Índice

Agradecimentos

Ao meu orientador Professor Paulo Gusmão pelo estímulo e parceria para a realização deste trabalho.

À CAPES e a UFF, pelos auxilios concedidos, sem os quais este trabalho não poderia ter sido realizado.

Aos meus pais, pela educação, atenção e carinho de todas as horas.

Ao Professor Nilson da Costa Bernardes Junior e à Professora Maria de Lourdes Merlini Giuliani, pelas importantes contribuições e palavras de apoio.

Aos professores que participaram da comissão examinadora: Abramo Hefez, Adilson Gonçalves, Orlando Stanley Jurians e Mirian Abdón.

A todos professores e funcionários da pós graduação pelos ensinamentos e pela ajuda.

A todos os amigos e familiares que de uma forma ou de outra me estimularam ou me ajudaram.

Introdução

Em 1968 Milnor publica em [7] dois resultados relacionando a curvatura de variedades riemannianas ao crescimento de seu grupo fundamental.

Com base nestes resultados, Wolf publica em [16], também em 1968, mais alguns resultados envolvendo curvatura de variedades riemannianas, além de mostrar que todo grupo nilpotente finitamente gerado tem crescimento polinomial, no sentido definido por Milnor em [7]. Neste mesmo artigo, Wolf também mostra que todo grupo finitamente gerado que possui um subgrupo nilpotente de índice finito tem crescimento polinomial, além de garantir que todo grupo policíclico de crescimento não exponencial possui um tal subgrupo nilpotente.

Ainda em 1968, como parte da resposta à pergunta proposta em [8], Milnor mostra que todo grupo solúvel finitamente gerado ou tem crescimento exponencial ou possui um subgrupo nilpotente de índice finito.

Outro resultado interessante foi dado por Bass [1] em 1972, que utilizando as idéias propostas por Wolf em [16], construiu dois polinômios de mesmo grau limitando a função crescimento para todo grupo nilpotente finitamente gerado.

A partir destes resultados (dados por Wolf e Milnor) conjecturou-se que todo grupo finitamente gerado de crescimento não exponencial possui um subgrupo nilpotente de índice finito.

Ainda em 1972 J. Tits garante a veracidade desta conjectura para grupos lineares mostrando em [14] que todo grupo linear ou tem um subgrupo nilpotente de índice finito ou possui um subgrupo livre não abeliano de índice finito.

Uma resposta mais geral à conjectura de Milnor-Wolf só foi dada por M. Gromov em 1981. Em [4], Gromov mostra que todo grupo finitamente gerado de crescimento polinomial possui um subgrupo nilpotente de índice finito. Para mostrar isso, Gromov constrói uma sequência decrescente de espaços métricos e mostra que alguma subsequência é convergente no caso do grupo (infinito) ter crescimento polinomial.

As notas à seguir têm o objetivo de apresentar parte dos resultados mencionados em [1], [7], [9], [15], [16] e [17].

No capítulo 1, apresentamos as definições básicas que permitem um bom entendimento dos capítulos seguintes.

A partir do capítulo 2, definimos a função crescimento para grupos finitamente gerados, dando alguns exemplos e analisando o crescimento de subgrupos.

Dedicamos o capítulo 3 ao Teorema de Bass-Wolf que garante que todo grupo nilpotente finitamente gerado tem crescimento polinomial e ao Teorema de Milnor-Wolf que caracteriza a função crescimento para todo grupo solúvel finitamente gerado.

Pretendíamos apresentar o Teorema de Gromov usando as idéias propostas em [17] onde os autores, utilizando argumentos de análise não standard, constroem o mesmo espaço métrico associado a um subgrupo finitamente gerado dado por Gromov em [4]. Apesar de termos entendido as demonstrações de três das seis propriedades do espaço em questão, não foi possível, por falta de tempo, finalizá-las e ao mesmo tempo escrever um texto compreensível sobre os argumentos de análise não standard utilizados para as demonstrações das propriedades em questão. Por esse motivo, resolvemos não fazer a construção do espaço métrico mencionado e sim, admitir sua existência e provar o Teorema de Gromov.

Capítulo 1

Grupos

Este primeiro capítulo é dedicado às definições básicas de grupos, necessárias para o entendimento dos capítulos posteriores.

Algumas demonstrações deste capítulo são omitidas por serem fatos elementares ou por exigirem conceitos que não serão utlizados no decorrer dos capítulos.

1.1 Grupos - Definições Básicas

Definição 1.1.1. Um conjunto G com uma operação

$$(a, b) \in G \times G \mapsto ab \in G$$

é um grupo se as condições seguintes são satisfeitas:

(i) A operação é associativa, isto é, $a(bc) = (ab)c, \forall\ a, b, c \in G$;

(ii) Existe um elemento neutro, isto é, $\exists\ 1 \in G$ tal que $1a = a1 = a$, $\forall\ a \in G$;

(iii) Todo elemento é inversível, isto é, $\forall\ a \in G, \exists\ b \in G$ tal que $ab = ba = 1$.

O grupo é dito abeliano ou comutativo se:

(iv) A operação é comutativa, isto é, $ab = ba \ \forall\ a, b \in G$.

Definição 1.1.2. Seja H um subconjunto de G. Se H for um grupo com a operação de G então H é dito um subgrupo de G e será denotado por $H \leq G$.

Por exemplo, dado um grupo G, o subconjunto $Z(G) = \{g \in G; ga = ag, \forall\ a \in G\}$ é um subgrupo de G, chamado o *centro de* G.

Sejam $H \leq G$ e $g \in G$ então o conjunto

$$gH = \{gh; h \in H\}$$

é chamado *classe lateral à esquerda de* H *em* G.

De forma análoga, definimos a classe lateral à direita de H em G.

A função

$$gH \mapsto Hg^{-1}$$

é uma bijeção. Portanto, toda afirmação válida para classes à esquerda é válida para classes à direita e vice-versa.

O número das distintas classes laterais à esquerda de H em G é chamado o *índice de* H *em* G e será denotado por $(G : H)$.

Proposição 1.1.1. *Sejam* G *um grupo e* K, H *subgrupos de* G *tais que* $K \leq H \leq G$. *Então* $(G : K) = (G : H)(H : K)$.

Demonstração. Pode ser encontrada em [12]. $\square$

Proposição 1.1.2. *A interseção finita de subgrupos de índice finito em um grupo G tem índice finito em G.*

Demonstração. Pode ser encontrada em [10]. □

Se para todo elemento $g \in G$ tivermos

$$gH = Hg \Leftrightarrow gHg^{-1} = H \Leftrightarrow ghg^{-1} \in H, \forall\ h \in H,$$

diremos que H é *um subgrupo normal em* G e denotaremos isto por $H \lhd G$.

Seja $H \lhd G$ então o conjunto $G/H = \{gH; g \in G\}$ é um grupo com a seguinte operação

$$(xH, yH) \mapsto (xy)H$$

e é chamado o grupo quociente de G por H.

Sejam G e K dois grupos. Chamamos de *homomorfismo de grupos* a toda função

$$\varphi : G \to K$$

que preserve a operação dos grupos, isto é,

$$\varphi(ab) = \varphi(a)\varphi(b), \forall\ a, b \in G$$

Se φ é um homomorfismo bijetor diremos que φ é um *isomorfismo* e que G e K são *grupos isomorfos* e denotaremos $G \backsimeq K$.

O conjunto

$$ker(\varphi) = \{g \in G; \varphi(g) = 1_K\}$$

é um subgrupo normal de G, chamado *núcleo de* φ.

O conjunto

$$Im(\varphi) = \{\varphi(g); g \in G\}$$

é um subgrupo de K, chamado *imagem de* φ.

Seja N um subgrupo normal em um grupo G então a função $\varphi : G \to G/N$ dada por $\varphi(g) = gN$ é um homomorfismo de grupos e o chamaremos de *homomorfismo canônico*.

Teorema 1.1.1. *Sejam G, H grupos e $\varphi : G \mapsto H$ um homomorfismo. Então*

$$Im(\varphi) \backsimeq G/Ker(\varphi).$$

Este teorema é conhecido como Teorema dos Homomorfismos e sua demonstração pode ser encontrada, por exemplo, em [10].

Definição 1.1.3. Sejam G um grupo e $S \subseteq G$. Dizemos que S é um conjunto de geradores de G, se todo elemento de G pode ser expresso como um produto finito de elementos de $S \cup S^{-1}$. Se S é finito, dizemos que G é *finitamente gerado*.

Denotaremos $G =< S >$.

Seja G um grupo finitamente gerado. Um conjunto finito $S \subseteq G$ de menor cardinalidade tal que $G =< S >$ chamaremos de *conjunto minimal de geradores de* G.

Se S é composto por um único elemento e $G =< S >$, dizemos que G é um *grupo cíclico*.

Definição 1.1.4. Se G é um grupo então

$$G' =< [g_1, g_2]; g_1, g_2 \in G >$$

onde $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$, é um subgrupo de G chamado o *subgrupo dos comutadores* ou *subgrupo derivado de* G.

Proposição 1.1.3. *Seja G um grupo então G' é o menor subgrupo normal em G tal que G/G' é abeliano.*

Demonstração. De fato, se $g_1, g_2 \in G$ então $g_1 g_2 g_1^{-1} g_2^{-1} \in G'$, donde G/G' é abeliano.

Agora, seja H um subgrupo de G tal que G/H é abeliano. Então para quaisquer $g, h \in G$, $ghg^{-1}h^{-1} \in H$, donde $G' \subseteq H$. $\square$

Proposição 1.1.4. *Um grupo finitamente gerado tem somente um número finito de subgrupos de um dado índice finito j.*

Demonstração. Sejam G um grupo com geradores $a_1, ..., a_n$ e H um subgrupo de G tal que $(G : H) = j$.

Denotemos por

$$H = K_1, K_2, ..., K_j \tag{1.1.1}$$

as distintas classes laterais à esquerda de H em G.

Se $g \in G$, então $gK_1, ..., gK_j$ é uma permutação de (1.1.1), que denotaremos por $P(g)$.

Assim, obtemos uma função φ,

$$\varphi(g) = P(g), g \in G \tag{1.1.2}$$

de G no grupo simétrico S_j. Isto é um homomorfismo, ou seja,

$$P(g_1g_2) = P(g_1)P(g_2).$$

O homomorfismo φ está completamente determinado pelas imagens dos elementos $a_1, ..., a_n$. Consequentemente, existe um número finito de homomorfismos de G em S_j, no máximo $(j!)^n$. No entanto, o homomorfismo φ introduzido em (1.1.2) determina unicamente H, porque um elemento $g \in H$ se, e somente se, a permutação $P(g)$ deixa a classe K_1 invariante.

Portanto, um grupo G gerado por n elementos não contém mais que $(j!)^n$ subgrupos de índice j. □

Proposição 1.1.5. *Seja H um subgrupo de índice finito de um grupo finitamente gerado G. Então H é finitamente gerado.*

Demonstração. Sejam S um conjunto finito de geradores de G e $\{1 = t_1, ..., t_i\}$ um conjunto de representantes das classes laterais à direita de H em G.

Dado $g \in G$, $t_jg \in G$ donde $t_jg \equiv t_k \operatorname{mod}(H)$ para algum $k \in \{1, 2, ..., i\}$ e assim, definamos

$$Ht_jg = Ht_{(j)g}$$

onde $j \mapsto (j)g$ é uma permutação tal que $(j)g = k$.

Daí, obtém-se

$$t_j g = h(j,g)t_{(j)g} \tag{1.1.3}$$

onde $h(j,g) \in H$.

Fixemos $a \in H$ arbitrário, então $a = y_1 ... y_k$ onde $y_l \in S \cup S^{-1}$.

Aplicando (1.1.3), repetidamente, obtemos

$$a = t_1 a = h(1, y_1)h((1)y_1, y_2)...h((...(1)y_1)y_2)...)y_{k-1}, y_k)t_{(1)a}$$

Mas, $Ht_{(1)a} = Ht_1 a = Ha = H$, pois $a \in H$.

Daí, $t_{(1)a} \equiv 1 mod(H)$ donde $\{h(j,y); 1 \leq j \leq i, y \in S \cup S^{-1}\}$ gera H. □

Definição 1.1.5. Seja S um conjunto, possivelmente infinito, de símbolos diferentes. Uma palavra em S é toda expressão finita da forma $s_{i_1}^{\delta_1} s_{i_2}^{\delta_2} ... s_{i_k}^{\delta_k}$, onde $\delta_i \in \mathbb{Z}$ e $s_{i_1}, ..., s_{i_k} \in S$.

Definição 1.1.6. Um grupo abeliano finitamente gerado é dito abeliano livre se existe um inteiro $r \geq 0$ tal que $G \simeq \mathbb{Z}^r$. O inteiro r é denominado o posto de G.

Em particular, a cardinalidade de todo conjunto minimal de geradores de um grupo abeliano livre G é igual ao posto de G.

Pelo Teorema da Decomposição Primária todo grupo abeliano finitamente gerado pode ser escrito como a soma direta de sua parte de torção e sua parte livre.

Daí, o posto de um grupo abeliano finitamente gerado é definido como sendo o posto de sua parte livre e será denotado por $r(G)$.

Definição 1.1.7. Sejam F um grupo, X um conjunto não vazio e $f : X \to F$ uma função. Então F é dito um grupo livre em X se a cada função h de X em um grupo G existir um único homomorfismo $\varphi : F \to G$ tal que $h = \varphi \circ f$.

Definição 1.1.8. Seja X um conjunto e S uma família de palavras em X. Um grupo G tem gerador X e relação S se $G \backsimeq F/R$, onde F é um grupo livre em X e R é o subgrupo normal de F gerado por S.

O par (X, S) é chamado uma apresentação de G e denotado por

$$G =< X \mid S >$$

Na prática, é mais conveniente listar os geradores de G e definir relações $s_i(x) = 1$, $s_i \in S$ (onde i pertence a um conjunto finito de índices) e $x \in X$, isto é,

$$G =< X \mid s_i(x) = 1, s_i \in S >$$

Definição 1.1.9. Um grupo é dito finitamente apresentado se ele tem uma apresentação finita $< X \mid S >$, isto é, uma apresentação em que X e S são conjuntos finitos. Em outras palavras, quando o grupo pode ser representado por um conjunto finito de geradores e um conjunto finito de relações.

Proposição 1.1.6. *Sejam G um grupo e N um subgrupo normal em G. Se N e G/N são finitamente apresentados então G é também finitamente apresentado.*

Demonstração. Seja $\varphi : G \to G/N$ o homomorfismo canônico.

N é gerado por um subconjunto finito $\{y_1, ..., y_r\}$ sujeito a um número finito de relações $u_i(y_1, ..., y_r) = 1$, $i = 1, ..., s$.

G/N é gerado por um subconjunto finito $\{x_1N, ..., x_tN\}$ sujeito a um número finito de relações $v_i(x_1N, ..., x_tN) = 1$, $i = 1, ..., m$.

Então G é gerado por $\{x_1, ..., x_t, y_1, ..., y_r\}$ e estes geradores satisfazem relações da forma (1):

$$\begin{cases} u_i(y) = 1 & \text{se } i = 1, ..., s \\ v_i(x) = \lambda_i(y) & \text{se } i = 1, ..., m \\ x_j y_i x_j^{-1} = \mu_{ij}(y) & \text{se } i = 1, ..., s \\ x_j^{-1} y_i x_j = v_{ij}(y) & \text{se } j = 1, ..., m \end{cases}$$

onde $x = (x_1, ..., x_t)$, $y = (y_1, ..., y_r)$ e as duas últimas igualdades representam a normalidade de N em G.

Afirmação: (1) é um conjunto de relações para G associado ao conjunto $\{x_1, ..., x_t, y_1, ..., y_r\}$.

Para estabelecer isto, seja $\{\xi_1, ..., \xi_t, \eta_1, ..., \eta_r\}$ um conjunto de símbolos em correspondência injetiva com $\{x_1, ..., x_t, y_1, ..., y_r\}$ e considere o grupo Γ gerado por $\{\xi_1, ..., \xi_t, \eta_1, ..., \eta_r\}$ sujeito às relações obtidas em (1), substituindo x_i por ξ_i e y_j por η_j para cada i, j.

Temos um homomorfismo sobrejetor $\pi : \Gamma \to G$ enviando ξ_i em x_i e η_j em y_j para cada i, j. Mostraremos que $K = \ker(\pi)$ é trivial. Seja $\Delta =< \eta_1, ..., \eta_r >$. O terceiro e quarto conjunto das relações em (1) mostram que $\Delta \lhd \Gamma$ e a apresentação de G/N mostra que π induz um isomorfismo de Γ/Δ em G/N. Assim $K \leq \Delta$. Então , se $a \in K$ podemos expressar a da forma $a = w(\eta_1, ..., \eta_r)$. Daí,

$$1 = \pi(a) = w(y_1, ..., y_r)$$

Como as relações $u_i(y)$, $i = 1, ..., s$ são um conjunto de relações de N em $\{y_i, ..., y_r\}$ a relação $w(y_1, ..., y_r) = 1$ é uma consequência das relações $u_i(y) = 1$, $i = 1, ..., s$. Como $u_i(\eta_1, ..., \eta_r) = 1$, para $i = 1, ..., s$ segue-se que $w(\eta_1, ..., \eta_r) = 1$. Daí $a = 1$ e $K = \{1\}$. E portanto, $\Gamma \backsimeq G$. $\square$

1.2 Grupos Solúveis

Nesta seção apresentaremos a definição e algumas propriedades básicas dos grupos solúveis e, então estudaremos duas classes particulares de grupos solúveis: grupos nilpotentes e grupos policíclicos. E veremos no próximo capítulo que existe uma relação fundamental entre a função crescimento de um grupo e seus subgrupos nilpotentes de índice finito (quando tais subgrupos existirem).

Antes, porém, façamos algumas definições:

Definição 1.2.1. Uma série subnormal de um grupo G é uma coleção finita de subgrupos $\{G_i\}_{1\leq i\leq n}$ de G tais que

$$G = G_1 \rhd G_2 \rhd ... \rhd G_n \rhd G_{n+1} = \{1\} \tag{1.2.1}$$

Se $G_i \lhd G$ para todo $i = 2, ..., n$ a série (1.2.1) é chamada *série normal* de G.

Se G_i/G_{i+1} é um grupo abeliano para todo $i = 2, ..., n+1$ dizemos que (1.2.1) é uma *série solúvel*.

Se $G_i/G_{i+1} \subset Z(G/G_{i+1})$ dizemos que (1.2.1) é uma *série central*.

Se $G_{i+1} = [G, G_i]$ dizemos que (1.2.1) é uma *série central inferior* de G, onde

$$[G, G_i] =< \{[g, g_i]; g \in G, g_i \in G_i\} >$$

E, neste caso, (1.2.1) é uma série normal.

Se G_i/G_{i+1} é um grupo cíclico para todo $i = 2, ..., n+1$ dizemos que (1.2.1) é uma *série cíclica*.

Se H e K são dois subgrupos de um grupo G, definimos seu subgrupo de comutadores por $[H, K] =< hkh^{-1}k^{-1}; h \in H, k \in K >$. Definimos, por indução, $G^{(0)} = G$ e $G^{(i+1)} = [G^{(i)}, G^{(i)}]$, isto é, $G^{(i+1)}$ é o subgrupo dos comutadores do grupo $G^{(i)}$, para todo $i = 0, 1, 2, ...$

Lema 1.2.1. *Sejam G um grupo e $x, y \in G$. Se x, y comutam com $[x, y]$ então*

$$[x, y]^n = [x^n, y] = [x, y^n]$$

para todo $n \in \mathbb{Z}$.

Demonstração. Primeiro, provemos para n não negativo, por indução.

A igualdade é trivial para $n = 0$.

Suponhamos o resultado válido para $n > 0$. Então, por hipótese

$$[x, y]^n[x, y] = x[x, y]^n yx^{-1}y^{-1}$$

E pela hipótese de indução, temos

$$[x, y]^n[x, y] = x[x^n, y]yx^{-1}y^{-1} = x(x^n yx^{-n}y^{-1})yx^{-1}y^{-1}$$

Portanto,

$$[x, y]^n[x, y] = [x^{n+1}, y].$$

Agora, $x[x, y] = [x, y]x$, por hipótese, então $xxyx^{-1}y^{-1} = xyx^{-1}y^{-1}x$, isto é,

$$[x, y]^{-1} = [y, x^{-1}] = [x^{-1}, y].$$

Logo, se $n \geq 0$,

$$[x, y]^{-n} = [x^{-1}, y]^n = [x^{-n}, y].$$

$\square$

Definição 1.2.2. Seja G um grupo e H um subgrupo de G. O conjunto

$$N_G(H) = \{g \in G; gHg^{-1} = H\}$$

chama-se o normalizador de H em G.

Proposição 1.2.1. *Sejam H e K subgrupos de um grupo G. Então $N_G(H)$ admite as seguintes propriedades:*

(i) $H \lhd N_G(H)$;

(ii) $N_G(H) = G \Leftrightarrow H \lhd G$;

(iii) $H \lhd K \leq G \Rightarrow K \subseteq N_G(H)$.

Demonstração. Pode ser encontrada em [10]. $\square$

Proposição 1.2.2. *Seja G um grupo. As seguintes condições são equivalentes:*

(i) O grupo G possui uma série solúvel.

(ii) Existe um inteiro n tal que $G^{(n)} = \{1\}$.

Demonstração. Pode ser encontrada em [10]. $\square$

Definição 1.2.3. Um grupo G é dito solúvel se ele satisfaz alguma das condições equivalentes da Proposição 1.2.2.

Teorema 1.2.1. *Seja G um grupo.*

(i) Seja H um subgrupo de G. Se G é solúvel, então H é solúvel.

(ii) Seja H um subgrupo normal de G. Então o grupo G é solúvel se, e somente se, os grupos H e G/H são solúveis.

Demonstração. Pode ser encontrada em [10]. $\square$

Proposição 1.2.3. *Seja G um grupo. As seguintes condições são equivalentes:*

(i) G possui uma série central.

(ii) G possui uma série central inferior.

Demonstração. (i)$\Rightarrow$ (ii) Seja $G = G_1 \supset G_2 \supset ... \supset G_{k+1} = \{1\}$ uma série central para G, e sejam, $g \in G$ e $g_i \in G_i$. Como $G_i/G_{i+1} \subseteq Z(G/G_{i+1})$ segue-se que $gg_ig^{-1}g_i^{-1} \in G_{i+1}$ e logo, $[G, G_i] \subseteq G_{i+1}$.

Se denotarmos $H_i = [G, G_i] \subseteq G_{i+1}$ temos $H_{i+1} = [G, G_{i+1}] \subset [G, G_i] = H_i$. Em particular, $H_k = [G, G_k] \subset G_{k+1} = \{1\}$. Portanto, $G = H_1 \supset H_2 \supset ... \supset H_k = \{1\}$ é uma série central inferior para G.

(ii)$\Rightarrow$ (i) Seja $G = G_1 \supset G_2 \supset ... \supset G_{k+1} = \{1\}$ uma série central inferior de G.

Se $g \in G$ e $g_i \in G_i$ então, como $[g, g_i] \in G_{i+1}$ temos $[g^{-1}, g_i]G_{i+1} = G_{i+1}$. Logo, $G_i/G_{i+1} \subset Z(G/G_{i+1})$ e portanto, G possui uma série central. $\square$

Definição 1.2.4. Um grupo G é dito nilpotente se ele satisfaz alguma das condições equivalentes da Proposição 1.2.3. Em particular, todo grupo nilpotente é solúvel.

Definição 1.2.5. Seja $(G_i)_{i\in\mathbb{N}}$ uma série central inferior de G. O primeiro $k \geq 1$ tal que $G_k = \{1\}$ é chamado o índice de nilpotência de G.

Todo grupo nilpotente com índice de nilpotência 1 é abeliano.

Proposição 1.2.4. *Seja G um grupo nilpotente e H um subgrupo de G. Então:*

(i) H é nilpotente.

(ii) Se H é um subgrupo próprio de G então H está propriamente contido em seu normalizador.

(iii) Todo subgrupo próprio maximal de G é normal em G.

Demonstração. Sejam $G = G_1 \supset G_2 \supset ... \supset G_{k+1} = \{1\}$ uma série central de G e H um subgrupo.

Para (i), basta tomar $H_i = G_i \cap H$ e logo, $H = H_1 \supset H_2 \supset ... \supset H_{k+1} = \{1\}$ é uma série central para H.

(ii) Suponhamos que H seja um subgrupo próprio de G.

Considere o inteiro $j \in \{0, ..., k\}$ tal que $G_{j+1} \subset H$ e $G_j \nsubseteq H$.

Como $[G, G_j] \subset G_{j+1}$, temos

$$[H, G_j] \subset [G, G_j] \subset G_{j+1} \subset H$$

e logo, existe $\alpha \in G_j \backslash H$ tal que $[H, \alpha] \subseteq H$, isto é,

$$\alpha H \alpha^{-1} = H$$

e portanto, $H \subsetneq N_G(H)$.

(iii) Se H é um subgrupo maximal de G, segue-se de (ii) que $N_G(H) = G$ e portanto, pela Proposição 1.2.1, $H \lhd G$. $\square$

Definição 1.2.6. Seja p um primo e G um grupo. G é dito um p-grupo se para todo $g \in G$ existe um $k \in \mathbb{N}$ tal que $g^{p^k} = 1$.

Proposição 1.2.5. *Todo p-grupo finito é nilpotente.*

Demonstração. Pode ser encontrada em [10]. $\square$

A Proposição 1.2.5 não é verdadeira se G não for um p-grupo finito.

Por exemplo, se $G = \prod_{n=3}^{\infty} D_{2^n}$, onde D_{2^n} é o grupo diedral de ordem 2^n.

G é um 2-grupo, porém não é nilpotente.

Proposição 1.2.6. *Seja G um grupo nilpotente com série central inferior $G = G_1 \supseteq G_2 \supseteq ... \supseteq G_{k-1} \supseteq G_k = \{1\}$. Então $[G_i, G_j] \subset G_{i+j}$.*

Demonstração. Pode ser encontrada em [10] ou [13]. $\square$

Definição 1.2.7. Seja G um grupo abeliano. Diz-se que os elementos $g_1, ..., g_n \in G$ são linearmente independentes sobre $\mathbb{Z}$ se a equação $g_1^{m_1} ... g_n^{m_n} = 1_G$ só for possível quando todos os $m_j \in \mathbb{Z}$ forem nulos.

Proposição 1.2.7. *Seja G um grupo nilpotente finitamente gerado com série central inferior $G = G_1 \supsetneq G_2 \supsetneq ... \supsetneq G_{s+1} = \{1\}$. Então existem conjuntos $T_k = \{\tau_{k,1}, ..., \tau_{k,r_k}\} \subset G_k$ tais que:*

(i) Se $\varphi_k : G_k \to G_k/G_{k+1}$ denota a projeção canônica então $\{\varphi_k(\tau_{k,1}), ..., \varphi_k(\tau_{k,r_k})\}$ é um conjunto linearmente independente sobre $\mathbb{Z}$ de geradores para G_k/G_{k+1};

(ii) Se $k > 1$ então todo $\tau_{k,t} \in T_k$ é da forma

$$[\tau_{1,i}, \tau_{k-1,j}] \text{ com } \tau_{1,i} \in T_1 \text{ e } \tau_{k-1,j} \in T_{k-1}.$$

(iii) T_1 *gera* G.

Demonstração. Provemos (i) e (ii) por indução sobre k.

Sendo G finitamente gerado, cada quociente G_k/G_{k+1} é finitamente gerado.

Para construir T_1, tome um conjunto linearmente independente de geradores $\{a_1, ..., a_{r_1}\}$ de G/G_2 e escolha, arbitrariamente, $\tau_{1,i} \in \varphi^{-1}(a_i)$.

Seja $k > 1$ e suponha construídos $T_1, ..., T_{k-1}$ satisfazendo (i) e (ii).

Sejam $\Delta = G/G_{k+1}$, $\delta : G \to \Delta$ o homomorfismo canônico e $\Delta_t = \delta(G_t)$.

Seja $S_t = \{\sigma_{t,1}, ..., \sigma_{t,r_t}\}$ onde $\sigma_{t,m} = \delta(\tau_{t,m})$, $1 \leq t \leq k-1$.

Se $v \in \Delta_k$ então v é um produto de comutadores $[\alpha, \beta]$ com $\alpha \in \Delta$ e $\beta \in \Delta_{k-1}$.

Note que, se $\alpha' \in \alpha\Delta_k$ e $\beta' \in \beta\Delta_k$ então $[\alpha', \beta'] \in [\alpha, \beta]\Delta_k$.

Suponha então, $\alpha = \sigma_{1,1}^{a_1} ... \sigma_{1,n}^{a_n}$ e $\beta = \sigma_{k-1,1}^{b_1} ... \sigma_{k-1,r_k}^{b_{r_{k-1}}}$, sendo $a_i, b_j \in \mathbb{Z}$, $\sigma_{1,i} \in S_1$ e $\sigma_{k-1,j} \in S_{k-1}$.

Como $S_{k-1} \subset \Delta_{k-1}$ e Δ_k é central em Δ, segue-se que $\sigma_{k-1,j}\Delta_k \in Z(\Delta/\Delta_k)$, donde $[\sigma_{1,i}, \sigma_{k-1,j}]\Delta_k = \Delta_k$, qualquer que seja $\sigma_i \in \Delta$.

Portanto,

$$[\alpha, \beta]\Delta_k = [\prod_{i=1}^{n} \sigma_{1,i}^{a_i}, \prod_{j=1}^{r_{k-1}} \sigma_{k-1,j}^{b_j}]\Delta_k = \Delta_k = \prod_{i,j} [\sigma_{1,i}, \sigma_{k-1,j}]^{a_i b_j} \Delta_k.$$

Logo,

$$[\alpha, \beta] \equiv \prod_{i,j} [\sigma_{1,i}, \sigma_{k-1,j}]^{a_i b_j} \operatorname{mod}(\Delta_k)$$

isto é, Δ_k é gerado por $[\sigma_{1,i}, \sigma_{k-1,j}]$. Em outras palavras, G_k/G_{k+1} é gerado por $\varphi_k([\tau_{1,i}, \tau_{k-1,j}])$.

Agora, escolha um subconjunto linearmente independente sobre $\mathbb{Z}$ de geradores para G_k/G_{k+1} e defina $T_k = \{\tau_{k;1}, ..., \tau_{k,r_k}\}$, obtendo o resultado.

Em particular, T_1 gera G. $\square$

Definição 1.2.8. Um grupo G é dito policíclico se possui uma série cíclica.

Proposição 1.2.8. *Todo grupo policíclico tem apresentação finita. Em particular, todo grupo policíclico é finitamente gerado.*

Demonstração. Seja $G = G_1 \supset G_2 \supset ... \supset G_{k+1} = \{1\}$ uma série cíclica de G. Como G_k é cíclico, temos que G_{k-1}/G_k e G_k têm apresentações finitas e pela Proposição 1.1.6 segue-se que G_{k-1} tem apresentação finita. Agora, G_{k-1} e G_{k-2}/G_{k-1} têm apresentações finitas, donde, novamente pela Proposição 1.1.6, G_{k-2} tem apresentação finita. Argumentando da mesma maneira vemos que G_i tem apresentação finita, para todo $i \in \{1, 2, ..., k\}$. Portanto, G tem apresentação finita. □

Proposição 1.2.9. *Sejam G um grupo e H um subgrupo normal em G. As seguintes afirmações são equivalentes.*

(i) G é policíclico;

(ii) H e G/H são policíclicos.

Demonstração. (i)⇒ (ii) Seja $G = G_1 \supset G_2 \supset ... \supset G_k = \{1\}$ uma série cíclica de G.

Sendo H um subgrupo de G, defina, para cada i natural, $H_i = H \cap G_i$.

Note que $H_{i+1} = H \cap G_{i+1} \subset H \cap G_i = H_i$ e é fácil notar que $H_{i+1} \lhd H_i$. Pelo Teorema dos Homomorfismos

$$\frac{H_i}{H_{i+1}} = \frac{H_i}{(H_i \cap G_{i+1})} \simeq \frac{H_i G_{i+1}}{G_{i+1}}$$

que é um subgrupo do grupo cíclico G_i/G_{i+1}. Portanto,

$$H = H_1 \supset H_2 \supset ... \supset H_k = \{1\}$$

é uma série cíclica de H.

Sendo $H \lhd G$, considere os subgrupos G_iH de G. Como $G_{i+1} \lhd G_i$ segue-se que $G_{i+1}H \lhd G_iH$, o homomorfismo canônico $\varphi_i : G_i \to G_iH/H$ está bem definido e $\ker \varphi_i = H_i$. Logo pelo Teorema dos Homomorfismos, $G_i/H_i \simeq G_iH/H$.

Como $G_{i+1} \subset G_i$ segue-se que $G_{i+1}H/H \subset G_iH/H$. Note, ainda, que

$$G_{i+1}/H_{i+1} \supset G_{i+1}/H_i$$

e logo,

$$\frac{(G_iH/H)}{(G_{i+1}H/H)} \simeq \frac{(G_i/H_i)}{(G_{i+1}/H_{i+1})} \subset \frac{(G_i/H_i)}{(G_{i+1}/H_i)} \simeq G_i/G_{i+1}$$

e como todo subgrupo de um grupo cíclico é cíclico, segue-se que G/H é policíclico.

(ii) $\Rightarrow$(i) Sendo G/H policíclico, existem subgrupos $G_2, ..., G_{k-1}$ de G, contendo H e tais que a série $G/H = G_1/H \supset G_2/H \supset ... \supset G_{k-1}/H \supset G_k/H = \{H\}$ é uma série cíclica.

Por outro lado, como H é policíclico, existem subgrupos $H_2, ..., H_s$ tais que a série $H = H_1 \supset H_2 \supset ... \supset H_{s+1} = \{1\}$ é cíclica.

Então, a série $G = G_1 \supset ... \supset G_{k-1} = H_1 \supset H_2 \supset ... \supset H_{s+1} = \{1\}$ é uma séire cíclica de G. Donde G é policíclico. □

Observação 1.2.1. *Note que para mostrar que H é um grupo policíclico, não utilizamos o fato de H ser normal em G. Portanto, todo subgrupo de um grupo policíclico é policíclico.*

Proposição 1.2.10. *Um grupo abeliano é policíclico se, e somente se, é finitamente gerado.*

Demonstração. Pela Proposição 1.2.8, basta provar que se A é um grupo abeliano finitamente gerado então A é policíclico.
De fato, se $A =< a_1, ..., a_n >$ então

$$A =< a_1, ..., a_n >\supset< a_1, ..., a_{n-1} >\supset ... \supset< a_1, a_2 >\supset< a_1 >\supset \{1\}$$

é uma série cíclica de A. □

Capítulo 2

A Função Crescimento para Grupos

Neste capítulo definiremos a função crescimento para um grupo finitamente gerado, mencionando algumas propriedades e dando alguns exemplos. Definiremos dois tipos de crescimento de grupos que têm importância fundamental para os objetivos propostos. Também explicitaremos a função crescimento para uma classe particular de grupos.

2.1 A Função Crescimento e suas Propriedades

Dedicamos esta seção à definição da função crescimento para grupos finitamente gerados, suas propriedades e alguns exemplos simples.

Definição 2.1.1. Seja G um grupo gerado por um conjunto finito S. Suponha que, se $s \in S$ então $s^{-1} \in S$. A função comprimento

$$\ell_S : G \to \mathbb{N}$$

relativa a S é definida por

$$\ell_S(g) = \min\{n \in \mathbb{N}; g = s_1...s_n, s_i \in S\};$$

isto é, o comprimento da menor palavra em S representando g.

Por definição, $\ell_S(1) = 0$ e a função comprimento, que depende do conjunto finito S, admite a seguinte propriedade:

$$\text{Se } g, h \in G, \text{ então } \ell_S(gh) \leq \ell_S(g) + \ell_S(h).$$

Definição 2.1.2. Seja G um grupo gerado por um conjunto finito S. A função crescimento

$$\gamma_S : \mathbb{N} \to \mathbb{N}$$

relativa a S é definida por

$$\gamma_S(m) = \mathrm{Card}\{g \in G; l_S(g) \leq m\};$$

isto é, o número de elementos distintos de G expressos como palavras de comprimento menor que, ou igual a m em S.

Lema 2.1.1. *A função crescimento admite as seguintes propriedades:*
(i) $\gamma_S(0) = 1$*;*
(ii)$\gamma_S(m+n) \leq \gamma_S(m)\gamma_S(n)$*;*
(iii) $\gamma_S(m) \leq \gamma_S(1)^m$*.*

Demonstração. Para (i), basta notar que o único elemento de comprimento nulo em G é o elemento neutro.

Para (ii), considere $T(i) = \{g \in G; \ell_S(g) = i\}$ para todo $i \in \mathbb{N}$ e assim,

$$\gamma_S(m) = \sum_{i=0}^{m} c(i),$$

onde $c(i) = \mathrm{Card}\, T(i)$.

Dados $g, h \in G$ temos $c(i+j) \leq c(i)c(j)$, para quaisquer $i, j \in \mathbb{N}$.

Sejam $m < n$ naturais fixados, então

$$\begin{aligned}\gamma_S(m+n) &= \sum_{i=0}^{m+n} c(i) = \sum_{i=0}^{m} c(i) + \sum_{i=m+1}^{n-1} c(i) + c(n) + ... + c(m+n)\\ &\leq \gamma_S(m) + \sum_{i=m+1}^{n-1} c(i) + (1 + c(1) + ... + c(m))c(n)\\ &= \gamma_S(m)(1 + c(n)) + \sum_{i=m+1}^{n-1} c(i)\\ &\leq \gamma_S(m)(1 + c(n)) + \gamma_S(m)\sum_{i=1}^{n-1} c(i) = \gamma_S(m)\gamma_S(n)\end{aligned}$$

provando (ii).

Provemos (iii) por indução em m.

A asserção é óbvia para $m = 0$. Suponha, então a afimação válida para $m > 0$. Então, por (ii) e pela hipótese de indução,

$$\gamma_S(m+1) \leq \gamma_S(m)\gamma_S(1) \leq \gamma_S(1)^m\gamma_S(1) = \gamma_S(1)^{m+1}.$$

□

Exemplos.

1) Seja $G = \mathbb{Z} \times \mathbb{Z}$ e $S = \{(1,0),(0,1)\}$. Então $\gamma_S(m) = 2m^2 + 2m + 1$.

Demonstração. De fato, provemos a afirmação por indução em m.

O resultado é óbvio para $m = 0$.

Suponhamos o resultado válido para $m - 1$ e seja $T = \{g \in G; l_S(g) = m\}$. Então pela definição de função crescimento,

$$\gamma_S(m) = \gamma_S(m-1) + \mathrm{Card}(T).$$

Se $g \in G$ então existem inteiros r e s tais que $g = r(1,0) + s(0,1)$.

Pela definição de comprimento de uma palavra, a cardinalidade de T é exatamente o número de soluções inteiras da equação

$$\mid r \mid + \mid s \mid = m \tag{2.1.1}$$

Se $r, s \in \mathbb{N}$ então, por combinações repetidas, existem $m+1$ soluções inteiras não negativas para a equação

$$r + s = m. \tag{2.1.2}$$

Note que uma parte das soluções da equação (2.1.1) são soluções de (2.1.2) em $\mathbb{Z}$. Assim, se (r, s) é solução de (2.1.1) e (2.1.2) então $(-r, -s)$ também é solução de (2.1.1). As demais soluções de (2.1.1) são das formas $(\pm r, \mp s)$, sendo r e s inteiros não nulos que, em quantidade, são iguais ao número de soluções do tipo $(\pm r, \pm s)$, sendo r e s inteiros não nulos. Observe que se r ou s é nulo então (r, s) é solução de (2.1.1) se, e somente se, $r = 0$ e $s = m$ ou vice-versa, sendo que (2.1.1) possui quatro soluções deste tipo. Portanto, $\mathrm{Card}(T) = 2(m+1) + 2(m+1) - 4 = 4m$.

Assim, pela hipótese de indução,

$$\gamma_S(m) = 2(m-1)^2 + 2(m-1) + 1 + 4m = 2m^2 + 2m + 1.$$

$\square$

2) Seja G um grupo livre e $S = \{a, b\}$, $a \neq b$ então $\gamma_S(m) = 2.3^m - 1$.

Demonstração. Como no exemplo (1), provaremos esta afirmação por indução em m.

De fato, a asserção é óbvia para $m = 0$.

Suponhamos a afirmação válida para $m-1$ e, mantendo a notação anterior, temos

$$\gamma_S(m) = \gamma_S(m-1) + \mathrm{Card}(T)$$

Sendo G livre e gerado por dois elementos segue-se, indutivamente, que existem 4.3^{m-1} elementos de comprimento m em G, pois cada elemento de comprimento $m-1$ em S dá origem (quando operado com um elemento de S) a outros três de comprimento m em S.

Assim, pela hipótese de indução, temos

$$\gamma_S(m) = 2.3^{m-1} - 1 + 4.3^{m-1} = 2.3^m - 1.$$

$\square$

Proposição 2.1.1. *A sequência* $x_m = \gamma_S(m)^{\frac{1}{m}}$ *é convergente.*

Demonstração. De fato, para t fixado em $\mathbb{N}$, ponha $k = \frac{m}{t} + 1$, assim

$$\gamma_S(m) \leq \gamma_S(kt) \leq \gamma_S(t)^k = \gamma_S(t)^{\frac{m}{t}+1}.$$

Daí,

$$\gamma_S(m)^{\frac{1}{m}} \leq \gamma_S(t)^{\frac{1}{t}+\frac{1}{m}}$$

Logo,

$$\lim_{m\to\infty} \sup \gamma_S(m)^{\frac{1}{m}} \leq \gamma_S(t)^{\frac{1}{t}} \tag{2.1.3}$$

para todo t fixado.

Em particular,

$$\lim_{m\to\infty} \sup \gamma_S(m)^{\frac{1}{m}} \leq \gamma_S(1) = 2\,\mathrm{Card}(S) + 1 \in \mathbb{N}.$$

Donde $\lim\limits_{m\to\infty} \sup \gamma_S(m)^{\frac{1}{m}}$ não pode ser infinito.

Então, por 2.1.3, temos

$$\lim_{m\to\infty} \sup \gamma_S(m)^{\frac{1}{m}} \leq \inf_{t\in\mathbb{N}} \{\gamma_S(t)^{\frac{1}{t}}\} \leq \lim_{m\to\infty} \inf \gamma_S(m)^{\frac{1}{m}}$$

logo, $\lim\limits_{m\to\infty} \sup \gamma_S(m)^{\frac{1}{m}} = \lim\limits_{m\to\infty} \inf \gamma_S(m)^{\frac{1}{m}}$ e portanto, a sequência $(x_m)_{m\in\mathbb{N}}$ é convergente. $\square$

Observação 2.1.1. *Pela Proposição 2.1.1,*

$$e_S = \lim_{m\to\infty} \gamma_S(m)^{\frac{1}{m}}$$

sempre existe e $e_S \geq 1$*.*

Lema 2.1.2. *Sejam S e T subconjuntos finitos de um grupo finitamente gerado G e suponha $< T > \subseteq < S >$. Então existe um inteiro $a > 0$ tal que $\gamma_T(m) \leq \gamma_S(am)$ para todo $m \geq 0$.*

Demonstração. Basta tomar $a = \max\{l_T(s); s \in S\}$. □

Definição 2.1.3. Dizemos que um grupo G, gerado por um subconjunto finito S, tem crescimento exponencial se existem uma constante $a \in \mathbb{R}_+$ e $m_0 \in \mathbb{N}$ tais que $\gamma_S(m) \geq a^m$ para todo $m \geq m_0$.

Observação 2.1.2. *Pelo Lema 2.1.2 esta definição não depende do conjunto finito de geradores.*

Lema 2.1.3. *Seja G um grupo gerado por um conjunto finito S e tal que $e_S > 1$. Então G tem crescimento exponencial.*

Demonstração. Existe $a > 1$ tal que $\gamma_S(m)^{\frac{1}{m}} \geq a$ para todo m suficientemente grande. E daí,

$$\gamma_S(m) \geq a^m$$

donde G tem crescimento exponencial. □

Definição 2.1.4. Dizemos que um grupo G, gerado por um subconjunto finito S, tem crescimento polinomial de grau $\leq d$ ($d \in \mathbb{N}$) se existe uma constante $c \in \mathbb{R}_+$ tal que

$$\gamma_S(m) \leq cm^d$$

para todo $m \geq 1$.

2.2 Crescimento de Subgrupos

Nesta seção daremos condições necessárias e suficientes para que um grupo tenha o mesmo tipo de crescimento que alguns de seus subgrupos.

Sejam G um grupo e H um subgrupo. Escolha um conjunto U de representantes das classes G/H com $1 \in U$. Para cada $s \in G$ ponha $s = s^* h_s$ ($s^* \in U$ e $h_s \in H$).

Se $s, t \in G$ então

$$st = (st)^* h_{st}$$

Por outro lado,

$$st = st^* h_t = (st)^* h_{st^*} h_t$$

e daí,

$$h_{st} = h_{st^*} h_t.$$

Por indução em m segue que

$$h_{s_1 \ldots s_m} = h_{s_1 (s_2 \ldots s_m)^*} h_{s_2 (s_3 \ldots s_m)^*} \ldots h_{s_{m-1} s_m^*} h_{s_m} \tag{2.2.1}$$

Se $s \in G$ e $u \in U$, temos

$$1 = h_u = h_{ss^{-1}u} = h_{s(s^{-1}u)^*} h_{s^{-1}u^*} h_u = h_{s(s^{-1}u)^*} h_{s^{-1}u}$$

Donde,

$$h_{s^{-1}u} = h^{-1}_{s(s^{-1}u)^*} \tag{2.2.2}$$

Lema 2.2.1. *Seja S um conjunto de geradores para G e seja $V = \{h_{su}; s \in S, u \in U\}$. Então $H = < V >$.*

Demonstração. Se $h \in H$ ponha $h = s_1...s_m$, onde $s_i \in S \cup S^{-1}$ para cada $i = 1, 2, ..., m$.

Como $h \in H$ temos $h = 1.h_{s_1...s_m} = h_{s_1...s_m}$ que, por (2.2.1), é um produto finito de elementos $h_{s_i u_i}$ com $u_i \in U$. Mas, por (2.2.2), temos

$$h_{s_i^{-1} u_i} = h^{-1}_{s_i (s_i^{-1} u_i)^*}$$

então cada $h_{s_i u_i} \in V \cup V^{-1}$. □

Suponha agora, S finito e que H tenha índice finito em G.

Logo, U e V são finitos. De (2.2.1) e (2.2.2) vemos que se $g \in G$ e $\ell_S(g) = m$ então $\ell_V(h_g) \leq m$.

Como $g = g^* h_g$, com $g^* \in U e h_g \in H$, temos

$$\begin{aligned}
\gamma_S(m) &= \operatorname{Card}\{g \in G; \ell_S(g) \leq m\} \\
&\leq \operatorname{Card}\{g^* \in U; \ell_S(g^*) \leq m\}. \operatorname{Card}\{h_g \in H; \ell_S(h_g) \leq m\} \\
&\leq (\operatorname{Card} U)\gamma_V(m)
\end{aligned}$$

isto é,

$$\gamma_S(m) \leq (G : H)\gamma_V(m) \tag{2.2.3}$$

Extraíndo-se a raiz m-ésima de ambos lados de (2.2.3) segue-se que

$$e_S(G) = e_V(H).$$

Combinando os lemas 2.1.2 e 2.1.3 obtemos a seguinte:

Proposição 2.2.1. *Sejam G um grupo finitamente gerado e H um subgrupo de índice finito em G. Então*

G tem crescimento exponencial se, e somente se, H tem crescimento exponencial.

G tem crescimento polinomial de grau $\leq d$ se, e somente se, H tem crescimento polinomial de grau $\leq d$.

2.3 Crescimento de alguns Grupos

Iniciaremos esta seção determinando a função crescimento de alguns grupos.

Vimos na seção 2.1 (exemplo 1) que se $G = \mathbb{Z} \times \mathbb{Z}$ e $S = \{(1,0),(0,1)\}$, então $\gamma_S(m) = 2m^2 + 2m + 1$, ou seja, G tem crescimento polinomial de grau 2. Mais geralmente, temos a seguinte

Proposição 2.3.1. *Seja $S = \{s_1, s_2, ..., s_n\}$ um conjunto minimal de geradores para um grupo abeliano livre de posto n. Então*

$$\gamma_S(m) = \sum_{l=0}^{n} 2^l \binom{n}{l}\binom{m}{l}.$$

Demonstração. Para todo inteiro $l \geq 0$ denotemos por P_l a função inteira não negativa dada por $P_0(m) = 1$ para todo inteiro $m \geq 0$ e $P_l(m)$, $l > 0$, o número de sequências distintas $(a_1, ..., a_l)$ de inteiros positivos com $a_1 + ... + a_l \leq m$. Note que $P_0(m) = \binom{m}{0}$.

Se $l > 0$, então para cada $P_l(m)$ a sequência $(a_1, ..., a_l)$ dá origem a um subconjunto $\{a_1, a_1+a_2, ..., a_1+a_2+...+a_l\}$ de $\{1, 2, ..., m\}$ de cardinalidade l. Consequentemente, se um subconjunto de cardinalidade l em $\{1, 2, ..., m\}$ é colocado em ordem ascendente, ele pode ser visto da forma $\{a_1, a_1 + a_2, ..., a_1 + a_2 + ... + a_l\}$. Portanto, em geral, $P_l(m) = \binom{m}{l}$. Em particular, P_l é um polinômio em m de grau l com coeficientes inteiros e não negativos.

Observe que $\gamma_S(m) = \sum_{l=0}^{n} N_l(m)$, onde $N_l(m)$ é o número de expressões distintas $s_{j_1}^{a_1} ... s_{j_n}^{a_n}$, com $\sum \mid a_i \mid \leq m$, tal que exatamente l dos a_i's são não nulos.

Seja $U = \{u_1, ..., u_l\}$, onde $u_i \in S$, alguns dos $\binom{n}{l}$ subconjuntos de S com exatamente l elementos.

Por definição de P_l existem precisamente $P_l(m)$ elementos distintos da forma $u_1^{a_1} ... u_l^{a_l}$ com $a_i > 0$ e $\sum a_i \leq m$. Permutando os sinais de a_i vemos que existem precisamente $2^l P_l(m)$ elementos $u_1^{a_1} ... u_l^{a_l}$, distintos com $a_i \neq 0$ e $\sum \mid a_i \mid \leq m$.

Assim,

$$N_l(m) = 2^l \binom{n}{l} P_l(m) = 2^l \binom{n}{l}\binom{m}{l}$$

completando a prova da proposição. $\square$

Em particular, todo grupo abeliano livre de posto finito n tem crescimento polinomial de grau n.

Note também que a Proposição 2.3.1 garante que para todo n natural existe um grupo de crescimento polinomial de grau n.

No exemplo 2 da seção 2.1 mostramos que se G é um grupo livre com geradores $\{a, b\}$ então $\gamma_S(m) = 2.3^m - 1$, ou seja, G tem crescimento exponencial. Mais geralmente, temos a

Proposição 2.3.2. *Seja $S = \{s_1, s_2, ..., s_n\}$ um conjunto minimal de geradores para um grupo livre não abeliano. Então*

$$\gamma_S(m) = \frac{n(2n-1)^m - 1}{n-1}.$$

Antes de provarmos a Proposição 2.3.2, provemos a seguinte

Afirmação: *Seja G um grupo livre não abeliano gerado por $S = \{s_1, ..., s_n\}$. Então G possui $2n(2n-1)^{m-1}$ elementos distintos de comprimento m em S para cada $m \in \mathbb{N}$.*

Demonstração. Provemos a afirmação por indução em m.

Como $\mathrm{Card}(S \cup S^{-1}) = 2n$, a afirmação é verdadeira para $m = 1$.

Suponhamos que G possua $2n(2n-1)^{m-2}$ elementos distintos de comprimento $m-1$ em S.

Fixado, arbitrariamente, um elemento de G de comprimento $m-1$ em S e operando-o com cada elemento de $S \cup S^{-1}$ obtemos $2n-1$ elementos distintos de G de comprimento m em S.

Aplicando este método a cada elemento de G de comprimento $m-1$ em S obtemos um total de $2n(2n-1)^{m-2}(2n-1) = 2n(2n-1)^{m-1}$ elementos distintos de G de comprimento m em S. $\square$

Agora, provemos a Proposição 2.3.2 por indução em m.

Demonstração. A proposição é óbvia para $m = 0$.

Suponhamos a proposição válida para $m - 1$ e seja $T = \{g \in G; l_S(g) = m\}$. Pela definição de função crescimento,

$$\gamma_S(m) = \gamma_S(m-1) + \mathrm{Card}(T)$$

Pela afirmação anterior, $\mathrm{Card}(T) = 2n(2n-1)^{m-1}$ e pela hipótese de indução,

$$\gamma_S(m) = \frac{n(2n-1)^{m-1} - 1}{n-1} + 2n(2n-1)^{m-1} = \frac{n(2n-1)^m - 1}{n-1}.$$

□

Capítulo 3

Crescimento de Grupos Solúveis

Como já foi dito, este capítulo é dedicado à prova dos Teoremas de Bass-Wolf e Milnor-Wolf.

Dedicamos a seção 3.1 ao Teorema de Bass-Wolf que garante o crescimento polinomial para todo grupo nilpotente finitamente gerado.

Faremos então, a prova do Teorema de Milnor que garante que todo grupo solúvel finitamente gerado que não é policíclico tem crescimento exponencial.

Na seção 3.2 omitiremos a prova do Teorema de Wolf, cujo ferramental envolvido não é tratado nestas notas.

3.1 Crescimento de Grupos Nilpotentes

Como já foi dito, esta seção é dedicada ao Teorema de Bass-Wolf, que segue como corolário de duas proposições.

A primeira proposição, devida a J. A. Wolf, foi demonstrada em [16] em 1968. Neste artigo, Wolf mostra que todo grupo nilpotente finitamente gerado tem a função crescimento limitada por dois polinômios de graus diferentes.

Mais tarde, em 1972, fixado um grupo nilpotente finitamente gerado, Bass constrói, em [1], dois polinômios de mesmo grau que limitam a função crescimento deste grupo; porém, a demonstração da cota superior ocupa cinco páginas no artigo origial, o que a torna demasiadamente pesada. Quase uma década mais tarde, em 1981, J. Tits publica em [15] e como apêndice em [4] uma prova indutiva para o Teorema de Bass-Wolf, utilizando, essencialmente, as mesmas idéias propostas em [1].

A demonstração da Proposição 3.1.1 segue as mesmas linhas de idéias dadas por Bass em [1], enquanto que a Proposição 3.1.2 segue a idéia proposta por J. Tits em [15].

Seja G um grupo nilpotente finitamente gerado, com série central infeiror $G = G_1 \supset G_2 \supset ... \supset G_{s+1} = \{1\}$.

Na Proposição 1.2.7 mostramos que se T_1 é um conjunto finito de G, cuja imagem, pelo homomorfismo canônico, gera G_1/G_2 e se definirmos indutivamente $T_{h+1} = \{[s,t]; s \in T_1, t \in T_i\}$, então T_h é um subconjunto finito de G_h cuja imagem gera G_h/G_{h+1}. Em particular, segue-se que T_1 gera G.

Para a próxima proposição e seu resultado precedente, fixemos tais subconjuntos.

Lema 3.1.1. *Sejam h, m e n inteiros tais que $h \geq 1$, $m > 0$ e $\mid n \mid \leq m^h$. Se $t \in T_h$ então existe um elemento $t^{(n)} \in G_h$ tal que $t^{(n)} \equiv t^n \operatorname{mod}(G_{h+1})$ e $\ell_{T_1}(t^{(n)}) \leq 8^{h-1}m$.*

Demonstração. Definindo $t^{(-n)} = (t^{(n)})^{-1}$ basta verificar o Lema para o caso $n \geq 0$.

Provemos o resultado por indução em h.

Se $h = 1$, tome $t^{(n)} = t^n$ e o Lema segue-se.

Suponha, então, a asserção verdadeira para $h > 1$.

Sejam $u \in T_{h+1}$ e $0 \leq n \leq m^{h+1}$.

Se $n < m$, tome $t^{(n)} = t^n$; do contrário, pelo algorítmo de Euclides, existem inteiros a, b tais que

$$n = am + b \text{ com } 0 \leq b < m$$

Como $am \leq am + b \leq m^{h+1}$, tem-se $a \leq m^h$.

Pela hipótese de indução, existe $t^{(a)} \in G_h$ tal que

$$t^{(a)} \equiv t^a \operatorname{mod}(G_{h+1}) \text{ e } \ell_{T_1}(t^{(a)}) \leq 8^{h-1}m.$$

Seja $u = [s,t]$ para algum $s \in T_1$ e algum $t \in T_h$.

Como $uG_{h+2} \in G_{h+1}/G_{h+2} \subset Z(G/G_{h+2})$ e s, t comutam com com u módulo G_{h+2} temos pelo Lema 1.2.1:

$$u^n = [s,t]^{am+b} = [s,t]^{am}[s,t]^b \equiv [s^m, t^{(a)}][s^b, t] \operatorname{mod}(G_{h+2})$$

Tomando $u^{(n)} = [s^m, t^{(a)}][s^b, t] \equiv u^n \operatorname{mod}(G_{h+2})$ tem-se

$$\ell_{T_1}(u^{(n)}) = 2m + 2\ell_{T_1}(t^{(a)}) + 2b + 2\ell_{T_1}(t) \leq 4m + 4.8^{h-1}m = 4(1+8^{h-1})m \leq 8^h m.$$

Concluindo o lema. $\square$

Proposição 3.1.1. *Seja G um grupo nilpotente, gerado por um conjunto finito S, com série central inferior*

$$G = G_1 \supset G_2 \supset ... \supset G_p \supset G_{p+1} = \{1\}$$

Então para todo $m \in \mathbb{N}$, $P(m) \leq \gamma_S(m)$ onde $P \in \mathbb{Z}[X]$ tem grau $\leq \displaystyle\sum_{h=1}^{p} hr_h$ e $r_h = r(G_h/G_{h+1})$.

Demonstração. Fixado $m > 0$, para cada $h \geq 1$ escolha elementos $t_{h_1}, ..., t_{h_{r_h}} \in T_h$ que sejam linearmente independentes módulo G_{h+1}.

Considere o conjunto

$$S_h = \{t_{h_1}^{q_1} ... t_{h_{r_h}}^{q_{r_h}}; \mid q_i \mid \leq m^h \text{ } para \text{ } 1 \leq i \leq r_h\}$$

Pela escolha dos t_i, para cada h, existem $(2m^h + 1)^{r_h}$ elementos distintos em S_h, sendo cada um deles de comprimento no máximo $r_h 8^{h-1} m$ em T_1, pelo Lema 3.1.1.

Afirmação: A aplicação "produto" $\psi : S_1 \times ... \times S_p \to G$ é injetiva.

Com efeito, basta notar que se $a, b \in S_1 \times ... \times S_p$ e $\psi(a) = a_1...a_p = b_1...b_p = \psi(b)$ então $b_1^{-1}a_1 = b_2...b_p a_p^{-1}...a_2^{-1} \in G_2$, visto que $b_i, a_i^{-1} \in G_2$ para todo $i \geq 2$. Assim, $b_1^{-1}a_1 \equiv 1 \operatorname{mod} G_2$, mas pela escolha dos t_i, obtém-se que $b_1^{-1}a_1 = 1$. Repetindo este argumento para $b_2^{-1}a_2, ..., b_p^{-1}a_p$ segue que $a = b$, concluindo a afirmação.

Portando a imagem de ψ possui $P(m) = \displaystyle\prod_{h=1}^{p}(2m^h + 1)^{r_h}$ elementos distintos de comprimento no máximo $(\displaystyle\sum_{h=1}^{p} 8^{h-1} r_h)m = cm$ em T_1 e portanto

$$P(m) \leq \gamma_{T_1}(cm) \leq \gamma_{T_1}(c)\gamma_{T_1}(m).$$

Note que P é um polinômio em $\mathbb{Z}[X]$ cujo termo principal é $2^e m^d$, onde $e = \sum_{h=1}^{p} r_h$ e $d = \sum_{h=1}^{p} hr_h$. $\square$

O próximo resultado, que seguirá as mesmas idéias propostas em [15], resultará na existência de um polinômio $Q \in \mathbb{R}[X]$ de grau $\leq d$ tal que $\gamma_S(m) \leq Q(m)$ e então concluir-se-á que todo grupo nilpotente finitamente gerado tem crescimento polinomial de grau $\leq d$, onde $d = \sum_{h=1}^{p} hr_h$.

(Note que d depende do grupo nilpotente finitamente gerado fixado.)

Para este fim, consideremos as seguintes definições.

Seja G um grupo nilpotente e seja $G = G_1 \supseteq G_2 \supseteq ... \supseteq G_k = \{1\}$ uma série central para G tal que $[G_i, G_j] \subset G_{i+j}$ (por exemplo, uma série central inferior).

Definição 3.1.1. Por um conjunto de f-geradores de G (relativo à cadeia de subgrupos $(G_i)_{1 \leq i \leq k}$), entendemos como um subconjunto de geradores E de G tal que $E_i = E \cap G_i$ gera G_i para todo i.

Definição 3.1.2. Seja $E'_i = E - E_{i+1}$. Definimos o f-comprimento de uma palavra, em elementos de $E \cup E^{-1}$, como uma sequência crescente $(n_1, n_2, ...)$ onde n_i é o número de contribuições de $E'_i \cup (E'_i)^{-1}$ para a palavra.

Definição 3.1.3. Dizemos que um elemento de G tem f-comprimento $\leq (r_1, r_2, ...)$, com $r_i \in \mathbb{R}_+$, se ele pode ser expresso como uma palavra de f-comprimento $(n_1, n_2, ...)$, com $n_i \leq r_i$.

Assumindo E finito, denotemos por ${}_f c(r_1, r_2, ...)$ o número de elementos em G de f-comprimento $\leq (r_1, r_2, ...)$.

Se ${}_f c'$ é uma função definida do mesmo modo como ${}_f c$, mas partindo de outro conjunto de f-geradores finito então existem constantes não nulas $a, b \in \mathbb{R}_+$ tais que ${}_f c(ar_1, ar_2, ...) \leq_f c'(r_1, r_2, ...) \leq_f c(br_1, br_2, ...)$ para toda sequência (r_i).

Definição 3.1.4. Dizemos que o grupo G tem f-crescimento polinomial de grau $\leq d$ se existe uma constante $c \in \mathbb{R}_+$ tal que, para todo $r \in \mathbb{R}_+$, tem-se

$${}_f c(r, r^2, r^3, ...) \leq cr^d + 1$$

Sejam G um grupo nilpotente finitamente gerado e

$$G = G_1 \supseteq G_2 \supseteq ... \supseteq G_p \supseteq G_{p+1} = \{1\}$$

uma série central de G tal que $[G_i, G_j] \subset G_{i+j}$.

Sejam $a = \max\{i; G_i = G\}$ e $m = min\{\text{Card}(S); G_a/G_{a+1} =< S >\}$.

($\star$) Seja E um conjunto de f-geradores de G satisfazendo as seguintes condições:

(i) $[x, y] \in E$, quaisquer que sejam $x, y \in E \cup E^{-1}$;

(ii) $\text{Card}(E'_a) = m$;

(iii) se $x \in E'_a$ tal que para algum $p \in \mathbb{N}$, $x^p \in G_{a+1}$ então para o menor natural n tal que $x^n \in G_{a+1}$ tem-se $x^n \in E_a$.

Observação 3.1.1. *Note que a existência de um tal conjunto de f-geradores depende do fato de G ser um grupo nilpotente.*

Tomemos, arbitrariamente, $y \in E'_a$ e denotemos por $G(y)$ o subgrupo de G gerado por $E_a - \{y\}$.

Pelas definições de E e E'_a, temos:

$$E = E_a \supset E_{a+1} \supset E_{a+2} \supset ... \supset E_p \supset E_{p+1} = \{1\}$$

$$E = E'_p \supset E'_{p-1} \supset ... \supset E'_{a+2} \supset E'_{a+1} \supset E'_a \supset E'_{a-1} = \{1\}$$

Lema 3.1.2. *Se w é uma palavra de f-comprimento $(n_1, n_2, ..., n_p)$ em $E \cup E^{-1}$ e se $(y_1, y_2, ..., y_p)$ é a contribuição de $\{y, y^{-1}\}$ para w (isto é, $y_i = y$ ou y^{-1} para todo i, e $p \leq n_a$) então para $0 \leq q \leq p$ existe uma palavra w_q representando o mesmo elemento w de G e com a mesma contribuição de $\{y, y^{-1}\}$ iniciando por $y_1 y_2 ... y_q$ e cujo f-comprimento $(n'_1, n'_2, ..., n'_p)$ satisfaz:*

$$n'_i \leq n_i + q n_{i-a} + \binom{q}{2} n_{i-2a} + ...$$

Demonstração. Provemos por indução em q.

A afirmação é óbvia para $q = 0$.

Suponhamos o lema válido para palavras cuja contribuição de $\{y, y^{-1}\}$ seja $q-1$ e seja w uma palavra cuja contribuição de $\{y, y^{-1}\}$ seja q. Pela hipótese de indução existe uma palavra w_{q-1} iniciando com $y_1 y_2 ... y_{q-1}$ e de f-comprimento $(n''_1, n''_2, ..., n''_p)$, representando w e satisfazendo:

$$n''_i \leq n_i + (q-1)n_{i-a} + \binom{q-1}{2} n_{i-2a} + ...$$

Considere uma ocorrência y_q de $\{y, y^{-1}\}$ em w_{q-1}, digamos

$$w_{q-1} = y_1 y_2 ... y_{q-1} s_j ... s_l y_q ... s_t$$

Temos $s_l y_q = y_q s_l [s_l^{-1}, y_q^{-1}]$. Como $[s_l^{-1}, y_q^{-1}] \in E_a$, por $(\star)$ (i), e $[s_l^{-1}, y_q^{-1}] \in G_{a+i}$, para algum i, segue que $[s_l^{-1}, y_q^{-1}] \in E_a \cap G_{a+i} = E_{a+i}$.

Substituindo $s_l y_q$ por $y_q s_l [s_l^{-1}, y_q^{-1}]$ em w_{q-1} não mudamos o número de contribuição de $\{y, y^{-1}\}$ para w_{q-1} e movemos y_q um passo à esquerda, ao custo de um termo extra $[s_l^{-1}, y_q^{-1}]$ (possivelmente a identidade). Assim, se $s_l^{-1} \in E_{i-a}$ então $[s_l^{-1}, y_q^{-1}] \in E_i$ e, eventualmente, dando uma contribuição de E'_i. Aplicando esta operação, tantas vezes quanto necessário, construímos uma nova palavra w_q iniciando por $y_1 y_2 ... y_q$ e de f-comprimento $(n'_1, n'_2, ..., n'_p)$ tal que $n'_i \leq n''_i + n''_{i-a}$ (tendo a igualdade quando $n''_{i-a} = 0$, isto é, quando w_q não tem contribuição de E'_{i-a}).

Assim,

$$n'_i \leq n_i + \binom{q-1}{1} n_{i-a} + \binom{q-1}{2} n_{i-2a} + ... + n_{i-a} + \binom{q-1}{1} n_{i-2a} + \binom{q-1}{2} n_{i-3a} + ...$$

$$n'_i \leq n_i + (\binom{q-1}{1} + 1) n_{i-a} + (\binom{q-1}{1} + \binom{q-1}{2}) n_{i-2a} + ...$$

Portanto,

$$n'_i \leq n_i + q n_{i-a} + \binom{q}{2} n_{i-2a} + ...$$

$\square$

Lema 3.1.3. *Seja $G(y) =< E_a - \{y\} >$. Então:*

(1) $G(y)$ é um subgrupo normal em G;

(2) $\overline{G}_a = G(y) \supset G_{a+1} \supset ... \supset G_{p+1} = \{1\}$ é uma série central para $G(y)$ e $[\overline{G}_a, G_j] \subset G_{a+j}$.

Demonstração. (1) Como $y \in E'_a$ e $\text{Card}(E'_a) = m$ segue-se que $yG(y) \neq G(y)$. Logo, $G(y)$ é um subgrupo próprio e maximal de G.

Sendo G nilpotente, segue-se pela Proposição 1.2.4 que $G(y) \lhd G$.

Para (2), note que, como $G_i/G_{i+1} \subset Z(G/G_{i+1})$ temos que, dado $xG_{i+1} \in G_i/G_{i+1}$, então xG_{i+1} comuta com todo elemento de G/G_{i+1}, em particular, comuta com os elementos de $G(y)/G_{i+1}$ e logo $xG_{i+1} \in Z(G(y)/G_{i+1})$, donde $G_i/G_{i+1} \subset Z(G(y)/G_{i+1})$.

Agora, $[\overline{G}_a, G_j] \subset [G_a, G_j] \subset G_{a+j}$. □

Em particular, o Lema 3.1.2 vale para a série de $G(y)$ dada em (2).

Proposição 3.1.2. *Sejam G um grupo nilpotente finitamente gerado e*

$$G = G_1 \supseteq G_2 \supseteq ... \supseteq G_p \supseteq G_{p+1} = \{1\}$$

uma série central para G tal que $[G_i, G_j] \subset G_{i+j}$. Se d_i denota o posto do grupo abeliano G_i/G_{i+1} então o grupo G tem f-crescimento polinomial de grau $\leq \sum_{i=1}^{p} id_i$.

Antes de demonstrarmos a Proposição 3.1.2 demonstremos o seguinte

Lema 3.1.4. *Seja $(a, m) \in \mathbb{N}^2$ tal que*

$$a = \max\{i; G_i = G\} \text{ e } m = \min\{\text{Card}(S); G_a/G_{a+1} =< S >\}.$$

Se a Proposição 3.1.2 é verdadeira para (a, m) então a Proposição 3.1.2 também é verdadeira para $(a - 1, m + 1) \in \mathbb{N}^2$, onde

$$a - 1 = \max\{i; G_i = G\} \text{ e } m + 1 = \min\{\text{Card}(S); G_{a-1}/G_a =< S >\}.$$

Demonstração. Seja $G \neq \{1\}$ um grupo nilpotente finitamente gerado tal que

$$a - 1 = \max\{i; G_i = G\} \text{ e } m + 1 = \min\{\text{Card}(S); G_a/G_{a+1} =< S >\}.$$

Sendo E_{a-1} um conjunto finito de f-geradores para G_{a-1} satisfazendo as condições em $(\star)$, seja $G(y) =< E_{a-1} - \{y\} >$ para algum $y \in E'_{a-1}$ escolhido aleatoriamente.

Pelo Lema 3.1.3, $G(y)$ é um subgrupo normal em G_{a-1} e

$$G(y) = H_a \supset H_{a+1} \supset ... \supset H_{p+2} = \{1\}$$

é uma série central para $G(y)$ tal que $[H_i, H_j] \subset H_{i+j}$, onde $G_i = H_{i+1}$, $\forall\ i \geq a$.

Como todo grupo abeliano finitamente gerado pode ser decomposto como a soma direta de grupos cíclicos, podemos escrever

$$G_{a-1}/G_a = G_{a-1}/G(y) \oplus G(y)/G_a \tag{3.1.1}$$

onde $G_{a-1}/G(y)$ é cíclico e $G(y)/G_a$ é abeliano finitamente gerado, e note que

$$r(G_{a-1}/G_a) = r(G_{a-1}/G(y)) + r(G(y)/G_a) \tag{3.1.2}$$

Assumindo $n_i \leq r^i$ (para algum $r \in \mathbb{R}_+$), tomando $q = p \leq r^{a-1}$, majorando $\binom{q}{j}$ por q^j $(\leq r^{(a-1)j})$ (no Lema 3.1.2) e denotando $e = \min\{i; G_i = \{1\}\}$, deduzimos do Lema 3.1.2 que:

(*) todo elemento $g \in G$ de f-comprimento $\leq (r, r^2, ...)$ pode ser escrito como $g = y^s g'$, onde $\mid s \mid \leq r^{a-1}$ e g' é um elemento de $G(y)$ e de f-comprimento

$$\leq (er - \mid s \mid, er^2 - \mid s \mid, ...).$$

Se $G/G(y)$ é infinito, segue de (3.1.1) que $d_{a-1} = 1 + k$, onde $k = r(G(y)/G_a) \leq m$.

Como $\min\{\text{Card}(S); G(y)/G_a =< S >\} = m$, temos por hipótese que a Proposição 3.1.2 vale para $G(y)$ o que implica na existência de uma constante $c' \in \mathbb{R}_+$ tal que o número de possíveis escolhas para g' é majorado por $c' r^{d-a+1} + 1$, onde $d = \displaystyle\sum_{i=a-1}^{p} i d_i$.

Como existem no máximo $2r^{a-1} + 1$ valores admissíveis para s, temos

$$_f c(r, r^2, r^3, ...) \leq (c' r^{d-a+1} + 1)(2r^{a-1} + 1)$$

donde G tem f-crescimento polinomial de grau $\leq \displaystyle\sum_{i=a-1}^{p} i d_i$.

Se $G/G(y)$ é finito, isto é, tem ordem $t < \infty$, segue-se de (3.1.2) que $r(G/G_a) = r(G(y)/G_a)$.

Novamente, pelo Lema 3.1.2, podemos reescrever $g \in G$ como $y^s g_1$, onde $0 \leq s < t$, $g_1 \in G(y)$ e o f-comprimento de g_1 é $\leq (er, er^2, ...)$. Por hipótese temos garantida a existência de uma constante $c'' \in \mathbb{R}_+$ tal que o número de possíveis escolhas para g_1 é majorado por $c'' r^d + 1$, onde $d = \displaystyle\sum_{i=a-1}^{p} i d_i$.

Como $r(G/G(y)) = 0$ e o número de possíveis valores assumidos por s é finito, o Lema está concluido.

□

Demonstração da Proposição 3.1.2:

Provaremos a proposição fazendo indução descendente sobre $a = \max\{i; G_i = G\}$.

Se $a = p+1$ então $G = \{1\}$ e o resultado segue-se para todo $m \in \mathbb{N}$.

Suponhamos a proposição verdadeira para todo grupo tal que $a = \max\{i; G_i = G\} < p+1$ e para todo $m \in \mathbb{N}$.

Seja G um grupo nilpotente finitamente gerado dentro das hipótese da proposição tal que $a-1 = \max\{i; G_i = G\}$.

Pela hipótese de indução, a proposição é verdadeira para todo grupo nilpotente finitamente gerado tal que $a = \max\{i; G_i = G\}$ e $m = 0$, logo pelo Lema 3.1.4 a proposição é verdadeira para G e $m = 1$.

Analogamente, a proposição é verdadeira para todo grupo nilpotente finitamente gerado tal que $a = \max\{i; G_i = G\}$ e $m = 1$, logo pelo Lema 3.1.4 a proposição é verdadeira para G e $m = 2$.

Pela hipótese de indução, a proposição é verdadeira para todo grupo tal que $a = \max\{i; G_i = G\}$ e tal que $m = \{\text{Card}(S); G_a/G_{a+1} =< S >\}$, logo pelo Lema 3.1.4 a Proposição é verdadeira para G e tal que $m+1 = \{\text{Card}(S); G_{a-1}/G_a =< S >\}$.

O caso $m = 0$ é trivial.

Portanto, a proposição é verdadeira para G e todo $m \in \mathbb{N}$.

□

Observação 3.1.2. *Seja G um grupo nilpotente com série central inferior*

$$G = G_1 \supset G_2 \supset ... \supset G_p \supset G_{p+1} = \{1\}$$

e gerado por um conjunto finito S.

Sejam $m \in \mathbb{N}$ e $T = \{g \in G; g \text{ } tem \text{ } f-comprimento \text{ } \leq (m, m^2, ..., m^p)\}$. Note que $\text{Card}\, T = {}_f c(m, m^2, ..., m^p)$.

Seja $w \in G$ tal que $\ell_S(w) = m$ então, é claro que $w \in T$ donde $\gamma_S(m) \leq {}_f c(m, m^2, ..., m^p)$ e portanto, pela Proposição 3.1.2, existe um polinômio $Q \in \mathbb{R}[X]$ de grau $\leq \sum_{i=1}^{p} id_i$, onde $d_i = r(G_i/G_{i+1})$, tal que $\gamma_S(m) \leq Q(m)$.

Como resultado imediato das Proposições 3.1.1 e 3.1.2 temos o *Teorema de Bass-Wolf:*

Teorema 3.1.1. *Seja G um grupo nilpotente finitamente gerado, com série central inferior*

$$G = G_1 \supset G_2 \supset ... \supset G_p \supset G_{p+1} = \{1\}$$

Se d_i denota o posto do grupo abeliano G_i/G_{i+1} e $d = \sum_{i=1}^{p} id_i$, então G tem crescimento polinomial de grau d.

□

Definição 3.1.5. Dada uma classe $\mathcal{P}$ de grupos, dizemos que um grupo G é virtualmente $\mathcal{P}$ se G possui um subgrupo H de índice finito em G tal que H é $\mathcal{P}$.

Em particular, um grupo é virtualmente nilpotente se ele tem um subgrupo nilpotente de índice finito.

Corolário 3.1.1. *Seja G um grupo finitamente gerado e virtualmente nilpotente. Então G tem crescimento polinomial.*

Demonstração. Seja H um subgrupo nilpotente e de índice finito em G. Pela Proposição 1.1.5 H é finitamente gerado e logo tem crescimento polinomial pelo Teorema de Bass-Wolf.

Portanto, pela Proposição 2.2.1, G tem crescimento polinomial. □

3.2 O Teorema de Milnor-Wolf

O próximo Teorema que enunciaremos como proposição, foi publicado pela primeira vez por Wolf em [16] em 1968. Wolf prova este resultado usando argumentos da Teoria de Grupos de Lie. Mais tarde, em 1972, Bass em [1] propõe uma prova mais algébrica para este resultado, porém utilizando profundos resultados da Teoria de Módulos.

Como observado na introdução deste capítulo, faremos a demonstração do Teorema de Milnor que foi publicado em 1968 em [9]. A demonstração que faremos segue a mesma linha de idéias apresentadas em [9].

Com base nestes dois resultados, chegaremos ao Teorema de Milnor-Wolf que caracteriza o tipo de crescimento para todo grupo solúvel finitamente gerado. E tem uma forte aplicação na demonstração da recíproca do Corolário 3.1.1, que foi demonstrado por Gromov em [4] em 1981.

A demonstração da próxima proposição pode ser encontrada em [1] ou [16].

Proposição 3.2.1. *(Wolf) Seja G grupo policíclico de crescimento não exponencial. Então G é virtualmente nilpotente. Em particular, G tem crescimento polinomial.*

□

Proposição 3.2.2. *(Milnor) Seja G um grupo solúvel, finitamente gerado e que não é policíclico. Então G tem crescimento exponencial.*

A prova será baseada na seguinte extensão de grupos:

$$1 \longrightarrow A \longrightarrow B \xrightarrow{\varphi} C \longrightarrow 1$$

onde A é abeliano e B é finitamente gerado.

Lema 3.2.1. *Se B não tem crescimento exponencial então para cada $\alpha \in A$ e $\beta \in B$, o subconjunto de todos conjugados $\beta^k \alpha \beta^{-k}$, com $k \in \mathbb{Z}$, geram um subgrupo finitamente gerado de A.*

Demonstração. Para cada $i_1, ..., i_m \in \{0, 1\}$ consideremos a expressão

$$\beta\alpha^{i_1}\beta\alpha^{i_2}...\beta\alpha^{i_m} \in B$$

Se estas 2^m expressões representam elementos distintos em B então a função crescimento γ_S de B, calculada usando um conjunto finito S de geradores para B que contém α e $\beta\alpha$, satisfaria $\gamma_S(m) \geq 2^m$, contradizendo a hipótese. Assim, deve existir uma relação não trivial da forma:

$$\beta\alpha^{i_1}\beta\alpha^{i_2}...\beta\alpha^{i_m} = \beta\alpha^{j_1}\beta\alpha^{j_2}...\beta\alpha^{j_m},$$

para algum $m \in \mathbb{N}$ e $i_1, ..., i_m, j_1, ..., j_m \in \{0, 1\}$.

Se denotarmos $\alpha_k = \beta^k \alpha \beta^{-k} \in A$, então

$$\beta\alpha^{i_1}\beta\alpha^{i_2}...\beta\alpha^{i_m} = \beta\alpha^{i_1}\beta^{-1}\beta^2\alpha^{i_2}...\beta^m\alpha^{i_m}\beta^{-m}\beta^m = \alpha_1^{i_1}\alpha_2^{i_2}...\alpha_m^{i_m}\beta^m$$

E daí,

$$\alpha_1^{i_1}\alpha_2^{i_2}...\alpha_m^{i_m}\beta^m = \alpha_1^{j_1}\alpha_2^{j_2}...\alpha_m^{j_m}\beta^m$$

Sem perda de generalidade, suponhamos $i_1 \neq j_1$ e $i_m \neq j_m$. Então,

$$\alpha_m^{i_m - j_m} = \alpha_{m-1}^{-i_{m-1}}...\alpha_1^{-i_1}\alpha_1^{j_1}...\alpha_{m-1}^{j_{m-1}}$$

donde $\alpha_m \in < \alpha_1, ..., \alpha_{m-1} >$, visto que $i_m - j_m \in \{-1, 1\}$.

Conjugando por β, temos $\alpha_{m+1} \in < \alpha_2, ..., \alpha_m > = < \alpha_1, ..., \alpha_{m-1} >$.

Indutivamente, vê-se que todo α_k com $k \geq m$ pode ser expresso como uma palavra em $\alpha_1 ... \alpha_{m-1}$.

Similarmente, todo α_k, com $k \leq 0$ pode ser expresso em termos de $\alpha_1 ... \alpha_{m-1}$. Completando a prova do lema. $\square$

Note que na demonstração do Lema 3.2.1 não precisamos do fato de A ser abeliano.

Lema 3.2.2. *Se o grupo quociente $C = B/A$ tem uma apresentação finita então existem finitos elementos $\alpha_1, ..., \alpha_l \in A$ tal que todo elemento de A pode ser expresso como um produto finito de conjugados dos α_j 's.*

Demonstração. Escolha geradores $\beta_1, ..., \beta_k$ para B e note que as imagens $\varphi(\beta_1), ..., \varphi(\beta_k)$ geram C (pois φ é sobrejetiva). Como C tem apresentação finita, este conjunto de geradores esta sujeito somente a um número finito de relações:

$$r_1(\varphi(\beta_1), ..., \varphi(\beta_k)) = r_2(\varphi(\beta_1), ..., \varphi(\beta_k)) = ... = r_l(\varphi(\beta_1), ..., \varphi(\beta_k)) = 1$$

Tomando $\alpha_j = r_j(\beta_1, ..., \beta_k)$, sejam $\beta_{i_1}, ..., \beta_{i_s}$, que não são equivalentes módulo A, tais que $\varphi(\beta_{i_{j_0}}) \notin < \varphi(\beta_{i_{j_1}}), ..., \varphi(\beta_{i_{j_0 - 1}}), \varphi(\beta_{i_{j_0 + 1}}), ..., \varphi(\beta_{i_{j_s}}) >$, $\forall\ i_{j_0} \in \{i_1, ..., i_s\}$.

Então $S = \{\beta_{i_1}, ..., \beta_{i_s}, \alpha_1, ..., \alpha_l\}$ é um conjunto de geradores para B.

Afirmação: Se $T = \{\beta\alpha_j\beta^{-1}; \beta \in B\}$ então $A = < T >$.

Com efeito, suponha que exista $a \in A$ tal que $a \notin < T >$, então escrevendo a em função dos elementos de S, deve existir um inteiro não nulo ϵ_t, tal que

$$a = \kappa_1^{\epsilon_1}...\kappa_n^{\epsilon_n}\alpha_1^{i_1}...\alpha_l^{i_l},$$

onde $\kappa_j \in S \setminus \{\alpha_1, ..., \alpha_l\}$ e $\epsilon_i \in \{-1, 0, 1\}$. Assim,

$$a \equiv \kappa_1^{\epsilon_1}...\kappa_n^{\epsilon_n} \operatorname{mod}(A)$$

donde $\kappa_1^{\epsilon_1}...\kappa_n^{\epsilon_n} \in A$ e logo, pela escolha dos κ_j, devemos ter $\epsilon_t = 0$ para todo t. O que contradiz o fato de $a \notin < T >$.

E portanto, a última afirmação completa a prova do Lema. $\square$

Lema 3.2.3. *Se C é policíclico e B não tem crescimento exponencial então B é policíclico.*

Demonstração. Escolha geradores $\gamma_1, ..., \gamma_p$ de C. Então todo elemento de C pode ser expresso como

$$\gamma_{j_1}^{i_1}...\gamma_{j_k}^{i_k}$$

onde $i_1, ..., i_k \in \mathbb{Z}$ e $j_1, ..., j_k \in \{1, ..., p\}$.

Escolha elementos $\beta_1, ..., \beta_p \in B$ tais que $\varphi(\beta_1) = \gamma_1, ..., \varphi(\beta_p) = \gamma_p$.

Como, pela Proposição 1.2.8, todo grupo policíclico tem uma apresentação finita, segue-se do Lema 3.2.2 que existem elementos $\alpha_1, ..., \alpha_l \in A$ tal que todo elemento de A pode ser expresso como um produto de conjugados de α_j. Cada conjugado de α_j pode ser escrito como

$$(\beta_1^{i_1}...\beta_p^{i_p})^{-1}\alpha_j(\beta_1^{i_1}...\beta_p^{i_p})$$

Seja A_0 o subgrupo de A gerado por $\alpha_1, ..., \alpha_l$. Aplicando o Lema 3.2.1 aos elementos α_j e β_1 temos a existência de um grupo A_1 finitamente gerado, gerado por todos conjugados da forma

$$\beta_1^{-i_1}\alpha_j\beta_1^{i_1}$$

com $1 \leq j \leq l$, $i \in \mathbb{Z}$.

Analogamente, aplicando o Lema 3.2.1 a cada gerador de A_1 e β_2 temos que

$$\beta_2^{-i_2}(\beta_1^{-i_1}\alpha_j\beta_1^{i_1})\beta_2^{i_2}$$

geram um grupo finitamente gerado A_2. Continuando, indutivamente, construímos a cadeia

$$A_0 \subseteq A_1 \subseteq ... \subseteq A_p$$

e segue-se que $A = A_p$ também é um grupo abeliano finitamente gerado, e logo pela Proposição 1.2.10 A é policíclico.

Como C é policíclico, segue-se, pela Proposição 1.2.9, que B é policíclico. $\square$

Demonstração da Proposição 3.2.2

Seja G um grupo solúvel, finitamente gerado e que não é policíclico, e seja

$$G = G^{(0)} \supset G^{(1)} \supset ... \supset G^{(s)} \supset G^{(s+1)} = \{1\}$$

sua série derivada.

Provemos a Proposição 3.2.2 por indução sobre s.

Se $s = 1$ então temos a seguinte sequência exata

$$\{1\} \longrightarrow G^{(1)} \longrightarrow G \xrightarrow{\varphi} G/G^{(1)} \longrightarrow \{1\}$$

onde φ é o homomorfismo canônico.

Sendo G finitamente gerado segue-se que $G/G^{(1)}$ é abeliano e finitamente gerado, e logo $G/G^{(1)}$ é policíclico pela Proposição 1.2.10.

Logo, se G não tem crescimento exponencial, então pelo Lema 3.2.3 teríamos que G é policíclico, o que é uma contradição. Portanto G tem crescimento exponencial.

Suponhamos a Proposição 3.2.2 verdadeira para todo grupo solúvel, finitamente gerado, que não é policíclico e cujo comprimento derivado seja $n > 1$.

Seja G um grupo solúvel, finitamente gerado, que não é policíclico e cujo comprimento derivado seja $n+1$, isto é, tal que $G^{(n+1)}$ seja abeliano. Então temos a seguinte sequência exata

$$\{1\} \longrightarrow G^{(n+1)} \longrightarrow G \xrightarrow{\varphi} G/G^{(n+1)} \longrightarrow \{1\}$$

sendo φ o homomorfismo canônico.

Se G não tem crescimento exponencial, então $G/G^{(n+1)}$ não tem crescimento exponencial. Logo, por hipótese de indução, $G/G^{(n+1)}$ é policíclico e daí, pelo Lema 3.2.3, G é policíclico. Esta contradição demonstra a Proposição 3.2.2.

$\square$

Pelas Proposições 3.2.1 e 3.2.2 obtemos o *Teorema de Milnor-Wolf:*

Teorema 3.2.1. *Seja G um grupo solúvel finitamente gerado e de crescimento não exponencial. Então G é virtualmente nilpotente.*

□

O Teorema de Milnor-Wolf caracteriza os grupos solúveis finitamente gerados que tem crescimento exponencial; um grupo solúvel finitamente gerado tem crescimento exponencial se, e somente se, não é virtualmente nilpotente.

Capítulo 4

APÊNDICE - O Teorema de Gromov

Gromov mostra em [4] que a todo grupo infinito finitamente gerado de crescimento polinomial está associado um espaço métrico Y satisfazendo certas propriedades.

Como foi dito na introdução, admitiremos a existência do espaço Y e provaremos o Teorema de Gromov.

Definição. Dizemos que um grupo G finitamente gerado tem crescimento aproximadamente polinomial de grau $\leq d$ se existe $c > 0$ tal que $\gamma_S(n) \leq cn^d$ para infinitos n.

Esta definição não depende do conjunto finito S de geradores de G.

De fato, seja T outro conjunto de geradores para G, então se $b = \max\{\ell_S(g); g \in T\}$ temos $\gamma_T(n) \leq \gamma_S(bn)$ e, trocando as posições de S e T temos uma desigualdade semelhante. Donde γ_T e γ_S são equivalentes.

Lema 1. *Seja G um grupo finitamente gerado cujo crescimento é não exponencial. Suponha que existe uma sequência exata*

$$\{1\} \longrightarrow K \longrightarrow G \xrightarrow{h} \mathbb{Z} \longrightarrow \{0\}.$$

Então K é finitamente gerado.

Além disso,

(i) Se G tem crescimento aproximadamente polinomial de grau $\leq d+1$ então K tem crescimento aproximadamente polinomial de grau $\leq d$;

(ii) Se K é virtualmente solúvel então G também o é.

Demonstração. Seja $\alpha \in G$ tal que $h(\alpha) = 1$ e como $\mathbb{Z} \backsimeq G/K$ escolha $e_1, ..., e_k \in K$ tais que $G =< \alpha, e_1, ..., e_k >$. Defina $\alpha_{m,i} = \alpha^m e_i \alpha^{-m}$ para $m \in \mathbb{Z}$, $i = 1, ..., k$.

Afirmação: $K =< \alpha_{0,i}, ..., \alpha_{m-1,i} >$.

Com efeito, fixemos $i \in \{1, ..., k\}$.

Para $m > 0$ consideremos os elementos de G da forma $\alpha_{0,i}^{\epsilon_0} ... \alpha_{m,i}^{\epsilon_m}$, $\epsilon_i = 0$ ou 1. Existem 2^{m+1} palavras em $\{\alpha, e_1, ..., e_k\}$, cada qual de comprimento $\leq 2^m$. O fato de G não ter crescimento exponencial implica que, para algum $m > 0$, duas destas palavras representam o mesmo elemento, digamos $\alpha_{0,i}^{\epsilon_0} ... \alpha_{m,i}^{\epsilon_m} = \alpha_{0,i}^{\delta_0} ... \alpha_{m,i}^{\delta_m}$ e $\epsilon_m \neq \delta_m$. Então $\alpha_{m,i} \in< \alpha_{0,i}, ..., \alpha_{m-1,i} >$ e, indutivamente, obtemos que

$$\alpha_{p,i} \in< \alpha_{0,i}, ..., \alpha_{m-1,i} > \text{ para todo } p \geq 0.$$

Um argumento similar para m negativo garante que K é gerado por um conjunto finito

$$\{\alpha_{m,i}; 1 \leq i \leq k, \mid m \mid \leq M\},\ M \in \mathbb{N}.$$

Concluindo a afirmação.

Para provar (i), seja $c > 0$ e $X \subset \mathbb{N}$ infinito, tal que $\gamma_S(n) \leq cn^{d+1}$ para todo $n \in X$, onde S é um conjunto finito de geradores para G.

Sem perda de generalidade, suponhamos $S = Y \cup \{\alpha\}$, onde $K =< Y >$.

Sejam $x \in \mathbb{R} \mapsto [x] \in \mathbb{Z}$ a função menor inteiro, $n \in X$ e g_i $i = 1, ..., \gamma_Y([n/2])$, elementos distintos em K de comprimento $\leq [n/2]$ em Y. Então os $n\gamma_Y([n/2])$ elementos $g_i\alpha^j$, $i = 1, ..., \gamma_Y([n/2])$ e $-[n/2] \leq j \leq [n/2]$ são distintos e de comprimento $\leq n$ em S.

Assim, $n\gamma_Y([n/2]) \leq \gamma_S(n) \leq cn^{d+1}$, donde $\gamma_Y([n/2]) \leq cn^d \leq c'[n/2]^d$ para alguma constante $c' > 0$, independente de $n \in X$. Concluindo (i).

Para (ii), suponhamos que K possua um subgrupo H solúvel e de índice finito m.

Afirmação: *Tomando a interseção de todos os subgrupos de K que têm índice m em K, obtemos um subgrupo K_1 solúvel e de índice finito em K.*

Com efeito, como K é finitamente gerado, K possui um número finito de subgrupos de índice m, pela Proposição (1.1.4). Logo, pela Proposição (1.1.2), a interseção de todos estes subgrupos, K_1, tem índice finito em K. E, finalmente, K_1 é solúvel pois é subgrupo de um grupo solúvel, provando a afirmação.

Seja $\Gamma =< K_1, \alpha >$. Temos $\ker(h \restriction \Gamma) = K_1$ pois $K_1 \subset K = \ker(h)$.

Daí, $\Gamma/K_1 = \{K_1, \alpha K_1\}$, donde $(\Gamma : K_1) = 2$.

Como $K\Gamma =< K, \Gamma >= G$ segue-se que $K\Gamma/K = \{K, \alpha K\}$, donde $(G : K) = 2$.

Sendo $(G : K)(K : K_1) = (G : \Gamma)(\Gamma : K_1)$ temos $(G : \Gamma) = (K : K_1)$ é finito.

Sendo K_1 solúvel e $\{1\} \longrightarrow K_1 \longrightarrow \Gamma \xrightarrow{h} \mathbb{Z} \longrightarrow \{0\}$ é exata, segue-se que $\Gamma/K_1 \backsimeq \mathbb{Z}$ é solúvel, donde Γ é solúvel pelo Teorema (1.2.1). $\square$

Definição. Dado um espaço métrico Y com métrica d e um ponto arbitrário e_0. Seja $Isom(Y)$ o grupo de isometrias de Y.

Considere

$$\mathcal{F} = (U_{k,\epsilon})_{k \in \mathbb{N}^*, \epsilon > 0}$$

onde

$$U_{k,\epsilon} = \{\sigma \in Isom(Y); d(\sigma y, y) \leq \epsilon \ para\ todo\ y\ com\ d(y, e_0) \leq k\}.$$

Mostra-se que $\mathcal{F}$ é base de vizinhanças da identidade id_Y e logo, $Isom(Y)$ é um grupo topológico.

De acordo com Gromov, em [4], para cada grupo G infinito e finitamente gerado, pode-se associar um espaço métrico $Y = Y(G)$ e um homomorfismo

$$\varphi : G \longrightarrow Isom(Y)$$

com as seguintes propriedades:

(i) Y é homogêneo (dados $a, b \in Y$, existe $g \in Isom(Y)$ tal que $g(a) = b$);

(ii) Y é conexo e localmente conexo;

(iii) Y é completo;

(iv) Se $\varphi(G)$ é finito e G não é virtualmente abeliano então $\ker(\varphi)$ tem, para cada vizinhança U de id_Y, uma imagem homomórfica em $Isom(Y)$ intersectando $U \setminus \{1_Y\}$;

(v) Se G tem crescimento aproximadamente polinomial, então Y é localmente compacto e tem dimensão de Hausdorff finita;

(vi) Se G tem crescimento exponencial então Y não é localmente compacto.

Daqui em diante, simplesmente assumiremos (i)- (vi) e demonstraremos o Teorema de Gromov.

Para isto, enunciamos o seguinte teorema cuja demonstração pode ser encontrada em [17].

Teorema 1. *Suponhamos $Y = Y(G)$ localmente compacto, com dimensão de Hausdorff finita e G infinito. Então G tem um subgrupo de índice finito que tem $\mathbb{Z}$ como imagem homomórfica.*

□

Teorema de Gromov. Seja G um grupo finitamente gerado, de crescimento aproximadamente polinomial de grau $\leq d$. Então G é virtualmente nilpotente.

Demonstração. Faremos indução em d.

Se $d = 0$ então G é finito e logo, virtualmente nilpotente.

Suponha que G seja infinito, de crescimento aproximadamente polinomial de grau $\leq d + 1$ e que o Teorema seja verdadeiro para grupos infintos de crescimento aproximadamente polinomial de grau $\leq d$.

Pela propriedade (v) de Y e pelo Teorema 1, existe um homomorfismo sobrejetor $h : G \longrightarrow \mathbb{Z}$. Seja $K = \ker(h)$. Pela parte (i) do Lema 1, K é finitamente gerado e tem crescimento aproximadamente polinomial de grau $\leq d$.

Pela hipótese de indução K é virtualmente nilpotente e, consequentemente, virtualmente solúvel então, pela parte (ii) do Lema 1, G possui um subgrupo H solúvel e de índice finito em G. Pelo Teorema (3.2.1) H possui um subgrupo H_1 nilpotente e de índice finito em H.

Assim, $(G : H_1) = (G : H)(H : H_1)$ é finito. Donde G é virtualmente nilpotente. Completanto a prova do Teorema. □

Com o Teorema de Gromov e o Corolário 3.1.1 obtemos o seguinte resultado, que caracteriza os grupos que tem crescimento polinomial,

Teorema 2. *Seja G um grupo finitamente gerado. Para que G tenha crescimento polinomial é necessário e suficiente que G seja virtualmente nilpotente.*

□

Referências Bibliográficas

[1] H. Bass, The Degree of Polynomial Growth of Finitely Generated Nilpotent Groups, *Proc. London Math. Soc.* **25** (1972), 603–614.

[2] H. Bechtell, *Theory of Groups*, Addison–Wesley Series in Mathematics, 1971.

[3] R. I. Grigorchuk, On Milnor's Problem of Group Growth, *Amer. Math. Soc.* **28** (1983), 23–26.

[4] M. Gromov, Groups of Polynomial Growth and Expanding Maps, *Publ. Math. IHES* **53** (1981), 53–78.

[5] D. L. Johnson, Growth of Groups, *The Arabian Journal for Science and Engineering*, **25–2C** (2000), 53–68.

[6] A. G. Kurosh, *Theory of Groups*, Vol. II, translated by K. A. Hirsch, Chelsea, New York, 1956.

[7] J. Milnor, A Note on Curvature and Fundamental Group, *J. Differential Geometry* **2** (1968), 1–7.

[8] J. Milnor, 'Problem 5603', *Amer. Math. Monthly* **75** (1968), 685–686.

[9] J. Milnor, Growth of Finitely Generated Solvable Groups, *J. Differential Geometry* **2** (1968), 447–449.

[10] D. J. S. Robinson, *A Course in the Theory of Groups*, 2th ed., Springer-Verlag, New York, 1995.

[11] S. Rosset, A Property of Groups of Nonexponential Growth, *Amer. Math. Soc.* **54** (1976), 24–26.

[12] Rotman, *Theory of Groups*, 4th ed., Springer-Verlag, New York, 1994.

[13] D. Segal, *Polycyclic Groups*, Cambridge University Press, New York, 1983.

[14] J. Tits, Free Subgroups in Linear Groups, *J. Algebra.* **20** (1972), 250–270.

[15] J. Tits, Groupes à Croissance Polynomiale, *Séminaire Bourbaki, 33e anneé 1980/1981,* ***572****; Lectures Notes in Math.* **901**, 176–188, Springer-Verlag, Berlin/New York/Heidelberg, 1981.

[16] J. A. Wolf, Growth of Finitely Generated Solvable Groups and Curvature of Riemannian Manifolds, *J. Differential Geometry* **2** (1968), 421–446.

[17] L. van den Dries and A. J. Wilkie, Gromov's Theorem on Groups of Polynomial Growth and Elementary Logic, *J. Algebra*, **89** (1984), 349–374.