Universidade de Brasília

Larguras em grupos e álgebras de Lie

Ayrton Anjos Teixeira

Orientador: Dr. Raimundo de Araújo Bastos Júnior

Departamento de Matemática
Universidade de Brasília

Dissertação apresentada como requisito parcial para obtenção do grau de
Mestre em Matemática

Brasília, 27 de Maio de 2023

Agradecimentos

À minha família, em especial aos meus pais, Nilde e Sérgio, por todo amor e apoio que possibilitaram que eu seguisse meus estudos.

À minha namorada Bheatriz, por acreditar em mim e pelo carinho em todos esses anos.

Aos amigos e colegas, pela boa companhia e bons momentos.

Ao meu orientador, professor Raimundo, pela dedicação e paciência desde que eu estava na graduação.

Aos professores Theo Zapata e Danilo Sanção por terem aceitado participar da banca e pelas valiosas sugestões e correções.

Ao professor Csaba Schneider pelas recomendações e comentários sobre álgebras de Lie.

Ao CNPq pelo apoio financeiro.

Resumo

O objetivo desse trabalho é investigar certas questões sobre finitude em grupos e álgebras de Lie. Mais precisamente, o Problema de Burnside, cotas para a largura de um grupo e condições de finitude para a subálgebra derivada de uma álgebra de Lie.

Abstract

The aim of this work is to investigate certain questions about finiteness in groups and Lie algebras. More precisely, the Burnside Problem, bounds for the commutator lenght of a group and finiteness conditions for the derived subalgebra of a Lie algebra.

Conteúdo

Introdução

Em geral, dado um grupo G, o conjunto $\Gamma(G)$ dos comutadores $[x,y] = x^{-1}y^{-1}xy$ não coincide com seu subgrupo derivado G', nesse contexto, definimos a largura $\lambda(G)$ como o menor inteiro n, caso exista, tal que todo elemento no subgrupo derivado é um produto de n comutadores. Esse conceito, além de interessante por si só, pode ser uma ferramenta importante na resolução de alguns problemas de finitude.

O Teorema de Schur afirma que, se um grupo é central-por-finito, então seu subgrupo derivado é finito. Uma ideia geral de demonstração desse resultado consiste em provar que tais grupo tem finitos comutadores e largura finita. Porém, nesse caso, se quisermos cotas mais finas para a ordem do subgrupo derivado precisaremos de cotas mais finas para $|\Gamma(G)|$ e $\lambda(G)$.

Tendo isso como motivação, é interessante tentarmos limitar $\lambda(G)$ nesse caso. M. Rosenlitch [21] forneceu uma cota utilizando somente técnicas elementares de Teoria de Grupos e argumentos combinatórios, tal cota, porém, não é muito realista. Por outro lado, R. M. Guralnick [8] forneceu uma cota bem fina para $\lambda(G)$ utilizando técnicas de representações e caracteres complexos. A saber, R. M. Guralnick forneceu uma conexão entre $\lambda(G)$ e a quantidade de graus distintos de caracteres irredutíveis de G, provando o seguinte resultado

Teorema (Guralnick, 1979)**.** Seja G um grupo com $[G : Z(G)] = n$, então $\lambda(G) \leq 3\rho(n)/2$.

Onde a função ρ conta os divisores primos de n com multiplicidade, isto é, $\rho(p_1^{\alpha_1} \cdots p_n^{\alpha_n}) = \alpha_1 + \cdots + \alpha_n$.

A largura de um grupo também aparece na teoria dos grupos profinitos. Não iremos nos aprofundar no tema, mas podemos citar o seguinte resultado do matemático D. Segal (cf. [23])

Teorema (Segal, 1999)**.** Em um grupo prosolúvel finitamente gerado, todo subgrupo de índice finito é aberto.

No caso, D. Segal utilizou que a largura $\lambda(G)$ de um grupo solúvel d-gerado é, no máximo, $72d^2 + 46d$.

Além disso, podemos citar o trabalho de D. Calegari (cf. [2]) para uma visão mais geométrica envolvendo largura de grupos.

O conceito de largura, de uma forma mais geral, também figura de forma importante no Problema de Burnside. Tal problema consiste em provar que um grupo, finitamente gerado e de expoente finito, é finito. Apenas alguns casos particulares desse problema que admitem resposta positiva são conhecidos, no caso, quando o expoente é $2,3,4$ ou 6. No entanto, todos eles podem ser resolvidos ao se limitar uma certa largura. Além disso, é interessante tentar encontrar cotas ótimas para a ordem do grupo, para tanto, quando o expoente for 3, utilizaremos os chamados métodos de Lie para provar que

Teorema (Levi-Van der Waerden, 1933)**.** Se G é um grupo r-gerado de expoente 3, então G é nilpotente de classe no máximo 3 e

$$|G| \leq 3^{r+\binom{r}{2}+\binom{r}{3}}.$$

A cota apresentada nesse resultado é ótima, para efeito de comparação, se o expoente for 4 não há cota ótima conhecida.

As álgebras de Lie são estruturas que, em alguns casos, possuem propriedades similares aos grupos. Tendo isso mente, também apresentaremos análogos para álgebras de Lie de alguns resultados famosos de finitude em grupos.

Em linhas gerais, a divisão do trabalho é feita da seguinte forma:

Capítulo 1: Apresentaremos os resultados que serão necessários para o desenvolvimento do texto, em particular, discutiremos o Homomorfismo Transfer, o Teorema do subgrupo focal de Higman e algumas propriedades de grupos nilpotentes finitamente gerados. Também apresentaremos a definição e algumas propriedades das álgebras de Lie, em especial, demostraremos o Teorema de Kostrikin para $p = 3$.

Capítulo 2: Apresentaremos alguns teoremas famosos da teoria de grupos e seus análogos para álgebras de Lie. Em particular, discutiremos o conceito de largura de uma álgebra de Lie e condições de finitude para a álgebra derivada assumindo uma hipótese análoga à definição de BFC-grupo. Por fim, baseado em um exemplo dado por P. J. Cassidy em [3] construiremos uma álgebra de Lie de largura infinita.

Capítulo 3: Discutiremos os casos do Problema de Burnside que possuem resposta positiva, a saber, quando o expoente é 2, 3, 4 ou 6. Além disso, discutiremos algumas aplicações das álgebras de Lie para obtenção de uma cota ótima para a ordem de grupos finitamente gerados de expoente 3.

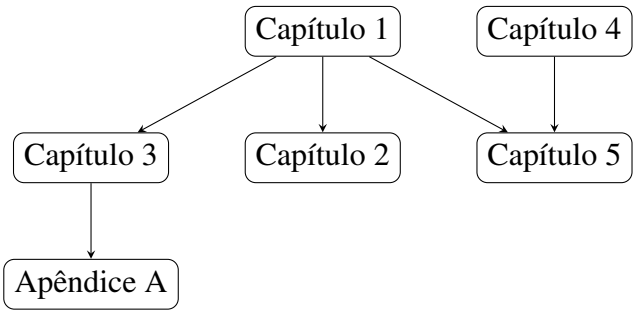
Capítulo 4: Faremos uma breve introdução à teoria das representações e caracteres complexos. Tal teoria fornecerá uma ferramenta extremamente importante para o desenvolvimento dos resultados do Capítulo 4.

Capítulo 5: Discutiremos os resultados do artigo [8] de R. M. Guralnick. O foco principal é obter cotas para a largura de um grupo satisfazendo certas hipóteses, como ter o índice do centro finito. Por fim, apresentaremos uma aplicação dos resultados no problema de encontrar um p-grupo G de menor ordem com largura 3, mais precisamente, mostraremos que é suficiente procurar entre os de ordem p^9 e p^{14} e que os índices $[G : Z(G)]$ e $[G : G']$ precisam ser maiores ou iguais a p^6 e p^3 respectivamente.

Apêndice A: Faremos alguns cálculos no software livre GAP que são necessários para uma das demonstrações do Capítulo 2.

Por fim, para a realização dessa dissertação os trabalhos dos seguintes matemáticos foram essenciais: R. M. Guralnick [8] cujos resultados foram o objeto de estudo principal; P. J. Cassidy [3], I. D. Macdonald [17], M. Rosenlitch [21] e J. Wiegold [29] pelos seus estudos sobre comutadores e largura em grupos; K. Erdmann, J. M. Wildon [4] e J. E. Humphreys [10] pelos seus livros sobre álgebras de Lie; I. M. Isaacs [11], G. James, M. Liebeck [14] pelos seus livros sobre representações e caracteres; M. Vaughan-Lee [27] por seu livro sobre o Problema de Burnside; por fim, os matemáticos do *The GAP Group* [26] pelo desenvolvimento do software GAP.

O seguinte diagrama mostra a dependência dos capítulos.



Capítulo 1

Preliminares

Começaremos apresentando definições e resultados que serão usados ao longo do texto, no entanto, a teoria básica relativa a grupos e espaços vetoriais, salvo exceções, será admitida e usada livremente.

1.1 Comutadores e o Teorema de Schur

Seja G um grupo, dados $x, y \in G$ definimos o *comutador* de x, y como o elemento $[x,y] = x^{-1}y^{-1}xy$, além disso, definimos $\Gamma(G)$ como o conjunto dos comutadores de G.

Já o subgrupo gerado por $\Gamma(G)$ é chamado de *subgrupo derivado* e denotado por G'. É conhecido que, em geral, $\Gamma(G) \neq G'$ (cf. [7]). Nesse contexto, faz sentido definir a largura de G, denotada por $\lambda(G)$, como o menor inteiro (caso exista) tal que todo elemento de G' pode ser escrito como um produto de $\lambda(G)$ comutadores. Se não existe um inteiro com essa propriedade, então dizemos que G tem largura infinita e escrevemos $\lambda(G) = \infty$ (cf. [3] para um exemplo).

A largura de um grupo é uma definição interessante por si própria, porém uma justificativa da sua importância pode ser a seguinte: suponha que um grupo G satisfaz $\lambda(G) = l$ e $|\Gamma(G)| = n$, então, por um argumento de contagem, temos que $|G'| \leq n^l$.

Nesse contexto, uma classe de grupos que se destaca é a dos grupos *centrais-por-finito*, i.e, grupos em que o índice do centro $[G : Z(G)]$ é finito. O próximo resultado dá uma justifica dessa importância.

Proposição 1.1. Se G é um grupo com $[G : Z(G)] = n$, então $|\Gamma(G)| \leq n^2$

Demonstração. Por hipótese $G/Z(G) = \{x_1Z(G), x_2Z(G), \ldots, x_nZ(G)\}$, assim, todo $g \in G$ é escrito como x_iz, onde $1 \leq i \leq n$ e $z \in Z(G)$. Tomando $g, h \in G$ e escrevendo esses elementos

como acima obtemos

$$[g,h] = [x_i z_1, x_j z_2] = [x_i, x_j].$$

Onde usamos que, por definição, os elementos do centro comutam com qualquer elemento de G. Assim, mostramos que todo comutador é da forma $[x_i, x_j]$, por um argumento de contagem vemos que existem, no máximo, n^2 desses elementos. □

Ou seja, grupos centrais-por-finito possuem finitos comutadores, portanto para garantir a finitude de G' bastaria garantir a finitude da largura. Felizmente, isso também acontece, como veremos mais adiante.

Por agora, consideraremos algumas identidades envolvendo comutadores.

Proposição 1.2. ([19, 5.1.5]) Se x, y, z são elementos do grupo G, então as seguintes identidades são válidas:

1. $[x,y]^{-1} = [y,x]$.
2. $[x,y]^z = [x^z, y^z]$.
3. $[xy,z] = [x,z]^y [y,z]$.
4. $[x,yz] = [x,z][x,y]^z$.
5. $[x^{-1},y]^x = [y,x]$.
6. $[x,y^{-1},z]^y [y,z^{-1},x]^z [z,x^{-1},y]^x = 1$. (Identidade de Witt)

O Teorema de Schur assegura a finitude do subgrupo derivado de grupos centrais-por-finito. Uma possibilidade, visto que tais grupos possuem finitos comutadores, é garantir a finitude da largura. Uma prova elementar deste último fato foi dada por M. Rosenlicht e se utiliza dos seguintes lemas.

Lema 1.3. Se G é um grupo com $[G : Z(G)] = n$, então $[x,y]^{n+1} = [x,y^2][x^y,y]^{n-1}$ para quaisquer $x, y \in G$.

Demonstração. Por hipótese temos que $[x,y]^n \in Z(G)$, logo

$$\begin{aligned}
[x,y]^{n+1} &= [x,y]^n [x,y] \\
&= x^{-1}y^{-1}x[x,y]^n y \\
&= x^{-1}y^{-1}x[x,y][x,y]^{n-1} y \\
&= x^{-1}y^{-1}xx^{-1}y^{-1}xy[x,y]^{n-1} y \\
&= x^{-1}y^{-2}xy^2y^{-1}[x,y]^{n-1} y \\
&= [x,y^2][x^y,y]^{n-1}.
\end{aligned}$$

□

Note que esse resultado nos dá algum controle sobre a largura de um grupo central-por-finito pois escrevemos um produto de $n+1$ comutadores como um produto de n comutadores.

Além disso, o lema seguinte nos permitirá escrever um produto de comutadores de uma forma conveniente, pois poderemos juntar os comutadores iguais sem alterar a quantidade de comutadores envolvidos no produto.

Lema 1.4. Sejam x, y elementos de G, então

$$xyx = x^2y^x.$$

Demonstração. Basta ver que $xyx = x(xx^{-1})yx = x^2y^x$. □

Assim, podemos escrever, por exemplo

$$[x,y][g,h][x,y] = [x,y]^2[g^{[x,y]}, h^{[x,y]}]$$

Proposição 1.5. Seja G um grupo. Se $[G : Z(G)]$ é finito, então $\lambda(G) \leq n^3$.

Demonstração. Suponha, por absurdo, que $\lambda(G) > n^3 + 1$, assim, existe $g \in G'$ tal que g é o produto de $n^3 + 1$ comutadores e não menos que isso, logo podemos escrever

$$g = c_1 c_2 \cdots c_{n^3+1},$$

onde cada c_i é um comutador.

Note que pela Proposição 1.1 existem, no máximo n^2 comutadores. Se todos ocorressem, no máximo, n vezes, então g seria escrito como n^3 comutadores, absurdo. Existe então um comutador, $c_k = [x,y]$, que aparece $n+1$ vezes na expressão de g, daí os lemas anteriores garantem que

$$g = [x,y]^{n+1} d_1 d_2 \cdots d_{(n^3-(n+1))} = [x,y^2][x^y,y]^{n-1} d_1 d_2 \cdots d_{(n^3-(n+1))},$$

onde cada d_j é também um comutador, por ser o conjugado de algum c_i. Dessa forma escrevemos g como um produto de n^3 comutadores, absurdo. □

Observação 1. A demonstração usa, de forma implícita, o *Princípio da Casa de Pombos* para garantir que entre $n^3 + 1$ comutadores existe um deles que aparece pelo menos $n+1$ vezes, já que só existem n^2 comutadores.

Agora o Teorema de Schur segue de forma direta dos resultados vistos.

Teorema 1.6. (Teorema de Schur) Seja G um grupo. Se $[G : Z(G)] = n$, então G' é finito.

Demonstração. Como vimos $|\Gamma(G)| \leq n^2$ e $\lambda(G) \leq n^3$, portanto $|G'| \leq n^{2n^3}$. □

Essa demonstração somente argumentos combinatórios e argumento básicos de comutadores, porém não oferece uma cota muito realista, veremos no Capítulo 5 como o matemático R. M. Guralnick obteve uma cota mais fina utilizando técnicas de Representações e Caracteres complexos.

Uma outra classe de grupos que se destaca é dos grupos simples não-abelianos, nesse caso, todos esses grupos têm largura 1. Tal fato foi conjecturado por O. Ore em 1951 e provado somente em 2010 pelos matemáticos M. W. Liebeck, E. A. O'Brien, A. Shalev, P. H. Tiep (cf. [16]). Hoje esse resultado é conhecido como L.O.S.T Theorem e é considerado seminal na Teoria de Grupos, em particular, na teoria dos grupos simples.

Vale comentar que até ordem 95 todos os grupos possuem largura 1 (cf. [7, Theorem 1]) e que existem dois grupos de ordem 96 com largura 2 (cf, [7]), ou seja, esses grupos são exemplos minimais de largura 2. Não é conhecido um exemplo minimal de largura 3, mas sabe-se, por exemplo, que tal exemplo precisa ter ordem maior que 1000 (cf. [15, Lemma 6.1]).

1.2 O Homomorfismo Transfer

O Homomorfismo Transfer é, grosso modo, uma forma de estendermos homomorfismos definidos em subgrupos "grandes" para o grupo todo. Para uma referência veja [19, Chapter 10.1] e para uma ideia da versatilidade do Transfer veja [24, Pages 120-122].

Definição 1.7. Sejam H um subgrupo de um grupo G com $[G : H] = n$, A um grupo abeliano e $\theta : H \to A$ um homomorfismo de grupos. Consideramos um transversal $\tau = \{t_1, t_2, \ldots, t_n\}$ de H em G, ou seja,

$$G = \dot{\bigcup_{i=1,\ldots,n}} Ht_i.$$

E dado qualquer elemento $x \in G$: existe um único par $(t_j, h) \in \tau \times H$ tal que $x = t_j h$. Agora, consideramos a seguinte ação nas classes laterais: $Ht_i x := Ht_{(i)x}$, assim $t_i x t_{(i)x}^{-1} \in H$. Definamos a seguinte aplicação:

$$\begin{array}{rccc} \theta^* : & G & \longrightarrow & A \\ & x & \longmapsto & \prod_{i=1}^{n} (t_i x t_{(i)x}^{-1})^{\theta} \end{array}$$

Proposição 1.8. ([19, 10.1.1]) Sejam H um subgrupo próprio de um grupo G com $|G:H|=n$, A um grupo abeliano e $\theta: H \to A$ um homomorfismo de grupos. Consideramos um transversal $\tau = \{t_1, t_2, \ldots, t_n\}$ de H em G. Então

(a) θ^* é um homomorfismo de grupos;

(b) O homomorfismo θ^* independe da escolha do transversal τ de H em G.

Proposição 1.9. ([19, 10.1.2]) Sejam A um grupo abeliano e H um subgrupo de índice finito no grupo G. Suponhamos que existe um homomorfismo $\theta: H \to A$ e $|G:H|=n$. Então para cada $x \in G$ existem $l_1, l_2, \ldots, l_m \in \mathbb{N}$ e $s_1, \ldots, s_m \in G$ tais que

$$(x)^{\theta^*} = \prod_{i=1}^{m} (s_i x^{l_i} s_i^{-1})^{\theta} \quad \text{e} \quad \sum_{i=1}^{m} l_i = n.$$

Teorema 1.10 (Teorema do subgrupo focal de Higman, [20, Corollary 10.34])**.** Sejam p um primo, G um grupo finito e $P \in \mathrm{Syl}_p(G)$. Então

$$P \cap G' = \langle [h,g] \mid h \in P, g \in G \text{ com } h^g \in P \rangle,$$

ou seja, $P \cap G'$ é gerado por comutadores de ordem potência de primo.

Proposição 1.11. Sejam G um grupo finito e S um p-subgrupo de Sylow de G. Então

$$S \cap G' \cap Z(G) = S' \cap Z(G).$$

Demonstração. A inclusão $S' \cap Z(G) \leq S \cap G' \cap Z(G)$ é imediata pois $S' \leq S$ e $S' \leq G'$. Para a inclusão inversa, usaremos a Proposição 1.9 com $A = S/S'$, $H = S$ e $\theta: S \to S'$ a projeção canônica $x \mapsto xS'$. Primeiramente note que $G' \leq \ker \theta^*$, pois dado um comutador $[g,h]$ qualquer, temos

$$[g,h]^{\theta^*} = (g^{-1})^{\theta^*} (h^{-1})^{\theta^*} (g)^{\theta^*} (h)^{\theta^*} = 1$$

pois θ^* leva em um grupo abeliano. Agora, se $x \in Z(G)$, então

$$x^{\theta^*} = \prod_{i=1}^{m} (s_i x^{l_i} s_i^{-1})^{\theta} = \prod_{i=1}^{m} s_i x^{l_i} s_i^{-1} S' = s^n S'.$$

Ou seja, mostramos que se $x \in Z(G) \cap G'$, então $x^n S' = S'$, logo, $x^n \in S'$. Por fim, se adicionalmente, $x \in S$, então $x \in S'$ pois $n = [G:S]$ é coprimo com $|S|$. Como x foi tomado arbitrariamente garantimos a inclusão desejada.

□

Corolário 1.12. Sejam G um grupo finito e p um divisor primo de $|G|$. Se $p \mid |G'|$, então $p \mid [G : Z(G)]$.

Demonstração. Suponha, por absurdo, que $p \mid |G'|$ e $p \nmid [G : Z(G)]$. Dessa forma, existe $S \in \mathrm{Syl}_p(G)$ contido em $Z(G)$ e, portanto, $S' \cap Z(G) = 1$. Por outro lado, $S \cap G' \cap Z(G) = S \cap G' \neq 1$, pois $S \cap G' \in \mathrm{Syl}_p(G')$. Usando a Proposição 1.11 obtemos um absurdo. □

1.3 Cotas para a ordem do subgrupo derivado

Munidos das consequências do Homomorfismo Transfer apresentaremos uma demonstração para uma versão do Teorema de Schur que, além da finitude de G', fornece uma limitação das potências de primos que dividem $|G'|$.

Definição 1.13. Sejam G um grupo e $H, K \leq G$. Definimos:

- O subgrupo $[H,K] = \langle [h,k] \mid h \in H, k \in K \rangle$.
- A série $\gamma_1(G) = G$ e $\gamma_i(G) = [G, \gamma_{i-1}(G)]$ se $i \geq 2$. Tal construção é chamada série central inferior.

Definição 1.14. Uma seção do grupo G é um quociente N/K, onde $N, K \leqslant G$ e $K \triangleleft N$.

Para o seguinte Lema usaremos o Teorema 1.35 que será provado mais a frente. Tal resultado diz que grupos nilpotentes finitamente gerados possuem um subgrupo de índice finito, característico e livre de torção.

Lema 1.15. Se $\gamma_r(G)$ é finito, então G tem uma sessão H finita tal que $\gamma_r(G) \cong \gamma_r(H)$. Em particular, se $r = 1$, então $\lambda(G) = \lambda(H)$.

Demonstração. Defina $\Gamma_r(G) = \{[x_1, \ldots, x_r] \mid x_i \in G, i = 1, \ldots, r\}$, dessa forma, $\gamma_r(G) = \langle \Gamma_r(G) \rangle$. Por hipótese $\Gamma_r(G)$ é finito, assim, escrevendo

$$\Gamma_r(G) = \left\{ [x_{11}, \ldots, x_{1r}], \ldots, [x_{s1}, \ldots, x_{sr}] \mid x_{ij} \in G, 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant r \right\},$$

podemos definir o subgrupo $K = \langle x_{ij} \mid 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant r \rangle$ de forma que $\Gamma_r(G) = \Gamma_r(K)$ e $\gamma_r(G) = \gamma_r(K)$. Defina $C = C_K(\gamma_r(G))$, como $\gamma_r(G) \triangleleft G$, em particular, temos $\gamma_r(G) \triangleleft K$, ou seja, $K = N_K(\gamma_r(G))$. Portanto

$$K/C = N_K(\gamma_r(G))/C_K(\gamma_r(G)) \lesssim \mathrm{Aut}(\gamma_r(G)),$$

como $\gamma_r(G)$ é finito segue que $\mathrm{Aut}(\gamma_r(G))$ é finito, como consequência do isomorfismo acima, K/C são finitos, dessa forma, C é finitamente gerado. Afirmamos que C é também nilpotente, de fato, temos $[C,\gamma_r(C)]=1$ pois C, por definição, centraliza qualquer comutador de peso r. Logo, pelo Teorema 1.35, C possui um subgrupo T característico, livre de torção e de índice finito. A seção $H=K/T$ é finita, pois $|K/T|=|K/C||C/T|$. Além disso, temos

$$\gamma_r(H)=\frac{\gamma_r(K)T}{T}\cong\frac{\gamma_r(G)}{\gamma_r(G)\cap T}.$$

Onde utilizamos o Teorema do Isomorfismo e que $\gamma_r(G)=\gamma_r(K)$. Como T é livre de torção e $\gamma_r(G)$ é finito temos $T\cap\gamma_r(G)=1$ e assim obtemos o resultado desejado. Por fim, tomando $r=1$ temos $G'\cong H'$ e portanto $\lambda(G)=\lambda(H)$. □

Os próximos dois resultados são devidos a J. Wiegold (cf. [28]), porém apresentaremos demonstrações elementares baseadas em [8, Lemma 5.3] e [8, Theorem 5.4] respectivamente.

Lema 1.16 (Wiegold)**.** Seja G um p-grupo com $|G/Z(G)|=p^{\alpha}$. Então $|G'|\leq p^{\alpha(\alpha-1)/2}$.

Demonstração. Antes de começarmos a demonstração, definiremos $Z_2(G)$ como o subgrupo de G satisfazendo $Z_2(G)/Z(G)=Z(G/Z(G))$.

A demonstração será por indução em α. Se G é abeliano, o que acontece se $\alpha=1$ ou $\alpha=0$, então o resultado é trivial. Suponha $\alpha\geq 2$ e G não-abeliano, assim, podemos tomar $a\in Z_2(G)/Z(G)$ não trivial. Defina $H=[G,a]\subseteq Z(G)$, afirmamos que $H=\{[g,a]\mid g\in G\}$, de fato,

$$[g,a][h,a]=[g,a]^h[h,a]=[gh,a].$$

Note que $|H|=[G:C_G(a)]$ pois $H=\left\{(a^{-1})^g a\mid g\in G\right\}$ e daí $|H|=|a^G|$, além disso, $Z(G)\subset C_G(a)$, pois $a\notin Z(G)$, dessa forma $|H|\leq p^{\alpha-1}$. Agora usaremos indução em G/H, para tanto, note que $Z(G)/H\subset Z(G/H)$, de fato, $aH\in Z(G/H)$ pois $[g,a]H=H$ para todo $g\in G$, mas se $aH\in Z(G)/H$, então $a\in Z(G)$, absurdo. Logo

$$[G/H:Z(G/H)]<\frac{G/H}{Z(G)/H}=\frac{G}{Z(G)}=p^{\alpha}.$$

Por indução, segue que

$$|G'|\leq|G'/H||H|\leq|(G/H)'||H|\leq p^{(\alpha-1)(\alpha-2)/2}p^{\alpha-1}=p^{\alpha(\alpha-1)/2}.$$

□

Teorema 1.17 (Wiegold)**.** Seja G um grupo. Se $[G:Z(G)]=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$, então $|G'|=p_1^{\beta_1}\cdots p_r^{\beta_r}$, onde $\beta_i\leq\alpha_i(\alpha_i+1)/2$.

Demonstração. Pelo Teorema de Schur e pela Proposição 1.15 podemos supor G finito. Se T é um p-subgrupo de Sylow de G', então $T = S \cap G'$ onde S é subgrupo de Sylow de G, além disso, pela Proposição 1.12 temos $p \in \{p_1, \ldots, p_r\}$. Dessa forma, $p = p_i$ para algum $i = 1, \ldots, r$. Como

$$[S \cap G' : S \cap G' \cap Z(G)] = [(S \cap G')Z(G) : Z(G)] \mid [G : Z(G)] = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

Temos $[S \cap G' : S \cap G' \cap Z(G)] \leq p_i^{\alpha_i}$. Pela Proposição 1.11 obtemos

$$|S \cap G' \cap Z(G)| \leq |S'|.$$

Por outro lado, utilizando ainda o Lema 1.16, segue que

$$|S'| \leq p_i^{\alpha_i(\alpha_i - 1)}.$$

Logo,

$$|S \cap G'| \leq p_i^{\alpha_i} |S \cap G' \cap Z(G)| \leq \alpha_i(\alpha_i + 1)/2.$$

Como todo grupo finito é gerado pelos seus subgrupos de Sylow o resultado segue.

□

1.4 Grupos nilpotentes finitamente gerados

Os resultados principais dessa seção foram baseados nas referências [1, Chapter 2] e [25, Chapter 7]. Começaremos com algumas definições.

Definição 1.18. Dizemos que um grupo G satisfaz MÁX se toda cadeia de subgrupos $H_1 < H_2 < \cdots$ é estacionária, isto é, existe n natural tal que $H_i = H_n$ para todo $i \geq n$.

Exemplo 1. Grupos finitos satisfazem MÁX. Além disso, o grupo dos inteiros aditivo $\mathbb{Z}$ e o dihedral infinito $D_\infty = \langle x, y \mid x^2 = y^2 = 1 \rangle$ satisfazem MÁX. Por outro lado, o grupo aditivo dos racionais $\mathbb{Q}$ não satisfaz MÁX.

Proposição 1.19. Um grupo G satisfaz MÁX se, e somente se, todo subgrupo $H \leq G$ é finitamente gerado.

Demonstração. ($\Rightarrow$) Suponha, por absurdo, que exista $H \leq G$ que não é finitamente gerado, tome $h_1 \in H$ e defina $H_1 = \langle h_1 \rangle$, como H não é finitamente gerado podemos tomar $h_2 \in H - H_1$. Defina $H_2 = \langle h_1, h_2 \rangle$ e repita o processo. Note que com isso construímos uma cadeia de subgrupos $H_1 < H_2 < \cdots$ de G que não é estacionária.

($\Leftarrow$) Considere $H_1 < H_2 < \cdots$ uma cadeia de subgrupos de G, dessa forma, $H = \cup_{i\geq 1} H_i$ é subgrupo de G, sendo assim, $H = \langle h_1, \ldots, h_n \rangle$. Para cada $i = 1, \ldots, n$ existe um índice n_i tal que $h_i \leq H_{n_i}$, tomando N como o máximo desses n_i obtemos que $H_N = H$ e a cadeia é estacionária. □

Proposição 1.20. Seja N subgrupo normal de um grupo G. Então G satisfaz MÁX se, e somente se, N e G/N satisfazem MÁX.

Demonstração. Suponha que G satisfaz MÁX, como todo subgrupo de N é também subgrupo de G, segue que N satisfaz MÁX. Considere agora um subgrupo $\overline{K}$ de G/N. Pela Proposição 1.19 o subgrupo K satisfazendo $K/N = \overline{K}$ é finitamente gerado e portanto K/N também é, assim, como $\overline{K}$ foi arbitrário a Proposição 1.19 garante que G/N satisfaz MÁX. Para a recíproca, considere $H_1 \leq H_2 \leq \cdots$ um cadeia de subgrupos de G. Por hipótese, as cadeias

$$H_1 \cap N \leq H_2 \cap N \leq \cdots,$$
$$H_1N/N \leq H_2N/N \leq \cdots.$$

são estacionárias, assim, existe n natural tal que $H_i \cap N = H_n \cap N$ e $H_iN = H_nN$ para todo $i \geq n$. Usando essas igualdades e a Lei de Dedekind obtemos

$$H_i = H_i \cap (H_iN) = H_i \cap (H_nN) = H_n(H_i \cap N) = H_n(H_n \cap N) = H_n,$$

para todo $i \leq n$, ou seja, a cadeia $H_1 \leq H_2 \leq \cdots$ tomada arbitrariamente é estacionária. □

Proposição 1.21. Grupos policíclicos satisfazem MÁX.

Demonstração. Basta usar a Proposição 1.20 nos fatores da série cíclica do grupo. □

Lema 1.22. Seja A um grupo abeliano. Então A é policíclico se, e somente se, A satisfaz MÁX.

Demonstração. Suponha que A satisfaz MÁX, em particular, A é finitamente gerado. Escrevendo $A = \langle a_1, a_2, \ldots, a_n \rangle$, segue que a cadeia

$$1 \lhd \langle a_1 \rangle \lhd \langle a_1, a_2 \rangle \lhd \cdots \lhd \langle a_1, a_2, \ldots, a_n \rangle$$

é uma série cíclica de A. A recíproca segue da Proposição 1.21. □

Proposição 1.23. Seja G um grupo solúvel. Então G satisfaz MÁX se, e somente se, G é policíclico.

Demonstração. Suponha que G satisfaz MÁX. A prova será por indução no comprimento derivado $\mathrm{dl}(G)$. Se $\mathrm{dl}(G) = 1$, então G é abeliano e o resultado segue pelo Lema 1.22.

Suponha agora que todos os grupos solúveis satisfazendo MÁX com comprimento de derivado menores que d são policíclicos. Considere um grupo G satisfazendo as hipóteses com $\mathrm{dl}(G) = d$, como G/G' é abeliano e $\mathrm{dl}(G') < d$ segue, por indução, que G/G' e G' são policíclicos. Daí G é policíclico.

A recíproca segue da Proposição 1.21. □

Proposição 1.24. Seja G um grupo nilpotente finitamente gerado, então G é policíclico.

Demonstração. Começaremos observando que a hipótese garante que os termos $\gamma_i(G)$ da série central inferior de G são finitamente gerados. Suponha G nilpotente de classe c, o subgrupo $\gamma_{c-1}(G)$ é abeliano e finitamente gerado, logo satisfaz MÁX, o mesmo vale para o quociente $\gamma_{c-2}(G)/\gamma_{c-1}(G)$, assim, pelo Lema 1.20, segue que $\gamma_{c-2}(G)$ satisfaz MÁX. Prosseguindo dessa forma obtemos que G satisfaz MÁX, usando agora a Proposição 1.23, obtemos que G é policíclico. □

Definição 1.25. Seja G um grupo, o conjunto $T(G) = \{x \in G \mid o(x) < \infty\}$ é chamado conjunto de torção de G.

Em geral $T(G)$ não é um subgrupo. Por exemplo, considere $G = \mathrm{GL}(2,\mathbb{R})$ um grupo linear geral e as matrizes

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Então $A^4 = B^3 = I_2$ mas AB tem ordem infinita. Porém, como veremos posteriormente, $T(G) \leq G$ caso G seja nilpotente.

Lema 1.26. Suponha que um grupo G seja gerado por elementos de ordem finita, então os fatores da série central inferior $\gamma_i(G)/\gamma_{i+1}(G)$ são grupos de torção.

Demonstração. A prova será por indução. Para $i = 0$, o fator G/G' é abeliano e gerado por elementos de ordem finita, portanto, a afirmação se verifica.

Suponha agora que $\gamma_i(G)/\gamma_{i+1}(G)$ é de torção. Como $\gamma_{i+1}(G)/\gamma_{i+2}(G)$ é abeliano, é suficiente provar que seus geradores têm ordem finita, para tanto, tome $[g,h] \in \gamma_{i+1}(G)$, onde $g \in G$ e $h \in \gamma_i(G)$, pela hipótese de indução, existe n natural tal que $h^n \in \gamma_{i+1}(G)$. assim $[g,h^n] \in \gamma_{i+2}(G)$, além disso, por $\gamma_{i+1}(G)/\gamma_{i+2}(G)$ ser abeliano, temos

$$[g,h]^n\gamma_{i+2}(G) = [g,h^n]\gamma_{i+2}(G) = \gamma_{i+2}(G).$$

Como $[g,h]$ é um gerador arbitrário de $\gamma_{i+1}(G)/\gamma_{i+2}(G)$, provamos o desejado. □

Proposição 1.27. O conjunto de torção $T(G)$ de um grupo nilpotente G é um subgrupo normal.

Demonstração. É imediato que $1 \in T(G)$ e que $T(G)$ é fechado para inversos. Tome $x, y \in T(G)$, para mostrar que $xy \in T(G)$ considere o subgrupo $H = \langle x, y \rangle$ e denote por c sua classe de nilpotência.

Pelo Lema 1.26 o quociente H/H' é de torção, assim existe n_1 natural tal que $(xy)^{n_1} \in H'$. Novamente pelo Lema 1.26 o quociente $H'/\gamma_3(H)$ é de torção, assim, existe n_2 tal que $((xy)^{n_1})^{n_2} \in \gamma_3(H)$, prosseguindo dessa forma podemos encontrar n natural tal que $(xy)^n \in \gamma_{c+1}(H) = 1$, como queríamos.

Para a normalidade basta observar que se $x \in T(G)$ tem ordem n, então x^g também tem ordem finita pois $(x^g)^n = (x^n)^g = 1$. □

Proposição 1.28. O subgrupo de torção $T(G)$ de um grupo G nilpotente finitamente gerado é finito.

Demonstração. Pela Proposição 1.24 segue que G é policíclico, assim, $T(G)$ também é. Considere $1 \leq H_1 \leq \cdots \leq H_n \leq T(G)$ um série cíclica para $T(G)$, como todo elemento de $T(G)$ tem ordem finita, segue que cada fator da série acima é finito, dessa forma, $T(G)$ também é finito. □

Agora definiremos e apresentaremos alguns fatos dos grupos residualmente finitos.

Definição 1.29. Um grupo G é dito residualmente finito se, para todo $1 \neq x \in G$, existe $N \trianglelefteq G$ de índice finito tal que $x \notin N$.

Lema 1.30. Se $G = \langle x \rangle$ é um grupo cíclico, então G é residualmente finito.

Demonstração. Seja $g = x^n \neq 1$ um elemento arbitrário de G. Se G for finito basta tomar $N_g = 1$, se G for infinito tome $N_g = \langle x^{n+1} \rangle$. □

Lema 1.31. Sejam G um grupo finitamente gerado e n um natural. Então existem apenas finitos subgrupos de G de índice n.

Demonstração. Apenas nessa demonstração denotaremos, mesmo que H não seja um subgrupo normal de G, o conjunto das classes laterais de H em G por G/H.

Se não existem subgrupos de índice n, terminamos. Suponha que exista $H \leq G$ com $[G : H] = n$. Primeiramente note que se G é r-gerado, então existem no máximo $(n!)^r$ homomorfismo de G em S_n.

Cada subgrupo H de índice n induz um homomorfismo ϕ_H de G em $\mathrm{Sym}(G/H)$ dado pela ação por multiplicação de G nas classes laterais de H. Associando cada classe lateral de H em G a um natural $j \in \{1,2,\ldots,n\}$ podemos considerar ϕ_H de G em S_n. Faremos tal associação de forma que a classe H e o natural 1 correspondam. Pelas observações estabelecidas, é suficiente provar que subgrupos distintos H,K de índice n induzem homomorfismos ϕ_H,ϕ_K distintos.

Para tanto, denote, respectivamente, por $S_H(j)$ e $S_K(j)$ os estabilizadores de $j \in \{1,2,\ldots,n\}$ das ações associadas aos homomorfismos ϕ_H e ϕ_K. Se $\phi_H = \phi_K$, teríamos $S_H(1) = S_K(1)$, mas

$$S_H(1) = \{g \in G \mid \phi_H(g)(1) = 1\} = \{g \in G \mid gH = H\} = H.$$

E analogamente $S_K(1) = K$. □

Teorema 1.32. Se G possui um subgrupo normal H finitamente gerado e residualmente finito tal que G/H é cíclico, então G é residualmente finito.

Demonstração. Suponha que $G/H = \langle aH \rangle$ e tome $g \in G$. Se $g \notin H$, então $gH \neq H$ e, como G/H é residualmente finito, segue que existe $N_g/H \leq G/H$ tal que $gH \notin N_g/H$ e o índice $[G/H : N_g/H]$ é finito. Logo $g \notin N_g$ e $[G : N_g]$ é finito.

Resta lidar com o caso em que $g \in H$. Afirmamos que existe $C \leq H$ característico e de índice finito tal que $g \notin C$. De fato, tome $N \in H$ tal que $g \notin N$, definindo C como a intersecção dos subgrupos K de H tal que $[H : N] = [H : K]$ obtemos o desejado, pois pelo Lema 1.31 e pelo Lema de Poincaré C tem índice finito, além disso, como automorfismos de H não alteram o índice de seus subgrupos segue que C é característico.

Se $[G : H]$ é finito, então $[G : C]$ é finito e podemos tomar $N_g = C$. Para terminar, suponha que G/H seja infinito e denote $\overline{G} = G/C$, $\overline{H} = H/C$, $\overline{g} = gC$ e $\overline{a} = aC$. Seja $\overline{D} = C_{\overline{G}}(\overline{H})$, o NC-Lema garante que $\overline{D}$ tem índice finito em $\overline{G}$. Se $[\overline{G} : \overline{D}] = m$, segue que $\overline{a}^m$ centraliza $\overline{H}$. Considere agora o subgrupo $\overline{A} = \langle \overline{a}^m \rangle$. Se $\overline{g} \in \overline{A}$, então existiria $k \in \mathbb{N}$ tal que $a^k \in H$, absurdo pois aH gera o cíclico infinito G/H.

Além disso $\overline{A} \triangleleft \overline{G}$ e $[\overline{G} : \overline{A}]$ é finito pois $G = \langle a \rangle H$. Tome então N_g satisfazendo $N_g/C = \overline{A}$, já que $[G : N_g]$ é finito e $g \notin N_g$. □

Definição 1.33. Um grupo G é dito policíclico se possui uma série cíclica, ou seja, se existem subgrupos $1 = H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_n = G$ tais que H_{i+1}/H_i é cíclico para todo $1 \leq i \leq n-1$.

Corolário 1.34 (Hirsch)**.** Grupos policíclicos são residualmente finitos.

Demonstração. Seja G um grupo policíclico. Considere $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G$ uma série cíclica para G. O Teorema 1.32 garante que H_2 é finitamente residualmente finito, pois H_2/H_1 é cíclico e H_1 é residualmente finito, já que é cíclico (Lema 1.30).

Ou seja, H_3 é residualmente finito, pois H_2 é residualmente finito e H_3/H_2 é cíclico. Prosseguindo dessa forma obtemos que G é residualmente finito. □

Teorema 1.35. Seja G um grupo nilpotente finitamente gerado. Então G possui um subgrupo característico, livre de torção e de índice finito.

Demonstração. Temos que G é residualmente finito (Corolário 1.34 e Proposição 1.24) e seu subgrupo de torção T é finito (Proposição 1.28). Para cada $x \in T$ tome $N_x \trianglelefteq G$ tal que $x \notin N_x$. Defina $N = \cap_{x \in T} N_x$, pelo Lema de Poincaré N possui índice finito.

Agora defina o conjunto $X = \{H \leq G \mid [G:H] = [G:N]\}$ e o subgrupo $C = \cap_{H \in X} H$. Pelo Lema 1.31 e pelo Lema de Poincaré segue que C têm índice finito, além disso, C é livre de torção pois $C \leq N$ e $N \cap T = 1$. Por fim, como um automorfismo de G preserva o índice de seus subgrupos segue que C é característico. □

1.5 Álgebras de Lie

Podemos pensar, grosso modo, uma álgebra de Lie como um espaço vetorial (ou um módulo) munido de um certo produto de vetores. No Capítulo 3 veremos suas aplicações na Teoria de Grupos, já no Capítulo 2 estudaremos algumas questões envolvendo finitude nesses objetos.

Definição 1.36. Sejam L um R-módulo e $[\cdot,\cdot]$ uma operação binária em L satisfazendo:

1. $[na+b,c] = n[a,c] + [b,c]$;
2. $[a,nb+c] = n[a,b] + [a,c]$;
3. $[a,a] = 0$;
4. $[[a,b],c] + [[b,c],a] + [[c,a],b] = 0$,

para quaisquer $a,b,c \in L$ e $n \in R$. Então L é dita uma álgebra de Lie.

Se, em particular, $R = \mathbb{Z}$ ou $R = \mathbb{Z}/n\mathbb{Z}$, então L é dita um anel de Lie.

Exemplo 2.

- Seja L um R-módulo qualquer, então L é uma álgebra de Lie se definirmos $[a,b] = 0$ para quaisquer $a,b \in L$.
- O $\mathbb{R}$-espaço vetorial $\mathbb{R}^3$ munido do produto vetorial é uma álgebra de Lie.
- Considere $gl(n,\mathbb{R})$ o espaço vetorial real das matrizes $n \times n$ com entradas em $\mathbb{R}$, então $gl(n,\mathbb{R})$ é uma álgebra de Lie se munido do produto $[A,B] = AB - BA$.

Definição 1.37. Sejam L uma álgebra de Lie e M um submódulo de L.

1. Dizemos que M é uma subálgebra de L se $[x,y] \in M$ para quaisquer $x,y \in M$.

2. Dizemos que M é um ideal de L se $[x,y] \in M$ para quaisquer $x \in M$ e $y \in L$.

Exemplo 3. Sejam L uma álgebra de Lie e X um subconjunto de L. É imediato que L e $\{0\}$ são ideais. O centralizador de X em L, definido como $C_L(X) = \{y \in L \mid [y,x] = 0, \forall x \in X\}$, é uma subálgebra. Em particular $C_L(L)$ é um ideal chamado de centro e denotado por $Z(L)$.

Proposição 1.38. Sejam L um álgebra de Lie e I,J ideais de L. Então $I+J = \langle x+y \mid x \in I, y \in J\rangle$ e $[I,J] = \langle [x,y] \mid x \in I, y \in J\rangle$ são ideais, em particular, $[L,L]$ é chamada de subálgebra derivada e é denotada por L'.

Definição 1.39. Seja L uma álgebra de Lie.

1. Se $[x,y] = 0$ para quaisquer $x,y \in L$ dizemos que L é abeliana.

2. Podemos definir recursivamente a seguinte sequência de ideais, $L^0 = L$ e $L^i = [L, L^{i-1}]$ se $i \geqslant 1$. Se existe um natural n tal que $L^n = 0$ dizemos que L é nilpotente. Além disso, se $L^c = 0$ e $L^{c-1} \neq 0$ dizemos que L é nilpotente de classe $c-1$.

Agora enunciaremos um resultado que será fundamental para a teoria apresentada nesse capítulo. Sua demonstração não é elementar, mas conseguiremos demonstrar o caso particular para $p = 3$, que será suficiente para os nossos objetivos.

Definição 1.40. Seja L uma álgebra de Lie. Dizemos que L satisfaz a n-ésima identidade de Engel se

$$[x, \underbrace{y, \ldots, y}_{\text{n vezes}}] = 0$$

para quaisquer $x,y \in L$.

Teorema 1.41. ([27, Chapter 3] Teorema de Kostrikin) Seja L uma álgebra de Lie sobre um corpo de característica p. Se L satisfaz a $(p-1)$-ésima identidade de Engel, então L é nilpotente.

Na realidade, para o caso desejado precisaremos apenas de parte da hipótese.

Teorema 1.42. (Teorema de Kostrikin para $p = 3$) Seja L uma álgebra de Lie (sobre um anel qualquer). Se L satisfaz a segunda identidade de Engel, então L é nilpotente de classe no máximo 3.

Demonstração. A ideia da demonstração é utilizar que essas álgebras de Lie possuem algum nível de comutatividade, mais precisamente, provaremos as identidades a seguir:

$$[[x,y],z] = [[y,z],x] = [[z,x],y] = -[[y,x],z] = -[[x,z],y] = -[[z,y],x].$$

Tome $x,y,z \in L$, por hipótese temos

$$[[x,y],y] = [[x,z],z] = [[x,y+z],y+z] = 0.$$

Portanto $[[x,y],z] = -[[x,z],y]$, pois

$$\begin{aligned} 0 = [[x,y+z],y+z] &= [[x,y]+[x,z],y+z] \\ &= [[x,y],y]+[[x,y],z]+[x,z],y]+[[x,z],z] \\ &= [[x,y],z]+[[x,z],y] \end{aligned}$$

Como x,y,z são arbitrários temos também

$$[[y,z],x] = -[[y,x],z], \quad [[z,x],y] = -[[z,y],x].$$

Para terminar usaremos a anticomutatividade ($[x,y] = -[y,x]$) para obter que

$$[[x,y],z] = -[[y,x],z], \quad [[y,z],x] = -[[z,y],x].$$

Agora, para provar a nilpotência, tome $x,y,z,t \in L$. Usando a Identidade de Jacobi e as identidades obtidas segue que

$$\begin{aligned} [[[x,y],z],t] &= [[[z,t],[x,y]] \\ &= [[[z,t],x],y]-[[[z,t],y],x] \\ &= [[[z,t],x],y]+[[[z,t],x],y] \\ &= 2[[[z,t],x],y]. \end{aligned}$$

Por outro lado,

$$\begin{aligned} [[[x,y],z],t] &= [[[z,x],y],t] \\ &= -[[[z,x],t],y] \\ &= [[[z,t],x],y]. \end{aligned}$$

Ou seja, $[[[z,t],x],y] = 0$ □

Para mais detalhes sobre o anel de Lie associado e o Teorema de Kostrikin veja [27, Chapters 2,3].

Capítulo 2

Finitude em álgebras de Lie

Nesse capítulo, o anel R na definição 1.36 será sempre um corpo, ou seja, as álgebras de Lie serão R-espaço vetoriais. Assim, a seguinte definição faz sentido.

Definição 2.1. Sejam L uma álgebra de Lie (sobre um corpo $\mathbb{K}$) e X um subconjunto de L.

1. Escrevemos $\langle X \rangle$ para denotar o subespaço de L gerado por X.
2. Definimos a dimensão de uma álgebra de Lie L como a dimensão de L visto como espaço vetorial, isto é $\dim_{\mathbb{K}}(L)$, ou simplesmente: $\dim(L)$.

O objetivo desse capítulo, em linhas gerais, é investigar como certos resultados clássicos da Teoria de Grupos podem ser pensados em álgebras de Lie. No caso, apresentaremos uma definição de largura para uma álgebra de Lie e também um teorema análogo ao Teorema de Neumann-Wiegold para BFC-grupos (cf. [29, Theorem 4.7]).

2.1 Largura de uma álgebra de Lie

Análogo ao que foi feito para grupos, definiremos o conjunto dos comutadores de uma álgebra de Lie L como $\Gamma(L) = \{[x,y] \mid x,y \in L\}$. Nesse contexto, podemos definir uma largura para uma álgebra de Lie, lembre-se que $L' = [L,L] = \langle [x,y] \mid x,y \in L \rangle$

Definição 2.2. Seja L uma álgebra de Lie. Definimos a largura de L como o menor natural n (caso exista) tal que todo elemento de L' pode ser escrito como uma combinação linear de n comutadores, isto é, se $x \in L'$ então existem $x_1, \ldots, x_n \in \Gamma(L)$ e $c_1, \ldots, c_n \in \mathbb{K}$ tais que

$$x = \sum_{i=1}^{n} c_i x_i.$$

Se tal natural não existe dizemos que L possui largura infinita.

OBSERVAÇÃO 1. Note que da linearidade do colchete de Lie podemos considerar $c_i = 1$ para $i = 1, 2, \cdots, n$.

Proposição 2.3. Seja L uma álgebra de Lie não abeliana de dimensão 2. Então $\dim(L') = 1$. Em particular, L tem largura 1.

Demonstração. Seja $\{x, y\}$ uma base de L, então o comutador de um par de elementos quaisquer de L é um múltiplo de $[x, y]$. Dessa forma, L' é gerada por $[x, y]$ e $[x, y] \neq 0$, caso contrário L seria abeliana, absurdo. Logo $\dim(L') = 1$. □

Proposição 2.4. Seja L uma álgebra de Lie na qual a subálgebra derivada tem dimensão finita. Então a largura da álgebra de Lie L é limitada por $\dim_{\mathbb{K}}(L')$.

Demonstração. Chamemos $k = \dim_{\mathbb{K}}(L')$, como $L' = \langle \Gamma(G) \rangle$ existem $x_1, \cdots, x_k$ comutadores tais que $L' = \langle x_1, \cdots, x_k \rangle$. Dessa forma, todo elemento de L' é soma de, no máximo, $k = \dim_{\mathbb{K}}(L')$ comutadores. □

2.2 Uma álgebra de Lie de largura infinita

Note que a Proposição 2.4 garante que álgebras de Lie de dimensão finita também possuem largura finita, nesse contexto considere o seguinte problema.

PROBLEMA 1. Existem Álgebras de Lie (de dimensão infinita) com largura infinita?

Veremos que a resposta é positiva. O exemplo que faremos aqui é baseado em uma construção análoga para grupos devida a P. J. Cassidy (cf. [3]). Para tanto, apresentaremos uma forma geral de construir álgebras de Lie a partir de álgebras associativas.

Definição 2.5. Seja $\mathbb{A}$ um $\mathbb{K}$-espaço vetorial.

1. Dizemos que uma operação binária:

$$\cdot : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$$

é uma multiplicação de vetores se

(a) $(\alpha a) \cdot b = a \cdot (\alpha b) = \alpha(a \cdot b)$ e $1a = a$.

(b) $(a + b) \cdot c = a \cdot c + b \cdot c$

(c) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Para quaisquer $a, b, c \in \mathbb{A}$ e $\alpha \in \mathbb{K}$.

2. O par $(\mathbb{A}, \cdot)$ é chamado de uma Álgebra (ou $\mathbb{K}$-álgebra).

3. Se adicionalmente $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, então dizemos que $\mathbb{A}$ é uma álgebra associativa.

Proposição 2.6. Seja $\mathbb{A}$ uma $\mathbb{K}$-álgebra associativa. Defina a seguinte operação binária:

$$[\cdot,\cdot] : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$$

dada por: $[a,b] \mapsto ab - ba$. Então $[\cdot,\cdot]$ é um produto de Lie.

Demonstração. Para todos $a,b,c \in A$ e $\alpha \in \mathbb{K}$ temos:

1. $[a,a] = a^2 - a^2 = 0$.

2. $[\alpha a + b, c] = (\alpha a + b)c - c(\alpha a + b) = (\alpha(ac - ca)) + (bc - cb) = \alpha[a,c] + [b,c]$.

3. $[a, \alpha b + c] = a(\alpha b + c) - (\alpha b + c)a = (\alpha(ab - ba)) + (ac - ca) = \alpha[a,b] + [a,c]$.

4. Note que

$$\begin{aligned}
[a,[b,c]] &= [a, bc - cb] = a(bc - cb) - (bc - cb)a = abc - acb - bca + cba, \\
[b,[c,a]] &= [b, ca - ac] = b(ca - ac) - (ca - ac)b = bca - bac - cab + acb, \\
[c,[a,b]] &= [c, ab - ba] = c(ab - ba) - (ab - ba)c = cab - cba - abc + bac.
\end{aligned}$$

   Como os termos das igualdades se cancelam vale a identidade de Jacobi, isto é, $[a,[b,c]] + [b,[c,a]] + [c,[a,b]] = 0$.

Portanto, $[\cdot,\cdot]$ é um produto de Lie. □

Considere o anel $\mathbb{R}[x,y]$ dos polinômios em duas incógnitas com coeficientes reais. Dados $f(x), g(y), h(x,y) \in \mathbb{R}[x,y]$ defina L como o conjunto das matrizes da forma

$$A(f(x), g(y), h(x,y)) = \begin{pmatrix} 0 & f(x) & h(x,y) \\ 0 & 0 & g(y) \\ 0 & 0 & 0 \end{pmatrix}.$$

Então L é uma $\mathbb{R}$-álgebra associativa com as operações usuais de matrizes, sendo assim, pela Proposição 2.6 podemos definir $[\cdot,\cdot] : L \times L \to L$ como $[A,B] = AB - BA$ de forma que L seja uma álgebra de Lie sobre os reais.

OBSERVAÇÃO 2. Até o fim dessa seção, L denotará a álgebra de Lie definida acima. Além disso, para simplificar a notação, denotaremos os elementos de L apenas por $A(f,g,h)$.

Proposição 2.7. Sejam $A(f,g,h),\ A(a,b,c) \in L$. Então

1. $[A(f,g,h),A(a,b,c)] = A(0,0,fb-ag)$;
2. $L' = \langle A(0,0,h)\rangle$,
3. $Z(L) = L'$;
4. L é nilpotente de classe 2.

Demonstração. 1. De fato,

$$\begin{aligned} A(f,g,h)A(a,b,c) &= \begin{pmatrix} 0 & f(x) & h(x,y) \\ 0 & 0 & g(y) \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & a(x) & c(x,y) \\ 0 & 0 & b(y) \\ 0 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & f(x)b(y) \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \\ &= A(0,0,fb). \end{aligned}$$

Logo,

$$\begin{aligned} [A(f,g,h),A(a,b,c)] &= A(f,g,h)A(a,b,c) - A(a,b,c)A(f,g,h) \\ &= A(0,0,fb) - A(0,0,ag) \\ &= A(0,0,fb-ag). \end{aligned}$$

2. Pelo item anterior, a subálgebra derivada L' é gerada por elementos de L da forma

$$A(0,0,fb-ag).$$

Assim é imediato que $L' \subseteq \langle A(0,0,h)\rangle$. Para a inclusão contrária tome $f(x) = x^i, b(y) = y^j, a(x) = g(y) = 0$, logo $A(0,0,x^i y^j) \in L'$ para todo $i,j \in \mathbb{N}$. Tomando combinações lineares desses elementos obtemos $A(0,0,h) \in L'$ para qualquer $h(x,y) \in \mathbb{R}[x,y]$ e, portanto, $L' = \langle A(0,0,h)\rangle$.

3. Mostraremos que $Z(L) = \langle A(0,0,h)\rangle$. A inclusão $\langle A(0,0,h)\rangle \subseteq Z(L)$ é imediata. Sejam $A(f,g,h) \in Z(L)$ e $A(a,b,c) \in L$, dessa forma

$$[A(f,g,h),A(a,b,c)] = A(0,0,fb-ag) = 0.$$

Tomando $a(x) = 0$ e $b(y) \neq 0$ obtemos $f(x) = 0$, já se tormarmos $a(x) \neq 0$ e $b(y) = 0$ obtemos $g(x) = 0$, logo $A(f,g,h) = A(0,0,h)$ e vale a inclusão contrária. Por fim $Z(L) = \langle A(0,0,h)\rangle = L'$.

4. O item anterior garante que $[L,L'] = [L,Z(L)] = 0$, logo a série central inferior de L tem comprimento igual a 2.

□

Uma álgebra de Lie V possui largura igual a 1 se, e somente se, todo elemento em V' é comutador de um par de elementos em V, ou seja, se e somente se, $V' = \Gamma(V)$. Antes de resolvermos o Problema 1 mostraremos que L possui largura maior do que 1.

Proposição 2.8. Se $k(x,y) = x^2 + xy + y^2$, então $A(0,0,k) \notin \Gamma(L)$.

Demonstração. Suponha, por absurdo, que existam elementos $A(f,g,h), A(a,b,c) \in L$ tais que

$$[A(f,g,h), A(a,b,c)] = A(0,0,h).$$

ou seja,

$$f(x)b(y) - a(x)g(y) = k(x,y) = x^2 + xy + y^2 \tag{2.1}$$

Podemos escrever para algum natural m,

$$f(x) = f_0 + f_1 x + \cdots + f_m x^m,\ a(x) = a_0 + a_1 x + \cdots + a_m x^m, \tag{2.2}$$

onde $a_i, f_j \in \mathbb{R}$ para $i, j = 1, \cdots, m$. Substituindo as expressões acima em 2.2 obtemos

$$(f_0 b(y) - a_0 g(y)) + (f_1 b(y) - a_1 g(y))x + \cdots + (f_m b(y) - a_m g(y))x^m = x^2 + xy + y^2.$$

Considerando essa igualdade no anel de polinômios $\mathbb{R}[y][x]$ temos

$$\begin{aligned} f_0 b(y) - a_0 g(y) &= y^2, \\ f_1 b(y) - a_1 g(y) &= y, \\ f_2 b(y) - a_2 g(y) &= 1. \end{aligned}$$

Absurdo, pois teríamos

$$\langle 1, y, y^2\rangle \subseteq \langle b(y), g(y)\rangle,$$

mas $\dim_{\mathbb{R}}(\langle 1, y, y^2\rangle) = 3$ e $\dim_{\mathbb{R}}(\langle b(y), g(y)\rangle) \leqslant 2$.

Ou seja, o conjunto dos comutadores $\Gamma(L)$ está propriamente contido na subálgebra derivada. □

A demonstração da Proposição 2.8 nos fornece uma ideia interessante que, com alguma adaptação, pode ser usada para responder o Problema 1.

Teorema 2.9. Para cada n natural defina $k_n(x,y) = \sum_{i=0}^{2n} x^i y^{2n-i}$. Então $A(0,0,k_n)$ não é soma de n comutadores.

Demonstração. Suponha, por absurdo, que existam n elementos da forma $A(0,0,f_j b_j - a_j g_j)$, com $j = 1,\cdots,n$, tais que

$$A(0,0,k_n) = \sum_{i=1}^{n} A(0,0,f_i b_i - a_i g_i) = A(0,0,\sum_{i=1}^{n} f_i b_i - a_i g_i)$$

Nesse caso,

$$k_n(x,y) = \sum_{i=0}^{2n} x^i y^{2n-i} = \sum_{i=1}^{n} f_i(x) b_i(y) - a_i(x) g_i(y) \tag{2.3}$$

Escrevendo para algum k,

$$f_i(x) = f_{0,i} + f_{1,i}x + \cdots + f_{k,i}x^k,$$

$$a_i(x) = a_{0,i} + a_{1,i}x + \cdots + a_{k,i}x^k,$$

e substituindo em (2) obtemos

$$\begin{aligned}\sum_{i=0}^{2n} x^i y^{2n-i} &= \sum_{i=1}^{n} (f_{0,i} + f_{1,i}x + \cdots + f_{k,i}x^k) b_i(y) - (a_{0,i} + a_{1,i}x + \cdots + a_{k,i}x^k) g_i(y) \\ &= \sum_{i=1}^{n} (f_{0,i} b_i(y) - a_{0,i} g_i(y)) + \sum_{i=1}^{n} (f_{1,i} b_i(y) - a_{1,i} g_i(y)x) + \cdots + \sum_{i=1}^{n} (f_{k,i} b_i(y) - a_{k,i} g_i(y)x^k)\end{aligned}$$

Novamente, podemos considerar a igualdade acima no anel de polinômios $\mathbb{R}[y][x]$ e, sem perda de generalidade, supor $k \geqslant 2n$, assim obtemos as expressões

$$\begin{aligned}\sum_{i=1}^{n} f_{0,i} b_i(y) - a_{0,i} g_i(y) &= y^{2n} \\ \sum_{i=1}^{n} f_{1,i} b_i(y) - a_{1,i} g_i(y) &= y^{2n-1} \\ &\cdots \\ \sum_{i=1}^{n} f_{2n,i} b_i(y) - a_{2n,i} g_i(y) &= 1.\end{aligned}$$

Que nos levam ao seguinte absurdo

$$\langle 1, y, \cdots, y^{2n} \rangle \subseteq \langle b_1(y), g_1(y), \cdots, b_n(y), g_n(y) \rangle,$$

pois $\dim_{\mathbb{R}}(\langle 1, y, \cdots, y^{2n} \rangle) = 2n+1$ e $\dim_{\mathbb{R}}(\langle b_1(y), g_1(y), \cdots, b_n(y), g_n(y) \rangle) \leqslant 2n$. Logo L é uma álgebra de Lie de largura infinita. □

OBSERVAÇÃO 3. Também poderíamos ter considerado L sobre um corpo $\mathbb{K}$ qualquer.

2.3 Condições de finitude para a álgebra derivada

O objetivo dessa seção é apresentar versões análogas para álgebras de Lie de teoremas famosos sobre grupos. Começaremos vendo que é possível provar uma versão do Teorema de Schur para álgebras de Lie.

Teorema 2.10. Seja L uma álgebra de Lie. Suponhamos que $\dim_{\mathbb{F}}(L/Z(L)) = n$. Então a subálgebra derivada tem dimensão $\dim_{\mathbb{F}}(L') \leqslant n(n-1)/2$.

Demonstração. Como $\dim_{\mathbb{F}}(L/Z(L)) = n$, existem $x_1, \ldots, x_n \in L$ tais que

$$\frac{L}{Z(L)} = \langle x_1 + Z(L), \ldots, x_n + Z(L) \rangle.$$

Escolha arbitrariamente $\alpha, \beta \in L$, daí existem $\lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n \in \mathbb{F}$ e elementos $z_1, z_2 \in Z(L)$ tais que

$$\alpha = \left(\sum_{i=1}^{n} \lambda_i x_i \right) + z_1 \text{ e } \beta = \left(\sum_{i=1}^{n} \mu_i x_i \right) + z_2.$$

Assim, usando a linearidade do colchete de Lie, temos

$$[\alpha, \beta] \in \langle [x_i, x_j] \mid 1 \leqslant i < j \leqslant n \rangle.$$

E, consequentemente, $\dim_{\mathbb{F}}(L') \leqslant n(n-1)/2$. □

Agora trataremos do Teorema de Neumann-Wiegold ([19, 14.5.11]). Esse resultado aparece no contexto dos BFC-grupos e garante a finitude do subgrupo derivado desses grupos.

Apresentaremos esse teorema e discutiremos sua versão para álgebras de Lie.

Definição 2.11. Sejam G um grupo e $x \in G$. Denotaremos a classe de conjugação de x por x^G.

Definição 2.12. Seja G um grupo. Se existe m natural tal que $|x^G| \leq m$ para todo $x \in G$, dizemos que G é um BFC-grupo.

Teorema 2.13 (Neumann-Wiegold)**.** Seja G um BFC-grupo. Então G' é finito.

Em virtude do Teorema da Órbita-Estabilizador os BFC-grupos são exatamente aqueles no qual existe m natural tal que $[G : C_G(x)] \leq m$ para todo $x \in G$. Usaremos essa caracterização e o resultado a seguir para definirmos as "BFC-álgebras de Lie".

Lema 2.14. Sejam L uma álgebra de Lie, $a \in L$ e $[L,a] = \{[x,a] \mid x \in L\}$. Então a aplicação

$$f : L/C_L(a) \to [L,a] \tag{2.4}$$
$$x + C_L(a) \mapsto [x,a] \tag{2.5}$$

é um isomorfismo de espaços vetoriais. Em particular, $\dim(L/C_L(a)) = \dim([L,a])$.

Ou seja, estaremos interessados nas álgebras de Lie em que as dimensões $\dim([L,a])$ são uniformemente limitadas. Para a demonstração do análogo do Teorema 2.13 precisaremos de mais um lema.

Lema 2.15. Sejam V um espaço vetorial e A, B subespaços de V. Então

$$\dim(V/(A \cap B)) \leqslant \dim(V/A) + \dim(V/B).$$

Demonstração. Basta considerar a aplicação

$$\begin{aligned} \varphi : V &\to V/A \oplus V/B \\ x &\mapsto (x+A, x+B) \end{aligned}$$

Temos que φ é uma transformação linear na qual $\ker(\varphi) = A \cap B$. Assim, pelo Teorema do Núcleo e da Imagem, obtemos

$$\frac{V}{A \cap B} = \frac{V}{\ker(\varphi)} \cong Im(\varphi) \leqslant \frac{V}{A} \oplus \frac{V}{B},$$

e o resultado segue. □

Naturalmente, o resultado anterior garante que

$$\dim(V/\bigcap_{i=1}^{k} A_i) \leqslant \sum_{i=1}^{k} \dim(V/A_i)$$

para qualquer $k \in \mathbb{N}$, onde cada A_i é subespaço do espaço vetorial V.

Por fim, resta observar que as questões de finitude da ordem se traduzem para a finitude das dimensões dos objetos envolvidos.

Teorema 2.16. Seja L uma álgebra de Lie. Suponha que exista $m \in \mathbb{N}$ tal que $\dim([L,x]) \leqslant m$ para todo $x \in L$, então $\dim(L') \leqslant m^3 + m$.

Demonstração. Seja $a \in L$ tal que $\dim([L,a]) = m$. Pelo Lema 2.14 temos $\dim(L/C_L(a)) = m$, daí existem $t_1, \cdots, t_m \in L$ tais que para qualquer $x \in L$ podemos escrever

$$x = c + \sum_{i=1}^{m} \alpha_i t_i,$$

para algum $c \in C_L(a)$. Assim, podemos construir uma base para $[L,a]$, pois

$$[x,a] = [c,a] + \sum_{i=1}^{m} [t_i,a] = \sum_{i=1}^{m} [t_i,a],$$

logo $[L,a]$ é gerado pelos m elementos $[t_i,a]$ e como $\dim([L,a]) = m$ esses elementos formam, de fato, uma base desse espaço vetorial.

Agora defina $C = \bigcap_{i=1}^{m} C_L(t_i)$. Pelo Lema 2.15 temos

$$\dim(L/C) = \dim(L/\bigcap_{i=1}^{m} C_L(t_i)) \leqslant \sum_{i=1}^{m} \dim(L/C_L(t_i)) = \sum_{i=1}^{m} \dim([L,t_i]) \leqslant m^2.$$

Chame $k = \dim(L/C)$, dessa forma existem $s_1, s_2, \cdots, s_k \in L$ tais que para qualquer $x \in L$ podemos escrever

$$x = c + \sum_{i=1}^{k} \alpha_i s_i,$$

para algum $c \in C$. Note que é suficiente construirmos um espaço vetorial V com $L' \subseteq V$ e $\dim(V)$ finita. Para tanto, defina

$$V = [L,a] + [L,s_1] + \cdots + [L,s_k].$$

É imediato que V possui dimensão finita, resta verificar que $L' \subseteq V$. Seja $[x,y] \in L'$, escreva $x = \sum_{i=1}^{k} \alpha_i s_i + c_1$ e $y = \sum_{i=1}^{k} \beta_i s_i + c_2$, onde $c_1, c_2 \in C$. Dessa forma

$$[x,y] = \sum_{1 \leqslant i,j \leqslant k} \alpha_i \beta_j [s_i, s_j] + \sum_{i=1}^{k} \alpha_i [s_i, c_2] + \sum_{i=1}^{k} [c_1, s_i] + [c_1, c_2],$$

segue da definição que os três somatórios acima estão em V. Note que os elementos $[t_i, a]$ geram o espaço vetorial $[L, a+c_1]$, de fato, $[t_i, a+c_1] = [t_i, a] + [t_i, c_1] = [t_i, a]$, pois $c_1 \in C$ e portanto $[c_1, t_i] = 0$ para $i = 1, \cdots, k$. Assim, $[L, c_1 + a]$ possui m elementos linearmente independentes e como $\dim([L, c_1 + a]) \leqslant m$ segue que esses elementos formam uma base de $[L, c_1 + a]$ e, em particular, geram esse espaço vetorial. Dessa forma temos

$$[c_2, c_1 + a] = \sum_{i=1}^{m} \lambda_i [t_i, a],$$

ou seja,

$$[c_1, c_2] = -\sum_{i=1}^{m} \lambda_i [t_i, a] + [c_2, a] \in [L, a] \subseteq V.$$

Como queríamos. Portanto $L' \subseteq V$ e assim $\dim(L') \leqslant \dim V \leqslant m^3 + m$. □

A demonstração acima foi baseada na prova do Teorema de Neumann- Wiegold em [19, 14.5.11], vale ressaltar que em grupos os cálculos são mais complicados.

A demonstração apresentada é completamente elementar, porém não oferece uma cota realista. A fim de apresentarmos alguns exemplos, denotaremos por $m(L)$ como o menor m tal que $\dim[L, x] \leq m$ para todo $x \in L$.

Exemplo 4.

- Se L é uma álgebra de Lie abeliana, então $m(L) = 0$. Nesse caso a cota obtida é zero e coincide com $\dim L'$.
- Considere $L = \mathbb{R}^3$ munido do produto vetorial "$\wedge$". Então $m(L) = 2$ e $\dim L' = 3$, por outro lado a cota obtida é $2^3 + 2 = 10$.

Capítulo 3

O Problema de Burnside

Esse capítulo foi baseado em [27, Chapters 2,3,5,6]. Usaremos o termo *Problemas de Burnside* para nos referimos a três problemas, o primeiro deles é chamado de:

PROBLEMA 2. (Problema Geral de Burnside.) Todo grupo de torção finitamente gerado é finito?

Alguns contra-exemplos para esse problema já são conhecidos (cf. [5], [6], [9]).

O segundo deles é chamado de:

PROBLEMA 3. (Problema de Burnside.) Todo grupo de expoente finito e finitamente gerado é finito?

Note que o Problema de Burnside possui a seguinte reformulação em termos de parâmetros: para quaisquer par de naturais (r,n) um grupo r-gerado de expoente n é finito.

Já são conhecidas respostas negativas para alguns valores (r,n), porém ainda está longe do problema ser bem conhecido para todo par (r,n). Por exemplo, ainda não sabemos se o caso $(2,5)$ possui resposta positiva ou negativa, por outro lado, como veremos mais a frente, os pares (r,n) possuem solução positiva quando $n = 2,3,4,6$ e r qualquer.

O último desses problemas é conhecido por:

PROBLEMA 4. (Problema Restrito de Burnside) Fixados m,n naturais, então existe um número finito de grupos m-gerados de expoente n finitos.

Diferentemente dos outros problemas, esse possui resposta positiva, porém nada elementar. Uma das primeiras contribuições nessa direção foi dada por A. Kostrikin. Ele mostrou que grupos r-gerados de expoente p tem ordem limitada. A solução completa foi dada pelo matemático E. I. Zelmanov em 1989. Devido a tal contribuição e diversas outras ele foi premiado com a medalha Fields em 1994. Não iremos estudar tal problema, porém

estudaremos um pouco de uma das técnicas relacionadas para resolver tal problema (cf. [27, Chapter 9]). Essa técnica é chamada de *Métodos de Lie (em grupos)* e a usaremos para limitar a classe de nilpotência de grupos finitamente gerados de expoente 3.

A referência [18] é um site que conta a história e avanços desse problema, fica a recomendação ao leitor interessado.

3.1 O anel de Lie de um grupo

A fim de estudar os grupos de expoente 3 faremos uso dos chamados *Métodos de Lie*. Grosso modo, associaremos um grupo a um anel de Lie de sorte que a estrutura do grupo e do anel de Lie se relacionem.

Note que todo grupo abeliano A possui estrutura natural de $\mathbb{Z}$-módulo, basta definir

$$na = \underbrace{a + a + \cdots + a}_{\text{n vezes}}.$$

para quaisquer $n \in \mathbb{Z}$ e $a \in A$.

Para construir o anel de Lie associado usaremos a série central inferior do grupo. Considere então cada fator $L_i(G) = \gamma_i(G)/\gamma_{i+1}(G)$ como um $\mathbb{Z}$-módulo e defina o $\mathbb{Z}$-módulo $L(G)$ como a soma direta dos $L_i(G)$, ou seja,

$$L(G) = L_1(G) \oplus L_2(G) \oplus \cdots \oplus L_n(G) \oplus \cdots.$$

Para definir um produto de Lie em $L(G)$ consideraremos primeiramente elementos $a \in L_i(G)$ e $b \in L_j(G)$ e depois estenderemos linearmente para $L(G)$.

Assim, tome $a = g\gamma_{i+1}(G) \in L_i(G)$ e $b = h\gamma_{j+1}(G) \in L_j(G)$ e defina

$$[a,b] = [g,h]\gamma_{i+j+1}(G).$$

Para ver que essa definição faz sentido usaremos o seguinte fato.

Proposição 3.1. ([19, Lemma 2.1.9]) Seja G um grupo. Então $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$ para tdo $i, j \geq 1$.

Note que a Proposição 3.1 garante que $[g,h] \in \gamma_{i+j}(G)$ e também que $[\cdot,\cdot]$ não depende dos representantes das classes. Ademais, temos que $[a,b] \in L_{i+j}(G)$.

Resta verificar que esse produto satisfaz os axiomas desejados, basicamente, veremos como as propriedades dadas na Proposição 1.2 se traduzem para o anel de Lie associado.

- (Linearidade) É suficiente verificar que

$$[a+b,c] = [a,c] + [b,c]$$

quando $a,b \in L_i(G)$, $c \in L_j(G)$. Começaremos escrevendo $a = g\gamma_{i+1}(G)$, $b = h\gamma_{i+1}(G)$, $c = z\gamma_{j+1}(G)$. Em grupos, a Proposição 1.2 garante que

$$[gh,z] = [g,z]^h[h,z],$$

que se traduz como

$$\begin{aligned}[a+b,c] = [gh,z]\gamma_{i+j+1}(G) &= [g,z]^h[h,z]\gamma_{i+j+1}(G) \\ &= [g,z]^h\gamma_{i+j+1}(G)[h,z]\gamma_{i+j+1}(G) \\ &= [g,z]\gamma_{i+j+1}(G)[h,z]\gamma_{i+j+1}(G) \\ &= [a,c]+[b,c].\end{aligned}$$

Pois como $[[g,z],h] \in \gamma_{2i+j}(G) \subseteq \gamma_{i+j+1}(G)$ temos $[[g,z],h]\gamma_{i+j+1}(G) = \gamma_{i+j+1}(G)$ e portanto

$$[g,z]^h\gamma_{i+j+1}(G) = [g,z]\gamma_{i+j+1}(G)$$

.

Analogamente provamos que $[a,b+c] = [a,b]+[a,c]$ para $a \in L_i(G)$ e $b,c \in L_j(G)$.

- ($[a,a] = 0$) Para um elemento qualquer $a = a_1 + a_2 \cdots + a_n + \cdots$ em $L(G)$, temos

$$[a,a] = \sum_{i,j\geq 1} [a_i,a_j].$$

Portanto é suficiente verificar que $[a_i,a_i] = 0$ e que $[a_i,a_j] = -[a_j,a_i]$. Para a primeira igualdade, observe que $[a_i,a_i] = [g_i,g_i]\gamma_{2i+1}(G) = \gamma_{2i+1}(G) = 0$. Para verificar a segunda, note que

$$[a_i,a_j] = [g_i,h_j]\gamma_{i+j+1}(G) = [h_j,g_i]^{-1}\gamma_{i+j+1}(G) = -[a_j,a_i].$$

- (Identidade de Jacobi) É suficiente mostrarmos que $[[a,b],c]+[[b,c],a]+[[c,a],b] = 0$ quando $a \in L_i(G)$, $b \in L_j(G)$ e $c \in L_k(G)$. Escreva $a = g\gamma_{i+1}(G)$, $b = h\gamma_{j+1}(G)$ e $c = f\gamma_{k+1}(G)$. Temos que $[[a,b],c],[[b,c],a],[[c,a],b] \in \gamma_{i+j+k+1}(G)$, sendo assim,

mostrar que

$$[[a,b],c]+[[b,c],a]+[[c,a],b]=0,$$

é equivalente a mostrar que

$$[[g,h],f]\cdot[[h,f],g]\cdot[[f,g],h]\gamma_{i+j+k+1}(G)=\gamma_{i+j+k+1}(G).$$

Para tanto, começaremos com a Identidade de Witt (1.2),

$$[[g,h^{-1}],f]^h[[h,f^{-1}],g]^f[[f,g^{-1}],h]^g=1.$$

Trabalharemos com o termo $[[g,h^{-1}],f]^h$. Usando a Proposição 1.2,

$$[[g,h^{-1}],f]^h=[([g,h]^{-1})^{-h^{-1}},f]^h$$

Mas como $[g,h]\in\gamma_{i+j}(G)$, temos que

$$([g,h]^{-1})^{-h^{-1}}\gamma_{i+j+1}(G)=[g,h]^{-1}\mod\gamma_{i+j+1}(G),$$

logo $([g,h]^{-1})^{-h^{-1}}=[g,h]^{-1}u$, onde $u\in\gamma_{i+j+1}(G)$. Substituindo, obtemos:

$$[[g,h^{-1}],f]^h=[[g,h]^{-1}u,f]^h=([[g,h]^{-1},f]^u[u,f])^h=(([[g,h],f]^{-1})^{[h,g]u}[u,f])^h.$$

Note que $[u,f]\in\gamma_{i+j+k+1}(G)$. Além disso

$$([[g,h],f]^{-1})^{[h,g]u}\gamma_{i+j+k+1}(G)=[[g,h],f]^{-1}\gamma_{i+j+k+1}(G).$$

Ou seja, $[[g,h^{-1}],f]^h\gamma_{i+j+k+1}(G)=[[g,h],f]^{-1}\gamma_{i+j+k+1}(G)$. Analogamente, obtemos também que

$$\begin{aligned}[[h,f^{-1}],g]^f&=[h,f^{-1}],g]^{-1}\gamma_{i+j+k+1}(G)\\ [[f,g^{-1}],h]^g&=[f,g^{-1}],h]^{-1}\gamma_{i+j+k+1}(G).\end{aligned}$$

Logo, unindo essas igualdades com a identidade de Witt obtemos

$$\begin{aligned}\gamma_{i+j+k+1}(G)&=[[g,h^{-1}],f]^h[[h,f^{-1}],g]^f[[f,g^{-1}],h]^g\gamma_{i+j+k+1}(G)\\ &=[[g,h],f]\cdot[[h,f],g]\cdot[[f,g],h]\gamma_{i+j+k+1}(G)\end{aligned}$$

Como queríamos.

Exemplo 5. Considere o grupo diedral D_8 de ordem 8, então $\gamma_2(D_8) \cong \mathbb{Z}/2\mathbb{Z}$ e $\gamma_i(D_8) = 1$ para $i \geq 3$. Portanto $L_1(D_8) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $L_2(D_8) \cong \mathbb{Z}/2\mathbb{Z}$ e $L_i(G) = 0$ para $i \geq 3$. Logo

$$L(D_8) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \oplus \mathbb{Z}/2\mathbb{Z}.$$

OBSERVAÇÃO 4. Se G é um grupo de expoente n, então podemos considerar $L(G)$ sobre $\mathbb{Z}/n\mathbb{Z}$ em vez de $\mathbb{Z}$ pois nesse caso os termos da série central inferior são grupos abelianos de expoente dividindo n.

O resultado a seguir trata do anel de Lie associado, perceba sua forte relação com o Teorema de Kostrikin e também com o Problema de Burnside (Capítulo 3).

Teorema 3.2. [27, 2.4.8] Seja G um grupo de expoente p, então o anel de Lie associado tem característica p e satisfaz a $(p-1)$-ésima identidade de Engel.

3.2 Grupos de expoente 2 e 3

O primeiro caso que estudaremos é $(r,2)$. Esse caso é bastante simples pois trataremos de grupos abelianos, como mostra o lema seguinte:

Lema 3.3. Seja G um grupo com expoente 2. Então G é abeliano.

Demonstração. Para todo $x \in G$ temos $x^{-1} = x$, logo

$$xyx^{-1}y^{-1} = xyxy = (xy)^2 = 1.$$

Ou seja $xy = yx$ para quaisquer $x, y \in G$. □

Teorema 3.4. Seja G um grupo r-gerado com expoente 2. Então $|G| \leq 2^r$. Além disso, a cota é atingida se $G = \oplus_{i=1}^{r} \mathbb{Z}/2\mathbb{Z}$.

Demonstração. Pelo lema anterior G é abeliano, dessa forma, se $x_1, \cdots, x_r$ são geradores de G, então todo elemento de G é da forma

$$x_1^{e_1} \ldots x_r^{e_r},$$

onde cada e_i é 0 ou 1. Por um argumento de contagem segue que $|G| \leq 2^r$. □

Note que utilizamos a abelianidade para limitar uma certa "largura" do grupo. Veremos que para expoente 3 e 4 a ideia será basicamente essa. Por fim, para expoente 6, conseguiremos reduzir aos casos de expoente 2 e 3.

Teorema 3.5. Seja G um grupo r-gerado de expoente 3, então G é um 3-grupo finito.

Demonstração. Se G é cíclico, então $|G| \leq 3$. Suponha que G possui pelos menos dois geradores, dessa forma, podemos escrever $G = \langle H, a \rangle$, onde H é um subgrupo $(r-1)$-gerado. Por indução em r, segue que H é finito.

Tome $g \in G$, naturalmente, ou $g \in H$ ou $g \notin H$. Como estamos provando a finitude de G, não precisaremos tratar do primeiro caso, já que H é finito.

No segundo caso, podemos escrever

$$g = h_1 a^{e_1} h_2 a^{e_2} \cdots h_k a^{e_k} h_{k+1}.$$

Onde cada $e_i \in \{1,2\}$ e cada $h_j \in H$. Mostraremos que se $k \geq 3$, então podemos diminuir a largura dessa expressão, dessa forma, obtemos a finitude de G, pois ou $g \in H$ ou

$$g = h_1 a^{e_1} h_2 a^{e_2} h_3.$$

De qualquer forma, existem apenas finitas escolhas para g.

Por hipótese, temos $ahahah = (ah)^3 = 1$, ou seja, $aha = h^{-1}a^{-1}h^{-1}$. Além disso, temos $h^{-1} = h^2$ e $a^{-1} = a^2$, portanto

$$aha = h^2 a^2 h^2.$$

Analogamente, usando que $(a^2h)^3 = 1$, obtemos

$$a^2 h a^2 = h^2 a h^2$$

Assim, se na expressão de g tivermos $e_i = e_{i+1}$ para algum índice i podemos substituir $a^{e_i} h_{i+1} a^{e_{i+1}}$ por $h_{i+1}^2 a^2 h_{i+1}^2$ ou por $h_{i+1}^2 a h_{i+1}^2$, caso $e_i = e_{i+1} = 1$ ou $e_i = e_{i+1} = 2$, respectivamente. Note que assim diminuímos a largura da expressão.

Resta considerar quando isso não acontece, ou seja, quando os e_i e e_{i+1} são sempre distintos. Nesse caso podemos multiplicar $aha = h^2 a^2 h^2$ por a para obter que $aha^2 = h^2 a^2 h^2 a$. Note que essa substituição não altera a largura da expressão, porém trocamos a ordem em que a e a^2 aparecem, dessa forma, podemos reduzir esse caso aos anteriores. □

Esse teorema também nos garante a nilpotência de G, já que G é um 3-grupo finito, além disso, podemos usar os resultados apresentados para limitar a classe de nilpotência de G. Uma consequência desse fato será uma cota ótima para a ordem de G, a fim de comparação, vale ressaltar que para expoente 4 ainda não foi encontrada uma cota ótima.

Teorema 3.6. [Levi-van der Waerden] Seja G um grupo r-gerado de expoente 3, então G é nilpotente de classe no máximo 3. Além disso, $|G| \leq 3^{r+\binom{r}{2}+\binom{r}{3}}$.

Demonstração. Pelo Teorema 3.2 o anel de Lie associado $L(G)$ (sobre $\mathbb{Z}_3$) satisfaz a segunda identidade de Engel, isto é, $[[x,y],y] = 1$ para quaisquer $x,y \in L(G)$, logo, pelo Teorema de Kostrikin (1.42), $L(G)$ é nilpotente de classe no máximo 3, ou seja,

$$[[[a,b],c],d] = 0,$$

para quaisquer $a,b,c,d \in L(G)$. Vamos verificar como essa identidade se traduz para o grupo G. Escrevendo $a = x\gamma_2(G), b = y\gamma_2(G), c = z\gamma_2(G), d = t\gamma_2(G)$, obtemos que

$$[[[x,y],z],t]\gamma_5(G) = 0.$$

Isso significa que $[[[x,y],z],t] \in \gamma_5(G)$ para quaisquer $x,y,z,t \in G$, ou seja, $\gamma_4(G) = \gamma_5(G)$. Mas isso só é possível se $\gamma_4(G) = 1$, pois caso contrário a série central inferior de G não chegaria em 1, contrariando a nilpotência de G.

Dessa forma, mostramos que G é nilpotente de classe no máximo 3, portanto,

$$|G| = |\gamma_1(G)/\gamma_2(G)||\gamma_2(G)/\gamma_3(G)||\gamma_3(G)|.$$

Onde cada um desses grupos é um grupo abeliano de expoente 3, além disso, obtemos a cota requerida pois $\gamma_i(G)/\gamma_{i+1}(G)$ é gerado por $\binom{r}{i}$ elementos, de fato, se $x_1, x_2, \cdots, x_r$ são geradores de G, então

$$\begin{aligned}
\gamma_1(G)/\gamma_2(G) &= \langle x_i\gamma_2(G) \mid 1 \leq i \leq r\rangle, \\
\gamma_2(G)/\gamma_3(G) &= \langle [x_i,x_j]\gamma_3(G) \mid 1 \leq i < j \leq r\rangle, \\
\gamma_3(G) &= \langle [x_i,x_j,x_k] \mid 1 \leq i < j < k \leq r\rangle.
\end{aligned}$$

□

OBSERVAÇÃO 5. Considere F_r o grupo livre de rank r e $N = \langle g^n \mid g \in F_r\rangle \trianglelefteq F_r$. Então o quociente F_r/N é denotado por $B(r,n)$ e é chamado grupo de Burnside r-gerado de expoente n.

O grupo de Burnside $B(r,3)$ de expoente 3 e r-gerado satisfaz $|B(r,3)| = 3^{r+\binom{r}{2}+\binom{r}{3}}$ (cf. [27, Theorem 5.2.1]), ou seja, a cota dada em 3.6 é ótima.

Podemos agora derivar algumas identidades satisfeitas por grupos finitamente gerados de expoente 3.

Proposição 3.7. Seja G um grupo finitamente gerado de expoente 3. Então

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

para quaisquer $x,y,z \in G$.

Demonstração. Novamente temos que o anel de Lie associado $L(G)$ satisfaz a segunda identidade de Engel. Assim, estamos nas condições do Teorema de Kostrikin (1.42), note que isso garante que as identidades desejadas são satisfeitas para $L(G)$, ou seja,

$$[[x,y],z] = [[y,z],x] = [[z,x],y] = -[[y,x],z] = -[[x,z],y] = -[[z,y],x] \pmod{\gamma_4(G)}.$$

Pelo Teorema 3.6, temos $\gamma_4(G) = 1$ e o resultado segue. □

OBSERVAÇÃO 6. Como dito anteriormente, para expoente 5 ainda não há uma resposta para o Problema de Burnside. É natural se perguntar onde a demonstração para expoente 3 falha para expoente 5. Uma possível resposta seria observar que as identidades obtidas para expoente 3 não teriam muita utilidade caso tentássemos aplicar a estratégia para expoente 5, por exemplo, considere o exemplo com poucos geradores: considere $G = \langle a,b \rangle$ um grupo 2-gerado de expoente 5, sendo assim, tomaríamos $H = \langle b \rangle$ e escreveríamos um $g \in G$ como

$$g = h_1 a^{e_1} h_2 a^{e_2} \cdots h_k a^{e_k} h_{k+1}.$$

Onde todo $h_i \in H$ e todo $e_i \in \{1,2,3,4\}$. A identidade $ahahahahah = (ah)^5$ pode ser reescrita como

$$aha = h^4 a^4 h^4 a^4 h^4 a^4 h^4.$$

Porém nesse caso essa identidade aumenta a largura da expressão de g, em contraste com a demonstração para expoente 3.

3.3 Grupos de expoente 4

O caso $(r,4)$ foi resolvido por I.N. Sanov [22], porém, baseamos essa seção nas demonstrações dadas em [19, Chapter 14] e [27, Chapter 6]. O ponto chave da demonstração será usar o seguinte lema.

Lema 3.8. Seja G um grupo de expoente 4. Se existem $H \leq G$ finito e $x \in G$ tal que $G = \langle H,x \rangle$ e $x^2 \in H$, então G é finito.

Demonstração. Como $x^2 \in H$ e $G = \langle H, x\rangle$ podemos escrever um elemento $g \in G$ qualquer como

$$g = h_1 x h_2 x \dots h_n x h_{n+1}, \tag{3.1}$$

onde $h_i \in H$. Diremos que a expressão acima têm largura n.

Mostraremos que todo $g \in G$ possui uma expressão de largura $n \leq |H| + 2$. Dessa forma, G será finito.

Por hipótese, para qualquer $h \in H$ temos $hxhxhxhx = (hx)^4 = 1$. Assim, temos que

$$xhx = h^{-1}x^{-1}h^{-1}x^{-1}h^{-1} = h^{-1}x^3h^{-1}x^3h^{-1},$$

onde usamos que $x^4 = 1$. Como $x^2 \in H$ podemos ainda escrever a igualdade acima como

$$xhx = h^{-1}xh'xh^{-1},$$

onde $h' = x^2h^{-1}x^2 \in H$.

Agora, usaremos isso para reescrever a expressão (3.1) trocando xh_ix por $h_i^{-1}xh'xh_i^{-1}$

$$\begin{aligned} g &= h_1 x h_2 x \dots h_{i-1}(xh_ix)h_{i+1}h_n x h_{n+1} \\ &= h_1 x h_2 x \dots h_{i-2} x h_{i-1}(h_i^{-1}xh'xh_i^{-1})h_{i+1}x\cdots x h_n x h_{n+1} \end{aligned}$$

Usando a associatividade,

$$g = h_1 x h_2 x \dots h_{i-2} x (h_{i-1}h_i^{-1}) x h' x (h_i^{-1}h_{i+1}) x \cdots x h_n x h_{n+1}.$$

Note que a expressão obtida possui a mesma largura da original pois $(h_{i-1}h_i^{-1}), (h_i^{-1}h_{i+1})$ e h' são elementos de H. Na expressão obtida $(i-1)$-ésimo fator de H é $h_{i-1}h_i^{-1}$. Repetindo o mesmo argumento para esse termo obtemos uma nova expressão, de mesma largura, com o $(i-2)$-elemento igual à $h_{i-2}(h_{i-1}h_i)^{-1}$.

Dessa forma, poderíamos trocar h_2 por outros elementos de H sem aumentar a largura. A ideia será contar tais elementos, de maneira geral, trocaríamos h_2 por um elemento da forma

$$\begin{aligned} &h_2,\ h_2h_3^{-1},\ h_2h_4h_3^{-1},\ h_2h_4(h_3h_5)^{-1}, \cdots, \\ &h_2h_4\cdots h_{2s}(h_3h_5\cdots h_{2s-1})^{-1},\ h_2h_4\cdots h_{2s}(h_3h_5\cdots h_{2s+1})^{-1} \end{aligned} \tag{3.2}$$

Onde s é o maior natural tal que $2s+1 < n+1$, ou seja, $2s+1 = n$ se n é ímpar e $2s+1 = n-1$ se n é par. Se $n \geq |H|+3$, então, $2s \geq |H|+1$. Como em 3.2 há $2s$ expressões podemos usar o Princípio da Casa dos Pombos para garantir que duas delas devem ser iguais.

Para terminar a demonstração, repare há dois tipos de elementos em 3.2, aqueles que possuem mais h_i de índice par e os que possuem mais h_i de índice ímpar, iremos considerar as igualdades tendo em vista as combinações possíveis dada essa divisão. Se dois elementos do primeiro tipo coincidem, então

$$h_2h_4\cdots h_{2r}(h_3h_5\cdots h_{2r-1})^{-1} = h_2h_4\cdots h_{2t}(h_3h_5\cdots h_{2t-1})^{-1}.$$

com $r > t$. Logo

$$h_{2t+2}\cdots h_{2r}(h_{2t+1}\cdots h_{2r-1})^{-1} = 1.$$

Mas esse é um dos elementos que aparem ao fazer o processo descrito anteriormente para h_{2r+2}, ou seja, obtemos uma expressão de largura menor. Analogamente, se dois elementos do segundo tipo coincidem, então

$$h_2h_4\cdots h_{2r}(h_3h_5\cdots h_{2r+1})^{-1} = h_2h_4\cdots h_{2t}(h_3h_5\cdots h_{2t+1})^{-1}.$$

Ou se um do primeiro tipo coincide com um do segundo tipo, então

$$h_2h_4\cdots h_{2r}(h_3h_5\cdots h_{2r+1})^{-1} = h_2h_4\cdots h_{2t}(h_3h_5\cdots h_{2t-1})^{-1}.$$

De qualquer forma, obteríamos a mesma conclusão. Dessa forma, para todo $g \in G$, podemos obter uma expressão de largura $n \leq |H| + 2$. □

Teorema 3.9. Seja G um grupo r-gerado com expoente 4. Então G é finito.

Demonstração. A prova será por indução em r. Primeiramente, sejam $x_1, \cdots, x_r$ geradores de G. Se $r = 1$, então $G = \{x_1, x_1^2, x_1^3, x_1^4\}$. Por indução, segue que $H = \langle x_1, \cdots, x_{r-1}\rangle$ é finito, podemos então aplicar o Lema 3.8 considerando H e $x = x_n^2$ para garantir que $K = \langle H, x_n^2\rangle$ é finito. Aplicando novamente o Lema 3.8 para K e $x = x_n$ obtemos que G é finito. □

OBSERVAÇÃO 7. Se G é um grupo r-gerado de expoente 4, então

$$|G| < 2^{\frac{1}{2}(4+2\sqrt{2})^r}.$$

Ao contrário dos casos para expoente 2 e 3 essa cota não é ótima. Por exemplo, o grupo de Burnside $B(2,4)$ satisfaz $|B(2,4)| = 2^{12}$, mas $2^{\frac{1}{2}(4+2\sqrt{2})^2} > 2^{23}$.

Para mais detalhes veja [27, Chapter 6], em particular, [27, Theorem 6.5.1].

3.4 Grupos de expoente 6

A demonstração desse caso é devida aos matemáticos P. Hall e G. Higman. Precisaremos utilizar os resultados para expoente 2 e 3. Além disso, também usaremos o software de Álgebra Computacional GAP (cf. Apêndice A) para provar o lema a seguir, dessa forma sua demonstração será dada na seção A.1.

Lema 3.10. Sejam G um grupo de expoente 6, $x \in G$ um elemento de ordem 2 e $A \subseteq G$ tal que se $a \in A$, então $a^3 = (ax)^2 = 1$. Então $\langle A \rangle$ tem expoente 3.

Para o próximo teorema precisaremos do seguinte resultado

Proposição 3.11. Seja G um grupo finitamente gerado. Se $H \leq G$ tem índice finito, então H é finitamente gerado.

Teorema 3.12. Seja G um grupo r-gerado de expoente 6. Então G é finito.

Demonstração. A ideia da demonstração é considerar subgrupos $P \leq M \leq G$ convenientes de sorte que G/M e P tenham expoente 3 e M/P tenha expoente 2, pois nesse caso temos as seguinte implicações: G/M é finitamente gerado e portanto é finito, assim M é um subgrupo de índice finito de um grupo finitamente gerado e portanto também é finitamente gerado, logo M/P é finitamente gerado e então finito, analogamente P é finitamente gerado e portanto finito. Por fim, como

$$|G| = |G/M|.|M/P|.|P|$$

o grupo G será finito.

Considere então $M = \langle g^3 \mid g \in G \rangle$ e $P = \langle w^2 \mid w \in M \rangle$, é imediato que G/M tem expoente 3 e que M/P tem expoente 2, resta verificarmos que P tem expoente 3. Nesse ponto o Lema 3.10 será fundamental.

Como G tem expoente 6 segue que M tem expoente 2, portanto podemos escrever $w \in M$ como um produto $w = x_1 x_2 \cdots x_k$ de elementos em M de ordem 2. Agora mostraremos que w^2 pode ser escrito como um produto de comutadores da forma $[x,u]$ onde $x,u \in M$ e $x^2 = 1$.

A prova será por indução em k. Se $k = 1$, então $w^2 = 1$ e a afirmação segue. Para $k = 2$ temos $w^2 = x_1 x_2 x_1 x_2 = [x_1, x_2]$, o que verifica a afirmação. Para $k > 2$ podemos escrever $w = x_1 v$, onde $v = x_2 \cdots x_k$. Por indução segue que v^2 é um produto de elementos da forma desejada. Como

$$w^2 = x_1 v x_1 v = [x_1, v^{-1}]v^2,$$

temos que a afirmação é válida para k, como queríamos.

Temos então que P é gerado por elementos da forma $[x,u]$ com $x,u \in M$ e $x^2 = 1$. Mostraremos que esses elementos tem ordem 3. Para tanto escreva $u = x_1 \cdots x_k$ onde cada $x_i \in$

M tem ordem 2. Novamente usaremos indução em k, se $k = 1$, então $[x,u] = [x,x_1] = (xx_1)^2$ e portanto $[x,u]^3 = (xx_1)^6 = 1$. Tomando agora $k > 1$ escreva $u = vx_k$ onde $v = x_1 \cdots x_{k-1}$, temos então

$$\begin{aligned}[x,u] &= [x,vx_k] \\ &= [x,x_k][x,v]^{x_k} \\ &= ([x,x_k]^{x_k}[x,v])^{x_k} \\ &= ([x,x_k]^{-1}[x,v])^{x_k}.\end{aligned}$$

Nesse momento usaremos o Lema 3.10 considerando $A = \{[x,x_k],[x,v]\}$. Por indução, segue que $[x,x_k]^3 = [x,v]^3 = 1$, além disso, uma simples calculação mostra que $([x,x_k]x)^2 = ([x,v]x)^2 = 1$. Assim, podemos aplicar o Lema 3.10 para garantir que $[x,x_k]^{-1}[x,v] \in \langle A \rangle$ tem ordem 3 e, consequentemente, seu conjugado $[x,u]$ também.

Agora, para cada $x \in M$ de ordem 2 defina $A(x) = \{[x,u] \mid u \in M\}$, como demonstramos segue que se $a \in A(x)$, então $a^3 = 1$, além disso temos $x^2 = (ax)^2 = 1$ e portanto podemos aplicar o Lema 3.10 para garantir que $\langle A(x) \rangle$ tem expoente 3. Agora tome $w \in M$, note que

$$\begin{aligned}[x,u]^w &= (x^{-1}x^u)^w \\ &= x^{-w}x^{uw} \\ &= (x^{-1}x^w)^{-1}(x^{-1}x^{uw}) \\ &= [x,w]^{-1}[x,uw],\end{aligned}$$

que é um elemento de $\langle A(x) \rangle$, ou seja, cada $\langle A(x) \rangle$ é normal em M.

Assim, podemos escrever P como um produto de 3-grupos e portanto ele próprio é um 3-grupo. Sendo também um subgrupo de um grupo de expoente 6, segue que P tem expoente 3, o que finaliza a demonstração. □

OBSERVAÇÃO 8. Se G é um grupo r-gerado de expoente 6, então

$$|G| \leq 2^a \cdot 3^{b+\binom{b}{2}+\binom{b}{3}},$$

onde $a = 1 + (r-1)3^{r+\binom{r}{2}+\binom{r}{3}}$ e $b = 1 + (r-1)2^r$. Além disso, o grupo de Burnside $B(r,6)$ de expoente 6 e r-gerado realiza a cota (cf. [27, Theorem 5.3.1]).

Capítulo 4

Representações de grupos

Este capítulo é baseado em [14] e [12], seu objetivo é desenvolvermos a teoria de representações de grupos finitos necessária para entendermos os resultados do artigo [8]. Grosso modo, uma representação pode ser pensada como uma forma concreta de visualizar um grupo abstrato através de um grupo de matrizes.

4.1 Representações e FG-módulos

Denotaremos por $\mathrm{GL}(n,F)$ o grupo das matrizes $n \times n$ invertíveis com entradas em um corpo F.

Definição 4.1. Sejam G um grupo finito e F um corpo. Uma representação de G sobre F é um homomorfismo ρ de G em $\mathrm{GL}(n,F)$, para algum n. Nesse caso, ρ é dita ter grau n.

Observação. Denotaremos $\rho(g)$ por $g\rho$.

Exemplo 6. Qualquer grupo G admite uma representação $\rho : G \to \mathrm{GL}(n,F)$ dada por $g\rho = I_n$, para todo $g \in G$. Em particular, se $n = 1$ então ρ é chamada de representação trivial.

Exemplo 7. Considere $G = \langle a,b : a^4 = b^2 = 1, a^b = a^{-1} \rangle$ o grupo diedral de ordem 8. Definindo $\rho : G \to \mathrm{GL}(2,\mathbb{R})$ por

$$a\rho = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ b\rho = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

obtemos uma representação real de grau 2 de D_8.

Definição 4.2. Sejam $\rho, \phi : G \to \mathrm{GL}(n,F)$ representações do grupo G sobre o corpo F. Se existe uma matriz $T \in \mathrm{GL}(n,F)$ tal que $g\rho = T^{-1}(g\phi)T$, para todo $g \in G$ então dizemos que ρ e ϕ são equivalentes.

Observação. Até o fim desse capítulo todos os grupos serão finitos e todos os espaços vetoriais de dimensão finita.

Uma outra definição importante é a de FG-módulo. Grosso modo, podemos pensar em FG-módulo como um grupo agindo em um espaço vetorial.

Definição 4.3. Sejam V um F-espaço vetorial e G um grupo. Se definirmos uma ação $V \times G \to V$ tal que, para quaisquer $u, v \in V$, $\lambda \in F$ e $g, h \in G$, temos:

1. $v(gh) = (vg)h$
2. $v1 = v$
3. $(\lambda v)g = \lambda(vg)$
4. $(u+v)g = ug + vg$.

Então V é chamado de FG-módulo.

Antes de darmos exemplos é interessante conhecer a relação entre FG-módulos e representações. Primeiramente, note que se V é um FG-módulo, então, dado $g \in G$, a função $v \to vg$ define um endomorfismo de V, dessa forma, fixada uma base $\mathcal{B}$ de V, a matriz associada ao endomorfismo $v \to vg$ será denotada por $[g]_{\mathcal{B}}$. Podemos então enunciar o seguinte teorema:

Teorema 4.4. [14, Theorem 4.4]

1. Se $\rho : G \to \mathrm{GL}(n, F)$ é uma representação do grupo G sobre o corpo F, então o espaço vetorial F^n é um FG-módulo munido da ação definida por $vg = v(g\rho)$, para quaisquer $g \in G$ e $v \in F^n$.
2. Se V é um FG-módulo com base $\mathcal{B}$ então a função $g \to [g]_{\mathcal{B}}$ é uma representação de G sobre F.

Exemplo 8. 1. No Exemplo 7 vimos uma representação real do grupo D_8, o $\mathbb{R}D_8$-módulo associado é o espaço vetorial real $\mathbb{R}^2$ com a multiplicação dada como no Teorema 4.4. Para exemplificar melhor essa construção podemos calcular como os geradores a, b de D_8 agem sobre a base $\mathcal{B} = \{(1,0),(0,1)\}$ de $\mathbb{R}^2$.

$$(1,0)a = (1,0)(a\rho) = (1,0)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (0,1).$$

$$(0,1)a = (0,1)(a\rho) = (0,1)\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = (-1,0).$$

Analogamente temos $(1,0)b = (1,0)$ e $(0,1)b = (0,-1)$. Logo para $(x,y) \in \mathbb{R}^2$ temos $(x,y)a = (-y,x)$ e $(x,y)b = (x,-y)$.

2. Seja $G = S_3$. Se $V = \mathbb{C}^3$ é um espaço vetorial complexo e $\mathcal{B} = \{e_1, e_2, e_3\}$ a base canônica de $\mathbb{C}^3$, então $\mathbb{C}^3$ é um $\mathbb{C}S_3$-módulo se definirmos $e_i g = e_{g(i)}$. Lembre que $S_3 = \langle (12), (123) \rangle$, assim, para calcular a representação associada ao $\mathbb{C}S_3$-módulo é suficiente determinar a imagem de (12) e (123). Note que

$$e_1(12) = e_2,\ e_2(12) = e_1,\ e_3(12) = e_3,$$

$$e_1(123) = e_2,\ e_2(123) = e_3,\ e_3(123) = e_1$$

logo

$$(12) \to \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, (123) \to \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

O Teorema 4.4 nos diz que há uma equivalência entre as definições de FG-módulo e de representação, nessa dissertação optaremos por utilizar majoritariamente a linguagem dos FG-módulos. Considere agora a seguinte definição.

Definição 4.5. Seja V um FG-módulo. Um subespaço W de V é dito ser um FG-submódulo se $wg \in W$ para quaisquer $w \in W$ e $g \in G$.

Exemplo 9. Considere o $\mathbb{C}S_3$-módulo definido no Exemplo 8. O subespaço $U = \langle (1,1,1) \rangle$ é um $\mathbb{C}S_3$-submódulo, de fato, $(1,1,1)(12) = (1,1,1)(123) = (1,1,1)$ e portanto $(1,1,1)g = (1,1,1)$ para qualquer $g \in G$ (note que é suficiente verificar a condição para um conjunto gerador do espaço vetorial).

Além disso, para qualquer FG-módulo V temos que $\{0\}$ e V são FG-submódulos. Assim, faz sentido a seguinte definição.

Definição 4.6. Um FG-módulo V é dito irredutível se seus únicos FG-submódulos são $\{0\}$ e V.

Uma vantagem de conhecer os FG-submódulos de um FG-módulo V é que podemos determinar uma base $\mathcal{B}$ de V cujas matrizes $[g]_{\mathcal{B}}$ dos endomorfismos $v \to vg$ tenham entradas

nulas. De fato, seja U um FG-submódulo de V e $\mathcal{A}$ uma base de U, podemos estender essa base para uma base $\mathcal{B}$ de V. Como $ug \in U$ para qualquer $g \in G$, temos

$$[g]_{\mathcal{B}} = \begin{pmatrix} X & Y \\ 0 & W \end{pmatrix}.$$

Onde X, Y, Z são matrizes.

Em particular, se conseguirmos escrever V como uma soma direta (no sentido de espaço vetorial) onde cada fator é um FG-submódulo de dimensão 1, então existe uma base $\mathcal{B}$ em que cada matriz $[g]_{\mathcal{B}}$ é diagonal. Futuramente veremos que para $\mathbb{C}G$-módulos, onde G é abeliano, sempre temos uma decomposição desse tipo (cf. Proposição 4.17).

4.2 A álgebra de grupo

Dado um grupo G, podemos construir uma álgebra associada a esse grupo que usaremos para determinar todos os FG-submódulos irredutíveis de G quando $F = \mathbb{C}$. Para tanto, considere a seguinte construção.

Definição 4.7. Seja $G = \{g_1, g_2, \ldots, g_n\}$ um grupo. Definimos o espaço vetorial FG sobre F como conjunto das expressões do tipo

$$\lambda_1 g_1 + \lambda_2 g_2 + \cdots + \lambda_n g_n,$$

com $\lambda_1, \ldots, \lambda_n \in F$. A soma é definida como

$$(\sum_{i=1}^{n} \lambda_i g_i) + (\sum_{i=1}^{n} \mu_i g_i) = \sum_{i=1}^{n} (\lambda_i + \mu_i) g_i$$

e a multiplicação por escalar é definida por

$$\lambda (\sum_{i=1}^{n} g_i) = \sum_{i=1}^{n} (\lambda \lambda_i) g_i.$$

Além disso, podemos usar o produto de G para definir uma multiplicação entre os vetores de FG da seguinte forma

$$(\sum_{i=1}^{n} \lambda_i g_i)(\sum_{i=1}^{n} \mu_i g_i) = \sum_{i=1}^{n} \sum_{j=1}^{n} \lambda_i \mu_j (g_i g_j)$$

Além disso, podemos mostrar que essa multiplicação satisfaz

1. $r(st) = (rs)t$;
2. $(\lambda r)s = \lambda(rs) = r(\lambda s)$;
3. $(r+s)t = rt + st$ e $t(r+s) = tr + ts$;
4. $r1 = 1r = r$;
5. $r0 = 0r = 0$.

Para todos $r, s, t \in$ FG e $\lambda \in F$. O espaço vetorial FG munido desse produto é uma álgebra com identidade $1e$, onde e é a identidade do grupo G e 1 a identidade do corpo F (escreveremos apenas 1 para denotar 1e). Tal álgebra é chamada de álgebra de grupo sobre F (associada ao grupo G).

Observação 2. Uma notação conveniente para um elemento da álgebra de grupo é

$$\sum_{g \in G} \lambda_g g$$

Assim, escrevemos, por exemplo,

$$(\sum_{g \in G} \lambda_g g)(\sum_{h \in G} \mu_h h) = \sum_{g,h \in G} \lambda_g \mu_h (gh)$$

Definição 4.8. Seja FG a álgebra de grupo de G sobre F. O grupo G age de forma natural em FG da seguinte forma

$$(\sum_{g \in G} \lambda_g g)h = \sum_{g \in} \lambda_g (gh).$$

Com essa ação FG é um FG-módulo chamado de FG-módulo regular. A representação associada é chamada de representação regular.

Observação 3. Note que FG age de forma natural em um FG-módulo V. De fato, dado $v \in V$ e $(\sum_{g \in G} \lambda_g g) \in$ FG podemos definir

$$v(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} \lambda_g (vg),$$

com as seguintes propriedades

1. $v(rs) = (vr)s$;
2. $(\lambda v)r = \lambda(vr) = v(\lambda r)$;

3. $(u+v)r = ur+vr$

4. $v(r+s) = vr+vs$;

5. $v1 = v$;

6. $v0 = 0$ e $0r = 0$.

Para todos $u, v \in V$, $r, s \in \mathrm{FG}$ e $\lambda \in F$.

Essa observação nos permite descrever FG-módulos irredutíveis, como mostra a proposição seguinte.

Proposição 4.9. Sejam W um FG-módulo irredutível e $w \in W$ não-nulo. Então $W = \{wr \mid r \in \mathrm{FG}\}$.

Demonstração. A Observação 3 garante que $\{wr \mid r \in \mathrm{FG}\}$ é um FG-submódulo não-nulo de W, assim como W é irredutível, segue que $W = \{wr \mid r \in \mathrm{FG}\}$. □

4.3 FG-homomorfismos

Usualmente denotamos por $\phi(x)$ a imagem do elemento x pela função ϕ, para manter uma certa compatibilidade com a notação utilizada também escreveremos $x\phi$ para denotar $\phi(x)$.

Definição 4.10. Sejam V e W FG-módulos. Uma transformação linear $\phi : V \to W$ é chamada de FG-homomorfismo se $(vg)\phi = (v\phi)g$ para quaisquer $v \in V$ e $g \in G$.

Além disso, se ϕ for invertível, então ϕ é chamada FG-isomorfismo e os FG-módulos V e W são ditos isomorfos, esse último caso denotaremos por $V \cong W$.

Proposição 4.11. Se $\phi : V \to W$ é um FG-homomorfismo entre os FG-módulos V e W, então $\mathrm{Ker}(\phi)$ é um FG-submódulo de V e $\mathrm{Im}(\phi)$ é um FG-submódulo de W.

Demonstração. Como ϕ é uma transformação linear então $\mathrm{Ker}(\phi)$ é um subespaço de V e $\mathrm{Im}(\phi)$ é um subespaço de W. Tome $v \in \mathrm{Ker}(\phi)$, então $(vg)\phi = (v\phi)g = 0\phi = 0$ para todo $g \in G$, logo $vg \in \mathrm{Ker}(\phi)$ e portanto $\mathrm{Ker}(\phi)$ é FG-submódulo de V. Agora, tomando $w \in \mathrm{Im}(\phi)$, existe $v \in V$ tal que $v\phi = w$, logo $(vg)\phi = (v\phi)g = wg \in \mathrm{Im}(\phi)$ para todo $g \in G$. Portanto $\mathrm{Im}(\phi)$ é um FG-submódulo de W. □

Considere agora os seguintes lemas. O primeiro deles nos dá um exemplo de FG-homomorfismo.

Lema 4.12. Sejam V um FG-módulo e $U_1, U_2, \ldots, U_n$ uma coleção de FG-submódulos de V tais que

$$V = U_1 \oplus U_2 \oplus \cdots \oplus U_n.$$

Assim, dado $v \in V$, existem únicos $u_1, u_2, \ldots, u_n$ tais que $v = u_1 + u_2 + \cdots + u_n$. Então, para cada $i = 1, 2, \ldots, n$, a função $\pi_i : V \to U_i$, dada por $v\pi_i = u_i$, é um FG-homomorfismo.

Demonstração. A verificação da linearidade de π_i é imediata. Para ver que π_i é um FG-homomorfismo tome $v = u_1 + \cdots + u_n \in V$ e $g \in G$ quaisquer, assim

$$(vg)\pi_i = u_i g = (v\pi_i)g.$$

□

O próxima lema é um fato básico de Álgebra Linear.

Lema 4.13. ([14, Proposition 2.32]) Sejam V um espaço vetorial e $\pi : V \to V$ uma transformação linear tal que $\pi^2 = \pi$. Então $V = \mathrm{Im}(\pi) \oplus \mathrm{Ker}(\pi)$.

Observação 4. Uma transformação linear π tal que $\pi = \pi^2$ é chamada projeção. As transformações do Lema 4.12 são projeções.

Agora enunciaremos uma versão do *Teorema de Maschke*[1], que será um dos resultados mais importantes desse texto.

Teorema 4.14 (Maschke)**.** Sejam G um grupo finito e V um FG-módulo, onde $F \in \{\mathbb{R}, \mathbb{C}\}$. Se U é um FG-submódulo de V, então existe um FG-submódulo W de V tal que $V = U \oplus W$.

Demonstração. Tome W_0 um subespaço de V tal que $V = U \oplus W_0$. Dado $v \in V$ escreva $v = u + w$ onde $u \in U$ e $w \in W_0$. Defina $\pi : V \to V$ por $\pi(v) = u$, assim π é uma projeção com $Ker(\pi) = W_0$ e $Im(\pi) = U$. A partir de π defina $\phi : V \to U$ por

$$v\phi = \frac{1}{|G|} \sum_{g \in G} vg\pi g^{-1}$$

Note que ϕ é uma transformação linear pois é a soma de compostas de transformações lineares, além disso, mostraremos que ϕ é um FG-homomorfismo, para tanto tome $h \in G$,

[1] Heinrich Maschke (1853-1908)

temos

$$\begin{aligned}(vh)\phi &= \frac{1}{|G|}\sum_{g\in G}(vh)g\pi g^{-1}\\ &= \frac{1}{|G|}\sum_{g\in G}v(hg)\pi g^{-1}\\ &= \frac{1}{|G|}\sum_{x\in G}vx\pi x^{-1}h\\ &= (\frac{1}{|G|}\sum_{x\in G}vx\pi x^{-1})h\\ &= (v\phi)h\end{aligned}$$

Onde fizemos $hg = x$ e utilizamos que x percorre G quando g percorre G. Portanto ϕ é um FG-homomorfismo. Como $u\pi = u$ e U é um FG-submódulo temos

$$\begin{aligned}u\phi &= \frac{1}{|G|}\sum_{g\in G}ug\pi g^{-1}\\ &= \frac{1}{|G|}\sum_{g\in G}ugg^{-1}\\ &= \frac{1}{|G|}\sum_{g\in G}u\\ &= \frac{1}{|G|}|G|u = u\end{aligned}$$

Em particular, como $\mathrm{Im}(\phi)\subseteq U$, temos $(v\phi)\phi = v\phi$, portanto ϕ é uma projeção. Além disso, segue que $\mathrm{Im}(\phi) = U$. Logo, pelo Lema 4.13 temos $V = U\oplus W$ onde $W = \mathrm{Ker}(\phi)$. □

Corolário 4.15. Seja V um FG-módulo, onde $F\in\{\mathbb{R},\mathbb{C}\}$. Então $V = U_1\oplus\cdots\oplus U_n$ onde cada U_i é um FG-submódulo irredutível de V.

Um resultado que complementa bem o Teorema de Machske é o *Lema de Schur*[2], pois trata de FG-módulos irredutíveis. Para tanto, precisaremos nos restringir aos $\mathbb{C}G$-módulos, dessa forma, até o fim da seção trataremos apenas esses casos.

Teorema 4.16 (Lema de Schur)**.** Sejam V e W ambos $\mathbb{C}G$-modulos irredutíveis.

1. Se $\phi : V\to W$ é um $\mathbb{C}G$-homomorfismo, então ou ϕ é um $\mathbb{C}G$-isomorfismo, ou $v\phi = 0$ para todo $v\in V$

[2]Issai Schur (1875-1941)

2. Se $\phi : V \to V$ é um $\mathbb{C}G$-isomorfismo, então existe $\lambda \in \mathbb{C}$ tal que $v\phi = \lambda v$ para todo $v \in V$.

Demonstração. Primeiramente, suponha que $\phi : V \to W$ é um $\mathbb{C}G$-homomorfismo. Podemos supor que existe $v \in V$ tal que $v\phi \neq 0$, logo $\mathrm{Ker}(\phi) \neq V$, portanto como V é irredutível segue que $\mathrm{Ker}(\phi) = \{0\}$ e assim, ϕ é invertível.

Agora suponha que $\phi : V \to V$ é um $\mathbb{C}G$-isomorfismo. Como V é um $\mathbb{C}$-espaço vetorial segue que ϕ possui um autovalor $\lambda \in \mathbb{C}$. Dessa forma o endomorfismo $(\phi - \lambda I) : V \to V$, dado por $v(\phi - \lambda I) = v\phi - \lambda v$, é um $\mathbb{C}G$-homomorfismo com $\mathrm{Ker}(\phi - \lambda) \neq \{0\}$, como V é irredutível temos $\mathrm{Ker}(\phi - \lambda I) = V$, ou seja, $v\phi - \lambda v = 0$ para todo $v \in V$ e o resultado segue. □

Proposição 4.17. Seja G um grupo abeliano. Se V é um $\mathbb{C}G$-módulo irredutível, então V tem dimensão 1.

Demonstração. Note que para grupos abelianos o endomorfismo de V dado por $v \to vg$ é um $\mathbb{C}G$-homomorfismo, pois $(vh)g = v(hg) = v(gh) = (vg)h$ para todo $h \in G$ e $v \in V$. Pelo Lema de Schur segue que existe $\lambda_g \in \mathbb{C}$ tal que $vg = \lambda_g v$, dessa forma todo subespaço de V é um $\mathbb{C}G$-módulo e como V é irredutível sua dimensão precisa ser 1. □

Com esse resultado podemos determinar todos as representações irredutíveis de um grupo finito abeliano, para tanto, lembremos que um grupo finito abeliano é isomorfo à um produto direto de grupos cíclicos.

Proposição 4.18. Considere o grupo $G = C_{n_1} \times \cdots \times C_{n_m}$. Então G possui exatamente $|G|$ representações irredutíveis.

Demonstração. Denotemos por g_i um gerador de C_{n_i}, dessa forma $G = \langle g_1, \ldots, g_m \rangle$ e para definirmos uma representação de G basta definirmos a imagem de cada g_i. Tendo isso em vista, tomemos λ_i uma raiz n_i-ésima da unidade. Para cada escolha de $\lambda_1, \ldots, \lambda_m$ podemos definir uma representação $\rho_{\lambda_1,\ldots,\lambda_m}$ de G dada por $g_i\rho = \lambda_i$, assim, se $g = g_1^{i_1} \cdots g_m^{i_m}$, então

$$g\rho = \lambda_1^{i_1} \cdots \lambda_m^{i_m}.$$

Cada $\rho_{\lambda_1,\ldots,\lambda_m}$ possui grau 1 e portanto é irredutível, além disso, como os elementos de $\mathbb{C}$ comutam, a única representação equivalente a $\rho_{\lambda_1,\ldots,\lambda_m}$ é ela própria. Assim, existem existem $n_1 \cdots n_m = |G|$ representações desse tipo. Para terminar, considere ρ uma representação irredutível qualquer de G, da Proposição 4.17 segue que ρ tem grau 1, portanto existem $\lambda_1, \ldots, \lambda_m$ satisfazendo $g_i\rho = \lambda_i$ e, como $g_i^{n_1} = 1$, temos que $\lambda_i^{n_i} = 1$ e assim λ_i é uma raiz n_i-ésima da unidade, ou seja, $\rho = \rho_{\lambda_1,\ldots,\lambda_m}$. □

Proposição 4.19. Sejam G um grupo e V um $\mathbb{C}G$-módulo. Dado $g \in G$ existe uma base $\mathcal{B}$ de V tal que a matriz $[g]_{\mathcal{B}}$ é diagonal. Além disso, se $n = o(g)$ então as entradas da diagonal de $[g]_{\mathcal{B}}$ são raízes n-ésimas da unidade.

Demonstração. Defina $H = \langle g \rangle$, temos que V é um $\mathbb{C}H$-módulo. Pelo Lema de Maschke podemos decompor V como soma direta de $\mathbb{C}H$-submódulos irredutíveis U_i, com $i = 1, \ldots, n$. Pela Proposição 4.17 cada U_i tem dimensão 1, dessa forma existe $\lambda_i \in \mathbb{C}$ tal que $u_i g = \lambda_i u_i$ para todo $u_i \in U_i$, além disso, tomando $u_i \neq 0$ temos que λ_i é raíz da unidade, de fato, $u_i = u_i e = u_i g^n = \lambda_i^n u_i$, logo $\lambda_i^n = 1$. Por fim, tomando $\mathcal{B} = \{u_1, u_2, \ldots, u_n\}$ tal que $U_i = \langle u_i \rangle$, temos

$$[g]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

□

Podemos definir o centro da álgebra de grupo de forma totalmente análoga à definição para grupos. Como veremos na próxima proposição, o centro da álgebra de grupo $\mathbb{C}G$ age de forma bastante simples em $\mathbb{C}G$-módulos irredutíveis.

Definição 4.20. Seja G um grupo e $\mathbb{C}G$ sua álgebra de grupo. O centro de $\mathbb{C}G$ é definido como $Z(\mathbb{C}G) = \{z \in \mathbb{C}G \mid zr = rz, \forall r \in \mathbb{C}G\}$.

Exemplo 10. Seja $G = D_8$, então os elementos $e, a^2, b + a^2 b, ab + a^3 b, a + a^3 \in \mathbb{C}G$ estão em $Z(\mathbb{C}G)$. Verificaremos isso apenas para $b + a^2 b$, note que é suficiente mostrarmos que $(b + a^2 b)r = r(b + a^2 b)$ para $r = a$ e $r = b$. Temos

$$(b + a^2 b)a = ba + a^2 ba = a^3 b + a^2 a^3 b = ab + a^3 b = a(b + a^2 b),$$

$$(b + a^2 b)b = b^2 + a^2 = b(b + ba^2) = b(b + a^2 b).$$

Proposição 4.21. Sejam V um $\mathbb{C}G$-módulo irredutível e $z \in Z(\mathbb{C}G)$. Então existe $\lambda \in \mathbb{C}$ tal que $vz = \lambda v$ para todo $v \in V$.

Demonstração. Note que o endomorfismo de V dado por $v \mapsto vz$ é um $\mathbb{C}G$-homomorfismo, uma vez que $(vz)g = v(zg) = v(gz) = (vg)z$ para todo $g \in G$. Sendo V irredutível o Lema de Schur garante que existe $\lambda \in \mathbb{C}$ satisfazendo $vz = \lambda v$. □

Anteriormente comentamos que $\mathbb{C}G$ pode ser usada para determinar todos os $\mathbb{C}G$-módulos irredutíveis de G, o próximo teorema nos mostra isso, mas antes precisaremos de alguns lemas.

Lema 4.22. Sejam V e W dois $\mathbb{C}G$-módulos e $\phi : V \to W$ um $\mathbb{C}G$-homomorfismo. Então existe um $\mathbb{C}G$-submódulo U de V tal que $V = \mathrm{Ker}(\phi) \oplus U$, além disso, $U \cong \mathrm{Im}(\phi)$.

Demonstração. Pelo Teorema de Maschke existe um $\mathbb{C}G$-módulo U de V tal que $V = \mathrm{Ker}(\phi) \oplus U$. Mostraremos que a função $\overline{\phi} : U \to \mathrm{Im}(\phi)$ dada por $u\overline{\phi} = u\phi$ é um $\mathbb{C}G$-isomorfismo.

Note que $\overline{\phi}$ é uma $\mathbb{C}G$-homomorfismo pois herda as propriedades de ϕ. Temos $\mathrm{Ker}(\overline{\phi}) \subseteq \mathrm{Ker}(\phi) \cap U = 0$, além disso, se $w \in \mathrm{Im}(\phi)$, então $w = v\phi$ para algum $v \in V$. Escrevendo $v = k + u$ com $k \in \mathrm{Ker}(\phi)$ e $u \in U$, temos $w = v\phi = k\phi + u\phi = u\overline{\phi} \in \mathrm{Im}(\overline{\phi})$. Assim $U \cong \mathrm{Im}(\overline{\phi}) = \mathrm{Im}(\phi)$. □

Lema 4.23. Sejam V um $\mathbb{C}G$-módulo e $U_1, \ldots, U_n$ uma coleção de $\mathbb{C}G$-submódulos irredutíveis de V tais que $V = U_1 \oplus \cdots \oplus U_n$. Então qualquer $\mathbb{C}G$-submódulo U irredutível de V é $\mathbb{C}G$-isomorfo a algum U_i.

Demonstração. Tomemos $u = u_1 + \cdots + u_n \in U$ não-nulo, assim, para algum $i = 1, \ldots, n$ temos que u_i é não-nulo. Considere π_i a projeção de V em U_i, pelo Lema 4.12, π_i é um $\mathbb{C}G$-homomorfismo. Assim, restringindo π_i ao $\mathbb{C}G$-submódulo U segue pelo Lema de Schur que π_i é um $\mathbb{C}G$-isomorfismo, pois U é irredutível e π_i é não-nulo. □

Teorema 4.24. Seja $\mathbb{C}G$ o $\mathbb{C}G$-módulo regular e escreva $\mathbb{C}G = U_1 \oplus \cdots \oplus U_n$ onde cada U_i é um $\mathbb{C}G$-submódulo irredutível. Então qualquer $\mathbb{C}G$-módulo irredutível W é isomorfo a algum U_i.

Demonstração. Pela Proposição 4.9 segue que $W = \{wz \mid z \in \mathbb{C}G\}$ para algum $w \in W$ não-nulo, dessa forma $\phi : \mathbb{C}G \to W$ dado por $z\phi = wz$ é uma transformação linear sobrejetiva, além disso, ϕ é um $\mathbb{C}G$-homomorfismo pois $(zg)\phi = w(zg) = (wz)g = (z\phi)g$ para todo $g \in G$. Pelo Lema 4.22 existe um $\mathbb{C}G$-submódulo U de V tal que $V = \mathrm{Ker}(\phi) \oplus U$ e $U \cong \mathrm{Im}(\phi) = W$. Como W é irredutível segue que U também é irredutível, logo o Lema 4.23 garante que $U_i \cong U \cong W$ para algum $i = 1, \ldots, n$. □

Uma outra pergunta que podemos fazer é, dado W, quantos U_i existem com $W = U_i$? Veremos que essa quantidade é exatamente $\dim W$, para tanto, precisamos munir o conjunto dos $\mathbb{C}G$-homomorfismos de um grupo com uma estrutura linear.

Definição 4.25. Sejam V e W dois $\mathbb{C}G$-módulos. O conjunto dos $\mathbb{C}G$-homomorfismos é um $\mathbb{C}$-espaço vetorial se definirmos a soma $\phi + \psi$ e produto por escalar $\lambda\phi$ como

$$v(\phi + \psi) = v\phi + v\psi,$$

$$v(\lambda\phi) = \lambda(v\phi).$$

para todo $v \in V$. Denotaremos esse espaço por $\mathrm{Hom}_{\mathbb{C}G}(V,W)$.

O próximo resultado é uma consequência direta do Lema de Schur.

Proposição 4.26. Sejam V e W dois $\mathbb{C}G$-módulos irredutíveis. Então

$$\dim(\mathrm{Hom}_{\mathbb{C}G}(V,W)) = \begin{cases} 1, \text{ se } V \cong W \\ 0, \text{ se } V \ncong W \end{cases}$$

Proposição 4.27. Considere os $\mathbb{C}G$-módulos V e W. Se $\mathrm{Hom}_{\mathbb{C}G}(V,W) \neq \{0\}$, então V e W têm um fator de composição em comum.

Demonstração. Tome $\phi \in \mathrm{Hom}_{\mathbb{C}G}(V,W)$ não-nulo, pelo Teorema de Maschke (4.14) podemos escrever $V = \mathrm{Ker}(\phi) \oplus U$ para algum $\mathbb{C}G$-módulo U. Seja U_1 um $\mathbb{C}G$-submódulo irredutível de U, temos que $U_1\phi \neq \{0\}$, pois $U_1 \cap \mathrm{Ker}\phi = \{0\}$, assim pelo Lema de Schur (4.16), segue que $U_1\phi \cong U_1$, como queríamos. □

Uma outra propriedade interessante é que $\dim(\mathrm{Hom}_{\mathbb{C}G}(V,W))$ é "linear", mais precisamente:

Teorema 4.28. Sejam V e W ambos $\mathbb{C}G$-módulos, escrevendo $V = V_1 \oplus V_2$ e $W = W_1 \oplus W_2$, então

1. $\dim(\mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2)) = \dim(\mathrm{Hom}_{\mathbb{C}G}(V,W_1)) + \dim(\mathrm{Hom}_{\mathbb{C}G}(V,W_2))$.
2. $\dim(\mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W)) = \dim(\mathrm{Hom}_{\mathbb{C}G}(V_1,W)) + \dim(\mathrm{Hom}_{\mathbb{C}G}(V_2,W))$.

Demonstração. 1. Tome $\phi \in \mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2)$ e considere as projeções $\pi_1 : W \to W_1$ e $\pi_2 : W \to W_2$. Como π_1, π_2 são $\mathbb{C}G$-homomorfismos segue que $\phi\pi_1 \in \mathrm{Hom}_{\mathbb{C}G}(V,W_1)$ e $\phi\pi_2 \in \mathrm{Hom}_{\mathbb{C}G}(V,W_2)$, assim, defina

$$\begin{aligned} f : \mathrm{Hom}_{\mathbb{C}G}(V, W_1 \oplus W_2) &\to \mathrm{Hom}_{\mathbb{C}G}(V,W_1) \oplus \mathrm{Hom}_{\mathbb{C}G}(V,W_2) \\ \phi &\mapsto (\phi\pi_1, \phi\pi_2). \end{aligned}$$

Provaremos que f é um isomorfismo, primeiramente note que linearidade de f é imediata. Agora tome $\phi \in \mathrm{Ker}(f)$, assim, $\phi\pi_1 = \phi\pi_2 = 0$. Logo, dado $v \in V$, temos $v\phi = v\phi(\pi_1 + \pi_2) = 0$, ou seja, $v = 0$. Para a sobrejetividade, tome $\phi_1 \in \mathrm{Hom}_{\mathbb{C}G}(V,W_1)$ e $\phi_2 \in \mathrm{Hom}_{\mathbb{C}G}(V,W_2)$, assim (ϕ_1, ϕ_2) é a imagem por f do $\mathbb{C}G$-homomorfismo dado por $v \mapsto v\phi_1 + v\phi_2$, $v \in V$.

2. Considere $\phi \in \mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W)$. Dado $i = 1,2$ defina o $\mathbb{C}G$-homomorfismo $\phi_i : V_i \to W$ dado por $v_i\phi_i = v_i\phi$. Agora defina

$$f : \mathrm{Hom}_{\mathbb{C}G}(V_1 \oplus V_2, W) \to \mathrm{Hom}_{\mathbb{C}G}(V_1, W) \oplus \mathrm{Hom}_{\mathbb{C}G}(V_2, W)$$
$$\phi \mapsto (\phi_1, \phi_2).$$

Se $\phi \in \mathrm{Ker}(f)$, então dado $v = v_1 + v_2 \in V$ segue que $v\phi = (v_1 + v_2)\phi = v_1\phi_1 + v_2\phi_2 = 0$, ou seja, $\phi = 0$. Por outro lado, dados $\psi_1 \in \mathrm{Hom}_{\mathbb{C}G}(V_1, W)$ e $\psi_2 \in \mathrm{Hom}_{\mathbb{C}G}(V_2, W)$ temos (ψ_1, ψ_2) é imagem por f do $\mathbb{C}G$-homomorfismo dado por $v = v_1 + v_2 \mapsto v_1\psi_1 + v_2\psi_2$. Assim, verificamos que f é um isomorfismo.

□

Combinando a Proposição 4.26 e o Teorema 4.28 obtemos o seguinte corolário.

Corolário 4.29. Sejam V e W ambos $\mathbb{C}G$-módulos com W irredutível. Escreva $V = U_1 \oplus \cdots \oplus U_n$ onde cada U_i é um $\mathbb{C}G$-submódulo irredutível de V. Então

$$\dim(\mathrm{Hom}_{\mathbb{C}G}(V, W)) = \dim(\mathrm{Hom}_{\mathbb{C}G}(W, V)) = \#\{U_i \mid U_i \cong W\}.$$

Proposição 4.30. Se V é um $\mathbb{C}G$-módulo, então $\dim(\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G, V)) = \dim V$.

Demonstração. Denote $\dim V = d$ e sejam $v_1, \ldots, v_d$ uma base de V. A partir dessa base construiremos uma base do espaço $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G, V)$. Defina, para cada $i = 1, \ldots, d$, a função $\phi_i : \mathbb{C}G \to V$ por $r\phi_i = v_i r$ para todo $r \in \mathbb{C}G$. Temos que cada ϕ_i está em $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G, V)$. Tome $\phi \in \mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G, V)$, existem $\lambda_i \in \mathbb{C}$ tais que $1\phi = \lambda_1 v_1 + \cdots + \lambda_d v_d$, dessa forma temos

$$r\phi = (1r)\phi = (1\phi)r = (\sum_{i=1}^{d} \lambda_i v_i)r = \sum_{i=1}^{d} \lambda_i v_i r = r(\sum_{i=1}^{d} \lambda_i \phi_i).$$

Logo os $\mathbb{C}G$-homomorfismos ϕ_i, $i = 1, \ldots, d$ geram $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G, V)$. Para verificar que também são linearmente independentes suponha que $\lambda_1\phi_1 + \cdots + \lambda_d\phi_d$ é o $\mathbb{C}G$-homomorfismo identicamente nulo, logo

$$0 = 1(\lambda_1\phi_1 + \cdots + \lambda_d\phi_d) = \lambda_1 v_1 + \cdots + \lambda_d v_d.$$

Ou seja, $\lambda_i = 0$ para $i = 1, \ldots, d$. Portanto $\phi_1, \ldots, \phi_d$ formam uma base do espaço $\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G, V)$ e o resultado segue. □

Agora podemos provar o resultado mais importante dessa seção.

Teorema 4.31. Seja $\mathbb{C}G$ o $\mathbb{C}G$-módulo regular. Escrevendo $\mathbb{C}G = U_1 \oplus \cdots \oplus U_n$ onde cada U_i é um $\mathbb{C}G$-submódulo irredutível de $\mathbb{C}G$. Se U é um $\mathbb{C}G$-módulo irredutível, então

$$\#\{U_i \mid U_i \cong U\} = \dim U.$$

Demonstração. Pela Proposição 4.30 e Corolário 4.29 temos

$$\dim U = \dim(\mathrm{Hom}_{\mathbb{C}G}(\mathbb{C}G, U)) = \#\{U_i \mid U_i \cong U\}.$$

□

Até o momento vimos que existem finitos $\mathbb{C}G$-módulos irredutíveis de um grupo G, além disso, o $\mathbb{C}G$-módulo regular determina todos eles. Nesse contexto, considere a seguinte definição.

Definição 4.32. Dizemos que os $\mathbb{C}G$-módulos irredutíveis $V_1, \ldots, V_n$ formam um conjunto completo de $\mathbb{C}G$-módulos irredutíveis se são dois a dois não-isomorfos e se todo $\mathbb{C}G$-submódulo irredutível U é isomorfo a algum dos V_i.

O seguinte teorema fornece uma relação entre as dimensões de $\mathbb{C}G$-módulos irredutíveis e a ordem de G.

Teorema 4.33. Seja $V_1, \ldots, V_n$ um conjunto completo de $\mathbb{C}G$-módulos irredutíveis. Então

$$\sum_{i=1}^{n} (\dim V_i)^2 = |G|.$$

Demonstração. Segue da definição de conjunto completo de $\mathbb{C}G$-módulos irredutíveis e do Teorema 4.31 que

$$\mathbb{C}G = (\dim V_1 \oplus \cdots \dim V_1) \oplus \cdots \oplus (\dim V_n \oplus \cdots \oplus \dim V_n).$$

Onde cada V_i aparece $d_i = \dim V_i$ vezes, para $i = 1, \ldots, n$. Logo

$$|G| = \dim \mathbb{C}G = \sum_{i=1}^{n} d_i(\dim V_i) = \sum_{i=1}^{n} (\dim V_i)^2.$$

□

4.4 Caracteres

Caracteres são funções que associam elementos de um grupo finito G a um elemento de um corpo F (no nosso caso $F = \mathbb{C}$) de uma forma particular. Grosso modo, os caracteres levam cada $g \in G$ em traços de certas matrizes, dessa forma, são funções bem simples mas que podem determinar muito sobre o grupo e seus FG-módulos.

Definição 4.34. Seja V um $\mathbb{C}G$-módulo. Fixada uma base $\mathcal{B}$ de V defina o caracter de V como a função $\chi : G \to \mathbb{C}$ dada por $\chi(g) = \text{tr}[g]_{\mathcal{B}}$.

Além disso, se tivermos uma representação ρ de G, definimos o caracter de ρ como o caracter do $\mathbb{C}G$-módulo associado, ou seja, $\chi(g) = \text{tr}(g\rho)$.

O caracter não depende da base escolhida, pois se $\mathcal{B}$ e $\mathcal{A}$ são duas bases de V então, dado $g \in G$, existe uma matriz invertível T tal que $[g]_{\mathcal{B}} = T[g]_{\mathcal{A}}T^{-1}$. Logo $\text{tr}[g]_{\mathcal{B}} = \text{tr}[g]_{\mathcal{A}}$, por esse motivo escreveremos apenas $[g]$ em algumas ocasiões.

Ademais, $\mathbb{C}G$-módulos isomorfos possuem o mesmo caracter, de fato, suponha que ϕ seja um $\mathbb{C}G$-isomorfismo entre V e W. Dada uma base $\mathcal{B} = \{v_1, \ldots, v_n\}$ de V podemos considerar a base $\mathcal{C} = \{v_1\phi, \ldots, v_n\phi\}$ de W de forma que $[g]_{\mathcal{B}} = [g]_{\mathcal{C}}$.

Exemplo 11. Considere o $\mathbb{C}S_3$-módulo do Exemplo 8, temos

$$\chi((1,2)) = \text{tr}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 1,\ \chi((1,2,3)) = \text{tr}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = 0$$

Definição 4.35. Seja G um grupo. Então:

1. Dizemos que χ é um caracter de G se χ é o caracter de algum $\mathbb{C}G$-módulo.
2. Dizemos que χ é um caracter irredutível de G se χ é o caracter de um $\mathbb{C}G$-módulo irredutível.
3. O grau do caracter é definido como a dimensão do seu $\mathbb{C}G$-módulo associado. Caracteres de grau 1 são ditos lineares.

Observação. Ao identificarmos $\text{GL}(1,\mathbb{C})$ e $\mathbb{C}^*$ podemos identificar também um caracter linear χ à sua representação associada ρ, tendo em vista que $g\rho = [\lambda]$ e assim $\chi(g) = \lambda$. Faremos, em geral, essa identificação.

Agora daremos algumas propriedades básicas de caracteres.

Proposição 4.36. Sejam χ o caracter de um $\mathbb{C}G$-módulo V e $g, h \in G$. Então:

1. Se $h \in g^G$ então $\chi(h) = \chi(g)$.
2. $\chi(1) = \dim V$
3. $\chi(g)$ é uma soma de raízes n-ésimas da unidade, onde $n = o(g)$.
4. $\chi(g^{-1}) = \overline{\chi(g)}$.

Demonstração. 1. Como $h \in g^G$ existe $x \in G$ tal que $h = x^{-1}gx$, portanto $\chi(h) = \chi(x^{-1}gx) = \operatorname{tr}([x^{-1}gx]) = \operatorname{tr}([x]^{-1}[g][x]) = \operatorname{tr}[g]$.

2. Temos $v1 = v$ para todo $v \in V$, logo $[1] = I_m$ onde $m = \dim V$ e daí $\chi(1) = \operatorname{tr}[1] = \dim V$.

3. Pela Proposição 4.19 temos que existe uma base $\mathcal{B}$ de V tal que

$$[g]_{\mathcal{B}} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_m \end{pmatrix},$$

onde cada λ_i é uma raiz n-ésima da unidade, portanto, $\chi(g) = \operatorname{tr}[g]_{\mathcal{B}} = \lambda_1 + \cdots + \lambda_m$.

4. Escolha uma base $\mathcal{B}$ como no item anterior. Temos

$$[g^{-1}]_{\mathcal{B}} = \begin{pmatrix} \lambda_1^{-1} & & 0 \\ & \ddots & \\ 0 & & \lambda_m^{-1} \end{pmatrix}.$$

Onde cada λ_i é uma raíz da unidade, assim, $\lambda_i^{-1} = \overline{\lambda_i}$. Logo $\chi(g^{-1}) = \lambda_1^{-1} + \cdots + \lambda_m^{-1} = \overline{\lambda_1} + \cdots + \overline{\lambda_m} = \overline{\lambda_1 + \cdots + \lambda_m} = \overline{\chi(g)}$.

□

Proposição 4.37. Seja V um $\mathbb{C}G$-módulo. Se V é escrito como uma soma direta de $\mathbb{C}G$-submódulos $U_1, \ldots, U_n$, então χ é a soma dos caracteres dos $\mathbb{C}G$-submódulos $U_1, \ldots, U_n$.

Demonstração. Podemos construir uma base $\mathcal{B}$ de V unindo bases $\mathcal{B}_i$ de U_i, com $i = 1, \ldots, n$. Assim, para qualquer $g \in G$

$$[g]_{\mathcal{B}} = \begin{pmatrix} [g]_{\mathcal{B}_1} & & 0 \\ & \ddots & \\ 0 & & [g]_{\mathcal{B}_n} \end{pmatrix}.$$

Logo $\chi(g) = \mathrm{tr}[g]_{\mathcal{B}} = \mathrm{tr}[g]_{\mathcal{B}_1} + \cdots \mathrm{tr}[g]_{\mathcal{B}_n} = \chi_1(g) + \cdots + \chi_n(g)$, onde χ_i é o carácter de U_i, $i = 1, \ldots, n$. □

Definição 4.38. Sejam G um grupo e $\mathbb{C}G$ sua álgebra de grupo. Então o caracter de $\mathbb{C}G$ será chamado de caracter regular e denotado por χ_{reg}.

Tal caracter é bastante simples, como mostra a próxima proposição.

Proposição 4.39. Seja χ_{reg} o caracter regular de G. Então

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

Demonstração. Considere a base $\mathcal{B}$ de $\mathbb{C}G$ formada pelos elementos $g_1, \ldots, g_n$ do grupo G. Como vimos $\chi(1) = \dim(\mathbb{C}G) = |G|$. Agora considere $1 \neq g \in G$. O *ii* termo da matrix $[g]_{\mathcal{B}}$ é zero pois $g_i g \neq g_i$ para todo $i = 1, \ldots, n$, assim $\chi(g) = \mathrm{tr}[g]_{\mathcal{B}} = 0$. □

4.5 Produto interno de caracteres

Começaremos relembrando a definição de produto interno.

Definição 4.40. Seja V um $\mathbb{C}$-espaço vetorial. Um produto interno sobre V é uma função $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ satisfazendo as condições abaixo para quaisquer $u, v, w \in V$ e $\lambda \in \mathbb{C}$:

1. $\langle \lambda u + v, w \rangle = \lambda \langle u, w \rangle + \langle v, w \rangle$.
2. $\langle u, v \rangle = \overline{\langle v, u \rangle}$.
3. $\langle u, u \rangle > 0$, se $u \neq 0$.

Em especial, dado um grupo finito G, consideraremos V como o espaço das funções $\phi : G \to \mathbb{C}$ munido da soma e produto por escalar usuais. Note que o conjunto dos caracteres de G está contidos em V.

Proposição 4.41. Seja G um grupo e $\phi, \psi : G \to \mathbb{C}$ funções. Defina

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g) \overline{\psi(g)}.$$

Então $\langle \cdot, \cdot \rangle$ definido como acima é um produto interno no espaço das funções de G em $\mathbb{C}$.

Antes de continuar precisaremos de algumas definições.

Definição 4.42. Seja χ um caracter de um grupo G. Defina os conjuntos:

- $Z(\chi) = \{g \in G \mid |\chi(g)| = \chi(1)\}$.
- $\mathrm{Ker}(\chi) = \{g \in G \mid \chi(g) = \chi(1)\}$.

Caso $\mathrm{Ker}(\chi) = \{1\}$ dizemos que χ é fiel.

OBSERVAÇÃO 9. Se χ é um carácter de G associado à representação ρ, então $\mathrm{Ker}(\chi) = 1$ se, e somente se, $\mathrm{Ker}(\rho) = 1$, ou seja, χ é fiel se, e somente se, ρ é fiel (cf. [11, Lemma 2.19]).

Dado um subgrupo H de G, note que um $\mathbb{C}G$-módulo V é também um $\mathbb{C}H$-módulo. Assim, podemos definir o seguinte.

Definição 4.43. Se V é um $\mathbb{C}G$-módulo e $H \leqslant G$, então o $\mathbb{C}H$-módulo associado é denotado por $V \downarrow H$. Nesse contexto, se χ é o caracter de V, então o caracter de $V \downarrow H$ é denotado por $\chi \downarrow H$.

Note que o caracter $\chi \downarrow H$ coincide com $\chi|_H$.

Lema 4.44. Seja χ um caracter de um grupo G e ρ a representação associada. Então

1. $Z(\chi) = \{g \in G \mid g\rho = \lambda I, \text{ para algum } \lambda \in \mathbb{C}\}$.
2. $Z(\chi)$ é um subgrupo de normal G.
3. $\chi \downarrow Z(\chi) = \chi(1)\psi$, onde ψ é um caracter linear (e portanto irredutível) de $Z(\chi)$. Além disso ψ é fiel se χ é fiel.
4. Se χ é fiel, então $Z(G) = Z(\chi)$.

Demonstração. 1. Seja $g \in G$ com $g\rho = \lambda I$ para algum λ unitário, então $|\chi(g)| = \chi(1)|\lambda| = \chi(1)$. Reciprocamente, suponha $g \in Z(\chi)$, pela Proposição 4.19 existe uma base de $\mathbb{C}^n$ tal que

$$g\rho = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Onde cada λ_i é uma raiz m-ésima da unidade. Assim, $n = \chi(1) = \chi(g) = \lambda_1 + \cdots + \lambda_n$.

Nesse ponto utilizaremos uma propriedade de números complexos que garante que, para quaisquer $z_1, \ldots, z_n \in \mathbb{C}$, vale a seguinte desigualdade

$$|z_1 + \cdots + z_n| \leq |z_1| + \cdots + |z_n|.$$

Além disso, a igualdade é satisfeita somente quando todos os z_i's coincidem. Note que para $\lambda_1, \ldots, \lambda_n$ a igualdade acima é satisfeita pois $|\lambda_i| = 1$ para todo $i = 1, \ldots, n$, garantindo então que $\lambda_1 = \cdots = \lambda_n = \lambda$, ou seja, $g\rho = \lambda I$.

2. Temos $1 \in Z(\chi)$ pois $1\rho = I$. Tome $g, h \in Z(\chi)$, temos $(xy^{-1})\rho = (x\rho)(y\rho)^{-1} = (\lambda_g I)((\lambda_y)^{-1} I) = (\lambda_g \lambda_y^{-1})I$, como $|\lambda_g \lambda_y^{-1}| = |\lambda_g||\lambda_y^{-1}| = 1$ segue que $xy^{-1} \in Z(\chi)$, assim, $Z(\chi)$ é um subgrupo de G. Para a normalidade basta lembrar que χ é constante nas classes de conjugação de G.

3. Considere a função $\psi : Z(\chi) \mapsto \mathbb{C}^*$ que associada cada $g \in Z(\chi)$ ao valor $\psi(g)$ que satisfaz $g\rho = \psi(g)I$. Note que ψ é um homomorfismo pois

$$(xy)\rho = (x\rho)(y\rho) = \psi(g)I\psi(y)I = \psi(g)\psi(y)I,$$

para quaisquer $x, y \in Z(\chi)$. Ou seja, ψ é uma representação (de grau 1) de $Z(\chi)$, além disso, para todo $g \in Z(\chi)$, temos $\chi(g) = \mathrm{tr}(g\rho) = \mathrm{tr}(\psi(g)I) = \chi(1)\psi(g)$, ou seja, $\chi \downarrow Z(\chi) = \chi(1)\psi$. Por fim, se $\psi(g) = \psi(1) = 1$ para $g \in Z(\chi)$, então $\chi(g) = \chi(1)$, logo ψ é fiel se χ for fiel.

4. Como $Z(G)$ é abeliano, dado $x \in Z(G)$, então $x\rho = \lambda I$ para algum $\lambda \in \mathbb{C}$, assim $x \in Z(\chi)$. Reciprocamente, fixe $x \in Z(\chi)$. Dado $g \in G$, os itens anteriores garantem que

$$\chi([g,x]) = \chi(g^{-1}g^x) = \chi(1)\psi(g^{-1}g^x) = \chi(1)\psi(g)^{-1}\psi(g) = \chi(1).$$

Logo $[g,x] \in \mathrm{Ker}(\chi) = 1$ para qualquer $g \in G$, ou seja, $x \in Z(G)$, como queríamos.

□

Lema 4.45. Sejam G um grupo e χ um caracter de G. Se $H \leq G$, então

$$\langle \chi \downarrow H, \chi \downarrow H \rangle \leq [G : H]\langle \chi, \chi \rangle.$$

Demonstração. O resultado é uma consequência direta de $\langle \cdot, \cdot \rangle$ ser um produto interno, de fato,

$$|H|\langle \chi \downarrow H, \chi \downarrow H \rangle = \sum_{h \in H} |\chi(h)|^2 \leq \sum_{g \in G} |\chi(g)|^2 = |G|\langle \chi, \chi \rangle.$$

□

Teorema 4.46. Seja χ um caracter irredutível de um grupo finito G. Então $\chi(1)^2 \leq [G : Z(\chi)]$.

Demonstração. Pelo Lema 4.44 temos $\chi \downarrow Z(\chi) = \chi(1)\psi$ onde ψ é um caracter linear de $Z(\chi)$. Logo

$$\langle \chi \downarrow Z(\chi), \chi \downarrow Z(\chi) \rangle = \chi(1)^2 \langle \psi, \psi \rangle = \chi(1)^2.$$

Por outro lado, pelo Lema 4.45 temos $\langle \chi \downarrow Z(\chi), \chi \downarrow Z(\chi) \rangle \leq [G : Z(\chi)] \langle \chi, \chi \rangle = [G : Z(\chi)]$. Assim

$$\chi(1)^2 \leq [G : Z(\chi)].$$

□

Corolário 4.47. Seja χ um caracter irredutível de um grupo finito G. Então $\chi(1)^2 \leq [G : Z(G)]$.

Demonstração. Basta ver que $Z(G) \leq Z(\chi)$, assim $\chi(1)^2 \leq [G : Z(\chi)] \leq [G : Z(G)]$. □

Nesse ponto estudaremos as consequências de decompor a álgebra de grupo de uma certa forma, assim, considere a seguinte hipótese.

Hipótese 4.1. Sejam G um grupo e $\mathbb{C}G$ sua álgebra de grupo. Suponha que $\mathbb{C}G = W_1 \oplus W_2$ onde W_1 e W_2 são $\mathbb{C}G$-submódulos que não possuem fator de composição em comum. Além disso, escreva $1 = e_1 + e_2$ onde $e_1 \in W_1$ e $e_2 \in W_2$.

A ideia por trás da decomposição $1 = e_1 + e_2$ acima é que o termo e_1 possui duas expressões que, quando comparadas, fornecerão uma relação fundamental envolvendo caracteres.

Proposição 4.48. Assuma a Hipótese 4.1. Então, para quaisquer $w_1 \in W_1$ e $w_2 \in W_2$, temos

$$w_2 e_1 = 0, \quad w_1 e_2 = 0, \quad w_1 e_1 = w_1, \quad w_2 e_2 = w_2.$$

Demonstração. Como W_1 e W_2 não possuem fator de composição em comum, os homomorfismos $w_1 \mapsto w_1 e_2$ e $w_2 \mapsto w_2 e_1$, onde $w_1 \in W_1$ e $w_2 \in W_2$, precisam ser triviais, provando assim as duas primeiras igualdades, para as outras duas note que

$$w_i = w_i 1 = w_i(e_1 + e_2) = w_i e_i,$$

para $i = 1, 2$. □

Corolário 4.49. Assuma a Hipótese 4.1. Então

$$e_1^2 = e_1, \quad e_2^2 = e_2, \quad e_2 e_1 = e_1 e_2 = 0.$$

Demonstração. Tome $w_1 = e_1$ e $w_2 = e_2$ na Proposição 4.48. □

Proposição 4.50. Assuma a Hipótese 4.1. Seja χ o caracter de W_1, então

$$e_1 = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g$$

Demonstração. Fixado $x \in G$, defina o endomorfismo θ de $\mathbb{C}G$ dado por $w\theta = we_1x^{-1}$. A demonstração consistirá em calcular de duas formas expressões para o traço de θ.

Primeiramente calcularemos $\mathrm{tr}\theta$ quando restrito à W_1 e W_2, para tanto usaremos a Proposição 4.48. Tomando $w_1 \in W_1$, temos $w_1\theta = w_1e_1x^{-1} = w_1x^{-1}$, já tomando $w_2 \in W_2$, obtemos $w_2\theta = w_2e_1x^{-1} = 0$.

Logo θ possui traço 0 quando restrito à W_2. Já restrito à W_1 vemos que θ é da forma $w_1 \mapsto w_1x^{-1}$, ou seja, possui traço igual à $\chi(x^{-1})$. Como $\mathbb{C}G = W_1 \oplus W_2$ segue que $\mathrm{tr}\theta = \chi(x^{-1})$.

Por outro lado, escreva

$$e_1 = \sum_{g \in G} \lambda_g g.$$

Assim θ é soma de endomorfismos θ_g dados por $w \mapsto \lambda_g(wgx^{-1})$ para todo $g \in G$. Como $\mathrm{tr}\theta_g = \lambda_g\chi_{\mathrm{reg}}(gx^{-1})$ a Proposição 4.39 garante que $\mathrm{tr}\theta_g = |G|$ se $g = x$ e $\mathrm{tr}\theta_g = 0$ se $g \neq x$.

Obtemos então $\mathrm{tr}\theta = \lambda_g|G|$, combinando as duas expressões obtidas segue que $\lambda_g|G| = \chi(g^{-1})$, substituindo na expressão de e_1 obtemos

$$e_1 = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g.$$

□

Corolário 4.51. Seja W_1 o $\mathbb{C}G$-módulo da Hipótese 4.1 e χ seu caracter. Então

$$\langle \chi, \chi \rangle = \chi(1).$$

Demonstração. A ideia da demonstração é calcular o coeficiente de 1 em e_1^2 de duas formas distintas. Primeiramente, o Corolário 4.49 garante que $e_1^2 = e_1$ e portanto $\lambda_1 = \dfrac{\chi(1)}{|G|}$.

Por outro lado, temos

$$e_1^2 = \left(\frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g\right)\left(\frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g\right) = \left(\frac{1}{|G|^2} \sum_{g \in G} \chi(g^{-1})\chi(g)\right)1 + \cdots.$$

Daí

$$\frac{\chi(1)}{|G|} = \frac{1}{|G|^2}\sum_{g\in G}\chi(g^{-1})\chi(g) = \frac{\langle\chi,\chi\rangle}{|G|}.$$

□

Teorema 4.52. Considere os $\mathbb{C}G$-módulos irredutíveis e não-isomorfos U e V com caracteres χ e ψ, respectivamente. Então

$$\langle\chi,\chi\rangle = 1$$
$$\langle\chi,\psi\rangle = 0.$$

Demonstração. Pela Proposição 4.31 a álgebra de grupo $\mathbb{C}G$ pode ser escrita como $\mathbb{C}G = U_1 \oplus \cdots \oplus U_n$ onde cada U_i é irredutível e, além disso, a quantidade de U_i isomorfos à U é $m = \dim U$. Suponha, sem perda de generalidade, que $U_1, \ldots, U_m$ são isomorfos à U.

A fim de utilizar a Hipótese 4.1 defina $W = U_1 \oplus \cdots \oplus U_m$ e $Z = U_{m+1} \oplus \cdots \oplus U_n$, dessa forma, W e Z não possuem fator de composição em comum, como desejado. Note que o caracter de W é $m\chi$, assim, o Corolário 4.50 garante que $\langle m\chi, m\chi\rangle = m\chi(1) = m^2$, pois $m = \dim U = \chi(1)$. Por outro lado, usando linearidade, temos $\langle m\chi, m\chi\rangle = m^2\langle\chi,\chi\rangle$. Igualando as expressões obtemos $\langle\chi,\chi\rangle = 1$.

Para obtermos a segunda igualdade defina Y como a soma dos U_i que são isomorfos a U ou a V, novamente, defina Z como a soma dos U_i restantes. Como o caracter de Y é $m\chi + l\psi$, onde $l = \dim V$, o Corolário 4.51 garante que $\langle m\chi + l\psi, m\chi + l\psi\rangle = m\chi(1) + l\psi(1)$. Por outro lado

$$\langle m\chi + l\psi, m\chi + l\psi\rangle = m^2\langle\chi,\chi\rangle + l^2\langle\psi,\psi\rangle + mn\langle\chi,\psi\rangle.$$

Sabemos que $\chi(1) = m$ e $\psi(1) = n$, ademais, pelo o que acabamos de provar, $\langle\chi,\chi\rangle = \langle\psi,\psi\rangle = 1$, fazendo as substituições e igualando as expressões obtemos $\langle\chi,\psi\rangle = 0$.

□

4.6 Elevações de caracteres

Os caracteres de um grupo G se comportam bem quando passamos para algum quociente G/N ou mesmo quando passamos de um quociente G/N para o grupo G. Nessa seção exploraremos essa ideia com o objetivo de estudar os caracteres lineares de um grupo. Também estudaremos o processo de restrição de um caracter à um subgrupo de G.

Proposição 4.53. Sejam G um grupo, $N \triangleleft G$ e $\widetilde{\chi}$ um caracter de G/N. Então a função $\chi : G \to \mathbb{C}$, dada por, $\chi(g) = \widetilde{\chi}(gN)$ é um caracter de G. Ademais, $\widetilde{\chi}$ e χ possuem o mesmo grau.

Demonstração. Seja $\widetilde{\rho} : G/N \to \mathrm{GL}(n,\mathbb{C})$ a representação associada ao caracter $\widetilde{\chi}$, defina $\rho : G \to \mathrm{GL}(n,\mathbb{C})$ por $\rho = \widetilde{\rho} \circ \pi$, onde π é a projeção canônica de G em G/N. Temos que ρ é um homomorfismo, portanto, uma representação de G. Se χ for o caracter associada à ρ, então

$$\chi(g) = \mathrm{tr}(g\rho) = \mathrm{tr}((gN)\widetilde{\rho}) = \widetilde{\chi}(gN).$$

Por fim, temos $\chi(1) = \widetilde{\chi}(N)$, ou seja, χ e $\widetilde{\chi}$ possuem o mesmo grau. □

Definição 4.54. Sejam G um grupo, $N \triangleleft G$ e $\widetilde{\chi}$ um caracter de G/N, o caracter de G definido por $\chi(g) = \widetilde{\chi}(gN)$ é chamado de levantamento de $\widetilde{\chi}$.

O processo de levantamento de caracteres nos dá uma bijeção entre os caracteres de G/N e certos caracteres de G.

Proposição 4.55. Sejam G um grupo finito, χ um caracter de G e $\rho : G \to \mathrm{GL}(n,\mathbb{C})$ a representação associada. Então $\mathrm{Ker}(\chi) = \mathrm{Ker}(\rho)$, em particular, $\mathrm{Ker}(\chi)$ é um subgrupo de G.

Demonstração. Se $g \in \mathrm{Ker}(\rho)$, então $\chi(g) = \mathrm{tr}(g\rho) = \mathrm{tr}(I_n) = n = \chi(1)$, ou seja, $g \in \mathrm{Ker}(\chi)$. Por outro lado, tome $g \in \mathrm{Ker}(\chi)$, pela Proposição 4.19 existe uma base de $\mathbb{C}^n$ tal que

$$g\rho = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Onde cada λ_i é uma raiz m-ésima da unidade. Assim, $n = \chi(1) = \chi(g) = \lambda_1 + \cdots + \lambda_n$. Logo, temos

$$|\lambda_1 + \cdots + \lambda_n| = n = |\lambda_1| + \cdots + |\lambda_n| = n$$

e, como feito na demonstração do Lema 4.44, segue que $\chi(g) = \lambda_1 n$, já que todos os λ_i coincidem.

Por fim, como $g \in \mathrm{Ker}(\chi)$ e $\chi(1) = n$, temos $\chi(1) = \lambda_1\chi(1)$, assim $\lambda_1 = 1$ e portanto $g\rho = I$. Ou seja, $g \in \mathrm{Ker}(\rho)$. □

Agora podemos enunciar a construção dual à apresentada na Proposição 4.53.

Proposição 4.56. Sejam G um grupo, $N \triangleleft G$ e χ um caracter de G com $N \subseteq \mathrm{Ker}(\chi)$. Então a função $\widetilde{\chi} : G \to \mathbb{C}$ dada por $\widetilde{\chi}(gN) = \chi(g)$ é um caracter de G/N. Ademais, χ e $\widetilde{\chi}$ possuem o mesmo grau.

Demonstração. Seja $\rho : G \to \mathrm{GL}(n,\mathbb{C})$ a representação associada ao caracter χ, defina $\widetilde{\rho} : G/N \to \mathrm{GL}(n,\mathbb{C})$ por $(gN)\widetilde{\rho} = g\rho$. Note que $\widetilde{\rho}$ está bem definida pois se gh é outro representante da classe lateral gN, então

$$(ghN)\widetilde{\rho} = (gh)\rho = (g\rho)(h\rho) = g\rho = (gN)\widetilde{\rho}.$$

Afirmamos que $\widetilde{\rho}$ é uma representação. De fato, para quaisquer $gN, xN \in G/N$ temos

$$(gNxN)\widetilde{\rho} = (gxN)\widetilde{\rho} = (gx)\rho = (g\rho)(x\rho) = (gN)\widetilde{\rho}(xN)\widetilde{\rho}.$$

Por fim, o caracter $\widetilde{\chi}$ associado à $\widetilde{\rho}$ satisfaz

$$\widetilde{\chi}(gN) = \mathrm{tr}((gN)\widetilde{\rho}) = tr(g\rho) = \chi(g).$$

Para todo $g \in G$. Em particular $\widetilde{\chi}(N) = \chi(1)$. □

Nesse ponto é interessante sintetizar os últimos resultados, além disso, também é possível mostrar que o levantamento de caracteres “preserva a irredutibilidade". Esse é o conteúdo da próxima proposição.

Proposição 4.57. Sejam G um grupo e $N \triangleleft G$. O processo de levantamento dos caracteres de G/N define um bijeção entre os caracteres $\widetilde{\chi}$ de G/N e os caracteres χ de G tais que $N \subseteq \mathrm{Ker}(\chi)$. Ademais, $\widetilde{\chi}$ é irredutível se, e somente se, χ também é.

Demonstração. Em virtude das proposições 4.53 e 4.56 é suficiente provar que $\widetilde{\chi}$ é irredutível se, e somente se, χ é irredutível.

Para tanto, considere V um subespaço de $\mathbb{C}^n$, se ρ e $\widetilde{\rho}$ são as representações associadas aos caracteres χ e $\widetilde{\chi}$ respectivamente, então dado $v \in V$ temos $v(g\rho) = v((gN)\widetilde{\rho})$ para todo $g \in G$. Ou seja, V é $\mathbb{C}G$-submódulo, se e somente se, V é $\mathbb{C}(G/N)$-submódulo, em particular, χ é irredutível, se e somente se, $\widetilde{\chi}$ é irredutível. □

O levantamento de caracteres funciona especialmente bem quando consideramos o subgrupo derivado G', o próximo resultado tem como objetivo explorar esse caso particular, pois suas consequências serão necessárias mais a frente.

Proposição 4.58. Seja G um grupo. Então o processo de levantamento define uma bijeção entre os caracteres lineares de G e os caracteres irredutíveis de G/G'. Em particular, G possui $|G/G'|$ caracteres lineares.

Demonstração. Como G/G' é abeliano, a Proposição 4.17 garante que todo caracter $\widetilde{\chi}$ irredutível de G/G' tem grau 1, dessa forma, o levantamento χ de $\widetilde{\chi}$ é um caracter linear de G.

Por outro lado, note que se χ é um caracter linear de G, então $G' \leq \mathrm{Ker}(\chi)$. De fato, seja $[g,h]$ um comutador qualquer de G, temos

$$\chi([g,h]) = \chi(g^{-1}h^{-1}gh) = \chi(g)^{-1}\chi(h)^{-1}\chi(g)\chi(h) = 1,$$

pois χ leva G em um grupo abeliano. Ademais, cada caracter linear de G é também irredutível e portanto é associado à um caracter irredutível de G/G'.

Por fim, pela Proposição 4.18, G/G' possui $|G/G'|$ caracteres irredutíveis, dessa forma G possui $|G/G'|$ caracteres irredutíveis. □

4.7 Inteiros algébricos

Nessa seção exploraremos uma certa conexão dos caracteres com a Teoria dos Números, para tanto, assumiremos alguns resultados sobre inteiros algébricos. Para uma referência veja [14, Chapter 22].

Definição 4.59. Um número complexo λ é dito ser um inteiro algébrico se λ é raiz de um polinômio não-nulo com coeficientes inteiros da forma $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$.

Equivalentemente, $\lambda \in \mathbb{C}$ é um inteiro algébrico se é autovalor de uma matriz com coeficientes inteiros.

A próxima proposição é uma junção dos resultados 22.2, 22.3 e 22.4 da referência [14].

Proposição 4.60.

1. Se λ e μ são inteiros algébricos, então $\lambda + \mu$ e $\lambda\mu$ são inteiros algébricos.
2. Se $\lambda \in \mathbb{C}$ é uma raiz da unidade, então λ é inteiro algébrico.
3. Se $\lambda \in \mathbb{Q}$ é um inteiro algébrico, então $\lambda \in \mathbb{Z}$.

Proposição 4.61. Se χ é um caracter de um grupo G, então $\chi(g)$ é inteiro algébrico para todo $g \in G$.

Demonstração. Segue da Proposição 4.60 e do fato de $\chi(g)$ ser soma de raízes da unidade. □

Definição 4.62. Sejam G um grupo e C uma classe de conjugação de G. Então o elemento $\overline{C} = \sum_{g \in C} g \in \mathbb{C}G$ é chamado soma de classe.

Proposição 4.63. Sejam G um grupo e C uma classe de conjugação de G. Então a soma de classe $\overline{C}$ está em $Z(\mathbb{C}G)$.

Demonstração. Suponha que C é composta dos elementos $g^{y_1}, \ldots, g^{y_n}$ para algum $g \in G$, assim $\overline{C} = \sum_{i=1}^{n} g^{y_i}$. Dado $h \in G$ temos

$$\overline{C}^h = \sum_{i=1}^{n} (g^{y_i})^h = \overline{C}.$$

Pois conjugar por h define uma bijeção da classe C nela mesma. Assim, $\overline{C}$ comuta com todo elemento de G e portanto com todo elemento de $\mathbb{C}G$. □

Lema 4.64. Sejam G um grupo, $g \in G$ e $C = g^G$. Considere U um $\mathbb{C}G$-módulo irredutível com caracter χ. Então

$$u\overline{C} = \lambda u,\ u \in U,$$

onde

$$\lambda = |C| \frac{\chi(g)}{\chi(1)}.$$

Demonstração. Como $\overline{C} \in Z(\mathbb{C}G)$ a Proposição 4.21 garante que existe $\lambda \in \mathbb{C}$ satisfazendo $u\overline{C} = \lambda u$ para todo $u \in U$, ou seja, se $\mathcal{B}$ for uma base de U, então o endomorfismo

$$u \mapsto u\overline{C} = \sum_{x \in C} ux$$

tem, por um lado, traço

$$\sum_{x \in C} \chi(x).$$

E por outro lado tem traço $\lambda\chi(1)$. Como χ é constante em C podemos ainda escrever

$$\lambda\chi(1) = |C|\chi(g).$$

Como desejado. □

Teorema 4.65. Sejam G um grupo e χ um caracter irredutível de G. Então para todo $g \in G$

$$\lambda = |g^G| \frac{\chi(g)}{\chi(1)}$$

é um inteiro algébrico.

Demonstração. Tome $g \in G$, mostraremos que λ é autovalor de uma matriz com coeficientes inteiros, para tanto considere o endomorfismo de $\mathbb{C}G$ dado por $r \mapsto r\overline{C}$, onde $C = g^G$. Sejam $g_1, \ldots, g_n$ os elementos de G, então g_i é levado em $\sum_{x \in C} g_i x$, ou seja, a matriz associada a esse endomorfismo possui coeficientes inteiros, por fim, o Lema 4.64 garante que

$$\lambda = |x^G| \frac{\chi(g)}{\chi(1)}$$

é autovalor desse automorfismo, ou seja, λ é inteiro algébrico. □

Lema 4.66. Sejam χ um caracter do grupo G e $x \in G$. Então

$$\sum_{g \in G} x^g = |C_G(x)| \overline{C},$$

onde $C = x^G$.

Demonstração. O Lema é consequência do seguinte fato. Se x^g e x^h são dois conjugados de x em G, então $x^g = x^h$ se, e somente se, $g = ch$ com $c \in C_G(x)$. □

Proposição 4.67. Seja χ um caracter irredutível do grupo G. Então para quaisquer $g, h \in G$ temos

$$\chi(g)\chi(h) = \frac{\chi(1)}{|G|} \sum_{z \in G} \chi(gh^z).$$

Demonstração. Pelo Lema 4.66 temos

$$\sum_{z \in G} gh^z = g \sum_{z \in G} h^z = g|C_G(h)|\overline{C},$$

onde $C = h^G$. Usando o Lema 4.64 podemos ainda reescrever

$$\sum_{z \in G} gh^z = |C_G(h)| \frac{|C|\chi(h)}{\chi(1)} g = \frac{|G|\chi(h)}{\chi(1)} g.$$

Dessa forma obtemos

$$\sum_{z \in G} \chi(gh^z) = \frac{|G|\chi(h)}{\chi(1)} \chi(g).$$

Equivalentemente,

$$\frac{\chi(1)}{|G|}\sum_{z\in G}\chi(gh^z)=\chi(g)\chi(h).$$

□

Lema 4.68. Tome $x,y\in G$, então a relação definida em G por

$$x\sim y \text{ se, e somente se, existe } z\in Z(G) \text{ tal que } x\in (yz)^G.$$

é uma relação de equivalência. Além disso a classe de equivalência de $x\in G$ é da forma $\overline{x}=\{x^g z \mid g\in G, z\in Z(G)\}$.

Demonstração. Verificaremos as condições necessárias para $\sim$ ser uma relação de equivalência

- $x\sim x$ pois $x\in (x1)^G$.
- Se $x\sim y$, então $x=y^g z$ para certos $g\in G, z\in Z(G)$, equivalentemente $y=x^{g^{-1}}z$, assim $y\sim x$.
- Se $x\sim y$ e $y\sim z$, então $x=y^g r$ e $y=z^h s$ com $g,h\in G$ e $r,s\in Z(G)$. Portanto $x=y^{gh}rs$, ou seja, $x\sim z$.

□

Teorema 4.69. Sejam G um grupo e χ um caracter irredutível de G. Então $\chi(1)\mid [G:Z(\chi)]$.

Demonstração. Começaremos supondo que $\mathrm{Ker}(\chi)=1$, nesse caso, $Z(\chi)=Z(G)$ pelo Lema 4.44. Considere a relação $\sim$ definida anteriormente. Afirmamos que $|\chi|$ é constante nas $\sim$-classes, ou seja, que $|\chi(x)|=|\chi(x^g z)|$ para quaisquer $x,g\in G$ e $z\in Z(G)$. Note primeiramente que $|\chi(x^g z)|=|\chi((xz)^g)|=|\chi(xz)|$. Pela Proposição 4.67 temos

$$\chi(x)\chi(z)=\frac{\chi(1)}{|G|}\sum_{y\in G}\chi(xz^y)=\frac{\chi(1)}{|G|}\sum_{y\in G}\chi(xz)=\chi(1)\chi(xz),$$

pois $z\in Z(G)$. Agora pelo Lema 4.44 temos que $\chi(z)=\chi(1)\psi(z)$ onde ψ é um caracter linear fiel de $Z(\chi)=Z(G)$. Assim $\chi(x)\chi(z)=\chi(1)\chi(x)\psi(z)$, substituindo na expressão acima obtemos $\chi(xz)=\chi(x)\psi(1)$, como $|\psi(z)|=1$ segue que $|\chi(x)|=|\chi(xz)|$, como queríamos.

Considere $\mathscr{C}_1,\ldots,\mathscr{C}_r$ as $\sim$-classes em que χ não se anula, temos

$$|G|=\sum_{g\in G}\chi(g)^2=\sum_{i=1}^{r}|\mathscr{C}_i|\chi(g_i)^2.$$

onde g_i é um representante de $\mathscr{C}_i$.

Mostraremos agora que $|\mathscr{C}_i| = |g_i^G||Z(G)|$, como podemos escrever

$$\mathscr{C}_i = \left\{ yz \mid y \in g_i^G, z \in Z(G) \right\}$$

é suficiente provar que todos os elementos $yz \in \mathscr{C}$ são distintos, para tanto suponha $y_1z_1 = y_2z_2$ onde $y_1, y_2 \in g_i^G$ e $z_1, z_2 \in Z(G)$. Assim temos

$$\chi(y_1)\psi(z_1) = \chi(y_2)\psi(z_2),$$

mas $\chi(y_1) = \chi(y_2) = \chi(g_i) \neq 0$, logo $\psi(z_1) = \psi(z_2)$. Como ψ tem grau 1, então ψ é um homomorfismo, juntamente com ψ ser fiel, obtemos que $z_1 = z_2$ e portanto, $y_1 = y_2$.

Logo, denotando por $\lambda_i = |g_i^G| \dfrac{\chi(g_i)}{\chi(1)}$, temos

$$\begin{aligned} |G| &= \sum_{i=1}^{r} |g_i^G||Z(G)|\chi(g_i)^2 \\ &= \sum_{i=1}^{r} |g_i^G||Z(G)|\chi(g_i)\chi(g_i^{-1}) \\ &= \sum_{i=1}^{r} |Z(G)|\chi(1)\lambda_i\chi(g_i^{-1}). \end{aligned}$$

Portanto

$$\frac{[G : Z(G)]}{\chi(1)} = \sum_{i=1}^{r} \lambda_i \chi(g_i^{-1}).$$

O lado esquerdo da igualdade é um racional, já o lado direito, pelo o que foi visto, é um inteiro algébrico, assim, concluímos que $\dfrac{[G : Z(G)]}{\chi(1)}$ é um inteiro.

Para o caso geral, considere o quociente $\overline{G} = G/\mathrm{Ker}(\chi)$ e o caracter $\overline{\chi}$ de $\overline{G}$ associado à χ. Note que $\overline{\chi}$ é fiel, pois se $\overline{\chi}(g\mathrm{Ker}(\chi)) = \overline{\chi}(\mathrm{Ker}(\chi))$, então $\chi(g) = \chi(1)$ e daí $g \in \mathrm{Ker}(\chi)$, ou seja, $g\mathrm{Ker}(\chi) = \mathrm{Ker}(\chi)$. Logo obtemos que

$$\frac{[\overline{G} : Z(\overline{G})]}{\overline{\chi}(\mathrm{Ker}(\chi))}$$

é um inteiro. Como $\overline{\chi}(\mathrm{Ker}(\chi)) = \chi(1)$ e

$$[\overline{G} : Z(\overline{G})] \mid [G : Z(G)]$$

segue que $\frac{[G:Z(G)]}{\chi(1)}$ é inteiro. □

Corolário 4.70. Sejam G um grupo e χ um caracter irredutível de G. Então $\chi(1) \mid [G:Z(G)]$.

Demonstração. Basta usar que $Z(G) \leq Z(\chi)$ e portanto $\chi(1) \mid [G:Z(\chi)] \mid [G:Z(G)]$. □

Sintetizaremos no próximo resultado as relações entre o grau de um carácter irredutível e o índice do centro do grupo dadas no Corolário 4.47 e no Corolário 4.70

Corolário 4.71. Se χ é um caracter irredutível de G. Então $\chi(1) \mid [G:Z(G)]$ e $\chi(1)^2 \leq [G:Z(G)]$.

Capítulo 5

Largura de comutadores em grupos

Todos os resultados desse capítulo, salvo menção do contrário, são do artigo [8].

5.1 Comutadores e caracteres

A primeira relação que veremos entre largura e caracteres é o seguinte teorema, que foi conjecturado por W. Burnside e demonstrado por P. X. Gallagher (cf. [13, Theorem 1]).

Teorema 5.1 (Critério de Burnside-Gallagher)**.** Sejam G um grupo finito, $x \in G'$ e $\chi_1 \ldots, \chi_n$ os caracteres irredutíveis de G. Então x não é um produto de k comutadores se, e somente se,

$$\sum_{i=1}^{n} \frac{1}{\chi_i(1)^{2j-1}} \chi_i(x) = 0,$$

para todo $j = 0, \ldots, k$.

Agora considere algumas definições que serão úteis para o próximo resultado.

Definição 5.2. Sejam G um grupo e n um natural. Definimos:

- $m(G) = |\{\chi(1) \mid \chi \in \mathrm{Irr}(G)\}|$, onde $\mathrm{Irr}(G)$ é o conjunto dos caracteres irredutíveis de G.
- o número dos divisores de n, denotado por $d(n)$.
- o número de divisores primos de n, contando multiplicidade, por $\rho(n)$.

Ou seja, se $p_1^{a_1} \cdots p_m^{a_m}$ é a fatoração prima de n, então

$$d(n) = (a_1 + 1).\cdots(a_m + 1)$$

$$\rho(n) = a_1 + \cdots + a_m.$$

O próximo teorema fornecerá a conexão entre a largura e os caracteres irredutíveis de um grupo, para sua demonstração precisaremos do seguinte lema que trata sobre o determinante de certas matrizes.

Lema 5.3. Sejam $\lambda_1, \lambda_2, \ldots, \lambda_k$ números complexos e

$$M = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^k & \lambda_2^k & \ldots & \lambda_k^k \end{pmatrix}.$$

Então,

$$\det(M) = \prod_{1 \leq j < i \leq k} (\lambda_i - \lambda_j)$$

.

Demonstração. A demonstração será por indução sobre k. Para $k = 2$ o resultado é válido pois $\det(M) = \lambda_2 - \lambda_1$.

Agora suponha o resultado válido para $k-1$. Considere a operação elementar que consiste em trocar a i-ésima linha pela i-ésima linha somada com a $(i-1)$-ésima linha multiplicada por λ_1. Podemos aplicar essa operação para de $i = k$ até $i = 2$, como não alteramos o determinante de M obtemos

$$\begin{aligned}
\det(M) &= \begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & \lambda_2-\lambda_1 & \dots & \lambda_k-\lambda_1 \\ 0 & \lambda_2(\lambda_2-\lambda_1) & \dots & \lambda_k(\lambda_k-\lambda_1) \\ . & . & \dots & . \\ 0 & \lambda_2^{k-1}(\lambda_2-\lambda_1) & \dots & \lambda_k^{k-1}(\lambda_k-\lambda_1) \end{vmatrix} \\
&= 1 \cdot \begin{vmatrix} \lambda_2-\lambda_1 & \dots & \lambda_k-\lambda_1 \\ \lambda_2(\lambda_2-\lambda_1) & \dots & \lambda_k(\lambda_k-\lambda_1) \\ . & \dots & . \\ \lambda_2^{k-1}(\lambda_2-\lambda_1) & \dots & \lambda_k^{k-1}(\lambda_k-\lambda_1) \end{vmatrix} \\
&= \prod_{i=2}^{k}(\lambda_i-\lambda_1) \cdot \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \lambda_2 & \lambda_3 & \cdots & \lambda_k \\ . & . & . & . \\ \lambda_2^{k-1} & \lambda_3^{k-1} & \cdots & \lambda_k^{k-1} \end{vmatrix}
\end{aligned}$$

Por fim, a hipótese de indução garante que $\det(M) = \prod_{1\le j<i\le k}(\lambda_i-\lambda_j)$. □

Teorema 5.4. Seja G um grupo finito. Então $\lambda(G) < m(G)$.

Demonstração. A base da demonstração será aplicar o Critério de Burnside-Gallagher com $k = m(G)-1$. Antes disso, defina $m = m(G)$ e seja $f_1,\dots,f_m$ os diferentes graus dos caracteres irredutíveis de G. Podemos supor $f_1 = 1$. Defina também $\lambda_i = f_i^{-2}$ para $i = 1,\dots,m$. Agora, para cada i defina $\phi_i : G \to \mathbb{C}$ por

$$\phi_i = \sum \chi(1)\chi$$

onde os caracteres presentes em ϕ_i são tais que $\chi(1) = f_i$.

Tome $x \in G'$. Pelo Critério de Burnside-Gallagher x não é um produto de $k = m-1$ comutadores se, e somente se,

$$\sum_{\chi\in\mathrm{Irr}(G)} \frac{1}{\chi(1)^{2j-1}}\chi(x) = 0 \tag{5.1}$$

para todo $j = 0,\dots,k$. Com as definições estabelecidas no início da demonstração podemos escrever (5.1) como

$$\sum_{i=1}^{m} \lambda_i^j \phi_i(x) = 0,$$

para $j = 0, \ldots, k$. Assim, $x \in G'$ não é um produto de k comutadores se, e somente se,

$$\sum_{i=1}^{m} \lambda_i^j a_i = 0,$$

para $j = 0, \ldots, k$, onde $a_i = \phi_i(x)$. As equações acima definem um sistema homogêneo de m equações em m incógnitas. Note que o determinante da matriz associada é não-nulo, de fato, pelo Lema 5.3, o determinante

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ \lambda_1 & \lambda_2 & \ldots & \lambda_k \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_1^k & \lambda_2^k & \ldots & \lambda_k^k \end{vmatrix} = \prod_{1 \leq l < h \leq k} (\lambda_h - \lambda_j).$$

é não-nulo pois os λ_i são dois a dois distintos. Dessa forma, esse sistema possui apenas solução trivial, em particular, $a_1 = \phi_1(x) = 0$. Por outro lado, ϕ_1 é a soma dos caracteres lineares de G. Denote por L o conjunto dos caracteres lineares de G. Usando o Teorema 4.58 temos

$$\phi_1(x) = \sum_{\chi \in L} \chi(x) = \sum_{\overline{\chi} \in \mathrm{Irr}(G/G')} \overline{\chi}(xG') = \sum_{\overline{\chi} \in \mathrm{Irr}(G/G')} 1 = |G/G'|.$$

Assim, chegamos a um absurdo supondo que $x \in G'$ não pode ser escrito como um produto de $k = m - 1$ comutadores, ou seja, $\lambda(G) \leqslant m - 1$. □

Note que o ponto chave da demonstração é conseguir transformar um problema envolvendo largura em solucionar um sistema linear homogêneo com determinante não-nulo. Para o próximo teorema é interessante considerar o lema a seguir.

Lema 5.5. Seja G um grupo com $|G/Z(G)| = n$. Então G possui um subgrupo H finitamente gerado satisfazendo:

- $G' = H'$.
- $G/Z(G) \cong H/Z(H)$.

Demonstração. Por hipótese existem $x_1,\ldots,x_n$ tais que todo elemento $g \in G$ é produto de algum x_i por um elemento em $Z(G)$. Dessa forma $G = HZ(G)$ onde $H = \langle x_1,\ldots,x_n\rangle$. Por um lado, é imediato que $H' \subseteq G'$. Por outro lado, tome um comutador arbitrário $[g,h]$ de G. Podemos escrever $g = x_i z_1$ e $h = x_j z_2$ para algum $1 \leq i,j \leq n$ e $z_1, z_2 \in Z(G)$. Dessa forma,

$$[g,h] = [x_i z_1, x_j z_2] = [x_i, x_j] \in H'.$$

Logo $G' \subseteq H'$ e portanto, $G' = H'$.

Agora, pelo Teorema dos Isomorfismos, temos

$$G/Z(G) = HZ(G)/Z(G) \cong H/H \cap Z(G),$$

Assim, é suficiente provarmos que H satisfaz $H \cap Z(G) = Z(H)$. A inclusão $H \cap Z(G) \subseteq Z(H)$ é válida para qualquer subgrupo, para a inclusão inversa tome $g \in G$ e $h \in Z(H)$ quaisquer. Escrevendo $g = x_i z$ para algum $1 \leq i \leq n$ e $z \in Z(G)$ vemos que $h \in Z(G)$ pois

$$gh = x_i z h = x_i h z = h x_i z = hg.$$

Já que $x_i \in H$. Como $h \in H$ temos $Z(H) \subseteq H \cap Z(G)$. □

Teorema 5.6. Seja G um grupo com $|G/Z(G)| = n$. Então $\lambda(G) < d(n)/2$.

Demonstração. Tome H como no Lema 5.5. Note que $G' = H'$ e $G/Z(G) \cong H/Z(H)$ garantem que podemos supor, sem perda de generalidade, que G é finitamente gerado. Dessa forma, como $Z(G)$ tem índice finito, segue que $Z(G)$ também é finitamente gerado, assim, para qualquer k, o quociente $G/Z(G)^k$ é finito, pelo Teorema 5.4 segue que $\lambda(G/Z(G)^k) < m(G/Z(G)^k)$.

Se $\lambda = \chi(1)$ para algum caracter irredutível de $G/Z(G)^k$, então o Corolário 4.71 garante que $\lambda \mid n$ e $\lambda^2 \leqslant n$, logo $\lambda(G/Z(G)^k) < d(n)/2$.

Portanto, tomando $x \in G'$ temos que $x = y_k z_k$ onde y_k é um produto de até $d(n)/2$ comutadores e $z_k \in Z(G)^k$. Para cada k, escreva $z_k = y_k^{-1} x$, como existem finitos comutadores em G então existem finitos y_k e, consequentemente, finitos z_k. Dessa forma existe algum $z = z_l$ tal que $z \in Z(G)^k$ para todo k suficientemente grande. Por outro lado, sendo $Z(G)$ abeliano e finitamente gerado, segue que

$$\bigcap_{k=1}^{\infty} Z(G)^k = 1,$$

ou seja, $z = 1$ e daí $x = y_k$, onde, como mostrado acima, y_k é um produto de até $d(n)/2$ comutadores. □

Esse resultado já nos oferece uma melhor cota para a largura de um grupo central-por-finito (cf. Proposição 1.5), mas veremos que ainda é possível refiná-la ainda mais. Além disso, ele fornece uma outra demonstração do Teorema de Schur.

Usando o Lema 1.15 podemos obter uma nova cota caso G seja nilpotente, mais ainda, utilizando o resultado para grupos nilpotentes podemos refinar a cota no caso geral.

Teorema 5.7. Se G é um grupo nilpotente e $|G/Z(G)| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Então

$$\lambda(G) \leqslant \frac{1}{2}\max\{\alpha_1, \ldots, \alpha_r\}.$$

Demonstração. Como G é central-por-finito, então G' é finito pelo Teorema de Schur. Logo, pelo Lema 1.15 podemos supor que G é finito. Dessa forma, como G é nilpotente, podemos escrevê-lo como produto dos seus subgrupos de Sylow (cf. [19, 5.2.4]), como $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \cdot |Z(G)|$, podemos escrever $G \cong P_1 \times \cdots \times P_r \times P$, onde $P_i \in \mathrm{Syl}_{p_i}(G)$ e P é produto direto dos subgrupos de Sylow de G contidos no centro $Z(G)$. Observe que P, por ser central, não será relevante para a estimativa de $\lambda(G)$.

Pelo Teorema 5.6 temos $\lambda(P_i) < (\alpha_i + 1)/2$, ou seja, $\lambda(P_i) \leqslant \alpha_i/2$, pois caso contrário teríamos $\alpha_i < 2\lambda(P_i) < \alpha_i + 1$, absurdo. Como $G' \cong P_1' \times \cdots \times P_r'$, segue que

$$\lambda(G) \leqslant \max\{\lambda(P_1), \ldots, \lambda(P_r)\} \leqslant \max\{\alpha_1/2, \ldots, \alpha_r/2\} = \frac{1}{2}\max\{\alpha_1, \ldots, \alpha_r\}.$$

□

Para o próximo lema, note que, dados um grupo finito G e $T \in \mathrm{Syl}_p(G')$, podemos tomar $S \in \mathrm{Syl}_p(G)$ tal que $T = G' \cap S$, de fato, como T é um p-subgrupo de G, existe $S \in Syl_p(G)$ tal que $T \subseteq S$, ou seja, $T \subseteq G' \cap S$, mas como $G' \cap S$ é um p-subgrupo de G' e T é maximal nesse sentindo, temos $T = G' \cap S$.

Teorema 5.8. Seja G um grupo finito com $|G/Z(G)| = p^\alpha q$, onde $(p,q) = 1$. Se $x \in T$, com $T \in \mathrm{Syl}_p(G')$, então x é um produto de, no máximo, $3\alpha/2$ comutadores.

Demonstração. Pelo Teorema do Subgrupo Focal [Teorema 1.10] temos

$$T = \langle [g,s] \mid g \in G, s \in S, [g,s] \in S \rangle,$$

onde $S \in \mathrm{Syl}_p(G)$ é tal que $T = S \cap G'$. Como T é finito podemos escolher $g_1, \ldots, g_\beta \in G$ e $s_1, \ldots, s_\beta \in S$ de sorte que $T = \langle [g_1, s_1], \ldots, [g_\beta, s_\beta], S' \rangle$.

Agora, note que $[g,s]^m S' = [g,s^m]S'$. Para $m = 1$ é imediato, a fim de utilizar indução, considere o caso $m = 2$.

$$\begin{aligned}[g,s^2]S' &= g^{-1}s^{-2}gs^2S' \\ &= g^{-1}s^{-1}gss^{-1}g^{-1}s^{-1}gs^2S' \\ &= [g,s]s^{-1}[g,s]sS' \\ &= [g,s]^2[s,g]s^{-1}[g,s]sS' \\ &= [g,s]^2[[g,s],s]S' = [g,s]^2S'.\end{aligned}$$

Já que $[[g,s],s] \in S'$.

Agora supondo que a igualdade vale para $m-1$, com $m > 2$, temos:

$$\begin{aligned}[g,s^m]S' &= g^{-1}s^{-m}gs^mS' \\ &= g^{-1}s^{-(m-1)}gs^{m-1}s^{-(m-1)}g^{-1}s^{-1}gs^mS' \\ &= [g,s^{m-1}]s^{-(m-1)}[g,s]s^{m-1}S' \\ &= [g,s]^{m-1}[g,s][s,g]s^{-(m-1)}[g,s]s^{m-1}S' \\ &= [g,s]^m[[g,s],s^{m-1}] = [g,s]^mS'.\end{aligned}$$

pois $[[g,s],s^{n-1}] \in S'$. Assim, dado $x \in T$, temos

$$xS' = \prod_{i=1}^{\beta}[g_i,s_i]^{e_i}S' = \prod_{i=1}^{\beta}[g_i,s_i^{e_i}]S'.$$

Logo $x = \prod_{i=1}^{\beta}[g_i,s_i^{e_i}]s$, onde $s \in S'$. Portanto $\lambda(T) = \beta + \lambda(S)$.
Primeiramente, mostraremos que $\lambda(S) \leqslant \alpha/2$. Como S é p-grupo, usaremos o Teorema 5.7. Note que

$$|S/Z(S)| \leqslant |S/(S \cap Z(G))| = |SZ(G)/Z(G)| \leqslant |G/Z(G)| = p^\alpha q,$$

mas como S é p-grupo, temos $|S/Z(S)| \leqslant p^\alpha$ e portanto, $\lambda(S) \leqslant \alpha/2$.

Resta mostrarmos que $\beta \leq \alpha$. Temos primeiramente que $|T/S'| \geq p^\beta$ pois tal quociente é abeliano e gerado por β elementos. Por outro lado, temos

$$|T/S \cap G' \cap Z(G)| = |T/T \cap Z(G)| = |TZ(G)/Z(G)| \leq |G/Z(G)| \leq p^\alpha q$$

e como T é p-grupo temos $|T| \leq p^{\alpha}|S \cap G' \cap Z(G)|$. Por fim, a Proposição 1.11 garante que

$$|T/S'| \leq p^{\alpha}\frac{|S \cap G' \cap Z(G)|}{|S'|} \leq p^{\alpha}\frac{|S \cap G' \cap Z(G)|}{|S' \cap Z(G)|} = p^{\alpha}.$$

Logo $\beta \leq \alpha$. □

Teorema 5.9. Seja G um grupo com $|G/Z(G)| = n$. Então $\lambda(G) \leqslant 3\rho(n)/2$.

Demonstração. Usando o Lema 1.15 podemos supor G finito. Agora, pelo Corolário 1.12, se $p \mid |G'|$, então $p \mid n$. Assim, escrevendo $n = p_1^{\alpha_1} \cdots, p_r^{\alpha_r}$, dado $x \in G'$, temos $x = x_1 \cdots x_r$, onde $x_i \in \mathrm{Syl}_{p_i}(G')$. Para cada $i = 1, \ldots, r$ o Lema 5.8 garante que x_i é um produto de, no máximo, $3\alpha_i/2$ comutadores. Portanto x é um produto de, no máximo, $\sum_{i=1}^{r} 3\alpha_i/2 = 3\rho(n)/2$, ou seja, $\lambda(G) \leqslant 3\rho(n)/2$. □

5.2 Subgrupos abelianos e largura

Como vimos, o centro de um grupo tem bastante influência na sua largura, nesse contexto, é natural perguntar se subgrupos abelianos também teriam um papel similar. Nesse seção veremos que a resposta dessa pergunta é sim.

Começaremos com o seguinte resultado.

Proposição 5.10. Um grupo finito G de ordem $|G| = n$ pode ser gerado por $\rho(n)$ elementos.

Demonstração. Provaremos primeiramente, por indução, o caso em que $|G| = p^k$. Como $Z(G) \neq 1$, podemos tomar $x_1 \in Z(G)$ de ordem p de forma que $|G/\langle x_1 \rangle| = p^{k-1}$, por indução $G/\langle x_1 \rangle = \langle x_2\langle x_1\rangle, \ldots, x_k\langle x_1\rangle\rangle$. Logo, $G = \langle x_1, x_2, \ldots, x_k\rangle$ e como $\rho(p^k) = k$ obtemos o resultado.

Para terminar, escreva $n = p_1^{k_1} \cdots p_m^{k_m}$, nesse caso, $G = \langle P_1, \cdots, P_m\rangle$ onde $P_i \in \mathrm{Syl}_{p_i}(G)$. Usando o caso anterior, temos que G pode ser gerado por $k_1 + \cdots k_m = \rho(n)$. □

Considere agora o seguinte lema.

Lema 5.11. Sejam G um grupo e $K \leqslant G$. Suponha que $[G,K] \leqslant Z(K)$ e $G = \langle \{x_\alpha \mid \alpha \in I\}, C_G(K)\rangle$, onde I é um conjunto qualquer. Então

$$[G,K] = \left\{ \prod_{\alpha \in I} [x_\alpha, k_\alpha] \mid k_\alpha \in K \right\}$$

Demonstração. Denote $A = \left\{ \prod_{\alpha\in I} [x_\alpha, k_\alpha] \mid k_\alpha \in K \right\}$. Por definição, temos $A \subseteq [G,K]$. Note que A é um subgrupo de G, pois para todo $\alpha \in I$ e $k,h \in K$ temos

$$\begin{aligned}
[x_\alpha,k][x_\alpha,h]^{-1} &= [x_\alpha,k][x_\alpha,h]^{-1}(k^{-1}hh^{-1}k) \\
&= x_\alpha^{-1}k^{-1}x_\alpha k[x_\alpha,h]^{-1}(k^{-1}h)(h^{-1}k) \\
&= x_\alpha^{-1}k^{-1}x_\alpha k(k^{-1}h)(h^{-1}x_\alpha^{-1}hx_\alpha)(h^{-1}k) \\
&= x_\alpha^{-1}k^{-1}hx_\alpha h^{-1}k \\
&= [x_\alpha, h^{-1}k] \in A,
\end{aligned}$$

onde usamos que $[G,K] \subseteq Z(K)$. Logo,

$$\prod_{\alpha\in I}[x_\alpha,k_\alpha](\prod_{\alpha\in I}[x_\alpha,h_\alpha])^{-1} = \prod_{\alpha\in I}[x_\alpha,k_\alpha h_\alpha^{-1}] \in A,$$

como queríamos. Ademais, temos $A \triangleleft G$, pois tomando $\beta \in I$ temos

$$\begin{aligned}
x_\beta^{-1}[x_\alpha,k]x_\beta &= x_\beta^{-1}[x_\alpha,k]x_\beta[k,x_\alpha][x_\alpha,k] \\
&= [x_\beta,[x_\alpha,k]^{-1}][x_\alpha,k] \in A.
\end{aligned}$$

Portanto, como $G = \langle \{x_\alpha \mid \alpha \in I\}, C_G(K)\rangle$, segue que $g^{-1}[x_\alpha,k]g \in A$ para todo $g \in G$. Por fim, como

$$g^{-1}(\prod_{\alpha\in I}[x_\alpha,k_\alpha])g = \prod_{\alpha\in I} g^{-1}[x_\alpha,k_\alpha]g \in A$$

para todo $g \in G$ obtemos que $A \triangleleft G$. Para terminar a demonstração, usaremos que

$$[x_\alpha x_\beta, k] = [x_\alpha,k]^{x_\beta}[x_\beta,k] \in A.$$

Logo, dado $g = \prod_{i=1}^{m} x_{\alpha_i} y$, onde $\alpha_i \in I$ e $y \in C_G(K)$, podemos usar indução em m para mostrar que $[g,k] \in A$ para todos $g \in G$ e $k \in K$, ou seja, $[G,K] \subseteq A$ e portanto $[G,K] = A$. □

Esse teorema vale, em particular, para subgrupos normais abelianos de índice finito. De fato, se $K \leqslant G$ satisfaz essas condições, então

$$G = \langle x_1,\ldots,x_r,K\rangle = \langle x_1,\ldots,x_r,C_G(K)\rangle,$$

pois $K \subseteq C_G(K)$. Além disso, para quaisquer $g \in G$ e $k \in K$ temos $[g,k] = (k^{-1})^g k \in K$, ou seja, $[G,K] \subseteq K = Z(K)$. Dessa forma, temos o seguinte corolário.

Corolário 5.12. Sejam G um grupo e $K \triangleleft G$ abeliano com $[G:K] = n$, então todo elemento de $[G,K]$ é um produto de $\rho(n)$ comutadores.

Demonstração. Pela Proposição 5.10 podemos tomar $r \leqslant \rho(n)$ tal que $G = \langle x_1, \ldots, x_r, K\rangle$, logo

$$[G,K] = \left\{ \prod_{i=1}^{r} [x_r, k_r] \mid k \in K \right\},$$

como queríamos. □

Usaremos esse fato para provar um análogo do Teorema 5.9.

Teorema 5.13. Sejam G um grupo e A um subgrupo subnormal abeliano de G. Se $[G:A] = n$, então $\lambda(G) \leqslant 5\rho(n)/2$.

Demonstração. Primeiramente, se $A \triangleleft G$, então pelo corolário anterior, temos que os elementos de $[G,A]$ se escrevem como um produto de $r \leqslant \rho(n)$ comutadores. Assim, temos $\lambda(G) \leq \lambda(G/[G,A]) + r$, pois tomando $x \in G'$, temos $x[G,A] \in (G/[G,A])'$, ou seja, podemos escrever $x = x_1x_2$, onde $x_1 \in G$ é um produto de até $\lambda(G/[G,A])$ comutadores e $x_2 \in [G,A]$ é um produto de até r comutadores.

Podemos limitar $\lambda(G/[G,A])$ com o Teorema 5.9, para tanto note que $[G,A] \leqslant A$, pois $A \triangleleft G$, além disso, temos $A/[G,A] \leqslant Z(G/[G,A])$ e portanto

$$[G/[G,A] : Z(G/[G,A])] \;\Big|\; [G/[G,A] : A/[G,A]] = [G,A] = n.$$

Logo $\lambda(G/[G,A]) \leqslant 3\rho(n)/2$. Por fim, temos $\lambda(G) \leqslant 3\rho(n)/2 + \rho(n) = 5\rho(n)/2$.

Agora, supondo $A = A_0 \triangleleft A_1 \triangleleft \cdots A_k = G$, com $k > 0$, usaremos indução em k. O caso $k = 1$ já foi feito, suponha que o resultado vale para algum $k > 1$. Denote $[A_{k-1} : A] = m$, por indução, temos $\lambda(A_{k-1}) \leqslant 5\rho(m)/2$. Além disso,

$$\frac{A_{k-1}}{(A_{k-1})'} \triangleleft \frac{G}{(A_{k-1})'}.$$

E também que,

$$[G/(A_{k-1})' : A_{k-1} : (A_{k-1})'] = [G : A_{k-1}] = [G:A]/[A_{k-1}/A] = n/m.$$

Portanto pelo caso base temos, $\lambda(G/(A_{k-1})') \leqslant 5\rho(m/n)/2$. Por fim, temos

$$\begin{aligned}\lambda(G) \leqslant \lambda(G/(A_{k-1})') + \lambda(A_{k-1}) &= \frac{5\rho(n/m)}{2} + \frac{5\rho(m)}{2} \\ &= \frac{5(\rho(n/m)+\rho(m))}{2} \\ &= \frac{5\rho(n)}{2}\end{aligned}$$

□

Para grupos solúveis é possível refinar ainda mais a cota.

Proposição 5.14. Sejam G um grupo solúvel e um A subgrupo subnormal abeliano de G com $[G:A] = n$, então $\lambda(G) \leqslant \rho(n)$.

Demonstração. Usaremos indução em n, para $n = 1$ o resultado segue pois teríamos $G = A$, daí $\lambda(G) = 0 = \rho(1)$, assim suponha $n > 1$. Como A é subnormal, existe $M \triangleleft G$ normal maximal tal que $A \leqslant M$. Como G é solúvel temos $[G,M] = p$, para algum p primo, logo $[M:A] = n/p < n$, portanto a hipótese de indução garante que $\lambda(M) \leqslant \rho(n/p) = \rho(n) - 1$. Além disso, como G/M é cíclico, temos $G' = [G,M]$, de fato, dado $[g,h] \in G'$ podemos escrever $g = x^l n$ e $h = x^k m$, onde $m,n \in M$ e x é tal que xM gera G/M. Daí

$$\begin{aligned}[g,h] &= [x^l n, x^k m] \\ &= x^l n x^k m n^{-1} x^{-l} m^{-1} x^{-k} \\ &= (x^l n x^{-l}) x^l (x^k m x^{-k}) x^k x^{-l} (x^l n^{-1} x^{-l}) x^{-k} (x^k m^{-1} x^{-k}) \\ &= n_0 x^l m_0 x^k x^{-l} n_0^{-1} x^{-k} m_0^{-1} \\ &= (n_0 x^l m_0 x^{-l} n_0^{-1} m_0^{-1}) m_0 n_0 (x^l x^k x^{-l}) n_0^{-1} x^{-k} m_0^{-1} \\ &= [n_0 x^l, m_0] m_0 n_0 x^k n_0^{-1} x^{-k} m_0^{-1} \\ &= [n_0 x^l, m_0][n_0, x^k]^{m_0} \in [G,M].\end{aligned}$$

Onde $n_0 = x^l n x^{-l}$ e $m_0 = x^k m x^{-k}$. Logo $G' \subseteq [G,M]$, como também vale $[G,M] \subseteq G'$ temos a igualdade desejada. Ademais, note que, dado $[g,n] \in [G,M]$

$$[g,n] = [x^l m, n] = x^l m n m^{-1} x^{-l} n = [m,n]^{x^l}[x^l,n] \in [x^l,n]M',$$

ou seja, todo elemento de $G' = [G,M]$ é um comutador módulo M', dessa forma temos $\lambda(G/M') \leqslant 1$. Portanto $\lambda(G) \leqslant \lambda(G/M') + \lambda(M) \leqslant 1 + \rho(n) - 1 = \rho(n)$. □

Como vimos, o índice $[G : Z(G)]$ tem forte influência na largura $\lambda(G)$. É natural se perguntar o que aconteceria caso substituíssemos a hipótese do quociente $G/Z(G)$ ser finito por ser finitamente gerado. Se $G = F_2$ é o grupo livre 2-gerado, então $G/Z(G) \cong G$ e portanto é finitamente gerado, mas $\lambda(G)$ é infinita. Ou seja, pedindo somente que $G/Z(G)$ seja finitamente gerado não poderíamos dizer muito sobre $\lambda(G)$. Sendo assim, adicionaremos hipóteses de nilpotência para obter resultados mais interessantes.

Lema 5.15. Sejam G um grupo e $y_1, \ldots, y_m \in G$. Considere $H = \langle y_1, \ldots, y_m \rangle$, K o fecho normal de H em G, $K_1 = [G,K]$ e $K_{i+1} = [K,K_i]$ para $i \geq 1$. Suponha ainda que $G = \langle x_1, \ldots, x_n, C_G(K) \rangle$. Se $K_r = 1$ para algum r, então

$$[G,K] = \left\{ \prod_{i=1}^{n} [x_i, h_i] \prod_{j=1}^{m} [y_j, k_j] \mid h_i, h_j \in K \right\}.$$

Demonstração. A demonstração será por indução em r. Se $r = 2$, estamos nas condições do Lema 5.11, pois $[K,[G,K]] = 1$ e dessa forma $[G,K] \leq Z(K)$, a fim de obtermos a igualdade desejada, aplique o Lema 5.11 com $G = \langle x_1, \ldots, x_n, y_1, \ldots, y_m, C_G(K) \rangle$.

Suponha agora $r > 2$. Defina

$$A = \left\{ \prod_{i=1}^{n} [x_i, h_i] \prod_{j=1}^{m} [y_j, k_j] \mid h_i, h_j \in K \right\}.$$

E $B = [G, K_{r-1}]$. A fim de usar indução no grupo $\overline{G} = G/B$, suponha primeiramente que $B \neq 1$. Nesse caso, considere $\overline{H} = \langle y_1 B, \ldots, y_m B \rangle$ e $\overline{K}$ é o fecho normal de $\overline{H}$ em $\overline{G}$.

Note que $\overline{K} = K/B$ e $\overline{K}_{r-1} = 1$. Por indução, temos

$$[\overline{G}, \overline{K}] = [G,K]/B = \left\{ \prod_{i=1}^{n} [x_i B, h_i B] \prod_{j=1}^{m} [y_j B, k_j B] \mid h_i, h_j \in K \right\}.$$

Logo $[G,K] = AB$. Para terminarmos, é suficiente mostrar que $AB \subseteq A$. Usando novamente o Lema 5.11 obtemos

$$[G, K_{r-1}] = \left\{ \prod_{i=1}^{n} [x_i, z_i] \mid z_i \in K_{r-1} \right\}.$$

Como $K_{r-1} \leq Z(K)$, temos

$$\prod_{i=1}^{n} [x_i, h_i] \prod_{j=1}^{m} [y_j, k_j] \prod_{i=1}^{n} [x_i, z_i] = \prod_{i=1}^{n} [x_i, h_i][x_i, z_i] \prod_{j=1}^{m} [y_j, k_j] = \prod_{i=1}^{n} [x_i, z_i h_i] \prod_{j=1}^{m} [y_j, k_j] \in A.$$

Para quaisquer $h_1,\ldots,h_n,k_1,\ldots,k_m \in K$ e $z_1,\ldots,z_n \in K_{r-1}$, ou seja, $AB \subseteq A$ e assim $[G,K] = A$, como queríamos.

Suponha agora que $B = 1$, ou seja, que $K_{r-1} \leq Z(G)$. Usaremos indução em G/K_{r-1}, de forma análoga, temos $[G,K] = AK_{r-1}$. Note que estamos nas condições do Lema 5.11 considerando o subgrupo $K_{r-1} = [K,K_{r-2}] \leq Z(K)$, assim,

$$K_{r-1} = \left\{ \prod_{j=1}^{m} \prod_{g\in G} [y_i^g, h_{i,g}] \mid h_{i,g} \in K_{r-2} \right\}.$$

Já que K é gerado pelos conjugados dos geradores de H, mas como $K_{r-1} \leq Z(G)$ podemos reescrever os elementos de K_{r-1} da seguinte forma

$$\begin{aligned}
\prod_{j=1}^{m} \prod_{g\in G} [y_i^g, h_{i,g}] &= \prod_{j=1}^{m} \prod_{g\in G} [y_i, h_{i,g}^{g^{-1}}]^g \\
&= \prod_{j=1}^{m} \prod_{g\in G} [y_i, h_{i,g}^{g^{-1}}] \\
&= \prod_{j=1}^{m} [y_i, \prod_{g\in G} h_{i,g}^{g^{-1}}] \\
&= \prod_{j=1}^{m} [y_i, z_i].
\end{aligned}$$

Onde $z_i = \prod_{g\in G} h_{i,g}^{g^{-1}} \in K_{r-2}$. Novamente, usando que $K_{r-1} \leq Z(G)$, podemos mostrar que $AK_{r-1} \subset A$, pois

$$\prod_{i=1}^{n} [x_i,h_i] \prod_{j=1}^{m} [y_j,k_j] \prod_{j=1}^{m} [y_i,z_i] = \prod_{i=1}^{n} [x_i,h_i] \prod_{j=1}^{m} [y_j,k_j][y_j,z_j] = \prod_{i=1}^{n} [x_i,h_i] \prod_{j=1}^{m} [y_j,z_jk_j] \in A.$$

□

Teorema 5.16. Se G é um grupo nilpotente e $G/Z(G)$ pode ser gerado por n elementos, então $\lambda(G) \leq n$.

Demonstração. A demonstração é análoga ao Lema 5.15, mostraremos que $G' = A$, onde

$$A = \left\{ \prod_{i=1}^{n} [x_i, y_i] \mid y_i \in G \right\}.$$

Com $x_1,\ldots,x_n$ os geradores de G. Suponha G nilpotente de classe r e denote $K = \gamma_{r-1}(G)$, assim, temos $\gamma_{r-1}(G) \leq Z(G)$. Aplicando indução em G/K, obtemos que $G' = AK$. A

inclusão $K \subset A$ segue do Lema 5.11 e do subgrupo K ser central, assim como no Lema 5.15. Logo, qualquer elemento de G' é um produto de até n comutadores, ou seja, $\lambda(G) \leq n$.

□

Teorema 5.17. Se G é finitamente gerado e nilpotent-por-nilpotente, então $\lambda(G)$ é finita.

Demonstração. Seja $N \triangleleft G$ com N e G/N nilpotentes. Temos $\gamma_r(G/N) = 1$ para algum r, ou seja, $\gamma_r(G) \leq N$, como N é nilpotente segue que $\gamma_r(G)$ é nilpotente. Dessa forma, o Lema 5.15 se aplica fazendo $K = \gamma_r(G)$, pois

- $G = \langle x_1, \ldots, x_n \rangle$ por hipótese.
- $\gamma_r(G)$ é o fecho normal de um grupo finitamente gerado, a saber, o grupos gerado pelos comutadores de peso r formados pelos geradores de G.
- $K_1 = [G,K] \subseteq K$ e assim $K_i \subseteq \gamma_i(K)$. Como K é nilpotente, temos $K_r = 1$ para algum r.

Logo G tem largura finita. □

5.3 Grupos de Macdonald

Com o objetivo de apresentar exemplos elementares de grupos com largura maior do que 1, I. D. Macdonald construiu, para cada n natural, grupos de matrizes n-gerados ($n \geq 3$) e provou que para $n \geq 6$ esses grupos possuem, de fato, tal propriedade (cf. [17]).

Aqui mostraremos que esse fato também se realiza para $n = 4, 5$, mais do que isso, calcularemos a largura exata para n qualquer quando as entradas das matrizes estão sobre um corpo de característica 2. Com isso, também conseguiremos mostrar que as cotas obtidas por Guralnick são bastante finas.

Começaremos com alguns fatos sobre matrizes.

Definição 5.18. Seja M um matriz com entradas sobre algum corpo $\mathbb{F}$.

- Definimos $\text{rank}(M)$ como a dimensão do F-espaço vetorial gerado pelas linhas de M.
- Se M for uma matriz quadrada que satisfaz $M = -M^T$, então M é dita antissimétrica.

Proposição 5.19. Sejam A, B matriz reais. Então

- $\text{rank}(AB) \leq \min\{\text{rank}(A), \text{rank}(B)\}$.
- $\text{rank}(A+B) \leq \text{rank}(A) + \text{rank}(B)$.

Agora veremos que é possível ter algum controle sobre a largura de um grupo nilpotente de classe 2 associando cada elemento do subgrupo derivado a uma matriz antissimétrica.

Definição 5.20. Seja $G = \langle x_1, \ldots, x_n \rangle$ um grupo com $G' \subseteq Z(G)$. Defina $c_{ij} = [x_i, x_j]$ para $1 \leq i < j \leq n$. Tomando $c \in G$ podemos escrever $c = \prod_{i<j} c_{ij}^{\lambda_{ij}}$ para certos $\lambda_{ij} \in \mathbb{Z}$. Associaremos uma expressão do tipo a uma matriz antissimétrica, $\Delta(c) = (a_{ij})$ com coeficientes inteiros, onde $a_{ij} = \lambda_{ij}$ se $i < j$ e $a_{ii} = 0$, isto é,

$$\Delta(c) = \begin{pmatrix} 0 & \lambda_{12} & \lambda_{13} & \cdots & \lambda_{1n} \\ -\lambda_{12} & 0 & \lambda_{23} & \cdots & \lambda_{2n} \\ -\lambda_{31} & -\lambda_{32} & 0 & \cdots & \lambda_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -\lambda_{1n} & -\lambda_{2n} & -\lambda_{3n} & \cdots & 0 \end{pmatrix}$$

.

Lema 5.21. Seja $G = \langle x_1, \ldots, x_n \rangle$ um grupo com $G' \subseteq Z(G)$. Se w é um comutador de G, então $\text{rank}(\Delta(w)) \leq 2$.

Demonstração. Temos

$$w = [\prod_{i=1}^{n} x_i^{\alpha_i}, \prod_{i=1}^{n} x_i^{\beta_i}] = \prod_{i<j} c_{ij}^{\alpha_i\beta_j - \alpha_j\beta_i}. \tag{5.2}$$

Pois $G' \subseteq Z(G)$. Assim podemos escrever $\Delta(w) = AB^t - BA^t$, onde

$$A = \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ \alpha_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_n & 0 & \cdots & 0 \end{pmatrix} \text{ e } B = \begin{pmatrix} \beta_1 & 0 & \cdots & 0 \\ \beta_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \beta_n & 0 & \cdots & 0 \end{pmatrix}.$$

Sendo assim $\text{rank}(\Delta(w)) \leq 2$. □

De forma geral, denotaremos por $E(i, j) = (a_{r,s})$ a matriz quadrada (de alguma ordem) com coeficientes em $\mathbb{F}_2$ definida por $a_{r,s} = 1$ se $r = i, s = j$ e $a_{r,s} = 0$ caso contrário.

Definição 5.22. Definiremos M_n como o grupo gerado pelas matrizes, com entradas em $\mathbb{F}_2$ e ordem $(n^2+3n)/2 \times (n^2+3n)/2$, definidas por

$$A_i = I + E(2i-1, 2i) + \sum_{i=1}^{i-1} E(2j, i + (j+1)(n - (j(j+1))/2)).$$

Onde $i = 1, \cdots, n$.

Por exemplo, M_3 é gerado por

$$\begin{aligned} A_1 &= I + E(1,2). \\ A_2 &= I + E(3,4) + E(2,7). \\ A_3 &= I + E(5,6) + E(2,8) + E(4,9). \end{aligned}$$

A ideia por trás dessa definição é considerar matrizes "esparsas" de forma que calcular seus produtos seja simples, lembre-se que

Lema 5.23. $E(i,j)E(l,k) = 0$ se $j \neq l$ e $E(i,j)E(l,k) = E(i,k)$ se $j = l$.

Proposição 5.24. Sejam A_i e A_j geradores do grupo M_n, então

1. $A_iA_k = \begin{cases} A_i + A_k - I, & \text{se } i \geq k \\ A_i + A_k - I + E(2i-1, k+(i+1)(n-(i+1)/2)), & \text{se } i < k \end{cases}$.
2. $A_i^{-1} = A_i$.
3. $[A_i, A_k] = \begin{cases} I + E(2k-1, i+(k+1)(n-k(k+1)/2)), & \text{se } i > k \\ I + E(2i-1, k+(i+1)(n-i(i+1)/2)), & \text{se } i < k \end{cases}$.

Demonstração. 1. Usando distributividade temos

$$A_iA_k = A_i + A_iE(2k-1,2k) + A_i \sum_{i=1}^{k-1} E(2j, k+(j+1)(n-(j(j+1))/2)).$$

Agora suponha $i \geq k$. Note que pelo Lema 5.23 temos $A_iE(2k-1,2k) = E(2k-1,2k)$ e também

$$\begin{aligned} A_i \sum_{i=1}^{k-1} E(2j, k+(j+1)(n-(j(j+1))/2)) &= \sum_{i=1}^{k-1} E(2j, k+(j+1)(n-(j(j+1))/2)) \\ &= A_k - E(2k-1,2k) - I. \end{aligned}$$

Logo

$$A_iA_k = A_i + A_k - I.$$

Considere agora $i < k$. Da mesma forma $A_iE(2k-1,2k) = E(2k-1,2k)$, mas agora,

$$A_i \sum_{i=1}^{k-1} E(2j, k+(j+1)(n-(j(j+1))/2))$$

vale

$$E(2i-1,k+(i+1)(n-(i+1)/2))+\sum_{i=1}^{k-1}E(2j,k+(j+1)(n-(j(j+1))/2)),$$

ou seja,

$$A_iA_k = A_k - E(2k-1,2k) - I + E(2i-1,k+(i+1)(n-(i+1)/2)).$$

2. Do item anterior $A_iA_i = A_i + A_i - I = I$ pois estamos sobre $\mathbb{F}_2$.

3. Como os casos $i > k$ e $i < k$ são análogos faremos apenas o caso $i > k$. Temos

$$\begin{aligned}[A_i,A_k] &= (A_iA_k)^2 \\ &= A_iA_k + A_kA_i + I \\ &= A_i + A_k + I + A_i + A_k + I + E(2k-1,i+(k+1)(n-(k+1)/2)) + I \\ &= I + E(2k-1,i+(k+1)(n-(k+1)/2)).\end{aligned}$$

□

Proposição 5.25. Considere $G = M_n$. Então

1. G é nilpotente de classe 2.
2. $G' = Z(G)$.
3. $|G| = 2^{n+n(n-1)/2}$ e $|G'| = 2^{n(n-1)/2}$.

Demonstração. 1. Considere A_i, A_k, A_l geradores de M_n, suponha que $i > k$ e denote $E = E(2k-1,i+(k+1)(n-(k+1)/2))$. Então

$$\begin{aligned}[[A_i,A_k],A_l] &= (I+E)^{-1}A_l^{-1}(I+E)A_l \\ &= (1+E)A_l(I+E)A_l \\ &= (A_l + EA_l)^2 \\ &= (A_l + E)^2 \\ &= A_l^2 + E^2 = I + 0 = I.\end{aligned}$$

Analogamente $[[A_i,A_k],A_l] = I$ se $i < k$. De qualquer forma, vemos que $G' \leq Z(G)$.

2. Como $G' \leq Z(G)$ é suficiente mostrarmos que $[G:G'] = [G:Z(G)]$. Para tanto, observe que G/G' quanto $G/Z(G)$ são grupos 2-abeliano elementar gerados por n elementos, de forma que $|G/G'| = |G/Z(G)|$.

3. Mostraremos primeiramente que $|G'| = 2^{n(n-1)/2}$. Note que os comutadores $[A_i, A_k]$ com $1 \leq i < k \leq n$ geram G', além disso, tais comutadores são linearmente independentes (vendo G' como um $\mathbb{F}_2$-espaço vetorial). Para ver isso, observe que cada comutador $[A_i, A_k]$ tem 1 na posição $(2i-1, k+(i+1)(n-i(i+1)/2))$, de sorte que a equação

$$\prod_{1 \leq i < k \leq n} [A_i, A_k]^{\lambda_{ij}} = I$$

só tem solução quando cada λ_{ij} for nulo.

Assim $|G'| = 2^{n(n-1)/2}$. Agora, temos que $A_1G', A_2G', \ldots, A_nG'$ é uma base para G/G', ou seja, $|G/G'| = 2^n$. Por fim, temos $|G| = |G/G'||Z(G)| = 2^{n+n(n-1)/2}$.

□

Considere $G = M_n$. Tome $c \in G'$, como o conjunto $\left\{c_{ij} \mid 1 \leq i < j \leq n\right\}$ forma uma base para G', existem únicos λ_{ij} com $1 \leq i < j \leq n$ tais que

$$c = \prod_{1 \leq i < j \leq n} c_{ij}^{\lambda_{ij}}.$$

Assim, a matriz $\Delta(c)$ definida em 5.20 é única, usaremos isso para calcular a largura de M_n.

Teorema 5.26. Considere $G = M_n$. Então $\lambda(G) = n/2$ se n é par e $\lambda(G) = (n-1)/2$ se n é ímpar.

Demonstração. Como $[G:Z(G)] = 2^n$ o Teorema 5.7 garante que $\lambda(G) \leq n/2$. Suponha n par, tome $c = c_{12}c_{34}\cdots c_{n-1,n} \in G'$, assim

$$\Delta(c) = \begin{pmatrix} 0 & 1 & & & & & \\ -1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & -1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & -1 & 0 \end{pmatrix}$$

Logo $\text{rank}(\Delta(c)) = n$. Supondo que c pudesse ser escrito como um produto de $k < n/2$ comutadores $w_1, \ldots, w_k$ chegaremos ao seguinte absurdo,

$$\text{rank}(\Delta(c)) \leq \text{rank}(\Delta(w_1)) + \cdots \text{rank}(\Delta(w_k)) \leq 2k < n.$$

Sendo assim $\lambda(G) = n/2$.

Suponha $n = 2m+1$ ímpar, considere $c = c_{21}c_{43}\cdots c_{2m,2m-1} = c_{12}^{-1}c_{34}^{-1}\cdots c_{2m-1,2m}^{-1}$, logo

$$\Delta(c) = \begin{pmatrix} 0 & -1 & & & & & & \\ 1 & 0 & & & & & & \\ & & 0 & -1 & & & & \\ & & 1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & 0 & -1 & \\ & & & & & 1 & 0 & 0 \\ & & & & & & 0 & 0 \end{pmatrix}$$

Assim, $\text{rank}(\Delta(c)) = 2m$. Novamente, supondo que c pudesse ser escrito como um produto de $k < m$ comutadores temos um absurdo, pois

$$\text{rank}(\Delta(c)) \leq 2k < 2m.$$

Sendo assim, $(n-1)/2\lambda(G) \leq n/2$, logo $\lambda(G) = (n-1)/2$, como queríamos. □

Os grupos de Macdonald mostram que as cotas obtidas por Guralnick são bastante finas, para ver isso considere $G = M_{2m}$, então, como vimos, $\lambda(G) = m$. A tabela seguinte sintetiza algumas das cotas obtidas. Usaremos que $[G : Z(G)] = 2^{2m}$.

	Teorema 5.7	Teorema 5.9	Teorema 5.13	Proposição 5.14
$\lambda(G) \leq$	m	$3m$	$5m$	$2m$

Vemos que o Teorema 5.7 oferece a melhor a melhor estimativa, porém precisamos da nilpotência do grupo.

5.4 Grupos de Largura 3

Em sua tese de doutorado R. M. Guralnick encontrou os menores grupos de largura 2, a saber, tais grupos têm ordem 96 e são isomorfos a $((C_4 \times C_2) \rtimes C_4) \rtimes C_3$ e $(C_2 \times C_2 \times Q_8) \rtimes C_3$.

Nesse sentido, uma questão natural é encontrar um grupo minimal com largura 3, sendo assim, considere uma versão mais restrita desse problema.

PROBLEMA 5. Encontre um p-grupo G de menor ordem tal que $\lambda(G) = 3$.

As ferramentas construídas nesse capítulo possibilitam alguma consideração sobre essa questão.

Proposição 5.27. Se G é um p-grupo de largura 3, então $[G : Z(G)] \geq p^6$ e $[G : G'] \geq p^3$.

Demonstração. Pelo Teorema 5.4 temos $m(G) > \lambda(G) = 3$. Por outro lado, usando o Corolário 4.71 temos que $\chi(1) \mid [G : Z(G)]$ e $\chi(1)^2 \leq [G : Z(G)]$ para todo caracter irredutível χ de G. Logo, supondo $[G : Z(G)] \leq p^5$, então $\chi(1) \in \{1, p, p^2\}$, ou seja, $m(G) \leq 3$, absurdo.

Se $[G : G'] \leq p^2$, então pelo Teorema de Base de Burnside ([19, 5.3.2]) segue que G é 2-gerado, sendo assim, $G/Z(G)$ é 2-gerado. Portanto, o Teorema 5.16 garante que $\lambda(G) \leq 2$. □

Além disso, usando o Teorema [13, Theorem 1b], para que $\lambda(G) = 3$ é necessário que $|G'| \geq p^6$. Unindo isso com a proposição anterior obtemos que $|G| \geq p^9$. Em resumo, para que um p-grupo tenha largura 3 é necessário que

- $|G| \geq p^9$.
- $[G : Z(G)] \geq p^6$.
- $[G : G'] \geq p^3$.

Pelo resultado da seção anterior M_6 é um 2-grupo de ordem 2^{21} e largura 3. Mais ainda, em [8], Guralnick construiu, para cada p primo, um p-grupo de ordem p^{15} e largura 3. Sendo assim, a busca por um p-grupo de largura 3 de menor ordem fica restrita aos p-grupos de ordem entre p^9 e p^{14}.

Por fim, terminamos o capítulo deixando o survey [15] como recomendação para mais detalhes sobre comutadores.

Bibliografia

[1] BAUMSLAG, G., Lectures on Nilpotent Groups. Vol. 2. CBMS Regional Conference Series in Mathematics, 1971.

[2] CALEGARI, D., Stable commutator lenght is rational in free groups. J. of the American Mathematical Society, Vol. 2, Number 4 (2009), 941–961.

[3] CASSIDY, P. J., Products of commutators are not always commutators: an example. Amer. Math. Monthly **86** (1979), no. 9, 772.

[4] ERDMANN, K.; WILDON, M. J. Introduction to Lie Algebras. 1 ed. London: Springer-Verlag, 2006.

[5] GRIGORCHUCK, R., Bernside's problem on periodic groups. Funct Anal Its Appl, Vol. 14 (1980), 41–43.

[6] GOLOD, E. S., On nil-algebras and finitely approximable p-groups, Izv. Akad. Nauk SSSR Ser. Mat., V. 28, (1964) 273–276.

[7] GURALNICK, R. M., Expressing group elements as commutators. Rocky Mountain Journal of Mathematics, Vol. 10, (1980) 651–654.

[8] GURALNICK, R. M. On a Result of Schur. Journal of Algebra, Vol. 59 (1979), 302–310.

[9] GUPTA, N.; SIDKI, S. On the Burnside problem for periodic groups, Math. Z., Vol. 182 (1983), 385–388.

[10] HUMPHREYS, J. E. Introduction to Lie Algebras and Representation Theory. Vol. 9. New York: Springer-Verlag, 1972.

[11] ISAACS, I. M.; PASSMAN, D. S. a characterization of groups in terms of the degrees of their characters. Pacific Journal of Mathematics. Vol. 15, No 3. (1965), 877-903.

[12] ISAACS, I. M. Character theory of finite groups. 1 ed. New York: Dover Publications, 1976.

[13] GALLAGHER, P. X. Group characters and commutators. Mathematische Zeitschrift. Vol. 79, (1962), 122–126.

[14] JAMES, G.; LIEBECK, M. Representations and Characters of Groups. 2 ed. Cambridge: Cambridge University Press, 2001.

[15] KAPPE, L.-C.; MORSE, R. F., On commutators in groups. (English summary) Groups St. Andrews 2005. Vol. 2, 531–558, London Math. Soc. Lecture Note Ser., 340, Cambridge Univ. Press, Cambridge, 2007.

[16] LIEBECK, M. W.; O'BRIEN, E. A.; SHALEV, A.; TIEP, P. H. The Ore conjecture. J. Eur. Math. Soc. 12 (2010), no. 4, 939-–1008.

[17] MACDONALD, I. D., Commutators and their products. Amer. Math. Monthly 93 (1986), no. 6, 440–444.

[18] O'CONNOR, J. J.; ROBERTSON, E. F. A history of the Burnside problem. Disponível em https://mathshistory.st-andrews.ac.uk/HistTopics/Burnside_problem/

[19] ROBINSON, D. J. S., A course in the theory of groups, 2nd edition, Springer-Verlag, New York, 1996.

[20] ROSE, J. A course on group theory, 1st edition, Cambridge University Press, Cambridge, 1978.

[21] ROSENLITCH, M. On a Result of Baer. Proceedings of the American Mathematical Society, Vol. 13, No. 1 (1962), 99–101.

[22] SANOV, I. N., Solution of the Burnside problem for exponent 4. Leningrad State Univ. Ann. Math. Ser., Vol; 10, (1940), 166–170.

[23] SEGAL, D., Closed Subgrupos of Profinite Groups. Proceedings of the London Mathematical Society. Vol. 81, Issue 1 (1999), 29-54.

[24] SERRE, J-P., Local Fields. 1 ed. Springer New York, New York, 1979.

[25] SCOTT, W. R. Group Theory. 1 ed. New York: Dover Publications, 1964.

[26] THE GAP GROUP, Manual do GAP, disponível em http://www.gap-system.org/.

[27] VAUGHAN-LEE, M. The Restricted Burnside Problem. 2 ed. Oxford: Oxford University Press, 1990.

[28] WIEGOLD, J. Multiplieators and groups with finite central factor-groups. Mathematische Zeitschrift. Vol. 89 (1965), 345–347.

[29] WIEGOLD, J., Groups with boundedly finite classes of conjugate elements. Proc. Roy. Soc. London Ser. A 238 (1957), 389–401.

Apêndice A

Alguns cálculos e o software GAP

De forma sucinta, o GAP (Groups, Algorithms, Programming) é um software livre de Álgebra Computacional focado especialmente em Teoria de Grupos. De maneira geral, o GAP consegue realizar cálculos aritméticos e possui operadores lógicos comuns presentes em outras linguagens de programação, como loops e condicionais. Dessa forma, discutiremos apenas as funções e objetos particulares da Teoria de Grupos.

O GAP possui implementado funções para construir grupos particulares, como grupos de matrizes, diedrais, cíclicos, entre outros. Além disso, é possível construir grupos a partir de seus geradores, basta escrever

```
Group([gen]);
```

onde [gen] é uma lista dos geradores. Já para definir um grupo livre n-gerado escrevemos

```
FreeGroup(n);
```

Além disso, também é possível descrever as relações que os geradores satisfazem, ilustraremos tal construção através de um exemplo. Suponha que escrevemos

```
g:=FreeGroup(3);
```

definindo um grupo g 3-gerado. Denote por g_1, g_2, g_3 os geradores desse grupo, se por exemplo, quisermos um grupo satisfazendo $g_1g_2g_3 = g_1^2 = 1$ escrevemos

```
g/[g.1*g.2*g.3 , g.1^2]
```

De forma geral, escrevemos

```
g/[w_1,w_2,...,w_n]
```

onde w_1 são as relações que desejamos que os geradores satisfaçam.

A.1 Grupos de expoente 6

Na demonstração do Lema 3.10 utilizaremos GAP para realizar algumas contas. Essa parte do texto servirá para clarificar um pouco mais esse processo.

Primeiramente, escreveremos

```
f:=FreeGroup("x","a","b");
```

para definir o grupo livre gerado por x, a, b. Queremos o grupo satisfazendo

$$x^2 = (xa)^2 = (xb)^2 = a^3 = b^3 = (ab)^6 = (ab^{-1})^6 = (xab)^6 = (a(ab)^3)^6 = 1$$

Portanto escrevemos

```
g:=f/ [f.1^2,
(f.1*f.2)^2,
(f.1*f.3)^2,
f.2^3,
f.3^3,
(f.2*f.3)^6,
(f.2*((f.3)^(-1)))^6,
(f.1*f.2*f.3)^6,
(f.1*(f.2*f.3)^3)^6];
```

Já o grupo satisfazendo

$$a^3 = b^3 = c^3 = (ab)^3 = (bc)^3 = (ca)^3 = (bc^{-1})^3 = (ca^{-1})^3 = (ab^{-1})^3 = (abac)^3 =$$
$$= (abac^{-1})^3 = ab^{-1}ac)^3 = (ab^{-1}ca^{-1})^3 = (a^{-1}bc)^6 = (ab^{-1}c)^6 = (abc^{-1})^6 = 1$$

pode ser calculado com o comando:

```
h:=f/[f.1^3,f.2^3,f.3^3,
(f.2*f.3)^3,(f.3*f.1)^3,(f.1*f.2)^3,
(f.2*(f.3^(-1)))^3,(f.3*(f.1^(-1)))^3,
(f.1*(f.2^(-1)))^3,(f.1*f.2*f.1*f.3)^3,
(f.1*f.2*f.1*(f.3^(-1)))^3,
(f.1*(f.2^(-1))*f.1*f.3)^3,
(f.1*(f.2^(-1))*f.1*(f.3^(-1)))^3,
```

```
((f.1^(-1))*f.2*f.3)^6,
(f.1*(f.2^(-1))*f.3)^6,
(f.1*f.2*(f.3^(-1)))^6];
```

Por fim, para calcularmos as ordens desses grupos escrevemos

```
Order(g);Order(h);
```

e o GAP nos retorna que g e h têm ordens $2 \cdot 3^3$ e 3^7, respectivamente.

Agora estamos em condições de demonstrar o Lema 3.10.

Lema (3.10). Sejam G um grupo de expoente 6, $x \in G$ um elemento de ordem 2 e $A \subseteq G$ tal que se $a \in A$, então $a^3 = (ax)^2 = 1$. Então $\langle A \rangle$ tem expoente 3.

Demonstração do Lema 3.10. Tome $a, b \in A$, mostraremos que $\langle a, b \rangle$ tem expoente 3. Para tanto, defina H como o subgrupo gerado por a, b, x. Note que $\langle a, b \rangle \triangleleft H$, pois a hipótese nos garante que

$$x^{-1}ax = a^{-1}, x^{-1}bx = b^{-1}$$

Além disso, $\langle a, b \rangle$ tem índice 2 em H. Para finalizar, note que as hipóteses garantem que os geradores a, b, x de H satisfazem

$$x^2 = (ax)^2 = (bx)^2 = a^3 = b^3 = (ab)^6 = (ab^{-1})^6 = (xab)^6 = (a(ab)^3)^6 = 1.$$

Assim, usando as contas que foram feitas no GAP vemos que $|H| \leq 2.3^3$, portanto $|\langle a, b \rangle| = 3^3$. Por fim, como $\langle a, b \rangle$ é um 3-grupo que é subgrupo de um grupo de expoente 6, ele próprio precisa ter expoente 3.

Agora tomando $a, b, c \in A$ mostraremos que $\langle a, b, c \rangle$ também tem expoente 3. Como $aba, ab^{-1}a \in \langle a, b \rangle$ esses elementos tem ordem 3, além disso,

$$x(aba)x = (xax)(xbx)(xax) = a^{-1}b^{-1}a^{-1} = (aba)^{-1}.$$

Analogamente $x(ab^{-1}a)x = (ab^{-1}a)^{-1}$. Esses fatos e a igualdade

$$\langle A \rangle = \langle A, aba, ab^{-1}a \rangle,$$

garantem que podemos supor, sem perda de generalidade, que $aba, ab^{-1}a \in A$. Dessa forma segue que $\langle aba, c \rangle$ e $\langle ab^{-1}a, c \rangle$ têm expoente 3, portanto

$$a^3 = b^3 = c^3 = (ab)^3 = (bc)^3 = (ca)^3 = (bc^{-1})^3 = (ca^{-1})^3 = (ab^{-1})^3 = (abac)^3$$
$$= (abac^{-1})^3 = (ab^{-1}ac)^3 = (ab^{-1}ac^{-1})^3 = (a^{-1}bc)^6 = (ab^{-1}c)^6 = (abc^{-1})^6 = 1$$

Novamente, considerando as contas feitas no GAP vemos que $|\langle a,b,c\rangle| \leq 3^7$ e portanto $\langle a,b,c\rangle$ possui expoente 3.

Mostraremos agora que $\langle a,b,c,d\rangle$ é nilpotente verificando que $[x_1,x_2,x_3,x_4,x_5] = 1$ para quaisquer $x_1,x_2,x_3,x_4,x_5 \in \{a,b,c,d\}$.

O Teorema 3.6, garante que qualquer grupo de expoente 3 tem classe de nilpotência no máximo 3. Dessa forma, a identidade desejada para um comutador em que algum dos termos x_1,x_2,x_3,x_4 se repete é garantida. Resta verificar então que

$$[a,b,c,d,a] = [a,b,c,d,b] = [a,b,c,d,c] = [a,b,c,d,d] = 1$$

Para tanto, com um argumento análogo ao utilizando anteriormente, podemos supor que $[a,b,c] \in A$, pois $[a,b,c]^3 = 1$ e $x[a,b,c]x = [a,b,c]^{-1}$. Assim, o subgrupo $\langle [a,b,c],d,a\rangle$ tem expoente 3 e portanto a Proposição 3.7 garante que $[[a,b,c],d,a] = [[a,b,c],a,d]^{-1}$, ou seja,

$$[a,b,c,d,a] = [[a,b,c],d,a] = [[a,b,c],a,d]^{-1} = [[a,b,c,a],d]^{-1} = 1.$$

Pois, como vimos, $[a,b,c,a] = 1$. Analogamente provamos que

$$[a,b,c,d,b] = [a,b,c,d,c] = 1.$$

Por fim, como $\langle [a,b,c],d\rangle$ tem expoente 3, novamente o Teorema 3.6, garante que

$$[a,b,c,d,d] = [[a,b,c],d,d] = 1.$$

Logo $\langle a,b,c,d\rangle$ é nilpotente de classe no máximo 4.

Mostraremos agora que os fatores $\gamma_i(\langle a,b,c,d\rangle)/\gamma_{i+1}(\langle a,b,c,d\rangle)$ para $1 \leq i \leq 4$ tem expoente 3. O termo $\gamma_i(\langle a,b,c,d\rangle)/\gamma_{i+1}(\langle a,b,c,d\rangle)$ é gerado, módulo $\gamma_{i+1}(\langle a,b,c,d\rangle)$ por comutadores $[a_1,\cdots,a_i]$ onde $a_i \in \{a,b,c,d\}$, se $i \leq 3$, então $[a_1,a_2,a_3] \in \langle a_1,a_2,a_3\rangle$ que possui expoente 3. Se $i = 4$, então $[a_1,a_2,a_3,a_4]^3 = [[a_1,a_2,a_3]^3,a_4]$ pois $\gamma_i(\langle a,b,c,d\rangle)/\gamma_{i+1}(\langle a,b,c,d\rangle)$ é abeliano. Como $[a_1,a_2,a_3]^3 = 1$ terminamos.

Logo, os fatores da série central inferior de $\langle a,b,c,d\rangle$ são grupos de expoente 3 e, portanto, 3-grupos, o que garante que $\langle a,b,c,d\rangle$ também é 3-grupo. Sendo também um subgrupo de um grupo de expoente 6, $\langle a,b,c,d\rangle$ tem expoente 3. Portanto, pelo Teorema 3.6,

$\langle a,b,c,d\rangle$ tem classe de nilpotência no máximo 3, logo $[a,b,c,d]=1$ onde a,b,c,d foram tomados arbitrariamente em A, ou seja, $\langle A\rangle$ é nilpotente de classe no máximo 3, analogamente ao argumento para $\langle a,b,c,d\rangle$, temos que $\langle A\rangle$ possui expoente 3. □