Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Geração de Grupos Finitos e Crown-Based Powers

André Pereira Araújo

Brasília

2022

André Pereira Araújo

Geração de Grupos Finitos e Crown-Based Powers

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de MESTRE em Matemática.

Orientador:
Prof. Dr. Martino Garonzi

Brasília

2022

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Geração de grupos finitos e crown-based powers

por

André Pereira Araújo

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 02 de março de 2022.

Comissão Examinadora:

Prof. Dr. Martino Garonzi- MAT/UnB (Orientador)

Profa. Dra. Cristina Acciarri- MAT/UnB (Membro)

Prof. Dr. Mohsen Amiri– UFAM (Membro)

"Todas as vitórias ocultam uma abdicação."

(Simone de Beauvoir)

Agradecimentos

Desejo exprimir meus agradecimentos a todos aqueles que, de alguma forma, contribuíram para que eu chegasse até aqui.

Primeiramente, agradeço à minha família pelo apoio e incentivo que serviram de alicerce para as minhas realizações. Em especial, agradeço aos meus pais, José e Sônia, que estiveram ao meu lado durante essa caminhada e me acolheram nos momentos em que eu mais precisei. Também, agradeço ao meu irmão, Murilo, pela amizade e por compreender as minhas ausências durante o mestrado, e ao meu avô, Celso, pelo constante sorriso no rosto que, de certo modo, deixava meus dias mais felizes.

Ao Martino Garonzi, meu orientador, por toda a dedicação, compromisso, paciência e ensinamentos. Tenho admiração por sua genialidade e didática, as quais me ajudaram bastante na elaboração desta dissertação.

À minha psicóloga, Daiany, que me acompanhou desde o início dessa jornada, um momento em que minha saúde mental estava prejudicada. Agradeço por todo o suporte dado nesse período, que foi fundamental para a conclusão de cada etapa do mestrado.

Ao Felipe, que esteve presente em minha vida nesses últimos 6 anos. Agradeço pela amizade, pelas inúmeras ajudas e também por ter tomado a iniciativa para fazermos o mestrado em Brasília.

Aos meus amigos e colegas que tive a oportunidade de conhecer durante o mestrado – Amanda, Francisca, Júlia, Roberto e Wendy. Em especial, agradeço à Amanda pelo carinho, por ser uma pessoa com quem me sinto à vontade para me expressar e por todos os conselhos dados, dos quais só segui alguns. Agradeço também à Francisca pela amizade, pela confiança, por todo o incentivo e por ter feito propaganda do Martino quando fui procurar um orientador.

Aos meus amigos e colegas da UFG – Afonso, Gabriela Torres, Gabriella Cristina, Laura, Lucas, Marco Antônio, Marielson, Matheus, Vítor Emanoel e Vitória.

Ao meu amigo de infância, Fábio Leonardo, por ser uma pessoa bastante presente em minha vida, contribuindo indiretamente para a conclusão deste trabalho.

Aos professores que contribuíram para a minha formação como mestre – Daniele Nantes, José Luis Teruel, Manuela Caetano, Noraí Rocco, Raimundo Bastos e Willian Cintra.

Aos professores da UFG, e, em especial, ao Bruno Rodrigues, ao Glaydston de Carvalho, à Ivonildes Ribeiro, ao Marcos Leandro e à Maria Bethânia.

Agradeço também à ex-funcionária da UFG, Val Rocha, pelo carinho e pelas conversas nesses últimos 3 anos.

Aos membros da banca, Cristina Acciarri, Igor dos Santos Lima e Mohsen Amiri, por aceitarem fazer parte desse momento e pelas correções e sugestões propostas à versão final desta dissertação.

Por fim, agradeço ao CNPq pelo financiamento durante a elaboração deste trabalho.

Resumo

Este trabalho apresenta um estudo acerca da relação entre a geração de grupos finitos e os grupos crown-based power. Mais precisamente, respondemos a seguinte pergunta: qual a estrutura dos grupos finitos que precisam de mais geradores do que qualquer quociente próprio? Em paralelo com esta questão, estudamos a função $f(L, m)$, apresentada no artigo *Finite groups that need more generators than any proper quotient* [8], para um grupo primitivo monolítico m-gerado L. Além disso, fazemos um estudo dos grupos eficientemente gerados, definidos no artigo *Generating sets of finite groups* [4], mostrando que um grupo solúvel finito é eficientemente gerado se, e somente se, ou é um p-grupo finito, ou o quociente do subgrupo de Frattini é um certo grupo do tipo crown-based power.

Palavras-chave: grupos crown-based power; primitivo; monolítico; grupos eficientemente gerados.

Abstract

This work presents a study about the relationship between the generation of finite groups and crown-based power groups. More precisely, we answer the following question: what is the structure of finite groups that need more generators than any proper quotient? In parallel with this question, we study the function $f(L, m)$, presented in the article *Finite groups that need more generators than any proper quotient* [8], for a monolithic primitive m-generated group L. Furthermore, we study the efficiently generated groups, defined in the article *Generating sets of finite groups* [4], showing that a finite solvable group is efficiently generated if only if it is either a finite p-group or its quotient over the Frattini subgroup is a certain crown-based power group.

Keywords: crown-based power groups; primitive; monolithic; efficiently generated groups.

Notações

$\varnothing$	Conjunto vazio
$\lvert S\rvert$	Cardinalidade do conjunto S
$X \subseteq Y$	X é um subconjunto do conjunto Y
$H \leq G$	H é um subgrupo do grupo G
$H < G$	H é um subgrupo próprio do grupo G
$\{1\}$	Subgrupo trivial de um grupo
$H \trianglelefteq G$	H é um subgrupo normal do grupo G
$H \ntrianglelefteq G$	H não é um subgrupo normal do grupo G
$H \trianglelefteq_c G$	H é um subgrupo característico do grupo G
Hg	Classe lateral à direita de H em G contendo g
gH	Classe lateral à esquerda de H em G contendo g
$[G : H]$	Índice de H em G
$\langle X_\lambda \mid \lambda \in \Lambda \rangle$	Subgrupo gerado pelos subconjuntos X_λ de um grupo
x^α, $(x)\alpha$ ou $x\alpha$	Imagem de x pela aplicação α
X^α	$\{x^\alpha \mid x \in X\}$
x^y	$y^{-1}xy$
H^g	$\{h^g \mid h \in H\}$
H^G	$\langle H^g \mid g \in G \rangle$
$[x, y]$	$x^{-1}y^{-1}xy$
$[H, K]$	$\langle [h, k] \mid h \in H,\ k \in K \rangle$
G'	Subgrupo comutador $[G, G]$ de G

$H \cong G$	H é isomorfo a G
$H \cong_G K$	H é G-isomorfo a K
$A_1 \times \cdots \times A_n$	Produto cartesiano dos conjuntos $A_1, \ldots, A_n$
$\operatorname*{Dr}_{1 \leq i \leq n} G_i$	Produto direto (externo) de $G_1, \ldots, G_n$
G^n	Produto direto de n cópias de G
$\operatorname{diag}(G^n)$	Subgrupo diagonal $\{(g, \ldots, g) \mid g \in G\}$ de G^n
$\operatorname*{Dr}^{(i)}_{1 \leq i \leq n} H_i$	Produto direto interno dos subgrupos $H_1, \ldots, H_n$
$K \rtimes H$	Produto semidireto externo de K por H
$H \wr K$	Produto entrelaçado entre H e K
H_G	Coração normal de H em G
$Z(G)$	Centro de G
$C_G(H)$, $N_G(H)$	Centralizador, normalizador de H em G
$\Phi(G)$	Subgrupo de Frattini de G
$G^{\langle p \rangle}$	$\langle g^p \mid g \in G \rangle$
$O_p(G)$	Produto dos p-subgrupos normais de G
$\operatorname{soc}(G)$	Subgrupo gerado pelos normais minimais de G
L_k	Subgrupo crown-based power de L^k
$d(G)$	Número mínimo de geradores de G
$d_X(G)$	Número mínimo de elementos de G que geram G juntamente com X
$\phi_G(m)$	Número de m-bases de G
$\mathcal{O}_G(x)$, $\operatorname{Stab}_G(x)$	Órbita, estabilizador de x em G
$\operatorname{Im}(\varphi)$, $\ker(\varphi)$	Imagem, núcleo do homomorfismo φ
$\operatorname{Sim}(X)$	Grupo das permutações do conjunto X
S_n, A_n	Grupo simétrico, alternado de grau n
$\operatorname{End}(G)$, $\operatorname{Aut}(G)$	Grupo dos endomorfismos, automorfismos de G
$\mathcal{I}_g$	Automorfismo interno associado ao elemento g
$\operatorname{Inn}(G)$	Grupo dos automorfismos internos de G

$\mathrm{End}_G(H)$	Conjunto dos G-endomorfismos de H
C_n	Grupo cíclico de ordem n
$\mathbb{Z}_p$	Corpo com p elementos
$\dim_F V$	Dimensão do espaço vetorial V sobre o corpo F
$\mathbb{N}, \mathbb{Z}$	Conjunto dos números naturais, inteiros
$\mathbb{Z}_+$	Conjunto dos números inteiros positivos
R^*	Conjunto $R \setminus \{0\}$
Γ_L	Grupo dos automorfismos que agem trivialmente em L/M, sendo L um grupo primitivo monolítico com $\mathrm{soc}(L) = M$
$f(L, m)$	Função associada a um grupo primitivo monolítico não cíclico m-gerado L
$P_m(G)$	Probabilidade de uma m-upla gerar o grupo G
$P_G(X, t)$	Probabilidade de que uma t-upla gere G juntamente com os elementos do subconjunto X
$\equiv_{\mathrm{m}}$	Relação de equivalência associada aos subgrupos maximais de um grupo finito

Sumário

Introdução

Dado X um subconjunto de um grupo G, o *subgrupo gerado por* X é definido como a interseção de todos os subgrupos de G que contêm X, e este é denotado por $\langle X \rangle$. Quando X é vazio, $\langle X \rangle = \{1\}$. Se $G = \langle X \rangle$, então dizemos que X gera G. E se $|X| = n$ para algum inteiro positivo n, dizemos que G é *finitamente gerado*, ou mais precisamente, *n-gerado*. Observamos que se N é um subgrupo normal de G, então $G = \langle x_1, \ldots, x_k, N \rangle$ se, e somente se, $G/N = \langle Nx_1, \ldots, Nx_k \rangle$.

Seja G um grupo finito. Definimos $d(G)$ como a *menor* das cardinalidades dos conjuntos geradores de G. Temos, por exemplo, que $d(G) = 1$ se, e somente se, G é cíclico e não trivial. O grupo trivial é gerado pelo conjunto vazio, por isso $d(\{1\}) = 0$. Também, como mostrado em [1, 25], se G é um grupo simples, então $d(G) \leq 2$. Agora, sabemos do Teorema de Cayley que todo grupo finito G pode ser visto como um subgrupo de S_n (com $n = |G|$). Uma vez que $S_n = \langle (12), (12 \cdots n) \rangle$ é não cíclico, temos que $d(S_n) = 2$ (para $n \geq 3$), mas $d(G)$ não é necessariamente menor ou igual a 2. Ou seja, se H é um subgrupo de G, não é válido em geral que $d(H) \leq d(G)$. Ainda que H seja um subgrupo normal de G, esta afirmação continua sendo falsa. Como exemplo, podemos tomar $G = S \wr C_n$ (produto entrelaçado entre um grupo simples não abeliano finito S e $C_n = \langle (12 \cdots n) \rangle$ – vide Definição 1.6.10). É possível mostrar que $d(G) = 2$, todavia, considerando $H = S^n \times \{1\} \trianglelefteq G$, temos que $d(H)$ tende a infinito com n.

Observamos que, para espaços vetoriais, o conceito análogo à função $d(G)$ é a dimensão. A diferença é que, quando tratamos de geração de espaços vetoriais, estamos falando de combinações lineares, enquanto que para grupos não temos necessariamente um produto escalar definido sobre um corpo qualquer, ou seja, a geração de grupos é baseada apenas em sua operação, o que deixa o estudo mais complicado.

Contudo, os grupos abelianos elementares são uma interseção dessas teorias. Mais precisamente, os grupos C_p^n, com $n \in \mathbb{N}$, podem ser vistos de maneira natural como espaços vetoriais de dimensão n sobre o corpo finito $\mathbb{Z}_p$ de modo que um subconjunto

X gera C_p^n como um grupo se, e somente se, X gera C_p^n como um espaço vetorial. Isto é,

$$d(C_p^n) = \dim_{\mathbb{Z}_p} C_p^n = n.$$

Esses grupos também fornecem-nos que é sempre possível obter um grupo G com $d(G) = n$, para $n \in \mathbb{N}$ arbitrário.

O *subgrupo de Frattini* de um grupo G, denotado por $\Phi(G)$, é definido como a interseção de todos os subgrupos maximais de G; e se G não possui tais subgrupos, $\Phi(G) = G$. Observamos que $d(G) = d(G/\Phi(G))$, e se G é um p-grupo finito, então $G/\Phi(G) \cong C_p^n$, para algum primo p e algum número natural n, de maneira que

$$d(G) = d(G/\Phi(G)) = n.$$

Dado N um subgrupo normal de um grupo finito G, temos

$$d(G/N) \leq d(G) \leq d(N) + d(G/N).$$

Se existe $\{1\} \neq N \trianglelefteq G$ tal que $d(G) = d(G/N)$, o problema de calcular o valor de $d(G)$ é reduzido a um grupo quociente. Dessa forma, faz sentido estudar grupos em que esta igualdade nunca acontece, ou seja, $d(G/N) < d(G)$ para todo subgrupo normal não trivial N de G. O objetivo deste trabalho é caracterizar os grupos finitos com esta propriedade.

Seja $\{1\} \neq N \trianglelefteq G$. Dizemos que N é um subgrupo normal minimal de G se não existe subgrupo normal K de G tal que $\{1\} < K < N$. No sentido de comparar $d(G)$ com $d(G/N)$, Andrea Lucchini, em seu artigo *Generators and minimal normal subgroups* [18], de 1995, mostrou que se N é um subgrupo normal minimal de um grupo finito G, então

$$d(G) \leq \max\{2, d(G/N) + 1\}.$$

Também, nos artigos [1] e [20], os autores provaram que se G é um grupo não cíclico finito contendo um único subgrupo normal minimal N, então

$$d(G) = \max\{2, d(G/N)\}.$$

Para um grupo finito G, o *socle* de G é definido como o produto dos subgrupos normais minimais e é denotado por $\mathrm{soc}(G)$. Nesse sentido, dizemos que G é um grupo *monolítico* se este contém um único subgrupo normal minimal N, isto é, $N = \mathrm{soc}(G)$. Também, G é dito *primitivo* se existe um subgrupo maximal M de G tal que o coração

normal de M em G,

$$M_G = \bigcap_{g \in G} M^g,$$

é trivial. Temos que um grupo monolítico G é primitivo se, e somente se, $\Phi(G) = \{1\}$. Dessa forma, S_n, para $n \geq 3$, é um grupo primitivo monolítico. Um exemplo de um grupo primitivo não monolítico é o grupo $S \times S$, sendo S um grupo simples não abeliano. Este é primitivo, pois $\mathrm{diag}(S \times S) = \{(s,s) \mid s \in S\}$ é um subgrupo maximal com coração normal trivial, e não é monolítico porque $S \times \{1\}$ e $\{1\} \times S$ são subgrupos normais minimais de $S \times S$.

Seja L um grupo primitivo monolítico não cíclico finito, com $M = \mathrm{soc}(L)$. Observamos que se M é abeliano, este é complementado em L, ou seja, existe um subgrupo H de L tal que $HM = L$ e $H \cap M = \{1\}$. Para cada inteiro positivo k, definimos o *subgrupo crown-based power* L_k de L^k por

$$L_k = \{(l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \mod M\}.$$

Temos que o socle de L_k é M^k, um produto direto de k subgrupos normais minimais, e que $L_k/M^k \cong L/M$. Além disso, o grupo quociente de L_{k+1} sobre qualquer subgrupo normal minimal U é isomorfo a L_k, e $\mathrm{soc}(L_{k+1}/U) = \mathrm{soc}(L_{k+1})/U$. Com isso, a sequência $d(L_1), \ldots, d(L_k), \ldots$ é não decrescente. É possível mostrar que esta é ilimitada, e, pelo resultado acima, provado por Lucchini, $d(L_{k+1}) \leq d(L_k) + 1$. Desse modo, se L é um grupo m-gerado, então existe um (único) k tal que $d(L_k) = m < d(L_{k+1})$, e, então, definimos $f(L,m) = k+1$. Escrevemos simplesmente $f(m)$ se L pode ser identificado no contexto.

Com esta definição da função f, Francesca Dalla Volta e Andrea Lucchini, em [8], provaram o seguinte teorema estrutural:

Teorema A. *Seja m um inteiro positivo e H um grupo finito tal que $d(H/N) \leq m$ para todo subgrupo normal não trivial N, mas $d(H) > m$. Se $m = 1$, então ou $H \cong C_p \times C_p$ para algum primo p, ou H é um grupo primitivo monolítico com socle M e H/M é cíclico. Se $m \geq 2$, então existe um grupo primitivo monolítico L tal que $H \cong L_{f(L,m)}$.*

Ou seja, este resultado nos fornece uma caracterização dos grupos finitos com a propriedade que, para algum inteiro positivo m, todo grupo quociente próprio pode ser gerado por m elementos, mas o grupo não.

Dados G um grupo finito e m um inteiro positivo, seja $\phi_G(m)$ o número de *m-bases* de G, ou seja, m-uplas ordenadas $(g_1, \ldots, g_m)$ de elementos de G que geram G. Esta

função foi introduzida em 1936, por Philip Hall [15], com o nome de *função Euleriana*. Considerando L como acima, dizemos que um automorfismo $\gamma : L \to L$ *age trivialmente* em L/M se o homomorfismo induzido

$$\overline{\gamma} : L/M \to L/M, \quad Ml \mapsto Ml^{\gamma}$$

é a identidade. Isto equivale a dizer que $l^{\gamma} \in Ml$, para todo $l \in L$. Observamos que $\overline{\gamma}$ está bem definida, já que M é um subgrupo característico de L. O grupo dos automorfismos de L que agem trivialmente em L/M é denotado por Γ_L. Com o intuito de estudar o valor da função f, Francesca Dalla Volta e Andrea Lucchini também provaram em [8] o seguinte teorema:

Teorema B. *Se $m \geq d(L)$, então*

$$f(m) = 1 + \begin{cases} \phi_L(m)/|\Gamma_L|\phi_{L/M}(m) & \text{se } M' = M, \\ \log_q(1 + (q-1)\phi_L(m)/|\Gamma_L|\phi_{L/M}(m)) & \text{se } M' = \{1\}, \end{cases}$$

sendo $q = |\mathrm{End}_L(M)|$.

Para M abeliano, Wolfgang Gaschütz mostrou em [13] que

$$\phi_L(m)/\phi_{L/M}(m) = |M|^m - \omega,$$

sendo que ω é o número de complementos para M em L. Além disso, temos que $|\Gamma_L| = (q-1)\omega$, logo o Teorema B nos dá que

$$f(m) = 1 + \log_q(|M|^m/\omega).$$

Como exemplos do cálculo da função f, temos que

$$f(A_5, 2) = 20,$$

porque $d(A_5^{19}) = 2 < d(A_5^{20})$, e

$$n!/8 + 1 < f(A_n, 2) \leq n!/4 + 1,$$

para n suficientemente grande (vide Exemplos 2.4.7 e 2.4.8). Em geral, não é uma tarefa fácil calcular o valor da função f.

Agora, dado G um grupo finito, definimos a relação de equivalência $\equiv_{\mathrm{m}}$ em G por:

$x \equiv_{\mathrm{m}} y$ se, e somente se, x e y estão exatamente nos mesmos subgrupos maximais de G. Equivalentemente, $x \equiv_{\mathrm{m}} y$ se, e somente se,

$$(\forall r)(\forall z_1, \ldots, z_r \in G)((\langle x, z_1, \ldots, z_r\rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_r\rangle = G)).$$

Dado um inteiro positivo r, definimos a relação de equivalência $\equiv_{\mathrm{m}}^{(r)}$ pela regra: $x \equiv_{\mathrm{m}}^{(r)} y$ se, e somente se,

$$(\forall z_1, \ldots, z_{r-1} \in G)((\langle x, z_1, \ldots, z_{r-1}\rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_{r-1}\rangle = G)).$$

Observamos que as relações $\equiv_{\mathrm{m}}^{(r)}$ tornam-se mais finas à medida que r aumenta, e se $r = |G|$, então $\equiv_{\mathrm{m}}^{(r)}$ coincide com $\equiv_{\mathrm{m}}$. Logo, definimos $\psi(G)$ como o valor de r para o qual as equivalências $\equiv_{\mathrm{m}}^{(r)}$ se estabilizam, isto é, o menor valor r tal que $\equiv_{\mathrm{m}}^{(r)}$ coincide com a relação limite $\equiv_{\mathrm{m}}$. Para um grupo solúvel finito G, é possível provar que $\psi(G) \in \{d(G), d(G)+1\}$.

Dado um subconjunto X de um grupo finito G, denotamos por $d_X(G)$ a *menor* cardinalidade de um conjunto de elementos de G que gera G juntamente com os elementos de X. Notemos que $d_X(G) \leq d(G)$. Um grupo finito G é dito *eficientemente gerado* se, para todo $x \in G$, $d_{\{x\}}(G) = d(G)$ implica em $x \in \Phi(G)$. Temos que todo p-grupo finito é eficientemente gerado. Também, o grupo diedral D_5 é um tal grupo, e S_4 é um exemplo de um grupo não eficientemente gerado, pois $d_{\{x\}}(S_4) = 2$ para todo elemento x do subgrupo de Klein.

Se G é um grupo solúvel finito, então G é eficientemente gerado se, e somente se, $\psi(G) = d(G)$. Nesse sentido, Peter Cameron, Andrea Lucchini e Colva Mary Roney-Dougal, em [4], provaram um resultado que caracteriza os grupos solúveis eficientemente gerados. Esse, por sua vez, é uma aplicação dos Teoremas A e B. Mais precisamente,

Teorema C. *Um grupo solúvel finito G satisfaz $\psi(G) = d(G)$ se, e somente se, ou G é um p-grupo finito, ou existe um espaço vetorial finito V, um subgrupo solúvel irredutível não trivial H de* $\mathrm{Aut}(V)$ *e um inteiro $d > d(H)$ tal que*

$$G/\Phi(G) \cong V^{r(d-2)+1} \rtimes H,$$

sendo r a dimensão de V sobre $\mathrm{End}_H(V)$ *e H age da mesma maneira em cada um dos $r(d-2)+1$ fatores.*

Aqui, um subgrupo *irredutível* H de $\mathrm{Aut}(V)$ significa que se W é um subespaço

H-invariante de V ($w^h \in W$ para todos $w \in W$ e $h \in H$), então $W = \{0\}$ ou $W = V$.

Neste trabalho, apresentaremos as demonstrações dos Teoremas A, B e C.

No primeiro capítulo, apresentaremos resultados fundamentais acerca da Teoria de Grupos, como por exemplo a caracterização dos subgrupos normais minimais de um grupo finito, o Teorema da Base de Burnside, Lema de Schur, etc. Estes serão utilizados ao longo do trabalho.

O segundo capítulo é destinado ao assunto principal deste trabalho. Iremos construir as noções essenciais sobre grupos primitivos e monolíticos, a função $d(G)$, bem como apresentar as definições e resultados a respeito dos subgrupos crown-based power, que serão necessários para demonstrar os Teoremas A e B.

No terceiro e último capítulo, iremos inicialmente expor algumas noções de probabilidade envolvendo geração de grupos e, posteriormente, vamos desenvolver a teoria necessária para a demonstração do Teorema C.

Capítulo

1

Preliminares

Neste capítulo, apresentaremos conceitos básicos e resultados preliminares, que vamos utilizar ao longo deste trabalho. Resultados como Teorema de Lagrange, Teorema dos Isomorfismos, Teorema da Correspondência, Teorema de Sylow, bem como resultados a respeito de Grupos Simétricos e Álgebra Linear, serão assumidos como conhecidos, podendo ser encontrados em [12, 16, 22], por exemplo.

1.1 Teoria de Grupos

Os resultados presentes nesta seção podem ser encontrados em [12, 22, 24]. Iniciamos com algumas definições e resultados básicos acerca de geração de grupos.

Seja X um subconjunto de um grupo G. Definimos o *subgrupo gerado por* X

$$\langle X \rangle$$

como a interseção de todos os subgrupos de G que contêm X. Notemos que sempre existe pelo menos um tal subgrupo, a saber G. Uma vez que a interseção de subgrupos de um grupo é um subgrupo, segue-se que $\langle X \rangle$ é de fato um subgrupo de G. Mais ainda, $\langle X \rangle$ é o *menor* subgrupo de G contendo X: se $X \subseteq S \leq G$, então $\langle X \rangle \leq S$. No caso em que $X = \varnothing$, temos $\langle X \rangle = \{1\}$. Se $G = \langle X \rangle$, então dizemos que X gera G; e os elementos de X são chamados geradores.

Proposição 1.1.1. *Seja X um subconjunto não vazio de um grupo G. Então*

$$\langle X \rangle = \{x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \mid x_i \in X,\ \epsilon_i = \pm 1,\ k \in \mathbb{N}\}.$$

(Quando $k = 0$, o produto é interpretado como 1.)

Demonstração. Seja $S = \{x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \mid x_i \in X,\ \epsilon_i = \pm 1,\ k \in \mathbb{N}\}$. Temos que S é um subgrupo de G. De fato, $1 = xx^{-1} \in S$, $x \in X$ (visto que $X \neq \varnothing$). Além disso, dados $x = x_1^{\epsilon_1} \cdots x_k^{\epsilon_k}$ e $y = y_1^{\delta_1} \cdots y_l^{\delta_l}$ elementos arbitrários de S,

$$xy^{-1} = x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} y_l^{-\delta_l} \cdots y_1^{-\delta_1} \in S.$$

Assim, $S \leq G$, e este contém X. Pela definição de $\langle X \rangle$, obtemos que $\langle X \rangle \subseteq S$. Por fechamento, $S \subseteq \langle X \rangle$, e, portanto, $S = \langle X \rangle$. □

Seja n um inteiro positivo. Um grupo é dito *n-gerado* se pode ser gerado por algum subconjunto $\{x_1, x_2, \ldots, x_n\}$. Um grupo é *finitamente gerado* se é n-gerado para algum n.

Se $\{X_\lambda \mid \lambda \in \Lambda\}$ é um conjunto de subgrupos de G, o *subgrupo gerado pelos X_λ's* é definido como $\langle \bigcup_{\lambda \in \Lambda} X_\lambda \rangle$. Este é denotado por

$$\langle X_\lambda \mid \lambda \in \Lambda \rangle.$$

No caso em que $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$, escrevemos

$$\langle X_{\lambda_1}, \ldots, X_{\lambda_n} \rangle.$$

Se G é um grupo gerado por um subconjunto X, então qualquer homomorfismo de G em um grupo H é unicamente determinado pelas imagens dos elementos de X. Mais precisamente,

Proposição 1.1.2. *Sejam G e H dois grupos, e suponhamos que G seja gerado por X. Se ϕ e ψ são homomorfismos de G em H, e se ϕ e ψ coincidem em X, então $\phi = \psi$.*

Demonstração. Seja $g \in G$, logo pela Proposição 1.1.1, $g = x_1^{\epsilon_1} \cdots x_k^{\epsilon_k}$, com $k \in \mathbb{N}$, e, para cada $i = 1, \ldots, k$, $x_i \in X$ e $\epsilon_i = \pm 1$. Daí,

$$g^\phi = (x_1^{\epsilon_1} \cdots x_k^{\epsilon_k})^\phi = (x_1^\phi)^{\epsilon_1} \cdots (x_k^\phi)^{\epsilon_k} = (x_1^\psi)^{\epsilon_1} \cdots (x_k^\psi)^{\epsilon_k} = (x_1^{\epsilon_1} \cdots x_k^{\epsilon_k})^\psi = g^\psi,$$

já que ϕ e ψ coincidem em X. Como g é arbitrário, concluímos que $\phi = \psi$. □

Proposição 1.1.3. *Se ψ é um homomorfismo de um grupo G em um grupo H, e se $G = \langle X \rangle$, então $\mathrm{Im}(\psi) = \langle X^\psi \rangle$, sendo $X^\psi = \{x^\psi \mid x \in X\}$. Em particular, se ψ é sobrejetiva, então $H = \langle X^\psi \rangle$.*

Demonstração. Seja $h \in \mathrm{Im}(\psi)$. Então, existe $g \in G$ tal que $h = g^{\psi}$. Pela Proposição 1.1.1, $g = x_1^{\epsilon_1} \cdots x_k^{\epsilon_k}$, com $k \in \mathbb{N}$, e, para cada $i = 1, \ldots, k$, $x_i \in X$ e $\epsilon_i = \pm 1$. Logo,

$$h = g^{\psi} = (x_1^{\epsilon_1} \cdots x_k^{\epsilon_k})^{\psi} = (x_1^{\psi})^{\epsilon_1} \cdots (x_k^{\psi})^{\epsilon_k} \in \langle X^{\psi} \rangle.$$

Isto nos dá que $\mathrm{Im}(\psi) \subseteq \langle X^{\psi} \rangle$. Por outro lado, $\mathrm{Im}(\psi)$ é um subgrupo de H que contém X^{ψ}. Por definição, obtemos que $\langle X^{\psi} \rangle \subseteq \mathrm{Im}(\psi)$. Portanto, $\mathrm{Im}(\psi) = \langle X^{\psi} \rangle$. □

Em particular, se G é um grupo o qual admite um subgrupo normal N tal que $G = \langle x_1, \ldots, x_k, N \rangle$, então $G/N = \langle Nx_1, \ldots, Nx_k \rangle$ (basta considerar a projeção canônica $\pi : G \to G/N$ e aplicar a Proposição 1.1.3). Por outro lado, se $G/N = \langle Nx_1, \ldots, Nx_k \rangle$, então considerando $H = \langle x_1, \ldots, x_k, N \rangle$, temos que

$$G/N = \langle Nx_1, \ldots, Nx_k \rangle \subseteq H/N$$

donde, por correspondência, $G = H$. Ou seja, mostramos que $G = \langle x_1, \ldots, x_k, N \rangle$ se, e somente se, $G/N = \langle Nx_1, \ldots, Nx_k \rangle$. Nesse sentido, dizemos que $x_1, \ldots, x_k$ são *geradores para G módulo N*.

Dado G um grupo, definimos o *comutador de dois elementos $x, y \in G$* como

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

Com isso, segue-se facilmente que $[x, y] = [y, x]^{-1}$ e $[x, y] = 1$ se, e somente se, x e y comutam.

Agora, dados dois subgrupos H e K de G, definimos o *comutador de H e K* por

$$[H, K] = \langle [h, k] \mid h \in H,\ k \in K \rangle.$$

Como $[h, k] = [k, h]^{-1}$ para todos $h \in H$ e $k \in K$, temos que $[H, K] = [K, H]$. Denotamos por G' o subgrupo $[G, G]$.

Observação 1.1.4. *Sejam G um grupo e H um subgrupo de G. Então, $G' \leq H$ se, e somente se, $H \trianglelefteq G$ e G/H é abeliano. De fato, basta notar que dados $h \in H$ e $x, y \in G$, temos que $h^x = [x, h^{-1}]h$ (logo $H \trianglelefteq G$ se $G' \leq H$), como também $[Hx, Hy] = H[x, y]$ de modo que*

$$[Hx, Hy] = H \Leftrightarrow H[x, y] = H \Leftrightarrow [x, y] \in H,$$

e, portanto, a observação segue.

Definição 1.1.5. *Sejam $n \geq 2$ e $G_1, \ldots, G_n$ grupos. O produto direto (externo) de $G_1, \ldots, G_n$ é definido como sendo o produto cartesiano $G_1 \times \cdots \times G_n$ com a operação*

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) := (x_1 y_1, \ldots, x_n y_n),$$

e este é denotado por $\operatorname*{Dr}_{1 \leq i \leq n} G_i$ ou $G_1 \times \cdots \times G_n$. Se $G_1 = \cdots = G_n =: G$, então usamos a notação G^n para indicar o grupo $G \times \cdots \times G$ (produto direto de n cópias de G). Além disso, se a operação de G for aditiva, chamamos G^n por a soma direta de n cópias de G.

Observamos que os subconjuntos

$$\widetilde{G}_i = \{(1, \ldots, 1, g_i, 1, \ldots, 1) \mid g_i \in G_i\} \quad (1 \leq i \leq n)$$

são subgrupos normais de $G_1 \times \cdots \times G_n$. Estes são chamados os fatores diretos.

Teorema 1.1.6. *Sejam $G, G_1, \ldots, G_n$ grupos. Então o grupo G é isomorfo ao grupo $\operatorname*{Dr}_{1 \leq i \leq n} G_i$ se, e somente se, G admite subgrupos $H_1 \cong G_1, \ldots, H_n \cong G_n$ tais que:*

(i) $G = H_1 \cdots H_n$.

(ii) $H_i \trianglelefteq G$, $\forall i = 1, \ldots, n$.

(iii) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{1\}$, $\forall i = 1, \ldots, n$.

Ou, equivalentemente,

(iv) Para cada $g \in G$, existem únicos elementos $x_1 \in H_1, \ldots, x_n \in H_n$ tais que $g = x_1 \cdots x_n$.

(v) Para cada $i \neq j$ em $\{1, \ldots, n\}$, temos $xy = yx$, $\forall x \in H_i$ e $\forall y \in H_j$.

Um grupo G o qual admite subgrupos $H_1, \ldots, H_n$ satisfazendo as condições (i), (ii) e (iii) do Teorema 1.1.6 é chamado o *produto direto interno de $H_1, \ldots, H_n$* e é denotado por $\operatorname*{Dr}^{(i)}_{1 \leq i \leq n} H_i$.

Definição 1.1.7. *Seja H um subgrupo de um grupo G. Definimos o normalizador e o centralizador de H em G como sendo, respectivamente, os conjuntos $N_G(H) = \{g \in G \mid H^g = H\}$ e $C_G(H) = \{g \in G \mid h^g = h, \ \forall h \in H\}$.*

Ambos são subgrupos de G, e $C_G(H) \trianglelefteq N_G(H)$. De fato, sejam $g \in N_G(H)$ e $x \in C_G(H)$ arbitrários, e vamos mostrar que $x^g \in C_G(H)$. Sendo $N_G(H) \leq G$, temos que $g^{-1} \in N_G(H)$. Assim, dado $h \in H$, temos $ghg^{-1} \in H^{g^{-1}} = H$ e

$$\begin{aligned} x^g h &= g^{-1} x g h (g^{-1} g) = g^{-1} x (ghg^{-1}) g \\ &= g^{-1} (ghg^{-1}) x g = h g^{-1} x g = h x^g, \end{aligned}$$

pois $x \in C_G(H)$. Pela arbitrariedade dos elementos envolvidos, segue-se que $C_G(H) \trianglelefteq N_G(H)$. Em particular, se $H \trianglelefteq G$, então $C_G(H) \trianglelefteq G$, pois neste caso $N_G(H) = G$.

Proposição 1.1.8. *Sejam G um grupo e $H, K \trianglelefteq G$ tais que $H \cap K = \{1\}$. Então $H \leq C_G(K)$ e $K \leq C_G(H)$.*

Demonstração. Seja $h \in H$. Dado $k \in K$, temos

$$[h,k] = h^{-1}(k^{-1}hk) \in H, \qquad \text{pois } H \trianglelefteq G,$$

e

$$[h,k] = (h^{-1}k^{-1}h)k \in K, \qquad \text{pois } K \trianglelefteq G.$$

Portanto, $[h,k] \in H \cap K = \{1\}$ de sorte que $k^h = k$. Desse modo, $h \in C_G(K)$, e isto mostra que $H \leq C_G(K)$. A segunda parte da proposição é análoga. □

Proposição 1.1.9. *Sejam $G_1, \ldots, G_n$ grupos e $H_1 \leq G_1, \ldots, H_n \leq G_n$. Consideremos $G = G_1 \times \cdots \times G_n$ e $H = H_1 \times \cdots \times H_n$. Então*

$$C_G(H) = C_{G_1}(H_1) \times \cdots \times C_{G_n}(H_n).$$

Em particular, se $k \in \mathbb{Z}_+$ e $H \leq G$, então $C_{G^k}(H^k) = C_G(H)^k$.

Demonstração. Seja $g \in C_{G_1}(H_1) \times \cdots \times C_{G_n}(H_n)$, então $g = (g_1, \ldots, g_n)$, sendo que, para cada i, $1 \leq i \leq n$, $g_i \in C_{G_i}(H_i)$. Assim, dado $h = (h_1, \ldots, h_n) \in H$, temos

$$\begin{aligned} gh &= (g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n) \\ &= (h_1g_1, \ldots, h_ng_n) = (h_1, \ldots, h_n) \cdot (g_1, \ldots, g_n) = hg, \end{aligned}$$

logo $g \in C_G(H)$. Isto nos dá que $C_{G_1}(H_1) \times \cdots \times C_{G_n}(H_n) \leq C_G(H)$. Por outro lado, seja $g \in C_G(H)$. Temos que $g = (g_1, \ldots, g_n)$ com $g_i \in G_i$ $(1 \leq i \leq n)$. Dados $h_1 \in H_1, \ldots, h_n \in H_n$, seja $h = (h_1, \ldots, h_n)$. Assim, $gh = hg$, já que $g \in C_G(H)$. Isto implica $g_ih_i = h_ig_i$ $(1 \leq i \leq n)$. Então $g_i \in C_{G_i}(H_i)$ $(1 \leq i \leq n)$ de maneira que $g \in C_{G_1}(H_1) \times \cdots \times C_{G_n}(H_n)$. Concluímos então a segunda inclusão, e, assim, a proposição segue. □

Observamos que se $G_1, \ldots, G_n$ são grupos quaisquer, então $Z(G_1 \times \cdots \times G_n) = Z(G_1) \times \cdots \times Z(G_n)$. Isto é um caso particular da Proposição 1.1.9: basta escolher $H_i = G_i$ para cada $i \in \{1, \ldots, n\}$.

Definição 1.1.10. *Um subgrupo H de um grupo G é dito um subgrupo característico (denotado por $H \trianglelefteq_c G$) se este é estável por todos os automorfismos de G, isto é, se $H^\sigma \leq H$, $\forall \sigma \in \mathrm{Aut}(G)$. (Equivalentemente, se $H^\sigma = H$, $\forall \sigma \in \mathrm{Aut}(G)$).*

Se $H \trianglelefteq_c G$, então $H \trianglelefteq G$, pois $H^g = H^{\mathscr{I}_g} \leq H$ para todo $g \in G$, sendo $\mathscr{I}_g : G \to G$ o *automorfismo interno* dado por $x^{\mathscr{I}_g} = x^g$, sempre que $x \in G$. Como exemplos de subgrupos característicos, temos $\{1\}$, G, $Z(G)$ e G'.

Proposição 1.1.11. *Se $H \trianglelefteq_c K$ e $K \trianglelefteq G$, então $H \trianglelefteq G$.*

Demonstração. Seja g um elemento arbitrário de G. Dado que $K \trianglelefteq G$, temos que a aplicação $\sigma : K \to K$,

$$x^\sigma = x^{\mathscr{I}_g} = x^g, \qquad x \in K,$$

é um automorfismo de K. Como por hipótese H é característico em K, obtemos que $H^\sigma \leq H$, ou seja, $H^g \leq H$. Pela arbitrariedade de g, concluímos que $H \trianglelefteq G$. □

1.2 Ações de Grupo em Conjuntos

Nesta seção, G denota um grupo arbitrário.

Definição 1.2.1. *Dizemos que G age em um conjunto não vazio X se, para cada $g \in G$ e cada $x \in X$, corresponde um único elemento $xg \in X$ de forma que, para todos $x \in X$ e $g_1, g_2 \in G$,*

$$(xg_1)g_2 = x(g_1g_2)$$

e

$$x1 = x.$$

Mais precisamente, dizemos que, nessas condições, G age em X à direita. De forma análoga, podemos definir ações à esquerda.

Exemplo 1.2.2. *Seja S o conjunto dos subgrupos de G. Então G age em S por conjugação, ou seja, para cada $g \in G$ e cada $H \in S$, $Hg := H^g$. De fato, para todos $H \in S$ e $g_1, g_2 \in G$,*

$$(Hg_1)g_2 = (H^{g_1})g_2 = (H^{g_1})^{g_2} = H^{g_1g_2} = H(g_1g_2) \quad e \quad H1 = H^1 = H.$$

Teorema 1.2.3. *Seja G agindo em X. Então, para cada $g \in G$, corresponde uma aplicação $\rho_g : X \to X$ definida por $\rho_g : x \mapsto xg$, e esta é uma permutação de X. Além disso, a aplicação $\rho : G \to \mathrm{Sim}(X)$ definida por $\rho : g \mapsto \rho_g$ é um homomorfismo; esta é chamada a representação permutacional de G correspondende à ação do grupo.*

Demonstração. Seja $g \in G$. Por definição, ρ_g é uma aplicação de X em si próprio. Dados $g_1, g_2 \in G$ e $x \in X$,

$$x^{\rho_{g_1 g_2}} = x(g_1 g_2) = (xg_1)g_2 = (x\rho_{g_1})\rho_{g_2} = x^{\rho_{g_1}\rho_{g_2}},$$

logo

$$\rho_{g_1 g_2} = \rho_{g_1}\rho_{g_2}. \tag{1.1}$$

Além disso, temos $x^{\rho_1} = x1 = x$, daí

$$\rho_1 = 1 \in \mathrm{Sim}(X). \tag{1.2}$$

Por (1.1) e (1.2), segue-se que

$$\rho_g \rho_{g^{-1}} = 1 = \rho_{g^{-1}}\rho_g.$$

Portanto, ρ_g é uma aplicação inversível de X em si mesmo, ou seja, uma permutação de X. E (1.1) nos dá que ρ é um homomorfismo de G em $\mathrm{Sim}(X)$. □

Teorema 1.2.4. *Seja σ um homomorfismo de G em $\mathrm{Sim}(X)$, onde X é um conjunto não vazio. Então, G age em X quando definimos, para cada $g \in G$ e $x \in X$,*

$$xg = (x)g^{\sigma};$$

e a representação permutacional de G correspondente a esta ação é σ.

Demonstração. Para $g_1, g_2 \in G$ e $x \in X$, temos, por definição de composição de aplicações, que

$$\begin{aligned}((x)g_1^{\sigma})((x)g_2^{\sigma}) &= (x)(g_1^{\sigma}g_2^{\sigma}) \\ &= (x)(g_1 g_2)^{\sigma},\end{aligned}$$

pois σ é um homomorfismo; e $(x)1^{\sigma} = x$, pois σ leva $1 \in G$ em $1 \in \mathrm{Sim}(X)$. Portanto, definindo

$$xg = (x)g^{\sigma},$$

definimos uma ação de G sobre X. Seja ρ a representação permutacional de G correspondente. Então,

$$x^{\rho_g} = xg = (x)g^{\sigma},$$

logo $\rho_g = g^{\sigma}$, para todo $g \in G$, de modo que $\rho = \sigma$. □

Suponhamos que G age em X. Definimos a relação $\sim$ em X como segue: $x \sim y$ se, e somente se, $x, y \in X$ e existe um elemento $g \in G$ tal que $xg = y$. Notemos que esta é uma relação de equivalência em X. A classe de equivalência de $x \in X$ é chamada a *órbita de* x: é o subconjunto $\mathcal{O}_G(x) = \{xg \mid g \in G\}$ de X. A ação é chamada *transitiva* se existe algum $x \in X$ tal que $\mathcal{O}_G(x) = X$, ou seja, existe uma única órbita. Também, nesse sentido, definimos o *estabilizador de* x *em* G como sendo o subgrupo $\mathrm{Stab}_G(x) = \{g \in G \mid xg = x\}$. O próximo resultado estabelece uma relação entre esses dois conjuntos.

Teorema 1.2.5 (Princípio da Contagem)**.** *Sejam G agindo em um conjunto X e $x \in X$. Então $[G : \mathrm{Stab}_G(x)] = |\mathcal{O}_G(x)|$. Em particular, se a ação for transitiva, então $|X| = [G : \mathrm{Stab}_G(x)]$.*

Demonstração. Seja $H = \mathrm{Stab}_G(x)$, e vamos construir uma bijeção entre o conjunto C das classes laterais à direita de H em G e o conjunto $\mathcal{O}_G(x)$. Com efeito, definamos $f : C \to \mathcal{O}_G(x)$ por

$$(Hg)f = xg, \qquad \text{sempre que} \quad g \in G.$$

Se $Hg_1 = Hg_2$, então $g_1 g_2^{-1} \in H$, ou seja, $x(g_1 g_2^{-1}) = x$. Mas isto nos dá que $xg_1 = xg_2$ de maneira que $(Hg_1)f = (Hg_2)f$. Portanto, f está de fato bem definida. Além disso, se $xg_1 = xg_2$, então $x(g_1 g_2^{-1}) = x$, logo $g_1 g_2^{-1} \in H$, isto é, $Hg_1 = Hg_2$. Isto mostra que f é injetiva. Por fim, dado $xg \in \mathcal{O}_G(x)$, temos que $xg = (Hg)f$, o que nos fornece a sobrejetividade de f. Concluímos então que

$$[G : H] = |C| = |\mathcal{O}_G(x)|.$$

Em particular, se a ação é transitiva, $\mathcal{O}_G(x) = X$, e, portanto, $|X| = [G : \mathrm{Stab}_G(x)]$. □

No exemplo 1.2.2, a órbita $\mathcal{O}_G(H) = \{H^g \mid g \in G\}$ de um subgrupo H é chamada a *classe de conjugação* de H. O estabilizador $\mathrm{Stab}_G(H) = \{g \in G \mid H^g = H\}$ é o normalizador de H em G. O Teorema 1.2.5 nos dá que o número de conjugados de H em G é igual ao índice $[G : N_G(H)]$.

Definição 1.2.6. *Definimos o núcleo de uma ação de G em X como o núcleo da representação permutacional de G correspondente a esta ação. Uma ação é dita fiel se seu núcleo é trivial.*

Suponhamos G agindo em X e consideremos $\rho : G \to \mathrm{Sim}(X)$ a representação permutacional de G correspondente. Assim, o núcleo é

$$\ker(\rho) = \{g \in G \mid x^\rho = x,\ \forall x \in X\} = \{g \in G \mid xg = x,\ \forall x \in X\} = \bigcap_{x \in X} \mathrm{Stab}_G(x),$$

isto é, o núcleo de uma ação é a interseção dos estabilizadores.

1.3 Subgrupos Normais Minimais

O objetivo desta seção é mostrar que todo subgrupo normal minimal de um grupo finito é um produto direto de uma quantidade finita de cópias de um grupo simples. Esta seção é baseada no livro *A Course on Group Theory* [24].

Definição 1.3.1. *Seja $\{1\} \neq K \trianglelefteq G$. Dizemos que K é um subgrupo normal minimal de G se não existe subgrupo normal L de G tal que $\{1\} < L < K$.*

Observamos que, em um grupo finito, todo subgrupo normal não trivial contém um subgrupo normal minimal.

Proposição 1.3.2. *Sejam G um grupo e N, K dois subgrupos normais minimais de G distintos. Então $N \leq C_G(K)$ e $K \leq C_G(N)$.*

Demonstração. Pela Proposição 1.1.8, basta mostrar que $N \cap K = \{1\}$. E, de fato, dado que $N, K \trianglelefteq G$, temos que $N \cap K \trianglelefteq G$. Além disso, $N \cap K \leq N$ e $N \cap K \leq K$. Se $N \cap K \neq \{1\}$, então, pela minimalidade de N e K, obtemos que $N \cap K = N$ e $N \cap K = K$, ou seja, $N = K$, um absurdo. Portanto $N \cap K = \{1\}$, como queríamos. □

Seja K um subgrupo normal minimal de G e $\gamma \in \mathrm{Aut}(G)$, então K^γ é um subgrupo normal minimal de G. Com efeito, $K^\gamma \trianglelefteq G$, e se $L \leq K^\gamma$ com $L \trianglelefteq G$, então $L^{\gamma^{-1}} \leq K$ e $L^{\gamma^{-1}} \trianglelefteq G$. Uma vez que K é um subgrupo normal minimal de G, obtemos que $L^{\gamma^{-1}} = \{1\}$ ou $L^{\gamma^{-1}} = K$. Logo, $L = (L^{\gamma^{-1}})^\gamma = \{1\}$ ou $L = (L^{\gamma^{-1}})^\gamma = K^\gamma$, o que nos dá que K^γ é normal minimal em G. Além disso, $K \cong K^\gamma$, pois γ restrita a K possui núcleo trivial e imagem K^γ.

Definição 1.3.3. *Um grupo não trivial G é dito caracteristicamente simples se os únicos subgrupos característicos de G são $\{1\}$ e G.*

Grupos simples são exemplos de grupos caracteristicamente simples.

Proposição 1.3.4. *Suponhamos que K é um subgrupo normal minimal de G. Então K é um grupo caracteristicamente simples.*

Demonstração. Seja L um subgrupo característico de K. Então $L \trianglelefteq_c K \trianglelefteq G$ de modo que, pela Proposição 1.1.11, $L \trianglelefteq G$. Como $L \leq K$ e K é normal minimal em G, segue-se que $L = \{1\}$ ou $L = K$. Portanto, K é caracteristicamente simples. □

Definição 1.3.5. *Um grupo abeliano A é dito elementar se existe um primo p tal que $a^p = 1$ para todo $a \in A$.*

Proposição 1.3.6. *Seja A um grupo abeliano. Então as duas afirmações seguintes são equivalentes:*

(i) A é elementar.

(ii) Existe um primo p e um espaço vetorial V sobre $\mathbb{Z}_p$ tal que $A \cong V^+ := (V, +)$.

Demonstração. Suponhamos que A é elementar, então existe um primo p tal que $a^p = 1$ para todo $a \in A$. Definimos um espaço vetorial V sobre $\mathbb{Z}_p$ como segue. Os elementos de V são os elementos de A. A soma vetorial de dois elementos de V é definida como o produto de dois elementos de A. Os elementos de $\mathbb{Z}_p$ são classes residuais de inteiros módulo p. Seja $\bar{n} \in \mathbb{Z}_p$ e seja n um inteiro na classe residual $\bar{n}$. Então, para cada $a \in V$, o produto escalar $\bar{n}a$ é definido como o elemento $a^n \in A$. Notemos que este produto não depende da escolha de n na classe residual $\bar{n}$. Com efeito, se $r \in \bar{n}$, então $p|(n-r)$, logo $n - r = pq$ para algum $q \in \mathbb{Z}$, o que implica $a^{n-r} = a^{pq} = (a^p)^q = 1$, pois $a^p = 1$, e isto nos dá que $a^n = a^r$. Agora, é fácil ver que V é um espaço vetorial sobre $\mathbb{Z}_p$; e claramente, como grupos, $A \cong V^+$.

Reciprocamente, seja V um espaço vetorial sobre $\mathbb{Z}_p$. Então, V^+ é um grupo abeliano. Além disso, como $pv = 0$ para todo $v \in V$, V^+ é elementar. Consequentemente, se $A \cong V^+$, então A é elementar. □

Proposição 1.3.7. *Seja A um grupo abeliano finito, $A \neq \{1\}$. Então A é caracteristicamente simples se, e somente se, A é elementar.*

Demonstração. Suponhamos que A é elementar. Pela Proposição 1.3.6, podemos supor que $A = V^+$, com V é um espaço vetorial sobre $\mathbb{Z}_p$ para algum primo p; e, como A é finito, segue-se que V é de dimensão finita. Seja W um subgrupo característico não trivial de V^+ e $0 \neq w \in W$. Dado $0 \neq v \in V^+$, temos que v e w são elementos de certas bases de V. Logo, existe uma transformação linear inversível $T : V \to V$ tal que $(w)T = v$. Desse modo, $T \in \mathrm{Aut}(V^+)$ e, como W é característico em V^+, obtemos que $v \in W$. Portanto, $W = V^+$. Concluímos, assim, que V^+ é caracteristicamente simples.

Reciprocamente, suponhamos que A é caracteristicamente simples e consideremos p um primo divisor de $|A|$. Definimos então

$$B = \{a \in A \mid a^p = 1\}.$$

Dado que A é abeliano, temos que $B \leq A$. Seja $b \in B$ e $\gamma \in \mathrm{Aut}(A)$. Então

$$(b^\gamma)^p = (b^p)^\gamma = 1,$$

logo $b^\gamma \in B$. Portanto, B é característico em A. Pelo Teorema de Sylow, existe em A um elemento a de ordem p. Daí, $1 \neq a \in B$, logo $B \neq \{1\}$. Como A é caracteristicamente simples, segue-se que $B = A$, ou seja, A é elementar. □

Dados G um grupo e $H_1, \ldots, H_n \leq G$, com n um inteiro positivo, vamos denotar por $\prod_{i=1}^n H_j$ o subconjunto $H_1 \cdots H_n = \{h_1 \cdots h_n \mid h_i \in H_i \ (1 \leq i \leq n)\}$ de G.

Teorema 1.3.8. *Sejam $K_1, K_2, \ldots, K_n$ subgrupos normais minimais de G, com n um inteiro positivo, e consideremos $K = \prod_{j=1}^n K_j$. Então existe um subconjunto $\{i_1, \ldots, i_m\}$ de $\{1, \ldots, n\}$ tal que K é o produto direto interno de $K_{i_1}, \ldots, K_{i_m}$. Em particular, $K = \underset{1 \leq j \leq m}{\mathrm{Dr}} K_{i_j}$.*

Demonstração. Seja Γ o conjunto de todos os subconjuntos não vazios $\{i_1, \ldots, i_m\}$ de $\{1, \ldots, n\}$ tais que $i_1, \ldots, i_m$ são distintos e $\prod_{j=1}^m K_{i_j}$ é o produto direto interno de $K_{i_1}, \ldots, K_{i_m}$. Trivialmente, $\{j\} \in \Gamma$ para cada $j = 1, \ldots, n$.

Agora, escolhamos $\{i_1, \ldots, i_m\} \in \Gamma$ com m maior possível, e seja $L = \prod_{j=1}^m K_{i_j} = \underset{1 \leq j \leq m}{\mathrm{Dr}^{(i)}} K_{i_j}$. Temos que K e L são subgrupos normais de G e certamente $L \leq K$. Se $K \neq L$, então existe um inteiro $l \in \{1, \ldots, n\}$ tal que $K_l \not\subseteq L$. Uma vez que K_l é normal minimal em G e $L \trianglelefteq G$, segue-se que $K_l \cap L = \{1\}$. Seja $i_{m+1} = l$. Como $K_{i_j} \leq L$ para cada $j = 1, \ldots, m$, obtemos que i_{m+1} é distinto de $i_1, \ldots, i_m$. Por outro lado, sejam $x_{i_1}, y_{i_1} \in K_{i_1}, \ldots, x_{i_{m+1}}, y_{i_{m+1}} \in K_{i_{m+1}}$ tais que

$$x_{i_1} \cdots x_{i_m} x_{i_{m+1}} = y_{i_1} \cdots y_{i_m} y_{i_{m+1}}.$$

Então,

$$y_{i_m}^{-1} \cdots y_{i_1}^{-1} x_{i_1} \cdots x_{i_m} = y_{i_{m+1}} x_{i_{m+1}}^{-1} \in K_l \cap L = \{1\}$$

donde $x_{i_1} \cdots x_{i_m} = y_{i_1} \cdots y_{i_m}$ e $x_{i_{m+1}} = y_{i_{m+1}}$. Haja vista que L é o produto direto interno de $K_{i_1}, \ldots, K_{i_m}$, segue-se que $x_{i_j} = y_{i_j}$, $\forall j = 1, \ldots, m+1$. Com isso, concluímos que $\prod_{j=1}^{m+1} K_{i_j}$ é o produto direto interno de $K_{i_1}, \ldots, K_{i_{m+1}}$ de modo que $\{i_1, \ldots, i_m, i_{m+1}\} \in \Gamma$, uma contradição com a escolha de m. Portanto,

$$K = L = \underset{1 \leq j \leq m}{\mathrm{Dr}^{(i)}} K_{i_j}.$$

Em particular, pelo Teorema 1.1.6,

$$K = \underset{1\leq j\leq m}{\mathrm{Dr}} K_{i_j}.$$

□

Observação 1.3.9. *No teorema acima, se $n \geq 2$, então $m \geq 2$, pois neste caso N_1N_2 é o produto direto interno de N_1 e N_2 de modo que $\{1,2\} \in \Gamma$.*

Definição 1.3.10. *Seja G um grupo. Dizemos que G é completamente redutível se ou $G = \{1\}$, ou G é o produto direto de um número finito de grupos simples.*

Em particular, todo grupo simples é completamente redutível.

Lema 1.3.11. *Suponhamos que G é um grupo completamente redutível finito não trivial: digamos $G = \underset{1\leq j\leq m}{\mathrm{Dr}} K_j$, sendo que, para cada $j = 1,\ldots,n$, K_j é um subgrupo normal simples de G. Se $Z(G) = \{1\}$, então $K_1, K_2, \ldots, K_n$ são os únicos subgrupos normais minimais de G.*

Demonstração. Para cada $j = 1,\ldots,n$, K_j é um subgrupo normal simples de G de modo que K_j é normal minimal em G. Agora, assumamos que $Z(G) = \{1\}$ e suponhamos por absurdo que existe um subgrupo normal minimal L distinto de $K_1,\ldots,K_n$. Então, para cada $j = 1,\ldots,n$, $K_j \leq C_G(L)$ (vide Proposição 1.3.2). Logo,

$$C_G(L) \geq \prod_{j=1}^{n} K_j = G,$$

isto é, $L \leq Z(G) = \{1\}$, uma contradição. Portanto, $K_1,\ldots,K_n$ são os únicos subgrupos normais minimais de G. □

Teorema 1.3.12. *Seja G um grupo finito não trivial. Então G é caracteristicamente simples se, e somente se, G é um produto direto de um número finito de cópias de um grupo simples.*

Demonstração. Suponhamos que G é caracteristicamente simples. Seja K_1 um subgrupo normal minimal de G. Para cada $\gamma \in \mathrm{Aut}(G)$, sabemos que K_1^γ é um subgrupo normal minimal de G e $K_1^\gamma \cong K_1$. Como G é finito, existem somente um número finito de subgrupos distintos da forma K_1^γ com $\gamma \in \mathrm{Aut}(G)$, digamos n deles: $K_1,\ldots,K_n$. Seja

$$K = \prod_{j=1}^{n} K_j.$$

Agora, seja $\phi \in \mathrm{Aut}(G)$. Para cada $j \in \{1,2,\ldots,n\}$, $K_j = K_1^\gamma$ para algum $\gamma \in \mathrm{Aut}(G)$, e, então, como $\gamma\phi \in \mathrm{Aut}(G)$, $K_j^\phi = K_1^{\gamma\phi} = K_l$ para algum $l \in \{1,\ldots,n\}$. Além disso,

se $i, j \in \{1, \ldots, n\}$ com $i \neq j$, então $K_i^{\phi} \neq K_j^{\phi}$. Consequentemente, $\{K_1^{\phi}, \ldots, K_n^{\phi}\} = \{K_1, \ldots, K_n\}$, e, então,

$$K^{\phi} = \prod_{j=1}^{n} K_j^{\phi} = \prod_{j=1}^{n} K_j = K.$$

Isto é verdadeiro para todo $\phi \in \mathrm{Aut}(G)$, portanto K é característico em G. Como $\{1\} < K \leq G$ e G é caracteristicamente simples, segue-se que $K = G$. Pelo Teorema 1.3.8, obtemos que G é o produto direto de alguns dos subgrupos $K_1, \ldots, K_n$. Podemos escolher a notação

$$G = \operatorname*{Dr}_{1 \leq j \leq m} K_j,$$

com $m \leq n$. Agora, qualquer subgrupo normal de K_1 é normal em G. Uma vez que K_1 é normal minimal em G, segue-se que K_1 é simples. Portanto, como $K_j \cong K_1$ para cada $j = 1, 2, \ldots, m$, G é o produto direto de m cópias isomorfas ao grupo simples K_1.

Reciprocamente, suponhamos que G é o produto direto de m cópias isomorfas de K_1, com m é um inteiro positivo e K_1 é um grupo simples: digamos,

$$G = \operatorname*{Dr}_{1 \leq j \leq m} K_j,$$

onde, para cada $j = 1, \ldots, m$, $K_j \cong K_1$. Se K_1 é abeliano, então $|K_1| = p$ para algum primo p. Daí, $|K_j| = p$ para cada $j = 1, \ldots, m$, e, assim, G é um grupo abeliano elementar de ordem p^m. Como visto na Proposição 1.3.7, G é caracteristicamente simples. Se K_1 é não abeliano, então G é um produto direto de grupos simples não abelianos donde $Z(G) = \{1\}$. Seja K um subgrupo característico não trivial de G. Então K contém um subgrupo normal minimal de G de modo que, pelo Lema 1.3.11, $K \geq K_i$ para algum $i \in \{1, \ldots, m\}$. Sem perda de generalidade, podemos supor que

$$K \geq K_1.$$

Se $m > 1$, seja $j \in \{2, \ldots, m\}$. Temos que existe um isomorfismo $\varphi : K_1 \to K_j$. Cada elemento de G tem uma única expressão da forma $k_1 k_2 \cdots k_m$ com $k_i \in K_i$, para cada $i = 1, \ldots, m$. Então, podemos definir uma aplicação $\gamma : G \to G$ por

$$\gamma : k_1 k_2 \cdots k_{j-1} k_j k_{j+1} \cdots k_m \mapsto k_j^{\varphi^{-1}} k_2 \cdots k_{j-1} k_1^{\varphi} k_{j+1} \cdots k_m,$$

para todos $k_1 \in K_1, \ldots, k_n \in K_m$. Desse modo, temos que γ é um automorfismo de G,

e claramente $K_1^\gamma = K_j$. Como K é característico em G,

$$K = K^\gamma \geq K_1^\gamma = K_j.$$

Portanto, $K \geq K_j$ para todo $j = 1, \ldots, m$, o que implica $K = G$. Consequentemente, G é caracteristicamente simples. Isto completa a prova do teorema. □

Segue-se em particular que todo grupo finito caracteristicamente simples é completamente redutível.

Corolário 1.3.13. *Seja K um subgrupo normal minimal de um grupo finito G. Então existem um grupo simples S e um inteiro positivo n tais que*

$$K \cong S^n.$$

Demonstração. Pela Proposição 1.3.4, temos que K é caracteristicamente simples. Se K é abeliano, então K é elementar (vide Proposição 1.3.7) de sorte que existe um primo p e um espaço vetorial V sobre $\mathbb{Z}_p$ tal que $K \cong V^+$, pela Proposição 1.3.6. Assim, tomando $n = \dim_{\mathbb{Z}_p} V$ e $S = C_p$, obtemos que

$$K \cong V^+ \cong S^n.$$

Agora, se K é não abeliano, usamos o Teorema 1.3.12 para concluir que existem um grupo simples não abeliano S e um inteiro positivo n tais que

$$K \cong S^n,$$

pois se S fosse abeliano, teríamos $Z(S) = S$ e $Z(S^n) = Z(S)^n = S^n$, um absurdo. Isto encerra a demonstração do corolário. □

1.4 Grupos Solúveis e Nilpotentes

Esta seção é baseada no livro *A Course in the Theory of Groups* [22, Capítulo 5].

Definição 1.4.1. *Uma sequência finita de subgrupos*

$$\{1\} \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

é chamada uma série (subnormal) de G de comprimento n. Os subgrupos $G_0, G_1, \ldots, G_n$ são

chamados os termos da série e os grupos quocientes G_{i+1}/G_i ($0 \leq i \leq n-1$) são os fatores da série. Se $G_i \trianglelefteq G$ para todo $i \in \{0, 1, \ldots, n\}$, então a série é dita normal.

Definição 1.4.2. *Um grupo G é dito solúvel se este admite uma série abeliana, ou seja, uma série*

$$\{1\} \trianglelefteq G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

em que cada fator G_{i+1}/G_i é abeliano.

Naturalmente, todo grupo abeliano é solúvel. Por outro lado, o grupo simétrico S_3 é solúvel (pois $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ é uma série abeliana de S_3), mas este é não abeliano.

Se G é um grupo solúvel, o comprimento de uma menor série abeliana de G é chamado o *comprimento derivado* de G. Nesse sentido, G tem comprimento derivado 0 se, e somente se, tem ordem 1. Também, os grupos com comprimento derivado no máximo 1 são apenas os grupos abelianos.

O próximo resultado nos fornece algumas propriedades básicas de grupos solúveis.

Proposição 1.4.3 ([22], 5.1.1)**.** *A classe de grupos solúveis é fechada com respeito à formação de subgrupos, imagens homomórficas e produtos diretos finitos.*

Definição 1.4.4. *Seja G um grupo. A série derivada de G é dada por*

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots,$$

sendo $G^{(n+1)} = (G^{(n)})'$.

Notemos que esta é uma série normal de G e cada fator $G^{(n)}/G^{(n+1)}$ é abeliano.

Proposição 1.4.5 ([22], 5.1.8)**.** *Um grupo G é solúvel se, e somente se, $G^{(n)} = \{1\}$ para algum inteiro n. O comprimento derivado de G é igual ao comprimento da série derivada de G.*

Proposição 1.4.6. *Seja K um subgrupo normal minimal de um grupo solúvel finito G. Então K é abeliano elementar.*

Demonstração. Pela Proposição 1.1.11, temos que $K' \trianglelefteq G$, haja vista que $K' \trianglelefteq_c K \trianglelefteq G$. Como K é normal minimal em G, segue-se que $K' = \{1\}$ ou $K' = K$. Mas por hipótese G é solúvel, logo K também o é (vide Proposição 1.4.3), e, então, $K' = \{1\}$, pela Proposição 1.4.5. Portanto, K é abeliano.

Agora, como K é não trivial, existe um primo p divisor de $|K|$. Consideremos

$$A = \{x \in K \mid x^p = 1\}.$$

Como visto na demonstração da Proposição 1.3.7, A é um subgrupo característico não trivial de K, logo $A \trianglelefteq G$ e $A = K$, pela minimalidade de K. Ou seja, K é abeliano elementar. □

Definição 1.4.7. *Um grupo G é dito nilpotente se este possui uma série central, isto é, uma série normal*

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

tal que G_{i+1}/G_i está contido no centro de G/G_i, para todo $i \in \{0, 1, \ldots, n-1\}$.

Segue-se da definição que todo grupo nilpotente não trivial possui centro não trivial, pois $G_1 \leq Z(G)$.

O comprimento de uma menor série central de G é a *classe de nilpotência* de G. Um grupo nilpotente de classe 0 tem ordem 1, enquanto grupos nilpotentes de classe no máximo 1 são abelianos. Um exemplo de grupo solúvel não nilpotente é o S_3 (seu centro é trivial).

Proposição 1.4.8. *Todo p-grupo finito é nilpotente.*

Demonstração. Seja G um p-grupo finito de ordem > 1. Então $Z(G) \neq \{1\}$ [12, Afirmação 1, Página 256] de modo que $G/Z(G)$ é nilpotente por indução sobre $|G|$. Usando o Teorema da Correspondência nos termos de uma série central de $G/Z(G)$ e adicionando $\{1\}$, obtemos uma série central de G. Portanto, G é nilpotente. □

Proposição 1.4.9 ([24], Teoremas 7.46 e 7.49)**.** *A classe de grupos nilpotentes é fechada com respeito à formação de subgrupos, imagens homomórficas e produtos diretos finitos.*

Definição 1.4.10. *Seja M um subgrupo próprio de G. Dizemos que M é um subgrupo maximal de G se não existe subgrupo H tal que $M < H < G$.*

Observamos que, em um grupo finito, todo subgrupo próprio está contido em um subgrupo maximal.

O seguinte resultado nos fornece uma caracterização dos grupos nilpotentes finitos.

Teorema 1.4.11 ([22], 5.2.4)**.** *Seja G um grupo finito. Então as seguintes propriedades são equivalentes:*

(i) G é nilpotente.

(ii) Todo subgrupo maximal de G é normal.

(iii) Todo subgrupo de Sylow de G é normal.

(iv) G é o produto direto de seus subgrupos de Sylow.

1.5 Subgrupo de Frattini

Definição 1.5.1. *Seja G um grupo. O subgrupo de Frattini de G é definido como a interseção de todos os subgrupos maximais de G e é denotado por $\Phi(G)$. Caso G não possua subgrupos maximais, definimos $\Phi(G) = G$.*

Temos que $\Phi(G)$ é um subgrupo característico de G. Observamos também que, em um grupo finito, o subgrupo de Frattini é sempre próprio, uma vez que existe pelo menos um subgrupo maximal.

Agora, seja G um grupo finito. Suponhamos que $G' \leq \Phi(G)$, e seja M um subgrupo maximal de G. Então $G' \leq M$ de forma que M/G' é um subgrupo do grupo abeliano G/G'. Desse modo, obtemos que $M/G' \trianglelefteq G/G'$ e, por correspondência, $M \trianglelefteq G$.

Reciprocamente, assumamos que todo subgrupo maximal de G é normal. Assim, dado M um tal subgrupo, temos que $M \trianglelefteq G$, e, usando o Teorema da Correspondência juntamente com a maximalidade de M, obtemos que G/M não possui subgrupos próprios não triviais, logo é um grupo cíclico de ordem prima, em particular abeliano. Pela Observação 1.1.4, segue-se que $G' \leq M$. Isto é verdadeiro para todo subgrupo maximal M de G, e, então, pela definição de $\Phi(G)$, $G' \leq \Phi(G)$.

Ou seja, se G é um grupo finito, então pelo Teorema 1.4.11 G é nilpotente se, e somente se, $G' \leq \Phi(G)$.

Exemplo 1.5.2. *Seja $n \geq 3$. Então $\Phi(S_n) = \{1\}$. Com efeito, vamos considerar primeiro $n \neq 4$. Temos que $S_n' \trianglelefteq S_n$, logo $S_n' \in \{\{1\}, A_n, S_n\}$. Mas S_n/A_n tem ordem 2 (portanto abeliano) de modo que $S_n' \leq A_n$. E sendo S_n não abeliano, concluímos que $S_n' = A_n$. Agora, $\Phi(S_n) \in \{\{1\}, A_n\}$, já que $\Phi(S_n) \trianglelefteq S_n$ e S_n é um grupo finito. Por outro lado, uma vez que S_n não é nilpotente (pois tem centro trivial), temos que $A_n = S_n' \nsubseteq \Phi(S_n)$. Portanto, $\Phi(S_n) = \{1\}$. Para $n = 4$, basta considerar os subgrupos maximais $H = \langle (12), (123) \rangle$, $K = \langle (12), (124) \rangle$ e $L = A_n$ para concluir que $\Phi(S_n) \leq H \cap K \cap L = \{1\}$.*

Lema 1.5.3 ([24], Lema 11.4)**.** *Sejam G um grupo finito e $K \trianglelefteq G$. Então $K \leq \Phi(G)$ se, e somente se, não existe subgrupo próprio H de G tal que $HK = G$.*

Lema 1.5.4 (Argumento de Frattini)**.** *Se H é um subgrupo normal finito de um grupo G e P é um p-subgrupo de Sylow de H, então $G = N_G(P)H$.*

Demonstração. Seja $g \in G$. Dado que $H \trianglelefteq G$, temos

$$P^g \leq H^g = H$$

de modo que P^g é um p-subgrupo de Sylow de H. Pelo Teorema de Sylow, existe $x \in H$ tal que $P^g = P^x$, o que implica $P^{gx^{-1}} = P$, ou seja, $gx^{-1} \in N_G(P)$. Assim,

$$g = (gx^{-1})x \in N_G(P)H.$$

Portanto, $G = N_G(P)H$. □

Teorema 1.5.5 (Frattini)**.** *Seja G um grupo finito. Então $\Phi(G)$ é nilpotente.*

Demonstração. Seja P um subgrupo de Sylow qualquer de $\Phi(G)$. Haja vista que $\Phi(G) \trianglelefteq G$, o Argumento de Frattini (Lema 1.5.4) nos dá que $G = N_G(P)\Phi(G)$. Assim, pelo Lema 1.5.3, segue-se que $G = N_G(P)$, ou seja, $P \trianglelefteq G$. Portanto, pelo Teorema 1.4.11, concluímos que $\Phi(G)$ é nilpotente. □

Lema 1.5.6 ([24], Lemas 11.7 e 11.8)**.** *Sejam G um grupo finito, $H \leq G$ e $K \trianglelefteq G$.*

(i) Se $K \leq \Phi(H)$, então $K \leq \Phi(G)$.

(ii) $\Phi(K) \leq \Phi(G)$.

(iii) Se $K \leq \Phi(G)$, então $\Phi(G)/K = \Phi(G/K)$.

Proposição 1.5.7. *Seja G um p-grupo finito. Então $\Phi(G) = \{1\}$ se, e somente se, G é abeliano elementar.*

Demonstração. Podemos assumir que $G \neq \{1\}$. Suponhamos primeiro que G é abeliano elementar. Como $G \neq \{1\}$, $\Phi(G) < G$. Além disso, pela Proposição 1.3.7, G é caracteristicamente simples. Então, como $\Phi(G) \trianglelefteq_c G$, obtemos que $\Phi(G) = \{1\}$.

Reciprocamente, suponhamos que $\Phi(G) = \{1\}$. Pela Proposição 1.4.8, G é nilpotente de modo que $G' \leq \Phi(G)$. Assim, $G' = \{1\}$ e G é abeliano. Sejam M um subgrupo maximal de G e $g \in G$. Pelo Teorema 1.4.11, $M \trianglelefteq G$ donde G/M tem ordem prima. Como G é um p-grupo, $|G/M| = p$. Portanto, $g^p \in M$. Isto é verdadeiro para todo subgrupo maximal M de G, o que produz

$$g^p \in \Phi(G) = \{1\}.$$

Pela arbitrariedade de g, concluímos que G é abeliano elementar. □

Seja G um p-grupo finito. Pelo item (iii) do Lema 1.5.6, o subgrupo de Frattini de $G/\Phi(G)$ é trivial. Desse modo, a Proposição 1.5.7 nos fornece que $G/\Phi(G)$ é abeliano elementar, e, assim, $G/\Phi(G)$ pode ser visto de maneira natural como um espaço vetorial de dimensão finita sobre $\mathbb{Z}_p$. (vide Proposição 1.3.6).

Proposição 1.5.8. *Seja G um grupo finito tal que $G/\Phi(G)$ é um p-grupo. Então G é um p-grupo.*

Demonstração. Suponhamos que exista um primo $q \neq p$ divisor de $|G|$. Dado que $G/\Phi(G)$ é um p-grupo, temos que q não divide $|G/\Phi(G)|$ de modo que $\Phi(G)$ contém um q-subgrupo de Sylow Q de G. Pelos Teoremas 1.4.11 e 1.5.5, obtemos que $Q \trianglelefteq \Phi(G)$. Agora, notemos que $\text{mdc}(|Q|, [G : Q]) = 1$. Assim, pelo famoso Teorema de Schur-Zassenhaus [22, 9.1.2], existe $H \leq G$ tal que

$$G = QH \quad \text{e} \quad Q \cap H = \{1\}.$$

Desse modo, $H < G$ (porque $|Q| > 1$) donde existe um subgrupo maximal M de G com $H \leq M$. Daí, $Q \leq \Phi(G) \leq M$ e

$$G = QH \leq M,$$

um absurdo. Portanto, G é um p-grupo. □

Observação 1.5.9. *Para um grupo finito G, um número primo divide a ordem de G se, e somente se, divide a ordem do grupo $G/\Phi(G)$. A demonstração é essencialmente a mesma da Proposição 1.5.8.*

Definição 1.5.10. *Seja H um subgrupo de um grupo G. Um subgrupo K é dito um complemento para H em G se*

$$G = HK \quad e \quad H \cap K = \{1\}.$$

Proposição 1.5.11. *Seja G um grupo finito. Se A é um subgrupo normal abeliano de G tal que $\Phi(G) \cap A = \{1\}$, então existe um complemento H para A em G.*

Demonstração. Escolhamos $H \leq G$ minimal sujeito a $G = HA$. Como $A \trianglelefteq G$, temos que $H \cap A \trianglelefteq H$. Também, $H \cap A \trianglelefteq A$, pois A é abeliano. Logo $H \cap A \trianglelefteq HA = G$. Se $H \cap A \leq \Phi(H)$, então, pelo item (i) do Lema 1.5.6, $H \cap A \leq \Phi(G) \cap A = \{1\}$. Assim, podemos assumir que $H \cap A \nleq M$, para algum subgrupo maximal M de H. Neste caso,

$$H = M(H \cap A) \quad \text{e} \quad G = HA = MA,$$

uma contradição com a minimalidade de H. □

Observação 1.5.12. *Seja K um subgrupo normal minimal abeliano de um grupo finito G. Se $K \nleq \Phi(G)$, então $\Phi(G) \cap K = \{1\}$ (pela minimalidade de K) de modo que, pela Proposição 1.5.11, K admite um complemento em G. Reciprocamente, se existe um complemento H para K*

em G, então $H < G$ (já que $K \neq \{1\}$) donde $K \not\subseteq \Phi(G)$, pelo Lema 1.5.3. Ou seja, K admite um complemento em G se, e somente se, $K \not\subseteq \Phi(G)$.

Finalizamos esta seção com um resultado importante a respeito de geração de p-grupos, devido a William Burnside.

Teorema 1.5.13 (Teorema da Base de Burnside)**.** *Seja G um p-grupo finito. Então*

$$\Phi(G) = G'G^{\langle p\rangle},$$

sendo $G^{\langle p\rangle} = \langle g^p \mid g \in G\rangle$. Também, se $[G : \Phi(G)] = p^r$, todo conjunto de geradores de G possui um subconjunto de r elementos que também gera G.

Demonstração. Como visto na demonstração da Proposição 1.5.7, temos que $G', G^{\langle p\rangle} \leq \Phi(G)$ de forma que $G'G^{\langle p\rangle} \leq \Phi(G)$. Por outro lado, $G/G'G^{\langle p\rangle}$ é abeliano elementar, logo a Proposição 1.5.7 nos dá que

$$\Phi(G/G'G^{\langle p\rangle}) = \{1\} = G'G^{\langle p\rangle}/G'G^{\langle p\rangle}.$$

Mas pelo item (iii) do Lema 1.5.6,

$$\Phi(G/G'G^{\langle p\rangle}) = \Phi(G)/G'G^{\langle p\rangle},$$

portanto $\Phi(G) = G'G^{\langle p\rangle}$.

Agora, suponhamos que $G = \langle x_1, \ldots, x_s\rangle$, e seja $F = \Phi(G)$. Assim, $\overline{G} = G/F$ é gerado por $Fx_1, \ldots, Fx_s$. Haja vista que $\overline{G}$ é um espaço vetorial de dimensão r sobre $\mathbb{Z}_p$, $\overline{G}$ tem uma base da forma

$$\{Fx_{i_1}, \ldots, Fx_{i_r}\}.$$

Escrevendo $Y = \{x_{i_1}, \ldots, x_{i_r}\}$, obtemos que

$$\overline{G} = \langle Fx_{i_1}, \ldots, Fx_{i_r}\rangle \leq \langle Y\rangle F/F \quad \text{e} \quad G = \langle Y\rangle F,$$

portanto $G = \langle Y\rangle$, pelo Lema 1.5.3. □

1.6 Produto Semidireto de Grupos

Definição 1.6.1. *Sejam H e K grupos. Dizemos que H age em K (como um grupo) se, para cada $h \in H$ e cada $k \in K$, corresponde um único elemento $k^h \in K$ tal que, para todos $k, k_1, k_2 \in K$ e*

$h, h_1, h_2 \in H$,

$$(k^{h_1})^{h_2} = k^{h_1 h_2}, \qquad k^1 = k,$$

e

$$(k_1 k_2)^h = k_1^h k_2^h.$$

Exemplo 1.6.2. *Seja $H \leq \mathrm{Aut}(K)$. Então H age em K. Neste caso, cada $h \in H$ é um automorfismo de K e, para $k \in K$, k^h é a imagem de k por meio de h. Esta é chamada a ação natural de H em K.*

Exemplo 1.6.3. *Seja $K \trianglelefteq G$. Então G age em K (como um grupo) por conjugação: para cada $k \in K$ e cada $g \in G$, corresponde o elemento*

$$k^g = g^{-1} k g \in K.$$

Teorema 1.6.4. *Seja H agindo em K. Então, para cada $h \in H$, corresponde uma aplicação $\varphi_h : K \to K$, definida por $\varphi_h : k \mapsto k^h$, e esta é um automorfismo de K. Além disso, a aplicação $\varphi : H \to \mathrm{Aut}(K)$, definida por $\varphi : h \mapsto \varphi_h$, é um homomorfismo. Chamamos φ como a representação de H no grupo de automorfismos de K correspondente à ação, ou, com mais frequência, φ é simplesmente a ação.*

Demonstração. Seja $h \in H$. Como a ação de H em K é em particular uma ação em K como conjunto, o Teorema 1.2.3 nos dá que $\varphi_h \in \mathrm{Sim}(K)$. Dados $k_1, k_2 \in K$,

$$(k_1 k_2)^{\varphi_h} = (k_1 k_2)^h = k_1^h k_2^h = k_1^{\varphi_h} k_2^{\varphi_h},$$

logo $\varphi_h \in \mathrm{Aut}(K)$. Com isso, a aplicação $\varphi : h \mapsto \varphi_h$ (definida para todo $h \in H$) é uma aplicação de H em $\mathrm{Aut}(K)$ e, pelo Teorema 1.2.3, é um homomorfismo. □

Teorema 1.6.5. *Seja φ um homomorfismo de H em $\mathrm{Aut}(K)$. Então, H age em K quando definimos, para cada $h \in H$ e $k \in K$,*

$$k^h = k^{h^\varphi},$$

e a ação correspondente é φ.

Demonstração. Como $\mathrm{Aut}(K) \leq \mathrm{Sim}(K)$, o Teorema 1.2.4 nos dá que a equação acima define uma ação de H em K como conjunto. Esta é uma ação em K como um grupo

porque, dados $h \in H$ e $k_1, k_2 \in K$,

$$\begin{aligned}(k_1k_2)^h &= (k_1k_2)^{h^\varphi} \\ &= \left(k_1^{h^\varphi}\right)\left(k_2^{h^\varphi}\right) \quad (\text{pois } h^\varphi \in \mathrm{Aut}(K)) \\ &= k_1^h k_2^h.\end{aligned}$$

Por fim, pelos Teoremas 1.2.3, 1.2.4 e 1.6.4, obtemos que a ação correspondente é φ. □

Teorema 1.6.6. *Seja H agindo em K. Então o conjunto $K \times H$ adquire a estrutura de um grupo G quando definimos, para todos $k_1, k_2 \in K$ e $h_1, h_2 \in H$,*

$$(k_1, h_1)(k_2, h_2) = \left(k_1 k_2^{h_1^{-1}}, h_1h_2\right).$$

Demonstração. O fechamento é claro da definição de multiplicação. Sejam $k_1, k_2, k_3 \in K$ e $h_1, h_2, h_3 \in H$ arbitrários. Então, usando a associatividade da multiplicação em H e em K,

$$\begin{aligned}(k_1, h_1)((k_2, h_2)(k_3, h_3)) &= (k_1, h_1)\left(k_2 k_3^{h_2^{-1}}, h_2h_3\right) \\ &= \left(k_1\left(k_2 k_3^{h_2^{-1}}\right)^{h_1^{-1}}, h_1h_2h_3\right) \\ &= \left(k_1 k_2^{h_1^{-1}}\left(k_3^{h_2^{-1}}\right)^{h_1^{-1}}, h_1h_2h_3\right) \\ &= \left(k_1 k_2^{h_1^{-1}} k_3^{(h_1h_2)^{-1}}, h_1h_2h_3\right),\end{aligned}$$

pela Definição 1.6.1, e

$$\begin{aligned}((k_1, h_1)(k_2, h_2))(k_3, h_3) &= \left(k_1 k_2^{h_1^{-1}}, h_1h_2\right)(k_3, h_3) \\ &= \left(k_1 k_2^{h_1^{-1}} k_3^{(h_1h_2)^{-1}}, h_1h_2h_3\right).\end{aligned}$$

Portanto, a operação definida é associativa. Pela Definição 1.6.1, $k^1 = k$ para todo $k \in K$. Também, pelo Teorema 1.6.4, a aplicação $k \mapsto k^h$ é um automorfismo de K para todo $h \in H$. Assim, $1^h = 1$ e $(k^{-1})^h = (k^h)^{-1}$. Segue-se, pela regra de multiplicação, que $(1, 1)$ é o elemento neutro de G e que qualquer $(k, h) \in G$ tem um elemento inverso $((k^{-1})^h, h^{-1}) \in G$. □

Definição 1.6.7. *O grupo G, como no Teorema 1.6.6, é dito o produto semidireto externo de K por H e é denotado por $K \rtimes H$.*

Notemos que $K \times \{1\}$ e $\{1\} \times H$ são subgrupos de G, e $K \times \{1\} \trianglelefteq G$. De fato,

dados $k, k_1 \in K$ e $h \in H$, temos

$$\begin{aligned}(k,h)^{-1}(k_1,1)(k,h) &= ((k^{-1})^h, h^{-1})(k_1 k, h) \\ &= ((k^h)^{-1}(k_1 k)^h, h^{-1}h) = ((k^h)^{-1}k_1^h k^h, 1) \in K \times \{1\}.\end{aligned}$$

Observamos também que se $k^h = k$ para todos $k \in K$ e $h \in H$, então G é na verdade o produto direto de K e H.

Teorema 1.6.8 ([12], Teorema V.9.16)**.** *Sejam G, H, K grupos. Então, existe uma ação de H em K (como um grupo) tal que G seja isomorfo a $K \rtimes H$ se, e somente se, G possui subgrupos $H_1 \cong H$ e $K_1 \cong K$ tais que:*

(i) $G = K_1 H_1$.

(ii) $K_1 \trianglelefteq G$.

(iii) $K_1 \cap H_1 = \{1\}$.

Definição 1.6.9. *Sejam G um grupo, $K \trianglelefteq G$ e $H \leq G$. Se $G = KH$ e $K \cap H = \{1\}$, dizemos que G é o produto semidireto interno de K por H.*

Pelo Teorema 1.6.8, se G é o produto semidireto interno de K por H, então $G \cong K \rtimes H$. Notemos também que se $G = K \rtimes H$, então G é o produto semidireto interno de $K \times \{1\}$ por $\{1\} \times H$.

Definição 1.6.10. *Sejam H e K dois grupos com $K \leq S_n$. O produto entrelaçado entre H e K, denotado por $H \wr K$, é o produto semidireto $H^n \rtimes K$, onde K age em H^n permutando as coordenadas. Mais precisamente, $\pi \in K$ age em H^n por*

$$(x_1, \ldots, x_n)^\pi = (x_{1\pi^{-1}}, \ldots, x_{n\pi^{-1}}).$$

Vamos mostrar que esta é de fato uma ação de grupo. Sejam π, τ e θ elementos de K, e $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n)$ e $(z_1, \ldots, z_n)$ elementos de H^n. Definindo $t_i = x_{i\pi^{-1}}$, temos $t_{i\tau^{-1}} = x_{i\tau^{-1}\pi^{-1}} = x_{i(\pi\tau)^{-1}}$, logo

$$\begin{aligned}((x_1, \ldots, x_n)^\pi)^\tau &= (x_{1\pi^{-1}}, \ldots, x_{n\pi^{-1}})^\tau = (x_{1\tau^{-1}\pi^{-1}}, \ldots, x_{n\tau^{-1}\pi^{-1}}) \\ &= (x_{1(\pi\tau)^{-1}}, \ldots, x_{n(\pi\tau)^{-1}}) = (x_1, \ldots, x_n)^{\pi\tau}.\end{aligned}$$

Também, $(x_1,\ldots,x_n)^1 = (x_{(1)1},\ldots,x_{(n)1}) = (x_1,\ldots,x_n)$ e

$$\begin{aligned}((y_1,\ldots,y_n)\cdot(z_1,\ldots,z_n))^\theta &= (y_1z_1,\ldots,y_nz_n)^\theta = (y_{1\theta^{-1}}z_{1\theta^{-1}},\ldots,y_{n\theta^{-1}}z_{n\theta^{-1}})\\ &= (y_{1\theta^{-1}},\ldots,y_{n\theta^{-1}})\cdot(z_{1\theta^{-1}},\ldots,z_{n\theta^{-1}})\\ &= (y_1,\ldots,y_n)^\theta\cdot(z_1,\ldots,z_n)^\theta.\end{aligned}$$

O subgrupo H^n é dito a base do grupo $H \wr K$.

Proposição 1.6.11. *Seja S um grupo simples não abeliano e n um inteiro positivo. Então os subconjuntos*

$$N_i = \{1\}\times\cdots\times\{1\}\times S\times\{1\}\times\cdots\times\{1\},\quad 1\le i\le n,$$

onde apenas a i-ésima coordenada é igual a S, são os únicos subgrupos normais minimais de S^n.

Demonstração. Sabemos que os fatores diretos $N_1,\ldots,N_n$ são subgrupos normais de S^n. Além disso, dado $i\in\{1,\ldots,n\}$, N_i é isomorfo a S, pois a aplicação

$$s\mapsto(1,\ldots,1,s,1,\ldots,1)$$

é um isomorfismo. Logo N_i é simples, e, por conseguinte, é normal minimal em S^n.

Agora, suponhamos que exista um subgrupo normal minimal K de S^n distinto de $N_1,\ldots,N_n$. Pela Proposição 1.3.2, temos

$$K\le C_{S^n}(N_1)\cap\cdots\cap C_{S^n}(N_n) = C_{S^n}(S^n) = Z(S^n) = \{1\},$$

pois $Z(S^n) = (Z(S))^n$ e S é um grupo simples não abeliano. Esta contradição nos leva a concluir que $N_1,\ldots,N_n$ são os únicos subgrupos normais minimais de S^n. □

Definição 1.6.12. *Seja H um subgrupo de um grupo G. Um subconjunto $T\subseteq G$ é dito um transversal à direita de H em G se o grupo G é uma união disjunta*

$$G = \dot{\bigcup_{t\in T}} Ht.$$

Em outras palavras, T contém exatamente um elemento de cada classe lateral à direita de H em G.

Definição 1.6.13. *Sejam G um grupo e $H\le G$. Definimos o coração normal de H em G como*

$$H_G = \bigcap_{g\in G} H^g.$$

Temos que H_G é o maior subgrupo normal de G contido em H.

Lema 1.6.14 (Lema da Imersão, [23], Resultado (4.1))**.** *Sejam H um subgrupo de um grupo finito G, $\{x_1, \ldots, x_n\}$ um transversal à direita para H em G e ξ um homomorfismo qualquer com domínio H, digamos $\xi : H \to X$. Então a aplicação*

$$\begin{aligned} f : G &\to H^{\xi} \wr S_n, \\ x &\mapsto (((x_1 x x_{1\pi}^{-1})^{\xi}, \ldots, (x_n x x_{n\pi}^{-1})^{\xi}), \pi), \end{aligned}$$

onde $\pi \in S_n$ é a única permutação que satisfaz $x_i x \in H x_{i\pi}$ para todo $i \in \{1, \ldots, n\}$, é um homomorfismo bem-definido com núcleo igual ao coração normal de $\ker(\xi)$ em G, em outras palavras, $\ker(f) = (\ker(\xi))_G$.

Teorema 1.6.15. *Sejam S um grupo simples não abeliano finito e n um inteiro positivo. Então*

$$\mathrm{Aut}(S^n) \cong \mathrm{Aut}(S) \wr S_n.$$

Demonstração. Primeiro, definamos $\gamma : \mathrm{Aut}(S) \wr S_n \to \mathrm{Aut}(S^n)$ por

$$((\varphi_1, \ldots, \varphi_n), \sigma)^{\gamma} = \alpha[\varphi_i, \sigma], \quad \text{sempre que} \quad \varphi_1, \ldots, \varphi_n \in \mathrm{Aut}(S),\ \sigma \in S_n,$$

sendo $\alpha[\varphi_i, \sigma] \in \mathrm{Aut}(S^n)$ dada por

$$(s_1, \ldots, s_n)^{\alpha[\varphi_i, \sigma]} = (s_{1\sigma^{-1}}\varphi_{1\sigma^{-1}}, \ldots, s_{n\sigma^{-1}}\varphi_{n\sigma^{-1}}), \quad \text{sempre que} \quad s_1, \ldots, s_n \in S^n.$$

Afirmamos que γ é um homomorfismo injetivo. Com efeito, sejam $(\varphi_1, \ldots, \varphi_n), (\psi_1, \ldots, \psi_n) \in \mathrm{Aut}(S)^n$, $\sigma, \tau \in S_n$ e $(s_1, \ldots, s_n) \in S^n$. Temos que

$$\begin{aligned} ((\varphi_1, \ldots, \varphi_n),&\sigma)((\psi_1, \ldots, \psi_n), \tau) \\ &= \left((\varphi_1, \ldots, \varphi_n) \cdot (\psi_1, \ldots, \psi_n)^{\sigma^{-1}}, \sigma\tau\right) \\ &= ((\varphi_1, \ldots, \varphi_n) \cdot (\psi_{1\sigma}, \ldots, \psi_{n\sigma}), \sigma\tau) \\ &= (\varphi_1\psi_{1\sigma}, \ldots, \varphi_n\psi_{n\sigma}, \sigma\tau). \end{aligned}$$

Daí,

$$(((\varphi_1, \ldots, \varphi_n), \sigma)((\psi_1, \ldots, \psi_n), \tau))^{\gamma} = (\varphi_1\psi_{1\sigma}, \ldots, \varphi_n\psi_{n\sigma}, \sigma\tau)^{\gamma} = \alpha[\varphi_i\psi_{i\sigma}, \sigma\tau]$$

de modo que

$$\begin{aligned}(s_1,\ldots,s_n)^{\alpha[\varphi_i\psi_{i\sigma},\sigma\tau]} &= (s_{1\tau^{-1}\sigma^{-1}}\varphi_{1\tau^{-1}\sigma^{-1}}\psi_{1\tau^{-1}\sigma^{-1}\sigma},\ldots,s_{n\tau^{-1}\sigma^{-1}}\varphi_{n\tau^{-1}\sigma^{-1}}\psi_{n\tau^{-1}\sigma^{-1}\sigma})\\ &= (s_{1\tau^{-1}\sigma^{-1}}\varphi_{1\tau^{-1}\sigma^{-1}}\psi_{1\tau^{-1}},\ldots,s_{n\tau^{-1}\sigma^{-1}}\varphi_{n\tau^{-1}\sigma^{-1}}\psi_{n\tau^{-1}}).\end{aligned}$$

Por outro lado,

$$\begin{aligned}(s_1,\ldots,s_n)^{\alpha[\varphi_i,\sigma]\alpha[\psi_i,\tau]} &= \left((s_1,\ldots,s_n)^{\alpha[\varphi_i,\sigma]}\right)^{\alpha[\psi_i,\tau]}\\ &= (s_{1\sigma^{-1}}\varphi_{1\sigma^{-1}},\ldots,s_{n\sigma^{-1}}\varphi_{n\sigma^{-1}})^{\alpha[\psi_i,\tau]}\\ &= (s_{1\tau^{-1}\sigma^{-1}}\varphi_{1\tau^{-1}\sigma^{-1}}\psi_{1\tau^{-1}},\ldots,s_{n\tau^{-1}\sigma^{-1}}\varphi_{n\tau^{-1}\sigma^{-1}}\psi_{n\tau^{-1}}).\end{aligned}$$

Portanto, γ é um homomorfismo.

Agora, seja $((\varphi_1,\ldots,\varphi_n),\sigma)\in\ker(\gamma)$. Então

$$(s_{1\sigma^{-1}}\varphi_{1\sigma^{-1}},\ldots,s_{n\sigma^{-1}}\varphi_{n\sigma^{-1}}) = (s_1,\ldots,s_n)\quad\text{para todo}\quad(s_1,\ldots,s_n)\in S^n,$$

ou seja, $s_{i\sigma^{-1}}\varphi_{i\sigma^{-1}} = s_i$ para todo $i\in\{1,\ldots,n\}$ e para todo $s_i\in S$. Suponhamos que exista $i\in\{1,\ldots,n\}$ tal que $i\sigma\neq i$. Escolhendo $s_j = 1$, para todo $j\neq i$, e s_i um elemento não trivial de S, obtemos que $s_{i\sigma} = 1$ de modo que

$$s_i\varphi_i = s_{(i\sigma)\sigma^{-1}}\varphi_{(i\sigma)\sigma^{-1}} = s_{i\sigma} = 1,$$

e isto nos dá que $s_i = 1$ (pois φ_i é um automorfismo), uma contradição. Assim, σ é a permutação identidade 1 donde $s_i\varphi_i = s_i$ para todo $i\in\{1,\ldots,n\}$ e para todo $s_i\in S$, isto é, φ_i é a aplicação identidade id_S para todo $i\in\{1,\ldots,n\}$. Portanto, $((\varphi_1,\ldots,\varphi_n),\sigma) = ((\mathrm{id}_S,\ldots,\mathrm{id}_S),1)$ donde $\ker(\gamma)$ é trivial, e a afirmação segue.

Pelo Teorema dos Isomorfismos, segue-se que $\mathrm{Aut}(S)\wr S_n$ é isomorfo a $\mathrm{Im}(\gamma)\leq\mathrm{Aut}(S^n)$, logo

$$|\mathrm{Aut}(S)\wr S_n| = |\mathrm{Im}(\gamma)| \leq |\mathrm{Aut}(S^n)|.$$

Então, basta mostrar que $|\mathrm{Aut}(S^n)|\leq|\mathrm{Aut}(S)\wr S_n|$ para concluir que γ é um isomorfismo. Para isto, vamos usar o Lema da Imersão (Lema 1.6.14). Sabemos da Proposição 1.6.11 que os subgrupos normais minimais de S^n são os fatores diretos

$$N_i = \{1\}\times\cdots\times\{1\}\times S\times\{1\}\times\cdots\times\{1\}\quad(1\leq i\leq n)$$

com S na i-ésima entrada. Se $\beta \in \mathrm{Aut}(S^n)$, então β leva um subgrupo normal minimal N_i de S^n em um subgrupo normal minimal N_j de S^n. Desse modo, consideremos a ação $(\beta, N_i) \mapsto N_i^\beta$ de $\mathrm{Aut}(S^n)$ em $\{N_1, \ldots, N_n\}$. Esta ação é transitiva. De fato, dado $i \in \{1, \ldots, n\}$, considerando $\beta \in \mathrm{Aut}(S^n)$ dado por

$$(s_1, \ldots, s_i, \ldots, s_n)^\beta = (s_i, \ldots, s_1, \ldots, s_n),$$

temos que $N_i = N_1^\beta$, ou seja, existe apenas uma órbita. Agora, temos que o estabilizador de N_1 é o conjunto

$$\{\beta \in \mathrm{Aut}(S^n) \mid N_1^\beta = N_1\} =: N_{\mathrm{Aut}(S^n)}(N_1).$$

Seja $H = N_{\mathrm{Aut}(S^n)}(N_1)$. Pelo Teorema 1.2.5, $[\mathrm{Aut}(S^n) : H] = n$. Vamos então considerar $\eta : H \to \mathrm{Aut}(N_1)$ o homomorfismo induzido pela ação natural de H em N_1. Dado $\theta \in \mathrm{Aut}(N_1)$, temos que $\nu : S^n \to S^n$ dado por

$$(s_1, \ldots, s_n)^\nu = \left(s_1^{\theta^\delta}, \ldots, s_n^{\theta^\delta}\right) \quad (\theta^\delta = \delta^{-1}\theta\delta),$$

onde $\delta : N_1 \to S$ é o isomorfismo $(s, 1, \ldots, 1) \mapsto s$, é um automorfismo de S^n tal que $\nu^\eta = \theta$. Logo, η é sobrejetiva. Além disso,

$$\ker(\eta) = \{\beta \in \mathrm{Aut}(S^n) \mid x^\beta = x,\ \forall x \in N_1\} =: C_{\mathrm{Aut}(S^n)}(N_1).$$

Vamos calcular o coração normal de $\ker(\eta)$ em $\mathrm{Aut}(S^n)$. Temos

$$(\ker(\eta))_{\mathrm{Aut}(S^n)} = (C_{\mathrm{Aut}(S^n)}(N_1))_{\mathrm{Aut}(S^n)} = \bigcap_{\beta \in \mathrm{Aut}(S^n)} (C_{\mathrm{Aut}(S^n)}(N_1))^\beta =$$

$$\bigcap_{\beta \in \mathrm{Aut}(S^n)} C_{\mathrm{Aut}(S^n)}(N_1^\beta) = C_{\mathrm{Aut}(S^n)}(N_1) \cap \cdots \cap C_{\mathrm{Aut}(S^n)}(N_n) = C_{\mathrm{Aut}(S^n)}(S^n) = \{1\}.$$

Agora, considerando $\xi = \eta\zeta : H \to \mathrm{Aut}(S)$, onde $\zeta : \mathrm{Aut}(N_1) \to \mathrm{Aut}(S)$ é o isomorfismo $\theta \mapsto \theta^\delta$, temos, pelo Lema da Imersão, que existe um homomorfismo

$$f : \mathrm{Aut}(S^n) \to \mathrm{Aut}(S) \wr S_n$$

tal que $\ker(f) = (\ker(\xi))_{\mathrm{Aut}(S^n)} = (\ker(\eta))_{\mathrm{Aut}(S^n)} = \{1\}$. Portanto, $|\mathrm{Aut}(S^n)| \leq |\mathrm{Aut}(S) \wr S_n|$, como queríamos. Isto completa a prova do teorema. □

1.7 G-Grupos e G-Módulos

Nesta seção, G denota um grupo arbitrário.

Definição 1.7.1. *Um G-grupo é um grupo H com uma ação (como grupo) de G em H*

$$\begin{aligned} \varphi : G &\longrightarrow \mathrm{Aut}(H) \\ g &\longmapsto g^{\varphi} : H \longrightarrow H \\ & \qquad\quad h \longmapsto h^{g}, \end{aligned}$$

para quaisquer $g \in G$ e $h \in H$.

Notemos que se $N \trianglelefteq G$, então N é um G-grupo com φ sendo a ação de conjugação de G em N.

Dados dois G-grupos H e K, dizemos que $\gamma : H \to K$ é uma *G-aplicação* se

$$(h^{g})^{\gamma} = (h^{\gamma})^{g},$$

para quaisquer $h \in H$ e $g \in G$. Se γ é um homomorfismo, dizemos que γ é um *G-homomorfismo*. Se além disso $H = K$, γ é dita um *G-endomorfismo de H*, e denotamos por

$$\mathrm{End}_G(H)$$

o conjunto dos G-endomorfismos de H. E se γ é um isomorfismo, dizemos que esta aplicação é um *G-isomorfismo*. Neste caso, H e K são ditos *G-isomorfos*, e denotamos por $H \cong_G K$. Observamos que $\gamma^{-1} : K \to H$ também é um G-isomorfismo: dados $h \in H$ e $k \in K$ tais que $h^{\gamma} = k$, temos que

$$(k^{g})^{\gamma^{-1}} = ((h^{\gamma})^{g})^{\gamma^{-1}} = ((h^{g})^{\gamma})^{\gamma^{-1}} = h^{g} = (k^{\gamma^{-1}})^{g}.$$

Sejam H um G-grupo e $L \leq H$. Dizemos que L é um *G-subgrupo* se

$$l^{g} \in L,$$

para todos $l \in L$ e $g \in G$. Nesse sentido, H é dito ser um *G-grupo simples* se H é não trivial e os únicos G-subgrupos de H são $\{1\}$ e H.

Proposição 1.7.2. *Sejam H e K dois G-grupos. Se H é um G-grupo simples e $H \cong_G K$, então K também é um G-grupo simples.*

Demonstração. Temos que existe um G-isomorfismo $\gamma : K \to H$, pois $H \cong_G K$. Seja L um G-subgrupo de K e consideremos $N = L^\gamma \leq H$. Dados $g \in G$ e $n \in N$, existe $l \in L$ tal que $n = l^\gamma$, e dado que L é um G-subgrupo, temos $l^g \in L$. Daí,

$$n^g = (l^\gamma)^g = (l^g)^\gamma \in N,$$

pois γ é um G-isomorfismo. Desse modo, N é um G-subgrupo de H. Mas H é um G-grupo simples, consequentemente $N = \{1\}$ ou $N = H$. No primeiro caso, obtemos $L = \{1\}$, e no segundo, $L = K$. Concluímos, assim, que K é um G-grupo simples. □

Proposição 1.7.3. *Sejam G um grupo e $H, K \trianglelefteq G$. Então*

$$KH/K \cong_G H/(H \cap K).$$

Além disso, se H e K são subgrupos normais minimais distintos de G, então KH/K é um subgrupo normal minimal de G/K.

Demonstração. Temos que KH/K e $H/(H \cap K)$ são G-grupos com as respectivas ações

$$(Kh)^g = Kh^g \quad \text{e} \quad ((H \cap K)h)^g = (H \cap K)h^g \quad (\text{sendo } h^g = g^{-1}hg),$$

haja vista que $H \trianglelefteq G$. Pelo Teorema dos Isomorfismos, temos que a aplicação $\gamma : KH/K \to H/(H \cap K)$ dada por

$$(Kh)^\gamma = (H \cap K)h, \qquad \text{sempre que} \quad h \in H,$$

é um isomorfismo. Por outro lado, temos

$$((Kh)^g)^\gamma = (Kh^g)^\gamma = (H \cap K)h^g = ((H \cap K)h)^g = ((Kh)^\gamma)^g,$$

para quaisquer $h \in H$ e $g \in G$. Portanto,

$$KH/K \cong_G H/(H \cap K).$$

Agora, suponhamos que H e K são subgrupos normais minimais distintos de G. Dado que H e K são normais em G, temos que $KH \trianglelefteq G$ e $KH/K \trianglelefteq G/K$. Pelo que provamos acima, segue-se que

$$KH/K \cong_G H,$$

pois, como visto na demonstração da Proposição 1.3.2, $H \cap K = \{1\}$. Assim, KH/K é

não trivial. Seja $\overline{L} \trianglelefteq G/K$ tal que $\overline{L} \leq KH/K$. Sendo $\psi : KH/K \to H$ o G-isomorfismo envolvido, temos que $\overline{L}^{\psi} \leq H$. Dados $x \in \overline{L}$ e $g \in G$,

$$(x^{\psi})^{g} = (x^{g})^{\psi} \in \overline{L}^{\psi},$$

porque $x^{g} \in \overline{L}$. Ou seja, $\overline{L}^{\psi} \trianglelefteq G$ de modo que $\{1\} = \overline{L}^{\psi}$ ou $\overline{L}^{\psi} = H$, já que H é normal minimal em G. Portanto,

$$\{1\} = \overline{L} \quad \text{ou} \quad \overline{L} = KH/K,$$

isto é, KH/K é normal minimal em G/K. □

Definição 1.7.4. *Seja H um G-grupo. Uma G-série (de comprimento finito) de H é uma sequência finita*

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H,$$

onde cada termo H_i é um G-subgrupo. Os grupos quocientes G_{i+1}/G_i são chamados os fatores da série.

Consideremos o conjunto de todas as G-séries de um G-grupo H. Este é não vazio, pois contém a G-série $\{1\} \trianglelefteq H$. Se S e T são G-séries de H, dizemos que S é um *refinamento* de T se todo termo de T é também um termo de S. Se existe pelo menos um termo de S o qual não é um termo de T, então S é dita um *refinamento próprio* de T.

Uma G-série que não admite refinamentos próprios é chamada uma *G-série de composição*. Equivalentemente, como mostrado em [22, 3.1.3], uma G-série é uma G-série de composição se, e somente se, todos os seus fatores são G-simples.

Duas G-séries S e T de um G-grupo H são ditas *G-isomorfas* se existe uma bijeção entre o conjunto dos fatores de S e o conjunto dos fatores de T tal que os fatores correspondentes são G-isomorfos. Nesse sentido, temos o:

Teorema 1.7.5 (Teorema de Jordan-Hölder, [22], 3.1.4)**.** *Seja H um G-grupo. Se S é uma G-série de composição de H e T é uma G-série qualquer de H, então T admite um refinamento o qual é uma série de composição G-isomorfa a S. Em particular, se T é uma G-série de composição, esta é G-isomorfa a S.*

Agora, seja A um G-grupo abeliano. Neste caso, dizemos que A é um *G-módulo*. Os G-subgrupos de A são chamados de *G-submódulos*. Um G-submódulo $M < A$ é dito *maximal* se não existe G-submódulo H tal que $M < H < A$.

Lema 1.7.6 (Schur)**.** *Se $f : A \to B$ é um G-homomorfismo entre G-módulos simples e $f \neq 1$, então f é um G-isomorfismo.*

Demonstração. Temos que $\ker(f)$ é um G-submódulo de A, porque f é um G-homomorfismo. Como A é simples, segue-se que $\ker(f) = \{1\}$ ou $\ker(f) = A$. Contudo, dado que $f \neq 1$, concluímos que $\ker(f) = \{1\}$ e f é injetiva. Analogamente, $\mathrm{Im}(f) = \{1\}$ ou $\mathrm{Im}(f) = B$, mas uma vez que $f \neq 1$, segue-se que $\mathrm{Im}(f) = B$ e f é sobrejetiva. Portanto, f é um G-isomorfismo. □

Sejam G um grupo finito e A um G-módulo simples finito. Vamos usar a notação aditiva para a operação em A. Consideremos $F = \mathrm{End}_G(A)$ o anel dos G-endomorfismos de A com as operações de soma e composição de aplicações. Dado que A é um G-módulo simples, o Lema de Schur nos fornece que f é um G-isomorfismo para todo elemento $f \neq 0$ de F. Com isso, F é um anel de divisão donde, pelo Teorema de Wedderburn [17, Página 453], F é um corpo. Mais ainda, A é um espaço vetorial sobre F (basta considerar a multiplicação escalar fa sendo a^f, para quaisquer $f \in F$ e $a \in A$). Notemos também que uma soma direta de cópias de A também pode ser vista como um espaço vetorial sobre F.

Proposição 1.7.7 ([2], Lema 2)**.** *Sejam G um grupo finito, A um G-módulo simples e $F = \mathrm{End}_G(A)$. Seja V uma soma direta de d cópias de A, com uma estrutura de G-módulo dada pela ação por componentes. Então o número de G-submódulos maximais de V é*

$$\frac{q^d - 1}{q - 1},$$

com $q = |F|$.

Demonstração. Temos $V = \{(a_1, \ldots, a_d) \mid a_i \in A\}$ e aplicações

$$\gamma_i : A \to V,$$

definidas por $a^{\gamma_i} = (0, \ldots, 0, a, 0, \ldots, 0)$, sempre que $a \in A$, onde a entrada não nula é a i-ésima coordenada.

Seja M um G-submódulo maximal de V. Então existe um G-homomorfismo sobrejetivo

$$\psi : V \to A$$

com $\ker(\psi) = M$. De fato, temos que a série

$$S : \{0\} < A < A^2 < \cdots < A^d = V$$

é uma G-série de composição de V, pois seus fatores são todos G-isomorfos a A donde,

pela Proposição 1.7.2, são G-simples. Desse modo, pelo Teorema de Jordan-Hölder (Teorema 1.7.5), a G-série

$$\{0\} < M < V$$

admite um refinamento que é uma G-série de composição G-isomorfa a S. Consequentemente, uma vez que M um G-submódulo maximal de V, segue-se que existe um G-isomorfismo $\varphi : V/M \to A$. Portanto, basta considerar $\psi = \pi\varphi$, com $\pi : V \to V/M$ sendo a projeção canônica.

Agora, dado $i \in \{1, \ldots, d\}$, temos $\lambda_i \in F$ definido por

$$\lambda_i = \gamma_i\psi : A \to A.$$

Assim,

$$(a_1, \ldots, a_d)^\psi = (a_1, 0, \ldots, 0)^\psi + \cdots + (0, \ldots, 0, a_d)^\psi =$$

$$a_1^{\gamma_1\psi} + \cdots + a_d^{\gamma_d\psi} = \sum_{i=1}^{d} a_i^{\gamma_i\psi} = \sum_{i=1}^{d} a_i^{\lambda_i}.$$

Em particular, $\lambda_1, \ldots, \lambda_d$ não podem ser todos nulos já que ψ não é nulo. E $(a_1, \ldots, a_d) \in \ker(\psi) = M$ se, e somente se, $\sum_{i=1}^{d} a_i^{\lambda_i} = 0$. Observamos também que ψ é F-linear. Para ver isto, sejam $\lambda \in F$ e $(a_1, \ldots, a_d) \in V$. Haja vista que F é um corpo, a operação de composição em F é comutativa, logo para qualquer $\lambda_i \in F$ temos $\lambda\lambda_i = \lambda_i\lambda$. Consequentemente,

$$(\lambda a_1, \ldots, \lambda a_d)^\psi = \sum_{i=1}^{d} (a_i^\lambda)^{\lambda_i} =$$

$$\sum_{i=1}^{d} a_i^{\lambda\lambda_i} = \sum_{i=1}^{d} a_i^{\lambda_i\lambda} = \sum_{i=1}^{d} (a_i^{\lambda_i})^\lambda =$$

$$\left(\sum_{i=1}^{d} a_i^{\lambda_i} \right)^\lambda = \lambda(a_1, \ldots, a_d)^\psi.$$

Sejam agora $\lambda_1, \ldots, \lambda_d \in F$, não todos nulos, e definamos $\psi : V \to A$ por

$$(a_1, \ldots, a_d)^\psi = \sum_{i=1}^{d} a_i^{\lambda_i}, \qquad \text{sempre que} \quad (a_1, \ldots, a_d) \in V.$$

Afirmamos que ψ é um G-homomorfismo sobrejetivo. Com efeito, dado $g \in G$,

$$(a_1^g, \ldots, a_d^g)^\psi = \sum_{i=1}^{d} (a_i^g)^{\lambda_i} = \sum_{i=1}^{d} (a_i^{\lambda_i})^g = ((a_1, \ldots, a_d)^\psi)^g,$$

pois cada λ_i é um G-endomorfismo. Assim, ψ é um G-homomorfismo. Agora, tomando um λ_i não nulo, temos que a restrição de ψ ao i-ésimo fator de V coincide com λ_i, o qual é um isomorfismo (Lema de Schur). Logo ψ é sobrejetiva, pois admite uma restrição sobrejetiva. Seja $M = \ker(\psi)$, então $V/M \cong_G A$, e sendo A um G-módulo simples, segue-se que M é um G-submódulo maximal de V.

Ou seja, mostramos que os G-submódulos maximais de V são da forma $\ker(\psi)$, com $\psi : V \to A$ um G-homomorfismo sobrejetivo da forma

$$(a_1, \ldots, a_d)^\psi = \sum_{i=1}^{d} a_i^{\lambda_i},$$

onde $\lambda_1, \ldots, \lambda_d \in F$ não são todos nulos. Agora, dado $0 \neq \lambda \in F$, $(\lambda\lambda_1, \ldots, \lambda\lambda_d)$ define o mesmo G-submódulo maximal que $(\lambda_1, \ldots, \lambda_d)$. De fato, se $\eta : V \to A$ é definida por

$$(a_1, \ldots, a_d)^\eta = \sum_{i=1}^{d} a_i^{\lambda\lambda_i},$$

então

$$\sum_{i=1}^{d} a_i^{\lambda\lambda_i} = 0 \Leftrightarrow \sum_{i=1}^{d} a_i^{\lambda_i\lambda} = 0 \Leftrightarrow \left(\sum_{i=1}^{d} a_i^{\lambda_i}\right)^\lambda = 0 \Leftrightarrow \sum_{i=1}^{d} a_i^{\lambda_i} = 0,$$

isto é, $\ker(\eta) = \ker(\psi)$. Reciprocamente, sejam $\psi : V \to A$ e $\eta : V \to A$ G-homomorfismos sobrejetivos com $\ker(\eta) = \ker(\psi) := M$, cujas respectivas expressões são

$$(a_1, \ldots, a_d)^\psi = \sum_{i=1}^{d} a_i^{\lambda_i} \quad \text{e} \quad (a_1, \ldots, a_d)^\eta = \sum_{i=1}^{d} a_i^{\beta_i},$$

sendo que $\lambda_1, \ldots, \lambda_d \in F$ não são todos nulos, assim como $\beta_1, \ldots, \beta_d \in F$. Pelo Teorema dos Isomorfismos, ψ e η induzem G-isomorfismos $\overline{\psi} : V/M \to A$ e $\overline{\eta} : V/M \to A$ de forma que, considerando $\lambda = \overline{\psi}^{-1}\overline{\eta}$, temos que $\lambda \in F^*$ e $\eta = \psi\lambda$. Dados $i \in \{1, \ldots, d\}$ e $a_i \in A$, temos

$$a_i^{\beta_i} = (0, \ldots, 0, a_i, 0, \ldots, 0)^\eta = (0, \ldots, 0, a_i, 0, \ldots, 0)^{\psi\lambda} = a_i^{\lambda_i\lambda} = a^{\lambda\lambda_i},$$

já que F é comutativo. Pela arbitrariedade de i e a_i, segue-se que $(\beta_1, \ldots, \beta_d) =$

$(\lambda\lambda_1, \ldots, \lambda\lambda_d)$. Portanto, o número de G-submódulos maximais de V é

$$\frac{q^d - 1}{q - 1}.$$

□

1.8 Grupos Livres

Definição 1.8.1. *Sejam F um grupo, X um conjunto não vazio e $\gamma : X \to F$ uma função. Dizemos que F, ou mais precisamente (F, γ), é livre sobre X se para cada função α de X em um grupo G, existe um único homomorfismo $\beta : F \to G$ tal que*

$$\alpha = \gamma\beta.$$

Um grupo que é livre sobre algum conjunto é chamado um grupo livre.

A função $\gamma : X \to F$ é necessariamente injetiva. Com efeito, suponhamos que $x_1^\gamma = x_2^\gamma$ e $x_1 \neq x_2$. Seja G um grupo com pelo menos dois elementos distintos g_1 e g_2, e escolhamos uma função $\alpha : X \to G$ tal que $x_1^\alpha = g_1$ e $x_2^\alpha = g_2$. Então, $x_1^{\gamma\beta} = x_2^{\gamma\beta}$, consequentemente $x_1^\alpha = x_2^\alpha$ e $g_1 = g_2$, um absurdo.

Agora, seja $\theta : \mathrm{Im}(\gamma) \to F$ a aplicação inclusão, e consideremos $\gamma' : X \to \mathrm{Im}(\gamma)$ a restrição de γ. Esta última, como visto acima, é uma bijeção, logo admite inversa $(\gamma')^{-1}$. Notemos que para cada $x \in X$,

$$x^{\gamma'\theta} = (x^{\gamma'})^\theta = (x^\gamma)^\theta = x^\gamma,$$

ou seja, $\gamma'\theta = \gamma$ e $(\gamma')^{-1}\gamma = \theta$. Assim, dada uma função $\alpha : \mathrm{Im}(\gamma) \to G$, onde G é um grupo qualquer, consideremos a função $\gamma'\alpha : X \to G$. Dado que (F, γ) é livre sobre X, existe um único homomorfismo $\beta : F \to G$ tal que $\gamma'\alpha = \gamma\beta$, logo

$$\alpha = (\gamma')^{-1}\gamma'\alpha = (\gamma')^{-1}\gamma\beta = \theta\beta.$$

Agora, seja $\beta_1 : F \to G$ um homomorfismo tal que $\alpha = \theta\beta_1$. Daí,

$$\gamma'\alpha = \gamma'\theta\beta_1 = \gamma\beta_1.$$

Pela unicidade de β, segue-se que $\beta_1 = \beta$. Portanto, F também é livre sobre $\mathrm{Im}(\gamma)$, isto é, um grupo livre é sempre livre em um subconjunto. Neste caso, de acordo com a

definição de grupo livre, a restrição de β a X é α, logo β é a única extensão de α a F.

Observamos que os grupos livres sempre existem, mais precisamente:

Teorema 1.8.2 ([22], 2.1.1)**.** *Se X é um conjunto não vazio, existem um grupo F e uma função $\gamma : X \to F$ tais que (F, γ) é livre sobre X e $F = \langle \mathrm{Im}(\gamma) \rangle$.*

Proposição 1.8.3. *Se F_1 é livre sobre X_1 e F_2 é livre sobre X_2, e se $|X_1| = |X_2|$, então $F_1 \cong F_2$.*

Demonstração. Sejam $\gamma_1 : X_1 \to F_1$ e $\gamma_2 : X_2 \to F_2$ as funções injetoras dadas, e seja $\alpha : X_1 \to X_2$ uma bijeção. Desse modo, existem homomorfismos $\beta_1 : F_1 \to F_2$ e $\beta_2 : F_2 \to F_1$ tais que

$$\gamma_1\beta_1 = \alpha\gamma_2 \quad \text{e} \quad \gamma_2\beta_2 = \alpha^{-1}\gamma_1.$$

Logo,

$$\gamma_1\beta_1\beta_2 = \alpha\gamma_2\beta_2 = \alpha\alpha^{-1}\gamma_1 = \gamma_1.$$

Como a aplicação identidade id_{F_1} composta com γ_1 é igual a γ_1, segue-se pela unicidade que $\beta_1\beta_2 = \mathrm{id}_{F_1}$. Por outro lado,

$$\gamma_2\beta_2\beta_1 = \alpha^{-1}\gamma_1\beta_1 = \alpha^{-1}\alpha\gamma_2 = \gamma_2.$$

Uma vez que id_{F_2} composta com γ_2 é igual a γ_2, obtemos pela unicidade que $\beta_2\beta_1 = \mathrm{id}_{F_2}$. Portanto, β_1 é um isomorfismo e $F_1 \cong F_2$. □

Reciprocamente, se $F_1 \cong F_2$, então $|X_1| = |X_2|$ (vide [5, Teorema D.2.8]). Assim, definimos o *posto* de um grupo livre F como a cardinalidade de qualquer conjunto no qual F é livre.

Seja (F, γ) livre sobre um conjunto X. Pela Teorema 1.8.2, existem um grupo F_1 e uma função $\gamma_1 : X \to F_1$ tais que (F_1, γ_1) é livre sobre X e $F_1 = \langle \mathrm{Im}(\gamma_1) \rangle$. Usando a prova da Proposição 1.8.3 (considerando $\alpha : X \to X$ como a identidade), obtemos um isomorfismo $\psi : F_1 \to F$ tal que $\gamma_1\psi = \gamma$. Isto nos dá que $\mathrm{Im}(\gamma) = (\mathrm{Im}(\gamma_1))^{\psi}$ donde, pela Proposição 1.1.3, $F = \langle \mathrm{Im}(\gamma) \rangle$.

Para finalizar esta seção, vamos fazer a seguinte observação:

Observação 1.8.4. *Seja G um grupo gerado por um subconjunto X e seja F um grupo livre. Pelo que vimos anteriormente, existe um subconjunto Y de F tal que F é livre sobre Y e $F = \langle Y \rangle$. Assim, se $\alpha : Y \to X$ é uma sobrejeção, esta se estende a um homomorfismo de F em G, o qual é sobrejetivo, já que $G = \langle X \rangle$.*

Capítulo

2

Geração de Grupos Finitos

Neste capítulo, abordaremos a relação entre a geração de grupos finitos e os grupos crown-based power, a fim de classificar os grupos finitos G tais que todo grupo quociente próprio de G pode ser gerado por m elementos (com $m \in \mathbb{Z}_+$), mas o próprio G não pode. Também, vamos descrever como a função f, apresentada na introdução, pode ser calculada. Ou seja, o objetivo deste capítulo é demonstrar os Teoremas A e B. O estudo foi baseado no artigo *Finite groups that need more generators than any proper quotient* [8] de Francesca Dalla Volta e Andrea Lucchini.

2.1 Grupos Primitivos e Monolíticos

Nesta seção, vamos introduzir alguns conceitos que serão necessários para aprofundar na teoria de geração de grupos finitos.

Definição 2.1.1. *Seja G um grupo finito. Dizemos que G é um grupo primitivo se existe um subgrupo maximal M de G tal que $M_G = \{1\}$.*

Notemos que se G é um grupo primitivo, então $\Phi(G) = \{1\}$. De fato, por definição existe um subgrupo maximal M de G tal que $M_G = \{1\}$. Assim, $\Phi(G) \leq M$ e

$$\Phi(G) = \Phi(G)^g \leq M^g, \quad \forall g \in G,$$

pois $\Phi(G) \trianglelefteq G$. Portanto, $\Phi(G) \leq M_G = \{1\}$.

Exemplo 2.1.2. *O grupo alternado A_4 é primitivo porque $M = \langle(123)\rangle$ é um subgrupo maximal de A_4 (pois A_4 não possui subgrupos de ordem 6), e*

$$M_{A_4} \leq M \cap M^{(12)(34)} = \langle(123)\rangle \cap \langle(124)\rangle = \{1\}.$$

Definição 2.1.3. *Seja G um grupo. Definimos o socle de G, denotado por $\mathrm{soc}(G)$, como o subgrupo gerado por todos os subgrupos normais minimais de G.*

Observamos que, para um grupo finito G, se $N_1, N_2, \ldots, N_k$ são todos os subgrupos normais minimais de G, então $\mathrm{soc}(G) = N_1 N_2 \cdots N_k$. Desse modo, pelo Teorema 1.3.8, segue-se que $\mathrm{soc}(G)$ é o produto direto de alguns dos N_i's.

Definição 2.1.4. *Dizemos que um grupo finito G é monolítico se existe um único subgrupo normal minimal $N = \mathrm{soc}(G)$.*

Exemplo 2.1.5. *Sejam n um inteiro positivo e $G = S \wr C_n$, sendo que $C_n = \langle(12\cdots n)\rangle$ e S é um grupo simples não abeliano. Vamos mostrar que G é um grupo monolítico. Para isto, afirmamos que $N = S^n \times \{1\}$ é o único subgrupo normal minimal de G. Com efeito, sabemos que $N \trianglelefteq G$. Agora, seja $K \trianglelefteq G$ com $\{1\} < K \leq N$. Assim, K é um subgrupo normal não trivial de N; logo, pela Proposição 1.6.11, K contém algum dos fatores diretos de N, digamos*

$$N_1 = (S \times \{1\} \times \cdots \times \{1\}) \times \{1\}.$$

Seja $\sigma = (12\cdots n)$. Dado $i \in \{0, 1, \ldots, n-1\}$, temos que $(i+1)(\sigma^i)^{-1} = 1$, daí

$$((1, \ldots, 1, s, 1, \ldots, 1), 1) = ((s, 1, \ldots, 1), 1)^{((1,\ldots,1),\sigma^i)} \in K,$$

para todo $s \in S$ (observamos que s está na $(i+1)$-ésima entrada no elemento da esquerda), pois $N_1 \leq K \trianglelefteq G$ (em outras palavras, C_n age transitivamente no conjunto dos fatores diretos de N). Isto é válido para todo i, logo K contém todos os fatores diretos de N, e, portanto, $K = N$. Dessa forma, N é normal minimal em G.

Resta mostrar a unicidade. Pela Proposição 1.3.2, é suficiente provar que $C_G(N) = \{1\}$. Então, seja $1 \neq a \in S$. Qualquer elemento da forma $((s_1, \ldots, s_n), \sigma^i)$, com $i \in \{1, \ldots, n-1\}$, não pertence ao centralizador $C_G(N)$, pois, caso contrário, teríamos

$$\begin{aligned}((s_1, \ldots, s_{n-(i-1)}a, \ldots, s_n), \sigma^i) &= ((s_1, \ldots, s_n), \sigma^i)((a, 1, \ldots, 1), 1) \\ &= ((a, 1, \ldots, 1), 1)((s_1, \ldots, s_n), \sigma^i) = ((as_1, \ldots, s_n), \sigma^i)\end{aligned}$$

de modo que $as_1 = s_1$ e $a = 1$, um absurdo. Por outro lado, se $((s_1, \ldots, s_n), 1) \in C_G(N)$,

então dados $u_1, \ldots, u_n \in S$, temos

$$\begin{aligned}((s_1u_1, \ldots, s_nu_n), 1) &= ((s_1, \ldots, s_n), 1)((u_1, \ldots, u_n), 1) \\ &= ((u_1, \ldots, u_n), 1)((s_1, \ldots, s_n), 1) = ((u_1s_1, \ldots, u_ns_n), 1),\end{aligned}$$

ou seja, $s_1, \ldots, s_n \in Z(S)$. Consequentemente, $s_1 = \cdots = s_n = 1$. Portanto, $C_G(N) = \{1\}$, como queríamos. A afirmação segue, e concluímos que G é um grupo monolítico.

Proposição 2.1.6. *Seja G um grupo monolítico, com $N = \mathrm{soc}(G)$. Então, G é primitivo se, e somente se, $\Phi(G) = \{1\}$.*

Demonstração. Suponhamos que $\Phi(G) = \{1\}$. Se, para todo subgrupo maximal M de G, tivéssemos $N \subseteq M$, então $N \subseteq \Phi(G)$ donde $N = \{1\}$, uma contradição, pois N é normal minimal. Assim, existe um subgrupo maximal M de G tal que $N \nsubseteq M$. Sabemos que $M_G \trianglelefteq G$. Desse modo, se $M_G \neq \{1\}$, então M_G conteria um subgrupo normal minimal de G, logo $M_G \supseteq N$, já que por hipótese N é o único subgrupo normal minimal de G. Isto nos daria

$$N \subseteq M_G \subseteq M,$$

um absurdo. Portanto, $M_G = \{1\}$ e G é primitivo. A recíproca já foi observada anteriormente. □

Em outras palavras, a Proposição 2.1.6 nos diz que G é um grupo primitivo monolítico se, e somente se, admite um único subgrupo normal minimal e $\Phi(G) = \{1\}$.

Exemplo 2.1.7. *O grupo $G = S \wr C_n$ do Exemplo 2.1.5 acima é primitivo monolítico. De fato, se $\Phi(G)$ é não trivial, então este contém $N = S^n \times \{1\}$ (pois $\Phi(G) \trianglelefteq G$ e N é o único normal minimal de G). Agora, $Z(N) \trianglelefteq_c N \trianglelefteq G$, logo $Z(N) \trianglelefteq G$ (vide Proposição 1.1.11). Isto nos fornece que $Z(N) = \{1\}$, uma vez que N é normal minimal em G. Ou seja, N é não nilpotente. Por outro lado, pelo Teorema 1.5.5, $\Phi(G)$ é nilpotente de modo que N é nilpotente, um absurdo. Portanto, $\Phi(G) = \{1\}$ e G é primitivo monolítico.*

Exemplo 2.1.8. *Para $n \geq 3$, o grupo simétrico S_n é primitivo monolítico. De fato, mostramos no Exemplo 1.5.2 que $\Phi(S_n) = \{1\}$. Além disso, se $n \neq 4$, então A_n é o único subgrupo normal minimal de S_n, e se $n = 4$, temos que o subgrupo de Klein é o único tal subgrupo de S_n.*

Exemplo 2.1.9. *Todo grupo simples finito é primitivo monolítico. Com efeito, seja S um grupo simples finito. Por definição, $S \neq \{1\}$ e é o único subgrupo normal minimal. Como $\Phi(S) \trianglelefteq S$, temos que $\Phi(S) = \{1\}$ ou $\Phi(S) = S$. Mas o segundo caso não acontece, porque S é finito e não trivial. Portanto, $\Phi(S) = \{1\}$ e S é primitivo monolítico. Observamos*

que o grupo $G = S \times S$ é primitivo não monolítico. De fato, pela Proposição 1.6.11, $S \times \{1\}$ e $\{1\} \times S$ são (os) dois subgrupos normais minimais de G de modo que G é não monolítico. Agora, consideremos $D = \mathrm{diag}(G)$. Afirmamos que D é um subgrupo maximal de G com $D_G = \{1\}$. De fato, suponhamos primeiro que H é um subgrupo de G tal que $D \leq H$, e seja $N = \{s \in S \mid (s,1) \in H\}$. Claramente N é um subgrupo de S. Se $(s,1) \in H$ e $r \in S$, então

$$(r^{-1}sr, 1) = (r^{-1}, r^{-1}) \cdot (s,1) \cdot (r,r) \in H,$$

pois $D \leq H$. Consequentemente, $N \trianglelefteq S$. Por outro lado, dados $x, y \in S$, temos

$$(xy^{-1}, 1) \cdot (y,y) = (x,y),$$

logo

$$(x,y) \in H \Leftrightarrow (xy^{-1}, 1) \in H \Leftrightarrow xy^{-1} \in N.$$

Ou seja, $H = \{(x,y) \in G \mid xy^{-1} \in N\}$. Dado que S é simples, $N = \{1\}$ ou $N = S$ de forma que $H = D$ ou $H = G$. Isto mostra que D é um subgrupo maximal de G. Agora, seja d um elemento arbitrário de D_G. Pela definição de D_G, temos $d \in D^{(x,1)}$ para todo $x \in S$, isto é, $d = (s,s)$ com $s^x = s$ para todo $x \in S$. Ou melhor dizendo, $d = (s,s)$ com $s \in Z(S)$. Mas o centro de S é trivial, pois S é simples e não abeliano; portanto, $d = (1,1)$ e $D_G = \{1\}$. A afirmação segue, e concluímos que G é primitivo não monolítico.

Vamos agora demonstrar um resultado bastante importante acerca de grupos primitivos, devido a Øystein Ore e Reinhold Baer. Mas antes, precisaremos de alguns lemas auxiliares.

Lema 2.1.10 (Lei Modular de Dedekind)**.** *Sejam A, B, C subgrupos de um grupo G, e suponhamos que $A \leq B$. Então, $A(B \cap C) = B \cap AC$.*

Demonstração. A inclusão $\subseteq$ segue-se do fato de que $A \subseteq B$ e $B \cap C \subseteq C$. Agora, seja $x \in B \cap AC$, logo $x \in B$ e $x = ac$, para certos $a \in A$ e $c \in C$. Daí, $c = a^{-1}x \in B$, já que $A \leq B$. Portanto, $c \in B \cap C$, e, assim, $x \in A(B \cap C)$. Isto mostra a inclusão $\supseteq$. Concluímos então que $A(B \cap C) = B \cap AC$. □

Lema 2.1.11. *Seja G um grupo. Se $H \trianglelefteq K \leq G$ e $N \trianglelefteq G$, então $HN \trianglelefteq KN$.*

Demonstração. Vamos mostrar que $K, N \leq N_G(HN)$. Para isto, sejam $h \in H$, $n, n_1 \in N$ e $x \in K$ arbitrários. Temos que

$$(hn)^x = h^x n^x \in HN,$$

pois $H \trianglelefteq K$ e $N \trianglelefteq G$. Por outro lado,

$$(hn)^{n_1} = h^{n_1}n^{n_1} = h(n_1^{-1})^h n_1 n^{n_1} \in HN,$$

já que $N \trianglelefteq G$. Pela arbitrariedade dos elementos envolvidos, o lema segue. □

Lema 2.1.12. *Sejam G um grupo, $H \leq G$ e $g \in G$. Então*

$$N_G(H^g) = (N_G(H))^g.$$

Demonstração. Primeiro, mostremos que $N_G(H^g) \subseteq (N_G(H))^g$. Para isto, seja $x \in N_G(H^g)$. Por definição, temos que $(H^g)^x = H^g$. Daí, $H^{gx} = H^g$ de modo que $H^{gxg^{-1}} = H$, ou seja, $x^{g^{-1}} \in N_G(H)$. Portanto, $x = (x^{g^{-1}})^g \in (N_G(H))^g$. Pela arbitrariedade de x, a inclusão segue.

Agora, vamos mostrar a outra inclusão. Seja $x \in N_G(H)$, então $H^x = H$. Daí,

$$(H^g)^{x^g} = H^{gx^g} = H^{gg^{-1}xg} = H^{xg} = (H^x)^g = H^g.$$

Portanto, $x^g \in N_G(H^g)$. Pela arbitrariedade de x, obtemos que $(N_G(H))^g \subseteq N_G(H^g)$. Com isso, a proposição segue. □

Definição 2.1.13. *Seja p um número primo e G um grupo finito.*

$$O_p(G) = \prod_{N \in \mathscr{R}_p} N$$

é o maior p-subgrupo normal de G, sendo que $\mathscr{R}_p$ é o conjunto dos p-subgrupos normais de G.

Se G é um grupo solúvel finito não trivial, então G admite um subgrupo normal minimal N, o qual é abeliano elementar para algum primo p (vide Proposição 1.4.6). Dessa forma, $O_p(G) \neq \{1\}$.

Teorema 2.1.14 (Teorema de Ore-Baer, [24], 11.14)**.** *Seja G um grupo finito tal que $O_p(G) \neq \{1\}$, para algum primo p. Seja $L = O_p(G)$ e $|L| = p^n$. Suponhamos também que G é primitivo, ou seja, existe um subgrupo maximal M de G com $M_G = \{1\}$. Então*

(i) L é abeliano elementar,

(ii) M é um complemento para L em G; em particular, $[G : M] = p^n$,

(iii) L é normal minimal em G, e

(iv) $C_G(L) = L$*; consequentemente,* L *é o único subgrupo normal minimal de* G*, ou seja,* G *é primitivo monolítico.*

Suponhamos ainda que existe um primo q *tal que* $O_q(M) \neq \{1\}$*. Então, para qualquer tal* q*,*

(v) $p^n \equiv 1 \mod q$*; em particular,* $q \neq p$*, e*

(vi) todo complemento para L *em* G *é conjugado a* M*.*

Demonstração.

(i) Sendo G um grupo primitivo, temos $\Phi(G) = \{1\}$. Daí, como $L \trianglelefteq G$, o item (ii) do Lema 1.5.6 nos dá que $\Phi(L) = \{1\}$. Mas L é um p-grupo, logo pela Proposição 1.5.7, L é abeliano elementar.

(ii) Como $\{1\} \neq L \trianglelefteq G$ e $M_G = \{1\}$, temos que $L \nsubseteq M$. Assim, $M < ML \leq G$, e, então, pela maximalidade de M, obtemos que $ML = G$. Uma vez que $L \trianglelefteq G$, $M \cap L \trianglelefteq M$ e como, por (i), L é abeliano, $M \cap L \trianglelefteq L$. Logo $M \cap L \trianglelefteq ML = G$, e, então, $M \cap L \leq M_G = \{1\}$. Portanto, $ML = G$ e $M \cap L = \{1\}$; isto é, M é um complemento para L em G. Em particular, $[G : M] = |L| = p^n$.

(iii) Seja $\{1\} < K \trianglelefteq G$ com $K \leq L$. Então $M \leq MK \leq G$. Como $M_G = \{1\}$, $K \nsubseteq M$ e $MK \neq M$. Pela maximalidade de M, $MK = G$. Além disso, $M \cap K \leq M \cap L = \{1\}$, por (ii). Portanto, M é um complemento para K em G, e, assim, $|K| = [G : M] = |L|$, por (ii). Uma vez que $K \leq L$, segue-se que $K = L$. Dessa forma, L é normal minimal em G.

(iv) Por (i) e (ii),

$$L \leq C_G(L) \leq G = ML.$$

Usando a Lei Modular de Dedekind (Lema 2.1.10),

$$C_G(L) = C_G(L) \cap G = C_G(L) \cap ML = (M \cap C_G(L))L.$$

Como $L \trianglelefteq G$, temos $C_G(L) \trianglelefteq G$ de modo que $M \cap C_G(L) \trianglelefteq M$. Além disso, L centraliza, e, então, normaliza $M \cap C_G(L)$. Consequentemente, $M \cap C_G(L) \trianglelefteq ML = G$. Dado que $M_G = \{1\}$, segue-se que $M \cap C_L(G) = \{1\}$, e, portanto,

$$C_G(L) = L.$$

Suponhamos que G admite um subgrupo normal minimal $N \neq L$. Pela Proposição 1.3.2, $N \leq C_G(L) = L$. Mas isto contradiz a minimalidade de L. Com isso,

concluímos que L é o único subgrupo normal minimal de G, isto é, G é primitivo monolítico.

Agora, suponhamos que $O_q(M) \neq \{1\}$ para algum primo q. Seja $Q = O_q(M)$.

(v) Como $Q \trianglelefteq M$ e $L \trianglelefteq G$,

$$QL \trianglelefteq ML = G,$$

por (ii) e pelo Lema 2.1.11. Também, por (ii), $Q \cap L = \{1\}$, e, então,

$$|QL| = |Q| \cdot |L|.$$

Dado que $Q \neq \{1\}$ e $L = O_p(G)$, segue-se que $q \neq p$. De fato, se $q = p$, então QL seria um p-subgrupo normal de G de forma que $QL \leq L$ e $Q \leq L$, o que implicaria $Q \cap L = Q \neq \{1\}$, um absurdo. Portanto $q \neq p$, e, então, Q é um q-subgrupo de Sylow de QL.

Agora, $1 < Q \trianglelefteq M$ e, como $M_G = \{1\}$, $Q \not\trianglelefteq G$. Pela maximalidade de M, obtemos que

$$N_G(Q) = M.$$

Consequentemente,

$$N_{QL}(Q) = (QL) \cap N_G(Q) = (QL) \cap M = Q(L \cap M) = Q,$$

pela Lei Modular de Dedekind e (ii). Portanto,

$$|L| = [QL : Q] = [QL : N_{QL}(Q)] \equiv 1 \mod q,$$

pelo Teorema de Sylow; ou seja,

$$p^n \equiv 1 \mod q.$$

(vi) Seja M^* um complemento qualquer para L em G, e seja $Q^* = O_q(M^*)$. A projeção canônica $\pi : G \to G/L$ leva Q em QL/L e Q^* em Q^*L/L. Como, por (ii), M é um complemento para L em G, a restrição de π a M é um isomorfismo de M em G/L. Portanto, π leva $Q = O_q(M)$ em $O_q(G/L)$. De modo análogo, π leva Q^* em $O_q(G/L)$. Assim,

$$QL/L = O_q(G/L) = Q^*L/L$$

donde

$$QL = Q^*L.$$

Por (v), $q \neq p$, logo Q e Q^* são q-subgrupos de Sylow de QL. Desse modo, pelo Teorema de Sylow, existe $x \in QL$ tal que

$$Q^* = Q^x.$$

Como mostrado em (v), $M = N_G(Q)$, e uma vez que $Q^* \trianglelefteq M^*$, temos

$$M^* \leq N_G(Q^*) = N_G(Q^x) = M^x,$$

pelo Lema 2.1.12. Como M e M^* são complementos para L em G,

$$|M^*| = |G/L| = |M| = |M^x|.$$

Portanto,

$$M^* = M^x.$$

□

Observação 2.1.15. *Seja G um grupo solúvel finito não trivial com um subgrupo maximal M tal que $M_G = \{1\}$. Como visto anteriormente, existe um primo p tal que $O_p(G) \neq \{1\}$. Logo as afirmações $(i) - (iv)$ do Teorema 2.1.14 são válidas.*

Agora, $|G| = p$ se, e somente se, $M = \{1\}$. De fato, se $|G| = p$, então, pelo Teorema de Lagrange, $|M| \in \{1, p\}$, mas sendo $M < G$, segue-se que $M = \{1\}$. Reciprocamente, se $M = \{1\}$, então G não possui subgrupos próprios não triviais, logo $|G|$ é um número primo. Dado que p divide $|G|$, concluímos que $|G| = p$.

Ou seja, a menos que $|G| = p$, temos que $M \neq \{1\}$. Como G é solúvel, segue-se que M também o é e existe um primo q tal que $O_q(M) \neq \{1\}$ de modo que as afirmações (v) e (vi) do Teorema 2.1.14 também são válidas.

Em resumo, se G é um grupo solúvel primitivo, então todos os complementos do socle de G são conjugados.

Finalizamos esta seção com um fato a respeito da quantidade de subgrupos normais minimais de um grupo primitivo.

Proposição 2.1.16 (Baer)**.** *Um grupo primitivo G admite no máximo dois subgrupos normais minimais.*

Demonstração. Seja N um subgrupo normal minimal de G, e seja M um subgrupo maximal de G tal que $M_G = \{1\}$. Se $C_G(N)$ é trivial, então N é o único subgrupo normal minimal de G. Assim, assumamos que $C_G(N) \neq \{1\}$; logo, existe $L \leq C_G(N)$ um subgrupo normal minimal de G. Com argumentos análogos aos das demonstrações dos itens (ii) e (iv) do Teorema 2.1.14, obtemos que $G = ML$ e $C_G(N) = L$, ou seja, $C_G(N)$ é normal minimal em G. Suponhamos que existam $A \neq B$ normais minimais de G distintos de N. Pela Proposição 1.3.2, temos que $A, B \leq C_G(N)$ de modo que $A = C_G(N) = B$, um absurdo. Portanto, G admite no máximo dois subgrupos normais minimais. □

2.2 A Função $d(G)$

O objetivo desta seção é introduzir a função $d(G)$ para um grupo finito G, bem como apresentar três resultados que serão necessários para a teoria das próximas seções, especialmente para a demonstração do Teorema A. Aqui, todos os grupos são finitos. Esta seção é baseada nos artigos *Zu einem von BH und H. Neumann gestellten Problem* [14] (de W. Gaschütz) e *Generators and minimal normal subgroups* [18] (de A. Lucchini).

Definição 2.2.1. *Sejam G um grupo e $\mathscr{F} = \{X \subseteq G \mid \langle X \rangle = G\}$. Definimos $d(G) = \min\{|X| \mid X \in \mathscr{F}\}$, ou seja, a menor das cardinalidades dos conjuntos geradores de G.*

A função $d(G)$ está bem definida, na medida em que $\{|X| \mid X \in \mathscr{F}\} \subseteq \mathbb{N}$ é não vazio ($G = \langle G \rangle$). Como uma consequência imediata da definição, temos que um grupo G é cíclico e não trivial se, e somente se, $d(G) = 1$. Notemos que $d(\{1\}) = 0$, haja vista que o grupo trivial é gerado pelo conjunto vazio. Observamos que todo grupo simples G pode ser gerado por 2 elementos, ou seja, $d(G) \leq 2$. Isto foi provado para certos grupos simples em 1962, por Robert Steinberg [25]. Mais tarde, em 1984, Aschbacher e Guralnick [1] completaram a prova para os grupos simples restantes.

Para $n \geq 3$, temos $d(S_n) = 2$, pois $S_n = \langle (12), (12 \cdots n) \rangle$ é um grupo não cíclico. Em geral, não é válido que $d(H) \leq d(G)$ para $H \leq G$: o Teorema de Cayley nos fornece que todo grupo G pode ser visto como um subgrupo de S_n (com $n = |G|$), mas $d(G)$ não precisa ser menor ou igual a 2. Mesmo que H seja um subgrupo normal de G, não temos a validade dessa afirmação. De fato, basta tomar o subgrupo normal $H = S^n \times \{1\}$ do grupo $G = S \wr C_n$, visto nos Exemplos 2.1.5 e 2.1.7. Como veremos mais adiante,

$$d(G) \leq \max\{2, d(G/H) + 1\} = \max\{2, d(C_n) + 1\} = 2,$$

e a sequência $d(S), \ldots, d(S^n), \ldots$ é não decrescente e ilimitada.

Se N é um subgrupo normal de um grupo G, então

$$d(G/N) \leq d(G) \leq d(N) + d(G/N).$$

A primeira desigualdade segue da Proposição 1.1.3 aplicada à projeção canônica $\pi : G \to G/N$, ou seja,

$$G = \langle x_1, \ldots, x_k \rangle \Rightarrow G/N = \langle Nx_1, \ldots, Nx_k \rangle.$$

E como observado logo após a demonstração desta proposição,

$$G/N = \langle Nx_1, \ldots, Nx_k \rangle \Rightarrow G = \langle x_1, \ldots, x_k, N \rangle.$$

Portanto, a segunda desigualdade segue.

Uma outra consequência da Proposição 1.1.3 é que se $G \cong H$ são dois grupos, então $d(G) = d(H)$.

Agora, temos a seguinte questão: dado um número natural n, é possível obter um grupo G com $d(G) = n$? A resposta é sim, como veremos no próximo exemplo. Para este, lembremos que dado um conjunto finito de geradores de V (onde V é um espaço vetorial de dimensão finita sobre um corpo F), podemos extrair uma base.

Exemplo 2.2.2. *Seja p um número primo. Então, $d(C_p^n) = n$. Para ver isto, primeiro observamos que $C_p^n \cong \mathbb{Z}_p^n = (\mathbb{Z}_p^n, +)$, este último sendo um grupo abeliano elementar. Sabemos que $\mathbb{Z}_p^n$ é um espaço vetorial de dimensão n sobre o corpo $\mathbb{Z}_p$, basta definir a soma de dois vetores como a soma de dois elementos do grupo $\mathbb{Z}_p^n$ e o produto escalar $\bar{r}v$ como sendo rv (ver Proposição 1.3.6). Agora, seja $X \subseteq \mathbb{Z}_p^n$. Então, X gera $\mathbb{Z}_p^n$ como um grupo se, e somente se, X gera $\mathbb{Z}_p^n$ como um espaço vetorial. De fato, se $X = \{v_1, \ldots, v_l\}$ gera $\mathbb{Z}_p^n$ como um espaço vetorial, então dado $g \in \mathbb{Z}_p^n$, existem $\overline{\alpha_1}, \ldots, \overline{\alpha_l} \in \mathbb{Z}_p$ tais que*

$$\begin{aligned} g &= \overline{\alpha_1}v_1 + \cdots + \overline{\alpha_l}v_l = \alpha_1 v_1 + \cdots + \alpha_l v_l \\ &= v_1 + \cdots + v_1 + \cdots + v_l + \cdots + v_l. \end{aligned}$$

Portanto, g pertence ao grupo gerado por X, ou seja, X gera $\mathbb{Z}_p^n$ como um grupo. A recíproca é similar, observando que um elemento do grupo gerado por X é da forma

$$\epsilon_1 x_1 + \cdots + \epsilon_m x_m,$$

com $\epsilon_i = \pm 1$, $x_i \in X$ *e* $m \in \mathbb{N}$. *Desse modo,* g *é uma combinação linear dos vetores de* X. *Portanto,*

$$d(C_p^n) = d(\mathbb{Z}_p^n) = \dim_{\mathbb{Z}_p} \mathbb{Z}_p^n = n.$$

Exemplo 2.2.3. *Dado um grupo* G, *temos que*

$$d(G) = d(G/\Phi(G)).$$

De fato, sabemos que $d(G/\Phi(G)) \leq d(G)$. *Agora, sejam* $F = \Phi(G)$ *e* $d = d(G/F)$. *Escolhendo geradores* $Fx_1, \ldots, Fx_d$ *para o grupo* G/F, *temos que*

$$G = \langle x_1, \ldots, x_d, F\rangle = \langle x_1, \ldots, x_d\rangle F = \langle x_1, \ldots, x_d\rangle,$$

pelo Lema 1.5.3. Portanto, $d(G) \leq d$, *e a igualdade segue. Recordamos que se* G *é um p-grupo, então* G/F *pode ser visto de maneira natural como um espaço vetorial de dimensão finita sobre* $\mathbb{Z}_p$. *Desse modo, pelo exemplo 2.2.2,*

$$d(G) = d(G/F) = \dim_{\mathbb{Z}_p} G/F.$$

Enunciaremos e provaremos agora um resultado muito importante que nos auxiliará na demonstração do Teorema A, como também nas demonstrações de outros resultados posteriores. Mas antes, precisaremos do seguinte lema:

Lema 2.2.4. *Sejam* G *um grupo e* $H, N \leq G$. *Se* $x \in G$, *então* $Nx \cap H = \varnothing$ *ou* $Nx \cap H = (N \cap H)t$ *para algum* $t \in Nx \cap H$. *Ademais, se* $Nx \cap H \neq \varnothing$, *então* $Nx \cap H = (N \cap H)t$ *para todo* $t \in Nx \cap H$.

Demonstração. Suponhamos que $Nx \cap H \neq \varnothing$, logo existe $t \in Nx \cap H$. Desse modo, $t = nx \in H$ para algum $n \in N$. Seja $l \in N \cap H$, então $lt \in H$ (pois $l, t \in H$) e $lt = (ln)x \in Nx$, portanto $lt \in Nx \cap H$. Isto nos dá que $(N \cap H)t \subseteq Nx \cap H$. Por outro lado, se $g \in Nx \cap H$, então $g = mx \in H$ para algum $m \in N$. Daí,

$$g = mxt^{-1}t = mx(nx)^{-1}t = mxx^{-1}n^{-1}t = (mn^{-1})t.$$

Temos que $mn^{-1} \in N$ e $mn^{-1} = gt^{-1} \in H$, consequentemente $g \in (N \cap H)t$. Portanto, $Nx \cap H \subseteq (N \cap H)t$, e o lema segue. □

Teorema 2.2.5 (Gaschütz, [14], Teorema 1)**.** *Seja* N *um subgrupo normal de um grupo* G *e sejam* $g_1, \ldots, g_m \in G$ *tais que* $G = \langle g_1, \ldots, g_m, N\rangle$. *Se* $d(G) \leq m$, *então existem elementos*

$u_1, \ldots, u_m$ de N tais que $G = \langle u_1 g_1, \ldots, u_m g_m \rangle$. Além disso, a cardinalidade do conjunto

$$A(g_1, \ldots, g_m) = \{(u_1, \ldots, u_m) \in N^m \mid G = \langle u_1 g_1, \ldots, u_m g_m \rangle\}$$

é independente da escolha de $g_1, \ldots, g_m$.

A demonstração é baseada na prova do Teorema 1 do artigo [14]. Outras demonstrações podem ser encontradas em [3, Teorema 16.1], [11, Lema 17.7.2] e [21, Proposição 2.5.4].

Demonstração. Se todo subgrupo maximal de G contém N, então $A(g_1, \ldots, g_m) = N^m$. De fato, seja $(u_1, \ldots, u_m) \in N^m$ e suponhamos que $\langle u_1 g_1, \ldots, u_m g_m \rangle \neq G$. Assim, existe um subgrupo maximal M de G tal que $\langle u_1 g_1, \ldots, u_m g_m \rangle \leq M$. Dessa forma, $N \leq M$ de modo que $g_i = u_i^{-1}(u_i g_i) \in M$ para todo $i \in \{1, \ldots, m\}$ e $G = \langle g_1, \ldots, g_m, N \rangle \leq M < G$, um absurdo. Portanto, $(u_1, \ldots, u_m) \in A(g_1, \ldots, g_m)$.

Então, suponhamos que nem todo subgrupo maximal de G contenha N. Para cada $H \leq G$, definamos

$$\varepsilon_H := \begin{cases} 0 & \text{se} \quad NH \neq G, \\ 1 & \text{se} \quad NH = G. \end{cases}$$

Se para cada $i \in \{1, \ldots, m\}$, existe $y_i \in Ng_i \cap H$, então

$$\frac{NH}{N} \geq \langle Ny_1, \ldots, Ny_m \rangle = \langle Ng_1, \ldots, Ng_m \rangle = \frac{G}{N}$$

donde $G \leq NH$ e $\varepsilon_H = 1$. Por outro lado, se $\varepsilon_H = 1$, então por definição $NH = G$. Assim, dado $i \in \{1, \ldots, m\}$, temos $g_i = n_i y_i$, para certos $n_i \in N$ e $y_i \in H$, de modo que $y_i = n_i^{-1} g_i \in Ng_i \cap H$. Ou seja, $\varepsilon_H = 1$ se, e somente se, $Ng_i \cap H \neq \varnothing$, $\forall i \in \{1, \ldots, m\}$. Consequentemente, $\varepsilon_H = 0$ se, e somente se, $Ng_i \cap H = \varnothing$ para algum $i \in \{1, \ldots, m\}$.

Agora, sejam $M_1, \ldots, M_r$ os subgrupos maximais de G que não contêm N (observamos que $r \neq 0$). Também, consideremos o conjunto

$$\{(y_1, \ldots, y_m) \in Ng_1 \times \cdots \times Ng_m \mid \text{É falso que existe } H < G \text{ com } y_1, \ldots, y_m \in H\}.$$

Esta condição é equivalente a $\langle y_1, \ldots, y_m \rangle = G$. De fato, se $\langle y_1, \ldots, y_m \rangle \neq G$, então existe um subgrupo maximal M de G tal que $\langle y_1, \ldots, y_m \rangle \leq M$ de modo que $y_1, \ldots, y_m \in M < G$. Reciprocamente, se existe $H < G$ com $y_1, \ldots, y_m \in H$, então $\langle y_1, \ldots, y_m \rangle \leq H < G$, o que implica $\langle y_1, \ldots, y_m \rangle \neq G$.

Sendo Φ_N a cardinalidade do conjunto acima, afirmamos que

$$\Phi_N = |N|^m + \sum_{k=1}^{r} \sum_{1 \leq j_1 < \cdots < j_k \leq r} (-1)^k |N \cap M_{j_1} \cap \cdots \cap M_{j_k}|^m \cdot \varepsilon_{M_{j_1} \cap \cdots \cap M_{j_k}}.$$

Com efeito, para cada $j \in \{1, \ldots, r\}$, definamos

$$X_j = (M_j \cap Ng_1) \times \cdots \times (M_j \cap Ng_m).$$

Seja $(y_1, \ldots, y_m)$ uma m-upla pertencente a $Ng_1 \times \cdots \times Ng_m$ tal que existe $H < G$ com $y_1, \ldots, y_m \in H$. Então $Ng_i \cap H$ é não vazio para todo $i \in \{1, \ldots, m\}$ de sorte que $\varepsilon_H = 1$ e $G = NH$; sendo $H < G$, existe um subgrupo maximal M de G tal que $H \leq M$. Desse modo, $N \nsubseteq M$, pois, caso contrário, $G = NH \leq M < G$. Isto é, $M = M_j$ para algum $j \in \{1, \ldots, r\}$ donde $(y_1, \ldots, y_m) \in X_j \subseteq X_1 \cup \cdots \cup X_r$. Por outro lado, se $(y_1, \ldots, y_m) \in X_1 \cup \cdots \cup X_r$, então existe $j \in \{1, \ldots, r\}$ tal que $(y_1, \ldots, y_m) \in X_j$. Assim, $(y_1, \ldots, y_m)$ é uma m-upla tal que $y_i \in Ng_i$ para todo i e existe $H < G$ com $y_1, \ldots, y_m \in H$ (nesse caso, $H = M_j$). Portanto,

$$\Phi_N = |N|^m - |X_1 \cup \cdots \cup X_r|.$$

Usando o Princípio da Inclusão-Exclusão, obtemos que

$$\left| \bigcup_{j=1}^{r} X_j \right| = \sum_{k=1}^{r} \sum_{1 \leq j_1 < \cdots < j_k \leq r} (-1)^{k+1} |X_{j_1} \cap \cdots \cap X_{j_k}|.$$

Notemos que

$$X_{j_1} \cap \cdots \cap X_{j_k} = (Ng_1 \cap M_{j_1} \cap \cdots \cap M_{j_k}) \times \cdots \times (Ng_m \cap M_{j_1} \cap \cdots \cap M_{j_k}).$$

Como vimos acima, $\varepsilon_{M_{j_1} \cap \cdots \cap M_{j_k}} = 1$ se, e somente se, $Ng_i \cap M_{j_1} \cap \cdots \cap M_{j_k} \neq \varnothing$ para todo $i \in \{1, \ldots, m\}$. Pelo Lema 2.2.4, temos

$$|Ng_i \cap M_{j_1} \cap \cdots \cap M_{j_k}| = |N \cap M_{j_1} \cap \cdots \cap M_{j_k}|$$

quando este conjunto é não vazio, logo

$$|X_{j_1} \cap \cdots \cap X_{j_k}| = |N \cap M_{j_1} \cap \cdots \cap M_{j_k}|^m \cdot \varepsilon_{M_{j_1} \cap \cdots \cap M_{j_k}},$$

e a afirmação segue.

Com isso, mostramos o interessante fato que Φ_N não depende de $g_1, \ldots, g_m$. A fim de garantir a existência de elementos $u_1, \ldots, u_m$ de N tais que $G = \langle u_1 g_1, \ldots, u_m g_m \rangle$, precisamos provar que $\Phi_N \neq 0$. Ora, por hipótese, $d(G) \leq m$, logo existem $l_1, \ldots, l_m \in G$ tais que $\langle l_1, \ldots, l_m \rangle = G$ de modo que $G = \langle l_1, \ldots, l_m, N \rangle$. Assim, como Φ_N não depende de $g_1, \ldots, g_m$, podemos escolher $l_1, \ldots, l_m$ para fazerem o papel de $g_1, \ldots, g_m$ acima, isto é, existem Φ_N m-uplas $(y_1, \ldots, y_m) \in Nl_1 \times \cdots \times Nl_m$ tais que $\langle y_1, \ldots, y_m \rangle = G$. Uma vez que $\langle l_1, \ldots, l_m \rangle = G$, segue-se que $\Phi_N \neq 0$, como queríamos.

Por fim, a aplicação $(u_1, \ldots, u_m) \mapsto (u_1 g_1, \ldots, u_m g_m)$ é uma bijeção entre os conjuntos $A(g_1, \ldots, g_m)$ e $\{(y_1, \ldots, y_m) \in Ng_1 \times \cdots \times Ng_m \mid \langle y_1, \ldots, y_m \rangle = G\}$, ou seja, a cardinalidade do conjunto $A(g_1, \ldots, g_m)$ independe da escolha de $g_1, \ldots, g_m$. Isto completa a prova do teorema. □

Dado um grupo simples não abeliano S, podemos identificá-lo com o subgrupo dos automorfismos internos $\mathrm{Inn}(S)$ de $\mathrm{Aut}(S)$, pois temos que $Z(S) = \{1\}$, e é conhecido da teoria básica de grupos que $S/Z(S) \cong \mathrm{Inn}(S)$. Isto é, cada elemento $s \in S$ é identificado com o automorfismo interno $\mathscr{I}_s : x \mapsto x^s$. O seguinte resultado pode ser encontrado no artigo *Generation of almost simple groups* [9] de Francesca Dalla Volta e Andrea Lucchini.

Teorema 2.2.6. *Seja S um grupo simples não abeliano e identifiquemos S com o subgrupo normal $\mathrm{Inn}(S)$ de $\mathrm{Aut}(S)$. Então, para todo par x, y de elementos de $\mathrm{Aut}(S)$, o subgrupo $\langle x, y, S \rangle$ de $\mathrm{Aut}(S)$ pode ser gerado por dois elementos.*

Observação 2.2.7. *Pelo Teorema 2.2.5, a afirmação do Teorema 2.2.6 pode ser reformulada da seguinte maneira: para todos $x, y \in \mathrm{Aut}(S)$, existem $u, v \in S$ tais que $\langle x, y, S \rangle = \langle ux, vy \rangle$.*

Como visto acima, temos $d(G) \leq d(N) + d(G/N)$ para um subgrupo normal N de um grupo G. Agora, vamos comparar $d(G)$ com $d(G/N)$ quando N é um subgrupo normal minimal de G, a fim de estabelecer uma cota melhor para $d(G)$.

Teorema 2.2.8 (Lucchini, [18], Teorema 1.3)**.** *Se N é um subgrupo normal minimal de um grupo G, então*

$$d(G) \leq \max\{2, d(G/N) + 1\}.$$

Demonstração. Se $G = N$, então G é simples e $d(G) \leq 2$. Além disso, o teorema pode ser provado diretamente se N é abeliano: neste caso, se $g_1, \ldots, g_d$ são geradores para G módulo N, então para todo $x \in N$, $x \neq 1$, temos $G = \langle g_1, \ldots, g_d, x \rangle$. Com efeito, dado $x \in N$, $x \neq 1$, sejam $H = \langle g_1, \ldots, g_d, x \rangle$ e $K = \langle x^g \mid g \in \langle g_1, \ldots, g_d \rangle \rangle \leq N$.

Vamos mostrar que $K \trianglelefteq G$. Dados $g \in \langle g_1, \ldots, g_d \rangle$ e $t \in G$, temos que $t = t_1 \cdots t_k$ com $t_i \in \{g_1^{\pm 1}, \ldots, g_d^{\pm 1}\} \cup N$. Daí,

$$(x^g)^t = (x^g)^{t_1 \cdots t_k} = (\cdots((x^g)^{t_1})\cdots)^{t_k} = x^{gt_{i_1}\cdots t_{i_r}},$$

sendo $t_{i_1}, \ldots, t_{i_r}$ os elementos dentre $t_1, \ldots, t_n$ que não estão em N, haja vista que $N \trianglelefteq G$ e N é abeliano. Assim, $gt_{i_1} \cdots t_{i_r} \in \langle g_1, \ldots, g_d \rangle$ e $(x^g)^t \in K$ donde se segue que $K \trianglelefteq G$. Dado que $1 \neq x \in K$ e N é normal minimal em G, obtemos $K = N$. Dessa forma, H contém N (pois contém os conjugados de x em $\langle g_1, \ldots, g_d \rangle$) de sorte que $H \geq \langle g_1, \ldots, g_d, N \rangle = G$ e $H = G$. Portanto, $d(G) \leq d(G/N) + 1$.

Então, vamos assumir $N \neq G$ e N não abeliano.

Por indução na ordem de G, reduzimos ao caso: N é o único normal minimal em G. De fato, suponhamos que M é um subgrupo normal minimal de G com $M \neq N$ e seja $d = d(G/N)$. Existem $g_1, \ldots, g_d \in G$ tais que $G = \langle g_1, \ldots, g_d, N \rangle$. Agora, pela Proposição 1.7.3, $NM/M \cong_G N$ é um subgrupo normal minimal de G/M, logo por indução

$$d\left(\frac{G}{M}\right) \leq \max\left\{d\left(\frac{G/M}{NM/M}\right) + 1, 2\right\} = \max\left\{d\left(\frac{G}{NM}\right) + 1, 2\right\} =$$

$$\max\left\{d\left(\frac{G/N}{NM/N}\right) + 1, 2\right\} \leq \max\left\{d\left(\frac{G}{N}\right) + 1, 2\right\} \leq d\left(\frac{G}{N}\right) + 1 = d + 1,$$

onde a última desigualdade vale pois $N \neq G$. Afirmamos que existem elementos $x_1, \ldots, x_d, x_{d+1} \in N$ tais que $x_{d+1} \neq 1$ e $\langle Mx_1g_1, \ldots, Mx_dg_d, Mx_{d+1} \rangle = G/M$. De fato, temos $G = \langle g_1, \ldots, g_d, N \rangle$, logo $G = \langle g_1, \ldots, g_d, NM \rangle$ e $G/M = \langle Mg_1, \ldots, Mg_d, NM/M \rangle$. Se $d(G/M) \leq d$, então, pelo Teorema 2.2.5, existem $x_1, \ldots, x_d \in N$ tais que $\langle Mx_1g_1, \ldots, Mx_dg_d \rangle = G/M$. Assim, tomando $x_{d+1} \neq 1$ em N ($N \neq \{1\}$), obtemos que $\langle Mx_1g_1, \ldots, Mx_dg_d, Mx_{d+1} \rangle = G/M$. Agora, assumamos que $d(G/M) = d + 1$. Haja vista que $G/M = \langle Mg_1, \ldots, Mg_d, NM/M \rangle$, temos que $G/M = \langle Mg_1, \ldots, Mg_d, M, NM/M \rangle$. Aplicando o Teorema 2.2.5, existem $x_1, \ldots, x_d, x_{d+1} \in N$ tais que $\langle Mx_1g_1, \ldots, Mx_dg_d, Mx_{d+1} \rangle = G/M$. Neste caso, $x_{d+1} \neq 1$, já que $d(G/M) = d + 1$. Portanto, a afirmação segue. Agora, consideremos o subgrupo $L = \langle x_1g_1, \ldots, x_dg_d, x_{d+1} \rangle$. Como $\langle Mx_1g_1, \ldots, Mx_dg_d, Mx_{d+1} \rangle = G/M$, temos que $G = \langle x_1g_1, \ldots, x_dg_d, x_{d+1}, M \rangle$ de modo que $LM = G$. Por outro lado, $G = \langle g_1, \ldots, g_d, N \rangle$ donde $LN = G$. Além disso, $L \cap N \trianglelefteq L$ (pois $N \trianglelefteq G$) e é centralizado por M ($M \leq C_G(N) \leq C_G(L \cap N)$ – vide Proposição 1.3.2), logo $L \cap N \trianglelefteq LM = G$. Dado que N é normal minimal em G e $L \cap N \neq \{1\}$ (contém x_{d+1}), deduzimos que

$L \cap N = N$; mas então, $G = LN = L$ e $d(G) = d(L) \leq d + 1 = d(G/N) + 1$.

Então, para concluir nossa demonstração, temos apenas que considerar o caso: N é o único subgrupo normal minimal de G. Pelo Corolário 1.3.13,

$$N = S^n,$$

o produto direto de n cópias de um grupo simples não abeliano. Além disso, considerando a ação por conjugação de G em N, temos que o núcleo desta é o centralizador $C_G(N)$, o qual é trivial, pois, caso contrário, conteria o subgrupo normal minimal N donde este seria abeliano, um absurdo. Isto é, temos $S^n \trianglelefteq G \leq \mathrm{Aut}(S^n)$. Pelo Teorema 1.6.15,

$$\mathrm{Aut}(S^n) = \mathrm{Aut}(S) \wr S_n,$$

o produto entrelaçado entre $\mathrm{Aut}(S)$ e o grupo simétrico de grau n. Logo, os elementos de G são da forma $((h_1, \ldots, h_n), \sigma)$, com $h_i \in \mathrm{Aut}(S)$ e $\sigma \in S_n$. Para cada i, $1 \leq i \leq n$, seja

$$S_i = \{1\} \times \cdots \times \{1\} \times S \times \{1\} \times \cdots \times \{1\} \quad (S \text{ na } i\text{-ésima entrada}),$$

ou seja, $S_1, \ldots, S_n$ são os fatores diretos de S^n. Sejam $d = d(G/N)$ e $g_1, \ldots, g_d \in G$ tais que $G = \langle g_1, \ldots, g_d, N \rangle$. Daí, $G = NR$ com $R = \langle g_1, \ldots, g_d \rangle$ (pois $N \trianglelefteq G$) de modo que

$$N = S_1^G = S_1^{NR} = (S_1^N)^R = S_1^R = S_1^{\langle g_1, \cdots, g_d \rangle},$$

onde a primeira igualdade vale porque $S_1^G \trianglelefteq G$ e $S_1^G \leq N$, e a quarta porque $S_1 \trianglelefteq N$.

Para concluir nossa demonstração, é suficiente provar:

$(*)$ para todo $g \in \mathrm{Aut}(S^n)$, existem $x, y \in S^n$ tais que $S_1 \leq \langle xg, y \rangle$.

Com efeito, se $(*)$ é verdadeiro, tomemos $g = g_1$ e escolhamos $x, y \in N$ tais que $S_1 \leq \langle xg, y \rangle$. Afirmamos que

$$N = S_1^{\langle g_1, \cdots, g_d \rangle} \leq S_1^{\langle xg_1, \cdots, g_d \rangle}.$$

De fato, seja $u \in \langle g_1, \ldots, g_d \rangle$, logo $u = x_1 \cdots x_r$ com $r \in \mathbb{N}$ e $x_i \in \{g_1^{\pm 1}, \ldots, g_d^{\pm 1}\}$ $(1 \leq i \leq r)$. Agora, notemos que dado $v \in G$, $S_1^v = S_j$ para algum $j \in \{1, \ldots, n\}$, pois $G \leq \mathrm{Aut}(S^n)$ e os normais minimais de S^n são os fatores diretos $S_1, \ldots, S_n$ (vide Proposição 1.6.11). Além disso, dado $k \in \{1, \ldots, n\}$,

$$S_k^{g_1} = (S_k^x)^{g_1} = S_k^{xg_1} \quad \text{e} \quad S_k^{g_1^{-1}} = \left(S_k^{g_1^{-1}}\right)^{x^{-1}} = S_k^{g_1^{-1}x^{-1}} = S_k^{(xg_1)^{-1}},$$

pois $x \in N$ normaliza $S_1, \ldots, S_n$. Portanto,

$$S_1^u = S_1^{x_1 \cdots x_r} = S_1^{x_1' \cdots x_r'}$$

com $x_i' \in \{(xg_1)^{\pm 1}, \ldots, g_d^{\pm 1}\}$, ou seja, $S_1^u \subseteq S_1^{\langle xg_1, \ldots, g_d \rangle}$. Pela arbitrariedade de u, a afirmação segue. Como $S_1 \leq \langle xg_1, y \rangle$, o subgrupo $T = \langle xg_1, g_2, \ldots, g_d, y \rangle$ de G contém

$$S_1^{\langle xg_1, \ldots, g_d \rangle} \geq S_1^{\langle g_1, \ldots, g_d \rangle} = N$$

donde $T = G$ (pois $G = NR$), e, portanto,

$$d(G) = d(T) \leq d + 1.$$

Então, vamos provar $(*)$: seja $g = ((h_1, \ldots, h_n), \sigma) \in \mathrm{Aut}(S^n)$. Vamos dividir em dois casos:

(a) $(1)\sigma = 1$. Considerando os elementos h_1 e id_S de $\mathrm{Aut}(S)$, temos, pelo Teorema 2.2.6 (vide Observação 2.2.7), que existem $x_1, y_1 \in S$ tais que $S \leq \langle x_1 h_1, y_1 \rangle$: em particular, isto implica $S = \langle y_1 \rangle^{\langle x_1 h_1, y_1 \rangle}$. De fato, $\langle y_1 \rangle^S \trianglelefteq S$ e $y_1 \neq 1$ (pois, caso contrário, $S \leq \langle x_1 h_1, y_1 \rangle = \langle x_1 h_1 \rangle$ seria abeliano). Como S é simples, segue-se que $S = \langle y_1 \rangle^S \leq \langle y_1 \rangle^{\langle x_1 h_1, y_1 \rangle}$. Por outro lado, $\langle y_1 \rangle \leq S$ e $S \trianglelefteq \mathrm{Aut}(S)$, logo $\langle y_1 \rangle^{\langle x_1 h_1, y_1 \rangle} \leq S$ donde $S = \langle y_1 \rangle^{\langle x_1 h_1, y_1 \rangle}$. Agora, consideremos os elementos $x, y \in S_1$ assim definidos:

$$x = (x_1, 1, \ldots, 1),\ y = (y_1, 1 \ldots, 1).$$

Dado que $(1)\sigma = 1$, temos que $y^\sigma = y$ e os dois elementos $(x_1 h_1, 1, \ldots, 1)$ e $xg = ((x_1 h_1, h_2, \ldots, h_n), \sigma)$ agem por conjugação em S_1 da mesma maneira:

$$\begin{aligned}(s, 1, \ldots, 1)^{(x_1 h_1, 1, \ldots, 1)} &= (s^{x_1 h_1}, 1, \ldots, 1) = (s^{x_1 h_1}, 1, \ldots, 1)^\sigma \\ &= (s, 1, \ldots, 1)^{((x_1 h_1, h_2, \ldots, h_n), \sigma)} \\ &= (s, 1, \ldots, 1)^{xg},\ \forall s \in S.\end{aligned}$$

Também, dado $s \in S$,

$$\begin{aligned}(s,1,\ldots,1)^{(x_1h_1,1,\ldots,1)^{-1}} &= (s,1,\ldots,1)^{((x_1h_1)^{-1},1,\ldots,1)} = \left(s^{(x_1h_1)^{-1}},1,\ldots,1\right)\\ &= \left((s,1,\ldots,1)^{\sigma^{-1}}\right)^{(x_1h_1,h_2,\ldots,h_n)^{-1}}\\ &= (s,1,\ldots,1)^{((x_1h_1,h_2,\ldots,h_n),\sigma)^{-1}}\\ &= (s,1,\ldots,1)^{(xg)^{-1}}.\end{aligned}$$

Isto nos fornece $\langle y\rangle^{\langle xg,y\rangle} = \langle (y_1,1,\ldots,1)\rangle^{\langle (x_1h_1,1,\ldots,1),(y_1,1,\ldots,1)\rangle}$. Afirmamos que

$$\left\langle (t,1,\ldots,1) \mid t \in \langle y_1\rangle^{\langle x_1h_1,y_1\rangle}\right\rangle \leq \langle (y_1,1,\ldots,1)\rangle^{\langle (x_1h_1,1,\ldots,1),(y_1,1,\ldots,1)\rangle}.$$

De fato, seja $(t,1,\ldots,1)$ tal que $t \in \langle y_1\rangle^{\langle x_1h_1,y_1\rangle}$, então $t = t_1^{\epsilon_1}\cdots t_r^{\epsilon_r}$ com $r \in \mathbb{N}$ e para cada $i \in \{1,\ldots,r\}$, $\epsilon_i = \pm 1$ e $t_i = (y_1^{m_i})^{z_i}$ com $m_i \in \mathbb{Z}$ e $z_i \in \langle x_1h_1, y_1\rangle$. Agora, notemos que

$$(t,1,\ldots,1) = (t_1^{\epsilon_1}\cdots t_r^{\epsilon_r},1,\ldots,1) = (t_1,1,\ldots,1)^{\epsilon_1}\cdots(t_r,1,\ldots,1)^{\epsilon_r},$$

logo é suficiente mostrar que cada $(t_i,1,\ldots,1)$ pertence a $\langle (y_1,1,\ldots,1)\rangle^{\langle (x_1h_1,1,\ldots,1),(y_1,1,\ldots,1)\rangle}$. Temos $t_i = (y_1^{m_i})^{z_i}$ com $m_i \in \mathbb{Z}$ e $z_i \in \langle x_1h_1, y_1\rangle$. Assim, $z_i = u_1\cdots u_s$ com $s \in \mathbb{N}$ e $u_j \in \{(x_1h_1)^{\pm 1}, y_1^{\pm 1}\}$ $(1 \leq j \leq s)$. Como $(s,1,\ldots,1)^{(x_1h_1,1,\ldots,1)^{\pm 1}} = (s^{(x_1h_1)^{\pm 1}},1,\ldots,1)$ e $(s,1,\ldots,1)^{(y_1,1,\ldots,1)^{\pm 1}} = (s^{y_1^{\pm 1}},1,\ldots,1)$, para todo $s \in S$,

$$\begin{aligned}(t_i,1,\ldots,1) &= ((y_1^{m_i})^{z_i},1,\ldots,1)\\ &= (y_1^{m_i},1,\ldots,1)^{(u_1,1,\ldots,1)\cdots(u_s,1,\ldots,1)}\\ &= ((y_1,1,\ldots,1)^{m_i})^{(u_1,1,\ldots,1)\cdots(u_s,1,\ldots,1)} \in \langle (y_1,1,\ldots,1)\rangle^{\langle (x_1h_1,1,\ldots,1),(y_1,1,\ldots,1)\rangle},\end{aligned}$$

e a afirmação segue. Mas então $\langle xg, y\rangle$ contém

$$\begin{aligned}\langle y\rangle^{\langle xg,y\rangle} &= \langle (y_1,1,\ldots,1)\rangle^{\langle (x_1h_1,1,\ldots,1),(y_1,1,\ldots,1)\rangle}\\ &\geq \left\langle (t,1,\ldots,1) \mid t \in \langle y_1\rangle^{\langle x_1h_1,y_1\rangle}\right\rangle = \langle (t,1,\ldots,1) \mid t \in S\rangle = S_1.\end{aligned}$$

(b) $(1)\sigma \neq 1$. Escrevamos $\sigma = \sigma_1\cdots\sigma_t$ como um produto de ciclos disjuntos e seja $\sigma_1 = (1,n_2,\ldots,n_r)$ o ciclo contendo 1. Além disso, seja $h = h_1h_{n_2}\cdots h_{n_r} \in \mathrm{Aut}(S)$. Novamente, pelo Teorema 2.2.6, existem $x_1, y_1 \in S$ tais que $S \leq \langle x_1h, y_1\rangle$ e $S = \langle y_1\rangle^{\langle x_1h,y_1\rangle}$. Definamos

$$x = (x_1,1,\ldots,1),\ y = (y_1,1\ldots,1).$$

Dado $i \in \{1,\dots,r-1\}$, temos que $(x_1h_1,h_2,\dots,h_n)^{(\sigma^i)^{-1}} = (h_{n_{i+1}},\dots)$, pois sendo $t_1 = x_1h_1$ e $t_j = h_j$ para todo $j \in \{2,\dots,n\}$, temos $t_{1\sigma^i} = t_{n_{i+1}} = h_{n_{i+1}}$. Com isso, obtemos que

$$\begin{aligned}\bar{g} := (xg)^r &= (xg)(xg)\cdots(xg) = ((x_1h_1h_{n_2},\dots),\sigma^2)(xg)\cdots(xg)\\ &= ((x_1h_1h_{n_2}h_{n_3},\dots),\sigma^3)(xg)\cdots(xg)\\ &= \cdots\\ &= ((x_1h_1h_{n_2}\cdots h_{n_r},\dots),\sigma^r)\\ &= ((x_1h,\dots),\sigma^r).\end{aligned}$$

Agora, $(1)\sigma^r = 1$ de modo que $\bar{g}$ e $(x_1h,1,\dots,1)$ agem por conjugação em S_1 da mesma maneira. Como no caso anterior, obtemos

$$S_1 \leq \langle (y_1,1,\dots,1)\rangle^{\langle (x_1h,1,\dots,1),(y_1,1,\dots,1)\rangle} = \langle y\rangle^{\langle \bar{g},y\rangle} \leq \langle \bar{g},y\rangle \leq \langle xg,y\rangle.$$

Isto completa a prova de $(*)$, e, então, o teorema segue. □

Para um grupo monolítico não cíclico, conseguimos uma igualdade. Mais precisamente, temos o:

Teorema 2.2.9. *Se um grupo não cíclico G contém um único subgrupo normal minimal M, então $d(G) = \max\{2, d(G/M)\}$.*

Esse resultado é uma generalização do fato de que todo grupo simples é 2-gerado. Usá-lo-emos nas demonstrações dos Teoremas A e C. Observamos que a prova do Teorema 2.2.9 é feita por uma redução aos grupos simples, de modo a usar a classificação dos grupos simples finitos.

O caso M abeliano foi considerado no artigo *Some applications of the first cohomology group* [1] de Michael Aschbacher e Robert Guralnick. Para M não abeliano, isto foi provado no artigo *Generators for finite groups with a unique minimal normal subgroup* [20], por Andrea Lucchini e Federico Menegazzo.

2.3 Grupos Crown-Based Power

Esta e a próxima seção são baseadas em [8].

Seja L um grupo primitivo monolítico não cíclico finito, com $M = \mathrm{soc}(L)$. Em toda esta seção, L sempre denotará um tal grupo. Observamos que se M é abeliano, então este é complementado em L, pela Proposição 1.5.11 (uma vez que $\Phi(L) = \{1\}$).

Para cada inteiro positivo k, definimos o *subgrupo crown-based power* L_k do produto direto L^k por

$$L_k = \{(l_1, \ldots, l_k) \in L^k \mid l_1 \equiv \cdots \equiv l_k \mod M\}.$$

Vamos verificar que L_k é, de fato, um subgrupo de L^k. Claramente, $(1, \ldots, 1) \in L_k$, logo $L_k \neq \varnothing$. Sejam $(l_1, \ldots, l_k), (r_1, \ldots, r_k) \in L_k$ arbitrários. Então

$$l_1 \equiv \cdots \equiv l_k \mod M \qquad \text{e} \qquad r_1 \equiv \cdots \equiv r_k \mod M,$$

ou seja,

$$Ml_1 = \cdots = Ml_k \qquad \text{e} \qquad Mr_1 = \cdots = Mr_k.$$

Desse modo, obtemos

$$Ml_1r_1 = \cdots = Ml_kr_k \qquad \text{e} \qquad Ml_1^{-1} = \cdots = Ml_k^{-1},$$

isto é,

$$l_1r_1 \equiv \cdots \equiv l_kr_k \mod M \qquad \text{e} \qquad l_1^{-1} \equiv \cdots \equiv l_k^{-1} \mod M.$$

Isto nos fornece que $(l_1, \ldots, l_k) \cdot (r_1, \ldots, r_k)$ e $(l_1, \ldots, l_k)^{-1}$ pertencem a L_k. Portanto, $L_k \leq L^k$.

Observação 2.3.1. *Temos $L_k = M^k \cdot \mathrm{diag}(L^k)$. De fato, sejam $(m_1, \ldots, m_k) \in M^k$ e $(l, \ldots, l) \in \mathrm{diag}(L^k)$. Então, para todos $i, j \in \{1, \ldots, k\}$, temos $m_il \equiv m_jl \mod M$, pois $Mm_il = Ml = Mm_jl$. Consequentemente,*

$$(m_1, \ldots, m_k) \cdot (l, \ldots, l) = (m_1l, \ldots, m_kl) \in L_k.$$

Portanto, $M^k \cdot \mathrm{diag}(L^k) \subseteq L_k$. Reciprocamente, seja $(l_1, \ldots, l_k) \in L_k$, logo $l_1 \equiv \cdots \equiv l_k \mod M$. Daí, $Ml_1 = \cdots = Ml_k$ donde, para cada $i \in \{1, \ldots, k\}$, existe $m_i \in M$ tal que $l_i = m_il_1$, sendo $m_1 = 1$. Desse modo, obtemos que

$$(l_1, \ldots, l_k) = (m_1l_1, \ldots, m_kl_1) = (m_1, \ldots, m_k) \cdot (l_1, \ldots, l_1) \in M^k \cdot \mathrm{diag}(L^k).$$

Por conseguinte, $L_k \subseteq M^k \cdot \mathrm{diag}(L^k)$, e, portanto, $L_k = M^k \cdot \mathrm{diag}(L^k)$.

Vamos agora mostrar algumas propriedades desses subgrupos.

Proposição 2.3.2. *O socle de L_k é M^k, um produto direto de k subgrupos normais minimais (cada um isomorfo a M), e $L_k/M^k \cong L/M$.*

Demonstração. Primeiro, vamos mostrar que $L_k/M^k \cong L/M$. Para isto, definamos a aplicação $\gamma : L_k \to L/M$ por

$$(l_1, \ldots, l_k)^\gamma = Ml_1, \qquad \text{sempre que} \quad (l_1, \ldots, l_k) \in L_k.$$

Temos que, de fato, γ está bem definida, pois se $(l_1, \ldots, l_k) = (r_1, \ldots, r_k)$, então $l_1 = r_1$ de modo que $Ml_1 = Mr_1$ e $(l_1, \ldots, l_k)^\gamma = (r_1, \ldots, r_k)^\gamma$. Dado $Mr \in L/M$, temos $Mr = (r, \ldots, r)^\gamma$, com $(r, \ldots, r) \in \mathrm{diag}(L^k) \subseteq L_k$. Isto mostra que γ é sobrejetiva.

Agora, sejam $(l_1, \ldots, l_k), (r_1, \ldots, r_k) \in L_k$. Daí,

$$\begin{aligned}((l_1, \ldots, l_k) \cdot (r_1, \ldots, r_k))^\gamma &= (l_1 r_1, \ldots, l_k r_k)^\gamma = Ml_1 r_1 = (Ml_1)(Mr_1) \\ &= (l_1, \ldots, l_k)^\gamma (r_1, \ldots, r_k)^\gamma.\end{aligned}$$

Assim, γ é um homomorfismo. Vamos então calcular o $\ker(\gamma)$. Para isto, seja $(l_1, \ldots, l_k) \in \ker(\gamma)$. Temos $(l_1, \ldots, l_k) \in L_k$ e $Ml_1 = M$. Isto implica $M = Ml_1 = \cdots = Ml_k$ donde $l_1, \ldots, l_k \in M$, e, portanto, $(l_1, \ldots, l_k) \in M^k$. Por outro lado, dado $(m_1, \ldots, m_k) \in M^k$, temos $Mm_1 = \cdots = Mm_k = M$, logo $(m_1, \ldots, m_k) \in \ker(\gamma)$. Dessa forma, concluímos que $\ker(\gamma) = M^k$, em particular, $M^k \trianglelefteq L_k$. Portanto, pelo Teorema dos Isomorfismos, $L_k/M^k \cong L/M$.

Agora, vamos mostrar que $\mathrm{soc}(L_k) = M^k$. Com efeito, para cada i, $1 \leq i \leq k$, seja

$$M_i = \{1\} \times \cdots \times \{1\} \times M \times \{1\} \times \cdots \times \{1\},$$

onde M está na i-ésima entrada. Claramente, $M_i \cong M$, e como $M \trianglelefteq L$, obtemos que $M_i \trianglelefteq L^k$ donde $M_i \trianglelefteq L_k$, pois $M_i \leq L_k$ ($M_i \leq M^k \leq L_k$). Afirmamos que cada M_i é um subgrupo normal minimal de L_k. De fato, seja N um subgrupo normal não trivial de L_k contido em M_i. Assim, existe $(1, \ldots, m, \ldots, 1) \in N$ com $m \neq 1$. Dado $l \in L$, temos que $(l, \ldots, l) \in L_k$; logo, pela normalidade de N, obtemos que

$$(1, \ldots, m^l, \ldots, 1) = (1, \ldots, m, \ldots, 1)^{(l, \ldots, l)} \in N.$$

Além disso, $\langle m^l \mid l \in L \rangle$ é um subgrupo normal de L contido em M donde é igual a M, já que M é normal minimal em L e $m \neq 1$. Com isso, concluímos que $M_i \leq N$, e, então, $N = M_i$, completando a prova da afirmação. Por conseguinte,

$$\mathrm{soc}(L_k) \geq M_1 \cdots M_k = M^k.$$

Resta mostrar que $\mathrm{soc}(L_k) \leq M^k$. Para isto, vamos primeiro calcular $C_L(M)$. Dado que $M \trianglelefteq L$, temos que $C_L(M) \trianglelefteq L$. Agora, vamos dividir em casos.

Caso 1. M não abeliano: neste caso, $C_L(M) = \{1\}$, pois, caso contrário, $C_L(M)$ conteria um subgrupo normal minimal de L, o qual seria M (por ser o único), e, assim, M seria abeliano.

Caso 2. M abeliano: temos que M admite um complemento em L, digamos K. Afirmamos que $C_L(M) \cap K = \{1\}$. Com efeito, visto que $C_L(M) \trianglelefteq L$, temos $C_L(M) \cap K \trianglelefteq K$ donde $K \leq N_L(C_L(M) \cap K)$. Também, M centraliza, e, então, normaliza $C_L(M) \cap K$; consequentemente,

$$L = MK \leq N_L(C_L(M) \cap K).$$

Ou seja, $C_L(M) \cap K \trianglelefteq L$. Se $C_L(M) \cap K \neq \{1\}$, então teríamos $M \leq C_L(M) \cap K$ donde $M \leq K$, e, assim, $M \cap K = M \neq \{1\}$, um absurdo. Portanto, a afirmação segue. Usando a Lei Modular de Dedekind (Lema 2.1.10), concluímos que

$$C_L(M) = C_L(M) \cap L = C_L(M) \cap MK = M(C_L(M) \cap K) = M.$$

Pela Proposição 1.1.9, $C_{L^k}(M^k) = C_L(M)^k$, logo $C_{L^k}(M^k) = \{1\}$ se M é não abeliano, e $C_{L^k}(M^k) = M^k$ se M é abeliano.

Agora, seja N um subgrupo normal minimal de L_k distinto de todos os M_i's. Daí, pela Proposição 1.3.2, para cada i, $1 \leq i \leq k$, temos $N \leq C_{L_k}(M_i)$ donde $N \leq C_{L_k}(M^k)$. Como $L_k \leq L^k$, temos que $C_{L_k}(M^k) \leq C_{L^k}(M^k)$. Se M é não abeliano, obtemos $N = \{1\}$, um absurdo. Portanto, os únicos subgrupos normais de L_k, neste caso, são os fatores diretos $M_1, \ldots, M_k$ de modo que $\mathrm{soc}(L_k) = M^k$. Se M é abeliano, $N \leq C_{L^k}(M^k) = M^k$ e, neste caso, concluímos também que $\mathrm{soc}(L_k) = M^k$. Isto completa a prova da proposição. □

Lema 2.3.3. *O socle de L_k admite um complemento quando $M = \mathrm{soc}(L)$ é abeliano.*

Demonstração. Sabemos que M é complementado em L, logo existe $H \leq L$ tal que $L = MH$ e $M \cap H = \{1\}$. Afirmamos que

$$L_k = M^k \cdot \mathrm{diag}(H^k).$$

De fato, M^k e $\mathrm{diag}(H^k)$ estão contidos em L_k de modo que $M^k \cdot \mathrm{diag}(H^k) \leq L_k$. Reciprocamente, seja $x = (l_1, \ldots, l_k) \in L_k$, então $x = (m_1h_1, \ldots, m_kh_k)$ para certos $m_i \in M$

e $h_i \in H$ $(1 \leq i \leq k)$, pois $L = MH$. Mas como $x \in L_k$, temos $Mh_1 = \cdots = Mh_k$, e visto que $M \cap H = \{1\}$, obtemos $h_1 = \cdots = h_k$. Ou seja,

$$x = (m_1h_1, \ldots, m_kh_1) = (m_1, \ldots, m_k) \cdot (h_1, \ldots, h_1) \in M^k \cdot \mathrm{diag}(H^k).$$

Portanto, $L_k \leq M^k \cdot \mathrm{diag}(H^k)$, e a afirmação segue. Agora, $M^k \cap \mathrm{diag}(H^k) = \{1\}$, uma vez que $M \cap H = \{1\}$. □

Proposição 2.3.4. *Seja U um subgrupo normal minimal de L_k. Então $L_k/U \cong L_{k-1}$ e $\mathrm{soc}(L_k/U) = \mathrm{soc}(L_k)/U$.*

Demonstração. Vamos dividir a demonstração em dois casos.

Caso 1. M é não abeliano: vimos na prova da Proposição 2.3.2 que os únicos subgrupos normais minimais de L_k nesse caso são $M_1, \ldots, M_k$, os fatores diretos de M^k. Assim, sem perda de generalidade, suponhamos $U = M_k$, e definamos $\alpha : L_k \to L_{k-1}$ por

$$(l_1, \ldots, l_k)^\alpha = (l_1, \ldots, l_{k-1}), \qquad \text{sempre que} \quad (l_1, \ldots, l_k) \in L_k.$$

Dados $(l_1, \ldots, l_k), (r_1, \ldots, r_k) \in L_k$, temos

$$\begin{aligned}((l_1, \ldots, l_k) \cdot (r_1, \ldots, r_k))^\alpha &= (l_1r_1, \ldots, l_kr_k)^\alpha = (l_1r_1, \ldots, l_{k-1}r_{k-1}) \\ &= (l_1, \ldots, l_{k-1}) \cdot (r_1, \ldots, r_{k-1}) = (l_1, \ldots, l_k)^\alpha \cdot (r_1, \ldots, r_k)^\alpha.\end{aligned}$$

Isto mostra que α é um homomorfismo de grupos. Além disso, dado $(l_1, \ldots, l_{k-1}) \in L_{k-1}$, temos por definição de L_{k-1} que $l_1 \equiv \cdots \equiv l_{k-1} \bmod M$. Daí, $x = (l_1, \ldots, l_{k-1}, l_{k-1}) \in L_k$ e $(l_1, \ldots, l_{k-1}) = x^\alpha$. Portanto, α é sobrejetiva. Agora, vamos calcular $\ker(\alpha)$. Seja $(l_1, \ldots, l_k) \in \ker(\alpha)$. Então $(l_1, \ldots, l_{k-1}) = (l_1, \ldots, l_k)^\alpha = (1, \ldots, 1)$ de modo que $l_1 = \cdots = l_{k-1} = 1$. Dado que $(l_1, \ldots, l_k) \in L_k$, temos $Ml_k = Ml_{k-1} = M$ donde $l_k \in M$ e $(l_1, \ldots, l_k) \in U$. Ou seja, $\ker(\alpha) \leq U$. Por outro lado, $U \leq \ker(\alpha)$, e, consequentemente, $\ker(\alpha) = U$. Pelo Teorema dos Isomorfismos, $\overline{\alpha} : L_k/U \to L_{k-1}$ dada por $(Ux)^{\overline{\alpha}} = x^\alpha$ para cada $x \in L_k$, é um isomorfismo. Portanto, $L_k/U \cong L_{k-1}$.

Agora, notemos que se $T \leq L_k$, então $(TU/U)^{\overline{\alpha}} = T^\alpha$, logo $(\mathrm{soc}(L_k)/U)^{\overline{\alpha}} = (\mathrm{soc}(L_k))^\alpha = \mathrm{soc}(L_{k-1})$ (pois $M^k \overset{\alpha}{\longmapsto} M^{k-1}$). Por outro lado, como $\overline{\alpha}$ é um isomorfismo, temos que $(\mathrm{soc}(L_k/U))^{\overline{\alpha}} = \mathrm{soc}(L_{k-1})$. Portanto $(\mathrm{soc}(L_k)/U)^{\overline{\alpha}} = (\mathrm{soc}(L_k/U))^{\overline{\alpha}}$, e aplicando $\overline{\alpha}^{-1}$, obtemos $\mathrm{soc}(L_k/U) = \mathrm{soc}(L_k)/U$.

Caso 2. M é abeliano: se para todo $i \in \{1, \ldots, k\}$, $U \subseteq \prod_{j \neq i} M_j$, então

$U \subseteq \bigcap_{i=1}^{k} \prod_{j \neq i} M_j = \{1\}$, o que é uma contradição. Portanto, existem $k-1$ fatores diretos de M^k tais que U não está contido no produto destes. Sem perda de generalidade, assumamos que $U \nsubseteq M_1 \cdots M_{k-1}$. Desse modo, $U \cap M_1 \cdots M_{k-1} = \{1\}$, já que U é normal minimal em L_k. Observamos que nesse caso (M abeliano), existe $H \leq L$ um complemento para M em L tal que $\mathrm{diag}(H^k)$ é um complemento para M^k em L_k (vide Lema 2.3.3).

Agora, M é um H-grupo simples (a ação é por conjugação). Com efeito, se K é um H-subgrupo de M, então por definição $H \leq N_L(K)$. E uma vez que M é abeliano, $K \trianglelefteq M$ donde $M \leq N_L(K)$. Daí,

$$L = MH \leq N_L(K) \quad \text{e} \quad K \trianglelefteq L.$$

Como M é normal minimal em L, segue-se que $K = \{1\}$ ou $K = M$. Portanto, M é um H-grupo simples. Com isso, obtemos que

$$S : \{1\} < M_1 < M_1M_2 < \cdots < M_1M_2 \cdots M_k = M^k$$

é uma H-série de composição de M^k, pois os fatores são todos H-isomorfos a M, e, portanto, são H-grupos simples (vide Proposição 1.7.2). Por outro lado, temos que U também é um H-grupo simples (a ação de H sobre U é dada por $(u_1, \ldots, u_k)^h = (u_1^h, \ldots, u_k^h)$, para cada $(u_1, \ldots, u_k) \in U$). De fato, seja V um H-subgrupo de U, então por definição

$$(v_1, \ldots, v_k)^{(h,\ldots,h)} = (v_1^h, \ldots, v_k^h) = (v_1, \ldots, v_k)^h \in V,$$

para todos $(v_1, \ldots, v_k) \in V$ e $h \in H$. Isto é, $\mathrm{diag}(H^k) \leq N_{L_k}(V)$. E $V \leq U \leq M^k$, logo $V \trianglelefteq M^k$ e $M^k \leq N_{L_k}(V)$ (pois M é abeliano). Portanto,

$$L_k = M^k \cdot \mathrm{diag}(H^k) \leq N_{L_k}(V) \quad \text{e} \quad V \trianglelefteq L_k.$$

Dado que U é normal minimal em L_k, segue-se que $V = \{1\}$ ou $V = U$. Dessa forma, concluímos que U é um H-grupo simples. Então, pelo Teorema de Jordan-Hölder (Teorema 1.7.5), a H-série $\{1\} < U < M^k$ admite um refinamento o qual é uma série de composição H-isomorfa a S, e, então, $U \cong_H M$. Consequentemente, $|U| = |M|$ e

$$|UM_1 \cdots M_{k-1}| = |U| \cdot |M_1 \cdots M_{k-1}| = |M| \cdot |M|^{k-1} = |M|^k$$

de modo que $M^k = UM_1 \cdots M_{k-1}$. Portanto,

$$L_k = UM_1 \cdots M_k \cdot \mathrm{diag}(H^k)$$

e todo elemento de L_k pode ser escrito unicamente como $um_1 \cdots m_{k-1}h$, com $u \in U$, $m_i \in M_i$ $(1 \leq i \leq k-1)$ e $h \in \mathrm{diag}(H^k)$. Com isso, definamos $\beta : L_k \to L_{k-1}$ por

$$(um_1 \cdots m_{k-1}h)^\beta = m_1 \cdots m_{k-1}h,$$

sempre que $u \in U$, $m_i \in M_i$ $(1 \leq i \leq k-1)$ e $h \in \mathrm{diag}(H^k)$. Vamos mostrar que β é um homomorfismo de grupos. Sejam $um_1 \cdots m_{k-1}h$ e $vn_1 \cdots n_{k-1}h'$ dois elementos arbitrários de L_k. Temos

$$\begin{aligned}
(um_1 \cdots m_{k-1}h \cdot vn_1 \cdots n_{k-1}h')^\beta &= (um_1 \cdots m_{k-1}v^{h^{-1}} n_1^{h^{-1}} \cdots n_{k-1}^{h^{-1}} \cdot hh')^\beta \\
&= (uv^{h^{-1}} m_1 n_1^{h^{-1}} \cdots m_{k-1}n_{k-1}^{h^{-1}} \cdot hh')^\beta = m_1 n_1^{h^{-1}} \cdots m_{k-1}n_{k-1}^{h^{-1}} \cdot hh' \\
&= m_1 \cdots m_{k-1}n_1^{h^{-1}} \cdots n_{k-1}^{h^{-1}} \cdot hh' = m_1 \cdots m_{k-1}h \cdot n_1 \cdots n_{k-1}h' \\
&= (um_1 \cdots m_{k-1})^\beta \cdot (vn_1 \cdots n_{k-1}h')^\beta,
\end{aligned}$$

pois M é abeliano. Pela arbitrariedade dos elementos, concluímos que β é um homomorfismo. Além disso, β é sobrejetiva, pois como observado anteriormente, $L_{k-1} = M^{k-1} \cdot \mathrm{diag}(H^{k-1})$. Por fim, $\ker(\beta) = U$. Então, pelo Teorema dos Isomorfismos, $L_k/U \cong L_{k-1}$. Com o mesmo argumento do Caso 1, $\mathrm{soc}(L_k/U) = \mathrm{soc}(L_k)/U$, pois $(\mathrm{soc}(L_k))^\beta = (M^k)^\beta = M^{k-1} = \mathrm{soc}(L_{k-1})$. Isto completa a prova da proposição. □

Corolário 2.3.5. *Seja N um subgrupo normal de L_k. Então, ou $\mathrm{soc}(L_k) \leq N$, ou $N \leq \mathrm{soc}(L_k)$.*

Demonstração. A prova será feita por indução sobre k. Consideremos $k = 1$. Se $N = \{1\}$, então $N \leq \mathrm{soc}(L_k)$. Caso contrário, N contém um subgrupo normal minimal de $L_k = L$, o qual deve ser $M = \mathrm{soc}(L_k)$, pois M é o único subgrupo normal minimal de L. Portanto, o caso $k = 1$ é verdadeiro.

Então, suponhamos $k > 1$ e $N \neq \{1\}$, logo existe U um subgrupo normal minimal de L_k tal que $U \leq N$. Pela Proposição 2.3.4, existe um isomorfismo $\gamma : L_k/U \to L_{k-1}$ e $\mathrm{soc}(L_k/U) = \mathrm{soc}(L_k)/U$. Por indução, obtemos que ou $\mathrm{soc}(L_{k-1}) \leq (N/U)^\gamma$, ou $(N/U)^\gamma \leq \mathrm{soc}(L_{k-1})$. Daí, ou $\mathrm{soc}(L_k)/U = \mathrm{soc}(L_k/U) = (\mathrm{soc}(L_{k-1}))^{\gamma^{-1}} \leq N/U$, ou $N/U \leq (\mathrm{soc}(L_{k-1}))^{\gamma^{-1}} = \mathrm{soc}(L_k/U) = \mathrm{soc}(L_k)/U$ (pois γ é um isomorfismo). Ou seja, ou $\mathrm{soc}(L_k) \leq N$, ou $N \leq \mathrm{soc}(L_k)$, completando a indução. □

A Proposição 2.3.4 nos dá que o grupo quociente de L_k sobre qualquer subgrupo normal minimal é isomorfo a L_{k-1}. Em particular, a sequência $d(L_1), \ldots, d(L_k), \ldots$ é não decrescente.

Vamos agora nos concentrar em provar que esta sequência é ilimitada.

Definição 2.3.6. *Um automorfismo $\gamma : L \to L$ age trivialmente em L/M se o homomorfismo induzido $\overline{\gamma} : L/M \to L/M$,*

$$\overline{\gamma} : Ml \mapsto Ml^{\gamma},$$

é a identidade. Isto equivale a dizer que $l^{\gamma} \in Ml$, para todo $l \in L$.

Notemos que $\overline{\gamma}$ está bem definido, pois M é um subgrupo característico de L (é o único subgrupo normal minimal de L). O grupo dos automorfismos de L que agem trivialmente em L/M é denotado por Γ_L.

Para um grupo finito G e um inteiro positivo m, seja $\phi_G(m)$ o número de *m-bases* de G, ou seja, m-uplas ordenadas $(x_1, \ldots, x_m)$ de elementos de G tais que $\langle x_1, \ldots, x_m \rangle = G$. Esta função foi introduzida por Philip Hall [15], em 1936, com o nome de *função Euleriana*.

Lema 2.3.7. *Seja F um grupo livre de posto $m \geq d(L)$. Dado um homomorfismo sobrejetivo $\beta : F \to L/M$, consideremos o conjunto $\mathscr{R}$ dos subgrupos normais N de F os quais são núcleos de homomorfismos sobrejetivos de F em L que, compostos com a projeção canônica $\pi : L \to L/M$, produzem β. Então, a cardinalidade do conjunto $\mathscr{R}$ é*

$$\frac{\phi_L(m)}{|\Gamma_L|\phi_{L/M}(m)}.$$

Demonstração. Seja $x_1, \ldots, x_m$ uma base de F. Pelas Proposições 1.1.2 e 1.1.3, temos que β é unicamente determinado por $x_1^{\beta} = Ml_1, \ldots, x_m^{\beta} = Ml_m$ e $L = \langle l_1, \ldots, l_m, M \rangle$. Agora, seja A o conjunto dos homomorfismos sobrejetivos de F em L que, compostos com a projeção canônica $\pi : L \to L/M$, produzem β. Seja também

$$B = \{(z_1, \ldots, z_m) \in M^m \mid L = \langle z_1 l_1, \ldots, z_m l_m \rangle\}.$$

Definindo $f : B \to A$ por

$$(z_1, \ldots, z_m)f = \gamma_{(z_1,\ldots,z_m)},$$

onde $\gamma_{(z_1,\ldots,z_m)}$ é o único homomorfismo sobrejetivo tal que

$$x_1^{\gamma_{(z_1,\ldots,z_m)}} = z_1 l_1 \ , \ \ldots \ , \ x_m^{\gamma_{(z_1,\ldots,z_m)}} = z_m l_m,$$

temos que f é uma bijeção. De fato, f está bem definida, já que F é um grupo livre de posto m (vide Observação 1.8.4). Dado $\gamma \in A$, uma vez que $\gamma\pi = \beta$, temos

$$Mx_i^{\gamma} = (x_i^{\gamma})^{\pi} = x_i^{\gamma\pi} = x_i^{\beta} = Ml_i, \quad \forall i = 1, \ldots, m.$$

Assim, para cada i, $1 \leq i \leq m$, existe $z_i \in M$ tal que $x_i^{\gamma} = z_i l_i$, e como γ é sobrejetivo, obtemos que $L = \langle z_1 l_1, \ldots, z_m l_m \rangle$ (vide Proposição 1.1.3). Isto nos dá que $(z_1, \ldots, z_m) \in B$ e $(z_1, \ldots, z_m)f = \gamma$, ou seja, f é sobrejetiva. A injetividade segue do fato de que os l_i's estão fixados.

Vamos então calcular o número de elementos do conjunto B. Para isto, consideremos T um transversal à direita de M em L,

$$C = \left\{ \begin{array}{c} (v_1 r_1, \ldots, v_m r_m) \in L^m \mid r_1, \ldots, r_m \in T,\ v_1, \ldots, v_m \in M, \\ L/M = \langle Mr_1, \ldots, Mr_m \rangle \quad \text{e} \quad L = \langle v_1 r_1, \ldots, v_m r_m \rangle \end{array} \right\}$$

e

$$D = \{(y_1, \ldots, y_m) \in L^m \mid L = \langle y_1, \ldots, y_m \rangle\}.$$

Claramente, $C \subseteq D$. Agora, seja $(y_1, \ldots, y_m) \in D$. Como T é um transversal à direita de M em L, temos que para cada i, $1 \leq i \leq m$, $y_i = v_i r_i$, para certos $v_i \in M$ e $r_i \in T$ (de modo único). Dado que $L = \langle y_1, \ldots, y_m \rangle$, segue-se que $(y_1, \ldots, y_m) \in C$. Portanto, $D \subseteq C$, e, assim,

$$C = D.$$

Dada uma m-upla $(r_1, \ldots, r_m) \in L^m$ tal que $r_1, \ldots, r_m \in T$ e $L/M = \langle Mr_1, \ldots, Mr_m \rangle$, o número de m-uplas $(v_1, \ldots, v_m) \in M^m$ tais que $L = \langle v_1 r_1, \ldots, v_m r_m \rangle$ é $|B|$, pelo Teorema 2.2.5. Seja $(t_1, \ldots, t_m) \in L^m$ uma m-upla tal que $t_1, \ldots, t_m \in T$ e $L/M = \langle Mt_1, \ldots, Mt_m \rangle$, distinta de $(r_1, \ldots, r_m)$, digamos $t_1 \neq r_1$, e consideremos $(w_1, \ldots, w_m) \in M^m$ tal que $L = \langle w_1 t_1, \ldots, w_m t_m \rangle$. Então, $(w_1 t_1, \ldots, w_m t_m)$ é distinta de todas as m-uplas $(v_1 r_1, \ldots, v_m r_m)$ acima, pois $Mt_1 \neq Mr_1$. Isto nos dá que o número de elementos do conjunto C é

$$|C| = \phi_{L/M}(m)|B|.$$

Como $|C| = |D| = \phi_L(m)$, concluímos que

$$|A| = |B| = \phi_L(m)/\phi_{L/M}(m).$$

Para finalizar, sejam $\gamma_1, \gamma_2 \in A$. Então, $\ker(\gamma_1) = \ker(\gamma_2) = N$ se, e somente se,

existe um automorfismo α de L que age trivialmente em L/M tal que $\gamma_2 = \gamma_1\alpha$. Com efeito, se $\ker(\gamma_1) = \ker(\gamma_2) = N$, consideremos os isomorfismos $\overline{\gamma_1} : Nx \mapsto x^{\gamma_1}$ e $\overline{\gamma_2} : Nx \mapsto x^{\gamma_2}$ de F/N em L (via Teorema dos Isomorfismos). Seja $\alpha = \overline{\gamma_1}^{-1}\overline{\gamma_2}$. Assim, α é um automorfismo de L. Dado $x \in F$, temos

$$x^{\gamma_1\alpha} = x^{\gamma_1\overline{\gamma_1}^{-1}\overline{\gamma_2}} = (Nx)^{\overline{\gamma_2}} = x^{\gamma_2},$$

ou seja, $\gamma_2 = \gamma_1\alpha$. Além disso, α age trivialmente em L/M, pois dado $l \in L$, existe $x \in F$ tal que $l = x^{\gamma_1}$ donde

$$Ml^{\alpha} = Ml^{\overline{\gamma_1}^{-1}\overline{\gamma_2}} = Mx^{\gamma_2} = Mx^{\gamma_1} = Ml,$$

já que $\gamma_1\pi = \beta = \gamma_2\pi$. Reciprocamente, suponhamos que exista um tal automorfismo α de L. Como $\gamma_2 = \gamma_1\alpha$, temos que

$$x \in \ker(\gamma_2) \Leftrightarrow x^{\gamma_2} = 1 \Leftrightarrow x^{\gamma_1\alpha} = 1 \Leftrightarrow x^{\gamma_1} = 1 \Leftrightarrow x \in \ker(\gamma_1).$$

Portanto, $\ker(\gamma_1) = \ker(\gamma_2)$. Com isso, podemos definir uma relação de equivalência $\sim$ em A da seguinte forma: dados $\gamma_1, \gamma_2 \in A$, $\gamma_1 \sim \gamma_2 \Leftrightarrow \ker(\gamma_1) = \ker(\gamma_2)$. A classe de equivalência de um elemento $\gamma \in A$ por essa relação é

$$[\gamma] = \{\theta \in A \mid \ker(\theta) = \ker(\gamma)\} = \{\theta \in A \mid \exists\, \alpha \in \Gamma_L \text{ com } \theta = \gamma\alpha\} = \{\gamma\alpha \mid \alpha \in \Gamma_L\}.$$

Dado que γ é sobrejetivo, $\gamma\alpha_1 = \gamma\alpha_2 \Rightarrow \alpha_1 = \alpha_2$, consequentemente a aplicação $\alpha \mapsto \gamma\alpha$ é uma bijeção entre os conjuntos Γ_L e $[\gamma]$. Portanto,

$$\phi_L(m)/\phi_{L/M}(m) = |A| = |\mathscr{R}| \cdot |\Gamma_L|$$

donde $|\mathscr{R}| = \phi_L(m)/|\Gamma_L|\phi_{L/M}(m)$. Isto completa a prova do lema. □

Proposição 2.3.8. *A sequência $d(L_1), \ldots, d(L_k), \ldots$ é ilimitada.*

Demonstração. Suponhamos que esta seja limitada. Logo, existe um inteiro positivo m tal que $d(L_k) \leq m$, para todo $k \geq 1$ (em particular, $d(L) \leq m$). Seja F um grupo livre de posto m (vide Teorema 1.8.2), e consideremos o conjunto I dos inteiros positivos i tais que existe um homomorfismo sobrejetivo de F em L_i. Notemos que I é não vazio, pela Observação 1.8.4. Afirmamos que I tem um maior elemento. Com efeito, basta mostrar que I é limitado. Para isto, seja $i \in I$, logo existe um homomorfismo

sobrejetivo $\psi : F \to L_i$. Dado j, $1 \leq j \leq i$, seja

$$\gamma_j = \psi\pi_j,$$

onde $\pi_j : L_i \to L$ é a projeção na j-ésima coordenada, isto é, $(l_1, \ldots, l_i)^{\pi_j} = l_j$, sempre que $(l_1, \ldots, l_i) \in L_i$. Assim, cada γ_j é um homomorfismo sobrejetivo de F em L. Além disso, dado $x \in F$, temos que $x^{\psi} = (l_1, \ldots, l_i)$, para algum $(l_1, \ldots, l_i) \in L_i$. Daí, $Ml_1 = \cdots = Ml_i$, o que implica

$$x^{\gamma_1\pi} = \cdots = x^{\gamma_i\pi},$$

onde $\pi : L \to L/M$ é a projeção canônica. Desse modo,

$$\gamma_1\pi = \cdots = \gamma_i\pi = \beta,$$

com $\beta : F \to L/M$ um homomorfismo sobrejetivo. Sejam $j_1 \neq j_2$ em $\{1, \ldots, i\}$, e seja $(m_1, \ldots, m_i) \in M^i \subseteq L_i$ com $m_{j_1} = 1$ e $m_{j_2} \neq 1$ ($M \neq \{1\}$). Então existe $x \in F$ tal que $x^{\psi} = (m_1, \ldots, m_i)$ de modo que

$$x^{\gamma_{j_1}} = m_{j_1} = 1 \quad \text{e} \quad x^{\gamma_{j_2}} = m_{j_2} \neq 1,$$

ou seja, $x \in \ker(\gamma_{j_1})$ e $x \notin \ker(\gamma_{j_2})$. Isto implica em $\ker(\gamma_{j_1}) \neq \ker(\gamma_{j_2})$. Consequentemente, $|\{\ker(\gamma_1), \ldots, \ker(\gamma_i)\}| = i$ e, pelo Lema 2.3.7, obtemos que $i \leq \phi_L(m)/|\Gamma_L|\phi_{L/M}(m)$. Com isso, a afirmação segue, isto é, existe k o maior elemento de I.

Agora, $d(L_{k+1}) > m$, pois, caso contrário, existiria um homomorfismo sobrejetivo de F em L_{k+1} (já que F é um grupo livre de posto m – vide Observação 1.8.4) donde $k+1$ pertenceria a I, contradizendo a maximalidade de k. Mas $d(L_{k+1}) > m$ é uma contradição com a suposição inicial, portanto a sequência $d(L_1), \ldots, d(L_k), \ldots$ é ilimitada. □

Em particular, tomando $L = S$ um grupo simples não abeliano finito, obtemos que a sequência $d(S), d(S^2), \ldots, d(S^k), \ldots$ é ilimitada. Ao final deste trabalho, daremos uma outra prova para esse fato.

Mostramos que a sequência $d(L_1), \ldots, d(L_k), \ldots$ é não decrescente e ilimitada. Agora, seja $k \in \mathbb{Z}_+$. Tomando um subgrupo normal minimal de L_{k+1}, digamos U,

temos, pela Proposição 2.3.4 e pelo Teorema 2.2.8, que

$$d(L_{k+1}) \leq d(L_{k+1}/U) + 1 = d(L_k) + 1.$$

Portanto, se $m \geq d(L)$, então existe um único k tal que

$$d(L_k) = m < d(L_{k+1}).$$

Desse modo, definimos $f(L, m) := k + 1$. Quando L pode ser identificado a partir do contexto, escrevemos $f(m)$ em vez de $f(L, m)$. Na próxima seção, vamos fazer um estudo sobre como a função f pode ser calculada.

Lema 2.3.9. *Sejam G um grupo finito e $N_1, \ldots, N_k$ todos os seus subgrupos normais minimais. Se para cada $i \in \{1, \ldots, k\}$, N_i é não abeliano, então* $\mathrm{soc}(G)$ *é o produto direto interno de $N_1, \ldots, N_k$. Ademais,* $\mathrm{soc}(G) \cong N_1 \times \cdots \times N_k$.

Demonstração. Dado $i \in \{1, \ldots, k\}$, consideremos $T = N_i \cap N_1 \cdots N_{i-1} N_{i+1} \cdots N_k$. Temos $T \trianglelefteq G$ e $T \leq N_i$. Se $T \neq \{1\}$, então $T = N_i$ (pois N_i é normal minimal em G) donde

$$N_i \leq N_1 \cdots N_{i-1} N_{i+1} \cdots N_k \leq C_G(N_i),$$

pela Proposição 1.3.2. Mas isto é uma contradição, já que N_i é não abeliano. Portanto, $T = \{1\}$. Usando o Teorema 1.1.6, o lema segue. □

Os grupos L_k têm sua importância no estudo de grupos que necessitam de mais geradores do que qualquer quociente próprio. Mais precisamente, temos o:

Teorema A. *Seja m um inteiro positivo e H um grupo finito tal que $d(H/N) \leq m$ para todo subgrupo normal não trivial N, mas $d(H) > m$. Se $m = 1$, então ou $H \cong C_p \times C_p$ para algum primo p, ou H é um grupo primitivo monolítico com socle M e H/M é cíclico. Se $m \geq 2$, então existe um grupo primitivo monolítico L tal que $H \cong L_{f(L,m)}$.*

Por motivos de clareza, vamos usar a notação de classe lateral à esquerda na demonstração. Observamos que isto é indiferente quando o subgrupo em questão é normal.

Demonstração. Dado que $d(H) > m \geq 1$, temos que H é um grupo não cíclico. Suponhamos $m = 1$, ou seja, todo quociente próprio de H é cíclico. Como visto no Exemplo 2.2.3, $d(H) = d(H/\Phi(H))$. Daí $H/\Phi(H)$ é também não cíclico de modo que $\Phi(H) = \{1\}$.

Se H é nilpotente, então este é um produto direto $\prod_{i=1}^{n} P_i$, sendo que P_i é um p_i-grupo para cada $i \in \{1, \ldots, n\}$, e os p_i's são números primos dois a dois distintos. Visto que H é não cíclico, podemos supor que P_1 é não cíclico. Mas notemos que P_1 é um quociente de H via o subgrupo normal $\prod_{i=2}^{n} P_i$. Dado que os quocientes próprios de H são cíclicos, deduzimos que $H \cong P_1$. Uma vez que $\Phi(H) = \{1\}$, segue-se da Proposição 1.5.7 que H é abeliano elementar, isto é, $H \cong C_p^r$ (com $p = p_1$), e $r \geq 2$ porque H é não cíclico. Contudo, o grupo C_p^{r-1} é um quociente de H, logo é cíclico, e, assim, concluímos que $r = 2$ e $H \cong C_p \times C_p$.

Agora, assumamos H não nilpotente. Com isso, temos que existe um subgrupo maximal K de H que não é normal em H (vide Teorema 1.4.11). Se o coração normal K_H é não trivial, então H/K_H é cíclico (por hipótese) de forma que K/K_H é normal em H/K_H e, por correspondência, K é normal em H, uma contradição. Portanto, $K_H = \{1\}$. Isto prova que H é um grupo primitivo.

Se H é não monolítico, então este admite pelo menos dois subgrupos normais minimais, digamos A e B. Pelo Teorema de Ore-Baer (Teorema 2.1.14), obtemos que H é não solúvel (haja vista que H é primitivo). Por conseguinte, A e B são não abelianos, já que por hipótese H/A e H/B são cíclicos. Por outro lado, $AB/B \cong A$ é um subgrupo do grupo cíclico H/B, logo A é cíclico, um absurdo. Portanto, H é monolítico. Sendo $M = \mathrm{soc}(H)$, segue-se da hipótese que H/M é cíclico.

Assumamos, agora, $m \geq 2$, e suponhamos que H contém um único subgrupo normal minimal, digamos N. Sendo H não cíclico, temos, pelo Teorema 2.2.9, que

$$d(H) = \max\{2, d(H/N)\},$$

o que implica $d(H) = 2$ ou $d(H) = d(H/N)$, uma contradição com as hipóteses do teorema. Portanto, H contém pelo menos dois subgrupos normais minimais distintos. Sejam $N_1, \ldots, N_r, \ldots$ os subgrupos normais minimais de H. Como $d(H/N_1) \leq m$ por hipótese, existem m elementos $h_1, \ldots, h_m$ de H tais que $H = \langle h_1, \ldots, h_m, N_1 \rangle$. Agora, consideremos N_r com $r \neq 1$. Uma vez que $N_1 \leq N_1 N_r$, temos $H = \langle h_1, \ldots, h_m, N_1 N_r \rangle$. Daí, $H/N_r = \langle h_1 N_r, \ldots, h_m N_r, N_1 N_r/N_r \rangle$. Também, $N_1 N_r/N_r$ é um subgrupo normal de H/N_r (pois $N_1 N_r \trianglelefteq H$) e H/N_r é m-gerado por hipótese. Então, pelo Teorema 2.2.5, existem m elementos $x_1, \ldots, x_m \in N_1$ tais que $H/N_r = \langle (h_1 x_1)N_r, \ldots, (h_m x_m)N_r \rangle$, ou seja, $H = \langle h_1 x_1, \ldots, h_m x_m, N_r \rangle$.

Seja $K_r = \langle h_1 x_1, \ldots, h_m x_m \rangle$. Afirmamos que N_1 e N_r são ambos complementados por K_r em H. Claramente, $H = K_r N_r$, pois $H = \langle h_1 x_1, \ldots, h_m x_m, N_r \rangle$. Agora, $H = \langle h_1, \ldots, h_m, N_1 \rangle$. Temos $N_1 \leq K_r N_1$ e $h_i = (h_i x_i) x_i^{-1} \in K_r N_1$, $\forall i = 1, \ldots, m$ de modo

que $H \leq K_r N_1$, e, assim, $H = K_r N_1$. Resta provar que $K_r \cap N_j$ é trivial ($j = 1, r$). Pela Proposição 1.3.2, $N_r \leq C_H(N_1)$ e $N_1 \leq C_H(N_r)$. Assim, dados $\kappa_r \in K_r$, $n_r \in N_r$ e $x \in K_r \cap N_1$, temos

$$x^{\kappa_r n_r} = (x^{\kappa_r})^{n_r} = x^{\kappa_r} \in K_r \cap N_1,$$

isto é, $K_r \cap N_1 \trianglelefteq K_r N_r = H$. Como este subgrupo normal está contido no subgrupo normal minimal N_1 de H, se $K_r \cap N_1 \neq \{1\}$, então $N_1 \leq K_r$ e $H = K_r N_1 = K_r$ é m-gerado, um absurdo. A afirmação $K_r \cap N_r = \{1\}$ é provada de forma análoga.

Agora, é fácil mostrar que as projeções $\pi_r : K_r \cap (N_1 \times N_r) \to N_1$ e $\rho_r : K_r \cap (N_1 \times N_r) \to N_r$ são isomorfismos. Consideremos primeiro π_r. Temos

$$(n_1 n_r \cdot \overline{n_1}\ \overline{n_r})^{\pi_r} = (n_1 \overline{n_1} n_r \overline{n_r})^{\pi_r} = n_1 \overline{n_1} = (n_1 n_r)^{\pi_r} (\overline{n_1}\ \overline{n_r})^{\pi_r},$$

para todos $n_1 n_r, \overline{n_1}\ \overline{n_r} \in K_r \cap (N_1 \times N_r)$, logo π_r é um homomorfismo. Dado $n_1 \in N_1 \leq H = K_r N_r$, existem $t \in K_r$ e $n_r \in N_r$ tais que $n_1 = t n_r$: então, $t = n_1 n_r^{-1} \in K_r \cap (N_1 \times N_r)$ e $t^{\pi_r} = n_1$ donde π_r é sobrejetiva. Por fim, se $x = n_1 n_r \in \ker(\pi_r)$, então $n_1 = x^{\pi_r} = 1$, ou seja, $x = n_r \in K_r \cap N_r = \{1\}$. Isto nos fornece que $\ker(\pi_r) = \{1\}$ e π_r é injetiva. Argumentos análogos podem ser aplicados para ρ_r.

O que vamos usar a partir disso é que, para cada $r > 1$, existe um subgrupo K_r que complementa ambos N_1 e N_r, e um isomorfismo $\phi_r : N_1 \to N_r$ (a saber $\phi_r = \pi_r^{-1} \rho_r$) tal que

$$K_r \cap (N_1 \times N_r) = \{x x^{\phi_r} \mid x \in N_1\}.$$

Para ver esta última igualdade, seja $t = n_1 n_r \in K_r \cap (N_1 \times N_r)$. Assim, $t^{\pi_r} = n_1$, logo $n_1^{\pi_r^{-1}} = t = n_1 n_r$ donde

$$n_1^{\phi_r} = n_1^{\pi_r^{-1} \rho_r} = (n_1^{\pi_r^{-1}})^{\rho_r} = (n_1 n_r)^{\rho_r} = n_r,$$

ou seja, $t = n_1 n_1^{\phi_r} \in \{x x^{\phi_r} \mid x \in N_1\}$. Reciprocamente, dado $x \in N_1$, existe $t = n_1 n_r \in K_r \cap (N_1 \times N_r)$ tal que $x = t^{\pi_r}$ (pois π_r é sobrejetiva) de modo que

$$x x^{\phi_r} = t^{\pi_r} (t^{\pi_r})^{\pi_r^{-1} \rho_r} = t^{\pi_r} t^{\rho_r} = n_1 n_r = t \in K_r \cap (N_1 \times N_r).$$

Portanto, $K_r \cap (N_1 \times N_r) = \{x x^{\phi_r} \mid x \in N_1\}$. Como N_1 e N_r são normais em H, obtemos que $K_r \cap (N_1 \times N_r) \trianglelefteq K_r$, logo este é um K_r-grupo (com a ação por conjugação), assim

como N_1 e N_r. Além disso, dado $t = n_1 n_r \in K_r \cap (N_1 \times N_r)$, temos

$$(t^{\kappa_r})^{\pi_r} = ((n_1 n_r)^{\kappa_r})^{\pi_r} = (n_1^{\kappa_r} n_r^{\kappa_r})^{\pi_r} = n_1^{\kappa_r} = ((n_1 n_r)^{\pi_r})^{\kappa_r} = (t^{\pi_r})^{\kappa_r},$$

e

$$(t^{\kappa_r})^{\rho_r} = ((n_1 n_r)^{\kappa_r})^{\rho_r} = (n_1^{\kappa_r} n_r^{\kappa_r})^{\rho_r} = n_r^{\kappa_r} = ((n_1 n_r)^{\rho_r})^{\kappa_r} = (t^{\rho_r})^{\kappa_r},$$

para todo $\kappa_r \in K_r$, isto é, ambos π_r e ρ_r são K_r-isomorfismos de maneira que $\phi_r = \pi_r^{-1}\rho_r$ também o é.

Quando N_1 é abeliano, os ϕ_r's são na verdade H-isomorfismos. De fato, dados $x \in N_1$ e $h \in H = K_r N_1$, existem $\kappa_r \in K_r$ e $n_1 \in N_1$ tais que $h = \kappa_r n_1$. Daí,

$$(x^h)^{\phi_r} = (x^{\kappa_r n_1})^{\phi_r} = ((x^{\kappa_r})^{n_1})^{\phi_r} = (x^{\kappa_r})^{\phi_r} = (x^{\phi_r})^{\kappa_r} = ((x^{\phi_r})^{\kappa_r})^{n_1} = (x^{\phi_r})^{\kappa_r n_1} = (x^{\phi_r})^h,$$

pois $N_1 \leq C_H(N_r)$. Provamos nesse caso que cada subgrupo normal minimal de H é abeliano e complementado de modo que $\Phi(H) = \{1\}$ (vide Observação 1.5.12), e, por conseguinte, $\mathrm{soc}(H)$ admite um complemento. Com efeito, pelo Teorema 1.3.8 (vide Observação 1.3.9), existe um inteiro $k \geq 2$ tal que $\mathrm{soc}(H)$ é o produto direto interno de $N_{i_1}, N_{i_2}, \ldots, N_{i_k}$. Sem perda de generalidade, assumamos que $N_{i_j} = N_j$, $\forall j = 1, 2, \ldots, k$. Assim, $\mathrm{soc}(H)$ é abeliano e $\mathrm{soc}(H) \cap \Phi(H) \leq \Phi(H) = \{1\}$, logo a Proposição 1.5.11 nos dá que existe $K \leq H$ tal que $H = \mathrm{soc}(H)K$ e $\mathrm{soc}(H) \cap K = \{1\}$.

Agora, seja $L = N_1 K$. Temos $N_1 \trianglelefteq L$, pois $N_1 \trianglelefteq H$ e $N_1 \leq L$. Suponhamos que exista $N \trianglelefteq L$ tal que $\{1\} < N < N_1$. Dados $h = n_1 n_2 \cdots n_k \kappa \in H$ e $n \in N$,

$$n^h = (\kappa^{-1} n_k^{-1} \cdots n_2^{-1} n_1^{-1}) n (n_1 n_2 \cdots n_k \kappa) = \kappa^{-1} n \kappa = n^\kappa,$$

já que $n \in N_1 \leq C_H(N_i)$, $\forall i = 1, \ldots, k$. Dado que $\kappa \in K \leq L$ e $N \trianglelefteq L$, obtemos que $n^\kappa \in N$. Ou seja, $N \trianglelefteq H$, uma contradição com a hipótese de N_1 ser normal minimal em H. Portanto, N_1 é normal minimal em L. Afirmamos que este é o único subgrupo normal minimal de L. Para ver isto, mostremos primeiro que o coração normal de K em L é trivial: $K_L = \{1\}$. Ora, dado i, $1 \leq i \leq k$, temos

$$N_i \cap K_L \leq N_i \cap K \leq \mathrm{soc}(H) \cap K = \{1\}.$$

Por conseguinte, pela Proposição 1.1.8,

$$N_i \leq C_L(K_L) \leq C_H(K_L) \leq N_H(K_L).$$

E $K \leq N_H(K_L)$, pois $K_L \trianglelefteq L$ e $K \leq L$. Portanto,

$$H = N_1 N_2 \cdots N_k K \leq N_H(K_L)$$

donde $K_L \trianglelefteq H$. Se $K_L \neq \{1\}$, então K_L conteria um subgrupo normal minimal de H, digamos T. Assim,

$$T \leq \operatorname{soc}(H) \cap K_L \leq \operatorname{soc}(H) \cap K = \{1\},$$

o que seria um absurdo. Logo $K_L = \{1\}$, como queríamos. Visto que $N_1 \trianglelefteq L$, temos $C_L(N_1) \trianglelefteq L$ donde $C_L(N_1) \cap K \trianglelefteq K$ e $K \leq N_L(C_L(N_1) \cap K)$. Também, N_1 está contido neste normalizador de modo que $L = N_1 K \leq N_L(C_L(N_1) \cap K)$ e $C_L(N_1) \cap K \trianglelefteq L$. Haja vista que $K_L = \{1\}$, segue-se que $C_L(N_1) \cap K = \{1\}$. Pela Lei Modular de Dedekind (Lema 2.1.10),

$$C_L(N_1) = C_L(N_1) \cap L = C_L(N_1) \cap N_1 K = N_1(C_L(N_1) \cap K) = N_1.$$

Se existisse $N \neq N_1$ normal minimal em L, então, pela Proposição 1.3.2, $N \leq C_L(N_1) = N_1$. Mas isto seria uma contradição, já que N_1 é normal minimal em L. Portanto, a afirmação segue, ou seja, L é monolítico. Pela Observação 1.5.12, temos que $N_1 \nleq L$ donde $\Phi(L) = \{1\}$. Desse modo, L é primitivo monolítico (vide Proposição 2.1.6).

Vamos então mostrar que $H \cong L_k$. Definamos $\varphi : H \to L_k$ por

$$(x_1 x_2 \cdots x_k \kappa)^{\varphi} = \left(x_1^{\phi_1^{-1}} \kappa, x_2^{\phi_2^{-1}} \kappa, \ldots, x_k^{\phi_k^{-1}} \kappa\right), \qquad \text{onde} \quad \phi_1 = \mathrm{id}_{N_1}.$$

Para cada $i \in \{1, 2, \ldots, k\}$, $x_i^{\phi_i^{-1}} \kappa = \kappa(\kappa^{-1} x_i^{\phi_i^{-1}} \kappa) \in \kappa N_1$, ou seja,

$$x_1^{\phi_1^{-1}} \kappa \equiv x_2^{\phi_2^{-1}} \kappa \equiv \cdots \equiv x_k^{\phi_k^{-1}} \kappa \mod N_1.$$

Além disso, se $x_1 x_2 \cdots x_k \kappa_1 = y_1 y_2 \cdots y_k \kappa_2$, então $x_i = y_i$, $\forall i = 1, 2, \ldots, k$ e $\kappa_1 = \kappa_2$, pois H é o produto semidireto interno de $\operatorname{soc}(H)$ por K e $\operatorname{soc}(H)$ é o produto direto interno de $N_1, N_2, \ldots, N_k$. Dessa forma, $x_i^{\phi_i^{-1}} \kappa_1 = y_i^{\phi_i^{-1}} \kappa_2$, $\forall i = 1, 2, \ldots, k$, donde $(x_1 x_2 \cdots x_k \kappa_1)^{\varphi} = (y_1 y_2 \cdots y_k \kappa_2)^{\varphi}$ e φ está bem definida. Dado $(l_1, l_2, \ldots, l_k) \in L_k$, cada $l_i = y_i \kappa_i$ com $y_i \in N_1$ e $\kappa_i \in K$. Como $l_1 \equiv l_2 \equiv \cdots \equiv l_k \mod N_1$, obtemos que

$$\kappa_1 N_1 = \kappa_2 N_1 = \cdots = \kappa_k N_1.$$

Daí, $\kappa_i^{-1} \kappa_1 \in N_1 \cap K = \{1\}$, $\forall i = 2, \ldots, k$, isto é, $\kappa_1 = \kappa_2 = \cdots = \kappa_k$. Visto que ϕ_i é um

isomorfismo, $y_i = x_i^{\phi_i^{-1}}$, para algum $x_i \in N_i$, donde

$$(l_1, l_2, \ldots, l_k) = \left(x_1^{\phi_1^{-1}}\kappa_1, x_2^{\phi_2^{-1}}\kappa_1, \ldots, x_k^{\phi_k^{-1}}\kappa_1\right) = (x_1x_2\cdots x_k\kappa_1)^{\varphi}.$$

Isto mostra que φ é sobrejetiva. Dados $h_1 = x_1x_2\cdots x_k\kappa_1$ e $h_2 = y_1y_2\cdots y_k\kappa_2$ em H, temos

$$\begin{aligned} h_1h_2 &= (x_1x_2\cdots x_k\kappa_1)(y_1y_2\cdots y_k\kappa_2) = x_1x_2\cdots x_k y_1^{\kappa_1^{-1}} y_2^{\kappa_1^{-1}}\cdots y_k^{\kappa_1^{-1}}\kappa_1\kappa_2 \\ &= x_1y_1^{\kappa_1^{-1}} x_2y_2^{\kappa_1^{-1}}\cdots x_ky_k^{\kappa_1^{-1}}\kappa_1\kappa_2. \end{aligned}$$

Assim,

$$(h_1h_2)^{\varphi} = \left((x_1y_1^{\kappa_1^{-1}})^{\phi_1^{-1}}\kappa_1\kappa_2, (x_2y_2^{\kappa_1^{-1}})^{\phi_2^{-1}}\kappa_1\kappa_2, \ldots, (x_ky_k^{\kappa_1^{-1}})^{\phi_k^{-1}}\kappa_1\kappa_2\right)^{\varphi}.$$

Para cada $i \in \{1, 2, \ldots, k\}$, temos

$$(x_iy_i^{\kappa_1^{-1}})^{\phi_i^{-1}}\kappa_1\kappa_2 = x_i^{\phi_i^{-1}}(y_i^{\kappa_1^{-1}})^{\phi_i^{-1}}\kappa_1\kappa_2 = x_i^{\phi_i^{-1}}(y_i^{\phi_i^{-1}})^{\kappa_1^{-1}}\kappa_1\kappa_2 = x_i^{\phi_i^{-1}}\kappa_1 y_i^{\phi_i^{-1}}\kappa_2,$$

pois ϕ_i é um H-isomorfismo. Daí,

$$\begin{aligned} (h_1h_2)^{\varphi} &= (x_1^{\phi_1^{-1}}\kappa_1 y_1^{\phi_1^{-1}}\kappa_2, x_2^{\phi_2^{-1}}\kappa_1 y_2^{\phi_2^{-1}}\kappa_2, \ldots, x_k^{\phi_k^{-1}}\kappa_1 y_k^{\phi_k^{-1}}\kappa_2) \\ &= (x_1^{\phi_1^{-1}}\kappa_1, x_2^{\phi_2^{-1}}\kappa_1, \ldots, x_k^{\phi_k^{-1}}\kappa_1)\cdot(y_1^{\phi_1^{-1}}\kappa_2, y_2^{\phi_2^{-1}}\kappa_2, \ldots, y_k^{\phi_k^{-1}}\kappa_2) \\ &= (x_1x_2\cdots x_k\kappa_1)^{\varphi}\cdot(y_1y_2\cdots y_k\kappa_2)^{\varphi} = h_1^{\varphi}\cdot h_2^{\varphi}. \end{aligned}$$

Portanto, φ é um homomorfismo. Seja $x_1x_2\cdots x_k\kappa \in \ker(\varphi)$. Então, $x_i^{\phi_i^{-1}}\kappa = 1$, $\forall i = 1, 2, \ldots, k$. Daí, $x_1^{\phi_1^{-1}} = \kappa^{-1} \in N_1 \cap K = \{1\}$, o que implica $x_1 = \kappa = 1$. Analogamente, $x_2^{\phi_2^{-1}} = \cdots = x_k^{\phi_k^{-1}} = 1$ donde $x_2 = \cdots = x_k = 1$. Isto nos fornece que $\ker(\varphi) = \{1\}$, ou seja, φ é injetiva. Concluímos que φ é um isomorfismo e $H \cong L_k$.

Agora, assumamos que N_1 é não abeliano. Para este caso, escolhamos k tal que os subgrupos normais minimais de H são $N_1, \ldots, N_k$. Seja $\alpha_1 : H \to \mathrm{Aut}(N_1)$ o homomorfismo definido pela ação de conjugação de H em N_1,

$$h^{\alpha_1} : x \mapsto x^h \qquad \text{sempre que} \quad h \in H,\ x \in N_1.$$

Observamos que $\ker(\alpha_1) = C_H(N_1)$. Seja L a imagem de α_1. Este grupo possui somente um subgrupo normal minimal, a saber o grupo não abeliano $M = \mathrm{Inn}(N_1)$. Com

efeito, $Z(N_1) = \{1\}$, pois $Z(N_1) \trianglelefteq H$ (já que $Z(N_1) \trianglelefteq_c N_1 \trianglelefteq H$), $Z(N_1) \leq N_1$, $Z(N_1) \neq N_1$ (N_1 é não abeliano) e N_1 é normal minimal em H. Então, dado que $N_1 \neq \{1\}$, existe $1 \neq n_1 \in N_1$. Se $\mathscr{I}_{n_1} = \mathrm{id}_{N_1}$, então $x^{n_1} = x$, $\forall x \in N_1$, donde $n_1 \in Z(N_1) = \{1\}$, um absurdo. Assim, $M \neq \{1\}$. Se $\mathscr{I}_n \in \mathrm{Inn}(N_1)$, então $\mathscr{I}_n \in L$, pois $\mathscr{I}_n = n^{\alpha_1}$. Logo, $M \leq L$, e como $\mathrm{Inn}(N_1) \trianglelefteq \mathrm{Aut}(N_1)$, segue-se que $M \trianglelefteq L$. Suponhamos que exista $K \trianglelefteq L$ tal que $\{1\} < K < M$, logo existe $n \neq 1$ em N_1 tal que $n^{\alpha_1} \in K$. Considerando $N = \langle n^h \mid h \in H \rangle$, temos que $N \neq \{1\}$ (pois $n \in N$), $N \trianglelefteq H$ e $N \leq N_1$, consequentemente $N_1 = N$, já que N_1 é normal minimal em H. Dessa forma, como $K \trianglelefteq L$,

$$(n^h)^{\alpha_1} = (n^{\alpha_1})^{h^{\alpha_1}} \in K,\ \forall h \in H,$$

isto é, $M \leq K$ de modo que $M = K$, um absurdo. Com isso, concluímos que M é normal minimal em L. Agora, vamos calcular $C_L(M)$. Seja $h^{\alpha_1} \in C_L(M)$, então

$$h^{\alpha_1} n^{\alpha_1} = n^{\alpha_1} h^{\alpha_1},\ \forall n \in N_1,$$

isto é, $x^{hn} = x^{nh}$, para todos $x, n \in N_1$, ou melhor dizendo, $h^{-1}n^{-1}hn \in Z(N_1)$, para todos $x, n \in N_1$ ($h^{-1}n^{-1}hn \in N_1$, pois $N_1 \trianglelefteq H$). Como $Z(N_1) = \{1\}$, $n^h = n$, $\forall n \in N_1$, isto é, $h^{\alpha_1} = \mathrm{id}_{N_1}$. Portanto $C_L(M) = \{1\}$ donde M é não abeliano e é o único subgrupo normal minimal de L. Isto nos fornece que $Z(M) = \{1\}$ (pois $Z(M) \trianglelefteq_c M \trianglelefteq L$) donde M não é nilpotente, e, por conseguinte, $\Phi(L) = \{1\}$ (vide Teorema 1.5.5). Ou seja, L é um grupo primitivo monolítico, pela Proposição 2.1.6.

Para $r > 1$, definamos $\alpha_r : H \to \mathrm{Aut}(N_1)$ por

$$h^{\alpha_r} : x \mapsto ((x^{\phi_r})^h)^{\phi_r^{-1}} \qquad \text{sempre que} \quad h \in H,\ x \in N_1.$$

Seja $h \in H$. Dados $x_1, x_2 \in N_1$, temos

$$x_1 = x_2 \Leftrightarrow x_1^{\phi_r} = x_2^{\phi_r} \Leftrightarrow (x_1^{\phi_r})^h = (x_2^{\phi_r})^h \Leftrightarrow ((x_1^{\phi_r})^h)^{\phi_r^{-1}} = ((x_2^{\phi_r})^h)^{\phi_r^{-1}} \Leftrightarrow x_1^{h^{\alpha_r}} = x_2^{h^{\alpha_r}},$$

pois ϕ_r é um isomorfismo. Isto nos dá que h^{α_r} está bem definida e é injetiva. Além disso,

$$\begin{aligned}(x_1x_2)^{h^{\alpha_r}} &= (((x_1x_2)^{\phi_r})^h)^{\phi_r^{-1}} = ((x_1^{\phi_r}x_2^{\phi_r})^h)^{\phi_r^{-1}} = ((x_1^{\phi_r})^h(x_2^{\phi_r})^h)^{\phi_r^{-1}} \\ &= ((x_1^{\phi_r})^h)^{\phi_r^{-1}}((x_2^{\phi_r})^h)^{\phi_r^{-1}} = x_1^{h^{\alpha_r}}x_2^{h^{\alpha_r}},\end{aligned}$$

logo h^{α_r} é um homomorfismo. Dado $n \in N_1$, $n = x^{h^{\alpha_r}}$, onde $x = ((n^{\phi_r})^{h^{-1}})^{\phi_r^{-1}} \in N_1$, de modo que h^{α_r} é sobrejetiva. Portanto, h^{α_r} é, de fato, um automorfismo de N_1, e, assim,

α_r está bem definida. Também, dados $h_1, h_2 \in H$ e $x \in N_1$,

$$x^{h_1^{\alpha_r} h_2^{\alpha_r}} = (((x^{\phi_r})^{h_1})^{\phi_r^{-1}})^{h_2^{\alpha_r}} = (((((x^{\phi_r})^{h_1})^{\phi_r^{-1}})^{\phi_r})^{h_2})^{\phi_r^{-1}} = ((x^{\phi_r})^{h_1 h_2})^{\phi_r^{-1}} = x^{(h_1 h_2)^{\alpha_r}},$$

logo $(h_1 h_2)^{\alpha_r} = h_1^{\alpha_r} h_2^{\alpha_r}$ e α_r é um homomorfismo. Notemos que

$$\begin{aligned}\ker(\alpha_r) &= \{h \in H \mid h^{\alpha_r} = \mathrm{id}_{N_1}\} = \{h \in H \mid ((x^{\phi_r})^h)^{\phi_r^{-1}} = x,\ \forall x \in N_1\} \\ &= \{h \in H \mid (x^{\phi_r})^h = x^{\phi_r},\ \forall x \in N_1\} = C_H(N_r),\end{aligned}$$

pois ϕ_r é um isomorfismo. Agora, como $H = K_r N_1$, podemos escrever cada $h \in H$ como $h = uv$ com $u \in K_r$, $v \in N_1$, e, então, dado $x \in N_1$,

$$((x^{\phi_r})^h)^{\phi_r^{-1}} = ((x^{\phi_r})^u)^{\phi_r^{-1}} = x^u = (x^h)^{v^{-1}}, \tag{2.1}$$

onde a primeira igualdade vale pois N_1 centraliza N_r e a segunda porque ϕ_r é uma K_r-aplicação: assim, h^{α_r} é h^{α_1} seguido por um automorfismo interno de N_1 induzido por v^{-1}. Consequentemente,

$$h^{\alpha_1} \equiv \cdots \equiv h^{\alpha_k} \mod M \tag{2.2}$$

Além disso, provamos acima que $K_r \cap (N_1 \times N_r) = \{x x^{\phi_r} \mid x \in N_1\}$. Então, por (2.1), dado $n \in N_1$, visto que ϕ_r é um K_r-isomorfismo e N_r centraliza N_1,

$$x^{\mathscr{I}_n} = x^n = (x^n)^{n^{\phi_r}} = x^{n n^{\phi_r}} = ((x^{\phi_r})^{n n^{\phi_r}})^{\phi_r^{-1}} = x^{(n n^{\phi_r})^{\alpha_r}},$$

para todo $x \in N_1$, ou seja, $M \leq \mathrm{Im}(\alpha_r)$. Portanto, (2.2) nos dá que cada α_r tem imagem L. Por fim, vamos mostrar que $H \cong L_k$ (lembremos que $k \geq 2$ é o inteiro tal que os subgrupos normais minimais de H são $N_1, \ldots, N_k$). Definamos $\psi : H \to L_k$ por

$$h^{\psi} = (h^{\alpha_1}, \ldots, h^{\alpha_k}), \qquad \text{sempre que} \quad h \in H.$$

Temos que ψ está bem definida por (2.2) e, como cada α_i é um homomorfismo, segue-se facilmente que ψ também o é. O núcleo desse homomorfismo é a interseção dos núcleos dos α_i's, isto é, dos centralizadores $C_H(N_i)$ (com $i = 1, \ldots, k$). Esta interseção é um subgrupo normal de H, e, portanto, é trivial, pois, caso contrário, conteria algum N_i de modo que este seria abeliano, um absurdo. Com isso, concluímos que ψ é um homomorfismo injetivo de forma que $|H| \leq |L_k|$. Para obter que ψ é um isomorfismo, basta verificar que $|H| \geq |L_k|$. Pelo Lema 2.3.9, $\mathrm{soc}(H)$ é o produto direto interno de

$N_1, N_2, \ldots, N_k$. Sabemos que $N_1/Z(N_1) \cong \mathrm{Inn}(N_1) = M$, logo $N_1 \cong M$ e $|\mathrm{soc}(H)| = |M|^k$. Como $N_1 \cap N_2 \cdots N_k = \{1\}$, temos

$$|M|^k = |\mathrm{soc}(H)| = |N_1 N_2 \cdots N_k| = \frac{|N_1| \cdot |N_2 \cdots N_k|}{|N_1 \cap N_2 \cdots N_k|} = |M| \cdot |N_2 \cdots N_k|$$

donde $|N_2 \cdots N_k| = |M|^{k-1}$. Agora, afirmamos que $L/M \cong H/N_1C$, onde $C = C_H(N_1)$. De fato, pelo Teorema dos Isomorfismos, α_1 induz o isomorfismo $\overline{\alpha_1} : H/C \to L$ dado por $(hC)^{\overline{\alpha_1}} = h^{\alpha_1}$. Seja K a pré-imagem de M por $\overline{\alpha_1}$. Temos $N_1C/C \leq K$ e $|N_1C/C| = |N_1| = |M| = |K|$, logo $N_1C/C = K$. Consideremos $\theta = \overline{\alpha_1}\pi$, onde $\pi : L \to L/M$ é a projeção canônica. Assim,

$$\ker(\theta) = \{hC \in H/C \mid (hC)^{\overline{\alpha_1}} M = M\} = \{hC \in H/C \mid (hC)^{\overline{\alpha_1}} \in M\} = K = N_1C/C.$$

Pelo Teorema dos Isomorfismos,

$$\frac{L}{M} \cong \frac{H/C}{N_1C/C} \cong \frac{H}{N_1C}$$

donde a afirmação segue. Como $N_2 \cdots N_k \leq C$, obtemos que $|M|^{k-1} \leq |C|$. Além disso, pela Proposição 2.3.2, $L_k/M^k \cong L/M$. Daí,

$$|L_k| = |M|^k \left|\frac{L}{M}\right| = |M|^k \left|\frac{H}{N_1C}\right| = |M|^k \frac{|H|}{|N_1| \cdot |C|} \leq \frac{|M|^k}{|M| \cdot |M|^{k-1}} |H| = |H|,$$

isto é, $|H| \geq |L_k|$, como queríamos. Portanto, $H \cong L_k$.

Independentemente de N_1 ser abeliano, provamos que $H \cong L_k$ com $k \geq 2$, consequentemente $H/N_1 \cong L_{k-1}$. Ora, basta notar que se $\sigma : H \to L_k$ é um isomorfismo, então N_1^σ é normal minimal em L_k e σ induz um isomorfismo $\overline{\sigma} : H/N_1 \to L_k/N_1^\sigma$, a saber $hN_1 \mapsto h^\sigma N_1^\sigma$. Pela Proposição 2.3.4, obtemos que $L_k/N_1^\sigma \cong L_{k-1}$ donde $H/N_1 \cong L_{k-1}$. Portanto, $d(L_{k-1}) = d(H/N_1) \leq m$ e $d(L_k) = d(H) > m$. Sabemos que $d(L_k) \leq d(L_{k-1}) + 1$, logo $d(L_{k-1}) = m$, pois, caso contrário, teríamos

$$d(L_k) \leq d(L_{k-1}) + 1 \leq (m-1) + 1 = m,$$

um absurdo. Em resumo, temos

$$d(L_{k-1}) = m < d(L_k).$$

Pela definição da função f, isto significa que $k = f(L, m)$, e a prova do teorema está

completa. □

Observação 2.3.10. *Em ambos os casos de $m = 1$, temos que H é do tipo L_k para algum inteiro positivo k. De fato, se $H \cong C_p \times C_p$ para algum primo p, então $H \cong L_2$ com $L = C_p$. Mais ainda, $H \cong L_{f(L,1)}$, uma vez que*

$$d(L) = 1 < 2 = d(L^2) = d(L_2),$$

pelo Exemplo 2.2.2. Agora, no caso em que H é um grupo primitivo monolítico, basta considerar L sendo o próprio H de modo que $H = L_1$.

2.4 Cálculo da Função $f(L, m)$

Agora, descreveremos como a função f pode ser calculada. Aqui, L também denota um grupo primitivo monolítico não cíclico finito, com $M = \mathrm{soc}(L)$. O objetivo principal desta seção é demonstrar o Teorema B. Para isto, vamos começar com alguns lemas.

Lema 2.4.1. *Suponhamos que M é não abeliano e seja N um subgrupo normal não trivial de L_k contido em $\mathrm{soc}(L_k)$. Então N é um produto de alguns dos fatores M_i. Ademais, se $L_k/N \cong L$, então N é um produto de $k-1$ fatores M_i, e o conjunto $\mathscr{N}$ dos subgrupos normais de L_k contidos em $\mathrm{soc}(L_k)$ tais que o quociente é isomorfo a L tem cardinalidade k.*

Demonstração. Sabemos que $\mathrm{soc}(L_k) = M^k = M_1 \times \cdots \times M_k$, onde $M_i \cong M$, para cada $i = 1, \ldots, k$. Pelo Corolário 1.3.13, existe um grupo simples não abeliano S tal que $M \cong S^m$, para algum inteiro positivo m. Para cada $i = 1, \ldots, k$, escrevamos $M_i = S_{i1} \times \cdots \times S_{im}$.

Agora, seja $N \trianglelefteq L_k$ com $\{1\} \neq N \subseteq \mathrm{soc}(L_k)$. Temos que $\mathrm{soc}(L_k) = M^k \cong S^{mk}$, logo N é da forma

$$T_{11} \times \cdots \times T_{1m} \times T_{21} \times \cdots \times T_{2m} \times \cdots \times T_{k1} \times \cdots \times T_{km} = \prod_{i=1}^{k} \prod_{j=1}^{m} T_{ij},$$

onde cada T_{ij} é $\{1\}$ ou S_{ij} (vide [22, 3.3.12]). Afirmamos que se $T_{ij} = S_{ij}$ para algum par i, j, então $T_{il} = S_{il}$ para todo $l \in \{1, \ldots, m\}$. De fato, claramente,

$$N \cap M_i = T_{i1} \times \cdots \times T_{im}.$$

Além disso, $N \cap M_i \trianglelefteq L_k$, já que $N \trianglelefteq L_k$ e $M_i \trianglelefteq L_k$. Uma vez que existe j tal que $T_{ij} = S_{ij}$, obtemos $N \cap M_i \neq \{1\}$ donde $N \cap M_i = M_i$, pois M_i é normal minimal em L_k. Consequentemente, $M_i \subseteq N$ de modo que $T_{il} = S_{il}$ para todo $l \in \{1, \ldots, m\}$. Como N é um produto de alguns fatores S_{ij}, segue-se que N é um produto de alguns M_i's.

Com isso, temos que $|N| = |M|^r$, onde r é a quantidade de fatores do produto (notemos que $r \leq k$). Suponhamos que $L_k/N \cong L$. Então

$$|L_k| = |L_k/N| \cdot |N| = |L| \cdot |N|.$$

Por outro lado, a Proposição 2.3.2 nos fornece $L_k/M^k \cong L/M$ de modo que

$$|L_k| = |L_k/M^k| \cdot |M|^k = |L/M| \cdot |M|^k = |L| \cdot |M|^{k-1}.$$

Assim, $|N| = |M|^{k-1}$, e segue-se que $r = k-1$. Ou seja, N é um produto de $k-1$ fatores M_i.

Agora, seja K um produto de $k-1$ fatores M_i. Sem perda de generalidade, assumamos que $K = M_1 \cdots M_{k-1}$. Então $K \trianglelefteq L_k$ (pois cada fator M_i o é) e $K \leq M^k$. Considerando a k-ésima projeção $\psi_k : L_k \to L$, temos $L_k/K \cong L$. De fato, temos que ψ_k é um homomorfismo sobrejetivo. Se $(l_1, \ldots, l_k) \in \ker(\psi_k)$, então $l_k = (l_1, \ldots, l_k)^{\psi_k} = 1$. Dado que $(l_1, \ldots, l_k) \in L_k$, temos $Ml_1 = \cdots = Ml_k = M$ donde $l_1, \ldots, l_{k-1} \in M$, e, assim, $(l_1, \ldots, l_k) = (l_1, \ldots, l_{k-1}, 1) \in K$. Portanto, $\ker(\psi_k) = K$ e, pelo Teorema dos Isomorfismos, $L_k/K \cong L$. Com isso, concluímos que a cardinalidade de $\mathscr{N}$ é a quantidade de produtos de $k-1$ fatores diretos de M^k, ou seja, é k. Isto completa a prova do lema. □

Lema 2.4.2. *Sejam $g : G \to H$ e $h : G \to K$ homomorfismos sobrejetivos tais que $\ker(g) = \ker(h)$. Então existe um isomorfismo $\varphi : H \to K$ tal que $g\varphi = h$.*

Demonstração. Seja $N = \ker(g) = \ker(h)$. Pelo Teorema dos Isomorfismos, $g = \pi\widetilde{g}$ e $h = \pi\widetilde{h}$, onde $\pi : G \to G/N$ é a projeção canônica e $\widetilde{g} : G/N \to H$ e $\widetilde{h} : G/N \to K$ são os isomorfismos induzidos por g e h, respectivamente. Assim,

$$\pi = g\widetilde{g}^{-1} \;\Rightarrow\; h = \pi\widetilde{h} = g\widetilde{g}^{-1}\widetilde{h}.$$

Escolhendo $\varphi = \widetilde{g}^{-1}\widetilde{h}$, o lema segue. □

Lema 2.4.3. *Dado um homomorfismo sobrejetivo $\beta : L_k \to L/M$ tal que $\beta = \widetilde{\beta}\pi$, onde $\widetilde{\beta} : L_k \to L$ é um certo homomorfismo sobrejetivo e $\pi : L \to L/M$ é a projeção canônica,*

consideremos o conjunto $\mathscr{S}$ dos subgrupos normais N de L_k os quais são núcleos de homomorfismos sobrejetivos de L_k em L que, compostos com π, produzem β. A cardinalidade de $\mathscr{S}$ é k quando M é não abeliano; e é $(q^k-1)/(q-1)$ quando M é abeliano, sendo q o número de L-endomorfismos de M.

Demonstração. Pelo Teorema dos Isomorfismos, $L_k/\ker(\beta) \cong L/M$. Por outro lado, sabemos que $L_k/M^k \cong L/M$ (vide Proposição 2.3.2). Com isso, obtemos que $|\ker(\beta)| = |M|^k$ e, usando o Corolário 2.3.5, concluímos que $\ker(\beta) = M^k$.

Agora, seja $\mathscr{N} = \{T \trianglelefteq L_k \mid T \leq \mathrm{soc}(L_k) \text{ e } L_k/T \cong L\}$. Afirmamos que $\mathscr{S} = \mathscr{N}$. De fato, seja $N \in \mathscr{S}$, então $N = \ker(\beta^*)$, onde $\beta^* : L_k \to L$ é um homomorfismo sobrejetivo tal que $\beta^*\pi = \beta$. Isto nos fornece que $N \leq \mathrm{soc}(L_k)$ (pois $\ker(\beta) = M^k$), e pelo Teorema dos Isomorfismos, $L_k/N \cong L$. Portanto, $N \in \mathscr{N}$. Reciprocamente, seja $T \in \mathscr{N}$, logo $T \trianglelefteq L_k$, $T \leq \mathrm{soc}(L_k)$ e $L_k/T \cong L$. Por hipótese, $\beta = \widetilde{\beta}\pi$. Vamos então construir um homomorfismo sobrejetivo $\overline{\beta} : L_k \to L$ tal que $\ker(\overline{\beta}) = T$ e $\overline{\beta}\pi = \beta$. Para isso, vamos dividir em dois casos.

Caso 1. M não abeliano: notemos que $\ker(\widetilde{\beta}) \leq \mathrm{soc}(L_k)$ (pois $\ker(\beta) = \mathrm{soc}(L_k)$), $\ker(\widetilde{\beta}) \trianglelefteq L_k$ e $L_k/\ker(\widetilde{\beta}) \cong L$. Como na prova do Lema 2.4.1, $\ker(\widetilde{\beta}) = \ker(\psi_i)$ para algum $i \in \{1,\ldots,k\}$, onde $\psi_i : L_k \to L$ é a i-ésima projeção. E isto implica $\widetilde{\beta} = \psi_i\gamma$ para algum $\gamma \in \mathrm{Aut}(L)$, pelo Lema 2.4.2. Usando novamente o Lema 2.4.1, $T = \ker(\psi_j)$ para algum $j \in \{1,\ldots,k\}$. Notemos que $T = \ker(\psi_j\gamma)$, pois $\gamma \in \mathrm{Aut}(L)$. Afirmamos que

$$\psi_j\gamma\pi = \psi_i\gamma\pi.$$

De fato, sejam $x \in L_k$, $y = x^{\psi_i}$ e $z = x^{\psi_j}$. Pela definição de L_k, temos $My = Mz$. Logo $yz^{-1} \in M$. Agora, $M \trianglelefteq_c L$, já que $M = \mathrm{soc}(L)$; daí,

$$(yz^{-1})^\gamma \in M \;\Rightarrow\; y^\gamma(z^\gamma)^{-1} \in M \;\Rightarrow\; My^\gamma = Mz^\gamma \;\Rightarrow\; y^{\gamma\pi} = z^{\gamma\pi} \;\Rightarrow\; x^{\psi_i\gamma\pi} = x^{\psi_j\gamma\pi}.$$

Pela arbitrariedade de x, a afirmação segue. Portanto, considerando $\overline{\beta} = \psi_j\gamma$, temos $\ker(\overline{\beta}) = T$ e

$$\overline{\beta}\pi = \psi_j\gamma\pi = \psi_i\gamma\pi = \widetilde{\beta}\pi = \beta,$$

como queríamos. Nesse caso, a cardinalidade de $\mathscr{N}$ é k, pelo Lema 2.4.1.

Caso 2. M abeliano: notemos que M é um L-grupo abeliano (a ação é por conjugação), ou seja, M é um L-módulo. Dado que M é normal minimal em L, temos que M é um L-módulo simples. Notemos também que M^k é um L-módulo (com a ação de L em M^k dada por $(m_1,\ldots,m_k)^l = (m_1^l,\ldots,m_k^l)$, para cada $(m_1,\ldots,m_k) \in M^k$). Afirmamos que T é um L-submódulo maximal de M^k. De fato, T é um L-submódulo de M^k (pois

$T \trianglelefteq L_k$ e $T \leq \mathrm{soc}(L_k)$) e $|T| = |M|^{k-1}$ (vide prova do Lema 2.4.1). Agora, suponhamos que exista K um L-submódulo de M^k tal que $T < K < M^k$, e consideremos a seguinte L-série:

$$S : \{1\} < M < M^2 < \cdots < M^k.$$

Temos que S é uma L-série de composição, pois seus fatores são todos L-isomorfos a M, e, portanto são L-simples (vide Proposição 1.7.2). Pelo Teorema de Jordan-Hölder (Teorema 1.7.5), existe um refinamento

$$\{1\} < \cdots < T = H_0 < H_1 < \cdots < H_{r-1} < H_r = K < \cdots < M^k \quad (r \geq 1),$$

o qual é uma série de composição L-isomorfa a S de modo que os fatores são L-isomorfos a M. Então $|K/T| = |H_r/H_{r-1}| \cdots |H_1/H_0| = |M|^r$, o que implica

$$|K| = |K/T| \cdot |T| = |M|^r \cdot |M|^{k-1} = |M|^{r+k-1}.$$

Como $K < M^k$, temos $|M|^{r+k-1} = |K| < |M|^k$ donde $r + k - 1 < k$ e $r < 1$, um absurdo. Portanto, a afirmação segue. Usando a prova da Proposição 1.7.7, obtemos que existem $\lambda_1, \ldots, \lambda_k \in F = \mathrm{End}_L(M)$ não todos nulos, tais que

$$T = \{(m_1, \ldots, m_k) \in M^k \mid m_1^{\lambda_1} \cdots m_k^{\lambda_k} = 1\}.$$

Então, consideremos $\psi : L_k \to L$ definida por

$$((m_1, \ldots, m_k)h)^\psi = m_1^{\lambda_1} \cdots m_k^{\lambda_k} h,$$

sempre que $(m_1, \ldots, m_k) \in M^k$ e $h \in \mathrm{diag}(H^k)$ (lembremos que quando M é abeliano, $L_k = M^k \cdot \mathrm{diag}(H^k)$ - vide prova do Lema 2.3.3). Vamos mostrar que ψ é um homomorfismo sobrejetivo cujo núcleo é T. Com efeito, dados $(m_1, \ldots, m_k), (n_1, \ldots, n_k) \in M^k$ e $h, h' \in \mathrm{diag}(H^k)$, temos

$$\begin{aligned}
((m_1, \ldots, m_k)h \cdot (n_1, \ldots, n_k)h')^\psi &= ((m_1, \ldots, m_k)(n_1, \ldots, n_k)^{h^{-1}} \cdot hh')^\psi \\
&= ((m_1 n_1^{h^{-1}}, \ldots, m_k n_k^{h^{-1}}) \cdot hh')^\psi = (m_1 n_1^{h^{-1}})^{\lambda_1} \cdots (m_k n_k^{h^{-1}})^{\lambda_k} \cdot hh' \\
&= m_1^{\lambda_1} (n_1^{h^{-1}})^{\lambda_1} \cdots m_k^{\lambda_k} (n_k^{h^{-1}})^{\lambda_k} \cdot hh' \\
&= m_1^{\lambda_1} (n_1^{\lambda_1})^{h^{-1}} \cdots m_k^{\lambda_k} (n_k^{\lambda_k})^{h^{-1}} \cdot hh' \quad (\lambda_1, \ldots, \lambda_k \in \mathrm{End}_L(M)) \\
&= m_1^{\lambda_1} \cdots m_k^{\lambda_k} (n_1^{\lambda_1} \cdots n_k^{\lambda_k})^{h^{-1}} \cdot hh' \quad (M \text{ é abeliano}) \\
&= m_1^{\lambda_1} \cdots m_k^{\lambda_k} h \cdot n_1^{\lambda_1} \cdots n_k^{\lambda_k} h' = ((m_1, \ldots, m_k)h)^\psi \cdot ((n_1, \ldots, n_k)h')^\psi.
\end{aligned}$$

Assim, ψ é um homomorfismo de grupos. Se $(m_1,\dots,m_k)h \in \ker(\psi)$, então $m_1^{\lambda_1}\cdots m_k^{\lambda_k}h = 1$ donde $m_1^{\lambda_1}\cdots m_k^{\lambda_k} = h^{-1} \in M \cap H = \{1\}$. Logo $h = m_1^{\lambda_1}\cdots m_k^{\lambda_k} = 1$, ou seja, $(m_1,\dots,m_k)h \in T$. Por outro lado, $T \leq \ker(\psi)$, e, portanto, $\ker(\psi) = T$. Por fim, seja $l \in L = MH$, então existem $m \in M$ e $h \in H$ tais que $l = mh$. Tomando um λ_i não nulo ($1 \leq i \leq k$), temos que este é um isomorfismo (vide Lema de Schur – Lema 1.7.6), logo $m = m_i^{\lambda_i}$ para algum $m_i \in M$. Dessa forma,

$$l = mh = m_i^{\lambda_i}h = ((1,\dots,1,m_i,1,\dots,1)h)^{\psi}.$$

Isto é, ψ é sobrejetiva.

Agora, da mesma forma, existem $\lambda_1',\dots,\lambda_k' \in F$ tais que

$$\ker(\widetilde{\beta}) = \{(m_1,\dots,m_k) \in M^k \mid m_1^{\lambda_1'}\cdots m_k^{\lambda_k'} = 1\},$$

e existe um homomorfismo sobrejetivo $\psi' : L_k \to L$ tal que $\ker(\widetilde{\beta}) = \ker(\psi')$, a saber

$$((m_1,\dots,m_k)h)^{\psi'} = m_1^{\lambda_1'}\cdots m_k^{\lambda_k'}h,$$

sempre que $(m_1,\dots,m_k) \in M^k$ e $h \in \mathrm{diag}(H^k)$. Pelo Lema 2.4.2, $\widetilde{\beta} = \psi'\gamma$ para algum $\gamma \in \mathrm{Aut}(L)$. Dado $x = (m_1,\dots,m_k)h \in L_k$, notemos que

$$Mx^{\psi'} = M(m_1^{\lambda_1'}\cdots m_k^{\lambda_k'}h) = Mh = M(m_1^{\lambda_1}\cdots m_k^{\lambda_k}h) = Mx^{\psi}.$$

Desse modo, com o mesmo argumento do Caso 1, escolhendo $\overline{\beta} = \psi\gamma$, obtemos que $\ker(\overline{\beta}) = T$ e $\overline{\beta}\pi = \beta$. Isto conclui o Caso 2.

Portanto, $\mathscr{S} = \mathscr{N}$. No caso M não abeliano (Caso 1), vimos que $|\mathscr{N}| = k$, logo $|\mathscr{S}| = k$. No caso M abeliano (Caso 2), mostramos que todo elemento de $\mathscr{N}$ é um L-submódulo maximal de M^k. Mais ainda, mostramos que se R é um L-submódulo maximal de M^k, então existe um homomorfismo sobrejetivo de L_k em L cujo núcleo é R. Consequentemente, $R \trianglelefteq L_k$ e, pelo Teorema dos Isomorfismos, $L_k/R \cong L$. Ou seja, $\mathscr{N}$ é o conjunto dos L-submódulos maximais de M^k. Pela Proposição 1.7.7, concluímos que

$$|\mathscr{S}| = |\mathscr{N}| = (q^k - 1)/(q - 1),$$

onde $q = |\mathrm{End}_L(M)|$. Isto completa a prova do lema. □

Lema 2.4.4. *Sejam G um grupo e $N_1,\dots,N_k$ subgrupos normais de G. Se $N_i \cdot \bigcap_{\substack{j=1\\ j\neq i}}^{k} N_j = G$*

para todo $i \in \{1,\ldots,k\}$, *então*

$$\frac{G}{N_1 \cap \cdots \cap N_k} \cong \frac{G}{N_1} \times \cdots \times \frac{G}{N_k}.$$

Demonstração. A prova será feita por indução sobre k. Consideremos $k = 2$, ou seja, $G = N_1N_2 = N_2N_1$. Seja $\varphi : G \to G/N_1 \times G/N_2$ dada por

$$(xy)^\varphi = (N_1y, N_2x), \qquad \text{sempre que} \quad x \in N_1 \text{ e } y \in N_2.$$

Afirmamos que φ é um homomorfismo de grupos bem-definido e sobrejetivo. De fato, sejam $x,u \in N_1$ e $y,v \in N_2$ tais que $xy = uv$. Então $u^{-1}x = vy^{-1} \in N_1 \cap N_2$. Daí, $vy^{-1} \in N_1$ nos dá que $N_1v = N_1y$. E $u^{-1}x \in N_2$ implica $xu^{-1} = (u^{-1}x)^{x^{-1}} \in N_2$ (pois $N_2 \trianglelefteq G$) donde $N_2x = N_2u$. Assim, $(N_1y, N_2x) = (N_1v, N_2u)$, ou seja, $(xy)^\varphi = (uv)^\varphi$ e φ está bem definida. Seja $(N_1g, N_2h) \in G/N_1 \times G/N_2$ arbitrário. Dado que $G = N_1N_2 = N_2N_1$, existem $x,u \in N_1$ e $y,v \in N_2$ tais que $g = xy$ e $h = vu$. Logo $(N_1g, N_2h) = (N_1xy, N_2vu) = (N_1y, N_2u) = (uy)^\varphi$. Portanto, φ é sobrejetiva. Agora, dados $x,u \in N_1$ e $y,v \in N_2$, temos

$$\begin{aligned}(xy \cdot uv)^\varphi &= (xu^{y^{-1}} \cdot yv)^\varphi = (N_1yv, N_2xu^{y^{-1}}) = (N_1yv, N_2xyuy^{-1}) \\ &= (N_1yv, N_2x \cdot N_2y \cdot N_2u \cdot N_2y^{-1}) = (N_1yv, N_2xu) \\ &= (N_1y, N_2x) \cdot (N_1v, N_2u) = (xy)^\varphi \cdot (uv)^\varphi.\end{aligned}$$

Com isso, φ é um homomorfismo, e a afirmação segue. Temos que

$$\ker(\varphi) = \{xy \in N_1N_2 = G \mid x \in N_2 \text{ e } y \in N_1\} = N_1 \cap N_2.$$

Pelo Teorema dos Isomorfismos,

$$\frac{G}{N_1 \cap N_2} \cong \frac{G}{N_1} \times \frac{G}{N_2}.$$

Isto é, o caso $k = 2$ é verdadeiro.

Agora, suponhamos $k > 2$ e sejam $A_1 = N_1$ e $A_2 = N_2 \cap \cdots \cap N_k$. Dado $i \in \{2,\ldots,k\}$, notemos que $N_i \cdot \bigcap_{\substack{j=2 \\ j\neq i}}^{k} N_j = G$, pois por hipótese $N_i \cdot \bigcap_{\substack{r=1 \\ r\neq i}}^{k} N_r = G$, e

$\bigcap_{\substack{r=1\\ r\neq i}}^{k} N_r \subseteq \bigcap_{\substack{j=2\\ j\neq i}}^{k} N_j$. Consequentemente, por indução, obtemos que

$$\frac{G}{A_2} \cong \frac{G}{N_2} \times \cdots \times \frac{G}{N_k}.$$

Usando o caso $k = 2$ (já que $A_1 A_2 = G$), segue-se que

$$\frac{G}{N_1 \cap \cdots \cap N_k} = \frac{G}{A_1 \cap A_2} \cong \frac{G}{A_1} \times \frac{G}{A_2} \cong \frac{G}{N_1} \times \cdots \times \frac{G}{N_k}.$$

Portanto, pelo Princípio de Indução Finita, o lema segue. □

Com isso, vamos então provar o Teorema B.

Teorema B. *Se $m \geq d(L)$, então*

$$f(m) = 1 + \begin{cases} \phi_L(m)/|\Gamma_L|\phi_{L/M}(m) & \text{se } M' = M, \\ \log_q(1 + (q-1)\phi_L(m)/|\Gamma_L|\phi_{L/M}(m)) & \text{se } M' = \{1\}, \end{cases}$$

sendo $q = |\mathrm{End}_L(M)|$.

Demonstração. Seja F um grupo livre de posto m (vide Teorema 1.8.2). Dado um homomorfismo sobrejetivo $\beta : F \to L/M$, consideremos o conjunto $\mathscr{R}$ definido no Lema 2.3.7 (o conjunto dos subgrupos normais N de F os quais são núcleos de homomorfismos sobrejetivos de F em L que, compostos com a projeção canônica $\pi : L \to L/M$, produzem β), e seja $R = \bigcap_{N\in\mathscr{R}} N$. Sabemos do Lema 2.3.7 que $\mathscr{R}$ é finito e sua cardinalidade não depende de β. Suponhamos $R = N_1 \cap \cdots \cap N_k$, onde k é minimal com esta propriedade, e vamos mostrar que $F/R \cong L_k$. Lembremos que dado $i \in \{1, \ldots, k\}$, $N_i = \ker(\gamma_i)$ com $\gamma_i : F \to L$ um homomorfismo sobrejetivo tal que $\gamma_i \pi = \beta$, onde $\pi : L \to L/M$ é a projeção canônica. Se $k = 1$, basta usar o Teorema dos Isomorfismos em γ_1. Assim, assumamos $k > 1$. Notemos que $\gamma_1\pi = \cdots = \gamma_k\pi = \beta$ implica $x^{\gamma_1} \equiv \cdots \equiv x^{\gamma_k} \mod M$ para todo $x \in F$. Então, definamos $\psi_k : F \to L_k$ por

$$x^{\psi_k} = (x^{\gamma_1}, \ldots, x^{\gamma_k}), \qquad \text{sempre que} \quad x \in F.$$

Vamos mostrar que ψ_k é um homomorfismo. Com efeito, dados $x, y \in F$,

$$\begin{aligned} (xy)^{\psi_k} &= ((xy)^{\gamma_1}, \ldots, (xy)^{\gamma_k}) = (x^{\gamma_1}y^{\gamma_1}, \ldots, x^{\gamma_k}y^{\gamma_k}) \\ &= (x^{\gamma_1}, \ldots, x^{\gamma_k}) \cdot (y^{\gamma_1}, \ldots, y^{\gamma_k}) = x^{\psi_k} \cdot y^{\psi_k}. \end{aligned}$$

Agora, $\ker(\psi_k) = N_1 \cap \cdots \cap N_k = R$. Pelo Teorema dos Isomorfismos,

$$F/R \cong \mathrm{Im}(\psi_k) \leq L_k.$$

Afirmamos que ψ_k é sobrejetiva. De fato, dado $H \leq F$, vamos denotar $H(N_1 \cap N_2)/(N_1 \cap N_2)$ por $\widetilde{H}$ (observamos que este é finito, haja vista que F/N_1 e F/N_2 o são). Agora, temos que $\{1\} \neq N_1N_2/N_1$, pois, caso contrário, $N_2 \subseteq N_1$ e $N_1 \cap \cdots \cap N_k = N_2 \cap \cdots \cap N_k$, contradizendo a minimalidade de k. Daí, $\{1\} \neq N_1N_2/N_1 \trianglelefteq F/N_1 \cong L$. Uma vez que L é monolítico ($\mathrm{soc}(L) = M$), segue-se que

$$M \cong \mathrm{soc}(F/N_1) \subseteq N_1N_2/N_1.$$

Por outro lado, $N_1N_2/N_1 \cong N_2/N_1 \cap N_2 = \widetilde{N_2}$ donde $|\widetilde{N_2}| \geq |M|$. Considerando $\psi_2 : F \to L_2$ ($\psi_2 : x \mapsto (x^{\gamma_1}, x^{\gamma_2})$, sempre que $x \in F$), temos

$$\widetilde{F} = F/N_1 \cap N_2 = F/\ker(\psi_2) \cong \mathrm{Im}(\psi_2)$$

de modo que

$$|L_2| \geq |\widetilde{F}| = |\widetilde{N_2}| \cdot |\widetilde{F}/\widetilde{N_2}| = |\widetilde{N_2}| \cdot |L| \geq |M| \cdot |L| = |M| \cdot |M| \cdot |L/M| = |L_2|,$$

pois

$$\widetilde{F}/\widetilde{N_2} = \frac{F/N_1 \cap N_2}{N_2/N_1 \cap N_2} \cong F/N_2 \cong L$$

e $L_2/M^2 \cong L/M$ (vide Proposição 2.3.2). Assim, $|\widetilde{N_2}| \cdot |L| = |M| \cdot |L|$ donde $|\widetilde{N_2}| = |M|$. Poderíamos ter feito esse argumento com índices $i \neq j$ em $\{1,\ldots,k\}$ arbitrários, ou seja, $|\widetilde{N_i}| = |M|$ para todo $i \in \{1,\ldots,k\}$. Então, como

$$\widetilde{N_2} = N_2/N_1 \cap N_2 \cong N_1N_2/N_1$$

e $N_1N_2/N_1 \supseteq \mathrm{soc}(F/N_1) \cong M$, obtemos que $N_1N_2/N_1 = \mathrm{soc}(F/N_1)$, como também $N_iN_j/N_i = \mathrm{soc}(F/N_i)$ para todos $i \neq j$ em $\{1,\ldots,k\}$. Isto nos fornece que $N_iN_j \supseteq N_l$, para todo $l \in \{1,\ldots,k\}$, donde

$$N_1 \cdots N_k = N_iN_j$$

para todos $i \neq j$ em $\{1,\ldots,k\}$. Agora, temos que $N_1(N_2 \cap \cdots \cap N_k) = N_1 \cdots N_k$. Com efeito, sejam $S = N_1 \cdots N_k$ e $T = N_1(N_2 \cap \cdots \cap N_k)$. Assim, $T \neq N_1$, pois, caso contrário, $N_2 \cap \cdots \cap N_k \subseteq N_1$ e $N_1 \cap \cdots \cap N_k = N_2 \cap \cdots \cap N_k$, contradizendo a

minimalidade de k. Daí, $\{1\} \neq T/N_1 \trianglelefteq F/N_1 \cong L$ donde

$$S/N_1 = N_1N_2/N_1 = \mathrm{soc}(F/N_1) \subseteq T/N_1$$

e $S \subseteq T$. Como $T \subseteq S$, obtemos que $S = T$. Esse argumento pode ser feito com outros índices, isto é, $N_i \cdot \bigcap_{\substack{j=1 \\ j\neq i}}^{k} N_j = S$. Pelo Lema 2.4.4,

$$\frac{S}{N_1 \cap \cdots \cap N_k} \cong \frac{S}{N_1} \times \cdots \times \frac{S}{N_k}.$$

Além disso, $S/N_i = N_1N_i/N_i = \mathrm{soc}(F/N_i) \cong M$, logo

$$\frac{S}{N_1 \cap \cdots \cap N_k} \cong M^k.$$

Com isso,

$$\frac{F}{S} = \frac{F}{N_1N_2} \cong \frac{F/N_1}{N_1N_2/N_1} = \frac{F/N_1}{\mathrm{soc}(F/N_1)} \cong \frac{L}{\mathrm{soc}(L)} = \frac{L}{M}$$

de modo que

$$\left|\frac{F}{R}\right| = \left|\frac{F}{N_1 \cap \cdots \cap N_k}\right| = [F : S] \cdot [S : N_1 \cap \cdots \cap N_k] = [L : M] \cdot |M|^k = |L_k|,$$

pois $L_k/M^k \cong L/M$ (vide Proposição 2.3.2). Portanto,

$$|F/R| = |\mathrm{Im}(\psi_k)| \leq |L_k| = |F/R|$$

donde ψ_k é sobrejetiva e $F/R \cong L_k$. Dessa forma, a afirmação segue.

Agora, consideremos $I = \{i \in \mathbb{Z}_+ \mid F \text{ admite um quociente isomorfo a } L_i\} \neq \varnothing$, e seja $i \in I$. Então existe $T \trianglelefteq F$ tal que $F/T \cong L_i$, ou seja, existe $\varphi : F/T \to L_i$ um isomorfismo. Dado $j \in \{1, \ldots, i\}$, consideremos a projeção na j-ésima coordenada $\pi_j : L_i \to L$, e notemos que $\varphi\pi_j\pi$ (onde $\pi : L \to L/M$ é a projeção canônica) não depende de j, pela definição de L_i. Assim, sendo $\pi_T : F \to F/T$ a projeção canônica, temos que

$$\pi_T\varphi\pi_1\pi = \cdots = \pi_T\varphi\pi_i\pi = \beta_i,$$

com $\beta_i : F \to L/M$ um homomorfismo sobrejetivo. Seja $\mathscr{R}_{\beta_i}$ e $R_{\beta_i} = \bigcap_{N\in\mathscr{R}_{\beta_i}} N$ como visto anteriormente, logo existe $k_i \leq |\mathscr{R}_{\beta_i}| = \phi_L(m)/|\Gamma_L|\phi_{L/M}(m)$ (vide Lema 2.3.7) tal que $F/R_{\beta_i} \cong L_{k_i}$. Para cada $j \in \{1, \ldots, i\}$, $N_j := \ker(\pi_T\varphi\pi_j) \in \mathscr{R}_{\beta_i}$. Afirmamos que $T = N_1 \cap \cdots \cap N_i$. De fato, se $x \in N_1 \cap \cdots \cap N_i$, então $((Tx)^{\varphi})^{\pi_j} = 1$ para

todo $j \in \{1,\ldots,i\}$, o que implica $(Tx)^{\varphi} = 1_{L_i}$, e, então, $Tx = T$ (já que φ é um isomorfismo), isto é, $x \in T$. Reciprocamente, se $x \in T$, então $x^{\pi_T\varphi\pi_j} = T^{\varphi\pi_j} = 1$ para todo $j \in \{1,\ldots,i\}$, logo $x \in N_1 \cap \cdots \cap N_k$. Desse modo, a afirmação segue. Com isso,

$$T \supseteq R_{\beta_i} \quad \text{e} \quad F/T \cong \frac{F/R_{\beta_i}}{T/R_{\beta_i}}.$$

Consequentemente,

$$|L_i| = |F/T| \leq |F/R_{\beta_i}| = |L_{k_i}|$$

de modo que $|M|^i \cdot |L/M| \leq |M|^{k_i} \cdot |L/M|$ e $i \leq k_i$. Portanto, obtemos um conjunto $J = \{k_i \mid i \in I\}$ de cotas superiores para o conjunto I. Haja vista que cada $k_i \leq \phi_L(m)/|\Gamma_L|\phi_{L/M}(m)$, segue-se que J possui um maior elemento, digamos k (observamos que existe $\beta : F \to L/M$ um homomorfismo sobrejetivo com $\beta = \gamma\pi$, onde $\gamma : F \to L$ é um homomorfismo sobrejetivo e $\pi : L \to L/M$ é a projeção canônica. E $F/R_\beta \cong L_k$). Temos

$$d(L_k) = d(F/R_\beta) \leq d(F) \leq m.$$

Se $d(L_{k+1}) \leq m$, então existiria $\theta : F \to L_{k+1}$ um homomorfismo sobrejetivo (pois F é livre de posto m – vide Observação 1.8.4) de modo que $F/\ker(\theta) \cong L_{k+1}$ e $k+1 \leq k$, pela maximalidade de k, o que seria um absurdo. Portanto, $d(L_{k+1}) > m$, e isto nos dá que $f(m) = k+1$.

Por fim, notemos que β induz um homomorfismo sobrejetivo $\overline{\beta} : F/R_\beta \cong L_k \to L/M$ ($(R_\beta x)^{\overline{\beta}} = x^\beta$, para cada $x \in F$), pois $R_\beta \subseteq \ker(\gamma) \subseteq \ker(\beta)$. Assim, vamos estabelecer uma bijeção entre os conjuntos $\mathscr{R}_\beta$ e $\mathscr{S}_{\overline{\beta}}$ (vide Lema 2.4.3). Definamos $\alpha : \mathscr{R}_\beta \to \mathscr{S}_{\overline{\beta}}$ por

$$N^\alpha = N/R_\beta, \qquad \text{sempre que} \quad N \in \mathscr{R}_\beta.$$

Vamos verificar que α, de fato, está bem definida. Seja $N \in \mathscr{R}_\beta$, então $N = \ker(\eta)$ com $\eta : F \to L$ um homomorfismo sobrejetivo tal que $\eta\pi = \beta$. Temos que $R_\beta \subseteq N$ de modo que existe $\delta : F/R_\beta \to L$ um homomorfismo sobrejetivo (a saber, $(R_\beta x)^\delta = x^\eta$, para cada $x \in F$). Agora, sendo $\pi_{R_\beta} : F \to F/R_\beta$ a projeção canônica, temos $(\pi_{R_\beta})\delta = \eta$ donde

$$(\pi_{R_\beta})\delta\pi = \eta\pi = \beta.$$

Se $x \in F$, então

$$(R_\beta x)^{\delta\pi} = x^{(\pi_{R_\beta})\delta\pi} = x^\beta = (R_\beta x)^{\overline{\beta}}.$$

Portanto, $\delta\pi = \overline{\beta}$ e $\ker(\delta) = N/R_\beta$. Com isso, $N/R_\beta \in \mathscr{S}_{\overline{\beta}}$, e α está bem definida. Claramente, α é injetiva. Mostremos que α é sobrejetiva. Com efeito, seja $\overline{N} \in \mathscr{S}_{\overline{\beta}}$ arbitrário. Temos que $\overline{N} = \ker(\delta)$, onde $\delta : F/R_\beta \to L$ é um homomorfismo sobrejetivo tal que $\delta\pi = \overline{\beta}$. Pelo Teorema da Correspondência, $\overline{N} = N/R_\beta$ com $N \trianglelefteq F$. Temos que $N \in \mathscr{R}_\beta$. De fato, seja $\eta = (\pi_{R_\beta})\delta$, então

$$\eta\pi = (\pi_{R_\beta})\delta\pi = (\pi_{R_\beta})\overline{\beta} = \beta.$$

E

$$\ker(\eta) = \{x \in F \mid (R_\beta x)^\eta = 1\} = N,$$

pois $N/R_\beta = \overline{N} = \ker(\delta)$. Daí,

$$N^\alpha = N/R_\beta = \overline{N},$$

e, então, α é sobrejetiva. Portanto, α é uma bijeção. Usando os Lemas 2.3.7 e 2.4.3, obtemos que

$$\frac{\phi_L(m)}{|\Gamma_L|\phi_{L/M}(m)} = |\mathscr{R}_\beta| = |\mathscr{S}_{\overline{\beta}}| = \begin{cases} k & \text{se } M' = M, \\ (q^k - 1)/(q-1) & \text{se } M' = \{1\}, \end{cases}$$

sendo $q = |\mathrm{End}_L(M)|$. Haja vista que $k = f(m) - 1$, o teorema segue. □

Proposição 2.4.5. *Se M é abeliano, então*

$$|\Gamma_L| = (q-1)\omega,$$

onde $q = |\mathrm{End}_L(M)|$ e ω é o número de complementos para M em L.

Demonstração. Se $\gamma \in \Gamma_L$, então a restrição de γ a M é um elemento de $\mathrm{End}_L(M)$, pois $M \trianglelefteq_c L$, e dados $m \in M$ e $l \in L$,

$$(m^l)^\gamma = (l^{-1}ml)^\gamma = (l^\gamma)^{-1}m^\gamma l^\gamma = l^{-1}n^{-1}m^\gamma nl = l^{-1}m^\gamma l = (m^\gamma)^l,$$

onde $l^\gamma = nl$ com $n \in M$ (já que $\gamma \in \Gamma_L$), e usamos a hipótese de M ser abeliano. Observamos que γ leva um complemento de M em outro complemento de M.

Agora, fixemos um complemento H de M em L (lembremos que existe pelo menos um, haja vista que L é primitivo monolítico com $M = \mathrm{soc}(L)$ abeliano). Seja K outro complemento, então

$$K = \{hh^\psi \mid h \in H\},$$

para alguma função $\psi : H \to M$. De fato, dado $h \in H$, existem $\kappa \in K$ e $n \in M$ tais que $h = \kappa n$ (pois $L = KM$), logo $hm = \kappa \in K$ com $m = n^{-1}$, ou seja, existe $m \in M$ tal que $hm \in K$. Mais ainda, se $\overline{m} \in M$ é tal que $h\overline{m} \in K$, então

$$\overline{m}^{-1}m = (h\overline{m})^{-1}(hm) \in K \cap M = \{1\}$$

donde $m = \overline{m}$. Portanto, dado $h \in H$, existe um único $m_h \in M$ tal que $hm_h \in K$. Assim, ψ levando h em m_h é uma função bem-definida tal que $K = \{hh^\psi \mid h \in H\}$.

Dados $h_1, h_2 \in H$, temos

$$h_1 h_1^\psi h_2 h_2^\psi = h_1 h_2 (h_1^\psi)^{h_2} h_2^\psi$$

de modo que

$$(h_1 h_2)^\psi = (h_1^\psi)^{h_2} h_2^\psi.$$

Uma função com esta propriedade é dita é um *cociclo*. Então, reciprocamente, se $\psi : H \to M$ é um cociclo, esta define um complemento para M em L. Com efeito, consideremos $K = \{hh^\psi \mid h \in H\}$. Temos

$$1^\psi = (1 \cdot 1)^\psi = (1^\psi)^1 \cdot 1^\psi = 1^\psi \cdot 1^\psi$$

de maneira que $1^\psi = 1$ e $1 = 1 \cdot 1^\psi \in K$. Também,

$$h_1 h_1^\psi h_2 h_2^\psi = h_1 h_2 (h_1^\psi)^{h_2} h_2^\psi = h_1 h_2 (h_1 h_2)^\psi \in K,$$

para todos $h_1, h_2 \in H$. Portanto, $K \leq L$. Além disso, dado $l \in L$, existem $h \in H$ e $m \in M$ tais que $l = hm = (hh^\psi)((h^\psi)^{-1}m) \in KM$. Isto é, $L = KM$. Por fim, se $h \in H$ é tal que $hh^\psi \in M$, então existe $m \in M$ com $hh^\psi = m$ de forma que

$$h = m(h^\psi)^{-1} \in H \cap M = \{1\}.$$

Consequentemente, $h = 1$ e $h^\psi = 1$ donde $K \cap M = \{1\}$. Com isso, a função

$$\begin{aligned} \alpha : \{\psi : H \to M \mid \psi \text{ é um cociclo}\} &\longrightarrow \{\text{Complementos para } M \text{ em } L\} \\ \psi &\longmapsto K_\psi = \{hh^\psi \mid h \in H\} \end{aligned}$$

é bem-definida e sobrejetiva. Se ψ_1 e ψ_2 são dois cociclos tais que $K_{\psi_1} = K_{\psi_2}$, então

dado $h \in H$, temos $hh^{\psi_1} = \overline{h}\,\overline{h}^{\psi_2}$, para algum $\overline{h} \in H$, de maneira que

$$\overline{h}^{-1}h = \overline{h}^{\psi_2}(h^{\psi_1})^{-1} \in H \cap M = \{1\},$$

e, por conseguinte, $h = \overline{h}$ e $h^{\psi_1} = h^{\psi_2}$. Pela arbitrariedade de h, concluímos que $\psi_1 = \psi_2$ e α é injetiva. Portanto, o número de cociclos de H em M é ω.

Agora, seja C denotando o conjunto dos cociclos de H em M, e consideremos $\beta : C \times \mathrm{End}_L(M)^* \to \Gamma_L$ dada por

$$(\psi, \theta)^\beta = \gamma_{\psi,\theta} : L \to L, \qquad \text{sempre que} \quad \psi \in C,\ \theta \in \mathrm{End}_L(M)^*,$$

onde

$$(hm)^{\gamma_{\psi,\theta}} = hh^\psi m^\theta, \qquad \text{para todos} \quad h \in H,\ m \in M.$$

Vamos primeiro mostrar que $\gamma_{\psi,\theta} \in \Gamma_L$. Dados $h_1, h_2 \in H$ e $m_1, m_2 \in M$, temos

$$(h_1m_1h_2m_2)^{\gamma_{\psi,\theta}} = (h_1h_2m_1^{h_2}m_2)^{\gamma_{\psi,\theta}} = h_1h_2(h_1^\psi)^{h_2}h_2^\psi(m_1^\theta)^{h_2}m_2^\theta$$

e

$$(h_1m_1)^{\gamma_{\psi,\theta}}(h_2m_2)^{\gamma_{\psi,\theta}} = h_1h_1^\psi m_1^\theta h_2h_2^\psi m_2^\theta = h_1h_2(h_1^\psi)^{h_2}(m_1^\theta)^{h_2}h_2^\psi m_2^\theta,$$

que é igual a expressão anterior, pois M é abeliano. Assim, $\gamma_{\psi,\theta}$ é um homomorfismo. Se $hm \in \ker(\gamma_{\psi,\theta})$, então $hh^\psi m^\theta = 1$ de modo que $h = 1$ e $m^\theta = 1$. Uma vez que $\theta \in \mathrm{End}_L(M)^*$, segue-se do Lema de Schur (Lema 1.7.6) que $m = 1$, ou seja, $\ker(\gamma_{\psi,\theta}) = \{1\}$ e $\gamma_{\psi,\theta}$ é um automorfismo de L. Por fim, notemos que

$$M(hm)^{\gamma_{\psi,\theta}} = Mhh^\psi m^\theta = Mh = Mhm,$$

para todos $h \in H$ e $m \in M$, logo $\gamma_{\psi,\theta}$ age trivialmente em L/M. Portanto, β está bem definida. Afirmamos que β é uma bijeção. De fato, sejam $(\psi_1, \theta_1), (\psi_2, \theta_2) \in C \times \mathrm{End}_L(M)^*$ tais que $\gamma_{\psi_1,\theta_1} = \gamma_{\psi_2,\theta_2}$. Então,

$$hh^{\psi_1}m^{\theta_1} = hh^{\psi_2}m^{\theta_2},$$

para todos $h \in H$ e $m \in M$. Escolhendo $h = 1$, obtemos $m^{\theta_1} = m^{\theta_2}$, para todo $m \in M$, donde $\theta_1 = \theta_2$. Por outro lado, escolhendo $m = 1$ e usando que $M \cap H = \{1\}$, obtemos que $\psi_1 = \psi_2$. Ou seja, β é injetiva. Agora, seja $\gamma \in \Gamma_L$. Consideremos θ a restrição de γ a M (como visto no início da demonstração) e ψ o cociclo associado ao complemento H^γ. Dado $h \in H$, temos $h^\gamma \in Mh = hM$ donde $h^\gamma = hm$ com $m \in M$. Mas $h^\gamma = \overline{h}\,\overline{h}^\psi$

para algum $\overline{h} \in H$, logo $hm = \overline{h}\,\overline{h}^{\psi}$ e $h = \overline{h}$ (pois $H \cap M = \{1\}$). Isto é, dados $h \in H$ e $m \in M$,

$$(hm)^{\gamma} = h^{\gamma}m^{\gamma} = hh^{\psi}m^{\theta} = (hm)^{\gamma_{\psi,\theta}}.$$

Por conseguinte, $\gamma = \gamma_{\psi,\theta} = (\psi,\theta)^{\beta}$ e β é sobrejetiva. A afirmação segue, e, portanto,

$$|\Gamma_L| = |\mathrm{End}_L(M)^*| \cdot |C| = (q-1)\omega,$$

como queríamos demonstrar. □

Observação 2.4.6. *Para M abeliano, Gaschütz provou ([13, Teorema 2]) que*

$$\phi_L(m)/\phi_{L/M}(m) = |M|^m - \omega,$$

sendo que ω é o número de complementos para M em L. Desse modo, pelo Teorema B e pela Proposição 2.4.5,

$$f(m) = 1 + \log_q(|M|^m/\omega).$$

Vamos finalizar esta seção com dois exemplos acerca do cálculo da função f.

Exemplo 2.4.7. *Dado G um grupo, lembremos que $\phi_G(m)$ é a cardinalidade do conjunto $\mathscr{S}$ de m-uplas $(g_1,\ldots,g_m) \in G^m$ tais que $\langle g_1,\ldots,g_m\rangle = G$. Notemos que $\mathrm{Aut}(G)$ age naturalmente em $\mathscr{S}$ por*

$$((g_1,\ldots,g_m),\varphi) \mapsto (g_1^{\varphi},\ldots,g_m^{\varphi}).$$

Esta ação é semirregular (isto significa que os estabilizadores pontuais são triviais): o estabilizador de qualquer $(g_1,\ldots,g_m) \in \mathscr{S}$ em $\mathrm{Aut}(G)$ é trivial, pois se $\varphi \in \mathrm{Aut}(G)$ fixa $g_1,\ldots,g_m$, então este é a identidade, já que $g_1,\ldots,g_m$ são geradores de G (vide Proposição 1.1.2). O Princípio da Contagem (Teorema 1.2.5) agora nos fornece que todas as órbitas dessa ação têm cardinalidade $|\mathrm{Aut}(G)|$ de modo que $|\mathscr{S}|$ é divisível por $|\mathrm{Aut}(G)|$.

Em 1936, Philip Hall [15] provou que se G é um grupo simples não abeliano, então a fração $\phi_G(m)/|\mathrm{Aut}(G)|$ é igual ao número máximo k tal que G^k pode ser gerado por m elementos. Notemos que este é um caso particular do Teorema B, com $L = M = G$. De fato, $G/M = \{1\}$ de sorte que $\phi_{G/M}(m) = 1$, e $|\Gamma_G| = |\mathrm{Aut}(G)|$, pois todo automorfismo de G age trivialmente em $\{1\}$. Observamos que $k = f(m) - 1$, pela definição de f.

Se $G = A_5$, temos que $\mathrm{Aut}(G) \cong S_5$, como está provado em [26, (2.17), Página 299]. Desse modo, $|\mathrm{Aut}(G)| = 120$. Usando o GAP, é possível ver que $\phi_G(2) = 19 \cdot 120$. Portanto, o resultado de Hall nos fornece que $d(A_5^{19}) = 2$ e $d(A_5^{20}) > 2$, ou seja, $f(2) = 20$.

Exemplo 2.4.8. *A probabilidade $P_m(G)$ que uma m-upla $(g_1, \ldots, g_m)$ de elementos de G gere G é igual a*

$$\frac{|\{m\text{-uplas que geram } G\}|}{|\{m\text{-uplas}\}|} = \frac{\phi_G(m)}{|G|^m}.$$

Consideremos $G = A_n$. Por um resultado de Dixon [10], a probabilidade que 2 elementos de G gerem G tende a 1 quando n tende a ∞, logo se n é suficientemente grande, digamos $n > N$, então $P_2(G) = \phi_G(2)/|G|^2 > 1/2$. Por outro lado, $\phi_G(2)/|G|^2 \leq 1$. Como provado em [26, (2.17), Página 299], $\mathrm{Aut}(G) \cong S_n$ (para $n \geq 7$). Assim, para n suficientemente grande,

$$\frac{1}{2} < \frac{\phi_G(2)}{|G|^2} \leq 1 \;\Rightarrow\; \frac{|G|^2}{2} < \phi_G(2) \leq |G|^2 \;\Rightarrow\; \frac{|G|^2}{2|S_n|} < \frac{\phi_G(2)}{|\mathrm{Aut}(G)|} \leq \frac{|G|^2}{|S_n|}.$$

Haja vista que $f(2) = 1 + \phi_G(2)/|\mathrm{Aut}(G)|$, obtemos

$$\frac{n!}{8} + 1 < f(2) \leq \frac{n!}{4} + 1.$$

Como $f(2)$ é o menor k tal que G^k não é 2-gerado, então $G^{\frac{n!}{8}}$ é 2-gerado pois $n!/8 < f(2)$. Agora, $G^{\frac{n!}{4}+1}$ não é 2-gerado pois $f(2) \leq n!/4 + 1$. De fato, se $d\big(G^{\frac{n!}{4}+1}\big) \leq 2$, então usando a propriedade dos grupos L_k (a sequência $d(L_1), \ldots, d(L_k), \ldots$ é não decrescente), teríamos $d(G^{f(2)}) \leq d\big(G^{\frac{n!}{4}+1}\big) \leq 2$ donde $d(G^{f(2)}) \leq 2$, um absurdo. Portanto,

$$d\big(A_n^{\frac{n!}{8}}\big) = 2 \quad e \quad d\big(A_n^{\frac{n!}{4}+1}\big) > 2.$$

Capítulo

3

Grupos Solúveis Eficientemente Gerados

Neste capítulo, faremos um estudo a respeito das relações de equivalência $\equiv_{\mathrm{m}}^{(r)}$ com $r \in \mathbb{Z}_+$, apresentadas na introdução, a fim de definir a função $\psi(G)$ e caracterizar os grupos solúveis finitos G tais que $\psi(G) = d(G)$, ou seja, demonstrar o Teorema C. O estudo foi baseado no artigo *Generating sets of finite groups* [4] de Peter Cameron, Andrea Lucchini e Colva Mary Roney-Dougal.

3.1 A Probabilidade de Gerar um Grupo Finito

Antes de começar o assunto principal deste capítulo, vamos tratar de alguns conceitos sobre probabilidade em geração de grupos finitos, os quais serão necessários para introduzir um resultado que será de grande importância para a demonstração do Teorema C. Esta seção é baseada no artigo *Bias of group generators in the solvable case* [6] de Eleonora Crestani e Andrea Lucchini.

Seja $\mathscr{R}$ o anel dos *polinômios de Dirichlet* $P(s) = \sum_n a_n/n^s$ com coeficientes inteiros. Suponhamos que G é um grupo finito e fixemos um subconjunto X de G. Para qualquer inteiro positivo t, seja $\phi_G(X,t)$ o número de t-uplas ordenadas $(g_1,\ldots,g_t)$ de elementos do grupo tal que $G = \langle X, g_1,\ldots,g_t\rangle$. O número

$$P_G(X,t) = \phi_G(X,t)/|G|^t$$

é a probabilidade que t elementos escolhidos aleatoriamente gerem G juntamente com

os elementos do subconjunto X.

Observação 3.1.1. *Seja G um grupo finito e X um subconjunto de G. Então*

$$\sum_{X \subseteq H \leq G} \phi_H(X,t) = |G|^t.$$

Com efeito, dado H um subgrupo de G que contém X, definamos

$$A_H(X,t) = \{(h_1,\ldots,h_t) \in H^t \mid H = \langle X, h_1,\ldots,h_t\rangle\},$$

o qual tem cardinalidade $\phi_H(X,t)$. Claramente, $A_H(X,t) \subseteq G^t$ de modo que $\bigcup_{X\subseteq H\leq G} A_H(X,t) \subseteq G^t$. Por outro lado, seja $(g_1,\ldots,g_t) \in G^t$. Tomando $H = \langle X, g_1,\ldots,g_t\rangle$, temos que $X \subseteq H \leq G$ e $(g_1,\ldots,g_t) \in A_H(X,t)$. Com isso, a outra inclusão segue, e obtemos

$$\bigcup_{X \subseteq H \leq G} A_H(X,t) = G^t.$$

Agora, notemos que, pela definição dos conjuntos $A_H(X,t)$, estes são dois a dois disjuntos, portanto

$$\sum_{X \subseteq H \leq G} \phi_H(X,t) = |G|^t.$$

Definição 3.1.2. *Seja G um grupo finito e consideremos S o reticulado dos subgrupos de G. A função de Möbius μ_S é definida pelas equações*

$$\mu_S(G) = 1, \tag{3.1}$$

e

$$\sum_{K \geq H} \mu_S(K) = 0 \tag{3.2}$$

para todo $H < G$, sendo que a soma é tomada sobre todos os elementos K de S que contêm H.

As equações (3.1) e (3.2) são suficientes para determinar a função μ_S unicamente. Com efeito, seja $K \leq G$. Se $K = G$, então por definição $\mu_S(K) = 1$. Assim, assumamos que $K < G$, e seja $n = n(K)$ o maior índice n tal que existem $K_1,\ldots,K_n \leq G$ com

$$K = K_0 < K_1 < \cdots < K_n = G.$$

Vamos mostrar que $\mu_S(K)$ é determinada por (3.2), usando indução sobre $n(K)$. Se $n(K) = 0$, então K é um subgrupo maximal de G; neste caso, $\mu_S(K) = -1$, pelas equações (3.1) e (3.2). Agora, suponhamos que seja conhecido o valor de $\mu_S(L)$ para

todo $L \leq G$ com $n(L) < n(K)$, e vamos calcular $\mu_S(K)$. Por (3.2),

$$\mu_S(K) = -\sum_{K<H\leq G} \mu_S(H).$$

Notemos que, dado $H \leq G$ com $K < H$,

$$K < H < H_1 < \cdots < H_{n(H)} = G$$

de modo que $n(K) \geq n(H) + 1$, isto é, $n(K) > n(H)$. Por indução, obtemos o valor de $\mu_S(K)$.

Agora, seja t um inteiro positivo, e definamos

$$f(H) = \begin{cases} 0 & \text{se } X \nsubseteq H, \\ \phi_H(X,t) & \text{caso contrário.} \end{cases}$$

Pela Observação 3.1.1, temos

$$\sum_{K\leq H} f(K) = \sum_{X\subseteq K\leq H} \phi_K(X,t) = |H|^t,$$

logo

$$\begin{aligned}\sum_{X\subseteq H\leq G} \mu_S(H)|H|^t &= \sum_{X\subseteq H\leq G} \mu_S(H)\left(\sum_{K\leq H} f(K)\right) = \sum_{X\subseteq K\leq H\leq G} \mu_S(H)f(K) \\ &= \sum_{X\subseteq K\leq G}\left(\sum_{K\leq H}\mu_S(H)\right) f(K) = f(G) = \phi_G(X,t),\end{aligned}$$

onde a penúltima igualdade é válida pela Definição 3.1.2. Ou seja, temos

$$\phi_G(X,t) = \sum_{X\subseteq H\leq G} \mu_S(H)|H|^t. \tag{3.3}$$

Em vista de (3.3), podemos escrever

$$P_G(X,t) = \sum_{X\subseteq H\leq G} \frac{\mu_S(H)}{[G:H]^t}. \tag{3.4}$$

Reorganizando os adendos em (3.4), obtemos um polinômio de Dirichlet como segue:

$$P_G(X,s) := \sum_{n\in\mathbb{N}} \frac{a_n}{n^s} \quad \text{onde} \quad a_n := \sum_{\substack{[G:H]=n,\\ X\subseteq H\leq G}} \mu_S(H).$$

Nesse sentido, temos o seguinte resultado:

Proposição 3.1.3 ([19], Proposição 16)**.** *Seja N um subgrupo normal de um grupo finito G e seja $NX/N = \{Nx \mid x \in X\}$. Então*

$$P_G(X,s) = P_{G/N}(NX/N,s) \cdot P_{G,N}(X,s),$$

onde

$$P_{G,N}(X,s) := \sum_{n\in\mathbb{N}} \frac{b_n}{n^s} \quad \textit{onde} \quad b_n := \sum_{\substack{[G:H]=n\\ X\subseteq H\leq G\\ HN=G}} \mu_S(H).$$

Se $t \in \mathbb{N}$ e $P_{G/N}(NX/N,t) \neq 0$, então $P_{G,N}(X,t)$ expressa a probabilidade condicional que t elementos aleatórios de G gerem G juntamente com os elementos de X, dado que eles geram G módulo N juntamente com NX/N.

Lema 3.1.4. *Sejam G um grupo finito, $H \leq G$ e N um subgrupo normal minimal de G. Se N é abeliano, então $NH = G$ se, e somente se, ou $H = G$, ou H é um complemento para N em G e é um subgrupo maximal de G.*

Demonstração. Assumamos que $NH = G$ e $H \neq G$. Então existe um subgrupo maximal M de G tal que $H \leq M$. Daí, $G = NH \leq NM$ de modo que $NM = G$. Seja $T = N \cap M$. Como $N \trianglelefteq G$, temos que $T \trianglelefteq M$. Além disso, por hipótese N é abeliano, logo $T \trianglelefteq N$. Assim, $T \trianglelefteq NM = G$. Se T não fosse trivial, existiria um subgrupo normal minimal L de G contido em T donde $L = N$ (pois $L \leq N$ e N é normal minimal em G) e $G = NM = M$ (já que $L \leq M$), um absurdo. Portanto T é trivial, e M é um complemento para N em G. Pelo Teorema dos Isomorfismos,

$$H \cong \frac{H}{\{1\}} = \frac{H}{N\cap H} \cong \frac{NH}{N} = \frac{G}{N} = \frac{NM}{N} \cong \frac{M}{N\cap M} = \frac{M}{\{1\}} \cong M.$$

Com isso, $|H| = |M|$, e haja vista que $H \leq M$, segue-se que $H = M$ é um subgrupo maximal de G. A recíproca é imediata. □

Seja $\{1\} = N_l \leq \cdots \leq N_0 = G$ uma *série principal* de G, ou seja, uma série tal que cada termo $N_i \trianglelefteq G$ $(1 \leq i \leq l)$ e cada fator (*principal*) N_{i-1}/N_i é um subgrupo

normal minimal de G/N_i ($1 \leq i \leq l$). Iterando a Proposição 3.1.3, obtemos, para cada fator principal N_{i-1}/N_i, um polinômio de Dirichlet associado $P_{G/N_i,N_{i-1}/N_i}(X,s)$, com coeficientes inteiros e com a propriedade que

$$P_G(X,s) = \prod_{1\leq i\leq l} P_{G/N_i,N_{i-1}/N_i}(X,s). \tag{3.5}$$

Se G é um grupo solúvel, então

$$P_{G/N_i,N_{i-1}/N_i}(X,s) = 1 - \frac{c_i}{|N_{i-1}/N_i|^s}, \tag{3.6}$$

sendo c_i o número de complementos de N_{i-1}/N_i em G/N_i contendo N_iX/N_i. De fato, sem perda de generalidade vamos estudar os subgrupos normais minimais de G. Seja N um tal subgrupo. Pela Proposição 3.1.3,

$$P_{G,N}(X,s) = \sum_{X\subseteq H, HN=G} \frac{\mu_S(H)}{[G:H]^s}.$$

Como G é solúvel, N é abeliano (vide Proposição 1.4.6). Dado $H \leq G$ tal que $NH = G$, temos, pelo Lema 3.1.4, que ou $H = G$, ou H é um complemento para N em G e é um subgrupo maximal de G. No segundo caso, notemos que $\mu_S(H) = -1$, pela definição da função μ_S, uma vez que H e G são os únicos subgrupos de G contendo H, e $\mu_S(G) = 1$. Portanto,

$$P_{G,N}(X,s) = 1 - \frac{c_N}{|N|^s},$$

sendo c_N o número de complementos para N em G contendo X.

Seja agora N um subgrupo normal de G e suponhamos que

$$\{1\} = W_l < \cdots < W_0 = N = U_m < \cdots < U_0 = G$$

é uma série principal de G passando por N. Pela Proposição 3.1.3 e por (3.5), temos

$$\begin{aligned} P_{G,N}(X,s) &= \frac{P_G(X,s)}{P_{G/N}(NX/N,s)} \\ &= \frac{(\prod_{1\leq i\leq l} P_{G/W_i,W_{i-1}/W_i}(X,s))(\prod_{1\leq j\leq m} P_{G/U_j,U_{j-1}/U_j}(X,s))}{\prod_{1\leq j\leq m} P_{G/U_j,U_{j-1}/U_j}(X,s)} \\ &= \prod_{1\leq i\leq l} P_{G/W_i,W_{i-1}/W_i}(X,s), \end{aligned} \tag{3.7}$$

pois

$$\{1\} = U_m/N < \cdots < U_1/N < U_0/N = G/N$$

é uma série principal de G/N.

Agora, vamos nos concentrar na seguinte situação: V é um espaço vetorial finito sobre $\mathbb{Z}_p$ para algum primo p, e H é um subgrupo solúvel irredutível não trivial de $\mathrm{Aut}(V)$, ou seja, se W é um subespaço H-invariante de V ($w^h \in W$ para todos $w \in W$ e $h \in H$), então $W = \{0\}$ ou $W = V$. O Lema de Schur (Lema 1.7.6) juntamente com o Teorema de Wedderburn ([17, Página 453]) nos dá que $F = \mathrm{End}_H(V)$ é um corpo, e notemos que V é um espaço vetorial sobre F (o produto escalar γv é definido como v^γ, para $\gamma \in F$ e $v \in V$ arbitrários). Nesse sentido, dado $h \in H$, temos que

$$C_V(h) = \{v \in V \mid v^h = v,\ \forall v \in V\} \quad \text{e} \quad [V,h] = \langle v^h - v \mid v \in V\rangle_{\mathbb{Z}_p}$$

são F-subespaços vetoriais de V. De fato, estes são fechados para a adição porque $h \in \mathrm{Aut}(V)$. E dados $\gamma \in F$, $v \in V$ e $w \in C_V(h)$, temos que

$$\gamma(v^h - v) = (v^h - v)^\gamma = (v^h)^\gamma - v^\gamma = (v^\gamma)^h - \gamma v = (\gamma v)^h - \gamma v \in [V,h]$$

e

$$(\gamma w)^h = (w^\gamma)^h = (w^h)^\gamma = w^\gamma = \gamma w,$$

uma vez que γ é um H-endomorfismo de V.

Seja $q = |F|$ e u a dimensão de V sobre F. Consideremos também o produto semi-direto $G = V^n \rtimes H$, onde H age da mesma maneira em cada um dos n fatores. Então, temos o:

Lema 3.1.5 ([6], Lema 5)**.** *Fixemos um elemento $g = ((v_1,\ldots,v_n),h) \in G$. Sejam $a = \dim_F C_V(h)$ e $b = n - \dim_F\langle [V,h], v_1,\ldots,v_n\rangle + \dim_F[V,h]$. Temos*

$$P_{G,V^n}(g,t) = \begin{cases} 1 & \text{se } b = 0, \\ \left(1 - \frac{q^a}{q^{ut}}\right)\left(1 - \frac{q^{a+1}}{q^{ut}}\right)\cdots\left(1 - \frac{q^{a+b-1}}{q^{ut}}\right) & \text{caso contrário.} \end{cases}$$

A ideia da demonstração deste lema consiste em considerar a série principal

$$\{0\} = W_n \leq W_{n-1} \leq \cdots \leq W_0 = V^n \leq G,$$

onde $W_i = \{(\tilde{v}_1, \ldots, \tilde{v}_n) \in V^n \mid \tilde{v}_j = 0 \text{ para cada } j \leq i\}$. Por (3.6) e (3.7),

$$P_{G,V^n}(\{g\}, t) = \prod_{1 \leq i \leq n} P_{G/W_i, W_{i-1}/W_i}(\{g\}, s) = (1 - c_1/q^{ut}) \cdots (1 - c_n/q^{ut}),$$

sendo c_i o número de complementos para W_{i-1}/W_i em G/W_i contendo o elemento $W_i g$ (notemos que cada fator W_{i-1}/W_i é isomorfo a V $(1 \leq i \leq n)$). Com isso, o objetivo é determinar o valor de $c_1, \ldots, c_n$, a partir de técnicas e resultados que fogem do foco deste trabalho.

3.2 Grupos Solúveis com $\psi(G) = d(G)$

Nesta última seção, demonstraremos o Teorema C, que é uma aplicação dos Teoremas A e B, vistos no Capítulo 2. O conteúdo é baseado em [4]. Iniciamos com a definição da relação de equivalência $\equiv_{\mathrm{m}}$.

Definição 3.2.1. *Seja G um grupo finito. Definimos a relação de equivalência $\equiv_{\mathrm{m}}$ (*m *para "subgrupos maximais") em G por: $x \equiv_{\mathrm{m}} y$ se, e somente se, x e y estão exatamente nos mesmos subgrupos maximais de G.*

Notemos que a $\equiv_{\mathrm{m}}$-*classe* contendo a identidade é precisamente o subgrupo de Frattini de G. Também, qualquer $\equiv_{\mathrm{m}}$-classe é a união de classes laterais do subgrupo de Frattini. De fato, seja g um elemento arbitrário de G e seja $[g]_{\equiv_{\mathrm{m}}}$ a $\equiv_{\mathrm{m}}$-classe de g. Dados $h \in \Phi(G)$ e M um subgrupo maximal de G tal que $g \in M$, temos, pela definição de $\Phi(G)$, que $h \in M$ de modo que $hg \in M$. Por outro lado, se K é um subgrupo maximal de G tal que $hg \in K$, então $h \in K$ e $g = h^{-1}(hg) \in K$. Desse modo, $hg \in [g]_{\equiv_{\mathrm{m}}}$. Pela arbitrariedade de g e h, segue-se que $\Phi(G)g \subseteq [g]_{\equiv_{\mathrm{m}}}$ para todo $g \in G$, e, portanto,

$$[g]_{\equiv_{\mathrm{m}}} = \bigcup_{y \in [g]_{\equiv_{\mathrm{m}}}} \Phi(G)y.$$

A relação de equivalência $\equiv_{\mathrm{m}}$ também pode ser caracterizada por uma propriedade de substituição:

Proposição 3.2.2. *Seja G um grupo finito, e sejam x e y elementos de G. Então $x \equiv_{\mathrm{m}} y$ se, e somente se,*

$$(\forall r)(\forall z_1, \ldots, z_r \in G)((\langle x, z_1, \ldots, z_r \rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_r \rangle = G)).$$

Demonstração. Suponhamos primeiro que $\langle x, z_1, \ldots, z_r \rangle = G$, mas $\langle y, z_1, \ldots, z_r \rangle \neq G$.

Então existe um subgrupo maximal M de G contendo $y, z_1, \ldots, z_r$. Daí, $x \notin M$, e segue-se que $x \not\equiv_{\mathrm{m}} y$.

Reciprocamente, suponhamos que $x \not\equiv_{\mathrm{m}} y$, logo sem perda de generalidade existe um subgrupo maximal M de G contendo y mas não x. Escolhamos geradores $z_1, \ldots, z_r$ para M. Então $\langle y, z_1, \ldots, z_r \rangle = M < G$, mas $\langle x, z_1, \ldots, z_r \rangle$ contém M propriamente (pois $x \notin M$), o que nos dá que $\langle x, z_1, \ldots, z_r \rangle = G$. □

Definição 3.2.3. *Dado um inteiro positivo r, definimos a relação de equivalência $\equiv_{\mathrm{m}}^{(r)}$ pela regra: $x \equiv_{\mathrm{m}}^{(r)} y$ se, e somente se,*

$$(\forall z_1, \ldots, z_{r-1} \in G)((\langle x, z_1, \ldots, z_{r-1} \rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_{r-1} \rangle = G)).$$

Lema 3.2.4.

(i) As relações $\equiv_{\mathrm{m}}^{(r)}$ tornam-se mais finas à medida que r aumenta.

(ii) O menor valor de r para o qual $\equiv_{\mathrm{m}}^{(r)}$ não é a relação universal é $d(G)$. Para $r = d(G)$, existem pelo menos $r + 1$ classes de equivalência.

(iii) O valor limite dessa sequência de relações é $\equiv_{\mathrm{m}}$.

Demonstração.

(i) Se $x \equiv_{\mathrm{m}}^{(r)} y$, então

$$(\forall z_1, \ldots, z_{r-1} \in G)((\langle x, z_1, \ldots, z_{r-1} \rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_{r-1} \rangle = G)).$$

Escolhendo z_{r-1} como sendo a identidade, vemos que $x \equiv_{\mathrm{m}}^{(r-1)} y$.

(ii) Suponhamos que $r < d(G)$, então a dupla implicação $\langle x, z_1, \ldots, z_{r-1} \rangle = G \Leftrightarrow \langle y, z_1, \ldots, z_{r-1} \rangle = G$ é sempre verdadeira, quaisquer que sejam $x, y, z_1, \ldots, z_{r-1} \in G$, pois $\langle x, z_1, \ldots, z_{r-1} \rangle = G$ e $\langle y, z_1, \ldots, z_{r-1} \rangle = G$ não acontecem, já que $r < d(G)$. Ou seja, $\equiv_{\mathrm{m}}^{(r)}$ é a relação universal. Agora, suponhamos que $r = d(G)$, logo existem $z_1, \ldots, z_r \in G$ tais que $\langle z_1, \ldots, z_r \rangle = G$. Daí, $z_1 \not\equiv_{\mathrm{m}}^{(r)} 1$ pois $\langle 1, z_2, \ldots, z_r \rangle = \langle z_2, \ldots, z_r \rangle \neq G$, uma vez que $r = d(G)$. Por conseguinte, $\equiv_{\mathrm{m}}^{(r)}$ não é a relação universal, e a primeira parte do item segue. Para a segunda parte, notemos que $z_i \not\equiv_{\mathrm{m}}^{(r)} 1$ para todo $i \in \{1, \ldots, r\}$, pelo mesmo argumento acima. Também, $z_i \not\equiv_{\mathrm{m}}^{(r)} z_j$ para todos $i \neq j$ em $\{1, \ldots, r\}$. De fato, sem perda de generalidade sejam $i < j$ em $\{1, \ldots, r\}$. Então $\langle z_1, \ldots, z_{i-1}, z_j, z_{i+1}, \ldots, z_r \rangle = \langle z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_r \rangle \neq G$, pois $r = d(G)$. Portanto, existem pelo menos $r + 1$ classes de equivalência.

(iii) Segue-se imediatamente da Definição 3.2.3.

□

Notemos que se $r = |G|$, então $\equiv_{\mathrm{m}}^{(r)}$ coincide com $\equiv_{\mathrm{m}}$. Com efeito, sejam $x, y \in G$ tais que $x \equiv_{\mathrm{m}}^{(r)} y$. Sejam também s um inteiro positivo e $z_1, \ldots, z_s \in G$. Se $s \leq r-1$, então $(\langle x, z_1, \ldots, z_s\rangle = G) \Leftrightarrow (\langle y, z_1, \ldots, z_s\rangle = G)$, pela definição de $\equiv_{\mathrm{m}}^{(r)}$. Assim, assumamos $s \geq r$. Temos que $\{x, z_1, \ldots, z_s\} = \{x, z_{i_1}, \ldots, z_{i_{r-1}}\}$, para certos $z_{i_1}, \ldots, z_{i_{r-1}} \in \{z_1, \ldots, z_s\}$ (aqui estamos retirando algumas repetições, pois $r = |G|$). Dessa forma, se $\langle x, z_1, \ldots, z_s\rangle = G$, então $\langle x, z_{i_1}, \ldots, z_{i_{r-1}}\rangle = G$. Dado que $x \equiv_{\mathrm{m}}^{(r)} y$, obtemos que $\langle y, z_{i_1}, \ldots, z_{i_{r-1}}\rangle = G$. Consequentemente, $\langle y, z_1, \ldots, z_s\rangle = G$. De modo análogo, $\langle y, z_1, \ldots, z_s\rangle = G \Rightarrow \langle x, z_1, \ldots, z_s\rangle = G$, e concluímos que $x \equiv_{\mathrm{m}} y$. Portanto, $\equiv_{\mathrm{m}}^{(r)} \subseteq \equiv_{\mathrm{m}}$, e como por definição $\equiv_{\mathrm{m}} \subseteq \equiv_{\mathrm{m}}^{(r)}$, segue-se que $\equiv_{\mathrm{m}}^{(r)}$ coincide com $\equiv_{\mathrm{m}}$.

Dessarte, temos a seguinte definição:

Definição 3.2.5. *Seja $\psi(G)$ o valor de r para o qual as equivalências $\equiv_{\mathrm{m}}^{(r)}$ se estabilizam, isto é, o menor valor r tal que $\equiv_{\mathrm{m}}^{(r)}$ coincide com a relação limite $\equiv_{\mathrm{m}}$.*

Vamos agora estudar algumas cotas inferiores e superiores para $\psi(G)$.

Lema 3.2.6. *Seja G um grupo finito, e seja $d = d(G)$. Então $\psi(G) \geq d$, e se G tem um subgrupo normal N tal que $N \not\subseteq \Phi(G)$ e $d(G/N) = d$, então $\psi(G) \geq d+1$.*

Demonstração. Primeiro, suponhamos que $\psi(G) < d$, então pelo item (ii) do Lema 3.2.4, $\equiv_{\mathrm{m}} = \equiv_{\mathrm{m}}^{(\psi(G))}$ é a relação universal, um absurdo. Portanto, $\psi(G) \geq d$.

Agora, para a segunda a parte do lema, notemos que os elementos de N não pertencem a nenhum conjunto gerador de G com cardinalidade d. De fato, seja $x \in N$ e suponhamos que existam $z_1, \ldots, z_{d-1} \in G$ tais que $\langle x, z_1, \ldots, z_{d-1}\rangle = G$. Daí, $\langle Nz_1, \ldots, Nz_{d-1}\rangle = \langle Nx, Nz_1, \ldots, Nz_{d-1}\rangle = G/N$ donde $d(G/N) \leq d-1 < d$ (já que $Nx = N$), um absurdo. Ou seja, $x \equiv_{\mathrm{m}}^{(d)} 1$ para todo $x \in N$. Desse modo, $\psi(G) \geq d+1$. Com efeito, se não fosse assim, $\psi(G) = d$ e $x \equiv_{\mathrm{m}} 1$ para todo $x \in N$. Haja vista que a $\equiv_{\mathrm{m}}$-classe de equivalência da identidade é $\Phi(G)$, teríamos $N \leq \Phi(G)$, uma contradição. □

Seja G um grupo finito. É verdade que $\psi(G) \in \{d(G), d(G)+1\}$? Veremos que para grupos solúveis isto é válido.

Definição 3.2.7. *Sejam G um grupo finito e M um subgrupo maximal de G tal que $M_G = \{1\}$ (isto é, G é um grupo primitivo). Para cada $g \in G \setminus M$, seja $\delta_{G,M}(g)$ a menor cardinalidade de*

um subconjunto X de M com a propriedade que $G = \langle g, X\rangle$, e seja

$$\nu_M(G) = \sup_{g\notin M} \delta_{G,M}(g).$$

Notemos que $\nu_M(G) \leq d(M)$. De fato, seja $d = d(M)$. Suponhamos que $d < \nu_M(G)$, então, pela definição de supremo, existe $g \in G \setminus M$ tal que $d < \delta_{G,M}(g)$. Temos que existe $Y \subseteq M$ com $|Y| = d$ tal que $M = \langle Y\rangle$. Daí, $\langle g, Y\rangle \neq G$ donde, pela maximalidade de M, $\langle g, Y\rangle = M$ e $g \in M$, um absurdo. Portanto, $\nu_M(G) \leq d(M)$.

Lema 3.2.8. *Sejam G um grupo e $K \trianglelefteq G$. Se $K \leq H \leq G$, então*

$$(H/K)_{G/K} = H_G/K.$$

Demonstração. Temos

$$(H/K)_{G/K} = \bigcap_{Kg\in G/K} (H/K)^{Kg} = \bigcap_{g\in G} H^g/K = (\bigcap_{g\in G} H^g)/K = H_G/K.$$

□

Dessa forma, se M é um subgrupo maximal de um grupo finito G, o Lema 3.2.8 nos dá que G/M_G é um grupo primitivo, pois M/M_G é um subgrupo maximal de G/M_G tal que o coração normal é trivial. Assim, temos a seguinte definição:

Definição 3.2.9. *Seja $\widetilde{m}(G)$ o máximo de $\nu_{M/N}(G/N)$ sobre todos os subgrupos maximais M de G, onde $N = M_G$ (coração normal de M em G).*

Dado um subconjunto X de um grupo finito G, vamos denotar por $d_X(G)$ a *menor* cardinalidade de um conjunto de elementos de G que gera G juntamente com os elementos de X. Notemos que $d_X(G) \leq d(G)$. De fato, seja $d = d(G)$, então existe um subconjunto Y de G com cardinalidade d tal que $G = \langle Y\rangle$. Daí, $G = \langle X, Y\rangle$ e, pela definição de $d_X(G)$, segue-se que $d = |Y| \geq d_X(G)$. O seguinte resultado generaliza o Teorema de Gaschütz (Teorema 2.2.5) para $X = \varnothing$.

Lema 3.2.10 ([7], Lema 6)**.** *Sejam X um subconjunto de G e N um subgrupo normal de G, e suponhamos que $\langle g_1, \ldots, g_k, X\rangle N = G$. Se $k \geq d_X(G)$, então existem $n_1, \ldots, n_k \in N$ tais que $\langle g_1n_1, \ldots, g_kn_k, X\rangle = G$.*

Com isso, vamos provar o seguinte teorema:

Teorema 3.2.11. *Seja G um grupo finito. Então $\psi(G) \leq \max\{\widetilde{m}(G), d(G)\} + 1$.*

Demonstração. Seja $t = \max\{\widetilde{m}(G), d(G)\}$. Vamos mostrar que $\equiv_{\mathrm{m}}^{(t+1)} \subseteq \equiv_{\mathrm{m}}$. Com efeito, sejam x e y dois elementos de G tais que $x \not\equiv_{\mathrm{m}} y$. Sem perda de generalidade, assumamos que exista um subgrupo maximal M de G tal que $x \notin M$ e $y \in M$. Sejam $N = M_G$ e $X = \{x\}$. Uma vez que $t \geq \widetilde{m}(G)$, temos $t \geq \nu_{M/N}(G/N)$; consequentemente, existem $g_1, \ldots, g_t \in M$ tais que $\langle x, g_1, \ldots, g_t\rangle N = G$. De fato, dado que $x \notin M$, temos $Nx \notin M/N$. Como $t \geq \nu_{M/N}(G/N)$, segue-se que $t \geq \delta_{G/N, M/N}(Nx)$ donde existem $g_1, \ldots, g_t \in M$ tais que $\langle Nx, Ng_1, \ldots, Ng_t\rangle = G/N$, e, assim, $\langle x, g_1, \ldots, g_t\rangle N = G$. Agora, $t \geq d(G) \geq d_X(G)$ de modo que, pelo Lema 3.2.10, existem $n_1, \ldots, n_t \in N$ tais que $G = \langle x, g_1 n_1, \ldots, g_t n_t\rangle$. Por outro lado, $\langle y, g_1 n_1, \ldots, g_t n_t\rangle \leq M < G$, pois $y \in M$. Portanto, $x \not\equiv_{\mathrm{m}}^{(t+1)} y$. Dessa forma, $\equiv_{\mathrm{m}}^{(t+1)} \subseteq \equiv_{\mathrm{m}}$,e, então, $\equiv_{\mathrm{m}}^{(t+1)} = \equiv_{\mathrm{m}}$. Pela definição de $\psi(G)$, concluímos que $\psi(G) \leq t + 1$. □

Corolário 3.2.12. *Se G é um grupo solúvel finito, então $\psi(G) \leq d(G) + 1$.*

Demonstração. Seja M um subgrupo maximal de G, e seja $K = M_G$. Então $\widetilde{G} = G/K$ é um grupo solúvel primitivo, pois $\widetilde{M} = M/K$ é um subgrupo maximal de $\widetilde{G}$ tal que $\widetilde{M}_{\widetilde{G}}$ é trivial (vide Lema 3.2.8). Agora, seja $\widetilde{N}$ um subgrupo normal minimal de $\widetilde{G}$. O Teorema de Ore-Baer (Teorema 2.1.14) juntamente com a Observação 2.1.15, nos fornece que $\widetilde{M}$ é um complemento para $\widetilde{N}$ em $\widetilde{G}$. Por conseguinte,

$$\frac{\widetilde{G}}{\widetilde{N}} = \frac{\widetilde{M}\widetilde{N}}{\widetilde{N}} \cong \frac{\widetilde{M}}{\widetilde{M} \cap \widetilde{N}} = \frac{\widetilde{M}}{\{1\}} \cong \widetilde{M},$$

e, consequentemente,

$$\nu_{\widetilde{M}}(\widetilde{G}) \leq d(\widetilde{M}) = d(\widetilde{G}/\widetilde{N}) \leq d(\widetilde{G}) \leq d(G).$$

Esta desigualdade vale para todo subgrupo maximal de G, logo $\widetilde{m}(G) \leq d(G)$ e, pelo Teorema 3.2.11, $\psi(G) \leq d(G) + 1$. □

Agora, com o intuito de demonstrar o Teorema C, vamos estudar os grupos G para os quais $\psi(G) = d(G)$. Iniciamos com a seguinte definição:

Definição 3.2.13. *Um grupo finito G é dito eficientemente gerado se para todo $x \in G$, $d_{\{x\}}(G) = d(G)$ implica em $x \in \Phi(G)$.*

Exemplo 3.2.14. *O grupo diedral*

$$D_5 = \langle a, b \mid a^5 = 1 = b^2,\ a^b = a^{-1}\rangle = \{1, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}$$

é eficientemente gerado. Basta usar o Teorema de Lagrange para ver que $d_{\{x\}}(D_5) = 1 \neq 2 = d(D_5)$*, para todo* $x \neq 1$ *em* D_5*.*

Exemplo 3.2.15. *Seja* $G = S_4$*. Afirmamos que* G *não é eficientemente gerado. De fato, vimos no Exemplo 1.5.2 que* $\Phi(G) = \{1\}$*, e notemos que* $d(G) = 2$*, pois* $G = \langle (12), (1234) \rangle$ *e* G *não é cíclico. Vamos então mostrar que* $d_{\{x\}}(G) = 2$ *para todo elemento* x *do subgrupo de Klein. Com efeito, temos que* $d_{\{x\}}(G) \leq 2$ *porque* $d_{\{x\}}(G) \leq d(G)$*. Uma vez que* G *não é cíclico,* $d_{\{x\}}(G) \geq 1$*. Suponhamos que exista* $1 \neq y \in G$ *tal que* $G = \langle x, y \rangle$*. Se* y *tem ordem* 2 *ou* 4*, então existe* S *um* 2*-subgrupo de Sylow de* G *tal que* $y \in S$ *de modo que* $G = \langle x, y \rangle \leq S$*, um absurdo. Mas então* y *tem ordem* 3*, o que significa que* $G \leq A_4$*, novamente um absurdo. Portanto,* $d_{\{x\}}(G) = 2$*, e a afirmação segue.*

Proposição 3.2.16. *Se* G *é um* p*-grupo finito, então* G *é eficientemente gerado.*

Demonstração. Suponhamos que G não é eficientemente gerado, logo existe $x \in G \setminus \Phi(G)$ tal que $d_{\{x\}}(G) = d$, onde $d = d(G)$. Desse modo, obtemos um subgrupo maximal M de G com $x \notin M$. Daí $M \neq \langle x, M \rangle$ de modo que, pela maximalidade de M, $\langle x, M \rangle = G$. Assim, pelo Teorema da Base de Burnside (Teorema 1.5.13), existe $Y \subseteq \{x\} \cup M$ tal que $|Y| = d$ e $G = \langle Y \rangle$. Temos que $x \notin Y$, pois, caso contrário, $G = \langle x, Y \setminus \{x\} \rangle$ e $d_{\{x\}}(G) \leq d - 1$. Portanto, $Y \subseteq M$ e $G = \langle Y \rangle \leq M$, um absurdo. Esta contradição nos leva a concluir que G é eficientemente gerado. □

Lema 3.2.17. *Se* $\psi(G) = d(G)$*, então* G *é eficientemente gerado.*

Demonstração. Seja $d = d(G)$. Se G não é eficientemente gerado, então existe $x \notin \Phi(G)$ tal que $d_{\{x\}}(G) = d$. Isto implica em particular que $x \equiv_{\mathrm{m}}^{(d)} 1$, pois é sempre falso que $\langle x, z_1, \ldots, z_{d-1} \rangle = G$ e $\langle 1, z_1, \ldots, z_{d-1} \rangle = G$, quaisquer que sejam $z_1, \ldots, z_{d-1} \in G$. Agora, dado que $x \notin \Phi(G)$, temos que $x \not\equiv_{\mathrm{m}} 1$ de modo que $\psi(G) > d$. □

Lema 3.2.18. *Se* G *é eficientemente gerado e* $\widetilde{m}(G) < d(G)$*, então* $\psi(G) = d(G)$*.*

Demonstração. Seja $d = d(G)$. Pelo Teorema 3.2.11, a hipótese $\widetilde{m}(G) < d(G)$ implica em $\psi(G) \leq d + 1$ donde

$$\equiv_{\mathrm{m}}^{(d+1)} \subseteq \equiv_{\mathrm{m}}^{(\psi(G))} = \equiv_{\mathrm{m}} \quad \text{e} \quad \equiv_{\mathrm{m}}^{(d+1)} = \equiv_{\mathrm{m}} .$$

Assim, é suficiente provar que $\equiv_{\mathrm{m}}^{(d)} \subseteq \equiv_{\mathrm{m}}^{(d+1)}$, pois sabemos do Lema 3.2.6 que $\psi(G) \geq d$.

Sejam $x, y \in G$ tais que $x \not\equiv_{\mathrm{m}}^{(d+1)} y$, e sejam $d_x = d_{\{x\}}(G)$ e $d_y = d_{\{y\}}(G)$. Temos que existem subconjuntos X e Y de G de cardinalidades d_x e d_y, respectivamente, tais

que $G = \langle x, X\rangle$ e $G = \langle y, Y\rangle$. Pela minimalidade de d_x e d_y, temos que $x \notin X$ e $y \notin Y$ de modo que $d_x, d_y \geq d - 1$. Se $d_x = d_y = d$, então nossa suposição de que G é eficientemente gerado implica em $x, y \in \Phi(G)$ donde $x \equiv_{\mathrm{m}} y$, uma contradição pois $\equiv_{\mathrm{m}}^{(d+1)} = \equiv_{\mathrm{m}}$. Portanto, podemos supor sem perda de generalidade que $d_x = d - 1$; em particular, $G = \langle x, g_1, \ldots, g_{d-1}\rangle$ para certos $g_1, \ldots, g_{d-1} \in G$. Se $d_y = d$, então $G \neq \langle y, g_1, \ldots, g_{d-1}\rangle$ de modo que $x \not\equiv_{\mathrm{m}}^{(d)} y$, e acabamos.

Assumamos então que $d_x = d_y = d - 1$. Dado que $x \not\equiv_{\mathrm{m}} y$, sem perda de generalidade existe um subgrupo maximal M de G tal que $x \notin M$ e $y \in M$. Seja $N = M_G$. Como $d > \widetilde{m}(G)$, temos $d - 1 \geq \widetilde{m}(G)$. Com o mesmo argumento da demonstração do Teorema 3.2.11, existem $g_1, \ldots, g_{d-1} \in M$ tais que $\langle x, g_1, \ldots, g_{d-1}\rangle N = G$. Como $d_x = d - 1$, deduzimos do Lema 3.2.10 que existem $n_1, \ldots, n_{d-1} \in N$ tais que $G = \langle x, g_1 n_1, \ldots, g_{d-1} n_{d-1}\rangle$. Por outro lado, $\langle y, g_1 n_1, \ldots, g_{d-1} n_{d-1}\rangle \leq M$, já que $y \in M$. Portanto, $x \equiv_{\mathrm{m}}^{(d)} y$. Pela arbitrariedade de x e y, concluímos que $\equiv_{\mathrm{m}}^{(d)} \subseteq \equiv_{\mathrm{m}}^{(d+1)}$, e o lema segue. □

Notemos que se $d(M) < d(G)$ para todo subgrupo maximal M de G, então G é eficientemente gerado. De fato, caso contrário, existe $x \notin \Phi(G)$ tal que $d_{\{x\}}(G) = d(G)$. Dado que $x \notin \Phi(G)$, existe um subgrupo maximal M de G tal que $x \notin M$. Escolhendo $z_1, \ldots, z_d \in M$ tais que $\langle z_1, \ldots, z_d\rangle = M$ (onde $d = d(M)$), temos $M < \langle x, z_1, \ldots, z_d\rangle \leq G$ donde, pela maximalidade de M, $\langle x, z_1, \ldots, z_d\rangle = G$, e, assim, $d \geq d_{\{x\}}(G)$. Daí,

$$d(G) = d_{\{x\}}(G) \leq d(M) < d(G),$$

um absurdo. Portanto, G é eficientemente gerado.

Corolário 3.2.19. *Se $d(M) < d(G)$ para todo subgrupo maximal M de G, então $\psi(G) = d(G)$.*

Demonstração. Sendo $\widetilde{m}(G)$ o máximo de $\nu_{M/N}(G/N)$ sobre todos os subgrupos maximais M de G (onde $N = M_G$), temos que $\widetilde{m}(G) = \nu_{M/N}(G/N)$ para algum subgrupo maximal M de G. Mas sabemos que $\nu_{M/N}(G/N) \leq d(M/N)$, logo

$$\widetilde{m}(G) \leq d(M/N) \leq d(M) < d(G).$$

Além disso, como observado acima, G é eficientemente gerado, portanto o Lema 3.2.18 nos fornece que $\psi(G) = d(G)$. □

Lema 3.2.20. *Seja G um grupo solúvel finito. Se G é eficientemente gerado, então $\widetilde{m}(G) < d(G)$.*

Demonstração. Pela definição de $\widetilde{m}(G)$, é suficiente provar que $d(M/M_G) < d(G) =: d$, para todo subgrupo maximal M de G. Assumamos o contrário, ou seja, que existe um subgrupo maximal M de G tal que $d(M/N) \geq d$ (onde $N = M_G$). Com o argumento usado na demonstração do Corolário 3.2.12, existe um subgrupo normal A de G tal que A/N é não trivial e é complementado por M/N em G/N. Como $\Phi(G) \leq M$, temos $\Phi(G) \leq N$, e visto que A/N é não trivial, obtemos que $\Phi(G) < A$. Assim, seja $a \in A \setminus \Phi(G)$. Sabemos que $d_{\{a\}}(G) \in \{d-1, d\}$. Se $d_{\{a\}}(G) = d-1$, então existem $z_1, \ldots, z_{d-1} \in G$ tais que $G = \langle a, z_1, \ldots, z_{d-1}\rangle$. Daí, $G/A = \langle Az_1, \ldots, Az_{d-1}\rangle$ donde $d(G/A) \leq d-1$. Por outro lado,

$$\frac{G}{A} \cong \frac{G/N}{A/N} = \frac{M/N \cdot A/N}{A/N} \cong \frac{M/N}{M/N \cap A/N} \cong \frac{M/N}{\{1\}} \cong \frac{M}{N},$$

o que nos fornece $d(G/A) = d(M/N) \geq d$, uma contradição. Com isso, $d_{\{a\}}(G) = d$. Mas isto contradiz a hipótese de que G é eficientemente gerado. Portanto, $\widetilde{m}(G) < d(G)$. □

O seguinte resultado segue imediatamente dos Lemas 3.2.17, 3.2.18 e 3.2.20.

Corolário 3.2.21. *Seja G um grupo solúvel finito. Então $\psi(G) = d(G)$ se, e somente se, G é eficientemente gerado.*

Observação 3.2.22. *Um grupo finito G é eficientemente gerado se, e somente se, $G/\Phi(G)$ é eficientemente gerado. De fato, seja $F = \Phi(G)$. Como visto no Exemplo 2.2.3, $d(G) = d(G/F)$, e com o mesmo argumento, dados $x \in G$ e $Y \subseteq G$, $\langle x, Y\rangle = G$ se, e somente se, $\langle Fx, \overline{Y}\rangle = G/F$ (onde $\overline{Y} = \{Fy \mid y \in Y\}$), ou seja,*

$$d_{\{x\}}(G) = d_{\{Fx\}}(G/F),$$

para todo $x \in G$. Portanto, $d_{\{x\}}(G) = d(G)$ se, e somente se, $d_{\{Fx\}}(G/F) = d(G/F)$, e a observação segue.

Assim, feito os estudos preliminares, vamos finalizar esta seção demonstrando o Teorema C, o qual nos dá uma caracterização dos grupos solúveis eficientemente gerados. Mais precisamente,

Teorema C. *Um grupo solúvel finito G satisfaz $\psi(G) = d(G)$ se, e somente se, ou G é um p-grupo finito, ou existe um espaço vetorial finito V, um subgrupo solúvel irredutível não*

trivial H de $\mathrm{Aut}(V)$ *e um inteiro $d > d(H)$ tal que*

$$G/\Phi(G) \cong V^{r(d-2)+1} \rtimes H,$$

sendo r a dimensão de V sobre $\mathrm{End}_H(V)$ *e H age da mesma maneira em cada um dos $r(d-2)+1$ fatores.*

Demonstração. Suponhamos que G é um grupo solúvel com $\psi(G) = d(G)$. Sejam $d = d(G)$ e $F = \Phi(G)$. Pelo Corolário 3.2.21, G é eficientemente gerado. Seja A/F um subgrupo normal não trivial de G/F. Temos que $F < A$ e $d\left(\frac{G/F}{A/F}\right) = d(G/A)$. Pelo argumento usado na demonstração do Lema 3.2.20, obtemos que $d(G/A) < d$, e, portanto, $d\left(\frac{G/F}{A/F}\right) < d$. Por outro lado, $d(G/F) = d(G) = d$. Ou seja, G/F tem a propriedade que todo quociente próprio pode ser gerado por $d-1$ elementos, mas G/F não. Vamos então dividir em dois casos.

Caso 1. Quando $d = 2$: neste caso, $d - 1 = 1$ e, pelo Teorema A, temos que ou $G/F \cong C_p \times C_p$ para algum primo p, ou G/F é primitivo monolítico com socle M cujo quociente é cíclico. A primeira ocorrência implica que G é um p-grupo finito, pela Proposição 1.5.8. Assumamos então que G/F é primitivo monolítico com $M = \mathrm{soc}(G/F)$. Dado que G é solúvel, temos, pela Proposição 1.4.6, que M é abeliano elementar de modo que este pode ser visto como um espaço vetorial sobre $\mathbb{Z}_p$ para algum primo p, pela Proposição 1.3.6. Ou seja, $M \cong C_p^n$ para algum n. Lembremos que, pela Proposição 1.5.11, M admite um complemento em G/F; vamos denotá-lo por H. Desse modo, temos que

$$G/F \cong M \rtimes H,$$

onde H age em M por conjugação. Se H é trivial, então $G/F = M \cong C_p$ (porque G/F é simples) donde novamente G é um p-grupo finito, pela Proposição 1.5.8. Mas se $H \neq \{1\}$, então H é um subgrupo solúvel irredutível de $\mathrm{Aut}(M)$, como veremos com mais detalhes no próximo caso. E além disso, $d(H) = d((G/F)/M) = 1 < 2 = d$, uma vez que o quociente $(G/F)/M$ é cíclico.

Caso 2. Quando $d > 2$: temos agora que $d - 1 \geq 2$. Dado que G é solúvel, o Teorema A nos fornece que

$$G/F \cong L_k,$$

onde $k = f(L, d-1)$ e $L = MH$ com $H \leq L$, $M \cap H = \{1\}$ e M o único subgrupo normal minimal de L; além disso, M é abeliano. Lembremos que, pelo Lema 2.3.3,

$L_k = M^k \cdot \mathrm{diag}(H^k)$ com $M^k \cap \mathrm{diag}(H^k) = \{1\}$, ou seja,

$$L_k \cong M^k \rtimes H,$$

e H age da mesma maneira em cada um dos k fatores (por conjugação). Pelas Proposições 1.3.6 e 1.4.6, M pode ser visto como um espaço vetorial sobre $\mathbb{Z}_p$ para algum primo p, isto é, $M \cong C_p^n$ para algum n. Se $H = \{1\}$, então $L = M \cong C_p$ e $L_k \cong M^k \cong C_p^k$ donde G/F é um p-grupo finito. Neste caso, pela Proposição 1.5.8, segue-se que G é um p-grupo finito.

Assim, assumamos que $H \neq \{1\}$. Consideremos $\varphi : H \to \mathrm{Aut}(M)$ a ação por conjugação, e vamos mostrar que esta é injetiva. Para isto, sejam $N = \ker(\varphi) \trianglelefteq H$, $x \in N$ e $l = mh \in L$. Como $x \in N$, temos $xm = mx$ de modo que

$$x^l = x^{mh} = x^h \in N,$$

pois $N \trianglelefteq H$. Ou seja, $N \trianglelefteq L$. Agora, se $N \neq \{1\}$, então $M \subseteq N$, já que M é o único subgrupo normal minimal de L. Daí, $M \subseteq H$ e $M \cap H = M \neq \{1\}$, um absurdo. Portanto, φ é injetiva e H pode ser visto como um subgrupo de $\mathrm{Aut}(M)$. Pela Proposição 2.3.2,

$$H \cong L/M \cong L_k/M^k$$

é um subgrupo solúvel, pois G é solúvel e $G/F \cong L_k$. Também, dado que M é um subgrupo normal minimal de L, segue-se que H é um subgrupo irredutível de $\mathrm{Aut}(M)$. Vamos mostrar que $d > d(H)$. Com efeito, seja $T = M^k$. Temos

$$d(H) = d(L/M) = d(L_k/T).$$

Além disso, existe um isomorfismo $\sigma : L_k \to \widetilde{G}$ (onde $\widetilde{G} = G/F$), e este induz o isomorfismo $\overline{\sigma} : L_k/T \to \widetilde{G}/T^\sigma$ dado por

$$(Tx)^{\overline{\sigma}} = T^\sigma x^\sigma, \qquad \text{sempre que} \quad x \in L_k.$$

Temos que T é não trivial (pois $M \neq \{1\}$), logo T^σ é também não trivial, já que σ é um isomorfismo. Portanto, pela propriedade de $\widetilde{G}$,

$$d(H) = d(L_k/T) = d(\widetilde{G}/T^\sigma) \leq d - 1 < d.$$

Com isso, $d(L) < d$, pois, pelo Teorema 2.2.9, $d(L) = \max\{2, d(H)\}$, e por hipótese

$d > 2$.

Agora, pelo Lema 3.1.4, H é um subgrupo maximal de L. Também, o coração normal H_L é trivial, pois, caso contrário, este conteria M (já que $H_L \trianglelefteq L$) e $H_L \cap M = M \neq \{1\}$, um absurdo porque $H_L \cap M \leq H \cap M = \{1\}$. Pela Observação 2.1.15, todos os complementos para M em L são conjugados a H. Desse modo, o número de complementos para M em L é dado por $[L : N_L(H)]$ (vide Exemplo 1.2.2). Uma vez que H é não trivial e $H_L = \{1\}$, temos $H \ntrianglelefteq L$. Pela maximalidade de H, segue-se que $N_L(H) = H$ e

$$[L : N_L(H)] = [L : H] = |M|.$$

Dessarte, pela Observação 2.4.6,

$$k = f(L, d-1) = 1 + \log_q(|M|^{d-2}),$$

onde $q = |\mathrm{End}_L(M)| = |\mathrm{End}_H(M)|$. Por outro lado, sendo r a dimensão de M sobre $\mathrm{End}_H(M)$ (notemos que M pode ser visto como um espaço vetorial sobre $\mathrm{End}_H(M)$, definindo a soma de dois vetores como o produto destes em M, e o produto escalar γm sendo m^γ, para $\gamma \in \mathrm{End}_H(M)$ e $m \in M$ arbitrários), temos que $|M| = q^r$ de maneira que $|M|^{d-2} = q^{r(d-2)}$ e $k = r(d-2) + 1$. Portanto,

$$G/F \cong L_{r(d-2)+1} \cong M^{r(d-2)+1} \rtimes H.$$

Em ambos os casos, basta considerar $V = M$, e, assim, concluímos a primeira parte do teorema.

Reciprocamente, se G é um p-grupo finito, então G é eficientemente gerado, pela Proposição 3.2.16, donde $\psi(G) = d(G)$, pelo Corolário 3.2.21. Assim, pela Observação 3.2.22, é suficiente provar que se H é um subgrupo solúvel irredutível não trivial $(d-1)$-gerado de $\mathrm{Aut}(V)$ e r é a dimensão de V sobre $F = \mathrm{End}_H(V)$, então $X = V^{r(d-2)+1} \rtimes H$ é eficientemente gerado. Primeiro, afirmamos que $d(X) = d$. Com efeito, temos por hipótese que H age da mesma maneira em cada um dos $r(d-2)+1$ fatores. Então, consideremos $L = V \rtimes H$. Uma vez que H é um subgrupo irredutível de $\mathrm{Aut}(V)$, temos que V é normal minimal em L. Além disso, $C_L(V) = V$, pois se $(v, h) \in C_L(V)$, então

$$(x^h, 0) = ((v + x - v)^h, 0) = (x, 0)^{(v,h)} = (x, 0)$$

para todo $x \in V$ de modo que $x^h = x$ para todo $x \in V$, e, consequentemente, $h = \mathrm{id}_V$ e $(v, h) \in V$. Portanto, V é o único subgrupo normal minimal de L, isto é, L é monolítico. Por conseguinte, L é primitivo, pois $\Phi(L) = \{1\}$, uma vez que H complementa V em L e isto implica em $V \nsubseteq \Phi(L)$ (vide Observação 1.5.12).

Sejam $k = r(d-2)$ e $(l_1, \ldots, l_{k+1}) \in L_{k+1}$, então existem $v_1, \ldots, v_{k+1} \in V$ e $h_1, \ldots, h_{k+1} \in H$ tais que

$$(l_1, \ldots, l_{k+1}) = ((v_1, h_1), \ldots, (v_{k+1}, h_{k+1})).$$

Pela definição de L_{k+1},

$$(v_1, h_1) \equiv \cdots \equiv (v_{k+1}, h_{k+1}) \mod V,$$

ou seja,

$$(0, h_1) \equiv \cdots \equiv (0, h_{k+1}) \mod V \quad \text{e} \quad h_1 = \cdots = h_{k+1},$$

pois $V \cap H = \{0\}$. Com isso, definamos $\varphi : L_{k+1} \to X$ por

$$((v_1, h), \ldots, (v_{k+1}, h))^{\varphi} = ((v_1, \ldots, v_{k+1}), h), \quad \text{sempre que } v_1, \ldots, v_{k+1} \in V,\ h \in H.$$

Claramente, φ é uma bijeção. Vamos mostrar que φ é um homomorfismo. Sejam $u_1, v_1, \ldots, u_{k+1}, v_{k+1} \in V$ e $h, h' \in H$ arbitrários. Temos

$$\begin{aligned}
&((u_1, h), \ldots, (u_{k+1}, h)) \cdot ((v_1, h'), \ldots, (v_{k+1}, h')) \\
&= ((u_1 + v_1^{h^{-1}}, hh'), \ldots, (u_{k+1} + v_{k+1}^{h^{-1}}, hh')) \overset{\varphi}{\longmapsto} ((u_1 + v_1^{h^{-1}}, \ldots, u_{k+1} + v_{k+1}^{h^{-1}}), hh') \\
&= ((u_1, \ldots, u_{k+1}) + (v_1^{h^{-1}}, \ldots, v_{k+1}^{h^{-1}}), hh') = ((u_1, \ldots, u_{k+1}) + (v_1, \ldots, v_{k+1})^{h^{-1}}, hh') \\
&= ((u_1, \ldots, u_{k+1}), h)((v_1, \ldots, v_{k+1}), h').
\end{aligned}$$

Portanto, φ é um isomorfismo e $X \cong L_{k+1}$. Agora, por hipótese $d > d(H)$ e $H \neq \{1\}$, logo $d > 1$. Pelo Teorema 2.2.9, $d(L) = \max\{2, d(H)\}$. Se $d = 2$, então $X = L$ de maneira que

$$d(X) = d(L) = 2 = d,$$

e acabamos. Assumamos então que $d > 2$; logo, $d(L) < d$. Novamente, vamos usar a Observação 2.4.6. Temos que

$$f(L, d-1) = 1 + \log_q(|V|^{d-2}) = 1 + \log_q(q^{r(d-2)}) = 1 + r(d-2) = k + 1,$$

onde $q = |F|$. Pela definição de f, isto significa que

$$d(L_k) = d - 1 < d(L_{k+1}).$$

Mas sabemos que $d(L_{k+1}) \leq d(L_k) + 1$, logo

$$d(X) = d(L_{k+1}) = d,$$

e a afirmação segue.

Para concluir que X é eficientemente gerado, vamos mostrar que $d_{\{x\}}(X) \leq d - 1$ para todo $x \neq 1$. Suponhamos primeiramente que $d = 2$: neste caso, precisamos mostrar que $d_{\{x\}}(X) \leq 1$ para todo $x \neq 1$. Seja então um tal elemento $x \in X$. Pelo Lema 3.1.4, H é um subgrupo maximal de X. Por um argumento feito anteriormente, temos que $H_X = \{1\}$. Dessa forma, $x \notin H_X$ de sorte que existe um conjugado de H em X o qual não contém x, digamos H^w com $w \in V$. Uma vez que H é maximal, obtemos que H^w também o é, e, consequentemente, $\langle x, H^w \rangle = X$. Sendo h um gerador de H, temos que $\langle x, h^w \rangle = \langle x, H^w \rangle$; portanto, $X = \langle x, h^w \rangle$ e $d_{\{x\}}(X) \leq 1$.

Agora, consideremos $d > 2$. Seja $n = r(d-2)+1$. Fixemos um elemento não trivial $x = ((v_1, \ldots, v_n), h) \in X$, e sejam $a = \dim_F C_V(h)$ e $b = n - \dim_F \langle [V,h], v_1, \ldots, v_n \rangle + \dim_F [V,h]$. Notemos que $n > \dim_F \langle [V,h], v_1, \ldots, v_n \rangle$. De fato, caso contrário, $r(d-2)+1 = n \leq r$ (visto que $\langle [V,h], v_1, \ldots, v_n \rangle$ é um F-subespaço vetorial de V) de modo que $r(d-3)+1 \leq 0$, um absurdo pois $d > 2$. Portanto, $b > 0$. Pelo Lema 3.1.5,

$$P_{X,V^n}(\{x\}, d-1) = \left(1 - \frac{q^a}{q^{r(d-1)}}\right)\left(1 - \frac{q^{a+1}}{q^{r(d-1)}}\right) \cdots \left(1 - \frac{q^{a+b-1}}{q^{r(d-1)}}\right), \tag{3.8}$$

onde cada fator deste produto é não negativo. Além disso, pela Proposição 3.1.3,

$$P_X(\{x\}, d-1) = P_{X/V^n}(\{V^n x\}, d-1) \cdot P_{X,V^n}(\{x\}, d-1),$$

e notemos que

$$d_{\{x\}}(X) \leq d - 1 \Leftrightarrow \phi_X(\{x\}, d-1) > 0 \Leftrightarrow P_X(\{x\}, d-1) > 0.$$

Temos que $X/V^n \cong H$. Se y é a imagem de $V^n x$ por meio do isomorfismo associado, então

$$P_{X/V^n}(\{V^n x\}, d-1) = P_H(\{y\}, d-1) > 0,$$

pois H é $(d-1)$-gerado e isto implica $\phi_H(\{y\}, d-1) > 0$.

Assim, resta analisar quando $P_{X,V^n}(\{x\}, d-1) > 0$. Como visto em (3.8),

$$1 - q^{a+j}/q^{r(d-1)} \geq 0$$

para todo $j \in \{0, 1, \ldots, a+b-1\}$, logo $a + j \leq r(d-1)$ para todo $j \in \{0, 1, \ldots, a+b-1\}$. Se $a+b-1 = r(d-1)$, então $1 - q^{a+b-1}/q^{r(d-1)} = 0$ e $P_{X,V^n}(\{x\}, d-1) = 0$. Por outro lado, se $P_{X,V^n}(\{x\}, d-1) = 0$, então existe $j \in \{0, 1, \ldots, a+b-1\}$ tal que $a + j = r(d-1)$. Mas

$$r(d-1) = a + j \leq a + b - 1 \leq r(d-1),$$

o que implica $a + b - 1 = r(d-1)$. Portanto,

$$d_{\{x\}}(X) \leq d-1 \Leftrightarrow P_{X,V^n}(\{x\}, d-1) > 0 \Leftrightarrow a + b - 1 < r(d-1).$$

Em seguida, se $h \neq 1$, então $C_V(h) \neq V$ donde $a \leq r-1$. Também, $b \leq n$ pois $\dim_F[V,h] \leq \dim_F\langle [V,h], v_1, \ldots, v_n\rangle$. Se $h = 1$, então $C_V(h) = V$ e $a = r$. E $\dim_F\langle [V,h], v_1, \ldots, v_n\rangle = \dim_F\langle v_1, \ldots, v_n\rangle \geq 1$, já que $x = ((v_1, \ldots, v_n), h)$ é um elemento não trivial. Em qualquer caso,

$$a + b - 1 \leq r + n - 2 = r + r(d-2) - 1 = r(d-1) - 1 < r(d-1).$$

Isto completa a prova do Teorema. □

Apêndice

Daremos aqui uma demonstração alternativa do fato de que a sequência $d(S), d(S^2), \ldots, d(S^n), \ldots$ é ilimitada, para S um grupo simples não abeliano finito. Lembramos que isso foi visto como uma consequência imediata da Proposição 2.3.8.

Primeiramente, vamos mostrar que, dado $n \in \mathbb{Z}_+$, os subgrupos maximais de S^n são de dois tipos:

1) Produto: dado $i \in \{1, \ldots, n\}$,

$$S \times \cdots \times S \times K \times S \times \cdots \times S,$$

com K um subgrupo maximal de S na i-ésima entrada.

2) Diagonal: dados $i \neq j$ em $\{1, \ldots, n\}$, e dado $\varphi \in \mathrm{Aut}(S)$,

$$\Delta_{\varphi,i,j} = \{(s_1, \ldots, s_n) \in S^n \mid s_i^{\varphi} = s_j\}.$$

Com efeito, sejam $G = S^n = S_1 \times S_2 \times \cdots \times S_n$ e M um subgrupo maximal de G. Para cada $i \in \{1, \ldots, n\}$, consideremos as i-ésimas projeções $\pi_i : S^n \to S$. Se existe algum i para o qual $M^{\pi_i} \neq S$, então $M^{\pi_i} \leq K_i$, para algum subgrupo maximal K_i de S, de forma que

$$M \leq S_1 \times S_2 \times \cdots \times S_{i-1} \times K_i \times S_{i+1} \times \cdots \times S_n.$$

Notemos que vale na verdade a igualdade, já que M é maximal em G. Assim, assumamos que todas as projeções $\pi_1, \ldots, \pi_n$ restritas a M sejam sobrejetivas. Suponhamos o caso $n = 2$ verdadeiro e consideremos então $n > 2$. Seja $N = M_G \trianglelefteq G$. Pelo Lema 2.4.1, N é um produto de alguns dos fatores $S_1, \ldots, S_n$. Temos que N não pode ser um produto de $n - 1$ fatores, pois, caso contrário, $M \geq N$ conteria o outro fator restante (visto que as projeções restritas a M são sobrejetivas) de modo que $M = G$, uma con-

tradição. Também, notemos que M/N é maximal em G/N com coração normal trivial (vide Lema 3.2.8), isto é, G/N é um grupo primitivo. Pela Proposição 2.1.16, G/N admite no máximo dois subgrupos normais minimais, logo N é da forma

$$N = S_1 \times \cdots \times S_{i-1} \times \{1\} \times S_{i+1} \times \cdots \times S_{j-1} \times \{1\} \times S_{j+1} \times \cdots \times S_n,$$

para certos $i \neq j$ em $\{1, \ldots, n\}$, e $G/N \cong S \times S$ pelo isomorfismo $\psi : G/N \to S \times S$ dado por

$$N(s_1, \ldots, s_n) \overset{\psi}{\longmapsto} (s_i, s_j), \qquad \text{sempre que} \quad (s_1, \ldots, s_n) \in G.$$

Agora, observamos que $(M/N)^\psi$ é um subgrupo maximal de $S \times S$. Este não pode ser da forma $K \times S$ nem $S \times K$, com K um subgrupo maximal de S. De fato, suponhamos por exemplo que $(M/N)^\psi = K \times S$, sendo K maximal em S. Seja $t_i \in S \setminus K$. Como M^{π_i}=S, existe um elemento $(s_1, \ldots, s_{i-1}, t_i, s_{i+1}, \ldots, s_n) \in M$ de sorte que

$$(N(s_1, \ldots, s_{i-1}, t_i, s_{i+1}, \ldots, s_n))^\psi = (t_i, s_j) \notin K \times S,$$

um absurdo. Portanto, usando o caso $n = 2$, concluímos que existe um isomorfismo $\varphi : S \to S$ tal que $(M/N)^\psi = \Delta_\varphi = \{(x, y) \in S \times S \mid x^\varphi = y\}$. Daí,

$$M/N = (\Delta_\varphi)^{\psi^{-1}} = \{Ng \mid g \in G \text{ e } (g^{\pi_i})^\varphi = g^{\pi_j}\} = \Delta_{\varphi,i,j}/N$$

donde $M = \Delta_{\varphi,i,j}$. Dessarte, vamos nos concentrar em provar o caso $n = 2$, ou seja, $G = S_1 \times S_2$ com $M^{\pi_1} = M^{\pi_2} = S$. Primeiro, observamos que $\overline{S_1} = S_1 \times \{1\}$ não está contido em M. Para ver isto, suponhamos o contrário, e seja $s \in S$. Dado que $M^{\pi_2} = S$, existe $t \in S$ tal que $(t, s) \in M$. Por outro lado, $(t, 1) \in M$ porque $\overline{S_1} \leq M$. Consequentemente

$$(1, s) = (t, s) \cdot (t, 1)^{-1} \in M.$$

Pela arbitrariedade de s, segue-se que M contém $\overline{S_2}$, e, portanto, $M = G$, uma contradição. Analogamente, $\overline{S_2}$ não está contido em M. Agora, temos que $\overline{S_1} \cap M \trianglelefteq \overline{S_1}$. Com efeito, sejam $(a, 1) \in \overline{S_1} \cap M$ e $(s, 1) \in \overline{S_1}$. Dado que $M^{\pi_1} = S$, obtemos um elemento da forma (s, b) em M. Daí,

$$M \ni (s, b) \cdot (a, 1) \cdot (s, b)^{-1} = (sas^{-1}, 1) \in \overline{S_1}$$

donde $(a, 1)^{(s,1)} \in \overline{S_1} \cap M$. Uma vez que $\overline{S_1}$ é um grupo simples, segue-se que $\overline{S_1} \cap M$

é trivial, haja vista que $\overline{S_1} \not\subseteq M$. Da mesma forma, $\overline{S_2} \cap M$ é também trivial. Seja $s \in S$. Temos que existe $m \in M$ tal que $m^{\pi_1} = s$. Com isso, ponhamos $s^{\varphi} := m^{\pi_2}$. Afirmamos que $\varphi : S \to S$ é um isomorfismo. De fato, temos que φ está bem definida: se $m_1, m_2 \in M$ são tais que $m^{\pi_1} = m^{\pi_2} = s$, então

$$(m_1 \cdot m_2^{-1})^{\pi_1} = m_1^{\pi_1}(m_2^{\pi_1})^{-1} = ss^{-1} = 1$$

de maneira que $m_1 \cdot m_2^{-1} \in \overline{S_2} \cap M = \{1\}$; consequentemente, $m_1 = m_2$ e $m_1^{\pi_2} = m_2^{\pi_2}$. Também, φ é injetiva: sejam $s_1, s_2 \in S$ com $s_1^{\varphi} = s_2^{\varphi}$. Pela definição de φ, existem elementos $m_1 = (x, y)$ e $m_2 = (u, v)$ de M tais que $s_1 = m_1^{\pi_1}$ e $s_2 = m_2^{\pi_1}$, isto é, $s_1 = x$ e $s_2 = u$. E

$$y = m_1^{\pi_2} = s_1^{\varphi} = s_2^{\varphi} = m_2^{\pi_2} = v.$$

Assim,

$$(xu^{-1}, 1) = (x, y) \cdot (u, v)^{-1} = m_1 m_2^{-1} \in \overline{S_1} \cap M = \{1\}$$

de forma que $x = u$ e $s_1 = s_2$. Logo, φ é de fato injetiva. Agora, sejam $s_1, s_2 \in S$ arbitrários. Temos que existem $m_1, m_2 \in M$ tais que $m_1^{\pi_1} = s_1$ e $m_2^{\pi_1} = s_2$. Observamos que $s_1 s_2 = m_1^{\pi_1} m_2^{\pi_1} = (m_1 \cdot m_2)^{\pi_1}$, logo

$$(s_1 s_2)^{\varphi} = (m_1 \cdot m_2)^{\pi_2} = m_1^{\pi_2} m_2^{\pi_2} = s_1^{\varphi} s_2^{\varphi}.$$

Portanto, φ é um homomorfismo. Por fim, seja $t \in S$ arbitrário. Dado que $M^{\pi_2} = S$, existe $m = (s, t) \in M$. Daí $s = m^{\pi_1}$ de modo que $t = m^{\pi_2} = s^{\varphi}$. Ou seja, φ é sobrejetiva. Concluímos, assim, que φ é um isomorfismo, e a afirmação segue. Por construção,

$$M \leq \Delta_{\varphi} = \{(x, y) \in G \mid x^{\varphi} = y\}.$$

Dado que M é maximal em G, obtemos que $M = \Delta_{\varphi}$, encerrando a demonstração do caso $n = 2$, como queríamos.

Vamos nos concentrar agora em mostrar que a sequência $d(S), d(S^2), \ldots, d(S^n), \ldots$ é ilimitada. Sejam m um inteiro positivo e

$$\begin{aligned} y_1 &= (x_{11}, x_{12}, \ldots, x_{1i}, \ldots, x_{1j}, \ldots, x_{1n}) \\ y_2 &= (x_{21}, x_{22}, \ldots, x_{2i}, \ldots, x_{2j}, \ldots, x_{2n}) \\ &\vdots \\ y_m &= (x_{m1}, x_{m2}, \ldots, x_{mi}, \ldots, x_{mj}, \ldots, x_{mn}) \end{aligned}$$

m elementos de S^n. Dizemos que as colunas $C_i = [x_{1i}\ x_{2i} \cdots x_{mi}]$ e $C_j = [x_{1j}\ x_{2j} \cdots x_{mj}]$ estão na mesma $\mathrm{Aut}(S)$-*órbita* se $C_i^\varphi = C_j$, para algum $\varphi \in \mathrm{Aut}(S)$, isto é, $x_{kj} = x_{ki}^\varphi$ para todo $k \in \{1, \ldots, m\}$. Afirmamos que $\langle y_1, \ldots, y_m \rangle = S^n$ se, e somente se, cada uma das colunas $C_1, \ldots, C_n$ gera S e duas quaisquer destas estão em $\mathrm{Aut}(S)$-órbitas distintas. De fato, assumamos que $\langle y_1, \ldots, y_m \rangle = S^n$ e que exista $i \in \{1, \ldots, n\}$ tal que $C_i = [x_{1i}\ x_{2i} \cdots x_{mi}]$ não gere S. Dessa forma, existe um subgrupo maximal M de S com $x_{1i}, x_{2i}, \ldots, x_{mi} \in M$ de modo que

$$\langle y_1, \ldots, y_m \rangle \leq S \times \cdots \times S \times M \times S \times \cdots \times S < S^n,$$

um absurdo. Assim, cada coluna gera S. Por outro lado, se existissem $i \neq j$ em $\{1, \ldots, n\}$ e $\varphi \in \mathrm{Aut}(S)$ tais que $C_j = C_i^\varphi$, então

$$\langle y_1, \ldots, y_m \rangle \leq \Delta_{\varphi,i,j} < S^n,$$

novamente um absurdo. Ou seja, duas quaisquer colunas estão em $\mathrm{Aut}(S)$-órbitas distintas. A recíproca se argumenta de forma parecida: basta supor que $\langle y_1, \ldots, y_m \rangle \neq G$, logo existirá um subgrupo maximal H de S^n que contém $y_1, \ldots, y_m$. Se H for do tipo produto, então vamos obter uma coluna que não gera S; e se H for do tipo diagonal, chegaremos a duas colunas na mesma $\mathrm{Aut}(S)$-órbita. Portanto, a afirmação segue.

Seja m um inteiro maior ou igual a 2. Vamos mostrar que

$$f(S, m) = 1 + \frac{\phi_S(m)}{|\mathrm{Aut}(S)|},$$

sendo f a função estudada no Capítulo 2. Com efeito, queremos o maior valor de n para o qual $d(S^n) = m < d(S^{n+1})$. Isto equivale a determinar o maior número de colunas (m-uplas de elementos de S) satisfazendo as duas condições da afirmação provada acima. Seja $\mathscr{S}$ o conjunto das m-uplas $(t_1, \ldots, t_m) \in S^m$ tais que $\langle t_1, \ldots, t_m \rangle = S$. Como visto no Exemplo 2.4.7, $\mathrm{Aut}(S)$ age de maneira natural em $\mathscr{S}$ por

$$((t_1, \ldots, t_m), \varphi) \mapsto (t_1^\varphi, \ldots, t_m^\varphi),$$

e todas as órbitas têm cardinalidade $|\mathrm{Aut}(S)|$. Desse modo, sendo n o número de órbitas dessa ação, temos que $n = \phi_S(m)/|\mathrm{Aut}(S)|$. Tomando uma m-upla de cada órbita e colocando estas m-uplas em forma de colunas, obtemos uma matriz $m \times n$, onde as m linhas geram S^n, pois duas quaisquer dessas colunas estão em $\mathrm{Aut}(S)$-órbitas distintas.

Ou seja, S^n é m-gerado. E S^{n+1} não é m-gerado pois caso contrário a ação acima teria mais do que n órbitas. Portanto, $f(S,m) = 1 + \phi_S(m)/|\mathrm{Aut}(S)|$.

Por fim, se $d(S), d(S^2), \ldots, d(S^n), \ldots$ fosse limitada, então existiria $m \geq 2$ tal que $d(S^n) \leq m$ para todo $n \in \mathbb{Z}_+$. Mas tomando $k = \phi_S(m)/|\mathrm{Aut}(S)|$, teríamos, como acabamos de ver, que $d(S^{k+1}) > m$, uma contradição. Concluímos, assim, que $d(S^n)$ tende a infinito com n, como queríamos demonstrar.

Referências Bibliográficas

[1] ASCHBACHER, M; GURALNICK, R. Some applications of the first cohomology group. *Journal of Algebra*, 90(2): 446–460, 1984.

[2] BARNES, D. W. On complemented chief factors of finite soluble groups. *Bulletin of the Australian Mathematical Society*, 7(1): 101–104, 1972.

[3] BLACKBURN, S. R.; NEUMANN, P. M.; VENKATARAMAN, G. *Enumeration of Finite Groups*. Vol. 7, Cambridge University Press, 2007.

[4] CAMERON, P. J.; LUCCHINI, A.; RONEY-DOUGAL, C. M. Generating sets of finite groups. *Transactions of the American Mathematical Society*, 370(9): 6751–6770, 2018.

[5] CECCHERINI-SILBERSTEIN, T.; COORNAERT, M. *Cellular Automata and Groups*. Vol. 36, Springer-Verlag Berlin Heidelberg, 2010.

[6] CRESTANI, E.; LUCCHINI, A. Bias of group generators in the solvable case. *Israel Journal of Mathematics*, 207(2): 739–761, 2015.

[7] CRESTANI, E; LUCCHINI, A. The generating graph of finite soluble groups. *Israel Journal of Mathematics*, 198(1): 63–74, 2013.

[8] DALLA VOLTA, F.; LUCCHINI, A. Finite groups that need more generators than any proper quotient. *Journal of the Australian Mathematical Society*, (Series A) 64(1): 82–91, 1998.

[9] DALLA VOLTA, F.; LUCCHINI, A. Generation of almost simple groups. *Journal of Algebra*, 178: 194–223, 1995.

[10] DIXON, J. D. The probability of generating the symmetric group. *Mathematische Zeitschrift*, 110(3): 199–205, 1969.

[11] FRIED, M. F.; JARDEN, M. *Field Arithmetic*. 2nd edition, Springer-Verlag Berlin Heidelberg, 2005.

[12] GARCIA, A.; LEQUAIN, Y. *Elementos de Álgebra*. 6ª edição, SBM. Rio de Janeiro: IMPA, 2018.

[13] GASCHÜTZ, W. Die Eulersche funktion endlicher aufloÈsbarer gruppen. *Illinois Journal of Mathematics*, 3(4): 469–476, 1959.

[14] GASCHÜTZ, W. Zu einem von BH und H. Neumann gestellten Problem. *Mathematische Nachrichten*, 14(4-6): 249–252, 1955.

[15] HALL, P. The Eulerian functions of a group. *The Quarterly Journal of Mathematics*, (1): 134–151, 1936.

[16] HOFFMAN, K.; KUNZE, R. *Linear Algebra*. 2nd edition, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1971.

[17] JACOBSON, N. *Basic Algebra I*. 2nd edition, Dover Publications, 2009.

[18] LUCCHINI, A. Generators and minimal normal subgroups. *Archiv der Mathematik*, 64(4): 273–276, 1995.

[19] LUCCHINI, A. The X-Dirichlet polynomial of a finite group. *Journal of Group Theory*, 8: 171–188, 2005.

[20] LUCCHINI, A.; MENEGAZZO, F. Generators for finite groups with a unique minimal normal subgroup. *Rendiconti del Seminario Matematico della Università di Padova*, 98: 173–191, 1997.

[21] RIBES, L.; ZALESSKII, P. *Profinite Groups*. 2nd edition, vol. 40, Springer-Verlag Berlin Heidelberg, 2000.

[22] ROBINSON, D. J. S. *A Course in the Theory of Groups*. 2nd edition, Springer-Verlag New York, Inc., 1996.

[23] ROBINSON, D. J. S.; WILSON, J. S. Soluble groups with many polycyclic quotients. *Proceedings of the London Mathematical Society*, 3(2): 193–229, 1984.

[24] ROSE, J. S. *A Course on Group Theory*. Cambridge University Press, 1978.

[25] STEINBERG, R. Generators for simple groups. *Canadian Journal of Mathematics*, 14: 277–283, 1962.

[26] SUZUKI, M. *Group Theory I*. Springer-Verlag Berlin Heidelberg, 1982.