipendente allora

$$n_1s_1 + n_2s_2 + \cdots + n_ks_k = 0 \Rightarrow p \mid n_i \, \forall i$$

Proposizione 7.1.2. *Sia $S \subseteq A$ abeliano, allora S è indipendente se e solo se $\langle S \rangle = \bigoplus_{x \in S} \langle x \rangle$.*

Dimostrazione. Supponiamo che S sia indipendente, dobbiamo solo dimostrare che per ogni $x \in S$ si ha $\langle x \rangle \cap \langle y \mid y \in S, y \neq x \rangle = \{0\}$. Sia $g \in \langle x \rangle \cap \langle y \mid y \in S, y \neq x \rangle$ allora esistono $y_1, y_2, \dots, y_r \in S$ distinti e diversi da x ed $n, n_1, n_2, \dots, n_r \in \mathbb{Z}$ tali che

$$\begin{aligned} g = nx = n_1y_1 + n_2y_2 + \cdots + n_ry_r &\Rightarrow nx - n_1y_1 - n_2y_2 - \cdots - n_ry_r = 0 \\ &\Rightarrow g = nx = 0 \end{aligned}$$

e dunque formano un prodotto diretto.

Viceversa supponiamo che $\langle S \rangle = \bigoplus_{x \in S} \langle x \rangle$ e prendiamo $x_1, x_2, \dots, x_r \in S$ distinti ed $n_1, n_2, \dots, n_r \in \mathbb{Z}$ tali che $\sum_{i=1}^r n_ix_i = 0$. Chiaramente $n_ix_i \in \langle x_i \rangle$ e per l'unicità della scrittura nei prodotti diretti $n_1x_i = 0$. ■

Lemma 7.1.3. *Sia A abeliano ed $V \subseteq A$ non vuoto e contenente almeno un elemento diverso da 0. Se $X \subseteq V$ è un sottoinsieme indipendente di A allora la classe*

$$\mathcal{L}_V = \{S \subseteq V \mid X \subseteq S, S \text{ indipendente in } A\}$$

è induttiva rispetto all'inclusione, quindi possiede elementi massimali.

Dimostrazione. La dimostrazione è immediata, innanzitutto è non vuota poi la proprietà di indipendenza è una proprietà locale in quanto coinvolge solamente un numero di elementi finiti in ogni caso, dunque l'unione arbitraria di sottoinsiemi indipendenti totalmente ordinati rispetto all'inclusione è ancora indipendente. ■

Proposizione 7.1.4. *Un sottoinsieme $S \in \mathcal{L}_V$ di A è massimale in questa classe se e solo se $\langle g \rangle \cap \langle S \rangle \neq \{0\}$ per ogni $g \in V \setminus \{0\}$.*

Dimostrazione. Se S è massimale allora se $g \in S$ avremo che $\langle g \rangle \leq \langle S \rangle$, altrimenti per ogni $g \in V \setminus S$ l'insieme $S \cup \{g\}$ non è indipendente, ovvero esistono $y_1, y_2, \dots, y_r \in S$ distinti ed $n, n_1, n_2, \dots n_r \in \mathbb{Z}$ tali che $ng + n_1y_1 + n_2y_2 + \cdots + n_ry_r = 0$ e non tutti i termini sono nulli. Se $ng = 0$ allora S non sarebbe indipendente quindi $ng \neq 0$ e $ng \in \langle S \rangle \cap \langle g \rangle \neq \{0\}$.

Viceversa supponiamo che $\langle g \rangle \cap \langle S \rangle \neq \{0\}$ per ogni $g \in V \setminus \{0\}$ e prendiamo $T \subseteq A$ tale che $S \subseteq T \subseteq V$. Se prendiamo un qualunque $t \in T \setminus S$ allora per ipotesi esisteranno $y_1, y_2, \dots, y_r \in S$ distinti ed $n, n_1, n_2, \dots, n_r \in \mathbb{Z}$ tali che

$$nt = n_1y_1 + \cdots + n_ry_r \Leftrightarrow nt - n_1y_1 - \cdots - n_ry_r = 0$$

e soprattutto $nt \neq 0$. Poiché t è diverso da tutti gli y_i allora l'insieme T non è indipendente e dunque S è massimale. ■

Si osserva che non siamo dicendo che $\langle V \rangle = \langle S \rangle$ e quindi

L'importanza di queste proposizioni risiede principalmente in questo suo corollario.

Corollario 7.1.5. *Sia A un gruppo abeliano, allora*

- *Se A possiede elementi non periodici allora esiste un sottoinsieme massimale indipendente composto interamente da elementi aperiodici;*

- *Sia p primo tale che $A[p] \neq \{0\}$ allora esiste un sottoinsieme massimale indipendente contenuto in A_p (il sottogruppo contenente tutti gli elementi di ordine potenza di p).*

Infatti lavoreremo principalmente con sistemi indipendenti con elementi aperiodici o periodici di periodo potenza di primo. Prima però enunciamo i seguenti risultati

Teorema 7.1.6. *Sia A gruppo abeliano senza torsione allora l'applicazione $\mu : a \in A \to 1 \otimes a \in \mathbb{Q} \otimes A$ è un monomorfismo tra gruppi e $\mathbb{Q} \otimes A$ è un $\mathbb{Q}$-spazio vettoriale con il prodotto esterno*

$$q * \sum_i q_i \otimes a_i = \sum_i (qq_i) \otimes a_i \in \mathbb{Q} \otimes A$$

Dimostrazione. Omessa. ■

Precedentemente abbiamo osservato che se A è un p-gruppo abeliano elementare, allora A è un $\mathbb{Z}_p$-spazio vettoriale con prodotto esterno $[z]_p * a = za \in A$.

Teorema 7.1.7. *Sia A gruppo abeliano generico allora*

1. *Se A non è periodico e T è il suo sottogruppo di torsione allora, posto $V = A \setminus T$ l'insieme degli elementi aperiodici e S massimale in $\mathcal{L}_V$, il cardinale $|S|$ coincide con la dimensione dello spazio vettoriale $\mathbb{Q} \otimes A/T$.*

2. *Se $A_p \neq \{0\}$ con p primo allora posto $V = A_p$ ed S massimale avremo che il cardinale $|S|$ coincide con la dimensione dello $\mathbb{Z}_p$-spazio vettoriale $A[p]$.*

Dimostrazione. Dimostriamo i vari punti.

1. Poniamo $S' = \{s + T \mid s \in S\} \neq \emptyset$ dimostriamo che è equipotente ad S. Per ogni $x, y \in S$ tali che $x + T = y + T$ esiste $n \in \mathbb{N}$ tale che $n(x - y) = 0 = nx + (-n)y$ e dunque per l'indipendenza di S abbiamo o $x = y$ oppure $nx = ny = 0$. Ma gli elementi di S sono tutti aperiodici quindi la seconda opzione si riconduce alla prima con $x = y = 0$ e perciò $|S| = |S'|$.

   Prendiamo ora $x_1, x_2, \ldots, x_r \in S$ distinti ed $n_1, \ldots, n_r \in \mathbb{Z}$ tali che $\sum_{i=1}^r n_i x_i \in T$ allora esiste $m \in \mathbb{N}$ tale che $\sum_{i=1}^r mn_i x_i = 0 \Rightarrow mn_i x_i = 0$ per ogni i e perciò $n_i = 0$ in quanto $m \neq 0$. Dunque anche S' è indipendente, dobbiamo dimostrare che è indipendente massimale tra tutti i sistemi indipendenti di A/T.

   Preso $g + T \in A/T \setminus \{0\}$ allora $g \notin T$ e per massimalità di S avremo $\langle g \rangle \cap \langle S \rangle \neq \{0\}$. Questo significa che esiste $n \in \mathbb{N}$, $s_1, \ldots s_r \in S$ ed $n_i \in \mathbb{Z}$ tali che $ng = \sum_{i=1}^r n_i s_i$, ora se $ng \in T$ allora $mng = 0$ per un opportuno $m \in \mathbb{N}$ in contrasto con l'ipotesi iniziale su g perciò $ng \notin T$ e quindi $\langle g + T \rangle \cap \langle S' \rangle \neq \{0\}$. Per la proposizione di prima allora S' è anche massimale. Tutto il ragionamento che abbiamo fatto finora ci permette di limitarci a considerare solamente il caso in cui A sia senza torsione, altrimenti possiamo tranquillamente passare da A ad A/T e da S a S'.

   Dunque sia A abeliano senza torsione ed S un sistema indipendente massimale in $A \setminus \{0\}$. Preso $S^* = \{1 \otimes s \mid s \in S\} \cong S$ ed è chiaramente indipendente, ci basta dimostrare che S^* genera l'intero spazio, in particolare gli elementi nella forma $q \otimes a \in \mathbb{Q} \otimes A$.

Preso $q \otimes a \neq 0$ allora $a \neq 0$ e dunque per quanto detto prima $na = \sum_{i=1}^{r} n_i s_i$ e dunque

$$n(q \otimes a) = q \otimes (na) = q \otimes \left(\sum_{i=1}^{r} n_i s_i \right) = \sum_{i=1}^{r} n_i (q \otimes s_i)$$

$$\Rightarrow q \otimes a = \frac{1}{n} * [n(a \otimes b)] = \sum_{i=1}^{r} \frac{n_i q}{n} * (1 \otimes s_i)$$

in quanto $n \neq 0$ per ipotesi.

2. Sta $S = \{x_i \in A_p \mid i \in I\}$ indipendente massimale con le x_i distinte e $|\langle x \rangle_i| = p^{m_i}$, allora poniamo $y_i = p^{m_i - 1} x_i \neq 0$ ed $S^* = \{y_i \in A[p] \mid i \in I\}$. Per quanto detto all'inizio $\langle S \rangle = \bigoplus_{i \in I} \langle x_i \rangle$ e dunque anche le $\langle y_i \rangle$ formano un prodotto diretto e allora $|S| = |S^*| = |I|$ ed S^* è indipendente.

   Per mostrare che sia massimale in $A[p]$ prendiamo un qualunque $g \in A[p] \neq \{0\}$ allora $g \in A_p$ e $\langle g \rangle \cap \langle S \rangle \neq \{0\}$ ed esisterà r coprimo con p tale che $rg \in \langle S \rangle$ e dunque $g \in \langle S \rangle$. Ma per l'unicità della scrittura nei prodotti diretti avremo che $\langle S \rangle [p] = \langle S^* \rangle$ e perciò

$$g \in \langle S \rangle [p] = \langle S^* \rangle \Rightarrow \langle g \rangle \cap \langle S^* \rangle \neq \{0\}$$

   quindi S^* non solo è massimale ma $A[p]$ è contenuto interamente in $\langle S^* \rangle$ e quindi genera $A[p]$.

■

Questo teorema ci permette di affermare che la cardinalità dei sistemi indipendenti massimali aperiodici è la stessa sia per A che per A/T con T il suo sottogruppo di torsione, mentre quella dei sistemi p-indipendenti massimali è la stessa in A, in A_p e in $A[p]$.

Definizione 7.1.8. Preso un generico gruppo abeliano A.

- Si definisce il *rango senza torsione* di A il cardinale $r_0(A)$definito nella seguente maniera: se A è periodico allora $r_0(A) = 0$ altrimenti è la cardinalità di un qualunque sistema indipendente massimale S in $A \setminus T$ insieme degli elementi aperiodici.

- Per ogni primo p si definisce il *p-rango* di A il cardinale $r_p(A)$definito nella seguente maniera: se $A_p = \{0\}$ allora $r_p(A) = 0$ altrimenti è la cardinalità di un qualunque sistema indipendente massimale S in A_p insieme degli elementi di periodo potenza di p.

- Il *rango* di A è il cardinale

$$r(A) = r_0(A) + \sup_{p \text{ primo}} r_p(A)$$

Osserviamo innanzitutto che se A è ciclico diverso da $\{0\}$ allora $r(A) = 1$. Preso il gruppo di Klein K_4 osserviamo che $r(K_4) = r_2(K_4) = 2$ essendo prodotto diretto di due gruppi ciclici di ordine 2.

Se A è abeliano e $B \leq A$ allora $r(B) \leq r(A)$ in quanto sottogruppi indipendenti massimali in B sono chiaramente indipendenti anche in A.

Proposizione 7.1.9. *Sia A abeliano e finitamente generato. Allora*

$$r(A) = 1 \Leftrightarrow A \text{ ciclico}$$

Dimostrazione. Dal teorema di struttura dei gruppi Max A è somma diretta di un numero finito di gruppi ciclici. Se $r_0(A) = 1$ allora $r_p(A) = 0$ per ogni primo p e dunque A è abeliano libero quindi possiamo scrivere

$$A = \langle a_1 \rangle + \langle a_2 \rangle + \cdots + \langle a_t \rangle$$

con a_i aperiodico. Allora $S = \{a_1, \ldots, a_t\}$ è indipendente massimale e quindi $t = 1$.

Supponiamo adesso che $r_0(A) = 0$ allora A è periodico e dunque finito, quindi esisteranno solo un numero finito di primi $p_1, \ldots, p_l$ tali che $A_{p_i} \neq \{0\}$. Poiché $r_{p_i}(A) = 1$ con lo stesso ragionamento di prima segue che A_{p_i} è ciclico con ordine potenza di p_i e possiamo scrivere

$$A = A_{p_1} \oplus A_{p_2} \oplus \cdots \oplus A_{p_l}$$

Essendo gli p_i coprimi allora A è ciclico. ∎

Esempio 16. Se A non fosse finitamente generato allora non è detto che se $r(A) = 1$ allora A è ciclico, difatti preso $A = \mathbb{Z}(p^\infty)$ allora $r_0(A) = r_q(A) = 0$ per ogni $q \neq p$. L'unico sottoinsieme indipendente di $\mathbb{Z}(p^\infty)$ è costituito da un solo elemento, se esistessero $x, y \in \mathbb{Z}(p^\infty)$ con $x \neq y$ allora per il lemma 2.1.6 o $x \in \langle y \rangle$ oppure $y \in \langle x \rangle$ contraddicendo l'indipendenza.

Quindi $r_p(A) = 1$, lo stesso risultato si può ottenere in maniera più veloce utilizzando il teorema 7.1.7 poiché $A[p] \cong \mathbb{Z}_p$.

Osservazione. Se A fosse un p-gruppo allora $A[p^n]$ ha esponente finito per ogni n e dunque da Prüfer-Baer possiamo scrivere $A[p] = \bigoplus_{i \in I} \langle x_i \rangle$.

Quindi $r_p(A) = |I|$ in quanto $A[p]$ è uno spazio vettoriale con $\{a_i \mid i \in I\}$ come base.

Proposizione 7.1.10. *Sia A abeliano senza torsione e $r(A) = \aleph$ cardinale, allora esiste S indipendente e massimale in $A \setminus \{0\}$ tale che $|S| = \aleph$, $\langle S \rangle = \bigoplus_{x \in S} \langle x \rangle$ ma soprattutto $A/\langle S \rangle$ è periodico.*

Dimostrazione. Chiaramente $r(A) = r_0(A) = \aleph$, dobbiamo dimostrare solamente che quel quoziente è periodico. Ciò è immediato da mostrare in quanto per la massimalità di S avremo per ogni $g \in A \setminus \{0\}$

$$\langle g \rangle \cap \langle S \rangle \neq \{0\} \Rightarrow \exists n \in \mathbb{N} \text{ tale che } ng \in \langle S \rangle \Rightarrow n\left(g + \langle S \rangle\right) = \langle S \rangle$$

e quindi è periodico. ■

Proposizione 7.1.11. *Sia A abeliano e $B \leq A$ allora*

$$r_0(A) = r_0(B) + r_0\left(A/B\right)$$

Dimostrazione. Se A è periodico allora anche B ed A/B lo sono, quindi supponiamo che A non sia periodico.

Se A/B fosse periodico allora consideriamo un sottoinsieme S indipendente e massimale tra gli elementi aperiodici di B allora per ogni $g \in A$ aperiodico esiste $n \in \mathbb{N}$ tale che $ng \in B$ il quale è ovviamente aperiodico anche in B. Dunque

$$\langle g \rangle \cap \langle S \rangle \geq \langle ng \rangle \cap \langle S \rangle \neq \{0\}$$

e quindi S è massimale anche tra gli elementi aperiodici di A.

Se invece B fosse periodico allora a è aperiodico in A se e solo se $a + B$ lo è in A/B e quindi $r_0(A) = r_0\left(A/B\right)$. Supponiamo dunque che nessuno dei tre gruppi sia periodico.

Sia S_1 sistema indipendente massimale aperiodico di B ed $S_2^* = \{s + B \mid s \in S_2\}$ indipendente massimale aperiodico in A/B con elementi distinti. Inoltre poiché non contengono l'elemento neutro avremo che $s_1 \cap S_2 = \emptyset$ e perciò $|S_1 \cup S_2| = |S_1| + |S_2|$.

Dimostriamo innanzitutto che $S_1 \cup S_2$ è indipendente. Presi $s_1, s_2, \ldots, s_u \in S_1 \subseteq B$, $t_1, \ldots, t_v \in S_2$ e $n_1, \ldots, n_u, m_1, \ldots, m_v \in \mathbb{Z}$ tali che $\sum_i n_i s_i + \sum_j m_j t_j = 0$ allora

$$\begin{aligned}\sum_i^u n_i s_i + \sum_j^v m_j t_j = 0 \Rightarrow \sum_j^v m_j\left(t_j + B\right) = B \Rightarrow m_j = 0\,\forall j \\ \Rightarrow \sum_i^u n_i s_i = 0 \Rightarrow n_i = 0\,\forall i\end{aligned}$$

e dunque $S_1 \cup S_2$ è indipendente.

Passiamo ora a mostrare la massimalità di $S_1 \cup S_2$. Preso un generico $g \in A$ aperiodico allora esisterà sicuramente un $n \in \mathbb{N}$ tale che $ng + B \in \langle S_2^* \rangle$ anche se $g + B$ fosse periodico, quindi esiste $b \in B$ tale che $ng + b \in \langle S_2 \rangle$ con $ng + b = \sum_i n_i s_i$.

Ma allora $\sum_i n_i s_i - ng \in B$ e dunque esiste $m \in \mathbb{N}$ tale che $\sum_i mn_i s_i - mng \in \langle S_1 \rangle$ e quindi $mng \in \langle \cap \rangle \langle S_1 \cup S_2 \rangle \neq \{0\}$ in quanto $mn \neq 0$ e g aperiodico. ■

In generale il rango non è additivo, se prendiamo ad esempio $A = X \oplus Y$ con X ed Y ciclici di ordini primi distinti allora $r(A) = \max\{r(X), r(Y)\}$. Nemmeno se lavoriamo su un primo fissato continua a valere l'uguaglianza, basta prendere $A = \mathbb{Z}$ e $B = p\mathbb{Z}$.

Se però $B = T$ sottogruppo di torsione di A allora

$$r(A) = r_0(A) + \sup_{p \text{ primo}} r_p(A) = r_0\left(\frac{A}{T}\right) + \sup_{p \text{ primo}} r_p(T) = r\left(\frac{A}{T}\right) + r(T)$$

Corollario 7.1.12. *Siano A abeliano e $B \leq A$. Se A/B è periodico allora $r_0(A) = r_0(B)$ mentre se $r_0(A) = r_0(B) \in \mathbb{N}_0$ finito allora A/B è periodico.*

Proposizione 7.1.13. *Sia A abeliano e $r(A) \geq \aleph_0$ ($\aleph_0$ è il cardinale numerabile) allora esiste $B \leq A$ ed I insieme tale che $B = \bigoplus_{i\in I} \langle a_i \rangle$, $|I| = \infty$ e vale esattamente uno tra*

$$|\langle a_i \rangle| = \infty \qquad \forall i \in I \tag{7.1.1}$$
$$|\langle a_i \rangle| = p_i \text{ primo} \qquad \forall i \in I \tag{7.1.2}$$

Dimostrazione. Se $r_0(A) = \infty$ allora esiste un sistema indipendente massimale $S = \{a_i \in A \mid i \in I\}$ aperiodico infinito, allora $B = \langle S \rangle$ soddisfa tutte le ipotesi, si procede in maniera del tutto analoga se esiste un primo p per cui $r_p(A) = \infty$.

Supponiamo allora che $r_0(A), r_p(A) < \infty$ e che per ogni $n \in \mathbb{N}$ esiste un primo p_n tale che $r_{p_n}(A) > n$ e quindi $r(A) = \aleph_0$. Allora esisterà un insieme I_n finito con $|I_n| > n$ ed $a_i \in A_{p_n}$ tali che $A_{p_n} \geq \bigoplus_{i\in I_n} \langle a_i \rangle$ con $|\langle a \rangle_i| = p_n$. Definiamo

$$B = \bigoplus_{n\in\mathbb{N}} \bigoplus_{i\in I_n} \langle a_i \rangle$$

che formano una somma diretta in quanto $n \neq m \Rightarrow p_m \neq p_m$.

Questo significa che $r(B) \geq r_{p_n}(B) = r_{p_n}(A_{p_n}) = |I_n| > n$ e quindi $r(B) \geq \aleph_0$. ■

Non vale chiaramente il viceversa, basta infatti considerare

$$\bigoplus_{p \text{ primo}} \mathbb{Z}_p$$

l'insieme degli indici è infinito ma ha rango 1.

7.2 Rango e gruppi finitamente generati

Definizione 7.2.1. Un gruppo *generico* G è n-generato, con $n \in \mathbb{N}$ se e solo se esiste $X \subseteq G$ tale che $|X| \leq n$ ed $\langle X \rangle = G$.

Lo scopo di questa sezione è dimostrare che se un gruppo abeliano A ha rango n allora è n-generato e viceversa.

Iniziamo con qualche risultato più debole

Proposizione 7.2.2. *Se A è abeliano, n-generato e senza torsione allora $r(A) \leq n$.*

Dimostrazione. Utilizzeremo l'induzione su n. Se $n = 1$ allora A è ciclico infinito e dunque il suo rango è 1, supponendo l'asserto vero per $n - 1 \geq 1$ e $A = \langle a_1, \dots, a_n \rangle$ preso $L = \langle a_1, \dots, a_{n-1} \rangle \leq A$ allora per ipotesi induttiva $r(L) = r_0(L) \leq n - 1$ mentre $A/L = \langle a_n + L \rangle$ che è ciclico, dunque dalla proposizione 7.1.11 segue la tesi. ■

Corollario 7.2.3. *Se A è senza torsione e abeliano allora se $r(A) = n$ possiamo dedurre che A non è $n - 1$-generato.*

Proposizione 7.2.4. *Se A è un p-gruppo abeliano elementare n-generato allora $r(A) \leq n$.*

Dimostrazione. Procediamo per induzione come nella proposizione precedente, allora la cardinalità di A/L è pari a 1 o a p. Nel primo caso avremo che $A = L$, nel secondo invece $a_n \notin L$ e dunque $A = \langle a_n \rangle \oplus L$ e quindi se S è un sistema indipendente massimale per L allora $S \cup \langle a_n \rangle$ lo è per A. In entrambi i casi avremo che $r_p(A) \leq r_p(L) + 1 \leq n$. ■

Proposizione 7.2.5. *Se $A = L \oplus K$ con L abeliano libero e K abeliano con esponente p primo allora*

$$r_0(A) = r_0(L) = r(L)$$
$$r_p(A) = r_p(K) = r(K)$$

Dimostrazione. Il sottogruppo K è esattamente il sottogruppo di torsione di A quindi $r_p(A) = r_p(K)$. Inoltre dal teorema 7.1.7 $r_0(A) = r_0(A/K) = r_0(L)$. ■

Teorema 7.2.6. *Sia $A = L \oplus K$ con L abeliano libero e K abeliano con esponente p primo tale che $r(A) < \infty$. Allora ogni $H \leq A$ è scomponibile alla stessa maniera di A e se A/H è ciclico allora*

$$r(A) \leq r(H) + 1$$

Dimostrazione. Innanzitutto $H/(H \cap K) = HK/K \leq A/K \cong L$ abeliano libero, allora per la proposizione 2.5.6 esiste $F \leq H$ abeliano libero tale che

$$H = F \oplus (H \cap K)$$

Vi sono due possibilità

1. Se $K \leq H$ allora applicando l'identità di Dedekind $H = H \cap (L \oplus K) = (H \cap L) \oplus K$, inoltre $L/(L \cap H) \cong LH/H$ è banale o ciclico dunque $r_0 [L/(L \cap H)] \leq 1$.

   Per l'additività abbiamo $r_0(L) \leq 1 + r_0(L \cap H)$ inoltre il sottogruppo di torsione di H è proprio K dunque

   $$r(H) = r_0(H) + r(K) = r_0(H \cap L) + r(K) \geq r_0(L) - 1 + r(K) = r(A) - 1$$

2. Se invece $H \cap K < K$ allora $K/K \cap H \cong KH/H$ è periodico di esponente p e isomorfo ad un sottogruppo del gruppo ciclico A/H, quindi $|K : H \cap K| = p$, $r_0 [K/(H \cap K)] = 0$ e $r_p(K) = r_p(H \cap K) + 1$ in quanto esiste $a \in K$ tale che $K = \langle a \rangle \oplus (H \cap L)$.

   Quindi $r(H) = r_0(F) + r_p(H \cap K)$ essendo K un p-sottogruppo, ora A/H è un ciclico contenente un sottogruppo finito dunque anche A/H deve essere finito e $r_0(L) = r_0(H \cap L)$ di conseguenza. Ciò porta a

   $$r_0(A) = r_0(L) = r_0(H \cap L) \leq r_0(H) = r_0(F) \leq r_0(A) \Rightarrow r_0(A) = r_0(F)$$

   Combinando i risultati abbiamo

   $$r(H) = r_0(F) + r_p(H \cap K) = r_0(A) + r_p(A) - 1 = r(A) - 1$$

■

Corollario 7.2.7. *Se A soddisfa le ipotesi del teorema precedente allora*

$$r(A) = r(H) \Leftrightarrow K \leq H \text{ e } \frac{L}{H \cap L} \text{ finito}$$
$$r(A) = r(H) + 1 \Leftrightarrow K \nleq H \text{ o } \frac{L}{H \cap L} \text{ infinito}$$

Corollario 7.2.8. *Se $A = L \oplus K$ con L abeliano libero e K un p-gruppo abeliano elementare tale che $r(A) < \infty$, supponiamo che A sia n-generato allora $r(A) \leq n$. Viceversa se $r(A) = n$ finito allora A è n-generato ma non $n-1$-generato*

Dimostrazione. Dobbiamo solo verificare che se $r(A) = n$ allora A è n-generato, gli altri punti discendono immediatamente dai risultati precedenti.

Poiché il rango di A è finito abbiamo $L = \langle a_1 \rangle \oplus \cdots \oplus \langle a_l \rangle$ e $K = \langle b_1 \rangle \oplus \cdots \oplus \langle b_k \rangle$ con $l + k = n$ e A è generato dagli a_i e dai b_j. ■

Teorema 7.2.9. *Sia A un generico gruppo abeliano ed $r \in \mathbb{N}$, allora $r(A) = r$ se e solo se tutti i sottogruppi finitamente generati di A sono r-generati ed esiste un sottogruppo di A finitamente generato ma non $(r-1)$-generato.*

Ovvero

$$r = \min \{ n \in \mathbb{N} \mid K \text{ } n\text{-generato } \forall K \leq A \text{ finitamente generato} \}$$

Dimostrazione. Innanzitutto prendiamo A abeliano con $r(A) = r \in \mathbb{N}$ mostriamo innanzitutto che i suoi sottogruppi finitamente generati sono r-generati. Innanzitutto poniamo $r_0(A) = m$ e $\max_p r_p(A) = n$ con $m + n = r$ allora esiste un sottogruppo abeliano libero $L \leq A$ con $r(L) = m$ e A/L periodico e quindi anche $H/(H \cap L)$ è periodico oltre ad essere anche abeliano e finitamente generato e perciò finito.

Ora poiché H è finitamente generato esiste $F \leq H$ abeliano libero ed $H_{p_i} \leq H$ p_i-gruppo abeliano elementare tali che $H = F \oplus H_{p_1} \oplus H_{p_2} \oplus \cdots \oplus H_{p_l}$. Si vede immediatamente che $r(F) \leq r_0(A) = m$ e per la proposizione precedente F è m-generato.

Fissato un $p = p_i$ allora $H_p = \langle h_1 \rangle \oplus \cdots \oplus \langle h_s \rangle$ e quindi $r_p(H) = s \leq r_p(A) \leq n$ e quindi H_{p_i} è somma diretta di al più n gruppi ciclici e quindi possiamo scrivere $H_{p_i} = \bigoplus_{j=1}^n \langle k_{i,j} \rangle$ completando i termini mancanti ponendo $k_{i,j} = 0$ opportunamente. Posto

$$T_j = \bigoplus_{i=1}^{l} \langle k_{i,j} \rangle$$

allora $H_{p_1} \oplus H_{p_2} \oplus \cdots \oplus H_{p_l} = T_1 \oplus T_2 \oplus \cdots \oplus T_n$ dimostriamo che T_j è ciclico generato da

$$t_j = k_{1,j} + k_{2,j} + \cdots + k_{l,j}$$

Difatti gli ordini degli $k_{i,j}$ sono potenze di p_i e quindi a due a due coprimi, quindi esisterà un $n_i \in \mathbb{N}$ divisibile con gli ordini di tutti i $k_{i',j}$ per $i \neq i'$ ma coprimo con l'ordine di $k_{i,j}$ e perciò

$$\langle k_{i,j} \rangle = \langle n_i k_{i,j} \rangle = \langle n_i t_j \rangle \leq \langle t_j \rangle$$

e quindi $T = \langle t_j \rangle$ e il sottogruppo di torsione di H è dunque generato da n elementi. Allora H è $m+n = r$ generato e il primo punto è dimostrato, inoltre esisterà un p primo per cui $r_p(A) = n$ e quindi esiste $K \leq A$ p-gruppo abeliano elementare con $|K| = p^n$ allora $F \oplus K$ è r-generato con rango esattamente r e quindi dal corollario 7.2.8 non è $(r-1)$-generato.

Viceversa supponiamo ora che ogni sottogruppo di A finitamente generato sia anche r-generato ed esiste un suo sottogruppo finitamente generato ma non $(r-1)$-generato. Chiaramente se $r(A) < \infty$ allora per il punto precedente deve necessariamente coincidere con r quindi supponiamo che $r(A) = \infty$.

Se $r_0(A) = \infty$ per un certo primo p allora potremmo costruire un sottogruppo L generato da un numero infinito di gruppi ciclici infiniti o di ordine p e quindi possiede un sottogruppo di rango $r+1$ il quale non può essere r-generato, altrimenti esisterà un primo p per cui $r_p(A) \geq r+1$ e dunque la dimensione di $A[p]$ è almeno $r+1$ e possiamo allora costruire un sottogruppo $(r+1)$-generato ma non r-generato. ■

Il teorema 7.2.9 scollega il concetto di rango finito dalle limitazioni imposte dai gruppi abeliani, possiamo quindi definire il rango anche per gruppi che non sono abeliani nella seguente maniera

Definizione 7.2.10. Sia G gruppo generico ed $r \in \mathbb{N}_0$ diciamo che G ha *rango di Prüfer* r se e solo se ogni suo sottogruppo finitamente generato è anche r-generato e possiede un sottogruppo che non è $(r-1)$-generato.

Il gruppo G ha invece *rango infinito* se e solo se G non ha rango r per ogni $r \in \mathbb{N}$ e quindi possiede per ogni r un sottogruppo finitamente generato ma non r-generato.

Il prezzo da pagare per definire il rango su qualunque gruppo è quello di avere una definizione valida solamente nel finito, difatti il teorema 7.2.9 non continua a valere con un rango infinito.

Proposizione 7.2.11. *Sia G gruppo e $H \leq G$. Se G ha rango finito r allora H ha rango minore o uguale a r, viceversa se H ha rango infinito allora anche G ha rango infinito.*

Dimostrazione. Sia H con rango $r \in \mathbb{N}$ allora esiste $B \leq H$ che può essere generato da r elementi di H ma non da $r-1$ elementi. Se per assurdo esistessero $x_1, x_2, \ldots, x_{r-1} \in G$ tali che $\langle x_1, \ldots, x_{r-1} \rangle = B$ allora $x_i \in B \leq H$ e quindi B sarebbe $(r-1)$-generato anche in H assurdo. Quindi il rango di G non può essere più piccolo di r. ■

7.3 Rango e cardinalità

Rimaniamo ancora un po' sui gruppi abeliani per studiare la correlazione tra rango e cardinalità di un gruppo

Proposizione 7.3.1. *Sia A gruppo abeliano generico allora $r(A) \leq |A|$ e se $r(A)$ è finito allora $r(A) < |A|$.*

Dimostrazione. Ovviamente si ha $r_0(A) \leq |A|$ e $r_p(A) \leq |A|$ in quanto i sistemi indipendenti sono pur sempre sottoinsiemi di A. Se A è infinito allora la tesi è immediata essendo la somma di un cardinale infinito e un cardinale generico uguale al più grande dei due cardinali, quindi supponiamo A finito e $p_1, \ldots, p_t$ tutti e soli i primi che dividono $|A|$.

Per ogni indice i avremo $|A_{p_i}| \geq |A[p_i]| = p_i^{r(A_{p_i})} > r(A_{p_i}) = r_{p_i}(A)$ e quindi $|A| > r(A)$. ■

Il caso in cui $r(A)$ sia infinito richiede più cautela e vari risultati di teoria degli insiemi e dei cardinali.

Proposizione 7.3.2. *Preso un qualunque cardinale infinito $\aleph$ e una qualunque famiglia di insiemi non vuoti $\{A_i\}_{i\in I}$ tali che $A_i \preceq \aleph$ allora*

$$\left|\bigcup_{i\in I} A_i\right| \preceq |I|\,\aleph$$

Dimostrazione. Supponiamo valga l'assioma della scelta e sia S insieme tale che $|S| = \aleph$ allora per ogni $i \in I$ esiste $\psi_i : A_i \to S$ iniettiva. Dal teorema di Zermelo possiamo dotare I di buon ordine e possiamo quindi definire la funzione

$$f : a \in A = \bigcup_{i\in I} A_i \to \min\{i \in I \mid a \in A_i\} \in I$$

e quindi $a \in A_{f(a)}$ possiamo definire anche

$$\varphi : a \in A \to \left[f(a), \psi_{f(a)}(a)\right] \in I \times S$$

Siano $a, b \in A$ tali che $\varphi(a) = \varphi(b)$ allora $f(a) = f(b)$ e $\psi_{f(a)}(a) = \psi_{f(b)}(b) = \psi_{f(a)}(b)$ e quindi $a = b$ perciò φ è iniettiva e $|A| \leq |I \times S| = |I|\,\aleph$. ■

Proposizione 7.3.3. *Sia $\aleph$ cardinale infinito se $|I| \leq \aleph$ e $|A_i| \leq \aleph$ allora $\left|\bigcup_{i\in I} A_i\right| \leq \aleph$.*

Se $\aleph$ è anche regolare allora se $|I| < \aleph$ e $|A_i| < \aleph$ segue che $\left|\bigcup_{i\in I} A_i\right| < \aleph$.

Dimostrazione. Omessa. ■

Proposizione 7.3.4. *Sia G gruppo tale che $G = \mathrm{Dr}_{i\in I} G_i$ con $G_i \preceq \aleph_0$ e I infinito, allora $|G| = |I|$.*

Dimostrazione. Dal teorema di Zermelo I è equipotente ad un ordinale α che induce su I una relazione di buon ordine e per comodità poniamo $I = \alpha$. Per ogni $\gamma \leq \alpha$ poniamo $K_\gamma = \bigoplus_{i\in\gamma} G_i$ allora $K_\alpha = G$, $K_{\gamma+1} = K_\gamma \times G_\gamma$ e $K_\lambda = \bigcup_{\beta<\lambda} K_\beta$.

Poiché $G_i \neq \{1\}$ allora non è difficile verificare che $|I| \leq |G|$, se per assurdo $|I| < |G|$ allora esiste il minimo

$$\mu = \min\{\gamma \leq \alpha \mid |I| < |K_\gamma|\}$$

ovviamente $\mu \neq 0$ poiché $K_0 = \{1\}$.

Se μ fosse un cardinale limite allora

$$|K_\mu| = \left|\bigcup_{\gamma<\mu} K_\gamma\right| \leq |\gamma|\,|I| = |I|$$

in quanto $|\gamma| \leq |\alpha| = |I|$ e il prodotto di un cardinale infinito con un altro cardinale è il massimo tra essi. Se $\mu = \beta + 1$ allora

$$|K_\mu| = |K_\beta|\,|G_\beta| = |K_\beta|\,|G_\beta| \leq |I|\,\aleph_0 = |I|$$

generando così un assurdo. ■

Corollario 7.3.5. *Se A è un gruppo abeliano libero o un p-gruppo di rango infinito allora $r(A) = |A|$.*

Dimostrazione. Se A fosse abeliano libero o un p-gruppo abeliano elementare allora $A = \bigoplus_{i\in I} \langle a_i\rangle$ e $r(A) = |I|$. Essendo I infinito dalla proposizione precedente $|A| = |I| = r(A)$.

Sia ora A un p-gruppo generico allora per ogni $n \in \mathbb{N}$ $A\,[p^n] = \bigoplus_{i\in I_n} \langle a_i\rangle$ con $a_i \neq 0$ e quindi $|I_n| = r(A) \leq |A\,[p^n]| = |I_n|$ in quanto $r(A) = r\,(A[p]) = r\,(A\,[p^n])$.

Allora

$$A = \bigcup_{n\in\mathbb{N}} A\,[p^n] \preceq r(A)\aleph_0 = r(A)$$

e quindi $|A| = r(A)$. ■

Proposizione 7.3.6. *Sia G gruppo tale che $G = \mathrm{Dr}_{i\in\mathbb{N}}\, G_i$. Se esiste un cardinale $\aleph$ tale che $G_i \preceq \aleph$ allora $|G| \leq \aleph$.*

Dimostrazione. Posto $K_0 = \{1\}$ e $K_n = \bigoplus_{i=0}^{n-1} G_i$ allora $G = \bigcup_{n\in\mathbb{N}} K_n$, non è difficile vedere per induzione che $K_n \preceq \aleph$ e quindi $G \preceq \aleph\aleph_0 = \aleph$. ■

Proposizione 7.3.7 (Lagrange infinito)**.** *Se G ha cardinalità $\aleph$ infinito allora per ogni $H \leq G$ si ha o $|H| = \aleph$ oppure $|G : H| = \aleph$*

Dimostrazione. L'uguaglianza $|G| = |H|\,|G : H|$ vale anche tra cardinali infiniti. ■

Proposizione 7.3.8. *Se A abeliano con rango finito allora $A \preceq \aleph_0$.*

Dimostrazione. Lo spazio vettoriale $\mathbb{Q}\oplus A/T$ ha dimensione finita e $\mathbb{Q}$ numerabile dunque $A/T \preceq \aleph_0$. Inoltre $A_p = \bigcup_{n\in\mathbb{N}} A\,[p^n]$ è somma diretta di un numero finito di gruppi ciclici finiti da Prüfer-Baer, quindi $A_p \preceq \aleph_0$ e $T \preceq \aleph_0$ per il teorema di struttura dei gruppi abeliani. Perciò $|G| = |T|\,|A : T| \leq \aleph_0$. ■

Proposizione 7.3.9. *Sia A abeliano aperiodico e $B \leq A$ tale che A/B sia periodico, allora $|A| = |B|$.*

Dimostrazione. Dal teorema di struttura dei gruppi abeliani A/B è somma diretta dei suoi sottogruppi di Sylow $(A/B)_p$, supponendo per assurdo che $|B| < |A|$ allora dalla proposizione 7.3.7 $|A : B| = |A|$ e per la proposizione 7.3.6 deve esistere un primo p tale che $\left|(A/B)_p\right| > |B|$. Ora B non può essere finito poiché è sottogruppo di un gruppo senza torsione e se fosse finito allora $B = \{0\}$ e quindi A periodico il che é assurdo. Perciò B è infinito e $(A/B)_p$ è più che numerabile.

Adesso poniamo $S/B = (A/B)[p]$ essendo $(A/B)_p$ più che numerabile allora il suo rango deve essere infinito e per il corollario 7.3.5

$$\left|\frac{S}{B}\right| = r\left(\frac{S}{B}\right) = r\left[(A/B)_p\right] = \left|(A/B)_p\right| > |B|$$

Però l'applicazione $x \in S \to px \in B$ è un monomorfismo essendo A senza torsione e quindi $|S| \leq |B|$ generando così un assurdo. Dunque $|A| = |B|$ e la dimostrazione è conclusa. ■

Teorema 7.3.10. *Sia A abeliano di rango infinito allora*

$$r(A) = |A|$$

Dimostrazione. Sia T il sottogruppo di torsione di A. Se $A/T \neq \{T\}$ allora $r_0(A) = r(A/T)$ ed dalla proposizione 7.1.10 esiste un gruppo abeliano libero $F \leq A/T$ di rango $r_0(A)$ tale che $(A/T)/F$ è periodico quindi $|F| = |A/T|$ per quanto detto prima.

Adesso se $r_0(A)$ fosse finito allora $F \preceq \aleph_0 \leq r(A)$ altrimenti dal corollario 7.3.5 $r_0(A) = r(F) = |F| = |A/T|$ e quindi $|A/T| \leq r(A)$.

Supponiamo ora $T \neq \{0\}$ allora dal teorema di struttura dei gruppi abeliani $T = \bigoplus_{p \text{ primo}} A_p$ e inoltre $r_p(A) = r(A_p)$. Fissiamo un primo p allora se $r(A_p)$ è finito allora $A_p \preceq \aleph_0 \leq r(A)$ altrimenti sempre dal corollario 7.3.5 $|A_p| = r(A_p) \leq r(A)$. Infine dalla proposizione 7.3.2 $|T| \leq r(A)\aleph_0 = r(A)$.

Quindi se $T, A/T$ non siano identici allora

$$|A| = |T|\,|A : T| \leq r(A)$$

che combinata con la proposizione all'inizio della sezione ci fa ottenere la tesi. ■

Corollario 7.3.11. *Se A è un gruppo abeliano con $|A| > \aleph_0$ allora $|A| = r(A)$.*

Proposizione 7.3.12. *Sia A abeliano con rango $r(A) = \aleph$ infinito. Allora esiste un sottogruppo di A con rango $\aleph$ che è prodotto diretto di ciclici o tutti infiniti o tutti di ordine primo.*

Inoltre A contiene due sottogruppi B_1, B_2 che sono prodotto diretto di ciclici tali che $B_1 \cap B_2 = \{0\}$ e $r(B_1) = r(B_2) = \aleph$.

Dimostrazione. Supponiamo innanzitutto che $r_0(A) = \aleph$ oppure $r_p(A) = \aleph$ per un certo primo p allora esiste un sottoinsieme S di cardinalità $\aleph$ indipendente composto o da elementi aperiodici o p-elementi, quindi $\langle S\rangle$ è il sottogruppo cercato.

	$\lvert A\rvert < \aleph_0$	$\lvert A\rvert = \aleph_0$	$\lvert A\rvert > \aleph_0$
$r(A)$ finito	$\mathbb{Z}_p$	$\mathbb{Z}\left(p^\infty\right)$	impossibile
$r(A)$ infinito	impossibile	$\left(\left\{E \subseteq \mathbb{Z} \mid E \text{ finito}\right\}, \Delta\right)$	$\mathbb{R}$

Tabella 7.1: Correlazione tra rango e cardinalità di un gruppo abeliano (ponendo $E\Delta F = E \setminus F \cup F \setminus E$)

Se invece $r_0(A) < \aleph$ e $r_p(A) < \aleph$ per ogni primo p allora $\sup_{p \text{ primo}} = \aleph$. Quindi se S_p è un sistema indipendente di A_p con cardinalità $r_p(A)$ allora l'unione

$$S = \bigcup_{p \text{ primo}} S_p$$

è disgiunta e soprattutto

$$\langle S\rangle = \bigoplus_{p \text{ primo}} \langle S_p\rangle$$

Ora $S \preceq \aleph$ essendo un cardinale infinito, mentre essendo $r_p(A) \leq |S|$ abbiamo $\aleph \leq |S|$ e quindi la tesi.

Per il secondo punto supponiamo innanzitutto che $r_0(A) = \aleph$ oppure $r_p(A) = \aleph$ per un certo primo p allora esiste un sottoinsieme S di cardinalità $\aleph$ indipendente composto o da elementi aperiodici o p-elementi. Esisteranno allora S_1, S_2 tali che $S = S_1 \cup S_2$ e $\emptyset = S_1 \cap S_2$ e $|S_1| = |S_2| = \aleph$, per l'indipendenza di S si ha $B_1 = \langle S_1\rangle \cap B_2 = \langle S_2\rangle = \{0\}$ e B_1, B_2 soddisfano tutte le condizioni dell'enunciato.

Altrimenti l'insieme $\{r_p(A) \mid p \text{ primo}\}$ è un insieme infinito numerabile di cardinali strettamente minori di $\aleph$ con estremo superiore $\aleph$, quindi possiamo tranquillamente trovare una sua partizione $\{\Gamma_1, \Gamma_2\}$ son $\sup \Gamma_1 = \sup \Gamma_2 = \aleph$. Per ogni p con $r_p(A) \in \Gamma_1$ esiste S_p indipendente massimale in A_p con cardinalità $r_p(A)$ mentre per ogni q con $r_q(A) \in \Gamma_2$ esiste T_q indipendente massimale in A_q con cardinalità $r_q(A)$.

Definiamo

$$B_1 = \bigoplus_p \langle S_p\rangle$$
$$B_2 = \bigoplus_q \langle T_q\rangle$$

allora $r(B_1) = \sup_p |S_p| = \sup \Gamma_1 = \aleph$ e analogo B_2. Inoltre B_1 e B_2 hanno intersezione identica dato che S_p e T_q sono disgiunti. ■

Per concludere la sezione riassumiamo i risultati ottenuti nella tabella 7.1 con alcuni esempi per ogni caso esaminato.

7.4 Gruppi di Dedekind

Tramite la definizione 7.2.10 possiamo dotare ogni gruppo di un rango.

Definizione 7.4.1. Un gruppo G è di *Dedekind* se e solo se tutti i suoi sottogruppi sono normali.

I gruppi abeliani sono chiaramente gruppi di Dedekind, mentre il gruppo dei quaternioni Q_8 è un gruppo di Dedekind non abeliano.

Proposizione 7.4.2. *Sia G un gruppo di rango infinito tale che ogni suo sottogruppo di rango infinito è anche normale. Se inoltre G contiene un sottogruppo abeliano di rango infinito allora G è un gruppo di Dedekind.*

Dimostrazione. Dalla proposizione 7.3.12 esiste B di rango infinito prodotto diretto di un numero infinito di gruppi ciclici o tutti infiniti o tutti di ordine primo che indicheremo con

$$B = \operatorname*{Dr}_{i\in I} \langle a_i \rangle$$

con I infinito. Allora per ogni $g \in G$ esistono $i_1, i_2, \dots, i_t \in I$ tale che $B \cap \langle g \rangle = \langle b \rangle \leq \langle a_{i_1} \rangle \times \cdots \times \langle a_{i_t} \rangle = C'$ con $b \in \langle g \rangle$ in quanto i sottogruppi di gruppi ciclici sono ciclici. Allora $J = I \setminus \{i_1, \dots, i_t\}$ infinito e poniamo $C = \mathrm{Dr}_{i\in J} \langle a_i \rangle$ allora $B = C \times C'$ e quindi

$$C \cap \langle g \rangle = C \cap (B \cap \langle g \rangle) \leq C' \cap C = \{1\} \tag{7.4.1}$$

Applicando la medesima proposizione al gruppo C esistono $B_1, B_2 \leq C$ di rango infinito con $B_1 \cap B_2 = \{1\}$ quindi $B_1, B_2 \lhd G$, allora anche $B_1 \langle g \rangle$ e $B_2 \langle g \rangle$ sono sottogruppi di G.

Dalla proposizione 7.2.11 hanno entrambi rango infinito quindi sono anch'essi normali in G, inoltre dalla (7.4.1) e da $B_1 \cap B_2 = \{1\}$ con un calcolo semplice e standard il lettore può verificare che $\langle g \rangle B_1 \cap \langle g \rangle B_2 = \langle g \rangle$ il quale è perciò normale in G e quindi per l'arbitrarietà di g ogni sottogruppo di G è normale. ■

Proposizione 7.4.3. *Sia G gruppo con $|G| = \aleph > \aleph_0$ tale che ogni suo sottogruppo di cardinalità $\aleph$ è normale in G. Se esiste un sottogruppo abeliano con cardinalità $\aleph$ allora G è un gruppo di Dedekind.*

Dimostrazione. Per il corollario 7.3.11 esiste un sottogruppo abeliano con rango $\aleph$. Allora si procede esattamente come nella dimostrazione della proposizione precedente, in quanto tutti i gruppi abeliani di rango infinito che compaiono nella dimostrazione precedente hanno rango esattamente $\aleph$ e quindi sempre dalla 7.3.11 la loro cardinalità è ancora $\aleph$. Difatti se B_i ha cardinalità $\aleph$ allora anche $\langle g \rangle B_i$ ha cardinalità $\aleph$ poiché la cardinalità di ogni gruppo ciclico è sempre minore o uguale a $\aleph_0$. ■

La seguente proposizione mostra che la classe dei gruppi di rango finito è chiusa per estensioni.

Proposizione 7.4.4. *Sia G generico e $N \triangleleft G$ tale che $r(N) = r$ e $r(G/N) = s$ con $r, s \in \mathbb{N}$ allora $r(G) \leq r + s$ e quindi G ha rango finito.*

Dimostrazione. Preso $H \leq G$ finitamente generato allora $HN/N \cong H/(H \cap N)$ è s-generato, esisteranno $x_1, x_2, \ldots, x_s \in H$ tali che

$$H/(H \cap N) = \langle x_1 (H \cap N), \ldots, x_s (H \cap N) \rangle$$

Poiché H è finitamente generato esisteranno $g_1, g_2, \ldots, g_t \in H \cap N$ tali che

$$H = \langle x_1, \ldots, x_s, g_1, \ldots, g_t \rangle$$

Ancora, esistono $y_1, \ldots, y_r$ tali che $\langle g_1, \ldots, g_t \rangle = \langle y_1, \ldots, y_r \rangle$ e quindi la tesi. ∎

Corollario 7.4.5. *Se un gruppo G ha rango infinito allora per ogni $N \triangleleft G$ almeno uno tra N e G/N deve avere rango infinito.*

Lemma 7.4.6. *Se in un gruppo G i sottogruppi abeliani hanno rango finito allora per ogni $A \triangleleft G$ abeliano anche i sottogruppi abeliani di G/A hanno fango finito.*

Dimostrazione. Omessa. ∎

Teorema 7.4.7. *Se G è un gruppo risolubile di rango infinito allora contiene un sottogruppo abeliano di rango infinito.*

Dimostrazione. Utilizzeremo l'induzione sulla lunghezza derivata d di G. Se $d \leq 1$ allora G è abeliano e quindi l'asserto è immediato altrimenti supponiamo l'asserto vero per ogni gruppo risolubile di lunghezza $d - 1 \geq 1$. Se per assurdo tutti i sottogruppi abeliani di G hanno rango finito allora, posto $A = G^{(d-1)} \triangleleft G$ abeliano, il quoziente G/A ha rango infinito per il corollario precedente.

Per ipotesi induttiva G/A, avendo lunghezza derivata $d - 1$, possiede un sottogruppo di rango infinito ma ciò va in contrasto con il lemma precedente. Quindi il gruppo di partenza G deve necessariamente possedere un sottogruppo abeliano di rango infinito. ∎

Vale un risultato simile se sostituiamo il rango con la cardinalità. Abbiamo bisogno però del seguente risultato

Teorema 7.4.8 (Hall-Kulatilaka-Kargapolov)**.** *Se G è un gruppo infinito e anche localmente finito, allora esiste un sottogruppo abeliano infinito.*

Dimostrazione. Omessa. ∎

L'ipotesi della locale finitezza è necessaria, altrimenti si potrebbero prendere i gruppi di Tarski come controesempio i quali sono periodici infiniti e hanno come unici sottogruppi solo quelli di ordine primo.

Teorema 7.4.9. *Sia G risolubile e $|G| = \aleph_0$ allora esiste $A \leq G$ abeliano con $|A| = \aleph_0$.*

Dimostrazione. Se G possiede un elemento aperiodico g allora $A = \langle g \rangle$. Se invece G è periodico allora per la proposizione 4.5.2 $G \in L\mathfrak{F}$ e per il teorema di Hall-Kulatilaka-Kargapolov esiste $A \leq G$ infinito e quindi $|A| = \aleph_0$. ■

Se la cardinalità di G non è $\aleph_0$ allora non è detto che esista un tale sottogruppo, vale infatti il seguente risultato

Teorema 7.4.10 (Ehrenfeucht-Faber, 1971)**.** *Sia $\aleph > \aleph_0$ cardinale allora esiste G nilpotente di classe 2 con cardinalità $\aleph$ che non possiede alcun sottogruppo abeliano con cardinalità $\aleph$.*

Il gruppo G costruito per dimostrare il teorema possiede anche le seguenti proprietà per un certo primo p

- $|G'| = p$;
- $G' = Z(G)$;
- G/G' è un p-gruppo abeliano elementare.

quindi funge da controesempio anche per un ipotetico risultato inverso del teorema di Schur.

Tra l'altro in questo gruppo tutti i suoi sottogruppi equipotenti a G sono normali, difatti per ogni $H \leq G$ con $|H| = \aleph = |G|$ sappiamo già che H non può essere abeliano e dunque $H \cap G' \geq H'$ è non identico. Ora G' ha ordine primo perciò $H \cap G' = G'$ ovvero $G' \leq H$ e dal corollario 3.3.17 $H \lhd G$. Quindi il gruppo G soddisfa tutte le ipotesi della proposizione 7.4.3 tranne l'esistenza del sottogruppo abeliano equipotente a G, difatti G non è di Dedekind.

Concludiamo la sezione con un controesempio alla proposizione 7.4.3 nel caso in cui G sia numerabile.

Esempio 17. Prendiamo $G = \langle x \rangle \ltimes \mathbb{Z}(2^\infty)$ il 2-gruppo localmente diedrale, verifichiamo che i sottogruppi sottogruppi infiniti di G sono solo G ed $A \cong \mathbb{Z}(2^\infty)$. Sia infatti $H \leq G$ infinito allora $H/(H \cap A) \cong HA/A \leq G/A$ è finito quindi $H \cap A$ deve essere anch'esso infinito.

Ma allora $A \leq H$ poiché i gruppi di Prüfer non possiedono sottogruppi propri infiniti e quindi o $H = A$ oppure $H = G$. Quindi tutti i sottogruppi infiniti di G sono normali, ciononostante il gruppo G non è un gruppo di Dedekind poiché $\langle x \rangle$ non è normale in G.

7.5 Il gruppo dei quaternioni

Consideriamo un insieme di otto elementi indicati nella seguente maniera

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

definiamo su G un prodotto interno $\cdot$ che soddisfi i seguenti assiomi

$$\begin{tikzcd} & Q_8 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle i\rangle \arrow[dr, dash] & \langle j\rangle \arrow[d, dash] & \langle k\rangle \arrow[dl, dash] \\ & \langle -1\rangle \arrow[d, dash] & \\ & \{1\} & \end{tikzcd}$$

Figura 7.1: Sottogruppi di Q_8

- $1u = u1 = u$ per ogni $u \in Q_8$;
- $(-1)u = u(-1) = -u$ per ogni $u \in Q_8$;
- $i^2 = j^2 = k^2 = -1$, $(-1)^2 = 1$;
- $ij = k$, $jk = i$, $ki = j$;
- $ji = -k$, $kj = -i$, $ik = -j$.

È possibile dimostrare che G è un gruppo con questa operazione, e lo chiameremo *gruppo dei quaternioni*. Chiaramente il gruppo dei quaternioni non è abeliano. Inoltre per ogni $u, v \in Q_8$ abbiamo $[u; v] \in \{1, -1\}$ come è possibile vedere in questo esempio

$$[i; j] = (-i)(-j)ij = kk = -1$$

Proposizione 7.5.1. *Gli unici sottogruppi di Q_8 sono $\{1\}, Q_8, \langle -1\rangle, \langle i\rangle, \langle j\rangle, \langle k\rangle$ e sono tutti normali in Q_8.*

Dimostrazione. Osserviamo che $\langle -1\rangle = \{1, -1\}$ e $\langle i\rangle = \{1, i, -1, -i\}$ ciclico di ordine 4 e gli altri sono analoghi. Gli altri sottogruppi di Q_8 dovrebbero contenere necessariamente almeno due tra i, j, k oltre a -1, ma allora li contiene tutti e tre e otteniamo Q_8 daccapo.

Poiché $|Q_8 : \langle i\rangle| = 2$ allora $\langle i\rangle \lhd Q_8$ mentre per l'osservazione di prima $\langle -1\rangle = (Q_8)' = Z(Q_8)$ e quindi tutti i sottogruppi sono normali. ∎

In particolare Q_8 è metabeliano ma non abeliano. La struttura dei sottogruppi di Q_8 è mostrata nella figura 7.1.

Teorema 7.5.2. *Sia G un gruppo con $|G| = 8$, allora vale una ed una sola delle seguenti affermazioni*

- *G abeliano;*
- *$G \cong D_8$;*

- $G \cong Q_8$.

Infine osserviamo che $Q_8 = \langle i, j\rangle = \langle j, k\rangle = \langle k, i\rangle$.

Vogliamo dare una caratterizzazione dei gruppi di Dedekind non abeliani, per farlo utilizzeremo il seguente lemma che però non dimostriamo

Lemma 7.5.3. *Sia G un gruppo di Dedekind allora $G \in L\mathfrak{N}$ e quindi possiede il sottogruppo di torsione T (per la proposizione 6.1.1). Se inoltre T non è abeliano allora, presi $x, y \in T$ tali che $xy \neq yx$ e $|\langle x\rangle| + |\langle y\rangle|$ sia la più piccola possibile allora*

$$\langle x, y\rangle \cong Q_8$$

Proposizione 7.5.4. *Sia G gruppo e $X < G$ allora $G = \langle G \setminus X\rangle$.*

Dimostrazione. Dobbiamo dimostrare solamente che $X \leq \langle G \setminus X\rangle$. Fissiamo $g \in G \setminus X$ allora per ogni $x \in X$ avremo che $xg \in G \setminus X$ altrimenti $g = x^{-1}(xg)$ apparterrebbe a X. Dunque $x = (xg)g^{-1} \in \langle G \setminus X\rangle$ dimostrando così l'asserto. ■

Proposizione 7.5.5. *Sia $N \lhd G$ con $N = \{1, a\}$ allora $a^g = a$ per ogni $g \in G$ in particolare $N \leq Z(G)$.*

Dimostrazione. Banale. ■

Teorema 7.5.6 (Dedekind-Baer)**.** *Sia G gruppo non abeliano, allora G è un gruppo di Dedekind se e solo se*

$$G \cong Q_8 \times A \times B$$

con A e B abeliani tali che $A^2 = \{1\}$ e B composto esclusivamente da elementi di ordine dispari.

Dimostrazione. Sia innanzitutto G gruppo di Dedekind non abeliano allora $G \in L\mathfrak{N}$ e possiede un sottogruppo di torsione T. Ora poiché G non è abeliano esistono $a, b \in G$ tali che $1 \neq [a; b] \in \langle a\rangle \langle b\rangle$ dato che $\langle a\rangle, \langle b\rangle \lhd G$. Questo significa che il gruppo ciclico $\langle a\rangle/(\langle a\rangle \cap \langle b\rangle)$ è finito e quindi esiste $m \in \mathbb{N}$ tale che $a^m \in \langle b\rangle$.

Dalla proposizione 3.3.5 essendo $a \in \langle a\rangle \lhd G$ avremo che $[a; b]^m = [a^m; b] = 1$ quindi $[a; b]$ è un elemento periodico di $\langle a\rangle$. Ciò significa che il gruppo ciclico $\langle a\rangle$ è finito, con un procedimento del tutto analogo anche $\langle b\rangle$ è finito quindi $a, b \in T$. Abbiamo appena dimostrato che gli elementi che non commutano tra loro sono tutti periodici e quindi il sottogruppo di torsione non è abeliano.

Dunque gli elementi aperiodici di G apparterrebbero tutti al suo centro perciò $G \setminus Z(G) \subseteq T$. Dalla proposizione 7.5.4 $G = \langle G \setminus Z(G)\rangle = T$ e quindi G è un gruppo periodico.

Poiché T non è abeliano possiamo affermare per il lemma 7.5.3 che esistono $x, y \in T$ tali che $\langle x, y\rangle = Q \leq T$ con $Q \cong Q_8$, in particolare avremo che $x^4 = y^4 = 1$, $x^2 = y^2 \neq 1$ e $xy = y^{-1}x = y^3x$, in particolare avremo

$$[x; y] = x^3y^3xy = x^3xyy = y^2 = x^2 = [y; x] \tag{7.5.1}$$

Definito $C = C_G(Q)$ allora $C \cap Q = Z(Q) = \{1, x^2\}$ dimostriamo che $G = QC$. In generale per ogni $u \in G$ tale che $[x;u] = x^{-1}x^u \neq 1$ avremo che $x^u \neq x$, essendo $x^u \in \langle x \rangle$ e $|\langle x \rangle| = |\langle x^u \rangle| = 4$ allora $x^u = x^{-1} = x^3$ necessariamente e quindi $[x;u] = x^2$.

Con un procedimento analogo si vede che se $[y;u] \neq 1$ allora $[y;u] = y^2 = x^2$, inoltre osserviamo che per ogni $g \in G \setminus C$ g non commuta con x oppure con y quindi vale almeno una di queste disuguaglianze. Nel caso in cui $[x;g] \neq 1$ dalla proposizione 7.5.5 e dalla (7.5.1)

$$[x;yg] = [x;g][x;y]^g = [x;g][x;y] = [x;g]x^2 = x^4 = 1$$

quindi yg commuta con x.

Ora se $yg = gy$ avremmo $yg \in C$ e quindi $g = y^{-1}(yg) \in QC$ altrimenti $[y;g] = y^2$ e studiamo le quantità $[x;xyg]$, $[y;xyg]$. Innanzitutto $[x;xyg] = [x;yg] = 1$ per quanto detto sopra mentre

$$[y;xyg] = [y;yg][y;x]^{yg} = [y;g]y^2 = y^4 = 1$$

quindi $xyg \in C$ e $g = y^{-1}x^{-1}(xyg) \in QC$ e dunque $G = QC$.

Ora C è localmente nilpotente e quindi per la proposizione 6.1.1 esiste $B \leq C$ i cui elementi hanno ordine dispari e $C_2 \leq C$ i cui elementi hanno ordine potenza di 2 tali che $C = C_2 \times B$. Se B non fosse abeliano allora essendo comunque un gruppo di Dedekind dal lemma precedente possiederebbe un sottogruppo isomorfo a Q_8 il che è assurdo poiché gli elementi di B hanno ordine dispari.

Sia adesso $u \in C_2$ tale che $u^4 = 1$ quindi $(yu)^4 = y^4u^4 = 1$. Inoltre $[x;yu] = [x;y] = y^2 \neq 1$ quindi x non commuta con yu e quindi $(yu)^x = u^{-1}y^{-1} = (yu)^3$ e quindi

$$y^2 = [x;y] = [x;yu] = (yu)^3(yu)^3 = (yu)^6 = (yu)^2 = y^2u^2 \Rightarrow u^2 = 1$$

Se ora $u \in C_2$ avesse ordine 2^n con $n \geq 2$ allora $u^{2^{n-2}}$ ha ordine esattamente 4 il che è assurdo, perciò C_2 è un 2-gruppo abeliano elementare in quanto per ogni $x, y \in C_2$

$$xy = xy(yx)^2 = yx$$

Non possiamo prendere $C_2 = A$ poiché non è detto che il prodotto QC sia diretto.

Posto $K = Q \cap C_2$ dal lemma di Zorn esiste L sottoinsieme massimale di

$$\{L \leq C_2 \mid K \cap L = \{1\}\}$$

se per assurdo $KL = K \times L < C_2$ esiste $v \in C_2 \setminus KL$ e quindi $\langle L, v \rangle = L\langle v \rangle \cap K \neq \{1\}$ ed esiste allora $k \in K$ non identico e $g \in L$ tale che $k = gv$ ma allora $v \in KL$ assurdo dunque $K \times L = C_2$ e $Q \cap L = Q \cap C_2 \cap L = K\mathcal{L} = \{\infty\}$.

Quindi L è abeliano di esponente 2 e sarà la nostra A e dunque

$$Q \times L \times B = QC = G$$

Dimostriamo l'implicazione opposta, sia $G = Q \times A \times B$ dimostriamo che G è un gruppo di Dedekind. Innanzitutto $A \times B \leq Z(G) = Z(Q) \times A \times B = \langle -1 \rangle \times A \times B$ essendo abeliani mentre per il lemma 3.3.15

$$G' = Q' \times (A \times B)' \cong \langle -1 \rangle = \gamma_2(G)$$

e quindi $G \in \mathcal{N}$ con $\mathrm{cl}(G) = 2$.

Se per ogni $g \in G$ dimostriamo che $\langle g \rangle \lhd G$ allora seguirebbe immediatamente che G è di Dedekind. Per ogni g esistono e sono unici $h \in Q \times A$ e $k \in B$ tali che $g = hk$, poiché gli ordini di h e k sono coprimi avremo $h, k \in \langle g \rangle$ ed essendo $B \leq Z(G)$ avremo che $\langle k \rangle \lhd G$ e $\langle g \rangle = \langle h \rangle \ltimes \langle k \rangle$.

Ancora esistono $y \in Q$ e $a \in A$ tali che $h = ya$, a questo punto possiamo trovarci in una delle seguenti situazioni

- Se $h^2 = 1$ allora $1 = y^2 a^2 = y^2$ e quindi $y \in \langle -1 \rangle \Rightarrow h \in Z(G)$ e quindi $\langle h \rangle \lhd G$.
- Se $h^2 \neq 1$ allora $y^2 \neq 1$ e necessariamente avremo che $y^2 = -1$ e quindi $G' = \langle -1 \rangle \leq \langle h \rangle$ dunque $\langle h \rangle \lhd G$.

In entrambi i casi $\langle h \rangle \lhd G$ e quindi $\langle g \rangle = \langle h \rangle \langle k \rangle \lhd G$. ■

Corollario 7.5.7. *Se G è un gruppo di Dedekind allora valgono le seguenti proprietà:*

- *Se G non è periodico allora è abeliano;*
- $|G/Z(G)| \in \{1, 4\}$ *abeliano;*
- $|G'| \leq 2$*;*
- *G è nilpotente di classe minore o uguale a 2.*

Indice analitico