Università degli studi di Padova

Dipartimento di matematica "Tullio Levi-Civita"

Corso di Laurea Magistrale in Matematica

Studio del Virtually Generating Graph di alcuni gruppi profiniti

Relatore:
Prof. Andrea Lucchini

Laureando:
Fabrizio Mori
Matricola:
1239134

16 Dicembre 2022

Anno Accademico 2021-22

Indice

Introduzione

Negli ultimi anni parte della ricerca è stata rivolta allo studio di grafi associati a gruppi. Nella maggior parte dei casi tali grafi hanno come insieme di vertici gli elementi del gruppo a cui sono associati e in essi due vertici sono adiacenti se rispettano una determinata proprietà; si intuisce inoltre che ciò che si richiede è che grafi di questo tipo siano associabili ad un intera classe di isomorfismo di un gruppo, non solo ad un gruppo specifico.

Nel contesto della teoria dei gruppi finiti il più celebre esempio è costituito dal Generating graph: in esso due elementi sono adiacenti se generano l'intero gruppo; l'importanza di questo oggetto, il cui studio è non banale solo nel caso di gruppi 2-generati, è che tutti i gruppi semplici finiti sono generati al più da 2 elementi. Il concetto di generating graph è poi stato esteso al caso dei gruppi profiniti, considerando adiacenti quegli elementi che generano un sottogruppo astratto denso.

In questo lavoro di tesi verranno studiate alcune proprietà del Virtually Generating Graph di un gruppo profinito G. In questo grafo, indicato come $\Gamma(G)$, due vertici sono adiacenti se e solo se generano topologicamente un sottogruppo aperto. Saremo principalmente interessati a studiare le proprieta del grafo $\tilde{\Gamma}(G)$, ottenuto a partire da $\Gamma(G)$ rimuovendo i suoi vertici isolati, in particolare:

- si cercheranno condizioni necessarie sul gruppo G affinché $\tilde{\Gamma}(G)$ sia connesso.
- In caso di connessione si determinerà un bound sul diametro del grafo.

L'obiettivo di questo lavoro di tesi è introdurre il problema della connessione per la classe dei gruppi pronilpotenti.

Nel primo capitolo viene mostrato che il grafo può essere non connesso nel caso in cui G sia un gruppo prorisolubile. Successivamente ci si interroga sulla possibile proprietà di connessione nel caso pronilpotente. Sotto certe condizioni, grazie alla fattorizzazione in p-gruppi di Sylow, sarà possibile spostare il problema della connessione al caso dei pro-p-gruppi.

Nel secondo capitolo viene studiata la connessione di $\tilde{\Gamma}(G)$ nel caso in cui G sia un pro-p-gruppo abeliano finitamente generato. Le ipotesi che garantiscono la connessione ci consentiranno pure di stabilire che il diametro è sempre minore o uguale a 2.

Nel terzo capitolo viene studiata la connessione di $\tilde{\Gamma}(G)$, dove G è il pro-p-gruppo libero 2-generato. In questo caso si mostrerà che $\tilde{\Gamma}(G)$ coincide con il generating graph; come conseguenza di questo fatto si otterrà un grafo connesso con diametro 2.

Il quarto e ultimo capitolo è dedicato allo studio del gruppo di Nottingham $\mathcal{N}(p)$ al variare di un primo p. Tale gruppo ha come insieme degli elementi le serie formali f in $\mathbb{F}_p[[t]]$ nella forma:

$$f = t(1 + \sum_{k=1}^{\infty} a_k t^k), \quad a_k \in \mathbb{F}_p;$$

la struttura di gruppo è invece data dalla sostituzione formale. La motivazione per la quale viene annoverato questo caso nell'analisi del virtually generating graph dei pro-p-gruppi discende da una proprietà peculiare di $N(p)$: ogni pro-p-gruppo a base numerabile (e quindi anche finitamente generato) può essere immerso come sottogruppo chiuso in $\mathcal{N}_p$. Viene mostrato come $\mathcal{N}_p$ sia un pro-p-gruppo finitamente generato e viene introdotto il concetto di $profondità$ di un elemento $f \in \mathcal{N}_p$; in funzione della profondità vengono poi derivati dei criteri per i quali due elementi possano generare un sottogruppo aperto di $\mathcal{N}_p$.

Alla fine del capitolo si riesce a mostrare che nel caso $p \geq 5$ il grafo $\Gamma(\mathcal{N}_p)$, privato dell'identità, è connesso con diametro minore o uguale a 4.

Capitolo 1

Virtually generating graph di un gruppo profinito

1.1 Grafi associati a gruppi profiniti

Lungo tutta la trattazione verranno studiate le proprietà di un particolare grafo associato ad un qualsiasi gruppo profinito G, il virtually generating graph, che denoteremo con $\Gamma(G)$. Sarà anche utile in certe circostanze la nozione di generating graph di un gruppo profinito (indicato come $\Delta(G)$); verrà adottata la convenzione secondo cui, dato $\Theta(G)$ un grafo arbitrario associato ad un gruppo G, $\tilde{\Theta}(G)$ indicherà il nuovo grafo creato a partire da $\Theta(G)$ privato dei vertici isolati; saremo prevalentemente interessati a quest'ultima costruzione.

La seconda convenzione che verrà adottata riguarda la nozione di generazione topologica: dato un gruppo profinito G e due elementi $x, y \in G$ scriveremo $\langle x, y\rangle$ al posto di $\overline{\langle x, y\rangle}$, per indicare la chiusura del sottogruppo astratto generato da x e y.

Definizione 1.1.1. Sia G un gruppo profinito 2-generato, il generating graph $\Delta(G)$ associato a G è il grafo che ha come vertici gli elementi di G e in cui due vertici sono connessi se e solo se generano topologicamente G.

Definizione 1.1.2. Sia G un gruppo profinito , il virtually generating graph $\Gamma(G)$ associato a G è il grafo che ha come vertici gli elementi di G e in cui due vertici sono connessi se e solo se generano un sottogruppo aperto di G.

Si possono fare immediatamente alcune osservazioni:

- Nella definizione di $\Delta(G)$ non è restrittivo supporre che G sia 2-generato, in caso contrario $\tilde{\Delta}(G)$ risulterebbe privo di vertici.
- Il grafo $\Gamma(\tilde{G})$ è non privo di vertici solo nel caso in cui G è un gruppo profinito finitamente generato; supponiamo infatti che esistano due elementi $x, y \in G$ tali per cui $\langle x, y\rangle := H$ è aperto, allora si deve avere necessariamente che esiste un sottogruppo normale aperto di base N contenuto in H. Il gruppo G/N, essendo un

gruppo finito, è generato dagli elementi $\{x_1N, \ldots, x_dN\}$ e come conseguenza di ciò si ha che $\langle x_1, \ldots, x_d, x, y\rangle = G$.

- Due elementi $x, y \in G$ sono adiacenti nel grafo $\Gamma(\tilde{G})$ se e solo se $|G : \langle x, y\rangle|$ è finito; questo deriva dal fatto che un sottogruppo chiuso in un gruppo profinito è aperto se e solo se ha indice finito.

1.2 Connessione di $\tilde{\Gamma}(G)$, con G gruppo prorisolubile

In questa sezione verrà mostrato un esempio in cui la connessione di $\tilde{\Gamma}(G)$ fallisce per un particolare gruppo prorisolubile G.

Fissato un numero naturale t, si consideri $\mathbb{F}_2^{2t}$ assieme con l'insieme

$\Omega := \{(x_1, x_2, \ldots, x_{2t-1}, x_{2t}) \in \mathbb{F}_2^{2t} \mid (x_{2i-1}, x_{2i}) \neq (0, 0)\ \forall i = 1, \ldots, t\}$.

Ad ogni $\omega \in \Omega$ verrà associato un diverso primo dispari p_ω e a partire da esso verrà costruito il gruppo $N_\omega := (\mathbb{Z}_{p_\omega})^3$, dove $\mathbb{Z}_{p_\omega}$ è il gruppo degli interi p_ω-adici; si fissi $H := \langle y_1, y_2, \ldots, y_{2t-1}, y_{2t}\rangle$ 2-gruppo abeliano elementare di rango $2t$. Su ciascun N_ω possiamo definire un'azione a partire dai generatori di H nel seguente modo:

$$(z_1, z_2, z_3)^{y_i} := (z_1, z_2, (-1)^{x_i} z_3).$$

Ciò ci permette di definire di definire il gruppo $G := \left(\prod_\omega N_\omega\right) \rtimes H$.

Svolgendo alcuni calcoli non è difficile mostrare che, se per ogni $\omega \in \Omega$ definiamo $\nu_\omega := (1, 0, 1)$, $\mu_\omega := (0, 1, -1) \in N_\omega$ si ha che $N_\omega \leq \bigcap_{1\leq i\leq t} \langle \nu_\omega y_{2i-1}, \mu_\omega y_{2i}\rangle$. Un'immediata conseguenza di questo fatto è che se definiamo per ogni i

$$\sigma_{2i-1} := \big((\nu_\omega)_\omega\big) y_{2i-1},\ \sigma_{2i} := \big((\mu_\omega)_\omega\big) y_{2i},$$

otteniamo che $G = \langle \sigma_1, \sigma_2, \ldots, \sigma_{2i-1}, \sigma_{2t}\rangle$ e che per ogni $i \in \{1, \ldots, t\}$ il sottogruppo $\langle \sigma_{2t-1}, \sigma_{2i}\rangle$ è aperto.

Poniamo ora $N = \prod_\omega N_\omega$ e definiamo il sottogruppo $\Sigma_i := N \rtimes \langle y_{2i-1}, y_{2i}\rangle$.

Proposizione 1.2.1. Supponiamo che $g_1,\ g_2 \in G$ siano adiacenti in $\Gamma(G)$, allora deve esistere $i \in \{1, \ldots, t\}$ tale che $\{g_1, g_2\} \subset \Sigma_i \setminus N$.

Dimostrazione. Si pongano $g_1 = (n_1, \sum_{i=1}^{2t} a_i y_i)$, $g_2 = (n_2, \sum_{i=1}^{2t} b_i y_i)$; ciò che ci accingiamo a dimostrare è che

- esiste $\bar{i} \in \{1, \ldots, t\}$ tale per cui la matrice $C_{\bar{i}} := \begin{bmatrix} a_{2\bar{i}-1} & a_{2\bar{i}} \\ b_{2\bar{i}-1} & b_{2\bar{i}} \end{bmatrix}$ risulta invertibile
- $a_j = b_j = 0$ per ogni $j \in \{1, \ldots, 2t\} \setminus \{2\bar{i} - 1, 2\bar{i}\}$.

Cominciamo dimostrando che il sistema lineare in $\mathbb{F}_2$

$$\mathcal{S} = \begin{cases} a_1x_1 + a_2x_2 + \cdots + a_{2t}x_{2t} = 0 \\ b_1x_1 + b_2x_2 + \cdots + b_{2t}x_{2t} = 0 \end{cases}$$

non ha soluzioni in Ω. Se $\mathcal{S}$ avesse una soluzione $(x_1, \ldots, x_{2t})$ appartenente ad Ω, ciò comporterebbe che gli elementi $h_1 = \sum_{i=1}^{2t} a_i y_i, h_2 = \sum_{i=1}^{2t} b_i y_i$ centralizzano il gruppo N_ω e si avrebbe di consegenza che $\langle g_1, g_2\rangle \cap N_\omega = \langle n_{1,\omega}, n_{2,\omega}\rangle$ è un sottogruppo 2-generato di N_ω.

Osserviamo ora che

$$|G : \langle g_1, g_2\rangle| \geq |N_\omega\langle g_1, g_2\rangle : \langle g_1, g_2\rangle| = |N_\omega : \langle g_1, g_2\rangle \cap N_\omega| = \infty$$

ciò è in contraddizione con il fatto che $|G : \langle g_1, g_2\rangle|$ sia finito e ci fa concludere che $\mathcal{S}$ non ha soluzione in Ω.

Supponiamo che non esista alcun indice nell'insieme $\{1, \ldots, t\}$ tale per cui la matrice C_i risulti invertibile; questo fatto implica che, per ogni $i \in \{1, \ldots, t\}$, esiste una coppia $(x_{2i-1}, x_{2i}) \in {\mathbb{F}_2}^2 \setminus \{(0,0)\}$ tale per cui $C_i \begin{bmatrix} x_{2i-1} \\ x_{2i} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$.

In questo modo si ha che l'elemento $(x_1, x_2, \ldots, x_{2t-1}, x_{2t})$, ottenuto concatenando le soluzioni, è soluzione in Ω del sistema $\mathcal{S}$, assurdo.

Quello che abbiamo mostrato finora è che esiste sicuramente $\bar{i} \in \{1, \ldots, t\}$ tale per cui la matrice $C_{\bar{i}}$ risulti invertibile. Mostriamo adesso che, fissato tale $\bar{i}$, $a_j = b_j = 0$ per ogni $j \in \{1, \ldots, 2t\} \setminus \{2\bar{i} - 1, 2\bar{i}\}$.

Si costruisca la matrice $D_{\bar{i}} := \begin{bmatrix} a_1 & \ldots & a_{2\bar{i}-2} & a_{2\bar{i}+1} & \ldots & a_{2t} \\ b_1 & \ldots & a_{2\bar{i}-2} & a_{2\bar{i}+1} & \ldots & b_{2t} \end{bmatrix}$.

Il sistema $\mathcal{S}$ può essere riscritto in forma matriciale come:

$$C_{\bar{i}} \begin{bmatrix} x_{2\bar{i}-1} \\ x_{2\bar{i}} \end{bmatrix} + D_{\bar{i}} \begin{bmatrix} x_1 \\ \vdots \\ x_{2\bar{i}-2} \\ x_{2\bar{i}+1} \\ \vdots \\ x_{2t} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Sia ora $\Omega_{\bar{i}}$ l'insieme delle sequenze $(x_1, \ldots, x_{2\bar{i}-2}, x_{2\bar{i}+1}, \ldots, x_{2t})$ costruite a partire dalle sequenze in Ω e alle quali sono state rimosse le componenti $(2\bar{i}-1)$-esima e $2\bar{i}$-esima. Siccome $\langle \Omega_{\bar{i}}\rangle \simeq {\mathbb{F}_2}^{2(t-1)}$, nell'ipotesi in cui la matrice $D_{\bar{i}}$ non sia nulla, esiste un elemento $X_{\bar{i}} \in \Omega_{\bar{i}}$ tale che $D_{\bar{i}}X_{\bar{i}} = Z \neq (0,0)$. L'invertibilità di $C_{\bar{i}}$ d'altro canto garantisce che esiste $Y_{\bar{i}} = (x_{2\bar{i}-1}, x_{2\bar{i}}) \neq (0,0)$ tale che $C_{\bar{i}}Y_{\bar{i}} = Z$. Combinando queste informazioni si ottiene che $C_{\bar{i}}Y_{\bar{i}} + D_{\bar{i}}X_{\bar{i}} = Z + Z = (0,0)$, cioè che l'elemento $(x_1, \ldots, x_{2\bar{i}-1}, x_{2\bar{i}}, \ldots, x_{2t}) \in \Omega$ è soluzione di $\mathcal{S}$, assurdo.

□

Dalla precedente proposizione si può dedurre il seguente

Corollario 1.2.2. $\tilde{\Gamma}(G)$ non è connesso

Dimostrazione. Siccome $\sigma_{2i} \in \Sigma_i \setminus N$, $\sigma_{2j} \in \Sigma_j \setminus N$ e $\Sigma_i \setminus N \cap \Sigma_j \setminus N = \emptyset$ se $i \neq j$ si conclude che non può esserci nessun cammino che colleghi σ_{2i} e σ_{2j}. □

1.3 Virtually generating graph di un gruppo pronilpotente

Si prenda ora in esame un arbitrario gruppo pronilpotente finitamente generato G; in questa sezione verranno poste condizioni sufficienti affinché $\tilde{\Gamma}(G)$ risulti connesso. In seguito sarà chiaro come il problema relativo alla connessione di $\tilde{\Gamma}(G)$ venga spostato nel contesto dei pro-p-gruppi finitamente generati.

Ricordiamo anzitutto che un gruppo pronilpotente è il prodotto cartesiano dei suoi sottogruppi di Sylow al variare di ciascun primo. Esplicitamente se G è pronilpotente finitamente generato si ha:

$$G \simeq \prod_p S_p$$

dove S_p è il p-Sylow di G e $d(S_p) \leq d(G)$ per ogni primo p.

Siamo dunque interessati a stabilire quando un generico elemento $x = (x_p)_p$ di G è non isolato nel virtually generating graph.

Proposizione 1.3.1. Un vertice $x = (x_p)_p$ di $G \simeq \prod_p S_p$ è non isolato in $\tilde{\Gamma}(G)$ se e solo se:

1. Per ogni primo p la componente x_p è non isolata nel virtually generating graph di S_p.
2. Solo per un numero finito di primi la componente x_p è isolata nel generating graph di S_p.

Dimostrazione. Sia $x = \big(x_p\big)_p$ non isolato, dunque deve necessariamente esistere $y = (y_p)_p$ tale per cui $\langle x, y\rangle$ è un sottogruppo aperto di G, in particolare tale sottogruppo avrà indice finito. Dal momento che $\langle x, y\rangle \simeq \prod_p \langle x_p, y_p\rangle$ si ha $|G : \langle x, y\rangle| \leq \prod_p |S_p : \langle x_p, y_p\rangle|$; questa produttoria è finita se e solo se x_p e y_p generano sempre S_p tranne per un numero finito di primi e, per questi ultimi , generano un sottogruppo aperto.

□

Proposizione 1.3.2. Il generating graph di un pro-p-gruppo 2-generato, privato dei suoi vertici isolati, è connesso con diametro 2

Dimostrazione. Sia G un pro-p-gruppo 2-generato; analogamente al caso finito per un p-gruppo si può dimostrare che per un pro-p-gruppo G finitamente generato il sottogruppo di Frattini $\Phi(G)$, definito come l'intersezione di tutti i sottogruppi massimali aperti di G, è uguale al gruppo $G^p[G, G]$ e che $G/\Phi(G) = \mathbb{F}_p^d$ (spazio vettoriale di dimensione d sul

campo con p elementi) dove d è il numero minimo di generatori. Nel caso in cui si abbia $d(G) = 1$ la dimostrazione è terminata, siccome un qualsiasi generatore del gruppo sarà vertice universale del generating graph.

Supponiamo dunque $d(G) = 2$ e consideriamo $G/\Phi(G) \simeq \mathbb{F}_p^2$; si osserva che il suo generating graph, privato del vettore nullo, è connesso con diametro 2, siccome ciascun elemento non nullo in uno spazio vettoriale di dimensione 2 genera l'intero spazio con un altro opportuno elemento che non sia linearmente dipendente (multiplo di esso) e se due elementi sono linearmente dipendenti c'è sicuramente un terzo elemento linearmente indipendente con ciascuno dei due; se adesso prendiamo in esame un qualsiasi elemento x non appartenente al sottgruppo di Frattini in G ad esso sarà adiacente un qualsiasi elemento y che appartenga ad una classe laterale $y\Phi(G)$ tale per cui $\langle x\Phi(G), y\Phi(G)\rangle = \mathbb{F}_p^2$. Siccome $\langle x\Phi(G), y\Phi(G)\rangle = G/\Phi(G)$ si ottiene pure che $\langle x, y\rangle = G$. Concludiamo da queste considerazioni che gli unici vertici isolati nel generating graph sono tutti e soli gli elementi che appartengono al sottogruppo di Frattini e che il diametro è uguale a 2. □

Proposizione 1.3.3. Sia G un gruppo pronilpotente finitamente generato e sia $\{S_p\}_p$ l'insieme dei suoi sottogruppi di Sylow; supponiamo che:

1. per ogni primo p si ha che $\tilde{\Gamma}(S_p)$ è connesso,
2. $\exists M \in \mathbb{N}$ tale che $\mathrm{diam}(\tilde{\Gamma}(S_p)) \leq M$ per pgni primo p,
3. S_p è 2-generato, tranne al più per un numero finito di primi,

allora $\tilde{\Gamma}(G)$ è connesso e $\mathrm{diam}(\tilde{\Gamma}(G)) \leq M$.

Dimostrazione. Siano $x = (x_p)_p$, $y = (y_p)_p$ due vertici non isolati nel virtually generating graph, chiamiamo $\mathcal{P}$ l'insieme di tutti i numeri primi, $\tilde{\Delta}(S_p)$ il generating graph del gruppo S_p privato dei suoi vertici isolati e definiamo i due insiemi:

$$\mathcal{P}_x := \{p \in \mathcal{P} \ \mid \ x_p \notin \tilde{\Delta}(S_p)\} \ , \quad \mathcal{P}_y := \{p \in \mathcal{P} \ \mid \ y_p \notin \tilde{\Delta}(S_p)\}.$$

Siccome x e y non sono isolati, le ipotesi ci garantiscono che la cardinalità di questi due insiemi è sicuramente finita. Si osserva oltretutto che, qualora p appartenga a $\mathcal{P}_x$ (rispettivamente $\mathcal{P}_y$), si ha che x_p (rispettivamente y_p) è non isolato nel virtually generating graph di S_p.

Sia ora $\mathcal{P}_z := \mathcal{P}_x \cup \mathcal{P}_y$ e definiamo un elemento $z := (z_p)_p \in G$ nel seguente modo:

1. $p \in \mathcal{P}_z$: si sceglie un cammino $\{z_{1,p}, \ldots, z_{d,p}\} \in \tilde{\Gamma}(S_p)$ con $d \leq \mathrm{diam}(\tilde{\Gamma}(S_p)) - 1$ che connetta x_p e y_p; questo può essere fatto perché il virtually generating graph di S_p privato dei vertici isolati è connesso con diametro limitato.
2. $p \in \mathcal{P} \setminus \mathcal{P}_z$: si sceglie $z_p \in S_p$ in maniera che $\langle x_p, z_p\rangle = \langle y_p, z_p\rangle = S_p$, questo può essere fatto perché il generating graph di S_p privato dei vertici isolati è connesso con diametro al più 2.

Costruiamo dunque un cammino, con riferimento alla costruzione dei precedenti punti, $\{x, z_1, \dots, z_M, y\}$ in $\tilde{\Gamma}(G)$ nel seguente modo:

- $p \in \mathcal{P}_z$: si costruisce il cammino $\{x_p, \tilde{z}_{1,p}, \dots, \tilde{z}_{M,p}, y_p\}$ ponendo
  - $\tilde{z}_{i,p} = z_{i,p}$ quando $i \in \{1, \dots, d\}$
  - $\tilde{z}_{i,p} = y_p$ quando $i \in \{d+1, \dots, M\}$
- $p \in \mathcal{P} \setminus \mathcal{P}_z$: si pone $z_{i,p} = z_p$ per ogni $i \in \{1, \dots, M\}$.

  ciò conclude la dimostrazione.

□

Questa ultima caratterizzazione che è stata mostrata sposta dunque l'analisi circa la connessione del virtually generating graph al caso dei pro-p-gruppi; nei prossimi capitoli verrà provata la connessione di $\tilde{\Gamma}(G)$, nel caso in cui G risulti essere un pro-p-gruppo abeliano e nel caso in cui sia un pro-p-gruppo libero.

Capitolo 2

Virtually generating graph di un gruppo profinito abeliano

2.1 Virtually generating graph di un pro-p-gruppo abeliano

Enunciamo senza dimostrazione il seguente

Teorema 2.1.1. Sia G un pro-p-gruppo abeliano finitamente generato, allora esiste $r \in \mathbb{N}$ tale per cui $G \simeq \mathbb{Z}_p^r \times T$, con T gruppo finito.

Per un pro-p-gruppo abeliano finitamente generato possiamo isolare subito tre casi banali per lo studio del virtually generating graph:

- $G \simeq T$: $\Gamma(G)$ è il grafo completo di cardinalità $|T|$.
- $G \simeq \mathbb{Z}_p \times T$: $\Gamma(G)$ è connesso e ciascun genratore di $\mathbb{Z}_p$ è un vertice universale del grafo.
- $G \simeq \mathbb{Z}_p^r \times T$, con $r > 2$: $\Gamma(G)$ non possiede alcun lato.

Si conclude dunque che per questa classe di gruppi l'unico caso che rimane da studiare è quello in cui l'esponente della parte libera è pari a 2, quindi senza perdita di generalità sarà sufficiente studiare il virtually generating graph del gruppo $G := \mathbb{Z}_p^2 \times T$, con T un qualsiasi p-gruppo abeliano finito.

Proposizione 2.1.2. $\tilde{\Gamma}(\mathbb{Z}_p^2 \times T)$ è connesso con diametro uguale a 2

Dimostrazione. Siccome la parte libera non è prociclica gli elementi del tipo $(0, 0, t)$ con $t \in T$ sono necessariamente isolati. Si considerino dunque due vertici del tipo (x_1, x_2, t_1) e (y_1, y_2, t_2) con i seguenti casi:

1. $x_1, y_1 \neq 0$: Si osserva che $\langle (x_1, x_2, t_1), (0, 1, 0_T) \rangle$ è aperto così come lo è $\langle (y_1, y_2, t_2), (0, 1, 0_T) \rangle$.
2. $x_2, y_2 \neq 0$: Si osserva che $\langle (x_1, x_2, t_1), (1, 0, 0_T) \rangle$ è aperto così come lo è $\langle (y_1, y_2, t_2), (1, 0, 0_T) \rangle$.

3. $x_1, y_2 \neq 0$, $x_2 = y_1 = 0$: il sottogruppo $\langle (x_1, 0, t_1), (0, y_2, t_2) \rangle$ è aperto.

4. $x_2, y_1 \neq 0$, $x_1 = y_2 = 0$: il sottogruppo $\langle (0, x_2, t_1), (y_1, 0, t_2) \rangle$ è aperto.

Abbiamo dunque mostrato che gli elementi del tipo $(0, 0, t)$ con $t \in T$ sono gli unici vertici isolati di questo grafo e che se due vertici non isolati non sono connessi c'è al più un cammino di lunghezza 2 che li congiunge (il diametro pari a 2 è proprio, banalmente un vertice ha bisogno di un cammino di lunghezza 2 per tornare verso se stesso).

□

2.2 Virtually generating graph di gruppo profinito abeliano finitamente generato

Corollario 2.2.1. Sia G un gruppo abeliano profinito finitamente generato e sia $\{S_p\}_p$ l'insieme dei suoi sottogruppi di Sylow; supponiamo che:

1. Per ogni primo p si ha $S_p \simeq \mathbb{Z}_p^{r(p)} \times T_p$, con $r(p) \leq 2$, con T_p p-gruppo finito.

2. S_p è 2-generato, tranne al più per un numero finito di primi.

allora $\tilde{\Gamma}(G)$ è connesso con diametro 2.

Dimostrazione. La dimostrazione di questo fatto discende direttamente dalla proposizione 1.3.3. siccome si è mostrato che i sottgruppi di Sylow hanno il virtually generating graph connesso con diametro 2 e sono quasi sempre 2-generati. □

Capitolo 3

Virtually generating graph di un pro-p-gruppo libero

3.1 Il pro-p-gruppo libero di rango finito

Consideriamo un insieme X con $|X| < \infty$ e consideriamo $F(X)$, gruppo libero astratto sull'insieme X. Sia $\mathcal{I} := \{N_i\}$ l'insieme dei sottogruppi normali di $F(X)$ tale per cui $F(X)/N_i$ appartenga alla classe dei p-gruppi finiti; questo insieme è parzialmente ordinato: presi N_1, $N_2 \in \mathcal{I}$ possiamo scrivere $N_1 \leq_* N_2$ se $N_2 \leq N_1$. Per ogni N_i, $N_j \in \mathcal{I}$ nel caso in cui si abbia $N_i \leq_* N_j$ si può costruire un morfismo $\phi_{ij} : F(X)/N_j \longrightarrow F(X)/N_i$, dotando l'insieme $\mathcal{I}$ della struttura di inverse system.

Si ponga adesso $F := \varprojlim_{N\in\mathcal{I}} F(X)/N$ e si consideri la funzione

$$j : F(X) \longrightarrow F$$

definita da $j(h) := (hN)_{N\in\mathcal{I}}$; si può mostrare che, preso G un pro-p-gruppo arbitrario e considerata $f : X \longrightarrow G$ una qualsiasi funzione, esiste un unico omomorfismo di pro-p-gruppi $\hat{f} : F \longrightarrow G$ tale per cui $f = \hat{f}\iota$, con $\iota = j_{|X}$.

Questa proprietà universale del gruppo F, simile alla proprietà universale dei gruppi liberi astratti, rende F unico a meno di isomorfismi nella classe dei pro-p-gruppi; chiameremo dunque F il pro-p-gruppo libero sull'insieme X.

Un'importante proprietà dei gruppi liberi astratti viene mantenuta nel caso libero profinito: i sottogruppi aperti nei gruppi liberi profiniti sono ancora liberi profiniti (teorema di Nielsen—Schreier) , più nel dettaglio vale il seguente

Teorema 3.1.1. Sia F un pro-p-gruppo libero sull'insieme X con $|X| < \infty$ e sia H un sottogruppo aperto di F, allora:

1. esiste un trasversale destro T di H in F tale per cui H è un pro-p-gruppo libero sull'insieme

$$X_H = \{t_1 x t_2^{-1} \mid x \in X,\ t_1, t_2 \in H,\ t_1 x t_2^{-1} \in H \setminus \{1_F\}\}.$$

2. Vale la formula

$$|F : H|(|X| - 1) = |X_H| - 1.$$

3.2 Virtually generating graph di un pro-p-gruppo libero

Proposizione 3.2.1. Sia $|X|$ un insieme di cardinalità finita, F il pro-p-gruppo libero su X, allora:

1. $\tilde{\Gamma}(F)$ è privo di archi se $|X| > 2$.
2. $\Gamma(F)$ è connesso e ha vertici universali se $|X| = 1$.
3. $\tilde{\Gamma}(F)$ è connesso con diametro uguale a 2 se $|X| = 2$.

Dimostrazione. Proviamo in ordine i punti della proposizione, osservando che se $H = \langle x, y \rangle$ con $x, y \in F$ è un sottogruppo aperto si ha necessariamente $|X_H| \leq 2$:

1. $|X| > 2$: osservando la formula del teorema 1 otteniamo un assurdo, siccome $|F : H|(|X| - 1) \geq 2$ mentre $|X_H| - 1 \leq 1$
2. $|X| = 1$: in questo caso $F \simeq \mathbb{Z}_p$, ogni generatore è dunque vertice universale del grafo.
3. $|X| = 2$: Osservando di nuovo la formula nel teorema 1 ci accorgiamo che l'unico caso in cui il sottogruppo $H = \langle x, y \rangle$ può essere aperto è quello in cui $H = F$; concludiamo dunque che due vertici $x, y \in F$ sono non isolati nel virtually generating graph se e solo se sono non isolati nel generating graph. Siccome F è un pro-p-gruppo 2-generato si conclude per la proposizione 1.3.2.

□

Capitolo 4

Il gruppo di Nottingham

4.1 Definizione e proprietà fondamentali del gruppo di Nottingham

4.1.1 Struttura di gruppo

Dato un anello commutativo con identità R, il gruppo di Nottingham su R, che indicheremo con $\mathcal{N}(R)$, è l'insieme formato dagli elementi di $R[[t]]$ dell forma:

$$f = t(1 + \sum_{k=1}^{\infty} a_k t^k), \quad a_k \in R,$$

dotato dell'operazione "$*$" così definita:

$$f * g = g(1 + \sum_{k=1}^{\infty} a_k g^k).$$

L'operazione in questione viene anche chiamata *sostituzione formale*, in virtù della sua interpretazione tramite composizione di funzioni.

Proposizione 4.1.2. $(\mathcal{N}(R), *)$ è un gruppo

Dimostrazione. L'associatività dell'operazione e la verifica che l'indentità coincida con il monomio t sono immediate.
Per quanto riguarda l'esistenza dell'elemento inverso, si considerino prima due elementi generici $f, g \in \mathcal{N}(R)$ con:

$$f = t(1 + \sum_{k=1}^{\infty} a_k t^k), \quad g = t(1 + \sum_{k=1}^{\infty} b_k t^k)$$

allora si ha

$$g * f = t(1 + \sum_{k=1}^{\infty} c_k t^k)$$

con

1. $c_1 = a_1 + b_1$,

2. $c_i = a_i + bi + \sum_{s=1}^{i-1} b_s \phi_s(a_1, \ldots, a_s)$,

dove ϕ_s è un polinomio a coefficienti interi in $a_1, \ldots, a_s$ di grado al più s.

Si osserva dunque che possono essere definiti induttivamente i coefficienti $\{\tilde{a}_k\}_{k\in\mathbb{N}}$ dell'elemento f^{-1} nella seguente maniera:

1. $\tilde{a}_1 := -a_1$,
2. $\tilde{a}_i := -a_i - \sum_{s=1}^{i-1} \tilde{a}_s \phi_s(a_1, \ldots, a_s)$.

□

Lungo l'intera trattazione del capitolo, considereremo solo il caso in cui $R = \mathbb{Z}/p\mathbb{Z}$, con p un numero primo arbitrario, scrivendo per semplicità $\mathcal{N}(p)$ al posto di $\mathcal{N}(\mathbb{Z}/p\mathbb{Z})$, scriveremo inoltre $\mathcal{N}$ quando non sarà necessario esplicitare la dipendenza dal primo p.

Definizione 4.1.3. Si consideri ora al variare di un numero naturale r la famiglia costituita dai seguenti sottoinsiemi di $\mathcal{N}$:

$$\mathcal{N}_r := \{f \in \mathcal{N} \mid f = t(1 + \sum_{k=r}^{\infty} a_k t^k)\}.$$

La *profondità* di un elemento $f \in \mathcal{N}$, che indicheremo con $D(\cdot)$, è definita nel seguente modo:

$$D(f) := \max\{r \in \mathbb{N} \mid f \in \mathcal{N}_r\}$$

Proposizione 4.1.4. Per ogni r si ha che $\mathcal{N}_r \trianglelefteq \mathcal{N}$, ovvero la famiglia $\{\mathcal{N}_i\}_{i\in\mathbb{N}}$ è una filtrazione discendente di sottogruppi normali di $\mathcal{N}$.

Dimostrazione. Osservando la proposizione precedente si derivano due proprietà della profondità:

1. $D(fg) \geq \min\{D(f), D(g)\}$.
2. $D(f^{-1}) = D(f)$.

La condizione $f \in \mathcal{N}_r$ è equivalente a dire che $D(f) \geq r$, dunque considerato un elemento $f \in \mathcal{N}_r$ e un altro elemento $g \in \mathcal{N}$ siamo interessati a stimare $D(g^{-1}fg)$. Si presentano due casi:

1. $D(f) \leq D(g)$: Si ottiene $D(g^{-1}fg) \geq \min\{D(f), D(g)\} \geq D(f)$.
2. $D(f) > D(g)$: Nella regola generale per il prodotto di due elementi $g * f$ ci si accorge che la profondità dà informazioni circa i primi termini della serie formale risultante; in particolare, ponendo $D(f) = r$,si ha nell'anello $R[[x]]$:

$$g * f \equiv g \bmod (t^{r+1})$$

inoltre per come è stato costruito l'inverso si ottiene:

$$g^{-1} * f \equiv g^{-1} \bmod (t^{r+1}) \Longrightarrow (g^{-1} * f) * g \equiv t \bmod (t^{r+1}),$$

ovvero $D(g^{-1}fg) \geq r = D(f)$.

□

4.1.5 Classi laterali e generatori di $\mathcal{N}$

Si fissi $r \in \mathbb{N}$ e si consideri il gruppo $\mathcal{N}/\mathcal{N}_r$; preso un elemento arbitrario $g = t(1 + \sum_{k=1}^{\infty} a_k t^k) \in \mathcal{N}$ possiamo osservare che esso ammette come rappresentante il polinomio troncato $\bar{g} = t(1+\sum_{k=1}^{r-1} a_k t^k)$; questo avviene per il fatto che che $D(g^{-1}*\bar{g}) \geq r$. Ne consegue che le serie troncate sono una lista completa di rappresentanti per le classi laterali e che $|\mathcal{N}/\mathcal{N}_r| = p^{r-1}$.
A questo punto riusciamo anche a verificare che, dotato della topologia profinita indotta dalla base $\{\mathcal{N}_i\}_{i\in\mathbb{N}}$, il gruppo $\mathcal{N}$ è un pro-p-gruppo, essendo isomorfo al limite inverso $\varprojlim_{i\in\mathbb{N}} \mathcal{N}/\mathcal{N}_i$
più esplicitamente, la mappa

$$g = t(1 + \sum_{k=1}^{\infty} a_k t^k) \mapsto \big(t(1 + \sum_{k=1}^{i} a_k t^k)\big)_{i\in\mathbb{N}} \in \varprojlim_{i\in\mathbb{N}} \mathcal{N}/\mathcal{N}_i$$

è un isomorfismo.

Consideriamo adesso una particolare classe di elementi, poniamo $e_n[\alpha] := t(1 + \alpha t^n)$ (si scriverà semplicemente e_n nel caso $\alpha = 1$). Osserviamo subito che $e_n[\alpha] * e_n[\beta] = t(1 + (\alpha + \beta)t^n + n\alpha\beta t^{2n} + \cdots)$ e concludiamo che $\langle e_n \mathcal{N}_{n+1}\rangle = \mathcal{N}_n/\mathcal{N}_{n+1}$; da questa osservazione, siccome $\mathcal{N}$ è profinito concludiamo che $\{e_i\}_{i\in\mathbb{N}}$ è un insieme di generatori per $\mathcal{N}$.
Ciò che si può ulteriormente affermare è che, preso $f \in \mathcal{N}$ con $D(f) = r$ si ha $f \equiv e_r[\alpha] \bmod \mathcal{N}_{r+1}$ per un qualche $\alpha \in (\mathbb{Z}/p\mathbb{Z})^*$; da questo semplice fatto è immediato verificare che vale il seguente

Lemma 4.1.6. Sia H un sottogruppo chiuso di $\mathcal{N}$, supponiamo esista $m \in \mathbb{N}$ tale che, per ogni $n \geq m$ esiste $g \in H$ con $D(g) = n$; allora H è un sottogruppo aperto, siccome in particolare contiene il sottogruppo $\mathcal{N}_m$.

Dimostrazione. Si prenda $r \geq m$, il gruppo $H\mathcal{N}_{r+1}$ contiene $\mathcal{N}_r$; infatti in esso è presente un elemento h di profondità r e si ha $\langle h\rangle\mathcal{N}_{r+1} = \mathcal{N}_r$.
Dunque otteniamo $H\mathcal{N}_m \leq H\mathcal{N}_i$ se $i < m$ e $H\mathcal{N}_i = H\mathcal{N}_m$ se $i \geq m$. Siccome H è chiuso:

$$H = \bar{H} = \bigcap_{i\in\mathbb{N}} H\mathcal{N}_i = H\mathcal{N}_m.$$

□

4.1.7 $\mathcal{N}$ è finitamente generato

Enunciamo senza fornirne una dimostrazione la seguente

Proposizione 4.1.8 (B. Klopsch)**.** Siano $f, g \in \mathcal{N}$ tali che:

$$f \equiv t + f_m t^{m+1} + f_{m+k} t^{m+k+1} \bmod \mathcal{N}_{m+k+1}$$

$$g \equiv t + g_n t^{n+1} + g_{n+l} t^{n+l+1} \bmod \mathcal{N}_{n+l+1}$$

e sia $s := \min\{m+n+k, m+2n, m+n+l, 2m+n\}$, allora, considerando

$$\begin{cases} \gamma_1 := (m+k-n) f_{m+k} g_n & \text{se } s = m+n+k \text{ , 0 altrimenti} \\ \gamma_2 := \left(\binom{m+1}{2} - (n+1)(m-n)\right) f_m g_n^2 & \text{se } s = m+2n \text{ , 0 altrimenti} \\ \gamma_3 := -(n+l-m) f_m g_{n+l} & \text{se } s = m+n+l \text{ , 0 altrimenti} \\ \gamma_4 := -\left(\binom{n+1}{2} - (m+1)(n-m)\right) f_m^2 g_n & \text{se } s = 2m+n \text{ , 0 altrimenti} \end{cases}$$

e ponendo $\gamma := \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$, si ottiene

$$[f, g] \equiv t + (m-n) f_m g_n t^{m+n+1} + \gamma t^{s+1} \mod \mathcal{N}_{s+1}.$$

In particolare, presi $f, g \in \mathcal{N}$ otteniamo

$$D([f,g]) = D(f) + D(g) \quad \text{se} \quad D(f) \not\equiv_p D(g). \tag{4.1}$$

Proposizione 4.1.9. $\mathcal{N}(p)$ è 2-generato se $p \geq 3$, in particolare $\mathcal{N} = \langle e_1, e_2 \rangle$.

Dimostrazione. Osserviamo che $D[e_1, e_2] = 3$, da qui in poi si può continuare a commutare con e_1 fino a quando non raggiungiamo una profondità congrua a 1 modulo p; per ottenere la profondità basterà commutare con e_2 l'elemento trovato precedentemente di profondità congruo a 0 modulo p. Da questo punto in poi possiamo continuare a commutare con e_1, iterando ogni volta il procedimento per ottenere tutte le possibili profondità.

□

Osservazione 4.1.10. In [3] viene calcolata la serie centrale di $\mathcal{N}(2)$ e viene mostrato che è un gruppo 3-generato, più precisamente:

- $\mathcal{N}(2)' = \langle e_3 e_4 e_6, e_5, \mathcal{N}_7 \rangle$.
- $\mathcal{N}(2)/\mathcal{N}(2)' \simeq C_2 \times C_2 \times C_4$.

4.2 Sottogruppi aperti di $\mathcal{N}$

L'obiettivo della nostra indagine è stabilire quando il sottogruppo generato da due elementi è aperto o meno. Si osservano due fatti:

1. In virtù del lemma 4.1.6 se un sottogruppo chiuso contiene elementi di ciascuna profondità a partire da un certo numero naturale in poi possiamo sicuramente dire che è aperto, esso infatti conterrà $\mathcal{N}_d$, per un certo $d \in \mathbb{N}$.

2. La formula della proposizione 4.1.7 può essere usata per questo scopo, tutto sta nel trovare delle condizioni sulle profondità iniziali di due elementi in maniera tale che iterando commutatori tra essi non si ricada mai nel caso in cui i nuovi gradi ottenuti abbiano la medesima congruenza modulo p; a noi basterà che ci sia una sequenza di commutatori iterati che garantiscano questa condizione definitivamente.

Queste osservazioni ci consentono di trasporre il problema nel contesto di una particolare partizione dei numeri naturali che andremo ora a definire. L'esistenza di tale partizione per un determinato numero n ci garantisce di trovare sicuramente un elemento di grado n tramite iterazioni di commutatori fra due elementi fissati.

Definizione 4.2.1. Sia $m, q, r \in \mathbb{N}$, p un primo fissato, una (q, r)-allowable partition per m è una sequenza $\{b_i\}_{i=1,\dots,k}$ tale che:

1. $b_i \in \{q, r\} \quad \forall \quad i \in \{1, \dots, k\}$.
2. Se $s_j = \sum_{i=1}^{j} b_i$ allora $s_j \not\equiv_p b_{j+1}$.
3. $\sum_{i=1}^{k} b_i = m$.

Proposizione 4.2.2. Sia $p \geq 5$ un primo, siano q, r, $\in \mathbb{N}$ tali che

1. $q, r \not\equiv_p 0$.
2. $\gcd(q, r) = 1$.
3. $q \not\equiv_p r$.
4. $q + r \not\equiv_p 0$.

Allora definitivamente ogni numero naturale ammette una (q, r)-allowable partition.

Dimostrazione. Mostriamo anzitutto che esistono M,$l \in \mathbb{N}$ tali che per ogni numero naturale $m \geq M$ si ha $m = uq + vr$, dove $u, v \in \mathbb{N}$, $u \geq v$ e $u - v \leq l$.
Siccome q e r sono coprimi esistono $\alpha, \beta \in \mathbb{Z}$ tali che $1 = \alpha q + \beta r$. Possiamo supporre senza perdita di generalità $\alpha < 0$.
Facendo la divisione euclidea otteniamo in prima battuta $m = xq + d$ con $d < q, x \in \mathbb{N}$. Dunque:

$$m = xq + d \cdot 1 = xq + d(\alpha q + \beta r) = (x + d\alpha)q + (d\beta)r;$$

visto che $d\beta$ è limitato per ogni m scelto si deduce che definitivamente il termine $(x + d\alpha)$ è positivo e supera l'altro termine che moltiplica r. Abbiamo dunque mostrato che esiste la partizione richiesta del tipo $m = uq + vr$, manca il bound sulla quantità $u - v$.
Si consideri ora l'insieme

$$A := \{(u, v) \in \mathbb{N}^2 \mid u \geq v, \quad m = uq + vr\}$$

assieme con la funzione $f : A \to \mathbb{N}, f(u, v) = u - v$. Questa funzione ammette minimo raggiunto in un punto che denoteremo con (u_0, v_0).
Ora, $m = u_0q + v_0r = (u_0 - r)q + (v_0 + q)r$, poniamo $u' = u_0 - r, v' = v_0 + q$, si ha dunque

$$u' - v' = u_0 - r - v_0 - q < f(u_0, v_0) \Longrightarrow (u', v') \notin A$$

e, siccome $v' \geq 0$, si deve necessariamente avere $u' < v'$. In conclusione $0 \leq u_0 - v_0 = u' + r - v' + q < r + q := l$ ed evidentemente il bound trovato non dipende dalla scelta del numero naturale m.
Arrivati a questo punto abbiamo mostrato che possiamo scrivere una sequenza che rispetti le condizioni 1) e 2) per la costruzione di una allowable partition. Più precisamente, sia $k \in \mathbb{N}$ il più piccolo naturale (che per ipotesi è > 1) tale che si abbia $kq + r \equiv_p 0$ e definiamo la sequenza:

$$q, r, \underbrace{q, q, \ldots, q}_{k-1}, q, r, \underbrace{q, q, \ldots, q}_{k-1}, q, r, \ldots$$

continuiamo con questa regola fino a quando il numero di q che compare supera il numero di r di una quantità pari a $u - v$. Qualora la somma dei termini fino ad ora considerati sia uguale ad m abbiamo terminato, altrimenti dobbiamo ancora sistemare un numero eguale di q ed r per concludere, rispettando le opportune congruenze. Si presentano due casi (con l'accorgimento che il ruolo di q ed r può essere scambiato):

1. $x \not\equiv_p q, r$:
   (a) se $x + r \not\equiv_p q \Longrightarrow$ si continua con $x, r, q, \ldots$
   (b) se $x + r \equiv_p q \Longrightarrow$ si ha che $x + q \not\equiv_p r$, infatti questo implicherebbe che $q \equiv_p r$, contro le ipotesi; la sequenza continua dunque con $x, q, r, \ldots$
2. $x \equiv_p r \Longrightarrow x + q \not\equiv_p r$, quindi si continua con $x, q, r, \ldots$

Abbiamo dunque terminato, siccome possiamo iterare il ragionamento fino a quando non esauriamo i termini a disposizione.

□

Corollario 4.2.3. Se q, r soddisfano le ipotesi della proposizione 4.2.2 e f, g sono tali che $D(f) = r, D(g) = q$, allora $\langle f, g \rangle$ è aperto.

Dimostrazione. Per quanto abbiamo mostrato, esiste $M \in \mathbb{N}$ per cui ogni numero maggiore di M ammette una (q,r)-allowable partition. Si fissi ora $m \geq M$ e si sconsideri la sequenza $\{b_i\}_{i=1,\dots,k}$ come nella definizione 4.2.1; definiamo adesso una sequenza $\{x_i\}_{i=1,\dots,k} \subseteq \mathcal{N}$ in maniera tale che x_i sia uguale a f (rispettivamente g) se b_i è uguale a r (rispettivamente q).
Definiamo ricorsivamente una sequenza $\{y_i\}_{i=1,\dots,k} \subseteq \mathcal{N}$ nel seguente modo:

$$\begin{cases} y_1 = x_1 \\ y_i = [y_{i-1}, x_i] \quad 1 \leq i \leq k \end{cases}$$

Usando la proposizione 4.2.2 otteniamo $D(y_j) = s_j = \sum_{i=1}^{j} b_i$ e, siccome $D(y_j) \not\equiv_p b_{j+1}$, otteniamo $D(y_k) = s_k = m$.
Abbiamo dunque mostrato che esiste definitivamente un elemento di profondità arbitraria nel sottogruppo $\langle f, g \rangle$ concludendo per il lemma 4.1.6 che tale sottogruppo è aperto.

□

4.3 Il virtually generating graph di $\mathcal{N}$

Teorema 4.3.1. $\tilde{\Gamma}(\mathcal{N}(p))$ ha come unico vertice isolato l'identità e privato di essa è connesso per ogni $p \geq 5$.

Dimostrazione. Sia $x \in \mathcal{N}$ con $D(x) = n$, abbiamo 4 casi:

1. $n \not\equiv_p -1, 0, 1$: consideriamo $y \in \mathcal{N}$ di profondità 1, per il corollario 4.2.3 (lo useremo ripetutamente durante tutta la dimostrazione), ponendo
   $q = n, r = 1$, $\langle x, y \rangle$ è aperto.

2. $n \equiv_p 1$: consideriamo due casi

   - $n > 1$: $x = t(1 + a_n t^n + a_{n+1} t^{n+1} + \cdots)$,
     $y := t(1 + \gamma t)$ con $\gamma \in (\mathbb{Z}/p\mathbb{Z})^*$ da definire.
     La proposizione 4.1.7 ci permette di esplicitare il termine successivo nel calcolo del commutatore:

     $$z := [x, y] = t\left(1 + \Bigg(\underbrace{n a_{n+1}\gamma + \left(\binom{n+1}{2} - 2(n-1)\right) a_n \gamma^2}_{:=\delta_{n+2}}\Bigg) t^{n+2} + \cdots\right)$$

     sviluppando i calcoli modulo p si ha $\delta_{n+2} = \gamma(a_{n+1} + a_n \gamma)$ e siccome a_n è sicuramente diverso da zero si può scegliere γ in maniera che $\delta_{n+2} \neq 0$, concludendo che $D(z) = n + 2$ (più precisamente possiamo sicuramente scegliere in $p - 2$ modi l'elemento y) . Abbiamo
     $D(y) = 1, D(z) = n + 2, 1 + (n + 2) \equiv_p 4 \not\equiv_p 0$ ottendendo che $\langle y, z \rangle$ è aperto, di conseguenza lo è $\langle x, y \rangle$.

- $n = 1$: si pone $x = t(1+\alpha t+\beta t^2+\cdots)$, $y = t(1+\gamma t)$ come sopra. Con riferimento alla notazione della proposizione 4.1.7 abbiamo $m = 1, k = 1, n = 1, l \in \mathbb{N}$ ottendendo $s = 3$ che rende a priori non nulli i termini $\gamma_1 = \beta\gamma, \gamma_2 = \alpha\gamma^2, \gamma_4 = \alpha^2\gamma$. Si ha dunque

  $$[x, y] = t(1 + \gamma(\alpha^2 + \alpha\gamma + \beta)t^3 + \cdots)$$

  ed evidentemente possiamo scegliere ancora una volta l'elemento γ in $p - 2$ modi diversi in maniera tale che $D[x, y]$ sia uguale a 3; $\langle x, [x, y]\rangle$ è aperto, di conseguenza lo è $\langle x, y\rangle$.

3. $n \equiv_p -1$: sia $q \equiv_p 3$ un primo che non divide n (esso esiste per il teorema di Dirichlet), siccome $n - q \equiv_p -4 \not\equiv_p 0 \Rightarrow y := [x, e_q]$ ha profondità $n + q \equiv_p 2$. Evidentemente $(n, n + q) = (n, q) = 1$, $n + n + q \equiv_p 1$ e si ha dunque che $\langle x, y\rangle$ è aperto, concludendo che lo è pure $\langle x, e_q\rangle$. Si osserva pure che per come è stato scelto q l'elemento e_q è adiacente ad un qualsiasi elemento di profondità 1.

4. $n \equiv_p 0$: sia t tale che

   $$t \not\equiv_p 0, \quad t + 1 \not\equiv_p 0 \quad 2t + 1 \not\equiv_p 0, \quad 3t + 1 \not\equiv_p 0$$

   allora, sempre per il teorema di Dirichlet, l'insieme $\{n + t + pr \quad | r \in \mathbb{N}\}$ contiene infiniti primi; sia $q = t + pr$ con $n + t + pr$ un numero primo.
   Poniamo $x = t(1 + a_n t + a_{n+1}t^{n+1} + \cdots)$, $y := t(1 + t^q + \gamma t^{q+1} + \cdots)$, e calcoliamo

   $$y_2 := [x, y] = t(1 + \delta_{n+q}t^{n+q} + \delta_{n+q+1}t^{n+q+1} + \cdots)$$

   Con $\delta_{n+q} = (n - q)a_n = -qa_n$, $\delta_{n+q+1} = (1 - q)a_{n+1} - (1 + q)a_n\gamma$

   $$\text{si calcola inoltre} \quad y_3 := [y_2, y] = t(1 + \eta_{n+2q+1}t^{n+2q+1} + \cdots)$$

   ottenendo

   $$\eta_{n+2q+1} = (n + q + 1 - q)\delta_{n+q+1} - (q + 1 - n - q)\delta_{n+q}\gamma = \delta_{n+q+1} - \delta_{n+q}\gamma =$$

   $$(1 - q)a_{n+1} - (1 + q)a_n\gamma - qa_n\gamma = (1 - q)a_{n+1} - (2q + 1)a_n\gamma.$$

   Scegliamo γ in maniera tale che il termine $(1 - q)a_{n+1} - (2q + 1)a_n\gamma$ non sia nullo; questo può essere fatto perché $2q + 1 \equiv_p 2t + 1 \not\equiv_p 0$. Il sottogruppo $\langle x, y\rangle$ contiene un elemento di profondità $n + q$ e uno di profondità $n + 2q + 1$, questi due numeri:

   - hanno diversa congruenza modulo p;
   - non sono divisibili per p;
   - sono coprimi: infatti $(n + q, n + 2q + 1) = (n + q, q + 1) = 1$ siccome $n + q$ è primo e non divide $q + 1$ ($n > 1$, siccome in particolare è divisibile per p);
   - $(n + q) + (n + 2q + 1) \equiv_p 3q + 1 \equiv_p 3t + 1 \not\equiv_p 0$.

Si conclude che $\langle x, y\rangle$ è aperto. Abbiamo dunque mostrato che in questo ultimo caso l'elemento x è adiacente ad un opportuno elemento y che ha
profondità $\equiv_p q \equiv_p t \not\equiv_p 0, -1$.

Fatte queste considerazioni, i vertici del grafo possono essere raggruppati in base alle congruenze modulo p delle rispettive profondità, chiameremo "vertice di tipo i" con $i = 1, 2, 3, 4$ i vertici appartenenti ai casi numerati come sopra, specificando che un vertice è di tipo 4_1 se è adiacente a un vertice di tipo 1, di tipo 4_2 se è adiacente a un vertice di tipo 2, ovviamente un vertice può essere di entrambi questi ultimi due tipi. Riassumendo:

- Un vertice x_1 di tipo 1:
  - è a distanza al più 2 da un qualsiasi vertice di tipo 1, poiché due vertici di questo tipo sono entrambi adiacenti ad un qualsiasi vertice di profondità 1.
  - è a distanza al più 2 dai vertici di tipo 2: infatti se x_2 è di tipo 2 esiste $\gamma \in \mathbb{Z}/p\mathbb{Z}$ tale che $t(1 + \gamma t)$ è adiacente sia a x_1 che a x_2.
  - è a distanza al più 3 dai vertici di tipo 3: se x_3 è di tipo 3 esso è adiacente ad e_q per un opportuno primo q che è adiacente ad un arbitrario elemento di profondità 1 che è a sua volta adiacente ad x_1.
  - è a distanza al più 3 dai vertici di tipo 4_2, siccome un elemento di tipo 4_2 è adiacente ad un opportuno elemento di tipo 2 che è a distanza al più 2 da x_1.
  - è a distanza al più 3 dai vertici di tipo 4_1, siccome un elemento di tipo 4_1 è adiacente ad un opportuno elemento di tipo 1 che è a distanza al più 2 da x_1.
- Un vertice x_2 di tipo 2:
  - è a distanza al più 2 dai vertici di tipo 2: se $y \neq x_2$ è di tipo 2 esiste $\gamma \in \mathbb{Z}/p\mathbb{Z}$ tale che $t(1 + \gamma t)$ è adiacente sia a x_2 che a y.
  - è a distanza al più 3 dai vertici di tipo 3: se x_3 è di tipo 3 esiste un opportuno primo q congruo a 3 modulo p tale che e_q sia adiacente ad x_3; a sua volta x_2 è adiacente ad un opportuno elemento di grado 1 che è sicuramente adiacente ad e_q.
  - è a distanza al più 3 dai vertici di tipo 4_1, siccome un vertice di tipo 4_1 è adiacente ad un vertice di tipo 1 che è a distanza al più 2 da x_2.
  - è a distanza al più 3 dai vertici di tipo 4_2: se y è di tipo 4_2 esso è adiacente ad un opportuno elemento y_2, di tipo 2, distante al più 2 da x_2.
- Un vertice x_3 di tipo 3:
  - è a distanza al più 2 da un qualsiasi vertice y di tipo 3, siccome posso scegliere un primo q tale che e_q sia adiacente ad x_3 e a y.
  - è a distanza al più 4 dai vertici di tipo 4_1, poiché è a distanza al più 3 da un qualsiasi vertice di tipo 1

- è a distanza al più 4 dai vertici di tipo 4_2, poiché è a distanza al più 3 da un qualsiasi vertice di tipo 2

- Un vertice x_4 di tipo 4_1:

  - è a distanza al più 4 dai vertici di tipo 4_1, siccome è a distanza al più 3 da un qualsiasi vertice di tipo 1.
  - è a distanza al più 4 dai vertici di tipo 4_2, siccome è a distanza al più 3 da un qualsiasi vertice di tipo 2.

- Un vertice y_4 di tipo 4_2 è a distanza al più 4 da un vertice di tipo 4_2, poiché un qualsiasi vertice di tipo 4_2 è a distanza al più 3 da un vertice di tipo 2.

Queste osservazioni ci consentono di affermare che $\tilde{\Gamma}(\mathcal{N}_p)$ privato dell'identità è connesso e ha diametro minore o uguale a 4.

□

Bibliografia

[1] S. A. Jennings, Substitution groups of formal power series, Canadian J. Math. 6 (1954), 325–340.

[2] R. Camina, The Nottingham group, New horizons in pro-p groups (M. P. F. du Sautoy, D. Segal, and A. Shalev, eds.), Progr. Math., vol. 184, Birkhauser, Boston, MA 2000, pp. 205–221.

[3] C. R. Leedham-Green and S. McKay, The structure of groups of prime power order, London Math. Soc. Monogr. (N. S.), vol. 27, Oxford Univ. Press, Oxford 2002.

[4] I. York, The Group of Formal Power Series under Substitution, Ph.D. thesis, Nottingham, 1990.

[5] J.S. Wilson Profinite Groups, London Math. Soc. Monographs New Series, 19, Claredon, Oxford (1998).

[6] D.L. Johnson, The group of formal power series under substitution, J. Austral. Math. Soc., 45 (1988), pp. 296-302.

[7] R. Camina Subgroups of the Nottingham group J. Algebra, 196 (1997), pp. 101-113.

[8] A. Lucchini, The generating graph of a profinite group, Arch. Math. (2020) https://doi.org/10.1007/s00013-020-01502-y.

[9] A. Lucchini, The virtually generating graph of a profinite group , Canadian Mathematical Society, https://doi.org/10.41532Fs0008439520000843 (2020).

[10] B. Klopsh, Normal Subgroups in Substitution Groups of Formal Power Series, Journal of Algebra Volume 228, Issue 1, 1 June 2000, Pages 91-106.

[11] L. Ribes, P. Zalesskii, Profinite Groups ,Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics (MATHE3, volume 40).

[12] Anthony E.Clement, Stephen Majewicz, Marcos Zyman, The Theory of Nilpotent Groups, Springer, New York, 2017.