Universidade de Brasília - UnB
Instituto de Ciências Exatas - IE
Mestrado acadêmico em Matemática

SOBRE A ORDEM MÉDIA DE GRUPOS FINITOS

por

Gabriel Azevedo Miranda

Brasília/DF
2023

GABRIEL AZEVEDO MIRANDA

Sobre a ordem média de grupos finitos

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Igor dos Santos Lima

Brasília/DF

2023

GABRIEL AZEVEDO MIRANDA

Sobre a ordem média de grupos finitos

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática.

Aprovada em: 21/07/2023.

BANCA EXAMINADORA

Prof. Dr. Igor dos Santos Lima (Orientador)
Universidade de Brasília (UnB)

Prof. Dr. Martino Garonzi
Universidade de Brasília (UnB)

Prof. Dr. Mohsen Amiri
Universidade Federal do Amazonas (UFAM)

AGRADECIMENTOS

Este trabalho não seria possível sem os professores que tive. No entanto, seria difícil nomear todos que tiveram impacto significativo na formação deste que vos fala. Cito, portanto, professores que me inspiraram diretamente para prosseguir na carreira acadêmica. São eles: Jorge Augusto, Wembesom Mendes e Vinicius Facó. Obrigado pela generosidade ao atribuir minhas notas e por não medirem esforços ao apontar meus equívocos. Vocês faziam valer a pena cada minuto das quatro horas de ônibus gastas por dia de aula. Agradeço também, obviamente, meu orientador Igor dos Santos Lima pela compreensão, pela parceria, pela disposição, sempre com humildade e pé no chão. Anota ai!

Sou muito grato pelo apoio e inspiração que o IFB me proporcionou. Mais especificamente, agradeço aos amigos do IFB que cursaram o mestrado comigo: Eliézer e Paulo. Vocês foram minha companhia durante as qualificações. A trajetória de sair do IFB e ir à UnB foi comparável a sair de uma pequena cidade interiorana e chegar a uma grande metrópole. Por isso, agradeço vocês por transformarem o Departamento de Matemática num ambiente acolhedor. Obrigado também Leonardo, Sharmenya e Millena, companheiros que fiz neste trajeto. Foi ótimo estar presente nos grupos de estudo, correria do semestre e sobreviver às disciplinas.

Este trabalho não seria possível sem o apoio dos meus avós: Dona Jailma e Ademir Lopes. Dividir o mesmo teto com vocês durante e após a pandemia foi gratificante. Sempre me senti presente em seus corações, afinal o tamanho deles é diretamente proporcional à inabilidade de manipular aplicativos de celular. Neste sentido, há espaço para mim com relativa folga, e garanto que cada um dos outros sete netos sintam o mesmo. É um enorme prazer compartilhar minha vida com vocês. Saibam que amo vocês e espero que este amor esteja presente nas minhas ações.

Agora, cito a pessoa mais essencial neste percurso: Larissa. Obrigado por ouvir meus lamentos, minhas angústias, minhas alegrias, minhas reclamações. Você sempre me estimulou a seguir este rumo de pesquisa, mesmo possuindo um incrível desinteresse pela teoria de grupos. Não a culpo, complicado ser uma pessoa sã e, ao mesmo tempo, ver beleza em homomorfismos, nilpotências e outras loucuras. Suspeito que esses assuntos são gatilhos para suas crises de enxaqueca, peço perdão. Espero que minha presença ilumine seu dia, não a ponto de atiçar sua fotossensibilidade, mas sim uma presença que seja tão gratificante quanto você é para mim.

Agradeço também à gata Vânia Bambirra, companheira nestes dois anos de mestrado. Perdão por confundir você com sacos de lixo e pequenas aparições sobrenaturais,

os humanos possuem um grande problema com visão periférica e crenças tolas. Eu, em particular, tenho certa dificuldade em desenvolver simpatia por quem pratica fugas incessantes pulando o muro e subindo no teto. No entanto, não confundi você com nenhum alienígena, mesmo literalmente caindo dos céus direto para o teto aqui de casa. Pelo contrário, encarei você como um presente, um anjo, e obrigado por sempre estar à espreita de pequenos roedores e de insetos repugnantes. Mesmo que a vida adulta te torne uma gata preguiçosa e ranzinza, você continua sendo a bola de pelo mais linda que eu tive o prazer de cuidar.

Não posso esquecer de mencionar meus agradecimentos a toda ajuda financeira que o Departamento de Matemática da UnB proporcionou. Tive a oportunidade de apresentar trabalhos em João Pessoa, Curitiba e Rio de Janeiro; viagens muito bem aproveitadas, diga-se de passagem. Estas experiências me fizeram conhecer uma parcela significativa da comunidade de álgebra pelo Brasil, algo essencial para um estudante.

Quero agradecer à banca examinadora composta pelos Professores Mohsen Amiri e Martino Garonzi. Sem dúvida esta dissertação foi agraciada pelas contribuições relevantes propostas, algo somente possível graças a uma leitura atenta e cuidadosa.

Por fim, agradeço a todo ser humano que de alguma forma me presenteou com seu incentivo, sobretudo os amigos mais próximos. Pela impossibilidade do texto em reproduzir som, imaginem que neste momento toca *"We are the champions"*, da gloriosa banda *Queen*, enquanto vocês leem pausadamente os seguintes nomes (em ordem alfabética): Carol, Eldo, Lorena, Patric e Vine.

Abraço a todos e até a próxima.

"Logic is the beginning of wisdom, Valeris, not the end."
- Spock

"Dizia eu que a aritmética..."
- Mestre Lingui..., digo, Professor Girafales

RESUMO

Seja $o(G)$ a ordem média dos elementos de um grupo finito G definida como

$$o(G) = \frac{\psi(G)}{|G|},$$

tal que $\psi(G)$ é soma das ordens de todos os elementos de G. Uma Conjectura proposta por A. Jaikin-Zapirain consiste em: se N é um subgrupo normal de G, então $o(G) \geq o(N)^{1/2}$. Dito isto, E. I. Khukhro, A. Moreto e M. Zarrin apresentaram uma resposta negativa para esta Conjectura. Desta forma, temos como objetivo apresentar a construção dos contra-exemplos fornecida por eles. Além disso, também trataremos sobre as implicações deste trabalho que responde a Conjectura, sobretudo um critério de solubilidade que envolve o conceito de ordem média. O critério diz o seguinte: se $o(G) < o(A_5)$, então G é solúvel. Este resultado foi provado por M. Herzog, P. Longobardi e M. Maj.

Palavras-chave: Ordem média, soma de ordens, grupos solúveis, grupos simples.

ABSTRACT

Let $o(G)$ be the average order of the elements of a finite group G defined as

$$o(G) = \frac{\psi(G)}{|G|},$$

such that $\psi(G)$ is the sum of the orders of all elements of G. A conjecture proposed by A. Jaikin-Zapirain consists of: if N is a normal subgroup of G, then $o(G) \geq o(N)^{1/2}$. That said, E. I. Khukhro, A. Moreto and M. Zarrin gave a negative answer to this Conjecture. In this way, we aim to present the construction of the counterexamples provided by them. In addition, we will also deal with the implications of this work that responds to the Conjecture, especially a solubility criterion that involves the concept of average order. The following says: if $o(G) < o(A_5)$, then G is solvable. This result has been proved by M. Herzog, P. Longobardi and M. Maj.

Keywords: Average order, sum of orders, soluble groups, simple groups.

SUMÁRIO

Introdução

O estudo das funções aritméticas para a classificação de grupos finitos é uma área de grande abrangência. Essencialmente, quando lidamos com grupos finitos, frequentemente recorremos às propriedades aritméticas para resolver questões relacionadas à estrutura. Naturalmente, explorar temas como a ordem dos elementos, a soma das ordens dos elementos, o produto das ordens, entre outros, é uma extensão dessa abordagem para classificar grupos finitos. Assim, a motivação central é compreender as propriedades aritméticas de um grupo finito e relacionar com a estrutura do mesmo, uma vez que grupos finitos estão intimamente interligados com a aritmética. No contexto desta dissertação, trataremos da função que calcula a ordem média das ordens dos elementos de um grupo finito.

Definimos a ordem média de um grupo finito G, denotado por $o(G)$, como a razão de $\psi(G)$ por $|G|$, em que $\psi(G)$ denota a soma das ordens dos elementos de G. Em 2011, Andrei Jaikin-Zapirain introduziu a função $o(G)$ no artigo *"On the number of conjugacy classes of finite nilpotent groups"*. O autor relacionou este conceito para o estudo de outra função aritmética, $k(G)$, que informa a quantidade de classes de conjugação de um grupo finito G. Além disso, demonstrou a desigualdade $o(G) \geq o(Z(G))$, para todo grupo finito G. Logo após, no mesmo artigo, A. Jaikin Zapirain propõe a seguinte conjectura:

Conjectura 0.1. (Conjectura de Andrei Jaikin-Zapirain) Seja G um grupo finito e seja $N \trianglelefteq G$. Então $o(G) \geq o(N)^{1/2}$.

Tal Conjectura é o ponto inicial para o artigo de E. I. Khukhro, A. Moretó e M. Zarrin, denominado *"The average element order and the number of conjugacy classes of finite groups"*. Em 2021, os autores conseguiram demonstrar que a Conjectura de Andrei Jaikin-Zapirain é falsa para uma classe de p-grupos muito específica, os chamados p-grupos secretos de *Wall*. No mesmo artigo, os autores estipularam outra conjectura:

Conjectura 0.2. (Critério de Solubilidade) Seja G um grupo finito. Se $o(G) < o(A_5) = 211/60$, então G é solúvel.

Diferentemente da Conjectura de Andrei Jaikin-Zapirain, o Critério de Solubilidade foi

confirmado por M. Herzog, P. Longobardi e M. Maj no trabalho *Another criterion for solvability of finite groups*.

Esta dissertação, de modo geral, possui como objetivo apresentar a construção dos contraexemplos à Conjectura de Andrei Jaikin-Zapirain e apresentar a demonstração do Critério de Solubilidade que envolve a ordem média de um grupo finito G. Para tanto, recorreremos ao estudo de p-grupos, à classificação de grupos simples e aos resultados de grupos não-solúveis e seus respectivos automorfismos, mais especificamente automorfismos que invertem elementos.

No Capítulo 1 serão apresentados alguns conceitos elementares da Teoria de Grupos Finitos. Abordaremos temas como solubilidade e nilpotência, que nos darão condições para o estudo nos capítulos subsequentes.

No Capítulo 2, a referência principal deve-se a E. I. Khukhro, A. Moretó e M. Zarrin [2]. Neste capítulo, apresentaremos definições e resultados gerais relacionados à ordem média de grupos finitos, assim como a relação entre a quantidade de elementos de ordem 2, que denotamos por $i_2(G)$, e a ordem média de G. Discutiremos perguntas naturais, como a comparação entre a ordem média de um grupo finito e a ordem média de seus subgrupos, ordem média de grupos quocientes, fórmulas para o cálculo da ordem média etc. Outra pergunta que abordaremos: dois grupos com a mesma ordem média são necessariamente isomorfos? Além disso, relacionaremos a ordem média com três classes de p-grupos: p-grupos anti-Hughes, *powerful* e secretos. Os grupos anti-Hughes aparecem como uma expectativa de resposta à Conjectura de Andrei Jaikin-Zapiarain, enquanto os p-grupos *powerful* são apresentados com o objetivo de estimarmos a ordem média de um representante desta classe, algo que nos será útil no Capítulo 3. Já os p-grupos secretos, mais especificamente os p-grupos secretos de *Wall*, são apresentados como forma explícita da construção de contraexemplos à Conjectura de Andrei Jaikin-Zapirain.

Já no Capítulo 3 mostraremos que a Conjectura de Andrei Jaikin-Zapirain é falsa. Esta resposta traz consigo a construção de contraexemplo não somente para o expoente $1/2$, mas também para outros valores. De modo geral, a teorema principal a ser demonstrado neste momento do texto será o seguinte:

Teorema 0.1. (E. I. Khukhro, A. Moretó e M. Zarrin, Teorema 1.2 de [2]) Seja $c > 0$ um número real e seja $p \geq 3/c$ um primo. Então existe um p-grupo finito com um subgrupo normal abeliano N tal que $o(G) < o(N)^c$.

Ainda no Capítulo 3, demonstraremos dois resultados auxiliares cruciais ao envolver o grupo A_5 e o valor $o(A_5) = 211/60$, que nos permitirão demonstrar o Critério de Solubilidade. O primeiro deles trata-se de grupos simples e a quantidade de primos que dividem suas respectivas ordens. O segundo, toma como base teórica o trabalho de W. M.

Potter [20]. Antes de enunciá-los, definamos alguns conceitos. Dizemos que $\theta \in Aut(G)$ inverte $g \in G$ se $g^\theta = g^{-1}$. Com base nisso, definimos a função $r(G, \theta)$ como a razão entre $|S(\theta)|$ e $|G|$, em que $S(\theta)$ denota a quantidade de elementos de G invertidos pelo automorfismo θ. Além disso, denote por $\Pi(G)$ o conjunto de todos os primos que dividem $|G|$. Detalhadamente, demonstraremos os seguintes teoremas na seguinte ordem de aparição:

Teorema 0.2. (M. Herzog, P. Longobardi e M. Maj, Teorema 4.19 de [3]) Seja G um grupo finito simples e suponha $\Pi(G) \subseteq \{2, 3, 5, 7, 11, 13\}$. Então

$$G \cong A_5 \quad ou \quad o(G) \geq 3,55 > o(A_5).$$

Teorema 0.3. (M. Herzog, P. Longobardi e M. Maj, Teorema 5.5 de [3]) Seja G um grupo finito não-solúvel tal que G não contém subgrupos normais solúveis não triviais. Seja $\theta \in Aut(G)$. Se $r(G, \theta) > 2/9$, então $G \cong A_5$.

Teorema 0.4. (M. Herzog, P. Longobardi e M. Maj, Teorema B de [3]) Seja G um grupo finito e suponha que

$$o(G) < o(A_5) = \frac{211}{60}.$$

Então G é solúvel.

Capítulo 1

Preliminares

Neste capítulo abordaremos resultados básicos sobre a teoria de grupos finitos, mais especificamente, sobre solubilidade e nilpotência de grupos finitos. Estes resultados serão utilizados ao longo deste trabalho. Todo o capítulo foi baseado nas obras de A. Garcia e Y. Lequain [21], D. J. S. Robinson [22] e J. J. Rotman [23], com as devidas notações alteradas para nosso contexto.

1.1 Solubilidade e Nilpotência

Vejamos algumas definições e teoremas elementares da teoria de grupos finitos.

Definição 1.1. Sejam X um conjunto e G um grupo. Então X é um G-conjunto se existe uma função

$$\begin{aligned} \alpha : G \times X &\to X \\ (g, x) &\mapsto gx \end{aligned}$$

tal que

(1) $1x = x$, para todo $x \in X$;

(2) $g(hx) = (gh)x$, para todo $g, h \in G$ e $x \in X$.

Neste caso, dizemos que α é uma ação à esquerda de G sbre X.

Definição 1.2. Sejam X um conjunto e G um grupo. Então X é um G-conjunto se existe uma função

$$\begin{aligned} \alpha : X \times G &\to X \\ (g, x) &\mapsto xg \end{aligned}$$

tal que

(1) $x1 = x$, para todo $x \in X$;

(2) $(xg)h = x(gh)$, para todo $g, h \in G$ e $x \in X$.

Neste caso, dizemos que α é uma ação à direita de G sobre X.

Definição 1.3. Seja X é um G-conjunto. Se $x \in X$, dizemos que a G-órbita de x é

$$O(x) = \{gx \mid g \in G\} \subset X.$$

Definição 1.4. Seja X é um G-conjunto. Se $x \in X$, dizemos que o estabilizador de x é o subgrupo

$$G_x = \{g \in G \mid gx = x\} \leq G.$$

Se G age em $X = G$ da forma $(g, x) \mapsto x^g = g^{-1}xg$, a órbita de x coincide com o conjunto $cl(x) = \{x^g \mid g \in G\}$ e o estabilizador de x coincide com o conjunto $C_G(x) = \{g \in G \mid xg = gx\}$, que, por sua vez, são conhecidos como a classe de conjugação de x e o centralizador de x, respectivamente. Denotamos por $Z(G)$ o centro do grupo G, e dizemos que H é subgrupo central em G, ou simplesmente central em G, se $H \leq Z(G)$. Se P é um p-subgrupo de Sylow de G, escrevemos $P \in Syl_p(G)$.

Sejam G um grupo finito e N um subgrupo normal de G. Dado um elemento $g \in G$, denotaremos a ordem de g por $|g|$. Dado um elemento $gN \in G/N$, denotaremos a ordem de gN em G/N por $|gN|$. Detalhadamente, a ordem de gN é o menor inteiro n positivo tal que $g^n \in N$.

Proposição 1.1. Sejam G um grupo finito, $a \in G$ e n um número natural. Então

$$|a^n| = \frac{|a|}{mdc(n, |a|)}.$$

Proposição 1.2. Seja G um grupo finito. Então existem $x_1, \ldots, x_s \notin Z(G)$ tais que

$$|G| = |Z(G)| + \sum_{i=1}^{s} |G : C_G(x_i)|.$$

O próximo teorema é conhecido como o Teorema da Órbita-Estabilizador.

Teorema 1.1. Se X é um G-conjunto e $x \in X$, então $|O(x)| = [G : G_x]$.

Demonstração. Pode ser vista em [23], Teorema 3.19. □

Teorema 1.2. (Lema de Burnside) Seja G um grupo finito que age em um conjunto

X. Seja N o número de G-órbitas de X. Então

$$N = \frac{1}{|G|} \sum_{x \in X} |G_x|.$$

Demonstração. Pode ser vista em [23], Teorema 3.22. □

O Lema de Burnside nos permitirá estabelecer uma comparação entre $o(G)$ e $k(G)$, ou seja, a ordem média e a quantidade de classes de conjugação de G, respectivamente. Mais especificamente, demonstraremos que $k(G) \geq o(G)$, para todo grupo finito G.

Teorema 1.3. (1° Teorema do Isomorfismo) Sejam G e H grupos e $\psi : G \to H$ um homomorfismo. Então

$$\frac{G}{\ker(\psi)} \cong Im(\psi);$$

(2° Teorema do Isomorfismo) Sejam G um grupo, $N \trianglelefteq G$ e $H \leq G$. Então

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

(3° Teorema do Isomorfismo) Sejam G um grupo, $M \trianglelefteq G$ e $N \trianglelefteq G$. Se $M \leq N$, então

$$\frac{G/M}{N/M} \cong \frac{G}{N}.$$

Demonstração. Pode ser encontrada em [21], Teorema V.5.6. □

Teorema 1.4. (Teorema da Correspondência) Sejam G um grupo e $N \trianglelefteq G$. Seja

$$\begin{aligned} \psi \ : \ & G \longrightarrow G/N \\ & g \longmapsto gN \end{aligned}$$

Seja $\overline{G}$ o conjunto de todos os subgrupos de G que contém N e seja $\overline{G/N}$ o conjunto de todos os subgrupos de G/N. Então para todo $H \in \overline{G}$ temos

$$\begin{aligned} \psi \ : \ & \overline{G} \longrightarrow \overline{G/N} \\ & H \longmapsto H/N \end{aligned}$$

é uma bijeção. Além disso,

(1) $H/N \leq G/N$ se, e somente se, $H \leq G$ e $H/N \trianglelefteq G/N$ se, e somente se, $H \trianglelefteq G$;

(2) $K/N \leq H/N$ se, e somente se, $K \leq H$ e $K/N \trianglelefteq H/N$ se, e somente se, $K \trianglelefteq H$.

Demonstração. Pode ser encontrada em [23], Teorema 2.28. □

Agora, seja G um grupo. Definimos o comutador de $x_1 \in G$ e $x_2 \in G$ como

$$[x_1, x_2] := x_1^{-1} x_2^{-1} x_1 x_2.$$

Generalizando, definimos o comutador de $x_1, \ldots, x_n \in G$ como

$$[x_1, \ldots, x_n] := [[x_1, \ldots, x_{n-1}], x_n], \quad n \geq 3.$$

Podemos estabelecer algumas identidades de comutadores.

Proposição 1.3. Seja G um grupo e seja $x, y, z, w \in G$. Então

(1) $[x, yz] = [x, z][x, y]^z = [x, z][x, y][x, y, z]$;

(2) $[xy, z] = [x, z]^y[y, z] = [x, z][x, z, y][y, z]$;

(3) Se $[x, z] = 1$, então $[x, y]^z = [x, y^z]$;

(4) Se $[y, z] = 1$, então $[x, y]^z = [x^z, y]$;

(5) $([x, y]^z)^w = [x, y]^{zw} = [x^{zw}, y^{zw}]$.

Se H e K são subgrupos de G, o subgrupo comutador de H e K é definido por

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

Denotaremos por G' o subgrupo comutador $[G, G]$, mais conhecido como subgrupo derivado. Um resultado elementar nos diz que $G' \trianglelefteq G$ e G/G' é sempre abeliano, para todo grupo G.

Teorema 1.5. (Argumento de Frattini) Seja K um subgrupo normal de um grupo G. Se P é um p-subgrupo de Sylow de K, então $G = KN_G(P)$.

Demonstração. Pode ser vista em [22], Teorema 5.2.14. □

Teorema 1.6. Seja G um grupo e seja N um subgrupo de G. Então G/N é abeliano se, e somente se, $G' \leq N$.

Um dos principais resultados deste trabalho envolve um critério de solubilidade. Fundamentemos o conceito de grupos solúveis e suas implicações.

Definição 1.5. Seja G um grupo. Dizemos que G é **solúvel** se existe uma série

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$$

tal que cada quociente G_{i+1}/G_i é abeliano para $0 \leq i \leq n-1$. Neste caso, a série é dita

série abeliana. No caso em que todo $G_i \trianglelefteq G$, dizemos que a série é uma série normal. Cada quociente G_{i+1}/G_i é dito fator da série.

Proposição 1.4. Sejam G um grupo, $H \leq G$ e $N \trianglelefteq G$.

(1) Se G é solúvel, então H é solúvel;

(2) Se G é solúvel, então G/N é solúvel.

Demonstração. Pode ser vista em [21], Teorema VII.2.8. □

Proposição 1.5. Sejam N um subgrupo normal de um grupo G e H um subgrupo de G.

(1) Se N e G/N são solúveis, então G é solúvel;

(2) Se N e H são solúveis, então NH é solúvel.

Demonstração. (1) Sejam $\{N_i\}_{i=0}^{r}$ e $\{N_i/N\}_{i=r}^{s}$ séries abelianas de N e G/N, respectivamente. Logo, pelo 3° Teorema do Isomorfismo

$$\frac{N_{i+1}/N}{N_i/N} \cong \frac{N_{i+1}}{N_i}$$

é abeliano, para $r \leq i \leq s$. Portanto,

$$1 = N_0 \trianglelefteq \ldots \trianglelefteq N_r = N \trianglelefteq N_{r+1} \trianglelefteq \ldots \trianglelefteq N_s = G$$

é uma série abeliano para G.

(2) Suponha $G = NH$. Observe que

$$\frac{G}{N} = \frac{NH}{N} \cong \frac{H}{H \cap N}$$

é solúvel. Portanto, pelo item (1), G é solúvel. □

A próxima definição estabelece uma série específica para um grupo, na qual nos permitirá afirmar um critério de equivalência para G ser solúvel.

Definição 1.6. Considere $G^{(0)} = G$, $G^{(1)} = [G, G]$ e $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$, para $n \geq 2$. Daí, $1 \trianglelefteq G^{(k+1)} \trianglelefteq G^{(k)}$ e $G^{(k)}/G^{(k+1)}$ é abeliano, para $k \geq 0$. Quando $n = 1$, escrevemos $G' = G^{(1)}$. Tal série é denominada série derivada.

Proposição 1.6. Um grupo G é solúvel se, e somente se, existe um número natural n tal que $G^{(n)} = 1$.

Demonstração. Suponha G solúvel. Assim, existe uma série abeliana

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G.$$

Por indução em i, podemos mostrar que $G^{(i)} \leq G_i$, $0 \leq i \leq n$. Para $i = 0$, segue que

$$G = G^{(0)} \leq (G_0) = G.$$

Suponha que para $i = n - 1$ temos $G^{(n-1)} \leq G_{n-1}$. Agora, observe que G_{n-1}/G_n é abeliano, logo pelo Teorema 1.6 e pela hipótese de indução temos

$$G^{(n)} = [G^{(n-1)}, G^{(n-1)}] \leq [G_{n-1}, G_{n-1}] = (G_{n-1})' \leq G_n.$$

Portanto, existe n tal que $G^{(n)} = 1$.

Por outro lado, se existe n natural tal que $G^{(n)} = 1$, então a série derivada é uma série abeliana para G. Portanto, G é solúvel. □

Dizemos que G é um grupo simples se os únicos subgrupos normais de G são 1 e G. Uma observação imediata nos diz que todo grupo de ordem prima é simples e, neste caso, também é solúvel, pois $1 \lhd G$ é uma série abeliana para G.

Proposição 1.7. Seja $G \neq 1$ um grupo solúvel finito. Se G é simples, então existe um primo p tal que $|G| = p$.

Demonstração. Seja $G \neq 1$ um grupo solúvel. Pela Proposição 1.6, existe um inteiro positivo n tal que $G^{(n)} = 1$. Assim, $G' < G$. Por hipótese, G é um grupo simples e $G' \lhd G$, segue que $G' = 1$. Logo, G é abeliano a para todo $1 \neq g \in G$, temos que $\langle g \rangle \trianglelefteq G$, o que nos diz que $\langle g \rangle = G$. Neste caso, $|G| = p$, em que p é um primo, pois não há divisor de $|G|$ além de 1 e $|G|$. □

Um importante teorema sobre solubilidade de grupos finitos pode ser visto a seguir:

Teorema 1.7. (Teorema de Feit-Thompson) Todo grupo finito de ordem ímpar é solúvel.

Demonstração. A demonstração pode ser encontrada em [29]. □

No Capítulo 2 tratamos de p-grupos. A classe dos p-grupos é interligada à classe de grupos nilpotentes.

Definição 1.7. Seja G um grupo. Dizemos que G é **nilpotente** se existe uma série

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_n = G$$

tal que cada quociente $G_i \trianglelefteq G$ e $G_{j+1}/G_j \leq Z(G/G_j)$, para $1 \leq i \leq n$ e $0 \leq j \leq n-1$. Esta série é denominada série central.

Dizemos que H é subnormal em G se existe uma série da seguinte forma:

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G.$$

O grupo ser nilpotente possui relação intrínseca com subnormalidade, como veremos no Teorema 1.10.

Proposição 1.8. Seja P é um p-grupo finito. Então $Z(P) \neq 1$.

Definição 1.8. Definimos a **série central inferior de** G como uma sequência de subgrupos

$$\gamma_1(G) \geq \gamma_2(G) \geq \ldots$$

em que $\gamma_1(G) = G$ e $\gamma_{n+1}(G) = [\gamma_n(G), G]$.

Pela definição acima, constatamos que $\gamma_2(G) = [G, G] = G'$.

Definição 1.9. Definimos a **série central superior de** G como uma sequência de subgrupos

$$Z_0(G) \leq Z_1(G) \leq \ldots$$

em que $Z_0(G) = G$ e para todo $n \in \mathbb{N}$ temos

$$Z\left(\frac{G}{Z_{n-1}(G)}\right) = \frac{Z_n(G)}{Z_{n-1}(G)}.$$

Definição 1.10. Seja G um grupo. A classe de nilpotência de G é o menor inteiro positivo n tal que $\gamma_{n+1}(G) = 1$.

Os grupos abelianos G possuem classe de nilpotência igual a 1, pois $G' = \gamma_2(G) = 1$. Os grupos G que possuem classe 2 satisfazem $G' \leq Z(G)$, isto é, dizemos que G é nilpotente de classe 2 se, e somente se, $G' \leq Z(G)$. Isto acontece, pois, neste caso, se $G' \leq Z(G)$ temos que $G' = \gamma_2(G)$ é abeliano, logo $\gamma_3(G) = 1$. A recíproca vale pelo mesmo motivo.

Proposição 1.9. Seja G um grupo nilpotente de classe 2. Então

(1) $[x, y^{-1}] = [y, x]$, para todos $x, y \in G$;

(2) $(xy)^n = x^n y^n [y,x]^{\frac{n(n-1)}{2}}$, para todos $x, y \in G$.

Proposição 1.10. Sejam G um grupo e $N \trianglelefteq G$. Se G é nilpotente de classe n, então G/N é nilpotente de classe menor ou igual a n.

Demonstração. Pode ser vista em [23], Teorema 5.36. □

Teorema 1.8. (Teorema de Fitting) Sejam G um grupo, $H \trianglelefteq G$ e $K \trianglelefteq G$. Se H e K são nilpotentes de classe n e m, respectivamente, então HK é nilpotente de classe até $n+m$.

Demonstração. Pode ser vista em [22], Teorema 5.2.8. □

Há algumas formas de descobrir se um grupo não é nilpotente sem precisar descobrir se existe uma série central. Uma dessas maneiras é investigar se o centro do grupo é trivial.

Proposição 1.11. Seja G um grupo nilpotente não-trivial. Então $Z(G)$ é não-trivial.

Demonstração. Seja $G \neq 1$ um grupo nilpotente. Pela Proposição 1.6, existe um inteiro positivo minimal n tal que $\gamma_n(G) \neq 1$. Com isso, $\gamma_{n+1}(G) = 1$. Observe que

$$1 = \gamma_{n+1}(G) = [\gamma_n(G), G].$$

Logo, para todo $x \in \gamma_n(G)$ e $g \in G$ temos que $1 = [x,g]$, isto é, $gx = xg$. Portanto, $1 \neq \gamma_n(G) \leq Z(G)$. □

Se tivermos que responder rapidamente se o grupo S_3 é nilpotente ou não, naturalmente não teríamos dificuldade em responder que S_3 não é nilpotente frente à Proposição 1.11, uma vez que $Z(S_3) = 1$. Da mesma forma, todo grupo simples não-abeliano não é um grupo nilpotente.

Proposição 1.12. Seja P é um p-grupo finito. Então P é nilpotente.

Demonstração. Seja P um grupo finito tal que $|P| = p^n$, para algum primo p. Façamos a demonstração por indução em n. Para $|P| = p^1 = p$, o grupo P é cíclico, logo nilpotente. Agora, suponha que todo grupo de ordem p^i, com $i < n$, é um grupo nilpotente.

Considere que $|P| = p^n$. Pela Proposição 1.11, $Z(P) \neq 1$, logo $|P/Z(P)| < |P|$. Assim, $P/Z(P)$ é nilpotente existe uma série

$$\frac{Z(P)}{Z(P)} \trianglelefteq \frac{H_0}{Z(P)} \trianglelefteq \ldots \trianglelefteq \frac{H_{n-1}}{Z(P)} \trianglelefteq \frac{H_n}{Z(P)} = \frac{P}{Z(P)},$$

tal que $H_i/Z(P) \trianglelefteq P/Z(P)$, para $0 \leq i \leq n$, e

$$\frac{H_{i+1}/Z(P)}{H_i/Z(P)} = Z\left(\frac{P/Z(P)}{H_i/Z(P)}\right),$$

para $0 \leq i \leq n-1$. Pelo Teorema 1.3,

$$\frac{H_{i+1}}{H_i} \cong \frac{H_{i+1}/Z(P)}{H_i/Z(P)} = Z\left(\frac{P/Z(P)}{H_i/Z(P)}\right) \cong Z\left(\frac{P}{H_i}\right).$$

Portanto, a série

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = P$$

é uma série central para P e, com isso, P é nilpotente. □

O resultado abaixo é similar ao que acontece com os grupos solúveis e suas respectivas séries derivadas.

Proposição 1.13. Seja G um grupo. As afirmações abaixo são equivalentes:

(1) G é nilpotente;

(2) Existe um inteiro positivo n tal que $\gamma_{n+1}(G) = 1$;

(3) Existe um inteiro positivo n tal que $Z_n(G) = G$.

Teorema 1.9. Todo grupo nilpotente é um grupo solúvel.

Porém, nem todo grupo solúvel é nilpotente. Basta notar que o grupo S_3 é solúvel. De fato, $\langle(123)\rangle$ e $S_3/\langle(123)\rangle$ são solúveis e, pela Proposição 1.5, S_3 é solúvel. Mas, como vimos, S_3 não é nilpotente.

Considere G um grupo. Dizemos que um elemento $g \in G$ é um não-gerador, ou supérfluo, de G se $G = \langle X\rangle$ sempre que $G = \langle X, g\rangle$. Um importantíssimo subgrupo é o chamado subgrupo de Frattini.

Definição 1.11. Seja G um grupo. Dizemos que o subgrupo de Frattini é o subgrupo que coincide com o conjunto dos elementos não-geradores de G. Notação: $\Phi(G)$.

Proposição 1.14. Seja G um grupo finito. Então

(1) $\Phi(G) \leq$ G;

(2) $\Phi(G)$ é igual a interseção de todos os subgrupos maximais de G;

O próximo teorema estabelece equivalências para nilpotência de grupos finitos.

Teorema 1.10. Seja G um grupo finito. Então as afirmações são equivalentes:

(1) G é nilpotente;

(2) Todo subgrupo H de G é subnormal;

(3) Se $H < G$, então $H < N_G(H)$;

(4) Se M é subgrupo maximal de G, então M é normal em G. Além disso, existe um primo p tal que p divide $|G|$ e $|G : M| = p$;

(5) $G' \leq \Phi(G)$;

(6) Se P é p-subgrupo de Sylow de G, então P é normal em G;

(7) G é produto direto de todos os seus p-subgrupos de Sylow.

Demonstração. (1) $\implies$ (2): Seja H um subgrupo próprio de G. Sabemos que $Z_i(G) \trianglelefteq G$, logo $Z_i(G) \trianglelefteq HZ_{i+1}(G)$. Pelo Teorema da Correspondência, $HZ_{i+1}(G) \leq G$ se, e somente se,

$$\frac{HZ_{i+1}(G)}{Z_i(G)} \leq \frac{G}{Z_i(G)}.$$

Além disso, como $Z_i(G) \trianglelefteq HZ_{i+1}(G)$ temos que $Z_i(G) \trianglelefteq HZ_i(G)$. Pelo Teorema da Correspondência 1.4, H é subnormal em G.

(2) $\implies$ (3): Seja H um subgrupo próprio de G. Por hipótese, H é subnormal em G, logo existe uma série

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_{n-1} \trianglelefteq H_n = G,$$

tal que $H_i \trianglelefteq H_{i+1}$ para $0 \leq i \leq n-1$. Sem perda de generalidade, suponha que $H < H_1$. Então $H < H_1 \leq N_G(H)$.

(3) $\implies$ (4): Seja M um subgrupo maximal de G. Por hipótese, $M < N_G(M)$. Pela maximalidade M, temos que $M < N_G(M) = G$, logo $M \lhd G$. Como G é nilpotente, pelo Teorema 1.9, G é solúvel e pela Proposição 1.4, segue que G/M é solúvel. Se M é maximal, então G/M é simples e, pela Proposição 1.7, existe um primo p tal que $|G/M| = p$.

(4) $\implies$ (5): Seja M um subgrupo maximal de G. Por hipótese, $M \lhd G$ e $|G/M| = p$. Logo, G/M é abeliano e $G' \leq M$. Como M foi tomado arbitrariamente, segue pela Proposição 1.14 que

$$G' \leq \bigcap_{M \leq G} M = \Phi(G).$$

(5) $\implies$ (4): Como $G' \leq \Phi(G)$, pela Proposição 1.14, $G' \leq M$ para todo subgrupo maximal M de G. Como $G' \trianglelefteq G$, em particular, $G' \trianglelefteq M$. Assim, $M/G' \trianglelefteq G/G'$, pois G/G' é abeliano. Portanto, pelo Teorema 1.4, segue que $M \trianglelefteq G$. Além disso, G/M é nilpotente

e simples, logo existe um primo p tal que $|G/M| = p$.

(4) $\implies$ (6): Suponha que existe $P \in Syl_p(G)$ tal que P não é normal em G. Neste caso, $N_G(P) < G$, caso $N_G(P) = G$ teríamos que $P \trianglelefteq G$. Assim, existe um subgrupo maximal M tal que

$$N_G(P) \leq M \leq G.$$

Por hipótese, $M \trianglelefteq G$. Pelo Argumento de Frattini 1.5, $G = MN_G(P)$, pois $P \in Syl_p(M)$. Portanto, $M < G$, um absurdo, pois $N_G(P) = M$, logo $P \trianglelefteq G = N_G(P)$.

(6) $\implies$ (7): Considere $|G| = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, em que p_i é primo e $\alpha_i \geq 0$, para $i \in \{1, 2, \dots, n\}$. Por hipótese, cada $P_i \in Syl_{p_i}(G)$ é normal em G. Logo, $G = P_1 \dots P_n$ e $P_i \cap \langle P_{l_1}, \dots, P_{l_n} \rangle = 1$ para $i \notin \{l_1, \dots, l_n\}$. Portanto, $G = P_1 \times \dots \times P_n$.

(7) $\implies$ (1) Cada $P_i \in Syl_{p_i}(G)$ é p_i-grupo e, pela Proposição 1.12, cada P_i é nilpotente. Por fim, pelo Teorema de Fitting 1.8, $G = P_1 \dots P_n$ é nilpotente. □

Teorema 1.11. (Teorema de Frattini) Seja G um grupo finito. Então $\Phi(G)$ é nilpotente.

Demonstração. Por 1.14, sabemos que $\Phi(G) \trianglelefteq G$. Seja $P \in Syl_p(\Phi(G))$. Pelo Argumento de Frattini 1.5,

$$G = \Phi(G)N_G(P) = N_G(P).$$

Logo, todos os p-subgrupos de Sylow de $\Phi(G)$ são normais em G e, consequentemente, são normais em $\Phi(G)$. Portanto, pelo Teorema 1.10, $\Phi(G)$ é produto direto de seus p-subgrupos de Sylow e $\Phi(G)$ é nilpotente. □

Proposição 1.15. Seja G um p-grupo finito. Então $\Phi(G) = 1$ se, e somente se, G é abeliano elementar.

Proposição 1.16. Sejam G um grupo finito e $K \lhd G$ tal que $K \leq \Phi(G)$. Então

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

Demonstração. Pode ser vista em [22], Teorema 5.2.13. □

O próximo teorema chama-se Teorema da Base de Burnside. Este resultado é seminal para teoria de grupos. Com ele, conseguimos encontrar o subgrupo de Frattini mais rapidamente, além de notar que o grupo quociente $G/\Phi(G)$ se comporta como espaço vetorial. Utilizaremos muito este resultado na Subseção 2.2.2

Teorema 1.12. (Teorema da Base de Burnside) Seja G um p-grupo finito. Então

(1) $\Phi(G) = G^pG'$;

(2) $G/\Phi(G)$ é p-abeliano elementar, ou seja, $G/\Phi(G)$ pode ser visto como espaço vetorial sobre $\mathbb{F}_p$;

(3) O conjunto $\{x_1, \ldots, x_d\} \subset G$ é um conjunto minimal gerador G se, e somente se, $\{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ é uma base de $G/\Phi(G)$. Neste caso, $|G/\Phi(G)| = p^d$.

Demonstração. (1) Temos que G é um p-grupo, logo pela Proposição 1.12 G é nilpotente. Pelo Teorema 1.10, segue que $G' \leq \Phi(G)$ e todo subgrupo maximal M de G possui índice p e é normal em G. Logo, para todo $g \in G$ temos

$$g^pM = (gM)^p = M.$$

Assim, $G^p \leq M$ para todo M. Com isso, $G^p \leq \Phi(G)$. Além disso, $G' \leq \Phi(G)$. Como G' e G^p são normais em G, segue que $G^pG' \trianglelefteq \Phi(G)$. Denote $G^pG' = N$. Tome arbitrariamente $gN \in G/N$, temos

$$(gN)^p = g^pN = N.$$

Logo, G/N é abeliano elementar. Pela Proposição 1.15, temos

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

Como $N \leq \Phi(G)$, pela Proposição 1.16, temos

$$\Phi(G/N) = \frac{\Phi(G)}{N}.$$

Assim,

$$N/N = \Phi(G/N) = \frac{\Phi(G)}{N}.$$

Portanto, $\Phi(G) = N = G^pG'$.

(2) Precisamos mostrar que $xy\Phi(G) = yx\Phi(G)$ e $(g\Phi(G))^p = \Phi(G)$, para todos $x, y, g \in G$. Isto equivale a dizer que precisamos mostrar que $[x, y] \in \Phi(G)$ e $g^P \in \Phi(G)$, porém isto já foi feito no item anterior.

(3) Seja $\{x_1, \ldots, x_d\} \subset G$ um conjunto minimal gerador de G. Assim,

$$\frac{G}{\Phi(G)} = \langle x_1\Phi(G), \ldots, x_d\Phi(G)\rangle.$$

Pelo item anterior, $G/\Phi(G)$ é espaço vetorial e o conjunto $\{x_1\Phi(G), \ldots, x_d\Phi(G)\}$ é um conjunto minimal gerador de $G/\Phi(G)$. Além disso, se $G/\Phi(G)$ possui base com d elementos, então $G/\Phi(G) \cong C_p^d$. Logo, $|G/\Phi(G)| = p^d$. □

Capítulo 2

A função $o(G)$

Neste capítulo, trataremos de propriedades básicas da ordem média de elementos de grupos finitos e relacionaremos a ordem média com a quantidade de elementos de ordem 2. Após isso, na Seção 2.2 apresentaremos um estudo sobre três classes de p-grupos (p-grupos anti-Hughes, *powerful* e secretos) e suas relações com a ordem média. As principais referências são os artigos *The average element order and the number of conjugacy classes of finite groups*, de E. I. Khukhro, A. Moretó e M. Zarrin [2] e *Another criterion for solvability of finite groups*, de M. Herzog, P. Longobardi e M. Maj [3].

2.1 Propriedades gerais de $o(G)$

Seja $f : \mathbb{N} \to \mathbb{R}$ uma função e G um grupo finito. Considere

$$s_f(G) = \sum_{x \in G} f(|x|).$$

Um problema comum trata-se do estudo de como $s_f(G)$ determina propriedades sobre a estrutura de G.

Definição 2.1. Seja G um grupo finito. Definamos a somatória

$$\psi(G) := \sum_{x \in G} |x|,$$

e a razão

$$o(G) := \frac{\psi(G)}{|G|}.$$

O número $o(G)$ é chamado de **ordem média de** G.

Podemos estender esta definição para qualquer subconjunto S de G, ou seja, a

ordem média de S é dada por $o(S) = \psi(S)/|S|$.

A função $o(G)$ foi definida primeiramente por A. Jaikin-Zapirain [1].

Exemplo 2.1.

$$o(A_4) = \frac{31}{12} \quad \text{e} \quad o(A_5) = \frac{211}{60}.$$

Quando o cálculo da $\psi(G)$ não for possível manualmente, está subentendido que foi utilizado [GAP] e informações de [15].

A função ψ definida acima foi inicialmente estudada pelos autores H. Amiri, S. M. Jafarian Amiri e I. M. Isaacs [2]. Dentre suas contribuições, o teorema logo após é significativo.

Teorema 2.1. Seja C_n um grupo cíclico de ordem n. Então para qualquer grupo não-cíclico G de ordem n, temos que $\psi(G) < \psi(C_n)$.

A demonstração pode ser vista em [2].

Tal resultado também é válido para a ordem média, isto é, vale $o(G) < o(C_n)$. Observe que se G é um grupo finito, então $\psi(H) < \psi(G)$ para todo subgrupo próprio H de G. Porém, isto não necessariamente ocorre para ordem média. Vejamos um exemplo.

Exemplo 2.2. Considere $S_3 = \{1, (12), (13), (23), (123), (132)\}$ o grupo simétrico de ordem 6. Tome $H = \langle (123) \rangle \cong C_3$ um subgrupo de S_3. Assim,

$$o(H) = \frac{7}{3} > \frac{13}{6} = o(S_3).$$

Caso dois grupos H e K possuam a mesma ordem média, significa que $H \cong K$? A resposta é não! Vejamos um exemplo.

Exemplo 2.3. Considere $H = C_4 \times C_4$ e $K = C_2 \times Q_8$, em que Q_8 é o grupo dos quatérnions. Temos

$$o(H) = \frac{55}{16} = o(K).$$

No entanto, H é abeliano e K é não-abeliano.

Lema 2.1. (Lema 1.1 de [2]) Seja G um grupo finito tal que $G \neq 1$. Então as seguintes afirmações são válidas:

(1) $o(G) \geq 2-(1/|G|) \geq 3/2$. Em particular, se G é um 2-grupo abeliano elementar, então $o(G) = 2-(1/|G|)$ e se G não é um 2-grupo abeliano elementar, então $o(G) \geq 2+(1/|G|)$. Daí, $o(G) \leq 2$ se, e somente se, G é um 2-grupo abeliano elementar e $o(G) = 2-(1/|G|)$;

(2) Se G possui ordem ímpar, então $o(G) \geq 7/3$.

Demonstração. (1) Se G é um grupo finito tal que $G \neq 1$, então

$$\psi(G) \geq 2(|G| - 1) + 1 = 2|G| - 1.$$

Logo,

$$o(G) = \frac{\psi(G)}{|G|} \geq \frac{2|G| - 1}{|G|} = 2 - \frac{1}{|G|} \geq 2 - \frac{1}{2} = \frac{3}{2}.$$

Daí, se G é um 2-grupo abeliano elementar, segue que $\psi(G) = 2|G| - 1$, o que implica em $o(G) = 2 - (1/|G|)$.

Agora, mostraremos que se $o(G) \leq 2$, então G é 2-grupo abeliano elementar. Para tanto, suponha que G não é um 2-grupo abeliano elementar. Assim, existe $x \in G$ tal que $|x| = |x^{-1}| \geq 3$. Desde que $x \neq x^{-1}$, temos

$$\psi(G) \geq 2(|G| - 3) + 1 + 3 \cdot 2 = 2|G| + 1.$$

Logo,

$$o(G) \geq 2 + \frac{1}{|G|} > 2,$$

pois $1/|G| > 0$. Portanto, $o(G) \leq 2$ se, e somente se, G é um 2-grupo abeliano elementar tal que $o(G) = 2 - (1/|G|)$.

(2) Se G possui ordem ímpar, então

$$\psi(G) \geq 3(|G| - 1) + 1 = 3|G| - 2.$$

Portanto,

$$o(G) = 3 - \frac{2}{|G|} \geq 3 - \frac{2}{3} = \frac{7}{3}.$$

□

Naturalmente, a função $o(G)$ preserva algumas propriedades da função $\psi(G)$. Um exemplo disto diz respeito ao próximo resultado, que é uma adaptação do Lema 2.1 de [33].

Proposição 2.1. Sejam H e K grupos finitos. Então

$$o(H \times K) \leq o(H)o(K).$$

Além disso, $mdc(|H|, |K|) = 1$ se, e somente se, $o(H \times K) = o(H)o(K)$. Em particular, se $mdc(|H|, |K|) = 1$ e $H, K \neq 1$, então $o(G) \geq 7/2$.

Demonstração. Utilizaremos o fato de que $|(h, k)| \leq |h||k|$ para todo $h \in H$ e $k \in K$.

Dessa forma, temos

$$o(H \times K) = \frac{\sum_{h \in H} \sum_{k \in K} |(h,k)|}{|H \times K|} \leq \frac{\sum_{h \in H} \sum_{k \in K} |h||k|}{|H||K|} = o(H)o(K).$$

Temos $mdc(|H|, |K|) = 1$ se, e somente se, $|(h,k)| = |h||k|$ para todo $h \in H$ e $k \in K$, isto é, $o(H \times K) = o(H)o(K)$. Agora, se $|H| \neq 1$ e $|K| \neq 1$, então ou H ou K possui ordem ímpar, caso contrário $mdc(|H|, |K|) \neq 1$. Logo, pelo Lema 2.1, temos que

$$o(G) \geq \frac{3}{2} \cdot \frac{7}{3} = \frac{7}{2}.$$

□

Podemos explicitar a ordem média de grupos cíclicos de ordem p^k, tal que p é primo e k é um inteiro positivo. Com isso, temos o seguinte teorema, que por sua vez é uma adaptação do Lema 2.9 de [33] e o Lema 2.9 de [32]:

Teorema 2.2. São válidos cada um dos itens abaixo:

(1) Seja C_{p^k} um grupo cíclico de ordem p^k, para algum primo p. Então

$$o(C_{p^k}) = \frac{p^{2k+1} + 1}{p^{k+1} + p^k}.$$

(2) Considere, agora, C_n o grupo cíclico de ordem n, tal que $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}$, com $p_1 < p_2 < \ldots < p_t$ primos distintos. Denote $P_1, P_2, \ldots, P_t$ os respectivos subgrupos de Sylow de C_n. Então

$$o(C_n) = \prod_{i=1}^{t} o(P_i).$$

Demonstração. (1) Utilizaremos o fato de que um grupo cíclico possui $\varphi(d)$ elementos de ordem d, em que φ denota a função de Euler. Logo,

$$\begin{aligned}
o(C_{p^k}) &= \frac{1\varphi(1)+p\varphi(p)+p^2\varphi(p^2)+\ldots+p^k\varphi(p^k)}{p^k} \\
&= \frac{1+p(p-1)+p^2(p^2-p)+\ldots+p^k(p^k-p^{k-1})}{p^k} \\
&= \frac{1+p(p-1)+p^3(p-1)+\ldots+p^{2k-1}(p-1)}{p^k} \\
&= \frac{1+(p-1)(p+p^3+\ldots+p^{2k-1})}{p^k} \\
&= \frac{1+(p-1)\left[\dfrac{p(p^{2k}-1)}{p^2-1}\right]}{p^k} \\
&= \frac{1}{p^k}\left(\frac{p+1+p^{2k+1}-p}{p+1}\right) \\
&= \frac{p^{2k+1}+1}{p^{k+1}+p^k}.
\end{aligned}$$

(2) Pelo item anterior e o Proposição 2.1, segue imediatamente que

$$o(C_n) = \prod_{i=1}^{t} o(P_i).$$

□

Vejamos, agora, como a ordem média se comporta para grupos quocientes.

Lema 2.2. (Lema 3.1 de [2]) Sejam G um grupo finito e $1 \neq H \trianglelefteq G$. Então

(1) Se $x \in G \setminus H$, então a ordem $|xH|$ de xH em G/H divide a ordem de xh em G para todo $h \in H$. Em particular, $|xh| \geq |xH|$ para todo $h \in H$;

(2) $o(G/H) < o(G)$.

Demonstração. (1) Tome $h \in H$ tal que $|xh| = n$. Então $(xh)^n = 1$ e

$$(xH)^n = (xhH)^n = (xh)^n H = H.$$

Portanto, a ordem de xH em G/H divide n, ou seja, $|xH|$ divide $|xh|$ para todo $h \in H$. Em particular, $|xh| \geq |xH|$ para todo $h \in H$.

(2) Considere um transversal $\tau = \{1, x_1, x_2, \ldots, x_s\}$ de H em G. Assim,

$$G = H\dot{\cup}x_1H\dot{\cup}\ldots\dot{\cup}x_sH \qquad \text{e} \qquad \psi(G) = \psi(H) + \psi(x_1H) + \ldots + \psi(x_sH).$$

Considere $|H| = m$, $H = \{h_1, h_2, \ldots, h_m\}$ e $1 \leq j \leq s$. Por (1), temos que

$$\begin{aligned} \psi(x_jH) &= |x_jh_1| + |x_jh_2| + \ldots + |x_jh_m| \\ &\geq |x_jH| + |x_jH| + \ldots + |x_jH| \\ &= m|x_jH| = |H||x_jH| \end{aligned}$$

Daí,

$$\begin{aligned} \psi(G) &= \psi(H) + \psi(x_1H) + \ldots + \psi(x_sH) \\ &\geq \psi(H) + |H||x_1H| + \ldots + |H||x_sH| \\ &= \psi(H) - |H| + |H| + |H||x_1H| + \ldots + |H||x_sH| \\ &= \psi(H) - |H| + |H|(1 + |x_1H| + \ldots + |x_sH|) \\ &= \psi(H) - |H| + |H|\psi(G/H). \end{aligned}$$

Dividindo por $|G|$ em ambos os lados da desigualdade acima, obtemos

$$\begin{aligned} o(G) &\geq \frac{\psi(H) - |H|}{|G|} + \frac{|H|\psi(G/H)}{|G|} \\ &= \frac{\psi(H) - |H|}{|G|} + o(G/H) \\ &> o(G/H), \end{aligned}$$

uma vez que $\psi(H) > |H|$ e $(\psi(H) - |H|)/|G| > 0$.

□

Agora, temos outra propriedade da $o(G)$ que adaptamos da Proposição 2.6 em [34].

Teorema 2.3. Sejam G um grupo finito e H um subgrupo normal de G. Então

$$o(G) \leq o(G/H)|H|.$$

Demonstração. Considere $|G/H| = s$ e $G/H = \{x_1H, x_2H, \ldots, x_sH\}$. Denote a ordem do elemento x_iH em G/H por t_i, para todo $1 \leq i \leq s$. Então

$$\psi(G/H) = t_1 + t_2 + \ldots + t_s.$$

Além disso,

$$G = x_1H\dot{\cup}x_2H\dot{\cup}\ldots\dot{\cup}x_sH \qquad \text{e} \qquad \psi(G) = \psi(x_1H) + \psi(x_2H) + \ldots + \psi(x_sH).$$

Seja h um elemento arbitrário de H. Com isso, observe que $(x_ih)^{t_i} \in (x_iH)^{t_i} = H$. Logo, $(x_ih)^{t_i} \in H$ e a ordem de $(x_ih)^{t_i}$ em H divide $|H|$. Logo, $(x_ih)^{t_i|H|} = 1$. Assim, $|x_ih|$ divide $t_i|H|$, em particular, $|x_ih| \leq t_i|H|$. Agora, considere $H = \{h_1, h_2, \ldots, h_{|H|}\}$. Daí,

$$\begin{aligned} \psi(x_iH) &= |x_ih_1| + |x_ih_2| + \ldots + |x_ih_{|H|}| \\ &\leq t_i|H| + t_i|H| + \ldots + t_i|H| \\ &= t_i|H|^2. \end{aligned}$$

Assim,

$$\begin{aligned} \psi(G) &= \psi(x_1H) + \psi(x_2H) + \ldots + \psi(x_sH) \\ &\leq t_1|H|^2 + t_2|H|^2 + \ldots + t_s|H|^2 \\ &= (t_1 + t_2 + \ldots + t_s)|H|^2 \\ &= \psi(G/H)|H|^2 \end{aligned}$$

Portanto,

$$o(G) \leq \frac{\psi(G/H) \cdot |H|^2}{|G|} = \frac{\psi(G/H)}{[G:H]} \cdot |H| = o(G/H)|H|.$$

□

Ao combinar o Lema 2.2 e o Teorema 2.3, para todo grupo finito G e $1 \neq N \trianglelefteq G$ temos a desigualdade

$$o(G/N) < o(G) \leq o(G/N)|N|.$$

Denote por $i_r(G)$ a quantidade de elementos de ordem r do grupo G. Abreviamos por i_r se G está explícito dentro do contexto.

Teorema 2.4. Seja G um grupo finito não-solúvel. Então

(1) $i_2(G) \leq (4/15)|G| - 1$;

(2) $i_3(G) \leq (7/20)|G| - 1$.

A demonstração de (1) pode ser vista no Lema 2.16, em [4]] e para (2) segue do Teorema principal de [19].

O próximo resultado estabelece uma relação entre a quantidade de elementos de ordem 2 e a ordem média de um grupo finito não-solúvel. Tais resultados serão importantes

para o estudo sobre um critério de solubilidade na Subseção 3.2.

Lema 2.3. (Lema 3.2 de [2]) Seja G um grupo finito não-solúvel. Então

(1) $o(G) > 3,11$;

(2) Se $i_2(G) \leq (1/20)|G|$, então $o(G) \geq 3,55$;

(3) Se $i_2(G) \leq (10/99)|G|$, então $o(G) > 3,4479$;

(4) Se $i_2(G) < (1/15)|G|$, então $o(G) > o(A_5)$;

(5) Se $i_2(G) \leq (1/16)|G|$ e $i_3(G) + 1 \leq (1/14)|G|$, então $o(G) > 3,8$.

Demonstração. Sejam $R = \{x \in G \mid |x| \geq 4\}$ e $r = |R|$. Então

$$|G| = 1 + i_2 + i_3 + r,$$

o que implica que

$$r - i_2 = |G| - 1 - i_2 - i_3 - i_2 = |G| - 2i_2 - (i_3 + 1).$$

Como G é não-solúvel, então existem $y, y^{-1} \in R$ com $|y| \geq 5$. Suponha que y e y^{-1} são os únicos elementos com ordem 5. Observe que

$$\psi(R) = 4(r-2) + 5 \cdot 2 = 4r + 2.$$

Logo,

$$\psi(G) \geq 1 + 2i_2 + 3i_3 + 4r + 2 = 3|G| + (r - i_2).$$

O Teorema 2.4 afirma que $i_2(G) < (4/15)|G|$ e $i_3(G) + 1 \leq (7/20)|G|$.

(1) Com isso,

$$\begin{aligned} r - i_2 &= |G| - 2i_2 - (i_3 + 1) \\ &> |G| - (8/15)|G| - (7/20)|G| \\ &= (7/60)|G| \\ &> 0,11|G|. \end{aligned}$$

e assim

$$\psi(G) \geq 3|G| + (r - i_2) > 3|G| + 0,11|G| = 3,11|G|.$$

Daí, $o(G) > 3,11$.

(2) Se $i_2(G) \leq (1/20)|G|$, então

$$\begin{aligned} r - i_2 &= |G| - 2i_2 - (i_3 + 1) \\ &\geq |G| - (2/20)|G| - (7/20)|G| \\ &= (11/20)|G| \\ &= 0,55|G|, \end{aligned}$$

e assim

$$\psi(G) \geq 3|G| + (r - i_2) \geq 3|G| + 0,55|G| = 3,55|G|.$$

Daí, $o(G) \geq 3,55$.

(3) Se $i_2(G) \leq (10/99)|G|$, então

$$\begin{aligned} r - i_2 &= |G| - 2i_2 - (i_3 + 1) \\ &\geq |G| - (20/99)|G| - (7/20)|G| \\ &= (887/1980)|G| \\ &> 0,4479|G|, \end{aligned}$$

e assim

$$\psi(G) \geq 3|G| + (r - i_2) > 3|G| + 0,4479|G| = 3,4479|G|.$$

Daí, $o(G) > 3,4479$.

(4) Se $i_2(G) < (1/15)|G|$, então

$$\begin{aligned} r - i_2 &= |G| - 2i_2 - (i_3 + 1) \\ &> |G| - (2/15)|G| - (7/20)|G| \\ &= (31/60)|G| \\ &> 0,4479|G|, \end{aligned}$$

e assim

$$\psi(G) \geq 3|G| + (r - i_2) > 3|G| + (31/60)|G| = (211/60)|G| = o(A_5)|G|.$$

Daí, $o(G) > o(A_5)$.

(5) Se $i_2(G) \leq (1/16)|G|$ e $i_3(G) + 1 \leq (1/14)|G|$, então

$$\begin{aligned} r - i_2 &= |G| - 2i_2 - (i_3 + 1) \\ &\geq |G| - (2/16)|G| - (1/14)|G| \\ &= (90/112)|G| \\ &> 0,8|G|, \end{aligned}$$

e assim

$$\psi(G) \geq 3|G| + (r - i_2) > 3|G| + 0,8|G| = 3,8|G|.$$

Portanto, $o(G) > 3,8$.

□

Continuando a explorar a ordem média de grupos não-solúveis, segue abaixo uma propriedade mais específica, mas que também fornece uma estimativa para a ordem média de um grupo não-solúvel.

Lema 2.4. (Lema 6.1 de [2]) Seja G um grupo finito não-solúvel. Suponha que exista um subgrupo normal N de G tal que $|G/N| = 3$. Então

$$o(N) < 3(o(G) - 2,66).$$

Em particular, $o(G) > 3,66$.

Demonstração. Seja $Y = G \setminus N$. Tome $yN \in G/N$. Como $|G/N| = 3$, então $(yN)^3 = y^3N = N$ e $y^3 \in N$. Além disso,

$$|G| = |N| + |Y| = (1/3)|G| + |Y|.$$

Logo, $|Y| = (2/3)|G|$. Para $y \notin N$, temos $|yN| = 3$.

Escreva $Y = G \setminus N$. Tome $yN \in G/N$. Como $|G/N| = 3$, então $y^3N = (yN)^3 = N$ e $y^3 \in N$. Pelo Lema 2.2, $|yN|$ divide $|y|$, ou seja, existe um inteiro positivo h tal que $|y| = |yN|h = 3h$.

Sejam $T = \{y \in Y \mid |y| = 3\}$ e $V = Y \setminus T$. Além disso, $i_3(G) \geq |T|$ e, pelo Teorema 2.4, segue que $i_3(G) < i_3(G) + 1 < (7/20)|G|$. Suponha $|T| > (2/3)|Y|$. Então

$$(7/20)|G| > i_3(G) \geq |T| > (2/3)|Y| = (2/3)(2/3)|G| = (4/9)|G|,$$

uma contradição, pois $7/20 < 4/9$. Logo, $|T| < (2/3)|Y|$. Segue que

$$|V| = |Y| - |T| \geq |Y| - (2/3)|Y| = (1/3)|Y|.$$

Note que $3|V| \geq |Y|$. Dessa forma, como $|Y| = (2/3)|G|$, temos que

$$\begin{aligned} \psi(G) - \psi(N) = \psi(Y) &\geq 3|T| + 6|V| \\ &= 3(|T| + |V|) + 3|V| \\ &= 3|Y| + |Y| \\ &= 4|Y| \\ &= (8/3)|G|. \end{aligned}$$

Assim, $\psi(G) \geq \psi(N) + (8/3)|G|$. Dividindo por $|G|$ em ambos os lados da última desigualdade, temos

$$\begin{aligned} o(G) = \frac{\psi(G)}{|G|} &\geq \frac{\psi(N) + (8/3)|G|}{|G|} \\ &= \frac{\psi(N)}{|G|} + \frac{8}{3} = \frac{\psi(N)}{3|N|} + \frac{8}{3} = \frac{1}{3}o(N) + \frac{8}{3} > \frac{1}{3}o(N) + 2,66. \end{aligned}$$

Portanto,

$$o(N) < 3(o(G) - 2,66).$$

Pelo Lema 2.3, $o(N) > 3,11$, uma vez que N é não-solúvel. Logo,

$$3 < o(N) < 3(o(G) - 2,66) \qquad \text{e} \qquad 1 < o(G) - 2,66.$$

Portanto, $o(G) > 3,66$.

□

Lema 2.5. A quantidade de todos os elementos de ordem p^α, para $1 \leq \alpha \leq \alpha_m$, de um p-grupo abeliano

$$C_{p^{\alpha_1}} \times \ldots \times C_{p^{\alpha_m}}$$

é igual ao número

$$p^\alpha \cdot h_p^{m-1}(\alpha) - p^{\alpha-1} \cdot h_p^{m-1}(\alpha - 1),$$

em que

$$h_p^{m-1}(\alpha) = \begin{cases} p^{(m-1)\alpha}, & se \quad 0 \leq \alpha \leq \alpha_1 \\ p^{(m-2)\alpha+\alpha_1}, & se \quad \alpha_1 \leq \alpha \leq \alpha_2 \\ \vdots & \\ p^{\alpha_1+\alpha_2+\ldots+\alpha_{m-1}}, & se \quad \alpha_{m-1} \leq \alpha. \end{cases}$$

Demonstração. Pode ser vista em [30], Corolário 4.4. □

Um problema interessante é apurar a ordem média de integrantes da classe dos grupos finitos na reta real. Para quais intervalos, neste caso, a densidade ocorre? Seja o conjunto $Im(o) = \{o(G) \mid G \in \mathcal{G}\}$, em que $\mathcal{G}$ é a classe de todos os grupos finitos. Sabe-se que não existe grupo finito tal que $o(G)$ é um número par, isso ocorre pois $\psi(G)$ é sempre ímpar. De fato, se $|G|$ é ímpar, então $\psi(G) = 1 + R$, em que R é a soma de par parcelas ímpares, logo $\psi(G)$ é ímpar. Se $|G|$ é par, então $\psi(G) = 1 + A + B$, em que A é soma das parcelas pares e B é a soma das parcelas ímpares. Temos que B é par, pois elementos não triviais de ordem ímpar ocorrem em pares (o elemento e seu inverso). Assim, $\psi(G)$ é ímpar. Isso implica dizer que não existe grupo finito G tal que $o(G)$ é um número par.

Sabemos também que não existe G tal que $o(G) = 3$. De fato, suponha que exista um grupo G tal que $o(G) = 3$. Como $\psi(G)$ é ímpar e $o(G)$ é um inteiro positivo, segue que $|G|$ é ímpar. Se $\exp G = 3$, então

$$o(G) = \frac{1 + 3 \cdot (|G| - 1)}{|G|} = 3 - \frac{2}{|G|} < 3.$$

Caso contrário, G tem pelo menos 4 elementos de ordem maior ou igual a 5, então. Logo,

$$o(G) \geq \frac{1 + 4 \cdot 5 + 3 \cdot (|G| - 5)}{|G|} = 3 + \frac{6}{|G|} > 3.$$

Contradição nos dois casos.

Teorema 2.5. Seja $n \geq 2$ um inteiro. Então existe uma sequência $(G_m)_{m\geq 1}$ de grupos finitos tais que $\lim_{m\to\infty} o(G_m) = n$.

Demonstração. Seja $n = p_1^{n_1} \ldots p_n^{n_k}$ a fatoração do inteiro positivo n. Seja $G_{i,m} = C_{p_i^{n_i}}^m$, em que $m \geq 1$ é um inteiro. Pelo Lema 2.5, $G_{i,m}$ possui $p_i^{m\alpha} - p_i^{m(\alpha-1)}$ elementos de ordem p_i^α, para todo $\alpha \in \{1, 2, \ldots, n_i\}$. Assim,

$$\begin{aligned} \psi(G_{i,m}) &= 1 + p_i(p_i^m - 1) + p_i^2(p_i^{2m} - p_i^m) + \ldots + p_i^{n_i}(p_i^{mn_i} - p_i^{m(n_i-1)}) \\ &= \frac{p_i^{(m+1)(n_i+1)} - p_i^{(m+1)n_i+1} + p_i - 1}{p_i^{m+1} - 1} \end{aligned}$$

Logo,

$$\begin{aligned} o(G_{i,m}) &= \frac{p_i^{(m+1)(n_i+1)} - p_i^{(m+1)n_i+1} + p_i - 1}{p_i^{mn_i}(p_i^{m+1}-1)} \\ &= p_i^{n_i} \cdot \frac{1 - \frac{1}{p_i^m}}{1 - \frac{1}{p_i^{m+1}}} + \frac{p_i - 1}{p_i^{mn_i}(p_i^{m+1}-1)}. \end{aligned}$$

Considere a sequência $(G_m)_{m\geq 1}$, em que

$$G_m = G_{1,m} \times G_{2,m} \times \ldots \times G_{k,m}.$$

Por 2.1, temos

$$\lim_{m\to\infty} o(G_m) = \lim_{m\to\infty} \prod_{i=1}^{k} o(G_{i,m}) = \prod_{i=1}^{k} \left(\lim_{m\to\infty} o(G_{i,m}) \right) = \prod_{i=1}^{k} p_i^{n_i} = n.$$

□

2.2 p-Grupos

Agora, abordaremos algumas classes de p-grupos e as relacionaremos com a ordem média. O intuito é realizar um panorama geral sobre o tema e, ao final, expor resultados mais específicos que terão consequências no próximo capítulo.

2.2.1 p-Grupos anti-Hughes

Nesta Subseção discutiremos contraexemplos esperados para algumas questões propostas por E. I. Khukhro, A. Moretó e M. Zarrin [2]. A motivação inicial está relacionada à Conjectura de Hughes e aos chamados p-grupos anti-Hughes. Provaremos inicialmente um resultado que relaciona diretamente as funções $k(G)$ e $o(G)$, na qual $k(G)$ denota a quantidade de classes de conjugação de um determinado grupo finito G.

Teorema 2.6. (Lema 2.9 de [1]) Sejam G um grupo finito e S um subconjunto invariante de G. Então

$$k_G(S) = \frac{1}{|G|} \sum_{x\in S} |C_G(x)|.$$

Em particular, $k(G) \geq o(G)$.

Demonstração. Seja $S \subset G$. Considere uma ação ϕ tal que

$$\begin{aligned} \phi : G \times S &\to S \\ (g, x) &\mapsto x^g = g^{-1}xg, \end{aligned}$$

Logo,

$$G_x = \{g \in G \mid g^{-1}xg = x\} = \{g \in G \mid xg = gx\} = C_G(x).$$

Pelo Lema de Burnside 1.2, temos

$$k_G(S) = \frac{1}{|G|}\sum_{x\in S}|G_x| = \frac{1}{|G|}\sum_{x\in S}|C_G(x)|.$$

Se $G = S$, então

$$k(G) = \frac{1}{|G|}\sum_{x\in G}|C_G(x)|.$$

Como $|C_G(x)| \geq |x|$ para todo $x \in G$, temos

$$k(G) = \frac{1}{|G|}\sum_{x\in G}|C_G(x)| \geq \frac{1}{|G|}\sum_{x\in G}|x| = o(G).$$

□

A partir de agora, enunciaremos algumas questões propostas por E. I. Khukhro, A. Moretó e M. Zarrin [2] motivadas pelo estudo das funções $k(G)$ e $o(G)$.

Questão 2.1. Seja G um p-grupo finito. É verdade que $k(G) \geq \exp(G)^{1/2}$?

Se a Questão 2.1 tiver uma resposta afirmativa, ela mostrará que p-grupos com poucas classes de conjugação necessariamente têm expoente "pequeno". Os contraexemplos no Capítulo 3 não fornecem contraexemplo para a Questão 2.1. Tais contraexemplos mostram que, se essa cota existe, então ela não é consequência imediata de um resultado geral relacionando $o(G)$ e $o(N)$, onde N é o subgrupo abeliano normal de G. No próximo capítulo veremos mais detalhadamente a relação entre $o(G)$ e $o(N)$.

Dado este contexto, outra questão foi proposta similarmente à Questão 2.1, em [2].

Questão 2.2. Seja G um p-grupo finito. É verdade que $o(G) \geq \exp(G)^{1/2}$?

Observe que dado $H \leq G$, temos

$$o(H) = \frac{1}{|H|}\sum_{x\in H}|x| \leq \frac{\exp(G)\cdot|H|}{|H|} = \exp(G).$$

Logo, $o(H) \leq \exp(G)$ para qualquer subgrupo H de G.

Vejamos uma construção para possíveis contraexemplos à Questão 2.2. Para ca-

racterizá-los, elucidaremos o significado da Conjectura de Hughes, proposta por D. R. Hughes em 1957 [6].

Conjectura 2.1. (Conjectura de Hughes) Seja G um grupo finito e p um primo. Defina $H_p(G)$ o subgrupo de G gerado pelos elementos com ordem diferente de p. Então para $1 \neq H_p(G) \neq G$ temos que $[G : H_p(G)] = p$.

Antes de voltarmos para a Questão 2.2, vejamos um panorama histórico sobre a Conjectura de Hughes 2.1.

Os matemáticos D. R. Hughes e J. G. Thompson [7] provaram que a conjectura é válida para todos os grupos que não são p-grupos. No âmbito dos p-grupos, foi provado que a Conjectura de Hughes 2.1 também vale para $p = 2$ (finito ou infinito) e $p = 3$ (finito ou infinito), em 1955 (antes de 1957, mesmo que parcialmente) por D. R. Hughes [8] e em 1957 por Straus e Szekeres [9], respectivamente. São conhecidos contraexemplos para $p \in \{5, 7, 11, 13, 19\}$ e possivelmente para mais primos [2].

Definição 2.2. Um contraexemplo para a Conjectura de Hughes 2.1 é chamado de **grupo anti-Hughes**.

Os grupos anti-Hughes conhecidos possuem propriedades interessantes, por exemplo $[G : H_p(G)] = p^2$ e $\exp(G) = p^2$. Espera-se que existam contraexemplos para todo primo maior ou igual a 5 e que existam grupos anti-Hughes G tais que $[G : H_p(G)] > p^2$ e $\exp(G) > p^2$.

Pela definição de $H_p(G)$, todos os elementos de $G \setminus H_p(G)$ tem ordem p. Note que

$$\begin{aligned} |G \setminus H_p(G)| &= |G| - |H_p(G)| \\ &= p^2|H_p(G)| - |H_p(G)| \\ &= |H_p(G)|(p^2 - 1) \\ &= \frac{|G|}{p^2} \cdot (p^2 - 1). \end{aligned}$$

Assim, se G é um grupo anti-Hughes, então a proporção de elementos com ordem p é pelo menos $(p^2 - 1)/p^2$. É natural verificar se poderíamos ter um contraexemplo para as Questões 2.1 e 2.2 entre os grupos anti-Hughes. No entanto, temos o seguinte.

Observação 2.1. A Questão 2.2 possui resposta afirmativa para os p-grupos anti-Hughes. De fato, considere G um grupo anti-Hughes tal que $|G| = p^n$. Neste caso, $[G : H_p(G)] = p^2$

e $|H_p(G)| = p^{n-2}$. Então

$$\begin{aligned} o(G) = \frac{\sum_{x\in G}|x|}{|G|} &= \frac{\sum_{x\in H_p(G)}|x|}{p^n} + \frac{\sum_{x\in G\setminus H_p(G)}|x|}{p^n} \\ &\geq \frac{p\cdot p^{n-2}}{p^n} + \left(\frac{p\cdot p^n\cdot(p^2-1)}{p^2}\right)\cdot\frac{1}{p^n} \\ &= \frac{1}{p} + \frac{p^2-1}{p} \\ &= \frac{1}{p} + p - \frac{1}{p} = p = (p^2)^{1/2} = \exp(G)^{1/2}. \end{aligned}$$

Portanto, não há contraexemplos para estas questões entre os grupos anti-Hughes conhecidos. Entretanto, podemos considerar o seguinte.

Proposição 2.2. Seja G um grupo anti-Hughes com $\exp G = p^3$ e $|G : H_p(G)| = p^2$. Então G é um contraexemplo para a Questão 2.2.

Demonstração. Considere $|G| = p^n$. Como $|G : H_p(G)| = p^2$, temos $|H_p(G)| = p^{n-2}$. A quantidade de elementos com ordem p é

$$|G \setminus H_p(G)| = |G| - |H_p(G)| = p^n - p^{n-2}.$$

Observe que se $p \geq 5$, temos que $4p^2 < p^3 = p\cdot p^2$. Além disso, $\exp(G) = p^3$, logo

$$\begin{aligned} o(G) = \frac{\psi(G)}{|G|} &\leq \frac{p(p^n - p^{n-2}) + p^3p^{n-2}}{p^n} \\ &= \frac{2p^{n+1}}{p^n} - \frac{p^{n-1}}{p^n} \\ &= 2p - \frac{1}{p} \\ &< 2p = (4p^2)^{1/2} = (p^3)^{1/2} = \exp(G)^{1/2}, \end{aligned}$$

o que finaliza a demonstração.

□

2.2.2 p-Grupos *powerful*

Agora apresentaremos uma estimativa para a ordem média de uma importante classe de grupos, os chamados p-grupos *powerful*. Estimar a ordem média de uma classe de grupos é algo interessante por si só, ainda mais quando não se tem a ordem média explícita de um p-grupo *powerful* qualquer.

Para tanto, demonstraremos os Lemas 2.6 e 2.7, os quais oferecem uma base de entendimento para o principal resultado desta subseção, o Teorema 2.13. Antes disso, aproveitamos para discorrer sobre alguns resultados essenciais sobre p-grupos *powerful* que fundamentam a teoria. A principal referência é o livro *Analytic Pro-p Groups*, de J. D. Dixon [12]. Vale ressaltar que, ao longo desta subseção, utilizaremos fortemente o Teorema da Base de Burnside 1.12.

Começamos com a seguinte definição.

Definição 2.3. Seja G um p-grupo finito. Definimos

$$\Omega_i(G) = \langle g \in G \mid g^{p^i} = 1 \rangle,$$

$$G^{p^i} = \langle g^{p^i} \mid g \in G \rangle,$$

$$\Omega_{\{i\}}(G) = \{g \in G \mid g^{p^i} = 1\} \quad e$$

$$G^{p^{\{i\}}} = \{g^{p^i} \mid g \in G\}$$

para todo $i \geq 0$.

Note que se $\exp(G) = p^k$, então $\Omega_k(G) = G$ e $G^{p^k} = 1$. Além disso,

$$G^{p^{i+1}} \leq (G^{p^i})^p \leq \Phi(G^{p^i}) < G^{p^i}.$$

A próxima definição estabelece uma relação entre os subgrupos de G, de tal maneira que podemos construir uma série de subgrupos.

Definição 2.4. Seja G um p-grupo finito. Então $P_1(G) = G$ e $P_{i+1}(G) = P_i(G)^p[P_i(G), G]$, para $i \geq 1$. Para simplificar, $G_i = P_i(G)$. Esta série é denominada p-série.

Observe que

$$G_2 = P_2(G) = P_1(G)^p[P_1(G), G] = G^p[G, G] = \Phi(G).$$

Definamos, portanto, o conceito de p-grupo *powerful* e *powerfully embedded*.

Definição 2.5. Um p-grupo finito G é *powerful* se p é ímpar e G/G^p é abeliano, ou $p = 2$ e G/G^4 é abeliano.

Exemplos imediatos de grupos *powerful* são grupos abelianos, pois o subgrupo derivado de um grupo abeliano é trivial. Já exemplos de p-grupos *powerful* que não são abelianos são os p-grupos metacíclicos, com $p \geq 3$.

Definição 2.6. Um p-grupo metacíclico é um grupo G que possui um subgrupo normal cíclico N, de tal modo que o grupo quociente G/N também é cíclico.

Teorema 2.7. Seja p um primo ímpar. Todo p-grupo metacíclico é *powerful*.

Demonstração. Se G é cíclico, então é *powerful*. Suponha G não cíclico, um p-grupo metacíclico tal que p é ímpar. Tome $N \lhd G$ tal que N e G/N são cíclicos, isto é, existem $y \in N$ e $x \in G$ tais que $N = \langle y \rangle$ e $G/N = \langle xN \rangle$. Considere $|N| = p^m$, para algum inteiro positivo m. Seja $g \in G$ um elemento arbitrário. Se $g \in N$, então $g = y^i$, para algum i. Se $g \notin N$, então $gN \neq N$ e suponha sem perda de generalidade que $g = x^j$. Logo, $G = \langle x, y \rangle$. Como y é um dos geradores de G, segue que $y \notin \Phi(G)$. Além disso, G/N ser cíclico implica que, pelo Teorema 1.6, $G' \leq N$ e $G' = \langle y^r \rangle$, para algum r. Como G é um p-grupo, pela Proposição 1.12, G é nilpotente e, pelo Teorema 1.10, temos que $G' \leq \Phi(G)$ e, com isso, $y^r \in \Phi(G)$.

Assim, p divide r. De fato, pois se supormos que p não divide r, então $mdc(p^m, r) = 1$. Logo,

$$N = \langle y \rangle = \langle y^r \rangle \leq \Phi(G) \implies y \in \Phi(G),$$

absurdo. Com isso, existe q tal que $r = pq$, sendo assim

$$y^r = y^{pq} = (y^q)^p \in G^p \implies G' \leq G^p.$$

Portanto, G é *powerful*. □

Um exemplo de 2-grupo metacíclico é o grupo diedral

$$D_8 = \langle x, y \mid x^4 = y^2 = 1, x^y = x^{-1} \rangle,$$

pois $D_8/\langle x \rangle$ é cíclico. Como $\exp D_8 = 4$ e D_8 não é abeliano, segue que, respectivamente, $(D_8)^4 = 1$ e $D_8' \neq 1$. Portanto, D_8 não é *powerful*.

Exemplo 2.4. Podemos tomar um exemplo de 3-grupo *powerful*:

$$G = \langle a, b \mid a^9 = b^3 = 1, a^b = a^4 \rangle.$$

De fato, $G/\langle a \rangle$ é cíclico e portanto G é *powerful*.

Definição 2.7. Um subgrupo N de um p-grupo finito G é *powerfully embedded* em G, se p é ímpar e $[N, G] \leq N^p$, ou se $p = 2$ e $[N, G] \leq N^4$. Notação: N p.e. G.

Observe que se N p.e. G, então

$$[N, N] \leq [N, G] \leq N^p,$$

isto é, N é *powerful*.

Note que um p-grupo *powerful* G é *powerfully embedded* nele mesmo, basta notar que se $N = G$, então $[G, G] \leq G^p$, para $p > 2$, ou $[G, G] \leq G^4$, para $p = 2$.

Teorema 2.8. Seja G um p-grupo finito e seja N um subgrupo normal de G. Se N p.e G e $x \in G$, então $\langle N, x\rangle$ é *powerful*.

Demonstração. Seja $x \in G$. Suponha que N p.e. G. Denote $H = \langle N, x\rangle$. Provaremos que $[H, H] = [N, H]$. Evidente que $[N, H] \leq [H, H]$, pois $N \leq H$. Por outro lado, tome arbitrariamente $n_1x^i, n_2x^j \in H$ com $n_1, n_2 \in N$. Assim, pela Proposição 1.3, temos

$$\begin{aligned}
[n_1x^i, n_2x^j] &= [n_1, n_2x^j]^{x^i}[x^i, n_2x^j] \\
&= ([n_1, x^j][n_1, n_2]^{x^j})^{x^i}[x^i, x^j][x^i, n_2]^{x^j} \\
&= [n_1, x^j]^{x^i}([n_1, n_2]^{x^j})^{x^i}[x^i, n_2]^{x^j} \\
&= [n_1^{x^i}, x^j][n_1^{x^{i+j}}, n_2^{x^{i+j}}][x^i, n_2^{x^j}].
\end{aligned}$$

O subgrupo N é normal em G, logo $[n_1x^i, n_2x^j] \in [N, H]$ e $[H, H] \leq [N, H]$. Com isso, $[H, H] = [N, H]$. Para p ímpar, temos que

$$[H, H] = [N, H] \leq [N, G] \leq N^p \leq H^p.$$

E para $p = 2$ temos

$$[H, H] = [N, H] \leq [N, G] \leq N^4 \leq H^4.$$

Portanto, H é *powerful* para todo primo p. □

Teorema 2.9. Sejam G um p-grupo finito e $N \leq G$. Se N p.e. G, então N^p p.e. G.

Para uma demonstração veja em [12].

Teorema 2.10. Seja G um p-grupo *powerful*.

(1) Para cada i, G_i p.e. G e $G_{i+1} = G_i^p = \Phi(G_i)$;

(2) Para cada i, a aplicação $x \mapsto x^p$ induz um homomorfismo de G/G_{i+1} sobre G_{i+1}/G_{i+2}.

Demonstração. (1) Para $i = 1$, temos $G_1 = G$ p.e. G e $G_2 = P_2(G) = \Phi(G) = \Phi(G_1)$. Como G é *powerful*, segue que $\Phi(G) = G^p = G_1^p$, assim, $G_2 = G_1^p = \Phi(G_1)$.

Suponha que, por hipótese de indução, valha G_i p.e. G e $G_{i+1} = G_i^p = \Phi(G_i)$.

Vejamos para $i + 1$. Como $G_{i+1} = G_i^p$, então pela Teorema 2.9 temos G_{i+1} p.e. G.

Agora observe que

$$G_{i+2} = G_{i+1}^p[G_{i+1}, G].$$

Como G_{i+1} p.e. G, temos $[G_{i+1}, G] \leq G_{i+1}^p$. Logo, $G_{i+2} = G_{i+1}^p$.

Por fim, pelo Teorema da Base de Burnside 1.12, $G_{i+1}^p \leq \Phi(G_{i+1})$ e

$$\Phi(G_{i+1}) = G_{i+1}^p[G_{i+1}, G_{i+1}].$$

Logo,

$$\Phi(G_{i+1}) = G_{i+1}^p[G_{i+1}, G_{i+1}] \leq G_{i+1}^p[G_{i+1}, G] \leq G_{i+1}^p.$$

Logo, $\Phi(G_{i+1}) = G_{i+1}^p$.

(2) Pelo resultado anterior, G_i p.e. G, logo G_i é *powerful*, pois

$$[G_i, G_i] \leq [G_i, G] \leq G_i^p.$$

Além disso, pela Definição 2.4

$$P_2(G_i) = P_1(G_i)^p[P_1(G_i), G] = G_i^p[G_i, G] = G_{i+1}.$$

Analogamente, $P_3(G_i) = G_{i+2}$.

Primeiramente, assuma $i = 1$ e, substituindo G por G/G_3, $G_3 = 1$. Note que, pelo item anterior,

$$G_3 = P_3(G) = G_2^p[G_2, G] = G_3[G_2, G].$$

Com isso, $[G_2, G] \leq G_3 = 1$ e $G_2 \leq Z(G)$. Tome arbitrariamente $x, y \in G$. Como $G' \leq \Phi(G) = G_2 \leq Z(G)$, então G é nilpotente de classe 2. Então, pela Proposição 1.9, temos

$$(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}, \quad n \in \mathbb{N}.$$

Considere $n = p \geq 3$ um primo, daí p divide $p(p-1)/2$. Além disso, $[y, x]^p \in G_2^p = G_3 = 1$. Logo, $(xy)^p = x^p y^p$. Para $p = 2$, utilizando o fato de G ser *powerful* e o item anterior, segue que

$$[G, G] \leq G^4 \leq (G^2)^2 \leq (\Phi(G))^2 = G_2^2 = G_3 = 1.$$

Daí $[y, x] \in [G, G] \leq G_3 = 1$

$$(xy)^2 = x^2 y^2 [y, x] = x^2 y^2.$$

Por fim, $G_2^p = G_3 = 1$, $G^p = G_2$ e $x \mapsto x^p$ induz um homomorfismo sobrejetivo de G/G_2 sobre G_2/G_3. Analogamente prova-se para os casos em que $i > 1$, uma vez que G_i é

powerful. □

O próximo resultado estabelece uma semelhança entre os p-grupos *powerful* e os grupos abelianos no geral, mostrando que os geradores do subgrupo G^p são inteiramente determinados pelos geradores de G, basta aplicar a potência p em cada gerador.

Teorema 2.11. Seja G um p-grupo *powerful*. Se $G = \langle a_1, \ldots, a_d \rangle$, então $G^p = \langle a_1^p, \ldots, a_d^p \rangle$.

Demonstração. Pelo Teorema 2.10, aplicação φ tal que

$$\begin{aligned} \varphi : G/G_2 &\to G_2/G_3 \\ x &\mapsto x^p. \end{aligned}$$

é um homomorfismo. O quociente G/G_2 é gerado pelo conjunto $\{a_1G_2, \ldots, a_dG_2\}$, pois por hipótese G é gerado por $\{a_1, \ldots, a_d\}$. Assim, aplicando os geradores de G/G_2 no homomorfismo φ, temos que o quociente G_2/G_3 é gerado por $\{\varphi(a_1G_2), \ldots, \varphi(a_dG_2)\}$. Logo,

$$\begin{aligned} G_2/G_3 &= \langle \varphi(a_1G_2), \ldots, \varphi(a_dG_2) \rangle \\ &= \langle (a_1G_2)^p, \ldots, (a_dG_2)^p \rangle \\ &= \langle a_1^pG_2^p, \ldots, a_d^pG_2^p \rangle \\ &= \langle a_1^pG_3, \ldots, a_d^pG_3 \rangle. \end{aligned}$$

Com isso, $G_2 = \langle a_1^p, \ldots, a_d^p \rangle G_3$. Pelo Teorema 2.10, $G_3 = \Phi(G_2)$ e $G_2 = G^p$, assim $G^p = \langle a_1^p, \ldots, a_d^p \rangle \Phi(G_2)$. Como o $\Phi(G_2)$ é constituído dos elementos não geradores do grupo G_2, daí concluímos que $G^p = \langle a_1^p, \ldots, a_d^p \rangle$. □

Teorema 2.12. Se G é um p-grupo *powerful*, então $G^p = \langle g^p \mid g \in G \rangle = \{g^p \mid g \in G\}$.

Demonstração. O resultado segue quando $|G| = 1$. Suponha que o resultado valha para p-grupos *powerful* cuja ordem é estritamente menor que $|G|$.

Tome arbitrariamente $g \in G^p$. Como $G_2 = G^p$, podemos construir um homomorfismo φ tal que

$$\begin{aligned} \varphi : G/G^p &\to G^p/G_3 \\ x &\mapsto x^p. \end{aligned}$$

Como G_2 p.e G, pelo Teorema 2.8 o subgrupo

$$H = \langle G^p, x \rangle = \langle G_2, x \rangle$$

é *powerful*. Logo, pelos Teoremas 2.11 e 2.10, temos $H^p = \langle G_2^p, x^p \rangle = \langle G_3, x^p \rangle$. Neste

contexto, podemos escrever $g = x^p y$, para $x \in G$ e $y \in G_3$. Assim, $g \in H^p = \langle G_3, x^p \rangle$. No caso em que $H = G$, temos que

$$G = H = \langle G^p, x \rangle = \langle \Phi(G), x \rangle = \langle x \rangle,$$

ou seja, G é cíclico, o que satisfaz o teorema. Porém, se $H \neq G$, temos que $|H| < |G|$ e $H^p = \{h^p \mid h \in H\}$. Logo, $g \in h^p$, para $h \in H$. Em particular, todo $g \in G$ é potência de um elemento de G. □

O Teorema 2.12 é interessante, pois nos diz que o subconjunto $\{g^p \mid g \in G\}$ coincide com o subgrupo $\langle g^p \mid g \in G \rangle$, ou seja, dados $g^p, h^p \in G^p$ quaisquer, existe $k \in G$ tal que $g^p h^p = k^p$. Já o próximo lema generaliza este resultado para outras potências de p.

Lema 2.6. Seja $G = \langle a_1, \ldots, a_d \rangle$ um p-grupo *powerful*. Então

$$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle.$$

Demonstração. Façamos por indução sobre i. Se considerarmos $i = 1$, o resultado segue. Agora suponha que o resultado seja válido para inteiros positivos estritamente menores que i. Pelo Teorema 2.10, segue que $G_{i+1} = G_i^p = \Phi(G_i)$, para todo $i \geq 1$. Isso implica que G_i é *powerful*, uma vez que $[G_i, G_i] \leq G_i^p = \Phi(G_i)$. Utilizando o Teorema 2.12,

$$G_{i+1} = G_i^p = \{x^p \mid x \ \in G\}.$$

Temos também

$$G_i = G_{i-1}^p = \{y^p \mid y \ \in G_{i-1}\}.$$

Por hipótese de indução,

$$G_{i-1} = G^{p^{i-2}} = \{z^{p^{i-2}} \mid z \in G\} = \langle a_1^{p^{i-2}}, \ldots, a_d^{p^{i-2}} \rangle.$$

Assim,

$$G_i = G_{i-1}^p = (G^{p^{i-2}})^p = G^{p^{i-1}}$$

e

$$G_{i-1}^p = \{y^p \mid y \in G_{i-1}\} = \{(z^{p^{i-2}})^p \mid z \in G\} = \{z^{p^{i-1}} \mid z \in G\} = G^{p^{i-1}}.$$

Como G_{i-1} é *powerful* e $G_{i-1} = G^{p^{i-2}}$, pelo Teorema 2.11, temos que

$$(G^{p^{i-2}})^p = \langle (a_1^{p^{i-2}})^p, \ldots, (a_d^{p^{i-2}})^p \rangle = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle = G^{p^{i-1}}.$$

Concluímos

$$G_i = G^{p^{i-1}} = \{x^{p^{i-1}} \mid x \in G\} = \langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \rangle.$$

□

Lema 2.7. Sejam G um p-grupo *powerful* e $c = 1 - p^{-1}$. Então $k(G) \geq c \cdot \exp(G)$.

Demonstração. Sejam $\exp(G) = p^k$ e $S \subset G$ o conjunto dos elementos de ordem p^k. Observe que $\Omega_{k-1}(G) = G \setminus S$ é o conjunto dos elementos de ordem que divide p^{k-1}. Afirmação: $\Omega_{k-1}(G)$ não gera G. De fato. Suponha que $\Omega_{k-1}(G)$ gere G. Então $G = \langle a_1, \ldots, a_d \rangle$ de tal modo que $a_j \in \Omega_{k-1}(G)$, $1 \leq j \leq d$. Pelo Lema 2.6, segue que $G^{p^{k-1}} = \langle a_1^{p^{k-1}}, \ldots, a_d^{p^{k-1}} \rangle$. Porém, cada $a_j^{p^{k-1}} = 1$, pois $a_j \in \Omega_{k-1}(G)$. Logo, $G^{p^{k-1}} = 1$. Absurdo, pois $G^{p^k} < G^{p^{k-1}}$.

Assim, existe um subgrupo maximal M de G tal que $\Omega_{k-1}(G) \leq M$. Além disso, como $[G : M] = p$, pois M é maximal, temos

$$|S| \geq |G| - |M| = |G| - (1/p)|G| = (1 - p^{-1})|G| = c \cdot |G|.$$

Note que $|C_G(x)| \geq |\langle x \rangle| = p^k$ para todo $x \in S$. Pelo Teorema da Órbita-Estabilizador 1.1,

$$|cl(x)| = \frac{|G|}{|C_G(x)|} \leq \frac{|G|}{p^k},$$

para todo $x \in S$. O subconjunto S é normal em G, logo S é a união das t classes de conjugação. Daí,

$$|S| = \sum_{i=1}^{t} |G : C_G(x_i)| \leq \frac{|G| \cdot t}{p^k}.$$

Logo,

$$t \geq \frac{p^k \cdot |S|}{|G|} = \frac{|S|}{|G|/p^k} \geq \frac{c \cdot |G|}{|G|/p^k} = c \cdot p^k.$$

Uma vez que $k(G) \geq t$, então $k(G) \geq c \cdot p^k = c \cdot \exp(G)$.

□

Por fim, o resultado principal desta Subseção.

Teorema 2.13. (Lema 2.6 de [1]) Seja P um p-grupo *powerful* de expoente p^k. Então

$$p^k \geq o(P) \geq (p-1)p^{k-1}.$$

Demonstração. Considere S o conjunto de todos elementos de ordem p^k. Como vimos na demonstração do Lema 2.7, $|S| \geq c \cdot |P|$. Logo,

$$|\Omega_{k-1}(P)| = |P| - |S| \leq |P| - c \cdot |P| = p^{-1} \cdot |P|.$$

Se $x \in P \setminus \Omega_{k-1}(P)$, então $|x| = p^k$. Assim,

$$\begin{aligned} o(P) = \frac{1}{|P|}\sum_{x\in P}|x| &\geq \frac{1}{|P|}\sum_{x\in P\setminus\Omega_{k-1}(G)}|x| \\ &= \frac{1}{|P|}\cdot p^k\cdot(|P| - |\Omega_{k-1}(P)|) \\ &= p^k - \frac{p^k\cdot|\Omega_{k-1}(P)|}{|P|} \\ &\geq p^k - \frac{p^k\cdot p^{-1}\cdot|P|}{|P|} = (p-1)p^{k-1}. \end{aligned}$$

Por fim,

$$o(P) = \frac{1}{|P|}\sum_{x\in P}|x| \leq \frac{1}{|P|}\cdot p^k\cdot|P| = p^k.$$

□

Esta estimativa será importante para a construção de contraexemplos para a Conjectura de Andrei Jaikin-Zapirain no Capítulo 3.

2.2.3 p-Grupos secretos de *Wall*

A classe de grupos mais importante utilizada no próximo capítulo são os chamados p-grupos secretos de *Wall*. Com a construção destes p-grupos secretos, G. E. *Wall* respondeu uma questão de L. G. Kovacs, Joachim Neubuser e B.H. Neumann proposta em [14]. Vejamos a seguir alguns conceitos para compreender este contexto, especificamente os chamados p-grupos secretos..

Seja G um grupo. Definimos o posto de G como o número $\min\{|X| \mid G = \langle X\rangle\}$, denotado por $d(G)$. Se G tem base finita, dizemos que G tem posto finito. Definimos $k_n(G)$ o conjunto dos elementos $g \in G$ que aparece em pelo menos um conjunto de geradores com n elementos de G. Seja $d(G) = d$ o posto do grupo G. Chamemos o primo p de ***hidden prime* (primo oculto)** de G se p divide $|G|$, mas não divide a ordem de nenhum elemento de $k_d(G)$.

Exemplo 2.5. Seja $G = A \rtimes Q_8$ tal que A é um grupo abeliano elementar de ordem 9 gerado por u e v e $Q_8 = \{-1, 1, -i, i, -j, j, -k, k\}$ o grupo dos quatérnios gerado por i e j. A ação de Q_8 sobre A é dada por:

$$u^i = v\ ,\quad u^j = uv\ ,\quad v^i = u^2\quad e\quad v^j = uv^2.$$

O grupo tem ordem $|G| = 72$ e tem no mínimo dois geradores. Com auxílio do [GAP], conforme o Apêndice 3.2.3, podemos verificar que todo elemento de $k_2(G)$ possui ordem

4. Portanto 3 é um primo oculto de G.

Dizemos que B é **secreto** se existe um subgrupo p-abeliano elementar A tal que $G = AB$, $A \cap B = 1$ e p é oculto em G. Quais condições para que o grupo B permite "ocultar" o primo p em um produto semidireto G de A por B? Para tanto, o teorema abaixo estabelece condições necessárias e suficientes, cuja demonstração pode ser vista em [14].

Teorema 2.14. (Teorema 5.1, [14]) Seja G um grupo finito tal que $G = A \rtimes B$ com A p-abeliano elementar e B um grupo. Então as três condições abaixo são necessárias e suficientes para "ocultar" p em G:

(1) $d(B) = d(G)$;

(2) p não divide a ordem de b, para todo $b \in k_d(B)$;

(3) Nenhum elemento de $k_d(B)$ comuta com os elementos não triviais de A.

Definição 2.8. Chamamos o grupo B de **secreto** se existe A tal que valem os itens do Teorema 2.14.

No caso do Exemplo, o grupo Q_8 é secreto. Comparando com os grupos *powerful* vistos anteriormente, observe que $(Q_8)^4 = 1$, pois $\exp(Q_8) = 4$. Como Q_8 é não-abeliano, então $Q_8' \neq 1$, portanto Q_8 não é *powerful*.

G. E. *Wall* desenvolveu os dois próximos resultados. Eles são a base de entendimento para o Lema 2.4 abaixo. As demonstrações destes resultados podem ser vistas em [13].

Teorema 2.15. Seja p um primo e seja d, m inteiros tais que $d \leq p^m$. Então existe um p-grupo finito B de posto d e expoente p^{m+1} que satisfaz as hipóteses do Teorema 2.14.

Corolário 2.1. Para cada primo p e um inteiro $d \geq 2$, existe um p-grupo secreto de posto d.

Para contexto deste trabalho, é suficiente usarmos os p-grupos secretos de *Wall*, que existem para todo primo p. Esta caracterização pode ser vista a seguir.

Lema 2.8. (p-Grupos secretos de *Wall*) Para todo primo, existe um p-grupo finito P tal que

(1) $\Phi(P)$ tem expoente p;

(2) $[P : \Phi(P)] = p^p$;

(3) todos os elementos em $P \setminus \Phi(P)$ possuem ordem p^2 e suas p-ésimas potências são elementos não triviais de um subgrupo central cíclico $\langle z \rangle = P^p$, no qual $|\langle z \rangle| = p$.

Esses grupos são mais específicos de uma construção mais geral de G. E. *Wall* em [13]. Porém, os p-grupos secretos de *Wall* são suficientes para atender nosso objetivo no próximo capítulo. Os p-grupos secretos de *Wall* são uma forte restrição aos grupos secretos. Uma observação imediata nos diz que se G é um p-grupo abeliano elementar, então G não pode ser um grupo secreto de *Wall*, pois

$$\Phi(G) = G'G^p = 1 \neq p.$$

O Exemplo 2.4 nos mostra que

$$G = \langle a, b \mid a^9 = b^3 = 1, a^b = a^4 \rangle.$$

é *powerful*. Porém, trata-se de outro exemplo que não é p-grupo secreto de *Wall*. Basta notar que, como vimos, $\Phi(G) \cong C_3$, logo $|G : \Phi(G)| = 3^2 \neq 3^3$.

Vejamos agora um breve estudo sobre representações de grupos e grupos abelianos livres, com base nas referências [27] e [24], respectivamente. Tais conceitos serão utilizados no Lema 2.10, o principal resultado para construção dos contraexemplos da Conjectura de Andrei Jaikin-Zapirain 3.1.

Definição 2.9. Sejam G um grupo e V é espaço vetorial sobre um corpo $\mathbb{F}$. Então V é chamado de $\mathbb{F}G$-módulo se para todo $v \in V$ e $g \in G$ o produto vg é bem definido e, além disso, se satisfaz as seguintes condições para $u, v \in V$, $\alpha \in \mathbb{F}$ e $g, h \in G$:

(1) $vg \in V$;

(2) $v(gh) = (vg)h$;

(3) $v1 = v$;

(4) $(\alpha v)g = \alpha(vg)$;

(5) $(u + v)g = ug + vg$.

Definição 2.10. Seja V um $\mathbb{F}G$-módulo. O subespaço vetorial W de V sobre $\mathbb{F}$ é chamado de $\mathbb{F}G$-submódulo de V se, para todo $w \in W$, $g \in G$, temos $wg \in W$.

Denote o grupo dos operadores lineares invertíveis do espaço vetorial V sobre $\mathbb{F}$ por $GL(V)$ e o grupo das matrizes invertíveis $n \times n$ com coeficientes em $\mathbb{F}$ por $GL(n, \mathbb{F})$, em que $\dim(V) = n$. Neste caso, $GL(V) \cong GL(n, \mathbb{F})$.

Uma representação de um grupo G é um homomorfismo

$$\lambda : G \to GL(V),$$

em que V é um $\mathbb{F}$-espaço vetorial de dimensão finita.

Seja λ uma representação do grupo G em V sobre $\mathbb{F}$. O núcleo de λ, denotado por K, isto é,

$$K = \{g \in G \mid \lambda(g) = 1_{GL(V)}\}$$

é denominado núcleo da representação de G, em que $1_{GL(V)}$ denota a aplicação identidade. Se λ é um homomorfismo injetivo, temos que K é trivial e dizemos que λ é uma representação fiel.

Definição 2.11. Seja ρ uma representação do grupo G em V sobre F. Dizemos que λ é uma representação irredutível se 0 e V são os únicos subespaços λ-invariantes de V. Em particular, neste caso, se V é um $\mathbb{F}G$-módulo dizemos que V é um $\mathbb{F}G$-módulo irredutível.

Para nosso contexto, considere um $\mathbb{C}G$-módulo V. Seja $v \in V$ e $g \in G$. Considere uma ação de G em V, definida por $(v, g) \mapsto vg$. Para cada $g \in G$, podemos definir a aplicação

$$\begin{aligned} \rho_g : V &\to V \\ v &\mapsto vg \end{aligned}$$

Com isso, a aplicação

$$\begin{aligned} \rho : G &\to GL(V) \\ g &\mapsto \rho_g \end{aligned}$$

é dita uma representação de G sobre $\mathbb{C}$, ou simplesmente uma representação complexa associada ao $\mathbb{C}G$-módulo V.

Lema 2.9. Sejam G um grupo finito e $1 \neq g \in G$. Então existe uma representação complexa irredutível ρ de G, tal que $g \notin \ker(\rho)$, o que equivale a dizer que a interseção dos núcleos das representações complexas irredutíveis é igual a 1.

Demonstração. A demonstração pode vista em [27], em que Lema 2.19 diz que o núcleo de uma representação é igual ao núcleo do seu caractere e o Lema 2.21 mostra que a interseção dos núcleos dos caracteres das representações irredutíveis é igual a 1. A definição de caractere pode ser vista na Definição 2.20. □

Agora, considere G um grupo abeliano aditivo. Denote o elemento identidade por 0 e o elemento inverso de $g \in G$ por $-g$. Se G é um grupo abeliano, $g \in G$ e $n \in \mathbb{Z}$, a notação ng significa

$$\underbrace{g + \ldots + g}_{n \text{ parcelas}}$$

e nG significa o subgrupo $\{ng \mid g \in G\}$. Uma combinação linear dos elementos de G é a

soma da forma

$$\sum_{i=1}^{k} n_i g_i,$$

em que $g_1, \ldots, g_k \in G$ e $n_1, \ldots, n_k \in \mathbb{Z}$. Denote $\mathbb{Z}G$ o grupo de todas as combinações lineares dos elementos de G. Neste caso, $\mathbb{Z}G$ é dito grupo abeliano livre. Observe que se $|G| = n$, então $\mathbb{Z}G \simeq \mathbb{Z}^n$ via aplicação

$$k_1 g_1 + \ldots + k_n g_n \to (k_1, \ldots, k_n).$$

O subconjunto S de G é dito linearmente independente se para quaisquer $s_1, \ldots, s_k \in S$, temos que

$$\sum_{i=1}^{k} n_i s_i = 0 \quad \textit{se, e somente se,} \quad n_1 = n_2 = \ldots = n_k = 0.$$

Uma base para G é um subconjunto linearmente independente que gera G.

Proposição 2.3. Se G é um grupo abeliano com base finita, então qualquer base finita tem a mesma quantidade de elementos.

Demonstração. Pode ser vista em [24], Lema 9.18. □

Dizemos que $g \in G$ é um elemento de torção se $ng = 0$, para algum inteiro não nulo n. Dizemos que um grupo G é livre de torção se o único elemento de torção é a identidade.

Proposição 2.4. Todo grupo abeliano finitamente gerado e livre de torção é um grupo abeliano livre de posto finito.

Demonstração. Pode ser vista em [24], Proposição 9.21. □

Seja G um p-grupo abeliano. Dizemos que o grupo G é um grupo **homocíclico** se G é produto direto de subgrupos cíclicos $K_1, \ldots, K_s$, com $|K_i| = p^n$, para $1 \leq i \leq s$ e n um inteiro positivo. O próximo resultado é fundamental para o Capítulo 3, mais especificamente sobre a construção de contraexemplos para a Conjectura de Andrei Jaikin-Zapirain 3.1.

Lema 2.10. (Lema 4.2, de [2]) Seja P um p-grupo secreto de *Wall* e seja $s > 0$ um inteiro. Então existe um grupo homocíclico U_s de expoente p^s que admite uma ação de P por automorfismos tal que o produto semidireto $U_s P$ satisfaz o seguinte:

(1) os elementos em $U_s P \setminus U_s \Phi(P)$ possuem ordem p^2;

(2) os elementos em $U_s\Phi(P)$ possuem ordem no máximo p^{s+1}.

Demonstração. Pelo Lema 2.8, $P^p = \langle z \rangle$ é um subgrupo central de P e $|z| = p$. Pelo Lema 2.9, existe uma representação complexa irredutível de P, digamos $\rho : P \to GL(V)$, tal que $z \notin \ker(\rho)$. Neste caso, V pode ser visto como um grupo aditivo. Considere o produto semidireto VP. A ação à direita de P sobre V é definida como ação de conjugação, isto é, $(v, x) \mapsto vx$, em que vx indica, por abuso de notação, o conjugado de um elemento $v \in V$ por um elemento $x \in P$.

Considere agora $\lambda = \rho|_{\langle z \rangle} : \langle z \rangle \to GL(V)$. A aplicação λ é injetiva. Para verificar isto, seja $\ker(\lambda) \leq \langle z \rangle$. Como $|z| = p$, segue que ou $|\ker(\lambda)| = 1$ ou $|\ker(\lambda)| = p$. Suponha que $|\ker(\lambda)| = p$, então $\ker(\lambda) = \langle z \rangle$. Logo, $z \in \ker(\lambda)$ e $\lambda(z) = 1_{GL(V)}$. Com isso,

$$\rho(z) = \rho|_{\langle z \rangle}(z) = \lambda(z) = 1_{GL(V)}.$$

Porém, ρ foi escolhido de tal forma que $z \notin \ker(\rho)$. Assim, λ é injetiva.

Como no produto semidireto VP a ação vz indica o conjugado de v por z, para $v \in V$ e $z \in P^p$, podemos denotar o centralizador de z em VP como

$$C_V(z) = \{v \in V \mid vz = v\}.$$

O conjunto $C_V(z)$ é um $\mathbb{C}P$-módulo de V. De fato, para quaisquer $w \in C_V(z)$ e $x \in P$ temos que

$$(wx)z = w(xz) = w(zx) = (wz)x = wx.$$

Logo, $wx \in C_V(z)$.

Seja

$$u := v + vz + vz^2 + \ldots + vz^{p-1} \in V.$$

Vamos mostrar que $u \in C_V(z)$. Como $z^p = 1$, temos

$$uz = (v + vz + vz^2 + \ldots + vz^{p-1})z = vz + vz^2 + \ldots + vz^{p-1} + v = u.$$

Logo, $uz = u$ e $u \in C_V(z)$. Como V é um $\mathbb{C}P$-módulo irredutível, temos que ou $C_V(z) = 0$ ou $C_V(z) = V$. Suponha que $C_V(z) = V$. Assim, para todo elemento $v \in V$, temos que $\rho(z) = 1_{GL(V)}$, pois $1_{GL(V)} : v \mapsto vz = v$. Logo, $z \in \ker(\rho)$, um absurdo. Portanto,

$$v + vz + vz^2 + \ldots + vz^{p-1} = 0 \quad \textit{para todo } v \in V. \tag{1}$$

Tome $0 \neq a \in V$ e seja

$$A = \langle ag \mid g \in P \rangle \leq V.$$

Pela Proposição 2.4, como A é um subgrupo finitamente gerado do grupo aditivo livre de torção V, então A é um grupo abeliano livre de posto finito. Construímos o grupo $U_s = A/p^sA$, em que é p-grupo finito homocíclico de expoente p^s que admite uma ação induzida por P.

Considere agora o produto semidireto U_sP com a notação multiplicativa. De modo similiar ao feito em (1), temos que

$$u \cdot u^z \cdot u^{z^2} \dots u^{z^{p-1}} = 1 \quad \textit{para todo } u \in U_s.$$

Como $z^p = 1$, a igualdade $u \cdot u^z \cdot u^{z^2} \dots u^{z^{p-1}} = 1$ é equivalente a

$$(uz)^p = u \cdot u^z \cdot u^{z^2} \dots u^{z^{p-1}} = 1$$

O mesmo vale para $(uz^k)^p = 1$, para qualquer $u \in U_s$ e qualquer $k \in \{1, 2, \dots, p-1\}$. Observe que se $g \in U_sP \setminus U_s\Phi(P)$, então $g = wh$, em que $w \in U_s$ e $h \in P \setminus \Phi(P)$. Assim,

$$g^p = (wh)^p = vh^p, \quad \textit{para algum} \quad v \in U_s.$$

Como $h \in P \setminus \Phi(P)$, pelo Lema 2.8, $|h| = p^2$ e $h^p = z^k$, para $k \in \{1, 2, \dots, p-1\}$, ou seja, $h^p = z^k \neq 1$. Logo,

$$g^{p^2} = (g^p)^p = ((wh)^p)^p = (vh^p)^p = (vz^k)^p = 1,$$

como queríamos.

Já o expoente de $U_s\Phi(P)$ é no máximo p^{s+1}. Basta observar que o expoente de U_s é igual a p^s e o expoente de $\Phi(P)$ é igual a p, pelo Lema 2.8. □

Capítulo 3

Conjectura de Andrei Jaikin-Zapirain e implicações

Abordaremos neste capítulo a construção dos contraexemplos para a Conjectura de Andrei Jaikin-Zapirain e apresentaremos um critério de solubilidade que envolve a função ordem média.

3.1 Construção de contraexemplos

A partir de agora apresentaremos uma conjectura proposta por Andrei Jaikin-Zapirain envolvendo uma relação entre $o(G)$ e $o(N)$, em que N é um subgrupo normal de G, respondida por E. I. Khukhro, A. Moretó e M. Zarrin [2]. Vale ressaltar que Andrei Jaikin-Zapirain, ao propor tal conjectura, investigava a função $k(G)$, isto é, o número de classes de conjugação de um grupo finito G, que por sua vez possui relação direta com a ordem média, conforme o Teorema 2.6 mostra. Para tanto, alguns resultados sobre ordem média de um grupo finito foram produzidos, incluindo uma estimativa da ordem média de um p-grupo *powerful*, os quais utilizaremos ao longo do texto abaixo.

O próximo teorema motiva a questão principal deste capítulo proposta por Andrei Jaikin-Zapirain.

Teorema 3.1. (A. Jaikin-Zapirain, Lema 2.7 de [1]) Seja G um grupo finito. Então $o(G) \geq o(Z(G))$.

Demonstração. Seja $x \in G$. Seja

$$m = min\{|y| \ ; \ y \in xZ(G)\}.$$

Neste caso, existe $y \in xZ(G)$ tal que $|y| = m$. Seja $a \in Z(G)$. Então $(ya)^m = a^m \in$

$Z(G)^m$. Assim, $l = |yaZ(G)^m|$ divide m. Por outro lado, existe $z \in Z(G)$ tal que $(ya)^l = z^m$. Logo, $(yaz^{-m/l})^l = 1$. Como m é minimal e $az^{-m/l} \in Z(G)$, temos que $m \leq l$. Assim, $m = l$. Pela Proposição 1.1, temos que $|(ya)^m| = |ya|/mdc(m, |ya|)$. Observe que $m = |yaZ(G)^m|$ divide $|ya|$, assim $(ya)^m| = |ya|/m$. Logo,

$$|ya| = m \cdot |(ya)^m| = m \cdot |a^m| = m \cdot \frac{|a|}{mdc(m, |a|)} \geq |a|.$$

Logo, como $|xZ(G)| = |Z(G)|$, temos

$$o(xZ(G)) = \frac{1}{|Z(G)|} \sum_{a \in Z(G)} |ya| \geq \frac{1}{|Z(G)|} \sum_{a \in Z(G)} |a| = o(Z(G)).$$

Com isso, obtemos que $\psi(xZ(G)) \geq \psi(Z(G))$. Considere

$$G = x_1 Z(G) \dot{\cup} \ldots \dot{\cup} x_j Z(G).$$

Portanto,

$$o(G) = \frac{\psi(x_1 Z(G)) + \ldots + \psi(x_j Z(G))}{|G|} \geq \frac{|G : Z(G)|\psi(Z(G))}{|G|} = o(Z(G)).$$

□

Este útimo teorema motiva a seguinte conjectura:

Conjectura 3.1. Seja G um grupo finito e seja $N \trianglelefteq G$. Então $o(G) \geq o(N)^{1/2}$.

Em suma, E. I. Khukhro, A. Moretó e M. Zarrin [2] forneceram uma resposta negativa à Conjectura de Andrei Jaikin-Zapirain 3.1, não apenas para o expoente 1/2. Vejamos o principal teorema produzido por estes autores.

Teorema 3.2. *(E. I. Khukhro, A. Moretó e M. Zarrin, Teorema 1.2 de [2])* Seja $c > 0$ um número real e seja $p \geq 3/c$ um primo. Então existe um p-grupo finito com um subgrupo normal abeliano N tal que $o(G) < o(N)^c$.

Demonstração. Seja c um número real e seja o primo p tal que $p \geq 3/c$. Mostraremos que há um p-grupo finito G com subgrupo normal abeliano N tal que $o(G) < o(N)^c$. Para tanto, utilizaremos fortemente o Lema 2.10.

Seja $s = p + 1$. Definamos $G = U_s P$ e $N = U_s$, em que U_s é um grupo homocíclico de expoente s e P um p-grupo secreto. Considere $|G| = p^n$. Pelo Lema 2.10, temos, respectivamente: se $x \in G \setminus U_s\Phi(P)$, então $|x| = p^2$; também, se $x \in U_s\Phi(P)$, então $|x| \leq p^{s+1} = p^{p+2}$.

Observe que G é produto semidireto de U_s e P, isto é, $U_s \cap P = 1$ e $|G| = |U_s||P|$. Como $\Phi(P) \leq P$, segue que $|U_s\Phi(P)| = |U_s||\Phi(P)|$. Daí,

$$[G : U_s\Phi(P)] = \frac{|G|}{|U_s\Phi(P)|} = \frac{|U_s||P|}{|U_s||\Phi(P)|} = \frac{|P|}{|\Phi(P)|} = p^p.$$

A última igualdade é válida pelo Lema 2.8, o que implica que $|U_s\Phi(P)| = p^{n-p}$. Assim, existem $p^n - p^{n-p}$ elementos com ordem p^2 e p^{n-p} elementos com ordem menor ou igual a p^{p+2}. Logo,

$$\begin{aligned} o(G) &\leq \frac{p^2(p^n - p^{n-p}) + p^{p+2} \cdot p^{n-p}}{p^n} \\ &= \frac{p^{n+2} - p^{n-p+2} + p^{n+2}}{p^n} \\ &= 2p^2 - p^{2-p} \\ &< 2p^2 \\ &\leq p^3. \end{aligned}$$

O subgrupo N é homocíclico e de expoente p^s. Em particular, N é um p-grupo *powerful*. Pelo Teorema 2.13,

$$o(N) \geq p^s - p^{s-1} = p^{p+1} - p^p \geq p^p.$$

Portanto,

$$o(G) < p^3 \leq p^{pc} = (p^p)^c \leq o(N)^c,$$

o que finaliza a demonstração.

□

Corolário 3.1. A Conjectura de Andrei Jaikin-Zapirain 3.1 tem resposta negativa para todo primo $p \geq 7$.

Demonstração. Se $c = 1/2$, pelo Teorema 3.2, há contraexemplos para Conjectura de Andrei Jaikin-Zapirain 3.1 para $p > 3/(1/2) = 6$, ou seja, para $p \geq 7$. A mesma construção da demonstração do Teorema 3.2 vale para $p = 5$ e $c = 1/2$. Para verificar isto, basta utilizar novamente o Teorema 2.13 Assim,

$$o(N)^{1/2} \geq (5^{5+1} - 5^5)^{1/2} > 50 = 2 \cdot 5^2 > o(G).$$

□

Para além da Conjectura de Andrei Jaikin-Zapirain 3.1, segundo E. I. Khukhro, A. Moretó e M. Zarrin [2], outras questões similares foram postas por Andrei Jaikin-Zapirain,

são elas:

Questão 3.1. Seja $mo(G)$ o máximo das ordens dos elementos de G. Existe uma constante $c_1 > 0$ tal que para todo grupo finito G temos que $o(G) \geq c_1 \cdot mo(G)^{1/2}$?

Questão 3.2. Existe uma constante $c_2 > 0$ tal que para todo grupo finito G e todo subgrupo normal N de G temos que $o(G) \geq c_2 \cdot o(N)^{1/2}$?

Ambas possuem resposta negativa, basta utilizarmos o Teorema 3.2 e a desigualdade

$$o(N) = \frac{\psi(N)}{|N|} < \frac{mo(G) \cdot |N|}{|N|} = mo(G).$$

Além disso, a seguinte questão permanece em aberta.

Questão 3.3. Seja p um primo. Existe um número $c = c(p) > 0$ tal que $o(G) \geq o(N)^c$ para qualquer p-grupo G e qualquer subgrupo normal N de G?

A seguir apresentamos um critério de solubilidade envolvendo a ordem média de um grupo finito. Para tanto, utilizaremos resultados acerca de automorfismos e a classificação de grupos simples.

3.2 Outro critério para solubilidade de grupos finitos

Nesta seção, apresentaremos um critério de solubilidade que envolve a ordem média de um grupo finito. Este critério foi inicialmente conjecturado por E. I. Khukhro, A. Moretó e M. Zarrin [2], presente no mesmo artigo em que os autores responderam a Conjectura de Andrei Jaikin-Zapirain 3.1. Tal conjectura é a seguinte:

Conjectura 3.2. Seja G um grupo finito. Se $o(G) < o(A_5)$, então G é solúvel.

Em 2022, M. Herzog, P. Longobardi e M. Maj [3] responderam positivamente esta conjectura. Com isso, o foco a partir de agora é demonstrá-la, tomando como base o estudo do artigo de M. Herzog, P. Longobardi e M. Maj [3]. Por isso, iniciamos com resultados que envolvem grupos simples e em seguida automorfismos.

3.2.1 Grupos simples

Primeiramente, denotamos o conjunto de todos os primos que dividem $|G|$ por $\Pi(G)$. Seja n um inteiro positivo, então, neste caso, denotamos $\pi(n)$ o conjunto de todos os primos que dividem n. Trataremos de grupos simples G tais que $\Pi(G) \subseteq \{2, 3, 5, 7, 11, 13\}$. Importante ressaltar algumas referências para o estudo destes grupos. M. Herzog [16] estudou casos em que $|\Pi(G)| = 3$. Para grupos simples com $|\Pi(G)| = 4$, temos Y. Bugeaud, Z. Cao e M. Mignotte [17] e para $|\Pi(G)| \in \{5, 6\}$ temos A. Jafarzadeh e A.

Iranmanesh [18]. Também há contribuições do artigo de D. Yu, J. Li, G. Chen, L. Zhang e W. Shi [19]. A notação dos grupos que utilizamos nesta Subseção, é baseada em [15], bem como as informações sobre ordem dos grupos, fatoração das ordens, classificação geral, enfim características que serão importantes para os próximos resultados.

Os grupos lineares, ortogonais, unitários e simpléticos são conhecidos como grupos clássicos. Com as contribuições de Claude Chevalley, Robert Steinberg, Michio Suzuki, Jacques Tits e Remhak Ree, os grupos clássicos tiveram algumas generalizações. Chamamos de grupos do tipo Lie os grupos clássicos somados aos ditos grupos de Chevalley [15]. Outra classe de grupo simples é conhecida como grupos esporádicos. Há 26 grupos desta categoria. Listamos abaixo os grupos simples conforme sua quantidade de primos que dividem suas respectivas ordens.

Denotamos a quantidade de elementos de um corpo finito $\mathbb{F}_q$ por q, ou seja, q é uma potência de primo.

Proposição 3.1. Seja G um grupo finito simples com $\Pi(G) \subseteq \{2,3,5,7,11,13\}$. Então:

(1) Se $|\Pi(G)| = 3$, então G é isomorfo a um dos seguintes grupos:

$$A_5, \quad A_6, \quad U_4(2) \cong S_4(3), \quad L_2(7), \quad L_2(8), \quad L_3(3), \quad U_3(3).$$

(2) Se $|\Pi(G)| = 4$, então G é isomorfo a um dos seguintes grupos:

$$L_2(q), \quad \textit{para } q \textit{ um primo}, \quad |\pi(q^2-1)| = 3,$$

$$L_2(2^m), \quad 2^m - 1 = u, \quad 2^m + 1 = 3t, \ u, \ t \textit{ primos}, \quad t > 3,$$

$$L_2(3^m), \quad 3^m - 1 = 2u, \quad 3^m + 1 = 4t, \ u, \ t \textit{ primos},$$

$$L_2(25), L_2(49), L_3(4), L_4(3), U_3(4), U_3(5), U_4(3), U_5(2), S_4(5), S_4(7), S_6(2),$$

$$O_8^+(2), G_2(3), \ {}^3D_4(2), \ {}^2F_4(2)', Sz(8), A_7, A_8, A_9, A_{10}, M_{11}, M_{12}, J_2.$$

(3) Se $|\Pi(G)| = 5$, então G é isomorfo a um dos seguintes grupos:

$$L_2(q), \quad \textit{para } q \textit{ uma potência de primo}, \quad |\pi(q^2-1)| = 4,$$

$$L_3(q), \quad \textit{para } q \textit{ uma potência de primo}, \quad |\pi((q^2-1)(q^3-1))| = 4,$$

$$U_3(q), \quad \textit{para } q \textit{ uma potência de primo}, \quad |\pi((q^2-1)(q^3+1))| = 4,$$

$$O_5(q) \cong S_4(q), \quad \textit{para } q \textit{ uma potência de primo}, \quad |\pi(q^4-1)| = 4,$$

$$Sz(2^{2m+1}) \cong {}^2B_2(2^{2m+1}), \quad \textit{com} \quad |\pi((2^{2m+1}-1)(2^{4m+2}+1))| = 4,$$

$$R(q),\ com\ \ q = 3^{2m+1},\ |\pi(q^2-1)| = 3\ e\ \ |\pi(q^2-q+1)| = 1,$$

$$L_4(3), S_6(3), U_4(5), U_6(2), O_7(3), O_8^+(3), G_2(4),$$

$$A_{11}, A_{12}, M_{22}, HS, McL.$$

(4) Se $|\Pi(G)| = 6$, então G é isomorfo a um dos seguintes grupos:

$$L_2(q),\ \ para\ q\ uma\ potência\ de\ primo,\ \ |\pi(q^2-1)| = 5,$$

$$L_3(q),\ \ para\ q\ uma\ potência\ de\ primo,\ \ |\pi((q^2-1)(q^3-1))| = 5,$$

$$L_4(q),\ \ para\ q\ uma\ potência\ de\ primo,\ \ |\pi((q^2-1)(q^3-1)(q^4-1))| = 5,$$

$$U_3(q),\ \ para\ q\ uma\ potência\ de\ primo,\ \ |\pi((q^2-1)(q^3+1))| = 5,$$

$$U_4(q),\ \ para\ q\ uma\ potência\ de\ primo,\ \ |\pi((q^2-1)(q^3+1)(q^4-1))| = 5,$$

$$O_5(q) \cong S_4(q),\ \ para\ q\ uma\ potência\ de\ primo,\ \ |\pi(q^4-1)| = 5,$$

$$G_2(q),\ \ para\ q\ uma\ potência\ de\ primo,\ \ |\pi(q^6-1)| = 5,$$

$$Sz(2^{2m+1}) \cong\ {}^2B_2(2^{2m+1}),\ \ com\ \ |\pi((2^{2m+1}-1)(2^{4m+2}+1))| = 5,$$

$$R(3^{2m+1}),\ \ com\ \ |\pi((3^{2m+1}-1)(3^{6m+3}+1))| = 5,$$

$$L_6(3), A_{13}, A_{14}, A_{15}, A_{16}, Suz, Fi_{22}.$$

A Tabela 3.1 apresenta limites inferiores para os valores de $i_2(G)$ e $|G|$, denotados por $f(G,2)$ e $g(G)$, respectivamente.

Tabela 3.1: Limites inferiores para $i_2(G)$ e $|G|$

Grupo	$f(G,2)$	$g(G)$
$L_n(q) = PSL_n(q)$	$(n^2+n-2)/2$	$2^{-1}\cdot(q+1)^{-1}\cdot q^{n^2-1}$
$U_n(q) = PSU_n(q)$	$(n^2+n-2)/2$	$2^{-1}\cdot(q+1)^{-1}\cdot q^{n^2-1}$
${}^2G_2(q)$	4	$q^7/2$
$G_2(q)$	8	$q^{14}/2$
$P\Omega_n(q) = O_n^+(q)$	$n^2/4$	$q^{(n^2-n)/2}/8$
${}^2B_2(q) = Sz(2^{2m+1})$, $q = 2^{m+1}$, $m \geq 1$	3	$q^5/2$
$PSp_n(q)' = S_n(q)$	$(n^2+2n)/4$	$q^{(n^2+n)/2}/4$
${}^3D_4(q)$	16	$q^{28}/2$

Fonte: T. C. Burness e S. D. Scott [4]

O próximo teorema estabelece uma cota da quantidade de elementos de ordem 2 e 3 para grupo simples do tipo Lie. Utilizaremos este resultado para estimar a ordem média destes grupos do tipo Lie. Observe que $g(G) < |G|$. Com isso, temos o seguinte resultado:

Teorema 3.3. Seja G um grupo simples do tipo Lie sobre $\mathbb{F}_p$. Para $r \in \{2, 3\}$,

$$i_r(G) \leq 2(1 + q^{-1})q^{f(G,r)}.$$

A demonstração pode ser encontrada no Lema 2.13 de [4].

Lema 3.1. As afirmações abaixo são válidas.

(1) Seja $G \cong A_n$, com $n \geq 5$. Então $G \cong A_5$ ou $o(G) \geq 3,55$;

(2) Seja $G \cong L_2(q)$, com $q \geq 4$ e $\Pi(G) \subseteq \{2, 3, 5, 7, 11, 13\}$. Então $G \cong A_5$ ou $o(G) \geq 3,55$;

(3) Seja $G \cong L_3(q)$, com $q \in \{3, 4\}$ ou $q \geq 8$. Então $o(G) \geq 3,55$;

(4) Seja $G \cong U_3(q)$, com $q \in \{3, 4, 5\}$ ou $q \geq 8$. Então $o(G) \geq 3,55$.

Demonstração. (1) Para $n = 6$, temos

$$o(A_6) = \frac{\psi(A_6)}{|A_6|} = \frac{1411}{360} > 3,91.$$

Suponha que $n \geq 7$. Pelo Lema 3.3 em [4], temos que

$$\frac{i_2(A_n)}{|A_n|} \leq \frac{2}{8(n-4)!} + \frac{2}{2^4 \cdot 23} = \frac{1}{4} \cdot \left(\frac{1}{(n-4)!} + \frac{1}{46} \right).$$

Observe que quanto maior o valor de n tomarmos, o fator

$$\left(\frac{1}{(n-4)!} + \frac{1}{46} \right)$$

diminui. Logo, é suficiente mostrar que $i_2(A_7)/|A_7| \leq 1/20$ e utilizar o Lema 2.3. Segue que

$$\frac{i_2(A_7)}{|A_7|} \leq \frac{1}{4} \cdot \left(\frac{1}{6} + \frac{1}{46} \right) = \frac{13}{276} < \frac{1}{20}.$$

(2) Se $q \in \{4, 5\}$, então $G \cong A_5$. Se $q = 7$, então

$$o(L_2(7)) = \frac{\psi(L_2(7))}{|L_2(7)|} = \frac{715}{168} \geq 4,2.$$

Se $q = 8$, então

$$o(L_2(8)) = \frac{\psi(L_2(8))}{|L_2(8)|} = \frac{3319}{504} \geq 6,5.$$

Se $q = 9$, então $L_2(9) \cong A_6$ e pelo item anterior $o(L_2(9)) > 3,55$. Se $q = 11$, então

$$o(L_2(11)) = \frac{\psi(L_2(11))}{|L_2(11)|} = \frac{3741}{660} \geq 5,6.$$

Se $q = 13$, então

$$o(L_2(13)) = \frac{\psi(L_2(13))}{|L_2(13)|} = \frac{7281}{1092} \geq 6,6.$$

Como 17 divide $|L_2(16)|$ e $|L_2(17)|$ e 19 divide $|L_2(19)|$, considere grupos $G = L_2(q)$ para $q \geq 23$. Se q é par, então $|G| = q(q^2-1)$ e $i_2(G) = q^2 - 1 = |G|/q$. Se q é ímpar, então pelo Lema 3.4 em [4] temos

$$|G| = \frac{1}{2}q(q^2-1) \quad e \quad i_2(G) \leq \frac{1}{2}q(q+1) = \frac{|G|}{q-1}.$$

Como $q \geq 23$, em ambos os casos

$$i_2(G) \leq \frac{|G|}{q-1} \leq \frac{|G|}{22}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$.

(3) Se $q \in \{4, 8, 9\}$, então, por [15], tem apenas uma classe de conjugação de involuções e as ordens de seus 2-subgrupos Sylow são $2^6, 2^9$ e 2^7, respectivamente. Se $q = 3$, então, por [15], $G \cong L_3(q)$ também tem apenas uma classe de conjugação de involuções, e o tamanho dessa classe é $\frac{|G|}{48}$. Nos outros casos, temos $i_2(G) < \frac{|G|}{20}$, logo $o(G) \geq 3,55$.

Resta verificar para $G \cong L_3(q)$ para $q \geq 11$. Pela Tabela 3.1 e o Teorema 3.3, temos que

$$\frac{|G|}{20} > \frac{1}{40} \cdot \frac{q^8}{q+1}$$

e

$$i_2(G) \leq 2(q+1)q^4 \leq \frac{2(q+1)q^8}{(q^2-1)(q^2-1)} = \frac{2q^8}{(q-1)^2(q+1)} \leq \frac{2q^8}{100(q+1)}.$$

Portanto,

$$i_2(G) < \frac{1}{40} \cdot \frac{q^8}{q+1} < \frac{|G|}{20}$$

e pelo Lema 2.3 temos $o(G) \geq 3,55$.

(4) Se $q \in \{3, 4, 8, 9\}$, então, por [15], tem apenas uma classe de conjugação de involuções e as ordens de seus 2-subgrupos Sylow são $2^5, 2^6, 2^9$ e 2^5, respectivamente. Se

$q = 5$, então, por [15], $G \cong U_3(5)$ também tem apenas uma classe de conjugação de involuções, e o tamanho dessa classe é $\frac{|G|}{240}$. Nos outros casos, temos $i_2(G) < \frac{|G|}{20}$, logo $o(G) \geq 3,55$.

Resta verificar com $G \cong U_3(q)$ para $q \geq 11$. Pela Tabela 3.1 e o Teorema 3.3, temos que

$$\frac{|G|}{20} > \frac{1}{40} \cdot \frac{q^8}{q+1} \quad e \quad i_2(G) \leq 2(q+1)q^4.$$

Portanto, conforme o item anterior temos $i_2(G) < |G|/20$ e $o(G) \geq 3,55$. □

Lema 3.2. São válidos cada um dos itens abaixo:

(1) Seja $G \cong L_4(q)$ ou $G \cong U_4(q)$, com $q \geq 3$. Então $o(G) \geq 3,55$;

(2) Seja $G \cong L_5(q)$ ou $G \cong U_5(q)$, com $q \geq 2$. Então $o(G) \geq 3,55$;

(3) Seja $G \cong R(q) \cong \ {}^2G_2(q)$, com $q = 3^{2n+1}$ e $n \geq 1$. Então $o(G) \geq 3,55$;

(4) Seja $G \cong G_2(q)$, com $q \geq 3$. Então $o(G) \geq 3,55$;

(5) Seja $G \cong S_4(q)$, com $q \geq 5$. Então $o(G) \geq 3,55$;

(6) Seja $G \cong Sz(2^{2m+1}) \cong \ {}^2B_2(q)$, com $q = 2^{2m+1}$, com $m \geq 1$. Então $o(G) \geq 3,55$;

(7) Seja $G \cong S_6(q)$, com $q \geq 2$. Então $o(G) \geq 3,55$;

(8) Seja $G \cong O_8^+(q)$, com $q \geq 2$. Então $o(G) \geq 3,55$;

(9) Seja $G \cong \ {}^3D_4(2)$. Então $o(G) \geq 3,55$;

(10) Seja $G \cong \ {}^2F_4(2)'$. Então $o(G) \geq 3,55$.

Demonstração. As demonstrações dos itens são relativamente similares.

(1) Como mencionado anteriormente, $|G| > g(G)$. Se $G \cong L_4(q)$ ou $G \cong U_4(q)$ com $q \geq 3$, então pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^{15}}{2(q+1)} = \frac{q^{15}}{40(q+1)}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^{\frac{4^2+4-2}{2}} &= 2(1+q^{-1})q^9 \\ &\leq \frac{2(q+1)q^{15}}{(q^2-1)(q^2-1)q^3} \\ &< \frac{2q^{15}}{100(q+1)}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^{15}}{100(q+1)} = \frac{q^{15}}{50(q+1)} < \frac{q^{15}}{40(q+1)} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$.

(2) O processo é análogo ao item anterior. Se $G \cong L_5(q)$ ou $G \cong U_5(q)$ com $q \geq 2$, então pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^{24}}{2(q+1)} = \frac{q^{24}}{40(q+1)}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^{\frac{5^2+5-2}{2}} = 2(1+q^{-1})q^{14} &= 2(q^{14}+q^{13}) \\ &\leq \frac{2(q+1)q^{24}}{(q^2-1)(q^2-1)q^7} \\ &\leq \frac{2q^{24}}{100(q+1)}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^{24}}{100(q+1)} = \frac{q^{24}}{50(q+1)} < \frac{q^{24}}{40(q+1)} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$.

(3) Se $G \cong {}^2G_2(q)$ com $q = 3^{2n+1}$ e $n \geq 1$, então pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^7}{2} = \frac{q^7}{40}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^4 = 2(q^4+q^3) = 2(q+1)q^3 = \frac{2(q+1)q^7}{q^4} &= \frac{2(q+1)q^7}{q^2q^2} \\ &\leq \frac{2(q+1)q^7}{(q^2-1)q^2} \\ &\leq \frac{2q^7}{100}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^7}{100} = \frac{q^7}{50} < \frac{q^7}{40} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$.

(4) Se $G \cong G_2(q)$ com $q \geq 3$, então pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^{14}}{2} = \frac{q^{14}}{40}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^8 = 2(q^8+q^7) = 2(q+1)q^7 = \frac{2(q+1)q^{14}}{q^7} &= \frac{2(q+1)q^{14}}{q^2q^5} \\ &\leq \frac{2(q+1)q^{14}}{(q^2-1)q^5} \\ &= \frac{2(q+1)q^{14}}{(q-1)(q+1)q^5} \\ &= \frac{2q^{14}}{(q-1)q^5} \\ &\leq \frac{2q^{14}}{100}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^{14}}{100} = \frac{q^{14}}{50} < \frac{q^{24}}{40(q+1)} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$.

(5) Se $G \cong S_4(q)$ com $q \geq 5$, então pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^{10}}{4} = \frac{q^{10}}{80}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^{\frac{4^2+2\cdot 4}{4}} = 2(1+q^{-1})q^6 = 2(q+1)q^5 = \frac{2(q+1)q^{10}}{q^5} &= \frac{2(q+1)q^{10}}{q^2q^3} \\ &\leq \frac{2(q+1)q^{10}}{(q^2-1)q^3} \\ &= \frac{2(q+1)q^{10}}{(q-1)(q+1)q^3} \\ &= \frac{2q^{10}}{(q-1)q^3} \\ &\leq \frac{2q^{10}}{200}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^{10}}{200} = \frac{q^{10}}{100} < \frac{q^{10}}{80} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$

(6) Para $m = 1$, então $G \cong Sz(8)$ tem apenas uma classe de conjugação de involuções e a ordem de seu 2-subgrupos de Sylow é 2^6. Assim, segue que $i_2(G) < |G|/20$ e, com isso, $o(G) \geq 3,55$.

Suponha $m > 1$ e $q \geq 32$. Pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^5}{2} = \frac{q^5}{40}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^3 = 2(q^3+q^2) = 2(q+1)q^2 = \frac{2(q+1)q^5}{q^3} &= \frac{2(q+1)q^5}{q^2 q} \\ &\leq \frac{2(q+1)q^5}{(q^2-1)q} \\ &= \frac{2(q+1)q^5}{(q-1)(q+1)q} \\ &= \frac{2q^5}{(q-1)q} \\ &\leq \frac{2q^5}{100}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^5}{100} = \frac{q^5}{50} < \frac{q^5}{40} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$

(7) Se $G \cong S_6(q)$ com $q \geq 2$, então pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^{\frac{6^2+6}{2}}}{4} = \frac{q^{21}}{80}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^{\frac{6^2+2\cdot 6}{4}} = 2(1+q^{-1})q^{12} = 2(q^{12}+q^{11}) &= 2(q+1)q^{11} \\ &= \frac{2(q+1)q^{21}}{q^2 q^8} \\ &\leq \frac{2(q+1)q^{21}}{(q^2-1)q^8} \\ &= \frac{2q^{21}}{(q-1)q^8} \\ &\leq \frac{2q^{21}}{200}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^{21}}{200} = \frac{q^{21}}{100} < \frac{q^{21}}{80} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$.

(8) Se $G \cong O_8^+(q)$ com $q \geq 2$, então pela Tabela 3.1, seque que

$$\frac{|G|}{20} > \frac{g(G)}{20} = \frac{1}{20} \cdot \frac{q^{\frac{8^2-8}{2}}}{8} = \frac{q^{28}}{160}.$$

Pelo Teorema 3.3, temos que

$$\begin{aligned} i_2(G) \leq 2(1+q^{-1})q^{\frac{8^2}{4}} = 2(1+q^{-1})q^{16} = 2(q^{16}+q^{15}) = 2(q+1)q^{15} &= \frac{2(q+1)q^{28}}{q^{13}} \\ &\leq \frac{2(q+1)q^{28}}{(q^2-1)q^{11}} \\ &= \frac{2(q+1)q^{28}}{(q-1)(q+1)q^{11}} \\ &\leq \frac{2q^{28}}{400}. \end{aligned}$$

Assim,

$$i_2(G) \leq \frac{2q^{28}}{400} = \frac{q^{28}}{200} < \frac{q^{28}}{160} < \frac{|G|}{20}.$$

Pelo Lema 2.3, concluímos que $o(G) \geq 3,55$.

(9) Por [15],

$$i_2(G) < 2 \cdot \frac{|G|}{3072} < \frac{|G|}{20}.$$

Pelo Lema 2.3 concluímos que $o(G) \geq 3,55$.

(10) Por [15],

$$i_2(G) < 2 \cdot \frac{|G|}{1536} < \frac{|G|}{20}.$$

Pelo Lema 2.3 concluímos que $o(G) \geq 3,55$.

□

Proposição 3.2. Seja G um grupo finito simples e suponha $\Pi(G) \subseteq \{2,3,5,7,11,13\}$.

(1) Se $|\Pi(G)| = 3$, então $G \cong A_5$ ou $o(G) \geq 3,55$;

(2) Se $|\Pi(G)| = 4$, então $o(G) \geq 3,55$;

(3) Se $|\Pi(G)| = 5$, então $o(G) \geq 3,55$;

(4) Se $|\Pi(G)| = 6$, então $o(G) \geq 3,55$.

Demonstração. (1) G é isomorfo a um dos grupos da Proposição 3.1. Pelo Lema 3.1, se G é isomorfo a A_6, $L_2(7)$, $L_2(8)$, $L_3(3)$ ou $U_3(3)$, então $o(G) \geq 3,55$. Restam A_5 e $U_4(2)$.

Suponha $G \cong U_4(2)$, então por [15]

$$i_2(G) < 2 \cdot \frac{|G|}{96} < \frac{|G|}{20}.$$

Portanto, pelo Lema 2.3 concluímos que $o(G) \geq 3,55$.

(2) G é isomorfo a um dos grupos da Proposição 3.1. Pelo Lema 3.2, apenas os grupos M_{11}, M_{12} e J_2 precisam ser verificados. Por [15], se $G \cong M_{11}$, então

$$i_2(G) = \frac{|G|}{48} < \frac{|G|}{20}.$$

Se $G \cong M_{12}$, então

$$i_2(G) < 2 \cdot \frac{|G|}{192} < \frac{|G|}{20}.$$

Se $G \cong J_2$, então

$$i_2(G) < 2 \cdot \frac{|G|}{240} < \frac{|G|}{20}.$$

Portanto, pelo Lema 2.3 concluímos que $o(G) \geq 3,55$.

(3) G é isomorfo a um dos grupos da Proposição 3.1. Pelo Lema 3.2, apenas os grupos $U_6(2)$, $O_7(3)$, M_{22}, HS e McL precisam ser verificados. Por [15], se $G \cong U_6(2)$, então

$$i_2(G) < 3 \cdot \frac{|G|}{36864} < \frac{|G|}{20}.$$

Se $G \cong O_7(3)$, então

$$i_2(G) < 3 \cdot \frac{|G|}{13824} < \frac{|G|}{20}.$$

Se $G \cong M_{22}$, então

$$i_2(G) = \frac{|G|}{384} < \frac{|G|}{20}.$$

Se $G \cong HS$, então

$$i_2(G) = 2 \cdot \frac{|G|}{2880} < \frac{|G|}{20}.$$

Se $G \cong McL$, então

$$i_2(G) = \frac{|G|}{40320} < \frac{|G|}{20}.$$

(4) G é isomorfo a um dos grupos da Proposição 3.1. Pelo Lema 3.2, apenas os grupos $L_6(3)$, Suz e Fi_{22} precisam ser verificados. Por [15], se $G \cong L_6(3)$, então pelo Teorema 3.3 e pela Tabela 3.1 segue que

$$\frac{|G|}{20} > \frac{1}{160} \cdot 3^{35} > 3^{21} \quad e \quad i_2(G) < 8 \cdot 3^{19} < 3^{21} < \frac{|G|}{20}.$$

Assim, pelo Lema 2.3 concluímos que $o(G) \geq 3,55$.

Se $G \cong Suz$, então

$$i_2(G) < 2 \cdot \frac{|G|}{161280} < \frac{|G|}{20}.$$

Se $G \cong Fi_{22}$, então

$$i_2(G) = 3 \cdot \frac{|G|}{1769472} < \frac{|G|}{20}.$$

Portanto, pelo Lema 2.3 concluímos que $o(G) \geq 3,55$. □

Teorema 3.4. *(M. Herzog, P. Longobardi e M. Maj, Teorema 4.19 de [3])* Seja G um grupo finito simples e suponha $\Pi(G) \subseteq \{2,3,5,7,11,13\}$. Então

$$G \cong A_5 \quad ou \quad o(G) \geq 3,55 > o(A_5).$$

Demonstração. Como G é um grupo simples, temos que $|\Pi(G)| \in \{3,4,5,6\}$. Portanto, pela Proposição 3.2 concluímos que

$$G \cong A_5 \quad ou \quad o(G) \geq 3,55 > o(A_5).$$

□

3.2.2 Automorfismos de grupos não-solúveis

Nesta Subseção, provaremos o Teorema 3.6, essencial para o critério de solubilidade que envolvem a ordem média. Primeiramente, abordaremos alguns lemas, em que para demonstrá-los serão utilizadas propriedades interessantes sobre automorfismos de grupos finitos. O estudo dos próximos resultados desta Subseção deve-se a W. M. Potter [20].

Vejamos alguns conceitos auxiliares. O primeiro deles é a definição de grupo p-nilpotente. Dizemos que um grupo finito G é p-nilpotente se existe $N < G$ tal que $G = PN$ e $P \cap N = 1$, em que $P \in Syl_p(G)$. Dizemos que N é um p-complemento normal de P em G. Agora, um teorema importante.

Teorema 3.5. Teorema do complemento normal de Burnside) Sejam p um primo, G um grupo finito e $P \in Syl_p(G)$. Se $P \leq Z(N_G(P))$, então G é p-nilpotente. Além disso, para P é abeliano temos que G é p-nilpotente se, e somente se, $N_G(P) = C_G(P)$.

Demonstração. Para uma demonstração, veja o Teorema 7.50 de [22]. □

Dizemos que $\theta \in Aut(G)$ inverte um elemento $g \in G$ se $g^\theta = g^{-1}$. Defina

$$S(\theta) := \{g \in G \mid g^\theta = g^{-1}\} \quad e \quad r(G,\theta) := \frac{|S(\theta)|}{|G|}.$$

Desta forma, $r(G,\theta)$ determina a proporção de elementos do grupo G que são invertidos pelo automorfismo θ.

Proposição 3.3. Sejam G um grupo finito e $\theta \in Aut(G)$. Se $r(G,\theta) > 4/15$, então G é solúvel.

Para uma demonstração veja o Corolário 3.2 [20].

Considere $x \in G$ e $\theta \in Aut(G)$. Utilizaremos a notação $x\theta$ para denotar o automorfismo de G definido por: $g^{x\theta} = (x^{-1}gx)^{\theta}$.

Lema 3.3. Sejam $\theta \in Aut(G)$ e $H \leq G$. Então

(1) se $x \in S(\theta)$, então $S(x\theta) = S(\theta)x^{-1}$;

(2) existe $x \in S(\theta)$ tal que

$$|Hx \cap S(\theta)| = |H \cap S(x\theta)| \geq r(G,\theta) \cdot |H|;$$

(3) Se $H \subseteq S(\theta)$, então para todo $z \in G$ ou

$$Hz \cap S(\theta) = \varnothing \quad ou \quad |Hz \cap S(\theta)| = |C_H(\langle z \rangle)|.$$

Demonstração. (1) Seja $x \in S(\theta)$. Então

$$y \in S(x\theta) \iff y^{-1} = y^{x\theta} = (x^{-1}yx)^{\theta} = x(yx)^{\theta} \iff (yx)^{-1} = (yx)^{\theta} \iff yx \in S(\theta).$$

Logo, existe

$$g \in S(\theta), \quad tal\ que \quad yx = g \implies y = gx^{-1} \implies S(x\theta) = S(\theta)x^{-1}.$$

(2) Como $|S(\theta)| = r(G,\theta) \cdot |G|$ e G é a união disjunta das classes laterais de H, então

$$|xH \cap S(\theta)| \geq r(G,\theta) \cdot |H|$$

para todo $x \in G$. Supondo que $x \in S(\theta)$ e conforme o item anterior, temos que

$$(xH \cap S(\theta)) \cdot x^{-1} = H \cap S(x\theta).$$

(3) Se $x, y \in S(\theta)$, temos que $xy \in S(\theta)$ se, e somente se, $[x,y] = 1$. Suponha $Hz \subset S(\theta)$ e, sem perda de generalidade $z \in S(\theta)$. Uma vez que $H \leq S(\theta)$, $hz \in S(\theta)$ se, e somente se, $h \in C_H(\langle z \rangle)$. □

Suponha que $\theta \in Aut(G)$ e que $N \trianglelefteq G$ tal que N é $\theta-$invariante. Então definimos o automorfismo $\overline{\theta} \in Aut(G/N)$ por $(gN)^{\overline{\theta}} = g^{\theta}N$, para todo $gN \in G/N$.

Lema 3.4. Sejam G um grupo finito, $N \trianglelefteq G$ e $\theta \in Aut(G)$ tal que $N^{\theta} = N$. Se

$$|gN \cap S(\theta)| \leq t|N|,$$

para todo $g \in S(\theta)$, então

$$t^{-1} \cdot r(G, \theta) \leq r(G/N, \overline{\theta}).$$

Demonstração. Seja $x \in S(\theta)$. Então

$$(xN)^{\overline{\theta}} = x^{\theta}N = x^{-1}N.$$

Logo, $xN \in S(\overline{\theta})$. Seja um transversal $\tau = \{x_1, \ldots, x_n\}$ de N em G, tal que $x_1, \ldots, x_k \in S(\theta)$ e $x_iN \cap S(\theta) = \emptyset$, para $k \leq i \leq n$. Então

$$S(\theta) = G \cap S(\theta) = \bigcup_{i=1}^{k} (x_iN \cap S(\theta)).$$

Logo,

$$|S(\theta)| = \sum_{i=1}^{k} |x_iN \cap S(\theta)| = k \cdot |x_iN \cap S(\theta)|.$$

Por hipótese, $|gN \cap S(\theta)| \leq t|N|$, assim

$$|S(\theta)| = k \cdot |x_iN \cap S(\theta)| \leq k \cdot t \cdot |N| \implies k \geq \frac{|S(\theta)|}{t \cdot |N|} = \frac{|S(\theta)| \cdot t^{-1}}{|N|}.$$

Observe que cada $x_i \in S(\theta)$, para $1 \leq i \leq k$, então

$$(x_iN)^{\overline{\theta}} = x_i^{\theta}N = x_i^{-1} \implies |S(\overline{\theta}| \geq k.$$

Assim,

$$|S(\overline{\theta}) \geq \frac{|S(\theta)| \cdot t^{-1}}{|N|}.$$

Dividindo por $|G/N|$ em ambos os lados da desigualdade obtemos

$$r(G/N, \overline{\theta}) = \frac{|S(\overline{\theta})|}{|G/N|} \geq \frac{|S(\theta)| \cdot t^{-1}}{|N| \cdot |G/N|} = r(G, \theta) \cdot t^{-1}.$$

□

Lema 3.5. Sejam G um grupo finito, $H \leq G$ e p o menor primo que divide $|H|$. Se

$\theta \in Aut(G)$ que inverte cada elemento de H e $r(G,\theta) > 1/p$, então

$$[G : C_G(H)] \leq \frac{p-1}{p \cdot r(G,\theta) - 1}.$$

Demonstração. Por hipótese, $H \subset S(\theta)$, logo H é abeliano e $H \leq C_G(H)$. Seja $\tau = \{x_1, \ldots, x_n\}$ um transversal de H em G, em que

$$C_G(H) = x_1 H \dot{\cup} \ldots \dot{\cup} x_k H.$$

Então

$$S(\theta) = (C_G(H) \cap S(\theta)) \bigcup_{i=k+1}^{n} (x_i H \cup S(\theta)).$$

Logo,

$$|S(\theta)| = |C_G(H) \cap S(\theta)| + \sum_{i=k+1}^{n} |x_i H \cup S(\theta)|.$$

Pelo Lema 3.3, temos $x_i H \cap S(\theta) = \emptyset$ ou $|x_i H \cap S(\theta)| = |C_H(\langle x_i \rangle)|$. Quando $i \geq k+1$, temos que $C_H(x_i) \leq H$ e como p é o menor primo que divide $|H|$, segue que $|C_H(x_i)| \leq p^{-1} \cdot |H|$. Como $|G_G(H) \cup S(\theta)| \leq |C_G(H)|$ e sendo

$$n - k = [G : N] - [C_G(H) : H],$$

temos

$$|S(\theta)| \leq |C_G(H)| + (n-k) \cdot |H| \cdot \frac{1}{p} = |C_G(H)| + \frac{1}{p}|G| - \frac{1}{p}|C_G(H)|.$$

Ao multiplicar p em ambos os lados da desigualdade obtemos

$$p \cdot |S(\theta)| \leq p \cdot |C_G(H)| + |G| - |C_G(H)| = (p-1)|C_G(H)| + |G|.$$

Logo,

$$p \cdot |S(\theta)| - |G| \leq (p-1)|C_G(H)|.$$

Dividindo $|G|$ em ambos os lados e utilizando a hipótese de que $r(G,\theta) > 1/p$ obtemos

$$p \cdot r(G,\theta) - 1 = \frac{p \cdot |S(\theta)| - |G|}{|G|} \leq \frac{|C_G(H)|}{|G|} \cdot (p-1).$$

Portanto,

$$[G : C_G(H)] \leq \frac{p-1}{p \cdot r(G,\theta) - 1}.$$

□

Lema 3.6. Sejam G um grupo finito, $\theta \in Aut(G)$ e P um p-subgrupo de Sylow de G. Se

$r(G,\theta) > 2/(p+1)$, então P é normal em G.

A demonstração pode ser vista no Teorema 2.5 de [20].

Teorema 3.6. *(M. Herzog, P. Longobardi e M. Maj, Teorema 5.5 de [3])* Seja G um grupo finito não-solúvel tal que G não contém subgrupos normais solúveis não triviais. Seja $\theta \in Aut(G)$. Se $r(G,\theta) > 2/9$, então $G \cong A_5$.

Demonstração. Suponha que $\theta \in Aut(G)$ e $r(G,\theta) > 2/9$. Suponha que G é um grupo simples. Sejam p é um primo que divide $|G|$ e P o p-subgrupo de Sylow de G. Neste caso, P não é normal em G e pelo Lema 3.6 temos que

$$\frac{2}{p+1} \geq r(G,\theta) > \frac{2}{9}.$$

Assim, $p+1 < 9$, isto é, $p \in \{2,3,5,7\}$. Como G é não-solúvel, segue que $|\Pi(G)| \geq 3$. Então G possui um 5-subgrupo de Sylow ou 7-subgrupo de Sylow. Neste caso, $p \geq 5$, logo pelo Lema 3.3 e ao substituir $x\theta$ por θ (pois $r(G,x\theta) > 2/9$), segue

$$|P \cap S(\theta)| > r(G,\theta)|P| > \frac{2}{9} \cdot |P| > \frac{1}{p} \cdot |P|.$$

Então $\langle P \cap S(\theta)\rangle = P$ e $P^\theta = P$. Como p é ímpar, pelo Lema 4.1 no Capítulo 10 de [25] temos que $P = C_P(\theta)(S(\theta) \cap P)$, logo

$$|C_P(\theta)| = \frac{|P|}{|S(\theta) \cap P|} < p.$$

Assim, $S(\theta) \cap P = P$. Logo, P é invertido ponto a ponto por θ, o que implica que P é abeliano. Como $r(G,\theta) > 2/9 > 1/p$, pelo Lema 3.5 temos que

$$|G : C_G(p)| \leq \frac{p-1}{p \cdot r(G,\theta) - 1} < \frac{p-1}{p \cdot \frac{2}{9} - 1} = \frac{9 \cdot (p-1)}{2p-9}.$$

Se $p = 5$, então

$$|G : C_G(P)| < \frac{9 \cdot (5-1)}{2 \cdot 5 - 9} = 36.$$

Se $p = 7$, então

$$|G : C_G(P)| < \frac{9 \cdot (7-1)}{2 \cdot 7 - 9} = \frac{54}{5} < 11.$$

Como P é abeliano e G não é p-nilpotente (pois assumimos que G é simples), segue pelo Teorema do complemento normal de Burnside 3.5 que $P \leq C_G(P) < N_G(P)$. Se $p = 7$, então $|G : N_G(P)| \geq 8$ e $|G : C_G(P)| \geq 16$, uma contradição. Portanto, $p = 5$. Logo, $\Pi(G) \in \{2,3,5\}$ e pela Proposição 3.1, G é isomorfo a um dos seguintes grupos: A_5. A_6 e $S_4(3)$. Por [15], no caso de $|P| = |C_G(P)| = 5$ e se G é isomorfo a A_6 ou $S_4(3)$, então

$|G : C_G(P)| > 36$, uma contradição. Assim, $G \cong A_5$.

Suponha que G é um grupo não-simples. Seja N um subgrupo normal minimal de G. Uma vez que G não contém subgrupos normais solúveis próprios, N é produto direto de grupos simples isomorfos. Pelo Lema 3.3, podemos escolher um automorfismo θ de G tal que

$$|N \cap S(\theta)| > \frac{2}{9}|N| > \frac{1}{5}|N|.$$

Como $N = N'$, então não possui subgrupo próprio de índice menor ou igual a 4, logo

$$N = \langle N \cap S(\theta) \rangle \quad e \quad N^\theta = N.$$

Seja X um dos fatores de N. Analogamente, e

$$|X \cap S(\theta)| > \frac{2}{9}|X| \quad e \quad X^\theta = X.$$

Então, pela primeira parte da prova segue que $X \cong A_5$. Como X é não-solúvel, pelo Lema 3.3 e Proposição 3.3 temos que

$$|X \cap S(y\theta)| = |Xy \cap S(\theta)| \leq \frac{4}{15}|X|, \quad \textit{para todo} \quad y \in N \cap S(\theta).$$

Assim, pelo Lema 3.4

$$r(N/X, \overline{\theta}) > \frac{15}{4} \cdot \frac{2}{9} = \frac{5}{6} > \frac{4}{15}.$$

Pela Proposição 3.3, N/X é solúvel. Assim, $N = X \cong A_5$. Como X é normal em G, segue analogamente que G/X é solúvel. Como X é simples, então $X \cap C_G(X) = 1$. Logo, $C_G(X)$ é subgrupo normal solúvel de G. Mas G não contém subgrupo normal solúvel próprio, então $C_G(X) = 1$. Assim,

$$G \cong H \leq Aut(A_5) \cong S_5.$$

O grupo S_5 não possui automorfismo interno que inverte mais que $(1/6)|S_5|$ elementos. Como $1/6 < 2/9$, então $X \leq G$ e $|G| < |S_5|$. Assim, $G = X \cong A_5$, uma contradição, pois supomos que G é não-simples. □

3.2.3 Critério

O critério que veremos agora deve-se a M. Herzog, P. Longobardi e M. Maj [3]. Em suma, utilizaremos os dois resultados principais das últimas duas subseções: o Teoremas 3.6 e 3.4. Para tanto, precisamos do conceito de grupo p-solúvel para prosseguir.

Primeiramente, considere um grupo G e uma série

$$\mathcal{S} : 1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G.$$

Dizemos que $\mathcal{S}$ é uma série de composição se cada fator G_{i+1}/G_i é um grupo simples, para $0 \leq i \leq n-1$.

Proposição 3.4. Todo grupo finito possui uma série de composição.

Demonstração. Seja G um grupo finito. Façamos por indução em $|G|$. Para $G = 1$, temos o resultado. Considere que para todo subgrupo H tal que $|H| < |G|$ o resultado vale. Se G é simples, então $1 \lhd G$ já é uma série de composição. Se G não é simples, podemos tomar um subgrupo normal M próprio de ordem máxima. Pelo Teorema da Correspondência 1.4, o quociente G/M é simples, pois o único subgrupo de G que contém M é o próprio G. Como $|M| < |G|$, a série

$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \ldots \trianglelefteq M_m = M$$

é uma série de composição. Como G/M é simples, concluímos que

$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \ldots \trianglelefteq M_m = M \trianglelefteq G$$

é uma série de composição para G. □

Agora, denote por $\mathbb{P}$ o conjunto de todos os primos. Seja $\pi \subseteq \mathbb{P}$. Defina $\pi' := \mathbb{P} \setminus \pi$. Se p é um primo, chamamos um grupo G de p'-grupo, se $|G|$ é coprima com p.

Definição 3.1. Seja G um grupo finito. Dizemos que G é um grupo p-solúvel se G possui uma série normal em que cada fator é p-grupo ou p'-grupo.

Uma observação direta é que todo grupo solúvel G é um grupo p-solúvel. Para verificar isto, basta tomar uma série de composição para G. Como G é solúvel, cada fator é abeliano e, como a série é de composição, cada fator é simples. Logo, todo fator da série de composição possui ordem prima, ou seja, cada fator é p-grupo ou p'-grupo.

Além disso, todo grupo 2-solúvel é também solúvel. Considere G um grupo 2-solúvel. Isto ocorre, pois todo fator possui ordem 2^n, para algum inteiro positivo n, ou possui ordem coprima com 2, isto é, ordem ímpar. Pelo Teorema de Feit-Thompson 1.7, cada um dos fatores é solúvel. Assim, G_1 e G/G_1 (a série é normal) são solúveis, logo G é solúvel.

Agora, seja

$$T(G) = \sum_{\chi \in Irr(G)} \chi(1)$$

em que $Irr(G)$ é o conjunto de caracteres irredutíveis (complexos) de G. Neste caso, $i_2(G) + 1 \leq T(G)$. Um estudo detalhado sobre este tema pode ser visto em [27] e [28].

Seja um primo $p \geq 7$. Defina

$$g_1(p) = \frac{p(p^2-1)}{p^2+p+2} \quad se \quad p \equiv 1 \pmod 4$$

$$g_1(p) = p - 1 \quad se \quad p \equiv 3 \pmod 4$$

$$g_2(p) = \frac{p(p-2)}{p-1}.$$

A demonstração do resultado abaixo pode ser visto em [26].

Proposição 3.5. Seja G um grupo finito. Se $p \geq 7$ e G é não-p-solúvel, então um dos casos abaixo ocorre:

$$T(G) = \frac{|G|}{g_1(p)}, \quad T(G) = \frac{|G|}{g_2(p)}, \quad T(G) \leq \frac{|G|}{p-1}$$

Proposição 3.6. Sejam G um grupo finito não-p-solúvel e p um primo. Se $p \geq 17$, então $i_2(G) < (1/15)|G|$.

Demonstração. Pela Proposição 3.5, temos que

$$i_2(G) < T(G) \leq \frac{1}{p-1}|G| < \frac{1}{p-2}|G|.$$

Para $p = 17$, segue que

$$i_2(G) < \frac{1}{17-2}|G| = \frac{1}{15}|G|.$$

□

Lema 3.7. Sejam G um grupo finito não-solúvel e p um primo tal que p divide $|G|$. Se $p \geq 17$ e $o(G) \leq o(A_5)$, então G é p-solúvel.

Demonstração. Seja G um grupo não-solúvel. Se $p \geq 17$ e G é não-p-solúvel, então, pela Proposição 3.6, $i_2(G) < (1/15)|G|$. Pelo Lema 2.3, $o(G) > o(A_5)$, uma contradição. □

Prosseguimos agora para o resultado principal deste capítulo. Este teorema fornece um critério de solubilidade para um grupo finito G.

Teorema 3.7. *(M. Herzog, P. Longobardi e M. Maj, Teorema B de [3])* Seja G um grupo finito e suponha que

$$o(G) < o(A_5) = \frac{211}{60}.$$

Então G é solúvel.

Demonstração. Suponha G um grupo não-solúvel finito que satisfaz duas condições: $o(G) \leq o(A_5)$ e G não é isomorfo ao grupo A_5. Suponha também que G possui a menor ordem possível que satisfaça tais condições. Primeiramente, mostraremos que G não é um grupo simples.

Suponha que G é um grupo simples. Seja p um primo que divide $|G|$. Se $p \geq 17$ e sendo G é um grupo não-solúvel que satisfaz $o(G) \leq o(A_5)$, então G é p-solúvel (Lema 3.7). Porém, G é um grupo simples, logo G não pode ser p-solúvel. Assim, $\Pi(G) \subseteq \{2, 3, 5, 7, 11, 13\}$ e pelo Teorema 3.4, $G \cong A_5$ ou $o(G) \geq 3,55 > o(A_5)$, uma contradição, pois estamos supondo que $o(G) \leq o(A_5)$. Portanto, G não é um grupo simples.

Assim existe $S \lhd G$ tal que $1 < |S| < |G|$. Pelo Lema 2.2, temos que $o(G/S) < o(G) \leq o(A_5)$, logo G/S não é isomorfo a A_5. Como $o(G/S) < o(A_5)$, pela minimalidade de G temos que G/S é solúvel. Então existem $N \lhd G$ e um primo p tal que $|G/N| = p$ e

$$o(G/N) < o(G) \leq o(A_5) = \frac{211}{60} = 3,51666... < 3,52.$$

Como G é não-solúvel, então N é não-solúvel.

Se $p > 3$, então $|G/N| = p$ e

$$o(G/N) = o(C_p) = \frac{p(p-1)+1}{p} = (p-1) + \frac{1}{p} > 4 > o(A_5),$$

uma contradição. Assim, $p = 2$ ou $p = 3$, então pelo Lema 2.4 temos que $o(G) \geq 3,66$, uma contradição, pois $o(G) < 3,52$. Logo, $p = 2$ e $G = N \dot{\cup} xN$, para algum $x \in G \setminus N$, com $|xN| = 2$ em G/N. Logo,

$$\psi(G) = \psi(N) + \psi(xN).$$

Por 2.2, $|xN| = 2$ divide $|xn|$, para cada $n \in N$.

Se $|xn| \geq 4$, para cada $n \in N$, então $\psi(xN) \geq 4|N|$ e $\psi(G) \geq \psi(N) + 4|N|$. Portanto,

$$o(G) = \frac{\psi(G)}{|G|} \geq \frac{\psi(N)}{|G|} + \frac{4 \cdot |N|}{|G|} = \frac{\psi(N)}{2 \cdot |N|} + \frac{4 \cdot |N|}{2 \cdot |N|} = \frac{1}{2} \cdot o(N) + 2.$$

Logo,

$$o(N) \leq 2 \cdot (o(G) - 2) < 2 \cdot (3,52 - 2) = 3,04,$$

uma contradição pelo Lema 2.3. Assim, existe $xn \in xN$ de ordem 2 e podemos assumir que $|x| = 2$. Defina

$$X := \{xn \ \mid \ n \in N, \ |xn| = 2\}$$

Temos que $(xn)^2 = 1$ se, e somente se, $xnx = n^{-1}$, isto é, $n^x = n^{-1}$. Dessa forma,

$$|X| = |\{n \in N \mid n^x = n^{-1}\}|.$$

Assim,

$$\psi(xN) \geq 2 \cdot |X| + 4 \cdot |xN \setminus X|.$$

Se N contém um subgrupo normal solúvel $K \neq 1$, isto é, $K \lhd N$, então $M = KK^x$ é um subgrupo normal solúvel próprio de G e

$$o(G/M) < o(G) \leq o(A_5).$$

Como G/M é não-solúvel, pela minimalidade de G, temos que $G/M \cong A_5$, uma contradição, pois $o(G/M) < o(A_5)$. Assim, N não contém subgrupo normal solúvel próprio e $N \cap C_G(N) = 1$. Além disso, se θ denota a conjugação de N por x, pelo Teorema 3.6, temos $N \cong A_5$ ou $|X| \leq (2/9)|N|$. Suponha $N \cong A_5$. Como $N \cap C_G(N) = 1$, se $C_G(N) \neq 1$, então $|C_G(N)| = 2$ e $G = N \times C_G(N)$. Assim,

$$o(N) = o(G/C_G(N)) < o(G) \leq o(A_5),$$

uma contradição, pois $N \cong A_5$. Logo, $C_G(N) = 1$ e

$$G = G/C_G(N) \leq Aut(A_5) = S_5.$$

Como $|G| = 2|N|$, então $G = S_5$. Porém

$$o(G) = o(S_5) = \frac{501}{120} = 4,175 > o(A_5),$$

uma contradição, pois $o(G) \leq o(A_5)$.

Suponha que $|X| \leq (2/9)|N|$. Então

$$|xN \setminus X| = |xN| - |X| \geq |xN| - \frac{2}{9}|N| = \frac{7}{9}|N|.$$

Logo,

$$\psi(G) = \psi(N) + \psi(xN) \geq \psi(N) + 2|X| + 4(|xN \setminus X|).$$

Observe que $2|X| + 4(|xN \setminus X|) = 2(|N| - |X|) + 2|N|$. Assim, temos

$$\begin{aligned} \psi(G) &\geq \psi(N) + 2|X| + 4(|xN \setminus X|) \\ &\geq \psi(N) + 2 \cdot \frac{7}{9}|N| + 2|N| \end{aligned}$$

Com isso,

$$\begin{aligned} o(G) = \frac{\psi(G)}{|G|} &\geq \frac{\psi(N) + (7/9) \cdot 2|N| + 2|N|}{|G|} \\ &> \frac{1}{2}o(N) + 1,777. \end{aligned}$$

$$o(N) < 2(o(G) - 1,777) < 2(3,52 - 1,777) = 2 \cdot 1,743 = 3,486 < o(A_5).$$

Como $N < G$ e $A_5 \neq N$, obtemos uma contradição pela minimalidade de $|G|$.

□

Considerações Finais

Ao longo do trabalho, notamos diversas técnicas de demonstração sobre o tema. No Capítulo 2 vimos propriedades gerais da função $o(G)$ e abordamos algumas questões, que, por sua vez, conectamos com o estudo de p-grupos. Vimos que a classe de p-grupos anti-Hughes aparece como candidata para construção de contraexemplos à Conjectura de Andrei Jaikin-Zapirain, diferente do caso dos p-grupos secretos de *Wall*, que de fato são utilizados para construir contraexemplos, conforme o Capítulo 3 nos apresentou.

Ainda no Capítulo 3, demonstramos um resultado importante que envolve a ordem média de grupos simples e o grupo A_5 e, também, demonstramos outro resultado importante que utiliza a função $r(G, \theta)$. Com isso, finalizamos o Capítulo 3 demonstrando o Critério de Solubilidade 3.7.

Agora, dedicamos esta parte da dissertação para apontar possíveis pesquisas futuras. Conforme foi visto no Capítulo 2, não existe um grupo finito G tal que $o(G)$ seja um inteiro positivo par ou igual a 3. Além disso, o Teorema 2.5 garantiu que todo inteiro positivo maior ou igual a 2 é ponto aderente de $Im(o)$.

Portanto, uma pergunta natural é se existe G em que $o(G)$ é um inteiro positivo ímpar? Em [31], os autores listaram alguns grupos cuja ordem média são números ímpares, com auxílio do [GAP]. No entanto, a ordem dos grupos investigados é até 5000.

Questão 3.4. Existem grupos de ordem maior que 5000 em que a ordem média é igual a um inteiro positivo ímpar? Se sim, qual a estrutura desses grupos?

Questão 3.5. Para quais grupos finitos G temos que $x \in G$ tal que $o(G) = |x|$?

Espera-se que este trabalho estimule novas respostas sobre o tema.

Bibliografia

[1] JAIKIN-ZAPIRAIN, Andrei. **On the number of conjugacy classes of finite nilpotent groups**. Advances in Mathematics, v. 227, n. 3, p. 1129-1143, 2011.

[2] KHUKHRO, E. I.; MORETÓ, Alexander; ZARRIN, Mohammad. **The average element order and the number of conjugacy classes of finite groups**. Journal of Algebra, v. 569, p. 1-11, 2021.

[3] HERZOG, Marcel; LONGOBARDI, Patrizia; MAJ, Mercede. **Another criterion for solvability of finite groups**. Journal of Algebra, v. 597, p. 1-23, 2022.

[4] BURNESS, Timothy C.; SCOTT, Stuart D. **On the number of prime order subgroups of finite groups**. Journal of the Australian Mathematical Society, v. 87, n. 3, p. 329-357, 2009.

[5] AMIRI, Habib; JAFARIAN AMIRI, S. M.; ISAACS, I. M. **Sums of element orders in finite groups**. Communications in Algebra®, v. 37, n. 9, p. 2978-2980, 2009.

[6] HUGHES, D. R. **A research problem in group theory**. Bull. Amer. Math. Soc, v. 63, p. 209, 1957.

[7] THOMPSON, J. G; HUGHES, D. H. **The H_p-problem and the structure of H_p-groups**. Pacif. J. of Math, v. 9, p. 1097-1101, 1959.

[8] HUGHES, D.R. **Partial difference sets**, Am. J. Math. 78 (1956) 650–677.

[9] STRAUS, E. G.; SZEKERES, G. **On a problem of D. R. Hughes**. In: Proc. Amer. Math. Soc. 1958. p. 157-158.

[10] *Wall*, G. E. **On the multilinear identities which hold in the Lie ring of a group of prime-power exponent**, J. Algebra 104 (1986) 1–22.

[11] KHUKHRO, E. I. **On a connexion between the Hughes conjecture and related questions in fmite groups of prime exponent**, Maf. Sb. (N. S.) 116 (158) (1981) 253-264.

[12] DIXON, J. D. et al. **Analytic pro-p groups**. Cambridge University Press, 2003.

[13] *Wall*, G. E. **Secretive prime-power groups of large rank**, Bull. Aust. Math. Soc. 12 (1975) 363–369.

[14] KOVACS, L. G.; NEUBUSER, J.; NEUMANN, B.H. **On finite groups with hidden primes**, J. Austral. Math. Soo. 12 (1971), 287-300.

[15] CONVEY, J. H.; CURTIS, R. T.; NORTON, S.P.; PARKER, R.A., WILSON, R.A. **ATLAS of Finite Groups, Maximal Subgroups and Ordinary Characters for Simple Groups**, Clarendon Press, Oxford, 2003, ISSN 978- 0-19-853299-9.

[16] HERZOG, M. **On finite simple groups of order divisible by three primes only**, J. Algebra 10 (1968) 383–388.

[17] BUGEAUD, Y.; CAO, Z.; MIGNOTTE, M. **On simple K_4-groups**, J. Algebra 241 (2) (2001) 58–668.

[18] JAFARZADEH, A.; IRANMANESH, A. **On simple K_n-groups for $n = 5, 6$** in: Group St. Andrews 2005, Vol. 2, in: London Mathematical Society Lecture Note Series, vol. 340, Cambridge University Press, 2007, pp. 517–526.

[19] YU, D.; LI, J.; CHEN, G.; ZHANG, L.; SHI, W. **A new characterization of simple K_5-groups of type $L_3(p)$**, Bull. Iran. Math. Soc. 45 (2019) 771–781.

[20] POTTER, Walter M. **Nonsolvable groups with an automorphism inverting many elements**. Archiv der Mathematik, v. 50, p. 292-299, 1988.

[21] GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de álgebra. Instituto de Matemática Pura e Aplicada**, 2006.

[22] ROBINSON, Derek J. S. **A Course in the Theory of Groups**. Springer Science Business Media, 2012.

[23] ROTMAN, Joseph J. **An introduction to the theory of groups**. Springer Science Business Media, 2012.

[24] LEE, John. **Introduction to topological manifolds**. Springer Science Business Media, 2010.

[25] GORENSTEIN, Daniel. **Finite groups**. American Mathematical Soc., 2007.

[26] Hongfei Pan; Xianhua Li. **On the character degree sums**, Comm. Algebra 45 (3) (2017), 1211-1217.

[27] ISAACS, I.M. **Character Theory of Finite Groups**, Academic Press, New York, San Francisco, London, 1976.

[28] MANN, A. **Finite Groups Containing Many Involutions**, Proc. Amer. Math. Soc. 122 (2) (1994), 383-385.

[29] FEIT, W., THOMPSON J. G. **Solvability of groups of odd order**, Pacific J. Math. 13 (1963), 773–1029.

[30] TĂRNĂUCEANU, Marius. **An arithmetic method of counting the subgroups of a finite abelian group**. Bulletin mathématique de la Société des Sciences Mathématiques de Roumanie, p. 373-386, 2010.

[31] LAZOREC, Mihai-Silviu; TĂRNĂUCEANU, Marius. **On the average order of a finite group**. Journal of Pure and Applied Algebra, v. 227, n. 4, p. 107276, 2023.

[32] HERZOG, Marcel; LONGOBARDI, Patrizia; MAJ, Mercede. **An exact upper bound for sums of element orders in non-cyclic finite groups**. Journal of Pure and Applied Algebra, v. 222, n. 7, p. 1628-1642, 2018.

[33] AMIRI, H.; JAFARIAN AMIRI, S. M. **Sum of element orders on finite groups of the same order**. Journal of Algebra and its Applications, v. 10, n. 02, p. 187-190, 2011.

[34] HERZOG, Marcel; LONGOBARDI, Patrizia; MAJ, Mercede. **Two new criteria for solvability of finite groups**. Journal of Algebra, v. 511, p. 215-226, 2018.

[GAP] The GAP Group, GAP–Groups, Algorithms, and Programming

Apêndice A
(GAP - Groups, Algorithms and Programming)

O [GAP] (Groups, Algorithms and Programming) é um sistema computacional algébrico, que possui como intuito auxiliar a investigação sobre temas relacionados à teoria de grupos e outras estruturas algébricas.

No Exemplo 2.5, comentamos sobre o grupo $G = A \rtimes Q_8$. A biblioteca do GAP cataloga o grupo G como $SmallGroup([72, 41])$, isto significa que $|G| = 72$ e a numeração de G nesta biblioteca é 41. Na ocasião, dizemos que todo elemento de $k_2(G)$ possui ordem 4. Abaixo, comentamos as funções do GAP utilizadas para verificar este fato. Agradecemos ao Professor Martino Garonzi pelo auxílio.

- **StructureDescription(G):** Retorna a descrição da estrutura do grupo G conforme a biblioteca do GAP.
- **MinimalGeneratingSet(G):** Retorna um conjunto gerador de menor cardinalidade.
- **Elements(G):** Retorna todos os elementos de G.
- **Combinations(Elements(G),2):** Retorna todos os pares possíveis formados por elementos de G.
- **A:=(Filtered(Combinations(Elements(G),2),x $\rightarrow$ Group(x[1],x[2])=G)):** Retorna a lista de todos os pares de elementos de G, em que cada par gera G.
- **Flat(A):** Retorna a mesma lista anterior sem os colchetes, isto é, lista todos os elementos da lista anterior sem distinção de pares, incluindo repetições. Um exemplo numérico: seja a lista t:=list([[1,2,3][4,1]]), assim Flat(t) retorna $[1, 2, 3, 4, 1]$.
- **B:=Set(Flat(A)):** Retorna a lista Flat(A), mas sem repetições.

- **C:= List(B,Order):** Retorna uma lista composta da ordem de cada elemento da lista B.
- **Collected(C):** Retorna uma nova lista composta com elementos da forma $[x, y]$, em que x é o elemento presente na lista B e y é o número de vezes que aparece na lista. No nosso caso, esta lista é composta unicamente por $[[4, 54]]$. Isto significa que a lista C possui 54 elementos e todos eles possuem ordem 4.

Ao utilizar estes comandos do GAP, constatamos que $|k_2(G)| = 54$. Além disso, para todo $x \in k_2(G)$, temos que $|x| = 4$.