Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Sobre a soma das ordens de elementos de um grupo finito

Autor: Adler Vieira Marques [1]

Orientador: Igor dos Santos Lima

Brasília

[1]O autor foi bolsista CNPq e CAPES durante a elaboração deste trabalho.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Sobre a soma das ordens de elementos de um grupo finito

por

Adler Vieira Marques*

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

MESTRE EM MATEMÁTICA

Brasília, 27 de julho de 2020.

Comissão Examinadora:

Igor dos Santos Lima

Prof. Dr. Igor dos Santos Lima - MAT/UnB (Orientador)

Martino Garonzi

Prof. Dr. Martino Garonzi – MAT/UnB (Membro)

Prof. Dr. Mohsen Amiri – UFAM (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Ms

Marques, Adler Vieira
Sobre a soma das ordens de elementos de um grupo finito / Adler Vieira Marques; orientador Igor dos Santos Lima. -- Brasília, 2020.
88 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2020.

1. teoria de grupos. 2. grupos . 3. algébra. 4. grupos finitos. 5. classificação de grupos. I. Lima, Igor dos Santos, orient. II. Título.

Agradecimentos

Agradeço, primeiramente, a toda minha família pela confiança e pelo incentivo que foram fundamentais para mim.

À Thais Cristina fica aqui os meus mais sinceros agradecimentos; por todo o apoio e companhia durante boa parte da graduação e todo mestrado, por estar sempre presente e me ajudar em muitos momentos difíceis.

Aos meus amigos da UnB por todas as conversas e cafés no departamento, principalmente aos amigos da Sala Top, fica aqui os meus agradecimentos.

Agradeço bastante ao meu orientador, Igor dos Santos Lima, pela confiança no trabalho, pelo suporte, pelos incentivos nesta vida acadêmica e por todas as correções na dissertações.

Agradeço a todos os professores do MAT-UnB que contribuíram bastante para a minha formação. Em especial, à professora Aline Pinto e aos professores Martino Garonzi, Theo Zapata e Salahoddin Shokranian.

Agradeço aos professores Mohsen Amiri e Martino Garonzi pela disponibilidade para participar da banca.

Agradeço também a todos os funcionários do MAT, principalmente a Cláudia Messias por sempre ser receptiva na portaria do departamento.

Por último, agradeço ao CNPq e a CAPES pelo apoio financeiro ao longo do mestrado.

Eu quero ser maior que essas muralhas
que eles construíram ao meu redor.
BK' - Titãs.

Resumo

Seja G um grupo finito. Denote por $\psi(G)$ a soma das ordens de todos os elementos de G. A função ψ foi considerada inicialmente por H. Amiri, S.M. Jafarian Amiri e I.M. Isaacs, em **[AAI09]**, onde foi mostrado que o valor máximo de ψ, sobre os grupos de mesma ordem n, ocorre no grupo cíclico C_n. Em **[HLM18a]**, M. Herzog, P. Longobardi e M. Maj deram uma cota superior exata para $\psi(G)$ sobre os grupos não-cíclicos de mesma ordem. Em **[AA11]** e **[AmiJ13]**, H. Amiri e S.M. Jafarian Amiri estudaram problema de encontrar o valor mínimo para $\psi(G)$ sobre todos os grupos de mesma ordem. Um dos objetivos deste trabalho é discorrer sobre estes resultados e problemas similares. Além disso, dado um inteiro positivo k, defina $\psi_k(G)$ como sendo a soma das k-ésimas potências das ordens de todos elementos de G. Mostraremos algumas propriedades básicas sobre $\psi_k(G)$ e que, para G não-cíclico, $\psi_k(G)$ é limitado superiormente por $\frac{1}{(q-1)^k}\psi_k(C_n)$ onde q é o menor divisor primo de $n = |G|$.

Abstract

Let G be a finite group. Denote by $\psi(G)$ the sum of all element orders of G. The function ψ was introduced by H. Amiri, S.M. Jafarian Amiri and I.M. Isaacs, in **[AAI09]**, where the authors showed that the maximum value of ψ, on the set of groups of the same order n, will occur at the cyclic group C_n. In **[HLM18a]**, M. Herzog, P. Longobardi e M. Maj gave an exact upper bound for $\psi(G)$ on the groups of the same order. In **[AA11]** and **[AmiJ13]**, H. Amiri e S.M. Jafarian Amiri studied the problem of finding the minimum value for $\psi(G)$. One of the objectives of this text is to discuss these results and similar problems. Finally, given a positive integer k, let $\psi_k(G)$ denote the sum of the k-th powers of all element orders of G. We will show some basic properties about ψ_k and that, for G non-cyclic, $\psi_k(G)$ is upper bounded by $\frac{1}{(q-1)^k}\psi_k(C_n)$ where q is the smallest prime divisor of $n = |G|$.

Sumário

Introdução **8**

1 Preliminares **12**

1.1 Ações de Grupos 12

1.2 Grupos Solúveis 16

1.3 Grupos Nilpotentes 19

1.4 O Teorema de Schur-Zassenhaus 24

2 A função ψ **31**

2.1 Conceitos iniciais 31

2.2 Uma cota superior exata para $\psi(G)$ 38

2.3 Cota inferior para $\psi(G)$ 51

2.4 Alguns resultados sobre solubilidade 57

3 Uma generalização da função ψ **71**

3.1 A função ψ_k 71

4 Considerações Finais **83**

Bibliografia **87**

Introdução

Seja G um grupo *periódico*, isto é, um grupo cujo todos os elementos de G possuem ordem finita. Um problema em Teoria dos Grupos é obter informações da estrutura de G através de $\omega(G) = \{o(x) \mid x \in G\}$, onde $o(x)$ denota a ordem de x. Por exemplo, $\omega(G) = \{1, 2\}$ se, e somente se, G é um 2-grupo abeliano elementar. Um problema muito conhecido nessa direção é o Problema Restrito de Burnside: se $\omega(G)$ é finito, então G é localmente finito (i.e., todo subgrupo finitamente gerado de G é finito)? P.S. Novikov e S.I. Adjan, em [NA68], deram uma resposta negativa para tal problema.

Restringindo para o caso de G ser um grupo finito, podemos considerar a soma das ordens dos elementos de G, denotada por $\psi(G)$. A função ψ foi introduzida em 2009 por H. Amiri, S.M. Jafarian Amiri e I.M. Isaacs no artigo "Sums of Element Orders in Finite Groups", [AAI09].

Problema. *O que podemos dizer sobre a estrutura de G através de $\psi(G)$?*

No artigo [AAI09], os autores mostraram o seguinte resultado que é a base do estudo da função ψ.

Teorema 1. *Seja C_n um grupo cíclico de ordem n. Então para todos grupos não-cíclicos G de ordem n, temos que*

$$\psi(G) < \psi(C_n).$$

Assim segue que para cada inteiro positivo n, o grupo cíclico C_n de ordem n é unicamente determinado, a menos de isomorfismo, pela sua ordem e soma das ordens de seus elementos. Em geral, os invariantes $|G|$ e $\psi(G)$ não determinam o grupo G, isto é, existem grupos G e H tais que $|G| = |H|$ e $\psi(G) = \psi(H)$, mas $G \ncong H$ (veja Exemplo 2.1.2).

Pelo Teorema 1, temos que o grupo cíclico de ordem n tem o valor maximal de $\psi(G)$ sobre todos os grupos de ordem n. Uma pergunta natural que surge disso é: qual é uma cota superior para $\psi(G)$ sobre todos os grupos não-cíclicos de mesma ordem? Respondendo essa questão, M. Herzog, P. Longobardi e M. Maj, em 2018, mostraram no artigo "An exact upper bound for sums of element orders in non-cyclic finite groups", **[HLM18a]**, o seguinte resultado:

Teorema A. *Seja G um grupo não-cíclico de ordem n. Então*

$$\psi(G) \leq \frac{7}{11}\psi(C_n).$$

Podemos observar que tal cota é a melhor possível. Por exemplo, temos que $\psi(C_2 \times C_2) = 7$ e $\psi(C_4) = 11$ e, portanto, $\psi(C_2 \times C_2) = \frac{7}{11} \cdot 11 = \frac{7}{11}\psi(C_4)$. No mesmo artigo, os autores também mostraram o seguinte teorema.

Teorema B. *Sejam G um grupo não-cíclico de ordem n e q o menor divisor primo de n. Então*

$$\psi(G) < \frac{1}{q-1}\psi(C_n).$$

Seja G um grupo não-cíclico de ordem n. Se n é par, o Teorema B nos diz que $\psi(G) < \psi(C_n)$ como no Teorema 1. Por outro lado se n é ímpar, então o Teorema B nos diz que $\psi(G) < \frac{1}{2}\psi(C_n)$.

Além disso, ao estudar o caso em que $\psi(G) \geq \frac{1}{q}\psi(C_n)$, M. Herzog, P. Longobardi e M. Maj também obtiveram condições suficientes, baseadas em $\psi(G)$, para solubilidade de grupos finitos.

Teorema 2. *Seja G um grupo finito de ordem n e sejam q e p o menor e o maior divisores primos de n, respectivamente. Se $\psi(G) \geq \frac{1}{2(q-1)}\psi(C_n)$, então G é solúvel e ou seus p-subgrupos de Sylow ou os seus q-subgrupos de Sylow são cíclicos.*

Outra condição suficiente para solubilidade dada em **[HLM18a]** é o seguinte teorema.

Teorema 3. *Seja G um grupo finito de ordem n. Se $\psi(G) \geq \frac{3}{5}n\varphi(n)$, então G é solúvel e $G'' \leq Z(G)$, onde φ denota a função de Euler.*

Os Teoremas A e B acima nos dão cotas superiores para $\psi(G)$. Alguns autores estudaram o problema de encontrar um valor mínimo para $\psi(G)$ sobre os grupos de mesma ordem. Em 2011, no artigo "Sum of element orders on finite groups of the same order", [AA11], H. Amiri, S.M. Jafarian Amiri mostraram que, sobre os grupos nilpotentes de ordem n, $\psi(G)$ assume valor mínimo para G cujo todos os p-subgrupos de Sylow possuem expoente p. Além disso, eles mostraram o seguinte resultado:

Teorema 4. *Seja n um inteiro positivo tal que existe um grupo não-nilpotente de ordem n. Então existe um grupo não-nilpotente K de ordem n tal que $\psi(K) < \psi(H)$ para todo grupo nilpotente de ordem H.*

Em outras palavras, o Teorema 4 diz que, quando existe grupo não-nilpotente de ordem n, então $\psi(G)$ assume valor mínimo sobre um grupo não-nilpotente.

Por fim, neste trabalho apresentamos uma generalização da função ψ, denotada por ψ_k, onde $\psi_k(G)$ é definido como sendo a soma das k-ésimas potências das ordens dos elementos de G, e obtemos alguns resultados relacionados. A função ψ_k foi considerada inicialmente por S.M. Jafarian Amiri e M. Amiri, em [AA14b], onde ela é denotada por ψ^k, onde os autores mostram que alguns resultados de ψ se estendem naturalmente para ψ_k. Além disso, de modo mais geral, temos que a função ψ_k aparece como caso particular da função $R_G(r,s)$ considerada por M. Garonzi e M. Patassini em [GP17]. A função ψ_k tem propriedades semelhantes a ψ. Por exemplo, podemos generalizar o Teorema 1 para ψ_k, ou seja, $\psi_k(G) < \psi_k(C_n)$ sempre que G é não-cíclico de ordem n. Além disso, vale que $\psi_k(G \times H) = \psi_k(G)\psi_k(H)$ sempre que $mdc(|G|, |H|) = 1$. O objetivo final deste trabalho é discorrer como alguns resultados se estendem para ψ_k e apresentar uma generalização inédita para o Teorema B da seguinte maneira:

Teorema 5. *Seja G um grupo não-cíclico de ordem n e seja q o menor divisor primo de n. Então*

$$\psi_k(G) < \frac{1}{(q-1)^k}\psi_k(C_n).$$

Este trabalho está organizado de maneira que seja o mais autocontido possível. Alguns resultados cujas demonstrações saem muito do nosso objetivo são apenas enunciados com as suas respectivas referências.

No Capítulo 1 temos as ferramentas básicas de Teoria de Grupos que serão necessárias no decorrer do trabalho. Veremos as definições e propriedades de ação de grupos, grupos solúveis, grupos nilpotentes e, por fim, o Teorema de Schur-Zassenhaus. As principais referências para este capítulo são **[Ser16]** e, para a demonstração do Teorema de Schur-Zassenhaus, **[Isa08]**.

O Capítulo 2 discute as noções da função ψ, suas propriedades básicas, os seus teoremas principais sobre o valor máximo e mínimo para $\psi(G)$ e resultados adicionais comentados anteriormente. Neste capítulo, seguiremos principalmente os artigos **[AAI09]**, **[HLM18a]** e **[AA11]**. O leitor interessado em outros trabalhos (recentes) sobre soma de ordens de elementos pode consultar **[AK18]**, **[AK19]**, **[HLM19]** e **[Tar19]**.

No Capítulo 3 será introduzido a função ψ_k e veremos alguns resultados apresentados em **[AA14b]**, no geral, sem seguir a mesma abordagem. Por fim, finalizaremos o capítulo provando o Teorema 5.

No último capítulo temos as conclusões finais do trabalho juntamente a muitos resultados adicionais que são, de certa forma, continuação dos temas tratados aqui e podem servir como motivação para trabalhos futuros para os leitores.

Capítulo 1

Preliminares

Neste capítulo inicial, apresentam-se algumas definições e resultados preliminares que serão úteis ao longo do texto. Alguns teoremas bem conhecidos como Teoremas dos Isomorfismos e o da Correspondência serão assumidos. As principais referências utilizadas neste capítulo são os livros: *Finite Groups: An introduction*, J-P. Serre, [Ser16], e *Finite Group Theory*, I. M. Isaacs, [Isa08].

1.1 Ações de Grupos

Seja G um grupo qualquer.

Definição 1.1.1. *Uma* ***ação*** *de grupo à esquerda de G sobre um conjunto X não-vazio é uma função*

$$G \times X \longrightarrow X$$
$$(g, x) \longmapsto gx$$

que satisfaz as seguintes condições:

1. $g(hx) = (gh)x$ *para todo* $x \in X$ *e quaisquer* $g, h \in G$;
2. $1x = x$, *para todo* $x \in X$ *onde* 1 *é o elemento identidade de* G.

Equivalentemente, podemos definir uma ação de grupo de G sobre X como um homomorfismo $\phi : G \longrightarrow Sym(X)$, a saber $\phi(g)(x) = gx$ para todo $g \in G$ e $x \in X$, onde $Sym(X)$ é o grupo de simetrias de X.

Observação 1.1.1. *Uma ação de grupo à direita $X \times G \longrightarrow X$, $(x, g) \mapsto xg$, é definida de maneira similar. Note que toda ação à direita pode ser substituída por uma ação à esquerda via $gx = xg^{-1}$.*

Sejam G um grupo e X um conjunto. A ação $G \times X \to X$ dada por $(g, x) \mapsto x$ é dita ação **trivial** de G sobre X. Neste caso dizemos que G age **trivialmente** sobre X.

Definição 1.1.2. *Suponha que G age sobre X. Dizemos que ação de G sobre X é **livre** (ou **livre de ponto fixo**) se dados $g, h \in G$, existe $x \in X$ tal que $gx = hx$, então $g = h$. Equivalentemente, se $gx = x$ para algum $x \in X$, então $g = 1$.*

Por exemplo, G age livremente sobre si mesmo via multiplicação.

Se temos uma ação de G sobre X, então G particiona X em **órbitas**, da seguinte maneira: dois elementos x e y de X estão na mesma órbita se, e somente se, existe $g \in G$ tal que $gx = y$. O quociente de X por G é o conjunto das órbitas. Assim, por definição, a órbita contendo x_0 é $Gx_0 = \{gx_0 \mid g \in G\}$.

Definição 1.1.3. *Se G age sobre X, então o **estabilizador** de x em G é definido por*

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

Agora, seja G um grupo finito. Suponha que X é finito e que G age sobre X. Assim, temos que $X = \dot{\bigcup}_{i \in I} Gx_i$ é uma união disjunta de suas órbitas Gx_i, onde x_i é um representante de cada órbita. Como temos uma bijeção $G/G_{x_i} \to Gx_i$, dada por $gG_{x_i} \mapsto gx_i$, segue que $|Gx_i| = |G : G_{x_i}| = |G| \cdot |G_{x_i}|^{-1}$. Portanto,

$$|X| = \sum_{i \in I} |G : G_{x_i}| = |G| \sum_{i \in I} \frac{1}{|G_{x_i}|}.$$

A equação acima é conhecida como **equação das órbitas**.

Um caso especial de ação de grupo é a ação via **conjugação** sobre G. Neste caso, dado um grupo G, consideremos $X = G$ (como conjunto) a ação é dada por

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto gxg^{-1}. \end{aligned}$$

As órbitas desta ação são chamadas de **classes de conjugação** de G. Os elementos da forma gxg^{-1} são chamados de **conjugados** de x, com $g \in G$. O estabilizador de um elemento $x \in G$ é o conjunto dos elementos g em G que comutam com x, o chamado **centralizador** de x, denotado por $C_G(x)$. Ou seja, $C_G(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}$.

Outro caso especial de ação é quando G age sobre os seus subgrupos por conjugação. Inicialmente, dado um subgrupo H de G e um elemento $g \in G$, temos que $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ é um subgrupo de G. Considerando $X := \{H \mid H \leq G\}$, temos que

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, H) &\longmapsto gHg^{-1} \end{aligned}$$

é uma ação de G sobre X. A órbita de tal ação contendo um subgrupo H é o conjunto dos conjugados de H, i.e., o conjunto $\{gHg^{-1} \mid g \in G\}$. O estabilizador de um subgrupo H é o conjunto $N_G(H) := \{g \in G \mid gHg^{-1} = H\}$, o chamado **normalizador** de H em G.

Definição 1.1.4. *O **centralizador** de um subgrupo H de G é definido como $C_G(H) = \{g \in G \mid gh = hg$ para todo $h \in H\}$.*

Observe que dado $g \in C_G(H)$, temos que $ghg^{-1} = h$ para todo $h \in H$ e, portanto, $gHg^{-1} = H$. Assim, $C_G(H) \leq N_G(H)$. Além disso, dados $x \in N_G(H)$ e $g \in C_G(H)$, temos $(x^{-1}gx)h(x^{-1}gx)^{-1} = x^{-1}g(xhx^{-1})g^{-1}x = x^{-1}(xhx^{-1})gg^{-1}x = h$ para cada $h \in H$. Logo $C_G(H)$ é normal em $N_G(H)$. Por fim, temos o seguinte resultado sobre o quociente $N_G(H)/C_G(H)$:

Teorema 1.1.1. *Sejam G um grupo e H um subgrupo de G. Então $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de $Aut(H)$, o grupo de automorfismos de H.*

Demonstração. Inicialmente note que, dado $g \in N_G(H)$ qualquer, $i_g(h) := ghg^{-1} \in H$. Assim, $i_g : H \to H$ dado por $i_g(h) = ghg^{-1}$ define uma aplicação de H em H a qual é um automorfismo. De fato, $i_g(h_1h_2) = g(h_1h_2)g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = i_g(h_1)i_g(h_2)$ para todos $h_1, h_2 \in H$. Agora podemos considerar a aplicação

$$\begin{aligned} \Phi : N_G(H) &\to Aut(H) \\ g &\mapsto i_g : H \to H, \end{aligned}$$

a qual é um homomorfismo, pois

$$\begin{aligned} \Phi(g_1g_2)(h) = i_{(g_1g_2)}(h) = (g_1g_2)h(g_1g_2)^{-1} &= g_1(g_2hg_2^{-1})g_1^{-1} \\ &= i_{g_1}(i_{g_2}(h)) = \Phi(g_1)(\Phi(g_2)(h)) \end{aligned}$$

para qualquer $h \in H$ e quaisquer $g_1, g_2 \in N_G(H)$. Veja também que

$$\begin{aligned} ker(\Phi) &= \{g \in N_G(H) \mid i_g(h) = h \text{ para todo } h \in H\} \\ &= \{g \in N_G(H) \mid ghg^{-1} = h \text{ para todo } h \in H\}, \end{aligned}$$

ou seja, $ker(\Phi) = C_G(H)$. Portanto, pelo Teorema do Isomorfismo, $N_G(H)/C_G(H)$ é isomorfo a $Im(\Phi) \leq Aut(H)$. □

Por fim enunciaremos os famosos Teoremas de Sylow que tem um papel muito importante na teoria de grupos finitos. As suas demonstrações podem ser vistas em **[Ser16]**, Capítulo 2.

Definição 1.1.5. *Sejam G um grupo finito e p um número primo. Dizemos que G é um **p-grupo** se a sua ordem $|G|$ é uma potência de p.*

Definição 1.1.6. *Seja G um grupo de ordem n. Se p^m é a maior potência de p que divide n, então um subgrupo de G de ordem p^m é dito um **p-subgrupo de Sylow** de G.*

Teorema 1.1.2 (Teoremas de Sylow)**.** *Seja G um grupo finito.*

1. *(Primeiro Teorema de Sylow) O grupo G possui um p-subgrupo de Sylow.*

2. *(Segundo Teorema de Sylow)*

   i) Todo p-subgrupo de G está contido em p-subgrupo de Sylow de G.

   ii) Os p-subgrupos de Sylow de G são conjugados entre si.

   iii) O número de p-subgrupos de Sylow de G, denotado por n_p, é congruente a 1 módulo p, i.e., $n_p \equiv 1 \pmod{p}$. Mais ainda, temos que $n_p = |G : N_G(P)|$ para qualquer p-subgrupo de Sylow P de G.

1.2 Grupos Solúveis

Seja G um grupo. Dados $x, y \in G$ definimos o comutador de x e y como sendo o elemento $[x, y] := x^{-1}y^{-1}xy$. Note que os elementos x e y comutam se, e somente se, $[x, y] = 1$.

Temos as seguintes propriedades básicas que seguem diretamente da definição de comutador:

Proposição 1.2.1. *Seja G um grupo. Então:*

i) $[x, yz] = [x, z] \cdot [x, y]^z = [x, z] \cdot [z, [y, x]] \cdot [x, y]$ *para quaisquer* $x, y, z \in G$.

ii) $[x, yz] \cdot [z, xy] \cdot [y, zx] = 1$.

iii) $[x^y, [y, z]] \cdot [y^z, [z, x]] \cdot [z^x, [x, y]] = 1$.

Definição 1.2.1. *Seja G um grupo e sejam H e K subgrupos de G. Definimos $[H, K]$ como sendo o grupo gerado pelos comutadores $[x, y]$ com $x \in H$ e $y \in K$. Definimos também o* ***subgrupo derivado*** *de G como sendo $D(G) := [G, G]$. Frequentemente, $D(G)$ é denotado por G'.*

Observe que $D(G) = 1$ se, e somente se, G é abeliano.

O seguinte teorema nos fornece uma condição suficiente para a solubilidade de um grupo em relação aos subgrupos normais.

Proposição 1.2.2 (Teorema 2.1 (vi), [Gor80])**.** *Seja H um subgrupo de G. Então as seguintes afirmações são equivalentes:*

i) H contém G'.

ii) H é normal e G/H é abeliano.

Motivado pela definição de $D(G)$ podemos definir indutivamente uma sequência $(D^n(G))_{n\geq 0}$ de subgrupos de G, como a seguir:

Definição 1.2.2. *Seja G um grupo. Definimos*

$$D^0(G) = G, \quad D^1(G) = D(G) \quad e \quad D^{n+1}(G) = [D^n(G), D^n(G)] \quad \text{para todo } n \geq 1.$$

*Além disso, dizemos que G é um grupo **solúvel** se existe $n \geq 0$ tal que $D^n(G) = 1$. O menor inteiro n tal que $D^n(G) = 1$ é chamado de **comprimento derivado** de G (ou **classe de solubilidade** de G), e é denotado por $dl(G)$.*

Note que $dl(G) = 0$ se, e somente se, $G = 1$. Ainda $dl(G) \leq 1$ é equivalente a G abeliano.

Teorema 1.2.1. *Seja G um grupo.*

i) Se G é solúvel, então subgrupos e quocientes de G são solúveis.

ii) Seja N um subgrupo normal de G. Se N e G/N são solúveis, então G é solúvel.

Demonstração. *i)* Note que se H é um subgrupo de G, então $D^i(H) \subseteq D^i(G)$ para todo $i \geq 0$. Assim, se $D^n(G) = 1$, então $D^n(H) = 1$ e logo H é solúvel. De forma análoga, por indução, temos que se N é normal em G, então $D^i(G/N) = D^i(G)N/N$. Logo, $D^n(G) = 1$ implica que $D^n(G/N) = D^n(G)N/N = N/N$, e portanto G/N é solúvel.

ii) Note que se $D^m(G/N) = N$, então $D(G)^m N/N = N$ e portanto $D^m(G) \subseteq N$. Por outro lado, se $D^n(N) = 1$, então $D^{m+n}(G) = D^n(D^m(G)) \subseteq D^n(N) = 1$, e portanto G é solúvel.

□

Definição 1.2.3. *Seja G um grupo. Um subgrupo H de G é dito **característico** se, para todo automorfismo ϕ de G, temos que $\phi(H) \subseteq H$. Em particular, um subgrupo*

característico H de G é normal, pois, dado $g \in G$ fixado, $\phi(x) = gxg^{-1}$ define um automorfismo de G, e portanto $gHg^{-1} = \phi(H) \subseteq H$.

Veremos agora temos algumas equivalências de solubilidade.

Teorema 1.2.2. *Sejam G um grupo e $n \geq 1$ um inteiro. Então as seguintes propriedades são equivalentes:*

i) G é solúvel com $dl(G) \leq n$.

ii) Existe uma sequência $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ de subgrupos característicos de G tais que cada fator G_i/G_{i+1} é abeliano para todo $0 \leq i \leq n-1$.

iii) Existe uma sequência $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ de subgrupos de G tal que G_i é normal em G_{i-1} e G_{i-1}/G_i é abeliano para todo $1 \leq i \leq n$.

iv) Existe um subgrupo abeliano característico A de G tal que G/A é solúvel com $dl(G/A) \leq n-1$.

Demonstração. i) $\implies$ ii): Suponha que G é solúvel com $dl(G) \leq n$. Agora, defina $G_i := D^i(G)$. Observe que, dado um homomorfismo ϕ de G em um grupo H,

$$\phi([x,y]) = \phi(x^{-1}y^{-1}xy) = \phi(x)^{-1}\phi(y^{-1})\phi(x)\phi(y) = [\phi(x), \phi(y)],$$

para quaisquer $x, y \in G$. Em particular, para qualquer automorfismo $\phi \in Aut(G)$, temos que $\phi(D(G)) \subseteq D(G)$ e, portanto , $\phi(D^i(G)) \subseteq D^i(G)$ para todo $i \geq 1$. Assim, temos que cada $G_i = D^i(G)$ é característico em G. Além disso, pela Proposição 1.2.2, segue que cada $G_i/G_{i+1} = D^i(G)/D^{i+1}(G)$ é abeliano.

ii) $\implies$ iii): Basta considerar a mesma sequência $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$ e o resultado segue imediatamente.

iii) $\implies$ i): Mostremos, por indução sobre k, que $D^k(G) \subseteq G_k$ para $k \geq 0$. Para $k = 0$, o resultado é trivial. Suponha, por hipótese de indução, que $D^k(G) \subseteq G_k$ para $k \geq 0$. Como G_{k+1} é normal em G_k e G_k/G_{k+1} pela Proposição 1.2.2, segue que $D(G_k) \subseteq G_{k+1}$. Logo,

$$D^{k+1}(G) = D(D^k(G)) \subseteq D(G^k) \subseteq G_{k+1}.$$

Portanto, por indução, temos o desejado. Por fim, segue que $D^n(G) \subseteq G_n = 1$, ou seja, $D^n(G) = 1$. Sendo assim, G é solúvel e $dl(G) \leq n$.

$i) \implies iv)$: Observe que basta tomar $A := D^{n-1}(G)$ e o resultado segue imediatamente do Teorema 1.2.1.

$iv) \implies i)$: Como A é característico, segue que A é normal em G. Sendo A abeliano, A é solúvel. Por fim, pelo Teorema 1.2.1, como A e G/A são solúveis, segue que G é solúvel e $dl(G) \leq n - 1 + 1 = n$. □

Temos dois teoremas importantes e bem conhecidos sobre solubilidade de grupos finitos, os quais apenas enunciaremos.

Teorema 1.2.3 (Burnside)**.** *Todo grupo finito de ordem $p^a q^b$, onde p e q são números primos, é solúvel.*

Teorema 1.2.4 (Feit-Thompson)**.** *Todo grupo finito de ordem ímpar é solúvel.*

Por fim, enunciaremos o próximo teorema devido a I. N. Herstein. A sua demonstração completa pode ser vista em [Mac12], Teorema 5.53.

Teorema 1.2.5 (Teorema de Herstein)**.** *Suponha que G é um grupo finito e que G possui um subgrupo maximal abeliano M. Então G é solúvel.*

1.3 Grupos Nilpotentes

Definição 1.3.1. *A **série central descendente** de G é a sequência de subgrupos $(C^{n+1}(G))_{n\geq 0}$ definida indutivamente por*

$$C^1(G) := G \quad e \quad C^{n+1}(G) = [G, C^n(G)] \quad para\ n \geq 0.$$

*Além disso, dizemos que um grupo G é **nilpotente** se existe um $n \geq 0$ tal que $C^{n+1}(G) = 1$, e o menor inteiro $n \geq 1$ tal que $C^{n+1}(G) = 1$ é chamado de **classe de nilpotência** de G.*

Um propriedade importante de $C^i(G)$ é o seguinte teorema:

Teorema 1.3.1 (Proposição 3.6, [Ser16]). *Dado um grupo G, temos que $[C^i(G), C^j(G)] \leq C^{i+j}(G)$ para todo $i \geq 1$ e $j \geq 1$.*

Com este teorema podemos mostrar que nilpotência implica solubilidade, a saber:

Proposição 1.3.1. *Um grupo nilpotente é solúvel.*

Demonstração. Primeiro mostremos, por indução sobre n que, para todo $n \geq 0$, $D^n(G) \subseteq C^{2^n}(G)$. Para $n = 0$, temos que $G = D^0(G) \subseteq C^1(G) = G$ e segue o desejado. Agora suponha por hipótese de indução que $D^i(G) \subseteq C^{2^i}(G)$ para $i \geq 0$. Assim, pelo Teorema 1.3.1,

$$D^{i+1}(G) = D(D^i(G)) \subseteq D(C^{2^i}(G)) = [C^{2^i}(G), C^{2^i}(G)] \subseteq C^{2^{i+1}}(G),$$

e o resultado segue por indução. Logo, para n suficientemente grande $D^n(G) \subseteq C^{2^n}(G) = 1$, i.e., $D^n(G) = 1$. Portanto, G é solúvel. □

Como no caso solúvel, temos que subgrupos e quocientes de grupos nilpotentes também são nilpotentes, porém a recíproca não é verdadeira. Para isso, considerando $G := S_3$ temos que $C^i(G) = A_3$ para $i \geq 2$, o qual não é trivial. Assim, G não é nilpotente, mas os seus subgrupos e quocientes o são. Por outro lado, $G = S_3$ solúvel, pois $D^2(G) = [A_3, A_3] = 1$, ou seja, S_3 é também um exemplo de grupo solúvel que não é nilpotente.

Observe que um grupo G ser nilpotente de classe de nilpotência $\leq c$ é equivalente a

$$[[..., [[g_1, g_2], g_3], ..., g_c], g_{c+1}] = 1,$$

para todo $g_1, ..., g_{c+1} \in G$. Agora, podemos ver que para $N \leq Z(G)$, vale que N e G/N nilpotentes implicam G nilpotente.

Teorema 1.3.2. *Sejam G um grupo e N um subgrupo de G tal que $N \leq Z(G)$. Se G/N é nilpotente de classe $\leq c$, então G é nilpotente de classe $\leq c + 1$.*

Demonstração. Considere $\pi : G \to G/N$ a projeção natural. Então

$$\pi([[..., [[g_1, g_2], g_3], ...g_c], g_{c+1}]) = [[..., [[\pi(g_1), \pi(g_2)], \pi(g_3)], ...\pi(g_c)], \pi(g_{c+1})] = 1$$

em G/N para todo $g_1, ..., g_{c+1} \in G$, pois G/N é nilpotente de classe $\leq c$. Logo, $[[..., [[g_1, g_2], g_3], ...g_c], g_{c+1}]$ $N \leq Z(G)$ e, assim, $[[..., [[g_1, g_2], g_3], ...g_{c+1}], g_{c+2}] = 1$ para todo $g_1, ..., g_{c+2} \in G$. Portanto G é nilpotente de classe $\leq c + 1$. □

Agora podemos mostrar que um p-grupo finito é nilpotente.

Corolário 1.3.1. *Seja P um p-grupo finito. Então P é nilpotente.*

Demonstração. Usemos indução sobre a ordem de P. Inicialmente pela equação das classes, $|P| = |Z(P)| + \sum_{y \in P \setminus Z(P)} |P : C_P(y)|$ e, como p divide $|P|$ e cada $|P : C_P(y)|$, segue que p divide $|Z(P)|$. Logo $Z(P)$ é não-trivial e, portanto, $|P/Z(P)| < |P|$. Agora, por hipótese de indução, $P/Z(P)$ e $Z(P)$ são nilpotentes. Portanto, pelo Teorema 1.3.2 P é nilpotente. □

Uma importante propriedade de grupos nilpotentes é a seguinte:

Teorema 1.3.3. *Seja G um grupo nilpotente não-trivial. Então $Z(G)$ é não-trivial.*

Demonstração. Suponha que $C_n = 1$, mas $C_{n-1}(G) \neq 1$. Então $C_n(G) = [C_{n-1}(G), G] = 1$ se, e somente se, para todo $x \in C_{n-1}(G)$ e $g \in G$, $x^{-1}g^{-1}xg = 1$, isto é, $xg = gx$. Logo, $C_{n-1}(G) \leq Z(G)$ é não-trivial pois $C_{n-1}(G) \neq 1$. □

Agora daremos uma caracterização de nilpotência de grupos finitos, a qual será usada adiante, por exemplo, para classificarmos os grupos com valor mínimo de $\psi(G)$ sobre todos os grupos nilpotentes de mesma ordem (veja Teorema 2.3.1). Para isso, começaremos com os seguintes dois lemas:

Lema 1.3.1. *Sejam G um grupo finito e P um p-subgrupo de Sylow de G. Então para cada subgrupo H contendo $N_G(P)$, temos que $N_G(H) = H$.*

Demonstração. Seja $g \in N_G(H)$, e assim $gHg^{-1} = H$. Logo, $H \supseteq gPg^{-1} = \overline{P}$, o qual é p-subgrupo de Sylow de H. Pelo Teorema de Sylow, $h\overline{P}h^{-1} = P$ para algum $h \in H$, e portanto $hgPg^{-1}h^{-1} \subseteq P$. Logo $hg \in N_G(P) \subseteq H$, e sendo assim $g \in H$. Portanto, $N_G(H) = H$. □

Lema 1.3.2. *Sejam G um grupo finito nilpotente e H um subgrupo próprio de G. Então $H \neq N_G(H)$.*

Demonstração. O resultado é claro para grupos abelianos. Suponha que G é não-abeliano. Usemos indução sobre a ordem de G. Como G é nilpotente, temos que $Z(G) \neq 1$. Observe que $Z(G)$ normaliza H. Agora se $Z(G) \not\subseteq H$, então $H \subsetneq Z(G)H \subseteq N_G(H)$. Por outro lado, suponha que $Z(G) \subseteq H$. Pelo Teorema da Correspondência, temos que $N_G(H)$ corresponde ao normalizador de $H/Z(G)$ em $G/Z(G)$, e assim por hipótese de indução,

$$H/Z(G) < N_{G/Z(G)}(H/Z(G)) = N_G(H)/Z(G).$$

Portanto, $H < N_G(H)$. □

Seja $G = H \times K$. Então

$$\begin{aligned}[(h_1,k_1),(h_2,k_2)] &= (h_1,k_1)^{-1}(h_2,k_2)^{-1}(h_1,k_1)(h_2,k_2) \\ &= (h_1^{-1}h_2^{-1}h_1h_2, k_1^{-1}k_2^{-1}k_1k_2) = ([h_1,h_2],[k_1,k_2]).\end{aligned}$$

Logo, $[H \times K, H \times K] = [H,H] \times [K,K]$. Com essa observação podemos mostrar que $C^{i+1}(G) = C^{i+1}(H) \times C^{i+1}(K)$. De fato, o caso $C^1(G) = C^1(H) \times C^1(K)$ segue da observação feita. Agora, suponha por hipótese de indução que $C^i(G) = C^i(H) \times C^i(K)$ para $i \geq 1$. Assim,

$$\begin{aligned}C^{i+1}(G) = [G,\ C^i(G)] &= [H \times K,\ C^i(H \times K)] \\ &= [H \times K,\ C^i(H) \times C^i(K)] \\ &= [H,\ C^i(H)] \times [K,\ C^i(K)] \\ &= C^{i+1}(H) \times C^{i+1}(K),\end{aligned}$$

e segue por indução o que queríamos. Em particular, temos a seguinte proposição.

Proposição 1.3.2. *Um produto direto finito de grupos nilpotentes é nilpotente.*

Demonstração. Seja $G = H \times K$ e suponha que H e K são grupos nilpotentes. Assim, existem inteiros positivos c_1 e c_2 tais que $C^{c_1+1}(H) = 1$ e $C^{c_2+1}(K) = 1$. Logo, tomando $c = \max\{c_1, c_2\}$, temos que $C^{c+1}(G) = C^{c+1}(H) \times C^{c+1}(K) = 1$. Portanto, G é nilpotente.

Para $G = H_1 \times \cdots \times H_n$, onde cada H_i é um grupo nilpotente, o resultado segue por indução. □

Uma importante caracterização de grupos nilpotentes finitos é a seguinte:

Teorema 1.3.4. *Um grupo finito G é nilpotente se, e somente se, G é o produto direto de seus subgrupos de Sylow.*

Demonstração. Seja G um grupo nilpotente. É suficiente mostrarmos que cada subgrupo de Sylow de G é normal em G. Seja P um tal subgrupo, e considere $N = N_G(P)$. Pelo Lema 1.3.1, temos que $N_G(N) = N$. Agora, pelo Lema 1.3.2, $N = G$. Portanto, P é normal em G. Reciprocamente, como o produto direto de grupos nilpotentes é nilpotente e cada subgrupo de Sylow de G é nilpotente, segue que G é nilpotente. □

Por fim enunciaremos uma série de equivalências de nilpotência em grupos finitos. A demonstração completa dessas equivalências podem ser vistas em **[Rose09]**.

Teorema 1.3.5 (Teorema 10.9, **[Rose09]**)**.** *Seja G um grupo finito. As seguintes afirmações são equivalentes:*

i) *G é nilpotente.*

ii) *Para algum inteiro positivo r, $C^r(G) = 1$.*

iii) *Para algum inteiro positivo s, $Z_s(G) = G$. Aqui $Z_i(G)$ denota o i-ésimo centro superior de G definindo indutivamente como a seguir: $Z_0(G) = 1$ e, para $i \geq 1$, $Z_i(G)$ é definido por*

$$g \in Z_i(G) \text{ se, e somente se, } [g, x] \in Z_{i-1}(G) \text{ para todo } x \in G.$$

iv) *Se $H < G$, então $H < N_G(H)$.*

v) *Todos subgrupos maximais de G são normais.*

vi) *Todos os subgrupos de Sylow de G são normais.*

vii) *G é o produto direto de seus subgrupos de Sylow.*

viii) *Se $a, b \in G$ e $mdc(o(a), o(b)) = 1$, então a e b comutam em G.*

iv) *O subgrupo derivado $D(G) = G'$ de G é um subgrupo do subgrupo de Frattini $\Phi(G)$ de G, onde $\Phi(G)$ é a interseção de todos os subgrupos maximais de G.*

1.4 O Teorema de Schur-Zassenhaus

Definição 1.4.1. *Dizemos que um grupo G é um **produto semidireto** (interno) de N por H se N é um subgrupo normal de G, H um subgrupo, $G = NH$ e $N \cap H = \{1\}$. Neste caso,*

$$G/N = NH/N \cong H/(N \cap H) = H/\{1\} \cong H,$$

*isto é, $G/N \cong H$. Dizemos que H é um **complemento** de N em G, e denotamos G por $G = N \rtimes H$.*

Seja N um subgrupo normal de G. Cada elemento $g \in G$ define um automorfismo de N, $i_{g|N} : N \to N$ dado por $i_g(n) = gng^{-1}$. Assim, temos um homomorfismo

$$\begin{aligned} \theta \colon G &\longrightarrow Aut(N) \\ g &\longmapsto i_{g|N} \colon N \longrightarrow N \\ &\qquad\quad n \longmapsto i_{g|N}(n) = gng^{-1}. \end{aligned}$$

Se existe um subgrupo H de G tal que a restrição de $G \to G/N$ por H é um isomorfismo, então podemos reconstruir o grupo G a partir de N, H e a restrição de θ a H. De fato, cada elemento $g \in G$ pode ser escrito unicamente na forma $g = nh$, com $n \in N$ e $h \in H$; neste caso, h é o único elemento de H cuja imagem é gN em G/N, e n é igual a gh^{-1}. Assim, temos uma correspondência 1-a-1 de conjuntos: $G \longleftrightarrow N \times H$. Agora, se $g = nh$ e $g' = n'h'$, então

$$gg' = (nh)(n'h') = n(hn'h^{-1})hh' = n \cdot \theta(h)(n') \cdot hh'.$$

Mais especificamente, podemos definir o produto semidireto da seguinte maneira.

Definição 1.4.2. *Um grupo G é o* ***produto semidireto*** *de seus subgrupos N e H se N é normal em G e o homomorfismo $G \to G/N$ induz um isomorfismo $H \to G/N$. Equivalentemente, G é o produto semidireto de N por H se $N \trianglelefteq G$, $G = NH$ e $N \cap H = \{1\}$.*

Denotamos $G = N \rtimes_\theta H$, onde $\theta : H \to Aut(N)$ nos dá a ação de H sobre N por automorfismos internos.

Se N é um subgrupo normal de G não-trivial, então existe um complemento para N em G? Isto é, existe um subgrupo H de G tal que $G = NH$ e $N \cap H = \{1\}$? Em geral, a resposta é não! Por exemplo, o grupo cíclico C_{p^2} possui apenas um subgrupo N de ordem p e assim não pode ser escrito com produto de N por outro subgrupo de C_{p^2}. Agora, se impormos a condição de $|N|$ e $|G/N|$ serem coprimos, então temos que G é um produto semidireto de N por G/N. Este é o resultado do seguinte Teorema de Schur-Zassenhaus.

Teorema 1.4.1 (Schur-Zassenhaus)**.** *Sejam G um grupo finito e N um subgrupo normal em G. Suponha que $|N|$ e $|G/N|$ são relativamente primos. Então N possui um complemento H em G.*

O Teorema de Schur-Zassenhaus também garante que todos os complementos de N são conjugados entre si, mas não iremos precisar de tal fato e demonstraremos apenas que um complemento para N de fato existe. A existência de complementos será muito importante principalmente nas demonstrações do Teorema A e do Teorema B do capítulo seguinte.

Para demonstração do Teorema de Schur-Zassenhaus seguiremos a abordagem dada em [**Isa08**], Capítulo 3B. Para isto começaremos definindo um novo tipo de "homomorfismo".

Definição 1.4.3. *Seja G agindo via automorfismo sobre N. Dizemos que uma aplicação $\varphi : G \to N$ é um homomorfismo cruzado se*

$$\varphi(xy) = \varphi(x)^y \varphi(y),$$

para quaisquer $x, y \in G$ (o expoente y na equação acima refere a ação via automorfismo de G sobre N).

Observação 1.4.1. *Observe que se a ação de G sobre N é trivial (ou seja, $n^g = n$ para todo $n \in N$ e $g \in G$), então um homomorfismo cruzado com tal ação é justamente um homomorfismo de grupos da maneira usual que conhecemos.*

Note também que se N é um subgrupo normal de G, então G age sobre N via conjugação. Por exemplo, dado $n \in N$ fixado, defina $\varphi : G \to N$ por $\varphi(x) = [x, n] = x^{-1}n^{-1}xn = (n^{-1})^x n$. Como N é normal em G, temos que $(n^{-1})^x \in N$, e portanto $\varphi(x) = (n^{-1})^x n \in N$. Assim, φ está bem definida. Além disso,

$$\begin{aligned}\varphi(xy) = [xy, n] &= (xy)^{-1}n^{-1}(xy)n \\ &= y^{-1}x^{-1}n^{-1}xyn \\ &= y^{-1}(x^{-1}n^{-1}xn)y(y^{-1}n^{-1}yn) \\ &= \varphi(x)^y\varphi(y),\end{aligned}$$

para quaisquer $x, y \in G$. Portanto, φ é um homomorfismo cruzado.

Como na maneira usual, podemos definir o "kernel" de um homomorfismo cruzado.

Definição 1.4.4. *Seja $\varphi : G \to N$ um homomorfismo cruzado. Então o kernel de φ é subconjunto* $\ker(\varphi) := \{x \in G \mid \varphi(x) = 1\}$.

Mostraremos agora algumas propriedades básicas de um homomorfismo cruzado.

Lema 1.4.1 (Propriedades básicas)**.** *Sejam G agindo via automorfismo sobre N e $\varphi : G \to N$ um homomorfismo cruzado com kernel K. Então valem que:*

i) $\varphi(1) = 1$.

ii) K *é um subgrupo de* G.

iii) *Se $x, y \in G$, então $\varphi(x) = \varphi(y)$ se, e somente se, $Kx = Ky$.*

iv) $|G : K| = |\varphi(G)|$.

Demonstração. *i)* Veja que $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)^1\varphi(1) = \varphi(1)^2$. Portanto, $\varphi(1) = 1$.

ii) Se $k \in K$, então

$$1 = \varphi(1) = \varphi(kk^{-1}) = \varphi(k)^{k^{-1}}\varphi(k^{-1}) \\ = 1^{k^{-1}}\varphi(k^{-1}) = \varphi(k^{-1}).$$

Logo $k^{-1} \in K$. Além disso, dados $x, y \in G$, temos que

$$\varphi(xy) = \varphi(x)^y\varphi(y) = 1^y \cdot 1 = 1.$$

Portanto, segue que K é um subgrupo de G.

iii) Sejam $x, y \in G$ e suponha que $\varphi(x) = \varphi(y)$. Para que $Kx = Ky$ basta mostrar que $xy^{-1} \in K$. Mas

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

ou seja, $xy^{-1} \in K$. Reciprocamente, suponha que $Kx = Ky$. Temos que existe $k \in K$ tal que $x = ky$. Logo

$$\varphi(x) = \varphi(ky) = \varphi(k)^y\varphi(y) = 1^y\varphi(y) = \varphi(y).$$

iv) Como $\varphi(x) = \varphi(y)$ se, e somente se, $Kx = Ky$, temos uma bijeção entre $\varphi(G)$ e as classes laterais à direita de K em G. Portanto, segue que $|\varphi(G)| = |G/K|$.

□

Agora queremos construir um homomorfismo cruzado de um grupo finito G em um subgrupo abeliano normal N de G. Para isto, considere $\mathcal{T}$ o conjunto de todos os transversais para N em G (lembre-se que um transversal T para N é um conjunto contendo exatamente um elemento de cada classe lateral em G/N).

Vamos definir a seguinte relação (de equivalência) sobre G. Dados $x, y \in G$, então $x \equiv y$ se, e somente se, $Nx = Ny$. Em outras palavras, x é equivalente a y se, e somente se, ambos os dois elementos pertencem a mesma classe lateral.

Se $S, T \in \mathcal{T}$, então a relação $s \equiv t$, para $s \in S$ e $t \in T$, define uma bijeção natural entre S e T. Usemos essa bijeção para definir o elemento

$$d(S,T) := \prod_{s \equiv t} s^{-1}t,$$

onde o produto acima percorre todo $s \in S$ e $t \in T$ com $s \equiv t$. Note que $sN = tN$ implica que $s^{-1}t \in N$ e, portanto, $d(S,T) = \prod_{s \equiv t} s^{-1}t \in N$. Além disso, como N é abeliano, temos que a ordem dos fatores do produto é irrelevante. Portanto, $d(S,T)$ é um elemento de N e está bem definido.

Agora, temos algumas propriedades básicas de $d(S,T)$, cujas demonstrações podem ser vistas em [Isa08].

Lema 1.4.2 (Lema 3.7, [Isa08]). *Seja N um subgrupo abeliano normal de um grupo finito G, e sejam S, T e U transversais para N. Então:*

i) $d(S,T)d(T,U) = d(S,U)$.

ii) $d(Sg, Tg) = d(S,T)^g$ *para todo* $g \in G$.

iii) $d(S, Sn) = n^{|G:N|}$ *para todo* $n \in N$.

Agora podemos demonstrar o Teorema de Schur-Zassenhaus para o caso em que N é abeliano.

Teorema 1.4.2 (Schur-Zassenhaus, caso N abeliano). *Sejam G um grupo finito e N um subgrupo abeliano normal em G. Suponha que $|N|$ e $|G/N|$ são relativamente primos. Então N possui um complemento H em G.*

Demonstração. Fixe um transversal arbitrário T para N em G, e defina $\theta : G \to N$ dada por $\theta(g) = d(T, Tg)$. Primeiro vamos mostrar que θ é um homomorfismo cruzado com respeito a ação de conjugação de G sobre N. Para isto, sejam $x, y \in G$, temos, pelo Lema

1.4.2, que

$$\begin{aligned}\theta(xy) = d(T, Txy) &= d(T, Ty)d(Ty, Txy)\\ &= d(T, Ty)d(T, Tx)^y\\ &= d(T, Tx)^y d(T, Ty) \quad \text{(pois } N \text{ é abeliano)}\\ &= \theta(x)^y\theta(y).\end{aligned}$$

Assim, θ é um homomorfismo cruzado de G em N. Agora, dado $n \in N$, temos que $\theta(n) = n^{|G:N|}$ pelo Lema 1.4.2, *iii*). Note que, por hipótese, $|N|$ e $|G : N|$ são relativamente primos, segue que $x \mapsto x^{|G:N|}$ é uma permutação dos elementos de N. De fato, existe $k \in \mathbb{Z}$ tal que $k|G : N| \equiv 1 \pmod{|N|}$, e assim $x \mapsto x^k$ é uma inversa para $x \mapsto x^{|G:N|}$. Disto temos que $\theta(N) = N$ e, em particular, $\theta(G) = N$. Considere $H := ker(\theta)$ que, pelo Lema 1.4.1, *ii*), é um subgrupo de G. Também temos que $|N| = |\theta(G)| = |G : H|$ pelo Lema 1.4.1, e portanto

$$|N| \cdot |H| = |G : H| \cdot |H| = |G| \quad \text{e} \quad |H| = |G : N|.$$

Por fim, como $|N|$ e $|G : N| = |H|$ são coprimos, temos que $N \cap H = 1$. Portanto, H é um complemento para N em G.

□

Provaremos agora o Teorema de Schur-Zassenhaus sem supor que N é um subgrupo normal abeliano.

Teorema 1.4.3. *Seja G um grupo finito e seja N um subgrupo normal de G. Suponha que $|N|$ e $|G : N|$ são relativamente primos. Então N possui um complemento H em G.*

Demonstração. Usemos indução sobre a ordem $|G|$ de G. O caso $|G| = 1$ é trivial. Inicialmente suponha que existe $K < G$ tal que $NK = G$. Então $|K : K \cap N| = |G : N|$ é coprimo a $|N|$ e, portanto, também é coprimo a $|N \cap K|$. Como $K \cap N \trianglelefteq K$, por hipótese de indução, temos que $K \cap N$ possui um complemento H em K. Assim,

$$|H| = |K : K \cap N| = |G : N|,$$

o que garante que H também é um complemento para N em G. Portanto, podemos supor que não existe um subgrupo próprio K de G tal que $NK = G$; assim, em particular, N deve estar contido em todo subgrupo maximal de G, pois $M = NM < G$. Logo, $N \subset \Phi(G) = \bigcap M$, o subgrupo de Frattini de G, e assim N é nilpotente. Também podemos supor que $N > 1$, caso contrário o próprio G é um complemento para N.

Agora seja $Z = Z(N)$ e observe que $1 < Z \trianglelefteq G$, pois o centro de grupo nilpotente é não-trivial. Considerando $\overline{G} = G/Z$ e $\overline{N} = N/Z$, temos que $|\overline{G} : \overline{N}| = |G : N|$ é coprimo a $|N|$, por hipótese, e portanto também é coprimo a $|\overline{N}|$. Logo, por hipótese de indução, existe um complemento $\overline{K}$ de $\overline{N}$ em $\overline{G}$. Então

$$\overline{G} = \overline{NK} = N/ZK/Z = NK/Z = \overline{NK},$$

e portanto $G = NK$. Por nossa suposição K não é um subgrupo próprio, logo segue que $K = G$. Como $\overline{K}$ é um complemento $\overline{N}$, temos que $\overline{K} \cap \overline{N} = \overline{1} = \overline{Z}$. Logo

$$\overline{Z} = \overline{N} \cap \overline{K} = \overline{N} \cap \overline{G} = \overline{N},$$

e $N = Z = Z(N)$ é abeliano. Portanto, o resultado segue pelo caso abeliano. □

Agora já temos uma base suficiente para entrar no assunto principal da dissertação. No próximo capítulo introduziremos novos conceitos e aplicaremos tudo que vimos até aqui.

Capítulo 2

A função ψ

Neste capítulo, introduziremos a função ψ, definida em [AAI09], bem como as suas propriedades básicas. Além disso, veremos alguns resultados que nos darão critérios de ciclicidade e nilpotência de grupos finitos, dados em [HLM18a] e [AA11]. Por último veremos algumas condições suficientes para solubilidade de grupos finitos.

2.1 Conceitos iniciais

Dado um grupo G, denote por $o(x)$ a ordem do elemento $x \in G$. Comecemos com a seguinte definição:

Definição 2.1.1. *Seja G um grupo finito. Definimos*

$$\psi(G) := \sum_{x \in G} o(x).$$

O valor $\psi(G)$ é definido como a soma das ordens de todos os elementos de um grupo finito G. Uma pergunta natural é:

Podemos obter informações de um grupo G a partir de $\psi(G)$ e $|G|$?

Vejamos alguns exemplos.

Exemplo 2.1.1. *Seja C_n o grupo cíclico de ordem n. Temos que para cada divisor d de n, existem $\varphi(d)$ elementos de ordem d em C_n, onde φ é a função de Euler, i.e.,*

$\varphi(m) := |\,(\mathbb{Z}/m\mathbb{Z})^\times\,|$. *Sendo assim, temos que*

$$\psi(C_n) = \sum_{d|n} d \cdot \varphi(d).$$

Em particular, se p é primo então

$$\psi(C_p) = 1 + (p-1)p.$$

Por exemplo,

$$\psi(C_2) = 3, \quad \psi(C_3) = 7, \quad \psi(C_5) = 21 \text{ e } \psi(C_7) = 43.$$

Temos ainda

$$\psi(C_4) = 1 + 2 + 2 \cdot 4 \quad \text{e} \quad \psi(C_6) = 1 + 2 + 2 \cdot 3 + 2 \cdot 6 = 21.$$

Como $\psi(C_5) = \psi(C_6) = 21$, temos que o valor de $\psi(G)$ não determina o grupo G. Além disso, em geral o valor de $\psi(G)$ e $|G|$ também não determinam G:

Exemplo 2.1.2. *Considere os seguintes grupos $G = C_4 \times C_4$ e $H = C_2 \times Q_8$, onde $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ é o grupo dos quatérnios de ordem 8 com $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$ e $ki = j$. Ambos os grupos G e H têm ordem 16 e podemos verificar que $\psi(G) = \psi(H) = 55$. Por outro lado, G é abeliano enquanto H não o é. Portanto $G \ncong H$.*

Por outro lado, em alguns casos, $\psi(G)$ determina G (a menos de isomorfismo) mesmo sem saber $|G|$.

Observação 2.1.1. *Note que, para qualquer grupo finito G, todo elemento $x \in G$ não-trivial tem ordem no mínimo 2. Assim, $\psi(G) \geq 1 + 2(|G| - 1)$, e portanto*

$$|G| \leq \frac{1}{2}(\psi(G) + 1).$$

Exemplo 2.1.3. *Os únicos grupos G e H tais que $\psi(G) = 13$ e $\psi(H) = 211$ são os grupos $G = S_3$ e o alternado $H = A_5$.*

De fato, se $\psi(G) = 13$, *temos* $|G| \leq \frac{1}{2}(13+1) = 7$. *Pelos exemplos feitos antes, vemos que* $G = S_3$ *é o único grupo com* $\psi(G) = 13$. *Agora se* $\psi(H) = 211$, *então* $|H| \leq \frac{1}{2}(211+1) = 106$. *Usando o* `GAP`, ***[GAP]***, *podemos verificar que apenas o grupo* $H = A_5$ *satisfaz* $\psi(H) = 211$.

Mais a frente daremos uma caracterização, devida a S.M. Jafarian Amiri, de A_5 *com a propriedade que* $\psi(A_5)$ *é o valor mínimo para* $\psi(G)$ *sobre todos os grupos de ordem* 60.

Agora, faremos um lema muito útil que diz que a função ψ é "multiplicativa".

Lema 2.1.1 (Lema 2.1, [AA11]). *Se* G *e* H *são grupos finitos, então*

$$\psi(G \times H) \leq \psi(G)\psi(H).$$

Além disso, $\psi(G \times H) = \psi(G)\psi(H)$ *se, e somente se,* $mdc(|G|, |H|) = 1$.

Demonstração. Como $o((g,h)) \leq o(g)o(h)$ para todo $(g,h) \in G \times H$, temos que

$$\begin{aligned}\psi(G \times H) &= \sum_{g \in G} \sum_{h \in H} o((g,h)) \\ &\leq \sum_{g \in G} \sum_{h \in H} o(g)o(h) \\ &= \left(\sum_{g \in G} o(g)\right)\left(\sum_{h \in H} o(h)\right) = \psi(G)\psi(H).\end{aligned}$$

Por outro lado note que $mdc(|G|, |H|) = 1$ se, e somente se, $mdc(o(g), o(h)) = 1$ para todos $g \in G$ e $h \in H$, o qual é equivalente a $o((g,h)) = o(g)o(h)$ para todos $g \in G$ e $h \in H$. Portanto, segue que $\psi(G \times H) = \psi(G)\psi(H)$ se, e somente se, $mdc(|G|, |H|) = 1$. □

A função ψ foi introduzida por H. Amiri, S.M. Jafarian Amiri, I.M. Isaacs no artigo [AAI09] de 2009. Nesse artigo foi provado o seguinte teorema:

Teorema I. *Seja* C_n *o grupo cíclico de ordem* n. *Então para todo grupo não-cíclico* G *de ordem* n, *temos que*

$$\psi(G) < \psi(C_n).$$

Desta forma, para cada inteiro positivo n, o grupo cíclico de ordem n fica unicamente determinado (a menos de isomorfismo) pela sua ordem n e a soma das ordens de seus elementos $\psi(C_n)$. Como vimos nos exemplos e observações feitas anteriormente, esse resultado não vale em geral.

Podemos definir a função ψ para qualquer subconjunto X de G, de maneira natural:

Definição 2.1.2. *Seja $X \subseteq G$ um subconjunto qualquer de um grupo G. Podemos estender a função ψ escrevendo $\psi(X) = \sum_{x \in X} o(x)$.*

A fim de provar o resultado principal desta subseção, o Teorema I, comecemos com o seguinte lema:

Lema 2.1.2 (Lema A, [AAI09])**.** *Seja $P \in Syl_p(G)$ um p-subgrupo de Sylow de G. Suponha que P é normal em G e que P é cíclico. Seja $x \in G$ e suponha que a classe lateral Px tem ordem m, como um elemento de G/P. Então $\psi(Px) \leq m\psi(P)$, com a igualdade se, e somente se, x centraliza P.*

Demonstração. Temos que m divide $o(x)$, e assim $o(x) = mq$ para algum q inteiro. Logo, $q = o(x^m)$. Como $x^m \in P$ (pois Px tem ordem m), temos que q é uma potência de p. Além disso, como m divide $|G/P|$ que não é divisível por p, segue que m e q são relativamente primos entre si. Logo, existe n tal que $qn \equiv 1 \pmod{m}$. Agora, $o(x^q) = m$ e escrevendo $y = (x^q)^n$, temos que $o(y) = m$, pois n é coprimo a m. Note que

$$Py = Px^{qn} = (Px)^{qn} = Px,$$

e além disso, y centraliza P se, e somente se, x centraliza P. De fato, se y centraliza P e $g \in P$, então por $Px = Py$ temos que $x = hy$ para algum $h \in P$, e portanto

$$xg = (hy)g = h(yg) = h(gy) = (hg)y = (gh)y = g(hy) = gx.$$

Podemos então substituir x por y e supor que $o(x) = m$. Agora todo elemento de Px tem a forma ux para algum $u \in P$. Mostremos que $o(ux) \leq m \cdot o(u)$ com a igualdade se, e somente se, x centraliza u.

De fato, como P é cíclico, P possui apenas um único subgrupo de cada ordem dividindo a ordem de P. Desta forma, para cada $\sigma \in Aut(P)$, o subgrupo $\sigma(\langle u\rangle)$ de P tem a mesma ordem que $\langle u\rangle$, e portanto $\sigma(\langle u\rangle) = \langle u\rangle$, i.e., $\langle u\rangle$ é um subgrupo característico de P. Note também que dado $g \in G$, $i_g : P \to P$ dado por $i_g(v) = g^{-1}ng$ é um automorfismo de P, e portanto $i_g(\langle u\rangle) = \langle u\rangle$, ou seja, $\langle u\rangle$ é normal em G. Logo $\langle u\rangle\langle x\rangle$ é um subgrupo de G, e portanto

$$o(ux) \leq |\langle u\rangle\langle x\rangle| = m \cdot o(u).$$

Por outro lado, se a igualdade ocorre então $\langle u\rangle\langle x\rangle$ é um subgrupo cíclico, gerado por ux, e assim x centraliza u. Reciprocamente, se x centraliza u, então como $o(x)$ e $o(u)$ são coprimos, temos que $o(ux) = o(x)o(u) = m \cdot o(x)$.

Por fim,

$$\psi(Px) = \sum_{u\in P} o(ux) \leq \sum_{u\in P} m \cdot o(u) = m \sum_{u\in P} o(u) = m\psi(P)$$

e a igualdade ocorre se, e somente se, x centraliza u para cada $u \in P$, ou seja, se, e somente se, x centraliza P. □

Agora temos um corolário, que será uma ferramenta muito importante durante todo o trabalho.

Corolário 2.1.1 (Corolário B, [AAI09]). *Seja P um p-subgrupo de Sylow de G e suponha que P seja cíclico e normal em G. Então*

$$\psi(G) \leq \psi(P)\psi(G/P)$$

com a igualdade se, e somente se, P é central em G.

Demonstração. Aplicando o Lema 2.1.2 em cada classe lateral de P em G, obtemos

$$\psi(G) = \sum_{Px\in G/P} \psi(Px) \leq \sum_{Px\in G/P} o(Px)\psi(P) = \psi(P) \sum_{Px\in G/P} o(Px) = \psi(P)\psi(G/P)$$

e a igualdade ocorre se, e somente se, cada elemento $x \in G$ centraliza P. □

Também mostremos um resultado de teoria dos números elementar:

Lema 2.1.3 (Lema C, [AAI09]). *Seja p o maior divisor primo de um inteiro $n > 1$. Então $\varphi(n) \geq n/p$.*

Demonstração. Seja k o número de divisores primos distintos de n. Usemos indução sobre k. Se $k = 1$, então $n = p^e$ para algum $e \geq 1$. Assim $\varphi(n) = p^{e-1}(p-1) = (p-1)n/p \geq n/p$, pois $p - 1 \geq 1$. Suponha que $k > 1$ e que o resultado é válido para números com $k - 1$ divisores primos. Escrevendo $n = p^e m$, com $e \geq 1$ e p não dividindo m, temos que m possui $k-1$ divisores primos e tomemos q como sendo o maior deles. Assim pela hipótese de indução, $\varphi(m) \geq m/q$ e como $q < p$, temos que $q \leq p - 1$. Logo

$$\varphi(n) = \varphi(p^e)\varphi(m) \geq (p-1)\frac{p^e}{p}.\frac{m}{q} = (p-1)\frac{n}{pq} \geq n/p$$

□

Como consequência temos o seguinte corolário que limita inferiormente $\psi(C_n)$ para grupos cíclicos.

Corolário 2.1.2 (Corolário D, [AAI09]). *Seja C_n o grupo cíclico de ordem $n > 1$, e seja p o maior divisor primo de n. Então,*

$$\psi(C_n) > n^2/p.$$

Demonstração. Temos que existem $\varphi(n)$ elementos de ordem n em C_n, e assim

$$\psi(C_n) \geq 1 + n\varphi(n) > n\varphi(n) \geq n^2/p,$$

onde a última desigualdade segue pelo Lema 2.1.3. Portanto, temos o desejado. □

Agora podemos demonstrar o Teorema I, que caracteriza os grupos cíclicos pela soma de suas ordens:

Teorema I (Teorema, [AAI09]). *Seja C_n um grupo cíclico de ordem n. Então para todo grupo não-cíclico G de ordem n, temos que*

$$\psi(G) < \psi(C_n).$$

Demonstração. Sejam G um grupo de ordem n e C_n o cíclico de ordem n, e suponha que $\psi(G) \geq \psi(C_n)$. Devemos mostrar que G é cíclico. Como isso é trivial no caso $n = 1$, podemos supor $n > 1$ e procedemos por indução sobre n. Pelo Corolário 2.1.2, temos que

$$\frac{\psi(G)}{|G|} \geq \frac{\psi(C_n)}{n} > \frac{n^2}{np} = \frac{n}{p},$$

isto é, $\psi(G) > \dfrac{n^2}{p}$, onde p é o maior divisor primo de n.

Note que existe um elemento $x \in G$ tal que $o(x) > \dfrac{n}{p}$, caso contrário teríamos que $o(y) \leq \dfrac{n}{p}$ para todo $y \in G$ e, portanto, $\psi(G) \leq n \cdot \dfrac{n}{p} = \dfrac{n^2}{p}$, uma contradição. Logo $|G : \langle x\rangle| < p$ e assim $\langle x\rangle$ contém um p-subgrupo de Sylow P de G, e P é cíclico por ser um subgrupo de $\langle x\rangle$. Como $\langle x\rangle$ é abeliano, temos $P \trianglelefteq \langle x\rangle$ e assim $\langle x\rangle \subseteq N_G(P)$. Logo $|G : N_G(P)| < p$ e, portanto, $P \trianglelefteq G$. Assim, pelo Corolário 2.1.1, $\psi(G) \leq \psi(P)\psi(G/P)$ e a igualdade ocorre se, e somente se, P é central em G.

Seja Q o p-subgrupo de Sylow de C_n, e note que Q e P são cíclicos de mesma ordem, e portanto $P \cong Q$ e $\psi(P) = \psi(Q)$. Usando o Corolário 2.1.1, obtemos

$$\psi(P)\psi(G/P) \geq \psi(G) \geq \psi(C_n) = \psi(Q)\psi(C_n/Q), \tag{2.1}$$

onde a última igualdade ocorre pois Q é central em C_n. Assim, temos que $\psi(G/P) \geq \psi(C_n/Q)$. Como C_n/Q é cíclico e $|G/P| = |C_n/Q|$, temos por hipótese de indução que G/P é cíclico. Então $G/P \cong C_n/Q$, e portanto $\psi(G/P) = \psi(C_n/Q)$. Segue que todas as desigualdades em (2.1) são igualdades, e assim P é central em G. Como P é central em G e G/P é cíclico, segue que G é abeliano, pois $G/Z(G) \leq G/P$ é cíclico. Além disso, como P é um p-subgrupo de Sylow de G, temos $G \cong P \times B$, onde $B \cong G/P$ é cíclico de ordem coprima com p. Logo, G é o produto direto dois grupos cíclicos de ordens coprimas

e, portanto, G é cíclico. □

2.2 Uma cota superior exata para $\psi(G)$

Como vimos na seção anterior, o grupo cíclico de ordem n tem a soma máxima sobre todos os grupos de ordem n. Alguns autores estudaram o problema de determinar o valor máximo de $\psi(G)$ para grupos não-cíclicos. Esse problema inicialmente foi estudado por S.M. Jafarian Amiri e M. Amiri em "Second maximum sum of element orders on finite groups", [AA14a]. M.Herzog, P. Longobardi, e M. Maj em 2018, [HLM18a], determinaram uma cota superior exata para $\psi(G)$ para grupos não-cíclicos de ordem n a qual é a melhor possível. Esse é o resultado do seguinte teorema:

Teorema A. *Se G é um grupo finito não-cíclico de ordem n, então*

$$\psi(G) \leq \frac{7}{11}\psi(C_n).$$

Pela proposição seguinte vemos que essa cota do Teorema **A** é a melhor possível.

Proposição 2.2.1. *Seja k um inteiro positivo ímpar e seja $n = 4k$. Então*

$$\psi(C_n) = 11\psi(C_k), \qquad \psi(C_{2k} \times C_2) = 7\psi(C_k)$$

e portanto

$$\psi(C_{2k} \times C_2) = \frac{7}{11}\psi(C_n).$$

Demonstração. Como $n = 4k$ e $mdc(4, k) = 1$, temos que $C_n \cong C_4 \times C_k$ e, portanto, pelo Lema 2.1.1,

$$\psi(C_n) = \psi(C_4 \times C_k) = \psi(C_4)\psi(C_k) = 11\psi(C_k)$$

e

$$\psi(C_{2k} \times C_2) = \psi(C_k \times C_2 \times C_2) = \psi(C_k)\psi(C_2 \times C_2) = 7\psi(C_k).$$

Logo,

$$\psi(C_{2k} \times C_2) = 7\psi(C_k) = \frac{7}{11}\psi(C_n).$$

□

Em particular, para $n = 4k$ com k ímpar, obtemos que $G = C_{2k} \times C_2$ tem a soma maximal das ordens dos elementos sobre todos os grupos não-cíclicos de ordem n.

Além disso, no mesmo artigo **[HLM18a]** foi provado o seguinte teorema.

Teorema B. *Seja G um grupo finito não-cíclico de ordem n e seja q o menor divisor primo de n. Então*

$$\psi(G) < \frac{1}{q-1}\psi(C_n).$$

Como consequência direta deste teorema, temos:

Corolário 2.2.1. *Seja G um grupo de ordem n ímpar. Então*

$$\psi(G) \leq \frac{1}{2}\psi(C_n).$$

Primeiramente, abordaremos o Teorema B e iremos utilizá-lo para demonstrar o Teorema A. Iniciamos com alguns resultados preliminares que serão úteis para ambos teoremas.

Lema 2.2.1 (Lema 2.9, **[HLM18a]**). (1) *Se P é um grupo cíclico de ordem p^r para algum primo p, então*

$$\psi(P) = \frac{p^{2r+1}+1}{p+1}.$$

(2) *Seja $n > 1$ um inteiro positivo e sejam $p_1 < p_2 < \cdots < p_t = p$ os divisores primos distintos de n, e denote por $P_1, P_2, \ldots, P_t$ os respectivos subgrupos de Sylow de C_n. Então*

$$\psi(C_n) = \prod_{i=1}^{t} \psi(P_i) \geq \frac{2}{p+1}n^2.$$

Demonstração. 1. Note que $\varphi(p^i) = p^{i-1}(p-1)$ para cada $i \geq 1$. Assim,

$$\begin{aligned}\psi(P) = \sum_{i=0}^{r} p^i \cdot \varphi(p^i) &= 1 + \sum_{i=1}^{r} p^i \cdot p^{i-1}(p-1) \\ &= 1 + \frac{p-1}{p} \sum_{i=1}^{r} p^{2i} \\ &= 1 + \frac{p-1}{p} \left(\frac{p^2(p^{2r}-1)}{p^2-1} \right) \\ &= 1 + \frac{p(p^{2r}-1)}{p+1} = \frac{p^{2r+1}+1}{p+1}.\end{aligned}$$

2. Como $C_n = P_1 \times P_2 \times \cdots \times P_t$, temos que $\psi(C_n) = \prod_{i=1}^{t} \psi(P_i)$. Além disso, como $p_{i+1} \geq p_i + 1$ para todo i e $p_i \geq 2$, segue, pelo *item (1)*, que

$$\begin{aligned}\psi(C_n) = \prod_{i=1}^{t} \psi(P_i) &= \prod_{i=1}^{t} \frac{p_i^{2r_i+1}+1}{p_i+1} \\ &> \prod_{i=1}^{t} \frac{p_i^{2r_i} p_i}{p_i+1} \\ &= p_1^{2r_1} \cdots p_t^{2r_t} \cdot \frac{p_1}{1} \cdot \frac{p_2}{p_1+1} \cdots \frac{p_t}{p_{t-1}+1} \cdot \frac{1}{p_t+1} \\ &\geq (p_1 \cdots p_t)^2 \frac{p_1}{p_t+1} \\ &= n^2 \frac{p_1}{p+1} \geq \frac{2}{p+1} n^2,\end{aligned}$$

como desejado.

□

Mais um resultado de teoria dos números elementar:

Lema 2.2.2 (Lema 2.1, [HLM18a])**.** *Seja n um inteiro positivo maior do que 1, e sejam p e q o maior e o menor divisor primo de n, respectivamente. Então*

$$\varphi(n) \geq \frac{q-1}{p} n.$$

Demonstração. Seja $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ onde os p_i's são primos distintos com $p = p_1 > p_2 >$

$\cdots > p_k = q$ e cada r_i é um inteiro positivo. Provaremos o resultado por indução sobre k.

Se $k = 1$, então $n = p^{r_1}$ e

$$\varphi(n) = \varphi(p^{r_i}) = (p-1)p^{r_1-1} = \frac{p-1}{p}n$$

e o resultado segue. Agora suponha $k > 1$ e que o lema é verdade para todos os inteiros com menos que k divisores primos distintos. Seja $m = p_2^{r_2} \cdots p_k^{r_k}$. Então, por hipótese de indução, $\varphi(m) \geq \frac{p_k - 1}{p_2}m$. Logo,

$$\varphi(n) = \varphi(p_1^{r_1})\varphi(m) \geq \frac{(p_1-1)}{p_1} \cdot p^{r_1} \cdot \frac{(p_k-1)}{p_2} \cdot m \geq \frac{(p_1-1)}{p_1} \cdot \frac{(p_k-1)}{p_1-1} \cdot n = \frac{q-1}{p}n,$$

como desejado. □

Agora estamos interessados em limitar o valor de $\psi(G)$, onde G é um produto semi-direto de um p-grupo cíclico por um p'-grupo F (ou seja, $mdc(p, |F|) = 1$). Precisaremos do seguinte teorema que fala sobre a ação de F sobre P.

Teorema 2.2.1 ([Gor80], Teorema 5.2.4)**.** *Se A é um p'-grupo de automorfismos do p-grupo abeliano P, o qual age trivialmente sobre $\Omega_1(P) := \{g \in P \mid g^p = 1\}$, i.e., A age trivialmente sobre o conjunto dos elementos de ordem p em P, então $A = 1$.*

Em geral, dado um p-grupo P, podemos definir os subgrupos $\Omega_i(P) := \langle\{g \in P \mid g^{p^i} = 1\}\rangle$. Observe que para o caso em que P é abeliano, como no teorema anterior, temos que $\Omega_i(P) = \{g \in P \mid g^{p^i} = 1\}$.

Agora podemos enunciar e demonstrar o seguinte lema nos diz um pouco sobre o valor $\psi(G)$ sendo G um produto semidireto específico.

Lema 2.2.3. *Seja G um grupo finito satisfazendo $G = P \rtimes F$, onde P é um p-grupo cíclico finito para algum primo p, F é não-trivial e $(p, |F|) = 1$. Então:*

(*i*) *Cada elemento de F age sobre P ou trivialmente ou livre de ponto fixo.*

(*ii*) *Se $x \in F$ com $o(x) = m$ e $u \in P$, então m é o menor inteiro positivo tal que $(ux)^m \in P$.*

(*iii*) *Se* $u \in P$ *e* $x \in C_F(P)$, *então* $o(ux) = o(u)o(x)$.

(*iv*) *Se* $u \in P$ *e* $x \in F \backslash C_F(P)$, *então* $o(ux) = o(x)$.

(*v*) *Seja* $Z = C_F(P)$. *Então*

$$\psi(G) = \psi(P)\psi(Z) + |P|\psi(F \backslash Z) < \psi(P)\psi(Z) + |P|\psi(F).$$

Demonstração.

(*i*) Suponha que $x \in F$ age trivialmente sobre $u \in P \backslash \{1\}$. Então x age trivialmente sobre o subgrupo $\langle u \rangle$. Como $u \neq 1$, temos $p \leq |\langle u \rangle|$ e, portanto, $\Omega_1(P) \leq \langle u \rangle$, ou seja, x age trivialmente sobre todos os elementos de ordem p em P. Portanto, pelo Teorema 2.2.1, x age trivialmente sobre P.

(*ii*) Inicialmente, mostraremos que se n é um inteiro positivo, então $(ux)^n = v_n x^n$ para algum $v_n \in P$. Para isto, usaremos indução sobre n. Para $n = 1$, $v_n = u$ e o resultado é trivial. Agora, suponha que $(ux)^{n-1} = v_{n-1}x^{n-1}$ para algum $v_{n-1} \in P$. Como P é normal em G, temos que $x^{n-1}ux^{-(n-1)} = u'$ para algum $u' \in P$, ou seja, $x^{n-1}u = u'x^{n-1}$. Logo,

$$(ux)^n = (ux)^{n-1}ux = v_{n-1}x^{n-1}ux = v_{n-1}u'x^{n-1}x = v_n x^n,$$

onde $v_n = v_{n-1}u' \in P$ e segue o desejado. Agora se $(ux)^n \in P$, então $x^n \in P$. Como $x^n \in F \cap P = \{1\}$, temos que $x^n = 1$ e portanto m divide n.

(*iii*) Segue diretamente do fato que u e x comutam e possuem ordens coprimas, e portanto $o(ux) = o(u)o(x)$.

iv) Suponha que $o(x) = m$. Pelo item (*ii*), $(ux)^m \in P$. Assim,

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

Como $x \in F\backslash C_F(P)$, pelo item (i), segue que x age sobre P livre de ponto fixo e, portanto, $(ux)^m = 1$. Logo, por (ii), $o(ux) = m = o(x)$.

$v)$ Temos que $G = PZ \cup P(F\backslash Z)$ é uma união disjunta, e assim $\psi(G) = \psi(PZ) + \psi(P(F\backslash Z))$. Agora por (iii), $\psi(PZ) = \psi(P)\psi(Z)$, e por $iv)$, $\psi(P(F\backslash Z)) = |P|\psi(F\backslash Z)$. Portanto,

$$\psi(G) = \psi(P)\psi(Z) + |P|\psi(F\backslash Z) < \psi(P)\psi(Z) + |P|\psi(F).$$

□

Agora podemos enunciar e provar o nosso segundo resultado principal desta seção, o Teorema B, o qual será utilizado na demonstração do nosso resultado principal. Aqui o Teorema de Schur-Zassenhaus (Teorema 1.4.1) será necessário.

Teorema B. *Seja G um grupo finito não-cíclico de ordem n e seja q o menor divisor primo de n. Então*

$$\psi(G) < \frac{1}{q-1}\psi(C_n).$$

Demonstração. Devemos mostrar que se $\psi(G) \geq \dfrac{1}{q-1}\psi(C_n)$, então $G \cong C_n$. Inicialmente, temos que $\psi(C_n) \geq 1 + n\varphi(n) > n\varphi(n)$. Assim, pelo Lema 2.2.2 ,

$$\psi(G) \geq \frac{1}{q-1}\psi(C_n) > \frac{(q-1)n^2}{(q-1)p} = \frac{n^2}{p},$$

o que implica que existe $x \in G$ com $o(x) > n/p$. Logo $|G : \langle x\rangle| < p$ e $\langle x\rangle$ contém um p-subgrupo de Sylow P de G. Como $\langle x\rangle \leq N_G(P)$, temos que

$$|G : N_G(P)| \leq |G : \langle x\rangle| < p.$$

Pelo Segundo Teorema de Sylow (veja Teorema 1.1.2), $|G : N_G(P)| \equiv 1 \pmod p$, e portanto $|G : N_G(P)| = 1$. Assim, segue que P é um subgrupo normal cíclico de G e pelo Corolário 2.1.2, temos

$$\psi(P)\psi(G/P) \geq \psi(G) \geq \frac{1}{q-1}\psi(C_n) = \frac{1}{q-1}\psi(C_{p^r})\psi(C_{n/p^r}),$$

onde $p^r = |P|$. Como P é cíclico, $P \cong C_{p^r}$, temos que $\psi(P) = \psi(C_{p^r})$ e, assim,

$$\psi(G/P) \geq \frac{1}{q-1}\psi(C_{n/p^r}).$$

Se $n = p^r$ com p primo, então a existência de $x \in G$ com $o(x) > n/p = p^{r-1}$ implica que $o(x) = n$ e, portanto, G é cíclico, como desejado. Assim, podemos supor que n é divisível por exatamente k primos distintos com $k > 1$. Aplicando indução sobre k, podemos supor que o resultado é verdadeiro para todo grupo de ordem com menos que k divisores primos distintos. Como $|G/P|$ tem $k-1$ divisores primos distintos e G/P satisfaz a nossa hipótese, segue que G/P é cíclico. Agora, como $(|P|, |G/P|) = 1$, temos, pelo Teorema de Schur-Zassenhaus, Teorema 1.4.1, que existe um subgrupo F de G tal que $F \cong G/P$, F não-trivial e $G = P \rtimes F$. Note que $n = |P||F|$ e P e F são cíclicos de ordens coprimas, e portanto

$$\psi(C_n) = \psi(P \times F) = \psi(P)\psi(F).$$

Se $C_F(P) = \{z \in F \mid zx = xz \text{ para todo } x \in P\} = F$, ou seja, todos os elementos de P comutam com os elementos de F, então $G = P \times F$. Neste caso, G é o produto direto de dois grupos cíclicos de ordens coprimas, e portanto G é cíclico, como desejado. Logo é suficiente provar o teorema para o caso em que $Z := C_F(P) \lneq F$ é um subgrupo próprio de F. Pelo Lema 2.2.3 (item (v)),

$$\psi(G) < \psi(P)\psi(Z) + |P|\psi(F) = \psi(P)\psi(F)\left(\frac{\psi(Z)}{\psi(F)} + \frac{|P|}{\psi(P)}\right).$$

Logo,

$$\psi(G) < \psi(C_n)\left(\frac{\psi(Z)}{\psi(F)} + \frac{|P|}{\psi(P)}\right).$$

Como P é um p-grupo cíclico, temos que

$$\frac{|P|}{\psi(P)} = \frac{|P|(p+1)}{p|P|^2+1} < \frac{|P|(p+1)}{p|P|^2} = \frac{p+1}{p|P|} \leq \frac{p+1}{p^2} < \frac{p+1}{p^2-1} = \frac{1}{p-1} \leq \frac{1}{q}.$$

Note que Z é um subgrupo próprio de F e F é o produto direto de seus subgrupos de Sylow. Temos também que Z é o produto direto de seus subgrupos de Sylow; em

particular, existe um r-subgrupo de Sylow R_Z de Z tal que $R_Z \lneq R_F$, digamos $|R_F| = r^s$. Note também que

$$\psi(R_F) = \prod_{i=1}^{k-1} \psi(R_{F_i}) \quad \text{e} \quad \psi(Z) = \prod_{i=1}^{k-1} \psi(R_{Z_i})$$

e além disso

$$\frac{\psi(R_{Z_i})}{\psi(R_{F_i})} \leq 1$$

para todo $1 \leq i \leq k-1$. Logo,

$$\frac{\psi(Z)}{\psi(F)} = \frac{\psi(R_{Z_1})}{\psi(R_{F_1})} \cdots \frac{\psi(R_{Z_{k-1}})}{\psi(R_{F_{k-1}})} \leq \frac{\psi(R_Z)}{\psi(R_F)}.$$

Como $1 \leq s, q \leq r$ e R_Z e R_F são r-grupos cíclicos, pelo Lema 2.2.1, obtemos que

$$\frac{\psi(R_Z)}{\psi(R_F)} = \frac{\frac{|R_Z|^2 r+1}{r+1}}{\frac{|R_F|^2 r+1}{r+1}} = \frac{|R_Z|^2 r+1}{|R_F|^2 r+1} \leq \frac{r^{2(s-1)+1}+1}{r^{2s+1}+1} < \frac{1}{q(q-1)}.$$

Portanto, temos que

$$\begin{aligned} \psi(G) &< \psi(C_n)\left(\frac{\psi(Z)}{\psi(F)} + \frac{|P|}{\psi(P)}\right) \\ &< \psi(C_n)\left(\frac{1}{q(q-1)} + \frac{1}{q}\right) = \frac{1}{q-1}\psi(C_n), \end{aligned}$$

o que é uma contradição. Assim, concluímos o teorema. □

Observe que para grupos de ordem par, temos que $q = 2$ e $\psi(G) < \psi(C_n)$, como mostrado anteriormente no Teorema I. Agora para grupos de ordem ímpar, $q \geq 3$, e podemos melhorar o resultado do Teorema I com o Teorema B.

Corolário 2.2.2. *Seja G um grupo não-cíclico de ordem ímpar n. Então*

$$\psi(G) < \frac{1}{2}\psi(C_n).$$

Demonstração. De fato, como n é ímpar temos que o menor divisor primo q de n é maior

ou igual a 3. Assim $2 \leq q-1$ e, portanto,

$$\psi(G) < \frac{1}{q-1}\psi(C_n) \leq \frac{1}{2}\psi(C_n).$$

□

Agora podemos demonstrar o Teorema A.

Teorema A. *Se G é um grupo finito não-cíclico de ordem n, então*

$$\psi(G) \leq \frac{7}{11}\psi(C_n).$$

Demonstração. Vamos demonstrar por contradição. Para isto suponha que G é um grupo não-cíclico de ordem n satisfazendo

$$\psi(G) > \frac{7}{11}\psi(C_n).$$

Sejam $p_1 < p_2 < \cdots < p_t = p$ os divisores primos de n e denote por $P_1, P_2, ..., P_t$ os respectivos subgrupos de Sylow de C_n. Agora, pelo Lema 2.2.1, $\psi(C_n) \geq \frac{2}{p+1}n^2$ e, portanto, por hipótese de contradição,

$$\psi(G) > \frac{7}{11}\psi(C_n) \geq \frac{14}{11(p+1)}n^2.$$

Agora usaremos indução sobre p a fim de chegar numa contradição. Note que existe $x \in G$ tal que $o(x) > \frac{14}{11(p+1)}n$, caso contrário teríamos que

$$\psi(G) \leq n \cdot \frac{14}{11(p+1)}n = \frac{14}{11(p+1)}n^2,$$

uma contradição. Desta forma, temos que

$$|G : \langle x\rangle| = \frac{|G|}{o(x)} < \frac{n}{\frac{14}{11(p+1)}n} < \frac{11}{14}(p+1).$$

Suponha, inicialmente, que $p = 2$. Então G é um 2-grupo e $|G : \langle x\rangle| < \frac{33}{14}$. Como G é

não-cíclico, $|G:\langle x\rangle| \neq 1$ e, portanto, $|G:\langle x\rangle| = 2$. Note que $\langle x\rangle \cong C_{n/2}$ e assim, pelo Lema 2.2.1, $\psi(\langle x\rangle) = \psi(C_{n/2}) = \dfrac{2(n/2)^2+1}{3}$. Logo, como $n \geq 4$ e $n^2 \geq 16$, temos que

$$\begin{aligned}\psi(G) \leq \psi(C_{n/2}) + \left(\frac{n}{2}\right)^2 = \frac{2(n/2)^2+1}{3} + \frac{n^2}{4} &= \frac{5}{12}n^2 + \frac{1}{3} \\ &\leq \frac{7}{11}\frac{2n^2+1}{3} = \frac{7}{11}\psi(C_n),\end{aligned}$$

onde a penúltima desigualdade segue do fato que $\dfrac{5}{12}n^2 + \dfrac{1}{3} \leq \dfrac{7}{11}\dfrac{2n^2+1}{3}$ é equivalente a $165n^2 + 132 \leq 168n^2 + 84$ que é verdadeira pois $16 \leq n^2$. Assim, $\psi(G) \leq \dfrac{7}{11}\psi(C_n)$, uma contradição. Agora, suponha que $p = 3$. Como $p = 3$ é maior divisor primo de n, temos dois casos: $n = 3^b$, i.e., G é um 3-grupo ou $n = 2^a 3^b$. Se G é um 3-grupo, então, pelo Teorema B, temos que

$$\psi(G) < \frac{1}{2}\psi(C_n) < \frac{7}{11}\psi(C_n),$$

que é uma contradição. Então podemos supor que $n = 2^a 3^b$ para alguns a e b inteiros positivos. Note que

$$|G:\langle x\rangle| < \frac{11(3+1)}{14} = \frac{44}{14},$$

donde $|G:\langle x\rangle| \leq 3$. Assim, temos que ou $|G:\langle x\rangle| = 2$ ou $|G:\langle x\rangle| = 3$. Além disso, observe que, para $n = 2^a 3^b$, temos $C_n \cong C_{2^a} \times C_{3^b}$ e, pelo Lema 2.2.1, $C_{2^a} = \dfrac{2^{2a+1}+1}{3}$ e $\psi(C_{3^b}) = \dfrac{3^{2b+1}+1}{4}$ e, portanto, pelo Lema 2.1.1,

$$\begin{aligned}\frac{7}{11}\psi(C_n) &= \frac{7}{11}\psi(C_{2^a})\psi(C_{3^b}) \\ &= \frac{7}{11}\left(\frac{2^{2a+1}+1}{3}\right)\left(\frac{3^{2b+1}+1}{4}\right) \\ &= \frac{7}{22}2^{2a}3^{2b} + \frac{7}{66}2^{2a} + \frac{7}{44}3^{2b} + \frac{7}{132}.\end{aligned}$$

Inicialmente, vamos supor que $|G:\langle x\rangle| = 2$. Desta forma $\langle x\rangle$ contém um 3-subgrupo de Sylow P de G, pois $|\langle x\rangle| = \dfrac{|G|}{2} = 2^{a-1}3^b$. Como $\langle x\rangle \leq N_G(P)$, e assim $|G:N_G(P)| < 3$, logo, pelo Segundo Teorema de Sylow (veja Teorema 1.1.2), segue que P é normal em G.

Se existe $y \in G\backslash\langle x\rangle$ com $|G:\langle y\rangle| = 2$, então $\langle y\rangle$ contém P. Logo $y \in C_G(P)$ e, portanto, $C_G(P) = G$, ou seja, $P \leq Z(G)$. Assim, $G = P \times Q$, onde Q é um 2-subgrupo

de Sylow não-cíclico de G. Pelo caso $p = 2$, temos que $\psi(Q) \leq \frac{7}{11}\psi(C_{|Q|})$, e portanto

$$\begin{aligned}\psi(G) = \psi(P \times Q) &= \psi(P)\psi(Q) \\ &\leq \psi(P)\frac{7}{11}\psi(C_{|Q|}) = \frac{7}{11}\psi(P \times C_{|Q|}) = \frac{7}{11}\psi(C_n),\end{aligned}$$

pois P é cíclico e $\psi(C_n) = \psi(P \times C_{|Q|}) = \psi(P)\psi(C_{|Q|})$ pelo Lema 2.1.1, contrariando a hipótese de contradição $\psi(G) > \frac{7}{11}\psi(C_n)$. Por fim, podemos supor que $o(y) \leq \frac{n}{3}$ para todo $y \in G/\langle x\rangle$. Como $a \geq 1$ e $b \geq 1$, obtemos a seguinte contradição com respeito a $|G : \langle x\rangle| = 2$:

$$\begin{aligned}\psi(G) &\leq \psi(C_{n/2}) + \left(\frac{n}{2}\right)\left(\frac{n}{3}\right) = \psi(C_{2^{a-1}})\psi(C_{3^b}) + \frac{n^2}{6} \\ &= \left(\frac{2^{2a-1}+1}{3}\right)\left(\frac{3^{2b+1}+1}{4}\right) + \frac{(2^a3^b)^2}{6} \\ &= \frac{1}{12}(2^{2a-1}3^{2b+1} + 2^{2a-1} + 3^{2b+1} + 1) + \frac{2^{2a}3^{3^b}}{6} \\ &= \frac{7}{24}2^{2a}3^{2b} + \frac{1}{24}2^{2a} + \frac{1}{4}3^{2b} + \frac{1}{12} \\ &= \frac{7}{22}2^{2a}3^{2b} + \frac{7}{66}2^{2a} + \frac{7}{44}3^{2b} + \frac{7}{132} \\ &\qquad + \left(\frac{7}{24} - \frac{7}{22}\right)2^{2a}3^{2b} + \left(\frac{1}{24} - \frac{7}{66}\right)2^{2a} + \left(\frac{1}{4} - \frac{7}{44}\right)3^{2b} + \left(\frac{11}{132} - \frac{7}{132}\right) \\ &\qquad\qquad \text{(somando e subtraindo } \frac{7}{11}\psi(C_n)) \\ &= \frac{7}{11}\psi(C_n) - \frac{7}{264}2^{2a}3^{2b} - \frac{17}{264}2^{2a} - \frac{3}{2}3^{2b} + \frac{4}{132} \\ &< \frac{7}{11}\psi(C_n) - \frac{7}{264}2^{2a}3^{2b} + \frac{1}{11}3^{2b} + \frac{4}{132} \qquad \text{(usando que } -\frac{17}{264}2^{2a} - \frac{3}{2}3^{2b} < \frac{1}{11}3^{2b}) \\ &\leq \frac{7}{11}\psi(C_n) - \frac{7}{264}2^2 3^{2b} + \frac{1}{11}3^{2b} + \frac{4}{132} \qquad \text{(pois } a \geq 1) \\ &= \frac{7}{11}\psi(C_n) - \frac{7}{66}3^{2b} + \frac{6}{66}3^{2b} + \frac{4}{132} \\ &= \frac{7}{11}\psi(C_n) - \frac{1}{66}3^{2b} + \frac{4}{132} < \frac{7}{11}\psi(C_n) \qquad \text{(pois } -\frac{3^{2b}}{66} + \frac{4}{132} < 0 \text{ para } b \geq 1).\end{aligned}$$

Agora analisaremos o caso $p = 3$ e $|G : \langle x\rangle| = 3$.

Se existe $y \in G$ tal que $o(y) = \frac{n}{2}$, então $|G\colon \langle y\rangle| = 2$ e $\langle y\rangle$ contém um 3-subgrupo de Sylow cíclico P de G. Além disso, $|G\colon N_G(P)| \leq 2$ e, portanto, P é normal em G. Logo,

pelo Corolário 2.1.1 e pelo Lema 2.1.1, temos a seguinte contradição

$$\psi(G) \leq \psi(P)\psi(G/P) \leq \frac{7}{11}\psi(P)\psi(C_{|G/P|}) = \psi(C_n).$$

Assim, como anteriormente, podemos supor que $o(y) \leq \frac{n}{3}$ para todo $y \in G$. Temos $G = \langle x\rangle \cup G\backslash\langle x\rangle$, e assim $\psi(G) = \psi(\langle x\rangle) + \psi(G\backslash\langle x\rangle) \leq \psi(C_{n/3}) + \frac{2n}{3}\frac{n}{3}$. Assim, como $b \geq 1$, obteremos a seguinte contradição:

$$\begin{aligned}
\psi(G) &\leq \psi(C_{2^a})\psi(C_{3^{b-1}}) + 2\left(\frac{n}{3}\right)^2 \\
&= \left(\frac{2^{2a+1}+1}{3}\right)\left(\frac{3^{2b-1}+1}{4}\right) + \frac{2n^2}{9} \\
&= \frac{1}{18}2^{2a}3^{2b} + \frac{1}{6}2^{2a} + \frac{1}{36}3^{2b} + \frac{1}{12} + \frac{2}{9}2^{2a}3^{2b} \\
&= \frac{5}{18}2^{2a}3^{2b} + \frac{1}{6}2^{2a} + \frac{1}{36}3^{2b} + \frac{1}{12} \\
&= \frac{7}{22}2^{2a}3^{2b} + \frac{7}{66}2^{2a} + \frac{7}{44}3^{2b} + \frac{7}{132} \\
&\qquad + \left(\frac{5}{18} - \frac{7}{22}\right)2^{2a}3^{2b} + \left(\frac{1}{6} - \frac{7}{66}\right)2^{2a} + \left(\frac{1}{36} - \frac{7}{44}\right)3^{2b} + \left(\frac{11}{132} - \frac{7}{132}\right) \\
&\qquad\qquad \text{(somando e subtraindo } \frac{7}{11}\psi(C_n)\text{)} \\
&= \frac{7}{11}\psi(C_n) - \frac{4}{99}2^{2a}3^{2b} + \frac{2}{33}2^{2a} - \frac{13}{99}3^{2b} + \frac{1}{33} \\
&< \frac{7}{11}\psi(C_n) - \frac{4}{99}2^{2a}3^{2b} + \frac{2}{33}2^{2a} + \frac{1}{33} \qquad (\text{pois } -\frac{13}{99}3^{2b} < 0) \\
&\leq \frac{7}{11}\psi(C_n) - \frac{4}{99}2^{2a}3^{2} + \frac{2}{33}2^{2a} + \frac{1}{33} \qquad (\text{pois } b \geq 1) \\
&= \frac{7}{11}\psi(C_n) - \frac{36}{99}2^{2a} + \frac{6}{99}2^{2a} + \frac{1}{33} \\
&= \frac{7}{11}\psi(C_n) - \frac{10}{33}2^{2a} + \frac{1}{33} < \frac{7}{11}\psi(C_n) \qquad (\text{pois } -\frac{10}{33}2^{2a} + \frac{1}{33} < 0 \text{ para } a \geq 1).
\end{aligned}$$

Por fim, suponha que $p > 3$ e que o resultado é válido para os valores menores do que p. Então

$$|G : \langle x\rangle| < \frac{11(p+1)}{14} \leq p,$$

onde a última desigualdade é válida pois ela é equivalente a $11p + 11 \leq 14p$ que é válida para qualquer $p > 3$. Assim, $\langle x\rangle$ contém um p-subgrupo de Sylow cíclico P de G. Como $\langle x\rangle \leq N_G(P)$, temos que P é um subgrupo cíclico normal de G, e portanto pelo Corolário

2.1.1,

$$\psi(P)\psi(G/P) \geq \psi(G) > \frac{7}{11}\psi(C_{p^r})\psi(C_{n/p^r}),$$

onde $p^r = |P|$. Como $P \cong C_{p^r}$, temos que $\psi(P) = \psi(C_{p^r})$ e assim

$$\psi(G/P) \geq \frac{7}{11}\psi(C_{n/p^r}).$$

Como o maior divisor primo de $\frac{n}{p^r}$ é menor que p, por hipótese de indução, segue que G/P é cíclico. Agora, pelo Teorema de Schur-Zassenhaus, Teorema 1.4.1, $G = P \rtimes F$ com $F \cong G/P$ e $F \neq 1$. Note que $|F||P| = n$ e sendo ambos P e F cíclicos com $mdc(|P|, |F|) = 1$, temos que $C_n \cong P \times F$ e, portanto, $\psi(C_n) = \psi(P)\psi(F)$.

Agora, se $C_F(P) = F$, então $G = P \times F$ e, portanto, G é cíclico, uma contradição. Assim, suponha que $C_F(P) =: Z \lneq F$ é um subgrupo próprio. Pelo Lema 2.2.3 item (v),

$$\begin{aligned}\psi(G) &< \psi(P)\psi(F)\left(\frac{\psi(Z)}{\psi(F)} + \frac{|P|}{\psi(P)}\right)\\ &= \psi(C_n)\left(\frac{\psi(Z)}{\psi(F)} + \frac{|P|}{\psi(P)}\right)\end{aligned}$$

Por outro lado, Z é um subgrupo próprio do grupo cíclico F e $\psi(F)$ é o produto de $\psi(S)$ onde S percorre os subgrupos de Sylow de F e temos o mesmo para $\psi(Z)$. Segue que ao menos um subgrupo de Sylow de Z, digamos um r-subgrupo de Sylow R_Z, está contido propriamente em um r-subgrupo de Sylow de F de ordem r^s. Note que, $|R_Z| \leq r^{s-1}$ e assim

$$\frac{\psi(Z)}{\psi(F)} \leq \frac{\psi(R_Z)}{\psi(R_F)} = \frac{\frac{r|R_Z|^2+1}{r+1}}{\frac{r|R_F|^2+1}{r+1}} = \frac{r|R_Z|^2+1}{r|R_F|^2+1} \leq \frac{r^{2(s-1)+1}+1}{r^{2s+1}+1}.$$

Como $r \geq 2$ e $s \geq 1$, temos

$$\frac{r^{2(s-1)+1}+1}{r^{2s+1}+1} \leq \frac{1}{r+1},$$

pois essa desigualdade é equivalente a $(r+1)(r^{2s-1}+1) \leq r^{2s+1}+1$, que por sua vez é

equivalente a $1 \leq r^{2s-2}(r^2 - r - 1)$, a qual é verdadeira. Logo

$$\frac{\psi(Z)}{\psi(F)} \leq \frac{1}{r} < \frac{1}{3},$$

e assim

$$\begin{aligned}\psi(G) &< \psi(C_n)\left(\frac{\psi(Z)}{\psi(F)} + \frac{|P|}{\psi(P)}\right) \\ &< \psi(C_n)\left(\frac{1}{3} + \frac{1}{4}\right) = \frac{7}{12}\psi(C_n) < \frac{7}{11}\psi(C_n),\end{aligned}$$

uma contradição. Portanto, a demonstração está completa. □

2.3 Cota inferior para $\psi(G)$

Como vimos anteriormente, Teorema I, a função ψ atinge o seu valor máximo, sobre os grupos de mesma ordem, no grupo cíclico. De modo que os grupos cíclicos são caracterizados pelo valor máximo de $\psi(G)$ sobre os grupos de mesma ordem. Naturalmente podemos ver o que ocorre para o valor mínimo de ψ sobre os grupos de mesma ordem. Os principais resultados desta subseção serão baseados nos artigos **[AA11]** e **[AmiJ13]**.

Começaremos obtendo o valor mínimo de $\psi(G)$ sobre os grupos nilpotentes de mesma ordem. Primeiro vejamos a seguinte definição.

Definição 2.3.1. *O expoente de um grupo finito G é o menor inteiro positivo n tal que $x^n = 1$ para todo $x \in G$. Neste caso, denotamos n por $exp(G)$. Equivalentemente, $exp(G) = mmc(o(x_1), ..., o(x_n))$ é o mínimo múltiplo comum das ordens dos elementos de G.*

Agora podemos obter o valor mínimo de $\psi(G)$ sobre os grupos nilpotentes de mesma ordem.

Teorema 2.3.1 (Teorema A, **[AA11]**)**.** *Seja G um grupo nilpotente de ordem n. Então $\psi(G) \leq \psi(H)$ para todo grupo nilpotente H de ordem n se, e somente se, cada subgrupo de Sylow de G tem expoente primo.*

Demonstração. A demonstração do Teorema 2.3.1 será vista no capítulo seguinte de maneira mais geral. □

Como corolário direto do Teorema 2.3.1 temos o seguinte:

Corolário 2.3.1. *Se G é um grupo finito de ordem $n = p_1^{r_1} \cdots p_k^{r_k}$ e*

$$\psi(G) < \prod_{i=1}^{k} (p_i(p_i^{r_i} - 1) + 1),$$

então G é não-nilpotente.

Outro teorema importante na direção de encontrar o valor mínimo de ψ é o seguinte:

Teorema 2.3.2 (Teorema B, [AA11])**.** *Seja n um inteiro positivo tal que existe um grupo não-nilpotente de ordem n. Então existe um grupo não-nilpotente K de ordem n tal que $\psi(K) < \psi(H)$ para todo grupo nilpotente H de ordem n.*

Em outras palavras, o Teorema 2.3.2 diz que sobre os grupos de ordem n, tal que existe grupo não-nilpotente de ordem n, o valor mínimo de ψ é atingindo em algum grupo não-nilpotente.

Para mostrar o Teorema 2.3.2 usaremos o seguinte lema:

Lema 2.3.1 (Lema 2.4, [AA11])**.** *Seja d um inteiro positivo com a propriedade que se $\min\{\psi(G) \mid |G| = d\} = \psi(K)$ para algum grupo K de ordem d, então K é não-nilpotente. Então $n = ds$ tem a mesma propriedade do inteiro d para qualquer inteiro positivo s com $mdc(d, s) = 1$.*

Demonstração. Seja G um grupo nilpotente de ordem $n = ds$ tal que $\psi(G) = \min\{\psi(H) \mid |H| = n\}$. Então $G \cong H' \times U$, onde $|H'| = d$ e $\psi(H')$ é mínimo sobre o conjunto dos grupos nilpotentes de ordem d. Por hipótese, existe um grupo não-nilpotente K de ordem d tal que $\psi(K) < \psi(H')$. Agora, tome $S = K \times U$, então $|S| = |G| = n$ e S é não-nilpotente. Como $mdc(|H'|, |U|) = 1$, pelo Lema 2.1.1 temos que

$$\psi(S) = \psi(K)\psi(U) < \psi(H')\psi(U) = \psi(H' \times U) = \psi(G).$$

□

Para demonstrarmos o Teorema 2.3.2 precisaremos também do seguinte resultado devido a Jonathan Pakianathan e Krishnan Shankar:

Teorema 2.3.3. *(Teorema 1, [PS00]) Seja $n = p_1^{a_1} \cdots p_t^{a_t}$ um inteiro positivo, onde os $p_i's$ são primos distintos. Então todos os grupos de ordem n são nilpotentes se, e somente se, $p_i^k \not\equiv 1 \pmod{p_j}$ para todos inteiros i, j e k com $1 \leq k \leq a_i$.*

Um número com tal propriedade é dito um **número nilpotente**.

Agora podemos demonstrar o Teorema 2.3.2.

Demonstração do Teorema 2.3.2.

Primeiro, note que pelo Teorema 2.3.3, existe um grupo não-nilpotente G de ordem n e existem dois divisores primos distintos p e q de n e um inteiro positivo i tais que $p \mid (q^i - 1)$, mas $p \nmid (p^j - 1)$ para todo inteiro positivo $j < i$. Suponha que $n = p^m q^r k$, onde $mdc(pq, k) = 1$. Como $|Aut(C_q^i)| = (q^i - 1)(q^i - q) \cdots (q^i - q^{i-1})$, então existe $\phi \in Aut(C_q^i)$ tal que $o(\phi) = p$, pois $p \mid (q^i - 1)$. Seja $\Phi : C_p \to Aut(C_q^i)$ o homomorfismo de grupos dado por $\Phi(a) = \phi$, onde a é um gerador de C_p. O produto semidireto de C_p e C_q^i com respeito ao homomorfismo Φ, que será denotado por $C_p \ltimes C_q^i$, é um grupo não-nilpotente de ordem pq^i. Note que, por hipótese, $p \mid (q^i - 1)$ e $p \nmid q^j$, e portanto $n_p = q^i$, ou seja, $C_p \ltimes C_q^i$ possui q^i p-subgrupos de Sylow. Portanto, o número de elementos de ordens p e q em $C_p \ltimes C_q^i$ são $q^i(p-1)$ e $q^i - 1$, respectivamente, e portanto $C_p \ltimes C_q^i$ não possui outros elementos. Defina agora o grupo $T := \left(C_p \ltimes C_q^i\right) \times C_p^{m-1} \times C_q^{r-i}$. Temos, então, que T é um grupo não-nilpotente de ordem $p^m q^r$, pois $C_p \ltimes C_q^i$ é isomorfo a um subgrupo de T. Além disso, como $C_p \ltimes C_q^i$ possui $q^i(p-1)$ elementos de ordem p e $q^i - 1$ elementos de ordem q, temos que:

- o nº de elementos de ordem p em T é: $q^i(p-1)p^{m-1} + p^{m-1} - 1$,
- o nº de elementos de ordem q em T é: $(q^i - 1)q^{r-i} + q^{r-i} - 1 = q^r - 1$,
- o nº de elementos de ordem pq em T é: $p^m q^r - q^i p^m + q^i p^m + q^i p^{m-1} - p^{m-1} + 1 - q^r$.

Logo, como $\psi(C_p^m \times C_q^r) = \psi(C_p^m)\psi(C_q^r)$ pelo Lema 2.1.1, temos que

$$\begin{aligned}\psi(C_p^m \times C_q^r) - \psi(T) &= \psi(C_p^m)\psi(C_q^r) - \psi(T)\\ &= ((p^m-1)p+1)((q^r-1)q+1) - \psi(T)\\ &= ((p^m-1)p+1)((q^r-1)q+1)\\ &\quad - (1+p(q^i(p-1)p^{m-1}+p^{m-1}-1)+q(q^r-1)\\ &\quad + pq(p^mq^r - q^ip^m + q^ip^m + q^ip^{m-1} - p^{m-1} + 1 - q^r))\\ &= p^m(p-1)(q-1)(q^i-1) > 0.\end{aligned}$$

Note que os subgrupos de Sylow de $C_p^m \times C_q^r$ possuem expoentes primos e, portanto, pelo Lema 2.3.1, têm o menor $\psi(G)$ sobre todos os grupos nilpotentes de ordem $d = p^mq^r$. Logo, o inteiro $d = p^mq^r$ possui a propriedade que se $\min\{\psi(M) \mid |M| = d\} = \psi(K)$ para algum grupo K de ordem n, então K é não-nilpotente. Agora, aplicando o Lema 2.3.1, concluímos a demonstração. □

O problema do valor mínimo de $\psi(G)$ para grupos de ordem n também foi investigado em relação a grupos simples não-abelianos. S.M. Jafarian Amiri, em **[AmiJ13]**, deu uma caracterização de A_5 mostrando que $\psi(A_5)$ é o único valor mínimo sobre $\psi(G)$ para grupos de ordem 60, mais precisamente:

Teorema 2.3.4 (**[AmiJ13]**, Teorema 2.1)**.** *Seja G um grupo de ordem* 60*. Então $\psi(G) \geq 211$ e $\psi(G) = 211$ se, e somente se, $G \cong A_5$.*

Demonstração. Inicialmente, podemos calcular $\psi(A_5) = 211$; a saber, A_5 possui 15 elementos de ordem 2, 20 elementos de ordem 3 e 24 elementos de ordem 5. Agora, seja G um grupo de ordem 60. Pelo Teorema de Sylow (veja Teorema 1.1.2), temos que $n_3 = 1$ ou $n_3 = 10$ e $n_5 = 1$ ou $n_5 = 6$ onde n_p denota o número de p-subgrupos de Sylow de G. Se $n_3 = 1$ ou $n_5 = 1$, então G contém um subgrupo de ordem 15, o qual é cíclico. Assim, G possui pelo menos $\varphi(15) = 8$ elementos de ordem 15; $\varphi(5) = 4$ elementos de ordem 5 e $\varphi(3) = 2$ elementos de ordem 3. Assim, G contém no máximo 45 elementos de ordem 2. Portanto,

$$\psi(G) \geq 1 + 45(2) + 2(3) + 4(5) + 8(15) = 237.$$

Assim podemos supor que $n_3 = 6$ e $n_5 = 6$. Logo G contém 20 elementos de ordem 3 e 24 elementos de ordem 5. Defina $I := \{x \in G \mid o(x) = 3 \text{ ou } o(x) = 5\}$, e temos que $|I| = 44$. Note que se existe um elemento em $G\backslash I$ de ordem maior que 2, então

$$\psi(G) > 1 + 20(3) + 24(5) + 15(2) = 211.$$

Assim, podemos supor que cada elemento não-identidade x em $G\backslash I$ tem ordem 2. Observe que $C_G(x)$ não possui um elemento y de ordem 3 ou 5, caso contrário, como x e y comutam, $o(xy) = 6$ ou $o(xy) = 10$, seria uma contradição. Logo, $|C_G(x)| = 2$ ou 4. Por fim, como $x \in C_G(x) \leq P_2$, para algum 2-subgrupo de Sylow P_2 de G, e P_2 é abeliano, segue que $C_2(x) = P_2 \cong C_2 \times C_2$ para todo elemento x de ordem 2. Disto segue que a interseção de dois 2-subgrupos de Sylow distintos de G é trivial, e portanto $n_2 = 5$. Portanto, G é isomorfo a um subgrupo de ordem 60 de S_5 e segue que $G \cong A_5$. □

E como consequência direta do Teorema 2.3.4:

Corolário 2.3.2. *Se G é um grupo não-simples de ordem 60, então $\psi(G) > \psi(A_5)$.*

No mesmo artigo **[AmiJ13]** S.M. Jafarian Amiri também mostrou que $PSL(2,7)$, o grupo linear projetivo especial, também é caracterizado pela soma das ordens de seus elementos. Mais ainda, temos para os seis grupos simples não-abelianos de menores ordens:

$$\begin{aligned}
A_5 \text{ possui ordem } 60 \quad &\text{e} \quad \psi(A_5) = 211;\\
PSL(2,7) \text{ possui ordem } 168 \quad &\text{e} \quad \psi(PSL(2,7)) = 715;\\
A_6 \text{ possui ordem } 360 \quad &\text{e} \quad \psi(A_6) = 1411;\\
PSL(2,8) \text{ possui ordem } 504 \quad &\text{e} \quad \psi(PSL(2,8)) = 3319;\\
PSL(2,11) \text{ possui ordem } 660 \quad &\text{e} \quad \psi(PSL(2,11)) = 3741;\\
PSL(2,13) \text{ possui ordem } 1092 \quad &\text{e} \quad \psi(PSL(2,7)) = 7281.
\end{aligned}$$

Utilizando o `GAP`, **[GAP]**, podemos verificar que em todos esses casos, o valor $\psi(G)$ desses grupos é o único valor mínimo de $\psi(G)$ sobre todos os grupos das ordens correspondentes.

A partir dessas observações, naturalmente, têm-se algumas perguntas:

Pergunta 1. *Se S é um grupo simples de ordem n, então $\psi(S)$ é o valor mínimo de $\psi(G)$ para grupos de ordem n?*

A resposta é "não". Por exemplo, existem dois grupos simples de ordem 20160*: A_8 e $PSL(3,4)$. Porém, $\psi(A_8) = 137047$ enquanto que $\psi(PSL(3,4)) = 103111$. Logo, $\psi(A_8) = 137047$ não é mínimo.*

Podemos adaptar a pergunta anterior para a seguinte, como foi conjecturado em [AmiJ13]:

Pergunta 2 (Conjectura 1.5, [AmiJ13])**.** *Se S é um grupo simples finito e G é um grupo não-simples tal que $|G| = |S|$, então $\psi(S) < \psi(G)$?*

Neste caso, a resposta também é "não"! Em 2013, Y. Marefat, A. Iranmanesh e A. Tehranian, em [MIT13], deram o seguinte contraexemplo: Seja $S_z(8)$ o grupo de Suzuki, o qual é um grupo simples de ordem 29120*. Temos que o grupo linear especial projetivo $PSL(2,64)$ é um grupo simples de ordem* 262080*. Agora considere $S = PSL(2,64)$ e $G = C_3^2 \times S_z(8)$. Temos que G é um grupo não-simples, S é simples e $|G| = |S|$. Por outro lado, $\psi(G) = 5482775$ e $\psi(S) = 12106687$, ou seja, $\psi(G) < \psi(S)$. Logo, a conjectura é falsa.*

Por fim, encerramos esta seção adaptando as perguntas anteriores como a seguinte que foi conjecturada em [HLM18b].

Pergunta 3 (Conjectura 4.6.5, [HLM18b])**.** *Sejam S um grupo simples e G um grupo solúvel tal que $|G| = |S|$. Então*

$$\psi(S) < \psi(G)?$$

A resposta também é "não". M. Jahani, Y. Marefat, H. Refaghat e B. V. Fasaghandisi, em [Mar19], construíram alguns contraexemplos para tal conjectura. Por exemplo, usando a biblioteca do `GAP`*, [GAP], consideremos $H := SmallGroup(780,16)$ e $K := SmallGroup(336,218)$, temos que $G = H \times K$ é um grupo solúvel de ordem* 262080*. Além disso, $S = PSL(2,64)$ é um grupo simples cuja ordem também é* 262080*, porém*

$$\psi(H \times K) = 11385563 \qquad e \qquad \psi(PSL(2,64)) = 12106687,$$

ou seja, $\psi(G) < \psi(S)$, que nos dá um contraexemplo para a conjectura.

2.4 Alguns resultados sobre solubilidade

Vimos anteriormente que, M. Herzog, P. Longobardi e M. Maj, em [HLM18a], mostraram que para grupos não-cíclicos de ordem n vale que

$$\psi(G) < \frac{1}{q-1}\psi(C_n),$$

onde q é o menor divisor primo de n. Outro problema também abordado em [HLM18a] foi o seguinte: o que podemos dizer sobre os grupos (não-cíclicos) que satisfazem

$$\psi(G) \geq \frac{1}{q}\psi(C_n)?$$

Note que existem grupos não-cíclicos satisfazendo tal propriedade. Por exemplo,

$$\psi(S_3) = 13 > \frac{1}{2}\psi(C_6) = \frac{21}{2}.$$

Em particular, para um inteiro positivo m tal que $mdc(6, m) = 1$, temos que

$$\psi(S_3 \times C_m) > \frac{1}{2}\psi(C_{6m}).$$

Veja, também, que como $q \geq 2$, temos que $2q - 2 \geq q$ e, portanto,

$$\frac{1}{2(q-1)} \leq \frac{1}{q}.$$

Agora, podemos abordar um caso mais geral que é: quais são os grupos que satisfazem

$$\psi(G) \geq \frac{1}{2(q-1)}\psi(C_n)?$$

Para isto comecemos com o seguinte resultado:

Proposição 2.4.1 (Proposição 2.4, [HLM18a]). *Seja G um grupo finito com um sub-*

grupo maximal cíclico C. Então G é solúvel e $G'' \leq Z(G)$.

Demonstração. Pelo Teorema de Herstein, Teorema 1.2.5, temos que G é solúvel. Agora se $G' \leq C$, então G' é abeliano e, portanto, $G'' = 1 \leq Z(G)$. Assim podemos supor que G' não está contido em C. Logo $G = G'C$. Observe que $G'' \leq C$, pois caso contrário teríamos que $G = G''C$ e, assim, $G' \leq G''$, contradizendo o fato de G ser solúvel e $G' \neq 1$. Logo G'' é cíclico. Agora, pelo Teorema 1.1.1, $G/C_G(G'')$ é isomorfo a um subgrupo de $Aut(G'')$ o qual é abeliano, e segue que $G/C_G(G'')$ é abeliano e, portanto pela Proposição 1.2.2, $G' \leq C_G(G'')$. Além disso, temos que $C \leq C_G(G'')$. Por fim, $G = G''C \leq C_G(G'')$, i.e., $G'' \leq Z(G)$. □

Outro resultado que será útil é o seguinte:

Proposição 2.4.2 (Proposição 2.5, [HLM18a]). *Seja G um grupo finito e suponha que existe um elemento $x \in G$ tal que*

$$|G : \langle x \rangle| < 2p,$$

onde p é o maior divisor primo de $|G|$. Então uma das seguintes afirmações é satisfeita:

(i) G possui um p-subgrupo de Sylow cíclico normal.

(ii) G é solúvel e $\langle x \rangle$ é um subgrupo maximal de índice ou p ou $p+1$.

Demonstração. Primeiro, suponha que p divide $|G : \langle x \rangle|$. Como $|G : \langle x \rangle|$ divide $|G|$ e $|G : \langle x \rangle| < 2p$, temos que $|G : \langle x \rangle| = p$. Logo $\langle x \rangle$ é maximal em G e, pela Proposição 2.4.1, G é solúvel. Assim, G satisfaz $ii)$.

Agora suponha que p não divide $|G : \langle x \rangle|$. Assim $\langle x \rangle$ contém um p-subgrupo de Sylow cíclico P de G. Se P é normal em G, então $i)$ é satisfeita. Suponha, então, que P não é normal em G. Como $\langle x \rangle \leq N_G(P)$, segue que $|G : N_G(P)| < 2p$. Assim, como P não é normal em G, pelo Teorema de Sylow (veja Teorema 1.1.2), temos que $|G : N_G(P)| = p+1$ e que $N_G(P)$ é um subgrupo maximal de G. Mas

$$|N_G(P) : \langle x \rangle| = \frac{|G : \langle x \rangle|}{|G : N_G(P)|} < \frac{2p}{p+1} < 2,$$

e assim $N_G(P) = \langle x \rangle$. Logo $\langle x \rangle$ é um subgrupo maximal cíclico de índice $p+1$. Portanto, pela Proposição 2.4.1, G é solúvel e $ii)$ é satisfeita. □

Para darmos uma classificação para os grupos satisfazendo

$$\psi(G) \geq \frac{1}{2(q-1)}\psi(C_n),$$

daremos a seguinte definição.

Definição 2.4.1. *Sejam G um grupo finito e P um p-subgrupo de Sylow de G. Se existe um subgrupo normal N de G tal que $G = PN$ e $P \cap N = 1$, então dizemos que G é um grupo p-**nilpotente** e, neste caso, N é dito um p-complemento de G.*

Por exemplo, $G = S_3$ é 2-nilpotente. De fato, $\langle (1\ 2) \rangle$ é um 2-subgrupo de Sylow de G e $\langle (1\ 2\ 3) \rangle \trianglelefteq G$ são tais que $\langle (1\ 2\ 3) \rangle \cap \langle (1\ 2) \rangle = 1$ e $G = \langle (1\ 2) \rangle \langle (1\ 2\ 3) \rangle$. Observe que S_3 não é 3-nilpotente pois S_3 não possui subgrupo normal de ordem 2.

Em geral, qualquer grupo nilpotente finito G é p-nilpotente para todo divisor primo p de $|G|$. Reciprocamente, se um grupo finito G é p-nilpotente para todo divisor primo p de $|G|$, então G é nilpotente.

Agora enunciaremos dois resultados cujas suas demonstrações podem ser vistas em [Rob93]. O primeiro é o seguinte teorema devido a Burnside:

Teorema 2.4.1 (Teorema 10.1.8, [Rob93])**.** *Sejam G um grupo finito e P um p-subgrupo de Sylow P de G. Se $N_G(P) = C_G(P)$, então G é p-nilpotente.*

O segundo resultado é o seguinte teorema:

Teorema 2.4.2 (Teorema 10.1.9, [Rob93])**.** *Sejam G um grupo finito e q o menor divisor primo de $|G|$. Suponha que G não é q-nilpotente. Então os q-subgrupos de Sylow de G não são cíclicos.*

Agora podemos enunciar e demonstrar o teorema principal desta subseção:

Teorema 2.4.3 (Teorema 6, [HLM18a])**.** *Seja G um grupo finito de ordem n e sejam q e p o menor e o maior divisores primos de n, respectivamente. Suponha que G satisfaz*

$$\psi(G) \geq \frac{1}{2(q-1)}\psi(C_n).$$

Então G é solúvel, os p-subgrupos de Sylow de G contém um subgrupo cíclico de índice p e uma das seguintes afirmações é satisfeita:

(*i*) *O p-subgrupo de Sylow P de G é cíclico e normal em G.*

(*ii*) *Os q-subgrupos de Sylow de G são cíclicos, G é q-nilpotente e $G'' \leq Z(G)$.*

(*iii*) *Os p-subgrupos de Sylow de G são cíclicos, G é p-nilpotente e $G'' \leq Z(G)$.*

Demonstração. Como $\psi(C_n) \geq 1 + n\varphi(n) > n\varphi(n)$ e pelo Lema 2.2.2, $\varphi(n) \geq \dfrac{(q-1)n}{p}$, segue, por hipótese, que

$$\psi(G) \geq \frac{1}{2(q-1)}\psi(C_n) > \frac{n}{2(q-1)} \cdot \frac{(q-1)n}{p} = \frac{n^2}{2p},$$

isto é, $\psi(G) > \dfrac{n^2}{2p}$. Logo, existe um elemento $x \in G$ tal que $o(x) > \dfrac{n}{2p}$. De fato, se $o(y) \leq \dfrac{n}{2p}$ para todo $y \in G$, então $\psi(G) \leq n \cdot \dfrac{n}{2p} = \dfrac{n^2}{2p}$, uma contradição. Assim, $\langle x \rangle$ é tal que $|G : \langle x \rangle| < 2p$.

Inicialmente mostraremos que G é solúvel. Seja k o número de divisores primos distintos de $|G|$. Mostraremos por indução sobre k. Se $k = 1$, então G é um p-grupo e, portanto, G é solúvel. Assim, podemos supor que $k > 1$ e que o resultado é verdadeiro para todos os grupos com ordem divisível por menos que k primos.

Suponha que p divide $|G : \langle x \rangle|$. Como $|G : \langle x \rangle| < 2p$, temos que $|G : \langle x \rangle| = p$ e $\langle x \rangle$ é um subgrupo maximal cíclico de G. Logo, pelo Teorema 1.2.5, G é solúvel.

Suponha, agora, que p não divide $|G : \langle x \rangle|$. Neste caso, $\langle x \rangle$ contém um p-subgrupo de Sylow cíclico P de G. Se P é normal em G, então, pelo Corolário 2.1.1,

$$\psi(P)\psi(G/P) \geq \psi(G) \geq \frac{1}{2(q-1)}\psi(C_{|P|})\psi(C_{|G/P|}).$$

Como P é cíclico, $\psi(P) = \psi(C_{|P|})$ e, portanto,

$$\psi(G/P) \geq \frac{1}{2(q-1)}\psi(C_{|G/P|}).$$

Logo, como $|G/P|$ tem $k-1$ divisores primos, segue, por hipótese de indução, que G/P

é solúvel. Sendo P e G/P solúveis, temos que G é solúvel. Por fim, suponha que P não é normal em G. Como $\langle x\rangle \leq N_G(P)$, segue que $|G : N_G(P)| < 2p$ e, portanto, $|G : N_G(P)| = p+1$. Como

$$|N_G(P) : \langle x\rangle| = \frac{|G : \langle x\rangle|}{|G : N_G(P)|} < \frac{2p}{p+1} < 2,$$

temos que $|N_G(P) : \langle x\rangle| = 1$, ou seja, $N_G(P) = \langle x\rangle$ é um subgrupo maximal cíclico de G. Portanto, G é solúvel.

Agora mostremos que os p-subgrupos de Sylow de G contém um subgrupo cíclico de índice p. Como mostrado no início da demonstração, existe um elemento $x \in G$ tal que $|G : \langle x\rangle| < 2p$. Pela Proposição 2.4.2, temos que ou G possui um p-subgrupo de Sylow cíclico normal, ou $\langle x\rangle$ é um subgrupo maximal de G de índice p ou $p+1$. Em ambos os casos os p-subgrupos de Sylow de G contém um subgrupo cíclico de índice p.

Se G tem um p-subgrupo de Sylow cíclico normal, então a afirmação $i)$ é satisfeita.

Se $\langle x\rangle$ é um subgrupo maximal de G de índice p, então G contém um q-subgrupo de Sylow Q de G. Como Q é cíclico e q é o menor divisor primo de n, segue, pelo Teorema 2.4.2, que G é q-nilpotente. Além disso como $\langle x\rangle$ é um subgrupo maximal de G, segue, pela Proposição 2.4.1, que $G'' \leq Z(G)$. Neste caso, $ii)$ é satisfeita.

Por fim, se $\langle x\rangle$ é um subgrupo maximal de G de índice $p+1$, então $\langle x\rangle$ contém um p-subgrupo de Sylow P de G. Se P é normal em G, então $i)$ é satisfeita. Assim, suponha que P não é normal em G. Como $\langle x\rangle \leq N_G(P)$ e $|G : \langle x\rangle| < 2p$, temos que $|G : N_G(P)| = p+1$. Como antes, $\langle x\rangle = N_G(P)$ e, por $\langle x\rangle \leq C_G(P) \leq N_G(P)$, temos que $N_G(P) = C_G(P)$. Assim, pelo Teorema 2.4.1, G é p-nilpotente e, como $\langle x\rangle$ é maximal, $G'' \leq Z(G)$ e a afirmação $iii)$ é satisfeita, como desejado. □

O Teorema 2.4.3 implica nos seguintes corolários:

Corolário 2.4.1. *As conclusões do Teorema 2.4.3 valem se G satisfaz*

$$\psi(G) \geq \frac{1}{q}\psi(C_n).$$

Demonstração. Como $q \geq 2$, segue que $q \leq 2(q-1)$ e, portanto,

$$\psi(G) \geq \frac{1}{q}\psi(C_n) \geq \frac{1}{2(q-1)}\psi(C_n).$$

□

Corolário 2.4.2. *Seja G um grupo de ordem ímpar. Então as conclusões do Teorema 2.4.3 valem se G satisfaz*

$$\psi(G) \geq \frac{1}{q+1}\psi(C_n).$$

Demonstração. Como $q \geq 3$, segue que $q \leq 2(q-1)$ e, portanto,

$$\psi(G) \geq \frac{1}{q+1}\psi(C_n) \geq \frac{1}{2(q-1)}\psi(C_n).$$

□

Os resultados feitos nesta subseção nos dão condições suficientes, baseadas em $\psi(G)$, para solubilidade de grupos finitos. Outra condição suficiente para solubilidade de grupos finitos dada por **[HLM18a]** é a seguinte:

Teorema 2.4.4 (Teorema 10, **[HLM18a]**)**.** *Seja G um grupo finito de ordem n tal que*

$$\psi(G) \geq \frac{3}{5}n\varphi(n).$$

Então G é solúvel e $G'' \leq Z(G)$.

Vejamos que essa condição não é necessária. Por exemplo, considere o grupo $G = C_2 \times C_2 \times C_2$ de ordem $n = 8$. Temos que G é solúvel com $\psi(G) = 1 + 7 \cdot 2 = 15$, porém

$$\psi(G) = 15 < \frac{3}{5} \cdot 96 = \frac{3}{5}8\varphi(8).$$

Para demonstrar o Teorema 2.4.4 precisaremos do próximo resultado que classifica os p-grupos finitos que possuem um subgrupo maximal cíclico, cuja demonstração por ser vista em **[Rob93]**, Teorema 5.3.4.

Teorema 2.4.5 (Teorema 5.3.4, [Rob93]). *Seja G um p-grupo de ordem p^n. Então G possui um subgrupo maximal cíclico se, e somente se, G é dos seguintes grupos:*

(*i*) $G \cong C_{p^n}$;

(*ii*) $G \cong C_{p^{n-1}} \times C_p$;

(*iii*) $G \cong \langle x, y \mid x^p = 1 = y^{p^{n-1}}, xyx^{-1} = y^{1+p^{n-2}} \rangle$, *para* $n \geq 3$;

(*iv*) $G \cong D_{2^n} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ srs^{-1} = r^{-1} \rangle$, *o grupo diedral de ordem* 2^n;

(*v*) $G \cong Q_{2^n} = \langle r, s \mid r^{2^{n-1}} = 1,\ s^2 = r^{2^{n-2}},\ s^{-1}rs = r^{-1} \rangle$, *o grupo dos quatérnios generalizado de ordem* 2^n, $n \geq 3$;

(*vi*) $G \cong \langle r, s \mid r^2 = 1 = s^{2^{n-1}}, s^r = s^{2^{n-2}-1} \rangle$, *o grupo semidiedral.*

Com a classificação dada no Teorema 2.4.5 podemos mostrar o seguinte resultado, o qual realmente será utilizado no Teorema 2.4.4.

Proposição 2.4.3. *As seguintes afirmações são verdadeiras:*

(*i*) *Se G é um 2-grupo finito com um subgrupo cíclico de índice 4, então $G'' \leq Z(G)$.*

(*ii*) *Se G é um grupo finito de ordem $|G| = 2^\alpha \cdot 3^\beta$ com um subgrupo cíclico de índice menor que 6, então $G'' \leq Z(G)$.*

Demonstração. (*i*) Seja $\langle a \rangle$ é um subgrupo cíclico de índice 4 em G, e seja M um subgrupo maximal de G contendo $\langle a \rangle$. Se $M = \langle a \rangle$, então o resultado segue pela Proposição 2.4.1. Assim, suponha que $\langle a \rangle < M$ é um subgrupo próprio. Como $|G : M| = 2$, temos que M é normal em G e, portanto, pela Proposição 1.2.2, $G' \leq M$ e $G'' \leq M'$. Além disso, $\langle a \rangle$ é um subgrupo maximal de M e, portanto, pelo Teorema 2.4.5, ou M é abeliano, ou $|M'| = 2$ (M do tipo *iii*) do Teorema 2.4.5), ou M é diedral, semidiedral ou os quatérnios generalizados. Observe que se $|M'| \leq 2$, temos que $|G''| \leq |M''| \leq 2$ e, por G'' ser normal em G, segue que $G'' \leq Z(G)$.

Agora, suponha que M é ou diedral, ou semidiedral, ou quatérnios generalizado. Então, afirmamos que existe $x \in M$ tal que $a^x = a^{-1}a^{\gamma 2^{n-1}}$, onde $o(a) = 2^n$, $\gamma \in \{0,1\}$, $o(x) \in \{2,4\}$ e $x^2 \in Z(M)$. De fato, basta considerar

$a = r$ e $x = s$ para o caso de M ser diedral ou semidiedral e, assim,

$$a^x = r^s = r^{-1} = a^{-1} \quad \text{(neste caso } \gamma = 0\text{)};$$

$a = s$ e $x = r$ para o caso de M ser o grupo dos quatérnios generalizado e, assim,

$$a^x = s^r = s^{2^{n-2}-1} = s^{-1}s^{2^{n-1}} = a^{-1}a^{2^{n-1}} \quad \text{(neste caso } \gamma = 1\text{)}.$$

Agora, escreva $G = M\langle y\rangle$, para algum $y \in G\backslash M$. Se $a^y \in \langle a\rangle$, então $\langle a\rangle$ é normal em G. Logo, $G' \leq \langle a\rangle$, pois $|G : \langle a\rangle| = 4$ e assim $G/\langle a\rangle$ é abeliano. Portanto G' é abeliano e $G'' \leq Z(G)$. Suponha, finalmente, que $a^y \notin \langle a\rangle$. Neste caso, como $a^y \in M$, temos que $a^y = a^\delta x$ para algum inteiro δ. Agora

$$\begin{aligned}(a^2)^y = a^\delta x a^\delta x = a^\delta x x (x^{-1}a^\delta x) &= a^\delta x^2 (a^x)^\delta \\ &= a^\delta x^2 (a^{-1}a^{\gamma 2^{n-1}})^\delta \\ &= a^\delta x^2 a^{-\delta} a^{\gamma 2^{n-1}\delta} \\ &= x^2 a^{\gamma 2^{n-1}\delta}, \quad \text{pois } x^2 \in Z(M),\end{aligned}$$

e

$$(a^y)^4 = (a^{\gamma 2^{n-1}\delta}x^2)^2 = a^{\gamma 2^n \delta}x^4 = x^4 = 1,$$

pois $o(a) = 2^n$ e $x^2 = 1$. Logo, temos que $o(a) = o(a^y) = 4$, e portanto $|M| = 8$ e $M' \leq \langle a^2\rangle$. Assim, $G'' \leq M'$ tem ordem no máximo 2, e portanto $G'' \leq Z(G)$.

(ii) Seja $\langle a\rangle$ um subgrupo cíclico de G tal que $|G : \langle a\rangle| < 6$.

Se $|G : \langle a\rangle| = 2$ ou $|G : \langle a\rangle| = 3$, então $\langle a\rangle$ é maximal em G e o resultado segue pela Proposição 2.4.1.

Suponha, finalmente, que $|G : \langle a\rangle| = 4$. Se $\beta = 0$, temos que G é um 2-grupo e

o resultado segue pelo item (i) e se $\langle a\rangle$ é maximal em G, o resultado segue pela Proposição 2.4.1. Assim, suponha $\beta > 0$ e $\langle a\rangle$ não é maximal em G. Então, pela Proposição 2.4.2, G possui um 3-subgrupo de Sylow cíclico normal P. Assim, pelo Teorema de Schur-Zassenhaus (veja Teorema 1.4.1), $G = P \rtimes D$, onde D é um 2-grupo com $|D| = 2^\alpha$. Como $|G : \langle a\rangle| = 4$, temos que $P \leq \langle a\rangle$ e $D \cong G/P$ possui um subgrupo cíclico $\langle a\rangle/P$ de índice 4. Portanto, pelo item (i), $D'' \leq Z(D)$. Agora, como $G = PD$, temos que $G' = D'[P, D]$, e além disso como $G' \leq C_G(P)$, segue que

$$G'' = D'' \leq Z(D) \cap C_G(P) = Z(G),$$

como queríamos.

□

Por último precisaremos também do seguinte resultado devido a Srinivasa Ramanujan

Proposição 2.4.4 (S. Ramanujan)**.** *Se $q_1 = 2$, $q_2 = 3$, ... é a sequência crescente de todos os números primos, então*

$$\prod_{i=1}^{\infty} \frac{q_i^2 + 1}{q_i^2 - 1} = \frac{5}{2}.$$

Demonstração. Inicialmente, temos que $\prod_{i=1}^{\infty} \left(1 - q_i^{-s}\right) = \zeta(s)^{-1}$ para $s > 1$, onde $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ denota a função zeta de Riemann. Tal igualdade pode ser vista **[Ser73]**, Capítulo 6, seção 3.2. Pelas Identidades de Euler, $\zeta(2) = \frac{\pi^2}{6}$ e $\zeta(4) = \frac{\pi^4}{90}$. Agora, observe que

$$\frac{\prod_{i=1}^{\infty} 1 - q_i^{-2s}}{\prod_{i=1}^{\infty} 1 - q_i^{-s}} = \prod_{i=1}^{\infty} \frac{1 - q_i^{-2s}}{1 - q_i^{-s}} = \prod_{i=1}^{\infty} \frac{(1 - q_i^{-s})(1 + q_i^{-s})}{1 - q_i^{-s}} = \prod_{i=1}^{\infty} (1 + q_i^{-s}).$$

Logo,

$$\prod_{i=1}^{\infty} (1 + q_i^{-s}) = \frac{\prod_{i=1}^{\infty} 1 - q_i^{-2s}}{\prod_{i=1}^{\infty} 1 - q_i^{-s}} = \frac{\zeta(2s)^{-1}}{\zeta(s)^{-1}} = \frac{\zeta(s)}{\zeta(2s)}.$$

Fazendo $s = 2$, temos que

$$\prod_{i=1}^{\infty} (1 - q_i^{-2}) = \zeta(2)^{-1} = \frac{6}{\pi^2}$$

e

$$\prod_{i=1}^{\infty}(1+q_i^{-2}) = \frac{\zeta(2)}{\zeta(4)} = \frac{\frac{\pi^2}{6}}{\frac{\pi^4}{90}} = \frac{15}{\pi^2}.$$

Por fim, observe que

$$\begin{aligned}\prod_{i=1}^{\infty}\frac{q_i^2+1}{q_i^2-1} &= \prod_{i=1}^{\infty}\frac{\frac{q_i^2+1}{q_i^2}}{\frac{q_i^2-1}{q_i^2}} \\ &= \prod_{i=1}^{\infty}\frac{1+q_i^{-2}}{1-q_i^{-2}} \\ &= \frac{\prod_{i=1}^{\infty}1+q_i^{-2}}{\prod_{i=1}^{\infty}1-q_i^{-2}} \\ &= \frac{\frac{15}{\pi^2}}{\frac{6}{\pi^2}} = \frac{5}{2}.\end{aligned}$$

Portanto, $\prod_{i=1}^{\infty}\frac{q_i^2+1}{q_i^2-1} = \frac{5}{2}$. □

Como consequência dessa proposição temos o seguinte lema:

Lema 2.4.1. *Seja $p_2, p_3, ..., p_s$ números primos tais que $3 < p_2 < p_3 < \cdots < p_s$, então*

$$\prod_{i=1}^{s}\frac{p_i^2-1}{p_i^2+1} > \frac{5}{6}.$$

Demonstração. Como $p_2 > 3$, temos que, pela Proposição 2.4.4,

$$\frac{2^2+1}{2^2-1}\cdot\frac{3^2+1}{3^2-1}\prod_{i=1}^{s}\frac{p_i^2+1}{p_i^2-1} < \frac{5}{2},$$

ou seja,

$$\prod_{i=1}^{s}\frac{p_i^2+1}{p_i^2-1} < \frac{6}{5}.$$

Portanto,

$$\prod_{i=1}^{s}\frac{p_i^2-1}{p_i^2+1} > \frac{5}{6}.$$

□

Agora, já temos todas as ferramentas para demonstrar o Teorema 2.4.4.

Demonstração do Teorema 2.4.4.

Suponha que $\psi(G) \geq \frac{3}{5}n\varphi(n)$, e seja p_1 o maior divisor primo de n. Pelo Lema 2.2.1, temos que $\varphi(n) \geq \frac{n}{p_1}$ e, assim por hipótese,

$$\psi(G) \geq \frac{3}{5}n\varphi(n) \geq \frac{3n^2}{5p_1}.$$

Logo, existe um elemento $x \in G$ tal que $o(x) > \frac{3n}{5p_1}$ e, portanto,

$$|G : \langle x \rangle| < \frac{5}{3}p_1 < 2p_1.$$

Logo, pela Proposição 2.4.2, ou G é solúvel ou G tem um p_1-subgrupo de Sylow cíclico normal P_1 de G.

Inicialmente, provaremos que G é solúvel. Se $n = p_1^k$ para algum inteiro positivo k, então G é um p_1-grupo e, portanto G é solúvel. Se $G = p^l p_1^k$, então, pelo Teorema de Burnside (veja Teorema 1.2.3), G também é solúvel. Logo, podemos supor que n é divisível por pelo menos três números primos distintos, e assim $p_1 \geq 5$. Também podemos supor que G possui um p_1-subgrupo de Sylow cíclico normal. Logo, pelo Teorema de Schur-Zassenhaus (veja Teorema 1.4.1), $G = P_1 \rtimes H$ para algum subgrupo H de G. Como $H \cong G/P_1$ e assim $\psi(H) = \psi(G/P_1)$, pelo Corolário 2.1.1 temos que

$$\psi(G) \leq \psi(P_1)\psi(G/P) = \psi(P_1)\psi(H),$$

e, portanto, $\psi(H) \geq \dfrac{\psi(G)}{\psi(P_1)}$.

Seja $h := |H|$. Então $n = h|P_1|$ e, por $mdc(h, |P_1|) = 1$, temos, também, que $\varphi(n) = \varphi(h)\varphi(|P_1|) = \varphi(h)(p_1 - 1)\dfrac{|P_1|}{p_1}$. Lembro que $p_1 \geq 5$ e $\psi(P_1) = \dfrac{p_1|P_1|^2 + 1}{p_1 + 1}$, temos que

$$\begin{aligned}
\psi(H) \geq \left(\frac{3}{5}\right)\frac{n\varphi(n)(p_1+1)}{(p_1|P_1|^2+1)} &= \frac{3}{5}\frac{(h|P_1|)(\varphi(h)(p_1-1)|P_1|)(p_1+1)}{p_1(p_1|P_1|^2+1)} \\
&= \frac{3}{5}\frac{h\varphi(h)|P_1|^2(p_1^2-1)}{p_1^2|P_1|^2+p_1} \\
&> \frac{3}{5}\frac{h\varphi(h)|P_1|^2(p_1^2-1)}{p_1^2|P_1|^2+|P_1|^2}
\end{aligned}$$

$$\begin{aligned} &= \frac{3}{5}\frac{h\varphi(h)|P_1|^2(p_1^2-1)}{(p_1^2+1)|P_1|^2} \\ &= \frac{3}{5}\frac{h\varphi(h)(p_1^2-1)}{p_1^2+1} \\ &\geq \frac{3}{5}\varphi(h)\frac{24}{26} > \frac{1}{2}h\varphi(h), \end{aligned}$$

ou seja, $\psi(H) > \frac{1}{2}h\varphi(h)$. Agora, seja p_2 o maior divisor primo de h. Pelo Lema 2.2.1, $\psi(H) > \frac{h^2}{2p_2}$ de modo que existe um elemento $y \in H$ tal que $o(y) > \frac{h}{2p_2}$ e, portanto,

$$|H : \langle y \rangle| < 2p_2.$$

Pela Proposição 2.4.2, ou H é solúvel ou H possui um p_2-subgrupo de Sylow normal cíclico P_2. Se H é solúvel, então G também o é, pois $H \cong G/P_1$ e P_1 são solúveis. Assim, podemos supor que H possui um p_2-subgrupo de Sylow normal cíclico P_2. Logo, $H = P_2 \rtimes V$, para algum subgrupo V de H e, portanto,

$$G = P_1 \rtimes (P_2 \rtimes V).$$

Agora, sejam $p_1 > p_2 > \cdots > p_t > 3$ números primos e suponha que

$$G = P_1 \rtimes (P_2 \rtimes (\cdots (P_t \rtimes K)...)),$$

onde P_i são p_i-subgrupos de Sylow cíclicos de G e K é um subgrupo adequado de G. Escreva $k = |K|$ e suponha que t é o maior inteiro positivo com essas condições. Pelo Corolário 2.1.2, segue que

$$\psi(G) \leq \psi(P_1)\psi(P_2)\cdots\psi(P_t)\psi(K),$$

e, portanto,

$$\psi(K) \geq \frac{\psi(G)}{\psi(P_1)\psi(P_2)\cdots\psi(P_t)}.$$

Como $\psi(P_i) = \dfrac{p_i|P_i|^2+1}{p_i+1}$, usando a nossa hipótese inicial, temos que

$$\begin{aligned}\psi(K) \geq \frac{\psi(G)}{\psi(P_1)\psi(P_2)\cdots\psi(P_t)} &\geq \frac{3}{5}n\varphi(n)\prod_{i=1}^{t}\frac{p_i+1}{p_i|P_i|^2+1}\\ &= \frac{3}{5}k\varphi(k)\prod_{i=1}^{t}\frac{|P_i|(p_i-1)|P_i|(p_i+1)}{p_i(p_i|P_i|^2+1)}\\ &\frac{3}{5}k\varphi(k)\prod_{i=1}^{t}\frac{|P_i|^2(p_i^2-1)}{p_i(p_i|P_i|^2+1)}\\ &> \frac{3}{5}k\varphi(k)\prod_{i=1}^{t}\frac{p_i^2-1}{p_i^2+1}\\ &> k\varphi(k)\left(\frac{3}{5}\right)\left(\frac{5}{6}\right) = \frac{1}{2}k\varphi(k).\end{aligned}$$

onde a última desigualdade segue pelo Lema 2.4.1.

Agora seja p_{t+1} o maior divisor primo de k. Assim, pelo Lema 2.2.2, temos que $\psi(K) > \dfrac{1}{2}\cdot\dfrac{k^2}{p_{t+1}}$ e, portanto, existe um elemento $v \in K$ tal que $o(v) > \dfrac{k}{2p_{t+1}}$. Assim, $|K:\langle v\rangle| < 2p_{t+1}$ e, pela Proposição 2.4.2, ou K é solúvel ou K tem um p_{t+1}-subgrupo de Sylow normal cíclico P_{t+1} de K. No primeiro caso, se K é solúvel temos que G também o é. Assim, podemos supor que K possui um p_{t+1}-subgrupo de Sylow normal cíclico P_{t+1}. Daí $K = P_{t+1} \rtimes W$ para algum subgrupo W de K; e, pela maximalidade de t, temos que $p_{t+1} \leq 3$. Logo, K é um $\{2,3\}$-grupo, i.e., $|K| = 2^\alpha 3^\beta$ para alguns $\alpha, \beta \in \mathbb{Z}$, e portanto K é solúvel. Disto segue que G é solúvel, como queríamos.

Observe que foi provado que

$$G = P_1 \rtimes (P_2 \rtimes (\cdots (P_t \rtimes K)...)),$$

onde P_i são p_i-subgrupos de Sylow cíclicos de G, e ou K possui um subgrupo maximal cíclico ou $|K| = 2^\alpha 3^\alpha$ e K tem um subgrupo cíclico $\langle v\rangle$ de índice menor que 6. Por fim, mostraremos por indução sobre t, que essas hipóteses implicam que $G'' \leq Z(G)$. Se $t = 0$, então o resultado segue pela Proposição 2.4.1 e pela Proposição 2.4.3 item (ii). Assim, suponha que $t > 0$ e seja $H = (P_2 \rtimes \cdots (P_t \rtimes K)...)$. Por hipótese de indução, temos que $H'' \leq Z(H)$. Como $G = P_1 \rtimes H$ e P_1 cíclico, temos que $G' \leq C_G(P_1)$ (pela Proposição

1.2.2) e $G' = [P_1, P_1][P_1, H][H, H] = H'[P_1, H]$. Logo,

$$G'' = H'' \leq Z(H) \cap C_G(P_1) \leq Z(G)$$

o que completa a demonstração.

□

Por último encerramos a seção com o seguinte resultado.

Teorema 2.4.6 (Teorema 11, [HLM18a])**.** *Seja G um grupo finito de ordem n e sejam q e p o menor e o maior divisores primos de n, respectivamente. Suponha que G satisfaz*

$$\psi(G) \geq \frac{1}{q} n\varphi(n).$$

Então ou G tem um p-subgrupo de Sylow cíclico normal ou G é um grupo solúvel com um subgrupo maximal cíclico com índice p ou $p+1$.

Demonstração. Suponha que G é um grupo de ordem n com $\psi(G) \geq \frac{1}{q} n\varphi(n)$. Pelo Lema 2.2.2, $\varphi(n) \geq \frac{(q-1)n}{p}$, segue que

$$\psi(G) \geq \frac{(q-1)n^2}{qp}.$$

Assim, existe um elemento $x \in G$ tal que $o(x) > \frac{(q-1)n}{qp}$ e assim

$$|G : \langle x \rangle| < \frac{q}{q-1} \cdot p \leq 2p.$$

Logo, pela Proposição 2.4.2, ou G tem p-subgrupo cíclico normal, ou G é solúvel com um subgrupo maximal cíclico de índice ou p ou $p+1$, como queríamos. □

No capítulo seguinte, generalizaremos a função ψ e veremos que muitos dos resultados deste capítulo podem ser generalizados de maneira natural.

Capítulo 3

Uma generalização da função ψ

Neste capítulo, iremos introduzir a função ψ_k e bem como alguns resultados que servirão de base para mostrarmos um análogo ao Teorema B do capítulo anterior. Vale ressaltar que a função ψ_k já foi considerada em **[AA14b]**, por S.M. Jafarian Amiri e M. Amiri, e ela também aparece como casos particulares de funções tratadas por M. Garonzi e M. Patassini, em **[GP17]**, e por M. Amiri, em **[AmiM20]**. Em **[AA14b]**, os autores definem ψ^k para tratar a função aqui definida como ψ_k.

3.1 A função ψ_k

Sejam G um grupo finito e $k \geq 1$ um inteiro. Considere

$$\psi_k(G) := \sum_{x \in G} o(x)^k,$$

onde $o(x)$ denota a ordem do elemento $x \in G$.

Iniciaremos mostrando, como no Lema 2.1.1, que a função ψ_k também é uma função multiplicativa.

Lema 3.1.1 (Lema 2.5, **[AA14b]**). *Se G e H são grupos finitos, então*

$$\psi_k(G \times H) \leq \psi_k(G)\psi_k(H).$$

Além disso, $\psi_k(G \times H) = \psi_k(G)\psi_k(H)$ se, e somente se, $mdc(|G|, |H|) = 1$.

Demonstração. Aqui basta observar que $o((g,h))^k \leq (o(g)o(h))^k = o(g)^k o(h)^k$, para quaisquer $g \in G$ e $h \in H$, e proceder como na demonstração do Lema 2.1.1. □

Vejamos agora, como no Lema 2.2.1, o valor de $\psi_k(P)$ para um p-grupo cíclico P e assim, usando o fato que ψ_k é multiplicativa, podemos analisar $\psi_k(C_n)$ do grupo cíclico C_n.

Lema 3.1.2. 1) *Se P é um grupo cíclico de ordem p^r para algum primo p, então*

$$\psi_k(P) = \frac{p^{(k+1)r}p^k + p^{k-1} + \cdots + p + 1}{p^k + \cdots + p + 1} = \frac{|P|^{k+1}p^k + p^{k-1} + \cdots + p + 1}{p^k + \cdots + p + 1}.$$

2) *Sejam $p_1 < p_2 < \cdots < p_t = p$ os divisores primos de n e denote os correspondentes subgrupos de Sylow de C_n por $P_1, P_2, ..., P_t$. Então*

$$\psi_k(C_n) = \prod_{i=1}^{t} \psi_k(P_i) > \frac{2^k}{p^k + \cdots + p + 1} n^{k+1}.$$

Demonstração. 1) Como no Exemplo 2.1.1, temos que $\psi_k(C_n) = \sum_{d|n} d^k \cdot \varphi(d)$. Em

particular,

$$\begin{aligned}
\psi_k(P) &= \sum_{i=0}^{t} \varphi(p^i)p^{ik} \\
&= 1 + \sum_{i=1}^{t} p^{i-1}(p-1)p^{ik} \\
&= 1 + \frac{p-1}{p}\sum_{i=1}^{t} p^{i(k+1)} = 1 + \frac{p-1}{p}\left(\frac{p^{k+1} - p^{(k+1)(r+1)}}{1-p^{k+1}}\right) \\
&= \frac{p - pp^{k+1} + pp^{k+1} - pp^{(k+1)(r+1)} - p^{k+1} + p^{(k+1)(r+1)}}{p(1-p^{k+1})} \\
&= \frac{1 - p^{(k+1)(r+1)} - p^k + p^{(k+1)r+k}}{1-p^{k+1}} \\
&= \frac{p^{(k+1)r+k}(1-p) + (1-p)(p^{k-1} + \cdots + p + 1)}{(1-p)(p^k + \cdots + p + 1)} \\
&= \frac{p^{(k+1)r}p^k + p^{k-1} + \cdots + p + 1}{p^k + \cdots + p + 1} \\
&= \frac{|P|^{k+1}p^k + p^{k-1} + \cdots + p + 1}{p^k + \cdots + p + 1},
\end{aligned}$$

isto é, $\psi_k(P) = \dfrac{|P|^{k+1}p^k + p^{k-1} + \cdots + p + 1}{p^k + \cdots + p + 1}$.

2) Como $C_n = P_1 \times P_2 \times \cdots \times P_t$, pelo Lema 3.1.1, temos que $\psi_k(C_n) = \prod_{i=1}^{t} \psi_k(P_i)$. Além disso, como $p_{i+1}^k \geq p_i^k + \cdots + p_i + 1$, i.e., $\dfrac{p_{i+1}^k}{p_i^k + \cdots p_i + 1} \geq 1$ para cada $1 \leq i \leq t-1$, e como $2 \leq p_1$, segue, pelo item 1), que

$$\begin{aligned}
\psi_k(C_n) = \prod_{i=1}^{t} \psi_k(P_i) &= \prod_{i=1}^{t} \frac{|P_i|^{k+1}p_i^k + p_i^{k-1} + \cdots + p_i + 1}{p_i^k + \cdots + p_i + 1} \\
&> \prod_{i=1}^{t} \frac{|P_i|^{k+1}p_i^k}{p_i^k + \cdots + p_i + 1} \qquad \text{(pois } p_i^{k-1} + \cdots + 1 > 0\text{)} \\
&= (|P_1| \cdots |P_t|)^{k+1} \prod_{i=1}^{t} \frac{p_i^k}{p_i^k + \cdots + p_i + 1} \\
&= n^{k+1} \frac{p_1^k}{p_t^k + \cdots + p_t + 1} \left(\prod_{i=1}^{t-1} \frac{p_{i+1}^k}{p_i^k + \cdots + p_i + 1}\right) \\
&\geq n^{k+1} \frac{p_1^k}{p_t^k + \cdots + p_t + 1} \\
&\geq n^{k+1} \frac{2^k}{p^k + \cdots + p + 1}.
\end{aligned}$$

Portanto, $\psi_k(C_n) > \dfrac{2^k}{p^k + \cdots + p + 1} n^{k+1}$.

□

Agora enunciaremos e demonstraremos o seguinte resultado que é similar ao Teorema 2.3.1.

Teorema 3.1.1. *Seja G um grupo nilpotente de ordem n. Então $\psi_k(G) \leq \psi_k(H)$ para todo grupo nilpotente H de ordem n se, e somente se, cada subgrupo de Sylow de G tem expoente primo.*

Demonstração. Suponha que H é um grupo nilpotente de ordem $n > 1$ e seja $n = p_1^{r_1} p_2^{r_2} ... p_t^{r_t}$, onde $p_1, p_2, ..., p_t$ são primos distintos e todos $r_i \geq 1$ são inteiros. Como H é nilpotente, temos que H é o produto direto de seus subgrupos de Sylow, i.e., $H = P_1 \times P_2 \times \cdots \times P_t$, onde P_i é o p_i-subgrupo de Sylow de H. Assim, pelo Lema 3.1.1,

$$\psi_k(H) = \psi_k(P_1)\psi_k(P_2) \cdots \psi_k(P_t).$$

Como todo elemento diferente 1 em P_i tem ordem maior ou igual a p_i, temos que $\psi_k(P_i) \geq 1 + p_i^k(p_i^{r_i} - 1)$ para todo $1 \leq i \leq t$, e a igualdade ocorre se, e somente se, $exp(P_i) = p_i$ para cada i. Portanto, segue que $\psi_k(G) \leq \psi_k(H)$ para todo grupo nilpotente H de ordem n se, e somente se, cada subgrupo de Sylow de G tem expoente primo. □

Como corolário direto do Teorema 3.1.1 temos o seguinte:

Corolário 3.1.1. *Se G é um grupo finito de ordem $n = p_1^{r_1} \cdots p_t^{r_t}$ e*

$$\psi_k(G) < \prod_{i=1}^{t} (p_i^k(p_i^{r_i} - 1) + 1),$$

então G é não-nilpotente.

Assim, quando n é um número nilpotente (i.e., quando todos os grupos de ordem n são nilpotentes), vemos que $\psi_k(G)$ assume valor mínimo sobre o grupo G de ordem n cujos subgrupos de Sylow tem expoente primos.

Agora, veremos um análogo para o item v) do Lema 2.2.3 para o caso ψ_k. Esse Lema terá grande importância na demonstração do Teorema 3.1.3.

Lema 3.1.3. *Seja G um grupo finito satisfazendo $G = P \rtimes F$, onde P é um p-grupo cíclico para algum primo p, $|F| > 1$ e $(p, |F|) = 1$. Considerando $Z = C_F(P)$, temos que*

$$\psi_k(G) = \psi_k(P)\psi_k(Z) + |P|\psi_k(F\backslash Z) < \psi_k(P)\psi_k(Z) + |P|\psi_k(F).$$

Demonstração. Note que $G = PF = P(Z \dot\cup (F\backslash Z)) = PZ \dot\cup P(F\backslash Z)$ é uma união disjunta. Assim

$$\psi_k(G) = \psi_k(PZ \dot\cup P(F\backslash Z)) = \psi_k(PZ) + \psi_k(P(F\backslash Z)),$$

e portanto por (3) temos que $\psi_k(PZ) = \psi_k(P)\psi_k(Z)$ e por (4) temos $\psi_k(G\backslash(PZ)) = |P|\psi_k(F\backslash Z)$. Portanto,

$$\psi_k(G) = \psi_k(P)\psi_k(Z) + |P|\psi_k(F\backslash Z) < \psi_k(P)\psi_k(Z) + |P|\psi_k(F).$$

□

Como no caso da ψ, o Corolário 2.1.1 tem uma grande importância no estudo do comportamento de $\psi(G)$. Para ψ_k também temos o mesmo resultado como a seguir:

Lema 3.1.4 (Lema 2.2, [AA14b])**.** *Seja $P \in Syl_p(G)$ um p-subgrupo de Sylow de G. Suponha que P é normal em G e que P é cíclico. Seja $x \in G$ e suponha que a classe lateral Px tem ordem m, como um elemento de G/P. Então $\psi_k(Px) \leq m^k\psi_k(P)$, com a igualdade se, e somente se, x centraliza P.*

Demonstração. Temos que m divide $o(x)$, e assim $o(x) = mq$ para algum q inteiro. Logo, $q = o(x^m)$. Como $x^m \in P$ (pois Px tem ordem m), temos que q é uma potência de p. Além disso, como m divide $|G/P|$ que não é divisível por p, segue que m e q são relativamente primos entre si. Logo, existe n tal que $qn \equiv 1 \pmod m$. Agora, $o(x^q) = m$ e escrevendo $y = (x^q)^n$, temos que $o(y) = m$, pois n é coprimo a m. Note que

$$Py = Px^{qn} = (Px)^{qn} = Px,$$

e além disso, y centraliza P se, e somente se, x centraliza P. De fato, se y centraliza P e

$g \in P$, então por $Px = Py$ temos que $x = hy$ para algum $h \in P$, e portanto

$$xg = (hy)g = h(yg) = h(gy) = (hg)y = (gh)y = g(hy) = gx.$$

Podemos então substituir x por y e supor que $o(x) = m$. Agora todo elemento de Px tem a forma ux para algum $u \in P$. Mostremos que $o(ux) \leq m \cdot o(u)$ com a igualdade se, e somente se, x centraliza u. De fato, como P é cíclico, P possui apenas um único subgrupo de cada ordem dividindo a ordem de P. Desta forma, para cada $\sigma \in Aut(P)$, o subgrupo $\sigma(\langle u \rangle)$ de P tem a mesma ordem que $\langle u \rangle$, e portanto $\sigma(\langle u \rangle) = \langle u \rangle$, i.e., $\langle u \rangle$ é um subgrupo característico de P. Note também que dado $g \in G$, $i_g : P \to P$ dado por $i_g(v) = g^{-1}ng$ é um automorfismo de P, e portanto $i_g(\langle u \rangle) = \langle u \rangle$, ou seja, $\langle u \rangle$ é normal em G. Logo $\langle u \rangle\langle x \rangle$ é um subgrupo de G, e portanto

$$o(ux) \leq |\langle u \rangle\langle x \rangle| = m \cdot o(u).$$

Por outro lado, se a igualdade ocorre então $\langle u \rangle\langle x \rangle$ é um subgrupo cíclico, gerado por ux, e assim x centraliza u. Reciprocamente, se x centraliza u, então como $o(x)$ e $o(u)$ são coprimos, temos que $o(ux) = o(x)o(u) = m \cdot o(x)$.

Por fim,

$$\psi_k(Px) = \sum_{u \in P} o(ux)^k \leq \sum_{u \in P} m^k o(u)^k = m^k \sum_{u \in P} o(u)^k = m^k \psi_k(P)$$

e a igualdade ocorre se, e somente se, x centraliza u para cada $u \in P$, ou seja, se, e somente se, x centraliza P. □

E como consequência, temos o importante resultado:

Corolário 3.1.2. *Se P é um p-subgrupo Sylow normal cíclico de um grupo finito G, então*

$$\psi_k(G) \leq \psi_k(P)\psi_k(G/P),$$

com a igualdade se, e somente se, P é central em G.

Demonstração. Observe que G é uma união disjunta de todas as classes laterais Px com

$Px \in G/P$, de forma que $\psi_k(G) = \sum_{Px \in G/P} \psi_k(Px)$. Logo, pelo Lema 3.1.4, temos que

$$\psi_k(G) = \sum_{Px \in G/P} \psi_k(Px) \leq \sum_{Px \in G/P} o(Px)^k \psi_k(P) = \psi_k(P) \sum_{Px \in G/P} o(Px)^k$$
$$= \psi_k(P)\psi_k(G/P),$$

ou seja, $\psi_k(G) \leq \psi_k(P)\psi_k(G/P)$. Por outro lado, a igualdade vale se, e somente se, cada $x \in G$ centraliza P. □

Como visto no capítulo anterior, em geral, $\psi_k(G)$ e $|G|$ não determinam a estrutura de G. Por outro lado, veremos que os grupos cíclicos são completamente determinados por $\psi_k(G)$ e $|G|$, uma generalização direta do Teorema I.

Teorema 3.1.2 (Teorema 2.6, [AA14b])**.** *Seja G um grupo não-cíclico de ordem n. Então $\psi_k(G) < \psi_k(C_n)$.*

Demonstração. Suponha que $\psi_k(G) \geq \psi_k(C_n)$. Devemos mostrar que $G \cong C_n$. Mostraremos por indução sobre n. O caso $n = 1$, é direto. Assim, suponha por hipótese de indução, que o resultado é verdadeiro para todos os grupos de ordem menor que $n > 1$. Agora, pelo Lema 2.1.3, $\varphi(n) \geq \frac{n}{p}$, onde p é o maior divisor primo de n, temos que

$$\psi_k(G) \geq \psi_k(C_n) > n^k \varphi(n) \geq \frac{n^{k+1}}{p},$$

i.e., $\psi_k(G) > \frac{n^{k+1}}{p}$. Logo, existe $x \in G$ tal que $o(x)^k > \frac{n^k}{p}$, caso contrário teríamos que $\psi_k(G) \leq n \cdot \frac{n^k}{p} = \frac{n^{k+1}}{p}$, uma contradição. Assim, $o(x) > \frac{n}{p^{1/k}} \geq \frac{n}{p}$ e, portanto, $|G : \langle x \rangle| < p$. Logo $\langle x \rangle$ contém um p-subgrupo de Sylow cíclico de G e, por $|G : N_G(P)| \leq |G : \langle x \rangle| < p$, P é normal em G. Assim, pelo Corolário 3.1.2,

$$\psi_k(G) \leq \psi_k(P)\psi_k(G/P),$$

com a igualdade se, e somente se, P é central em G. Observe que $P \cong C_{p^r}$ e $C_n \cong$

$C_{p^r} \times C_{n/p^r}$, onde $p^r = |P|$. Assim,

$$\psi_k(P)\psi_k(G/P) \geq \psi_k(G) \geq \psi_k(C_n) = \psi_k(C_{p^r})\psi_k(C_{n/p^r}) \tag{3.1}$$

e, portanto,

$$\psi_k(G/P) \geq \psi_k(C_{n/p^r}).$$

Como $|G/P| = \dfrac{n}{p^r}$, temos, por hipótese de indução, que G/P é cíclico e, portanto, $\psi_k(G/P) = \psi_k(C_{n/p^r})$. Assim, todas as desigualdades em 3.1 são igualdades, i.e., P é central em G. Como P é central em G, temos que $G/Z(G) \leq G/P$ é cíclico e, assim, G é abeliano. Logo, $G \cong P \times Q$, onde $Q \cong G/P$ é cíclico de ordem coprima com p. Portanto G é o produto direto de dois grupos cíclicos de ordens coprimas, isto é, G é cíclico. □

Por fim, veremos o nosso resultado principal que generaliza o Teorema B visto no Capítulo 2.

Teorema 3.1.3. *Sejam G um grupo não-cíclico de ordem n e q o menor divisor primo de n. Então*

$$\psi_k(G) < \frac{1}{(q-1)^k}\psi_k(C_n).$$

Demonstração. A ideia da demonstração é seguir os mesmos passos do Teorema B e adaptando as desigualdades que aparecem de maneira apropriada.

Mostremos que se $\psi_k(G) \geq \dfrac{1}{(q-1)^k}\psi_k(C_n)$, então $G \cong C_n$. Como o caso $k = 1$ já foi demonstrado no Teorema B, podemos supor que $k \geq 2$. Essa hipótese será necessária no final da demonstração.

Inicialmente note que $\psi_k(C_n) \geq 1 + n^k\varphi(n) > n^k\varphi(n)$. Pelo Lema 2.2.2, temos que $\varphi(n) \geq \dfrac{(q-1)n}{p}$, onde p é o maior divisor primo de n. Assim,

$$\psi_k(G) \geq \frac{1}{(q-1)^k}\psi_k(C_n) > \frac{n^{k+1}}{p(q-1)^{k-1}}$$

e portanto, existe $x \in G$ tal que $o(x)^k > \dfrac{n^k}{p(q-1)^{k-1}}$, isto é,

$$o(x) > \left(\frac{n^k}{p(q-1)^{k-1}}\right)^{1/k} = \frac{n}{(p(q-1)^{k-1})^{1/k}} > \frac{n}{(p^k)^{1/k}} = \frac{n}{p},$$

pois $p > q-1$. Assim $|G : \langle x\rangle| = |G|/o(x) < \dfrac{n}{n/p} = p$, e $\langle x\rangle$ contém um p-subgrupo de Sylow P de G. Como $\langle x\rangle \leq N_G(P)$, temos que $|G : N_G(P)| < p$ e portanto pelo Teorema de Sylow, $|G : N_G(P)| \equiv 1 \pmod p$ implica que $|G : N_G(P)| = 1$. Disto segue que P é um p-subgrupo de Sylow normal cíclico de G e pela Proposição 3.1.4, obtemos que

$$\psi_k(P)\psi_k(G/P) \geq \psi_k(G) \geq \frac{1}{(q-1)^k}\psi_k(C_n) = \frac{1}{(q-1)^k}\psi_k(C_{p^r})\psi_k(C_{n/p^r}),$$

onde $|P| = p^r$. Como $P \cong C_{p^r}$, fazendo os devidos cancelamentos temos que

$$\psi_k(G/P) \geq \frac{1}{(q-1)^k}\psi_k(C_{n/p^r}).$$

Se $n = p^r$, então a existência de x com $o(x) > n/p$, garante que $o(x) = n$ e, portanto, G é cíclico. Podemos supor que n é divisível por exatamente t primos diferentes com $t > 1$. Aplicando indução sobre t, podemos supor que o resultado é verdadeiro para todos os grupos de ordens com menos que t divisores primos distintos. Como $|G/P|$ tem $t-1$ divisores primos distintos e G/P satisfaz a nossa hipótese, segue que G/P é cíclico. Como $(|P|, |G/P|) = 1$, temos, pelo Teorema de Schur-Zassenhaus, Teorema 1.4.1, que $G = P \rtimes F$ com $F \cong G/P$ e $F \neq \{1\}$. Note que $n = |P||F|$, P e F são cíclicos de ordens coprimas, logo

$$\psi_k(C_n) = \psi_k(P \times F) = \psi_k(P)\psi_k(F).$$

Se $C_F(P) = F$, i.e., os elementos de P comutam com os elementos de F, então $G = P \times F$, e portanto G é cíclico, como desejado. Assim, é suficiente provar que se $C_F(P) =: Z \lneq F$, então $\psi_k(G) < \dfrac{1}{(q-1)^k}\psi_k(C_n)$. Pelo Lema 3.1.3, segue que

$$\psi_k(G) = \psi_k(P)\psi_k(Z) + |P|\psi_k(F\backslash Z) < \psi_k(P)\psi_k(Z) + |P|\psi_k(F),$$

logo

$$\psi_k(G) < \psi_k(P)\psi_k(F)\left(\frac{\psi_k(Z)}{\psi_k(F)} + \frac{|P|}{\psi_k(P)}\right).$$

Note que como P é um p-grupo cíclico, temos

$$\begin{aligned}
\frac{|P|}{\psi_k(G)} &= \frac{|P|(p^k + \cdots + p + 1)}{p^k|P|^{k+1} + p^{k-1} + \cdots + p + 1} \\
&< \frac{|P|(p^k + \cdots + p + 1)}{p^k|P|^{k+1}} \\
&= \frac{p^k + \cdots + p + 1}{p^k|P|^k} \\
&\leq \frac{p^k + \cdots + p + 1}{p^k p^k} \\
&< \frac{p^k + \cdots + p + 1}{p^{2k} - 1} \\
&\leq \frac{1}{(p-1)^k} \leq \frac{1}{q^k},
\end{aligned}$$

onde a penúltima desigualdade segue pelo fato que

$$\begin{aligned}
\frac{p^{2k} - 1}{(p-1)^k} &= \frac{(p-1)(p^{2k-1} + \cdots + p + 1)}{(p-1)^k} \\
&= \frac{1}{(p-1)^{k-1}} + \frac{p}{(p-1)^{k-1}} + \cdots + \frac{p^{2k-1}}{(p-1)^{k-1}} \\
&\geq \frac{p^{k-1}}{(p-1)^{k-1}} + \frac{p \cdot p^{k-1}}{(p-1)^{k-1}} + \cdots + \frac{p^k \cdot p^{k-1}}{(p-1)^{k-1}} \\
&= \left(\frac{p}{p-1}\right)^{k-1}(1 + p + \cdots + p^{k-1}) \geq 1 + p + \cdots + p^{k-1},
\end{aligned}$$

ou seja, $1 + p + \cdots + p^{k-1} \leq \dfrac{p^{2k} - 1}{(p-1)^k}$ e, portanto, $\dfrac{1 + p + \cdots + p^{k-1}}{p^{2k} - 1} \leq \dfrac{1}{(p-1)^k}$.

Como Z é um subgrupo próprio do grupo cíclico F e que F é o produto de seus subgrupos de Sylow, temos que ao menos um subgrupo de Sylow de Z, digamos um r-subgrupo de Sylow R_Z, está contido propriamente no r-subgrupo de Sylow R_F de F de ordem r^s. Note que $\psi_k(F) = \prod \psi_k(R_{iF})$, onde R_{iF} percorre por todos os subgrupos de Sylow de F. Analogamente, $\psi_k(Z) = \prod \psi_k(R_{iZ})$. Note também que $\dfrac{\psi_k(R_{iZ})}{\psi_k(R_{iF})} \leq 1$, de

forma que

$$\frac{\psi_k(Z)}{\psi_k(F)} = \frac{\prod \psi_k(R_{iZ})}{\prod \psi_k(R_{iF})} \leq \frac{\psi_k(R_Z)}{\psi_k(R_F)}.$$

Logo, como $r \geq q$, $s \geq 1$ e $k \geq 2$, usando o Lema 3.1.2,

$$\psi_k(R_F) = \frac{|R_F|^{k+1}r^k + r^{k-1} + \cdots + r + 1}{r^k + \cdots + r + 1} \quad \text{e} \quad \psi_k(R_Z) = \frac{|R_Z|^{k+1}r^k + r^{k-1} + \cdots + r + 1}{r^k + \cdots + r + 1}$$

e assim obtemos que

$$\begin{aligned}
\frac{\psi_k(Z)}{\psi_k(F)} \leq \frac{\psi_k(R_Z)}{\psi_k(R_F)} &= \frac{|R_Z|^{k+1}r^k + r^{k-1} + \cdots + r + 1}{|R_F|^{k+1}r^k + r^{k-1} + \cdots + r + 1} \\
&= \frac{|R_Z|^{k+1}r^k + r^{k-1} + \cdots + r + 1}{|R_F|^{k+1}r^k + r^{k-1} + \cdots + r + 1} \\
&\leq \frac{r^{(s-1)(k+1)+k} + r^{k-1} + \cdots + r + 1}{r^{s(k+1)+k} + r^{k-1} + \cdots + r + 1} && (\text{pois } |R_Z| \leq r^{s-1}) \\
&< \frac{r^{(s-1)(k+1)+k} + r^k}{r^{s(k+1)+1}} && (\text{pois } r^{k+1} + \cdots + r + 1 \leq r^k) \\
&= \frac{r^{(s-1)(k+1)} + 1}{r^{s(k+1)}} \\
&\leq 2\frac{r^{(s-1)(k+1)}}{r^{s(k+1)}} && (\text{pois } 1 \leq r^{(s-1)(k+1)}) \\
&= \frac{2}{r^{k+1}} \leq \frac{k}{q^{k+1}} && (\text{pois } 2 \leq k \text{ e } q \leq r).
\end{aligned}$$

Agora note que

$$\left(\frac{q}{q-1}\right)^k = \left(\frac{q-1+1}{q-1}\right)^k = \left(1 + \frac{1}{q-1}\right)^k \geq 1 + \frac{k}{q-1} > 1 + \frac{k}{q},$$

onde a penúltima desigualdade segue pela Desigualdade de Bernoulli (lembre-se que a Desigualdade de Bernoulli afirma que $(1+x)^n \geq 1 + nx$ para n inteiro positivo e $x \geq -1$ um número real qualquer). Portanto, pelo Lema 3.1.3 e usando que

$$\frac{\psi_k(Z)}{\psi_k(F)} < \frac{k}{q^{k+1}}, \quad \frac{|P|}{\psi_k(G)} < \frac{1}{q^k} \quad \text{e} \quad 1 + \frac{k}{q} < \left(\frac{q}{q-1}\right)^k,$$

obtemos

$$\begin{aligned}\psi_k(G) &< \psi_k(C_n)\left(\frac{\psi_k(Z)}{\psi_k(F)} + \frac{|P|}{\psi_k(P)}\right)\\ &< \psi_k(C_n)\left(\frac{k}{q^{k+1}} + \frac{1}{q^k}\right)\\ &= \psi_k(C_n)\frac{1}{q^k}\left(\frac{k}{q} + 1\right)\\ &< \psi_k(C_n)\frac{1}{q^k}\left(\frac{q}{q-1}\right)^k\\ &= \psi_k(C_n)\frac{1}{(q-1)^k},\end{aligned}$$

uma contradição. Logo temos o desejado. □

Para grupos de ordem ímpar, temos o seguinte:

Corolário 3.1.3. *Seja G um grupo finito de ordem ímpar. Então*

$$\psi_k(G) < \frac{1}{2^k}\psi_k(C_n).$$

Demonstração. Seja q o menor divisor de n. Se n é ímpar, então $3 \leq q$ e, portanto, $2 \leq q-1$. Logo, pelo Teorema 3.1.3,

$$\psi_k(G) < \frac{1}{(q-1)^k}\psi_k(C_n) \leq \frac{1}{2^k}\psi_k(C_n).$$

□

Uma última observação: Para grupos não-cíclicos de ordem n, o valor $\psi_k(G)$ provavelmente pode ser limitado superiormente por $\dfrac{\psi_k(C_2 \times C_2)}{\psi_k(C_4)}\psi_k(C_n) = \dfrac{1+3\cdot 2^k}{1+2^k+2\cdot 2^k}\psi_k(C_n)$, que seria uma generalização para ψ_k do Teorema A.

Finalizaremos a dissertação com o próximo capítulo fazendo uma pequena conclusão dos resultados trabalhados aqui e com indicações para estudos futuros que seguem na mesma linha tratada aqui.

Capítulo 4

Considerações Finais

Seja $\mathcal{G}$ a classe de todos os grupos finitos. Vimos neste trabalho, através da função $\psi\colon \mathcal{G} \to \mathbb{N}$, dada por $\psi(G) = \sum_{x\in G} o(x)$, e por algumas desigualdades envolvendo $\psi(G)$ e $|G|$, que é possível obtermos propriedades da estrutura de G. A saber, conseguimos alguns critérios de ciclicidade, condições necessárias para nilpotência e condições suficientes para solubilidade de grupos finitos. Além disso, vimos que alguns resultados podem ser generalizados através da função $\psi_k\colon \mathcal{G} \to \mathbb{N}$ definida por $\psi_k(G) = \sum_{x\in G} o(x)^k$.

Como resultado principal deste trabalho foi dada uma demonstração para o seguinte resultado, o qual generaliza o Teorema 3 em **[HLM18a]** para ψ_k:

Teorema 4.0.1. *Sejam G um grupo não-cíclico de ordem n e q o menor divisor primo de n. Então*

$$\psi_k(G) < \frac{1}{(q-1)^k}\psi_k(G).$$

Há muitos outros estudos relacionadas ao tratado aqui. No Capítulo 2, foi mostrado que para um grupo não-cíclico G vale que $\psi(G) \leq \frac{7}{11}\psi(C_n)$ e que $G \cong C_{4k} \times C_2$ satisfaz $\psi(G) = \frac{7}{11}\psi(C_n)$. A partir desse resultado temos o seguinte problema: determinar todos os grupos que atingem tal cota. Resolvendo esse problema M. Herzog, P. Longobardi e M. Maj, em **[HLM19]**, mostraram que tal igualdade é satisfeita se, e somente se, $n = 4k$ com $mdc(k, 2) = 1$ e $G \cong C_{4k} \times C_2$. Outros autores também estudaram o problema de determinar o valor maximal da soma das ordens de elementos sobre os grupos não-cíclicos de mesma ordem. Por exemplo, S.M. Jafarian Amiri e M. Amiri no artigo "Second

maximum sum of element orders on finite groups", [AA14a]; e Shen, R., Chen, G., Wu, C. no artigo "On groups with the second largest value of the sum of element orders", [SCW15].

Observe que o Teorema A, do Capítulo 2, nos dá um critério de ciclicidade para grupos finitos: Se $\psi(G) > \frac{7}{11}\psi(C_{|G|})$, então G é cíclico. Nesta direção, há outros resultados relacionados que não foram tratados no trabalho. Marius Tarnauceanu mostrou em seu artigo "A criterion for nilpotency of a finite group by the sum of element orders", [Tar19], que se $\psi(G) > \frac{13}{21}\psi(C_{|G|})$, então G é nilpotente e a igualdade vale se, e somente se, $G \cong S_3 \times C_m$ com $mdc(6, m) = 1$. M. Baniasad Azad e B. Khosravi mostraram no artigo "A criterion for solvability of a finite group by the sum of element orders", em [AK18], $\psi(G) > \frac{211}{1617}\psi(C_{|G|})$, então G é solúvel. Além disso, os mesmos autores mostraram, em [AK19], que se $\psi(G) > \frac{31}{77}\psi(C_n)$, então G é supersolúvel, i.e., G possui uma série normal

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$

onde cada G_i é normal em G e cujos fatores G_{i+1}/G_i são grupos cíclicos para todo $0 \leq i \leq n-1$.

Resumindo todos os resultados em um único teorema:

Teorema 4.0.2. *Seja G um grupo finito de ordem n.*

1) *(Herzog-Longobardi-Maj)* *Se $\psi(G) > \frac{7}{11}\psi(C_n)$, então G é cíclico.*

2) *(Tarnauceanu)* *Se $\psi(G) > \frac{13}{21}\psi(C_n)$, então G é nilpotente.*

3) *(Azad-Krosravi)* *Se $\psi(G) > \frac{211}{1617}\psi(C_n)$, então G é solúvel.*

4) *(Azad-Krosravi)* *Se $\psi(G) > \frac{31}{77}\psi(C_n)$, então G é supersolúvel.*

Uma observação interessante é observar de onde vem as constantes do Teorema 4.0.2. Definindo $\psi'(G) := \frac{\psi(G)}{\psi(C_n)}$, temos que

$$\psi'(C_2 \times C_2) = \frac{7}{11}, \quad \psi'(S_3) = \frac{13}{21}, \quad \psi'(A_5) = \frac{211}{1617} \text{ e } \psi'(A_4) = \frac{31}{77},$$

ou seja, as constantes do Teorema 4.0.2 são os valores de ψ' para o grupo de menor ordem que é não-cíclico, não-nilpotente, não-solúvel e não-supersolúvel, respectivamente.

Outras funções relacionadas foram definidas por M. Garonzi e M. Patassini em "Inequalities detecting structural properties of a finite group", [GP17],

$$P(G) := \prod_{x\in G} o(x) \qquad \text{e} \qquad R_G(r,s) := \sum_{x\in G} \frac{o(x)^s}{\varphi(o(x))^r},$$

onde r, s são números reais. Para tais funções temos o análogo do Teorema I, isto é, vale que $P(G) \leq P(C_{|G|})$ e, para $r \leq s-1$ e $s \geq 1$, então $R_G(r,s) \leq R_{C_{|G|}}(r,s)$ em ambos a igualdade ocorre se, e somente se, G é cíclico. Observe que $R_G(0,s) = \sum_{x\in G} o(x)^s$ e, assim, temos outra demonstração para o Teorema 3.1.2. Além disso, note que dado um elemento $x \in G$, o subgrupo $\langle x\rangle$ tem $\varphi(o(x))$ geradores. Assim

$$R_G(1,1) = \sum_{x\in G} \frac{o(x)}{\varphi(o(x))}$$

é igual a soma dos tamanhos dos subgrupos cíclicos de G e

$$R_G(1,0) = \sum_{x\in G} \frac{1}{\varphi(o(x))}$$

é igual ao número de subgrupos cíclicos de G. De forma que é possível obtermos outras informações, além das tratadas aqui no trabalho, do grupo G.

Por fim, encerramos sugerindo mais outro problema relacionado. No Kourovka Notebook, [Kou18], temos a seguinte conjectura:

Problema (Problema 18.1, [Kou18]). *Se G é um grupo finito de ordem n, então existe uma bijeção $f\colon G \to C_n$ tal que para cada elemento $x \in G$ vale que $o(x)$ divide $o(f(x))$.*

Mohsen Amiri, em [AmiM20], resolveu esse problema. Uma simples aplicação desse resultado é uma outra demonstração para o fato de $\psi_k(G) \leq \psi_k(C_n)$. De fato, como $o(x) \mid o(f(x))$ para todo $x \in G$, temos que $o(x) \leq o(f(x))$ para cada $x \in G$. Logo,

$$\psi_k(C_n) = \sum_{y\in C_n} o(y)^k = \sum_{x\in G} (o(f(x)))^k \geq \sum_{x\in G} o(x)^k = \psi_k(G).$$

Em **[AmiM20]** o autor denota $\psi_k(G) = \psi^{f,k}(G)$, onde $f(x) = x$ para todo $x \in \mathbb{R}$. No artigo **[AmiM20]** tem outras implicações para existência de tal bijeção.

Bibliografia

[AA11] AMIRI, Habib; AMIRI, S. M. Jafarian - Sum of element orders on finite groups of the same order, - *Journal of Algebra and Its Applications,* ***10****(2) (2011), 187-190.*

[AA14a] AMIRI, S. M. Jafarian; AMIRI, Mohsen - Second maximum sum of element orders on finite groups, - *Journal of Pure and Applied Algebra,* ***218****(3) (2014), 531-539.*

[AA14b] AMIRI, S. M. Jafarian; AMIRI, Mohsen - Sum of the Products of the Orders of Two Distinct Elements in Finite Groups, - *Communications in Algebra,* ***43****(12) (2014), 5319-5328.*

[AAI09] AMIRI, Habib; AMIRI, S. M. Jafarian; ISAACS, I. Martin - Sums of element orders in finite groups - *Communications in Algebra* ***37****(9) (2009) 2978–2980.*

[AmiJ13] AMIRI, S. M. Jafarian - Characterization of A_5 and $PSL(2,7)$ by sum of element orders, - *International Journal of Group Theory,* ***2****(2) (2013), 35-39.*

[AmiM20] AMIRI, Mohsen - A bijection from a finite group to the cyclic group with a divisibility property on the element orders , - *arXiv:2002.11455.*

[AK18] AZAD, M. Baniasad; KHOSRAVI, B. - A Criterion for Solvability of a Finite Group by the Sum of Element Orders, - *Journal of Algebra,* ***516*** *(2018), 115-124.*

[AK19] AZAD, M. Baniasad; KHOSRAVI, B. - On Two Conjectures about the Sum of Element Orders, - *arXiv:1905.00815.*

[GAP] The GAP Group, GAP – Groups, Algorithms, and Programming, - *Version 4.10*

[GP17] GARONZI, M.; PATASSINI, M. - Inequalities detecting structural properties of a finite group, - *Communications in Algebra,* ***45****(2) (2017), 677-687.*

[Gor80] GORENSTEIN, Daniel - Finite Groups, 2. ed. - *AMS Chelsea Publishing. New York, 1980.*

[HLM18a] 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* ***222****(7) (2018), 1628-1642.*

[HLM18b] HERZOG, Marcel; LONGOBARDI, Patrizia; MAJ, Mercede - Properties of Finite and periodic groups determined by their elements orders (a survey), - *Group Theory and Computation, Indian Statistical Institute Series, Editors N.S. Narasimha Sastry, Manoj Kumar Yadav, (2018), 59-90.*

[HLM19] HERZOG, Marcel; LONGOBARDI, Patrizia; MAJ, Mercede - The second maximal groups with respect to the sum of element orders, - *arXiv:1901.09662.*

[Isa08] ISAACS, I. Martin - Finite Group Theory - *Graduate studies in mathematics, 92. American Mathematical Society, 2008.*

[Kou18] MAZUROV, V. D.; KHUHRO, E. I. - Unsolved problems in group theory. The Kourovka Notebook. No. 19 - *Russian Academy of Sciences, Novosibirsk, 2018.*

[Mac12] MACHÌ, Antonio - Groups, An Introduction to Ideas and Methods of the Theory of Groups (2nd edition) - *UNITEXT - Springer-Verlag, 2012.*

[Mar19] MAREFAT, Yadollah et al. - The minimum sum of element orders of finite groups - *International Journal of Group Theory, DOI: 10.22108/IJGT.2019.115910.1538.*

[MIT13] MAREFAT, Y.; IRANMANESH, A.; TEHNARIAN, A. - On the sum of element orders of finite simple groups , - *Journal of Algebra and Its Applications,* ***12****(07) (2013)*

[NA68] NOVIKOV, P.S.; ADJAN, S.I. - Infinite periodic groups I, II, III, - *Izv. Akad. Nauk SSSR Ser. Mat.,* ***32*** *(1968), 212–244, 251–524, 709–731.*

[PS00] PAKIANATHAN, J.; SHANKAR, K. - Nilpotent Numbers, - *The American Mathematical Monthly,* ***107****(07) (2000), 631-634.*

[Rob93] ROBINSON - Derek J. S. - *Graduate Texts in Mathematics - Springer-Verlag, New York, 1993.*

[Rose09] ROSE, Harvey E. - A Course on Finite Groups, - *Universitext - Springer-Verlag, London, 2009.*

[SCW15] SHEN, R.; CHEN, G.; WU, C. - On groups with the second largest value of the sum of element orders, - *Communications in Algebra,* ***43****(06) (2015), 2618-2631.*

[Ser16] SERRE, Jean-Pierre - Finite Groups: An Introduction - *International Press, Boston Inc., 2016.*

[Ser73] SERRE, Jean-Pierre - A Course in Arithmetic - *Graduate texts in mathematics, 7. Springer-Verlag, New York, 1973.*

[Tar19] TARNAUCEANU, M. - A criterion for nilpotency of a finite group by the sum of element orders - *arXiv:1903.09744.*