UNIVERSIDADE FEDERAL DO AMAZONAS - UFAM
INSTITUTO DE CIÊNCIAS EXATAS - ICE
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

SOBRE ELEMENTOS EM GRUPOS FINITOS CUJOS ÍNDICES DE SEUS CENTRALIZADORES SÃO POTÊNCIAS DE PRIMO

Josean da Silva Alves

RIO BRANCO - 2014

UNIVERSIDADE FEDERAL DO AMAZONAS - UFAM
INSTITUTO DE CIÊNCIAS EXATAS - ICE
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Josean da Silva Alves

SOBRE ELEMENTOS EM GRUPOS FINITOS CUJOS ÍNDICES DE SEUS CENTRALIZADORES SÃO POTÊNCIAS DE PRIMO

Dissertação apresentada ao Programa de Pós-Graduação em Matemática - Mestrado Interinstitucional CAPES/FUNTAC/UFAM/UFAC, como requisito parcial para obtenção do título de Mestre em Matemática, na área de concentração: Álgebra.

Orientador: Prof. Dr. Sérgio Brazil Junior

RIO BRANCO - 2014

Josean da Silva Alves

SOBRE ELEMENTOS EM GRUPOS FINITOS CUJOS ÍNDICES DE SEUS CENTRALIZADORES SÃO POTÊNCIAS DE PRIMO

Dissertação apresentada ao Programa de Pós-Graduação em Matemática - Mestrado Interinstitucional CAPES/FUNTAC/UFAM/UFAC, como requisito parcial para obtenção do título de Mestre em Matemática, área de concentração: Álgebra.

Rio Branco, 04 de junho de 2014.

BANCA EXAMINADORA

.....

Prof° Dr. Sérgio Brazil Junior, Presidente

Universidade Federal do Acre

.....

Profº Dr. José Ivan da Silva Ramos, Membro

Universidade Federal do Acre

.....

Profº Dr. Antônio Carlos Tamarozzi, Membro

Universidade Federal de Mato Grosso do Sul

AGRADECIMENTOS

- À Deus por todas as graças concebidas em minha vida.
- À minha família pelo apoio e compreensão, em especial, minha mãe, Custódia e minha esposa, Janaína.
- Aos membros da banca examinadora pelas sugestões dadas para melhoria desta dissertação.
- Ao professor Sérgio pela orientação, paciência e estímulo constante.
- Aos professores do Programa de Pós-Graduação em Matemática da Universidade Federal do Amazonas e o professor José Ivan que contribuiram para minha formação acadêmica.
- Aos colegas do Mestrado pela convivência e apoio.
- À Fundação de Tecnologia do Estado do Acre - FUNTAC pelo apoio financeiro.

RESUMO

SOBRE ELEMENTOS EM GRUPOS FINITOS CUJO O ÍNDICE DE SEU CENTRALIZADOR É UMA POTÊNCIA DE PRIMO

No presente trabalho estamos interessados em encontrar condições suficientes para que o elemento $x \in G$ tenha índice potência de primo. Seja x um elemento de um grupo finito G, denotaremos por $Ind_G(x)$ o índice de $C_G(x)$ em G. De modo mais geral, se $H \leq G$, denotaremos o índice de $[H : C_H(x)]$ por $Ind_H(x)$.

Palavras-chave: Grupos Finitos e Centralizadores.

ABSTRACT

ON ELEMENTS IN FINITE GROUPS WHICH INDEX OF YOUR CENTRALIZER IS A PRIME-POWER

In the present work we are interested in finding sufficient conditions for element $x \in G$ to have prime-power index. Let x an be element in a group G, we will denote by $Ind_G(x)$ the index of $C_G(x)$ in G. More generally, if $H \leq G$ we denote the index $[H : C_H(x)]$ by $Ind_H(x)$.

Keywords: Finite Groups and Centralizers .

Sumário

Notações

G	Grupo.
$\|G\|$	Ordem de um grupo.
$\mathbb{S}_X$	Conjunto das permutações de X em X.
1_G	Identidade do grupo G.
$Z(G)$	Centro do grupo G.
$\mathcal{O}(x)$, Gx	A órbita de x.
gH	Classe Latreral à esquerda.
$C_G(x)$	Centralizador do subgrupo H no grupo G.
$N_G(H)$	Nomalizador do subgrupo H no grupo G.
$[G : H]$	Índece do subgrupo H no grupo G.
$N \lhd G$	N é subgrupo normal próprio do grupo G.
$N \trianglelefteq G$	N é subgrupo normal do grupo G.
$N \leq G$	N é subgrupo do grupo G.
$N < G$	N é subgrupo próprio do grupo G.
$\frac{G}{H}$	Grupo quociente de G pelo subgrupo normal H.
$[a, b] = a^{-1}b^{-1}ab$	Comutador dos elementos a e b.
$[H, K]$	Subgrupo comutador dos subgrupos H e K do grupo G.
$G' = [G, G]$	Subgrupo derivado de G.
$cl(G)$	Classe de nilpotência de G.
$\mathfrak{N}$	Classe dos grupos nilpotentes.
$\mathfrak{N}_c$	Classe dos grupos nilpotentes de classe menor ou igual a c.

$F(G)$	Subgrupo de Fitting.
$O_p(G)$	p-Radical de G.
$\langle x^G \rangle$	Fecho normal de $x \in G$ em G.
$\mathfrak{N}G$	Classe dos subgrupos nilpotentes de G.
$R(G)$	Radical solúvel de G.
$\mathbb{P}$	Conjunto dos números primos.
$\mathfrak{B}_\pi$	Classe dos π-grupos.
$\mathfrak{B}_\pi G$	Classe dos π-subgrupos de G.
$Ind_G(x)$	Índice de x em G.
H^g	Classe de conjugação de H em G.
$Syl_p(G)$	O conjunto dos Sylow p-subgrupos de ordem potência de primo p em G.

Introdução

No presente trabalho, estudamos algumas relações suficientes para garantir que o índice do centralizador de um elemento x de um grupo G seja uma potência de primo. Dado um elemento x em um grupo finito G, iremos denotar por $Ind_G(x)$, o índice de $C_G(x)$ em G, que será chamado, neste contexto, simplesmente de **índice de x em G**. De modo mais geral, se $H \leq G$, denotaremos o índice $[H : C_H(x)]$ por $Ind_H(x)$.

Recentemente, a seguinte questão foi conjecturada por Alan Camina, Pavel Shumyatsky e Carmela Sica [4]:

Seja G um grupo finito e $x \in G$. Suponha que $Ind_{\langle a,x\rangle}(x)$ é uma potência de primo, para qualquer $a \in G$. É verdade que $Ind_G(x)$ é uma potência de primo?

A resposta para esta questão é negativa. Poderemos obeservar no capítulo 2 dessa dissertação um exemplo que comprova tal resposta. Em seguida, a questão proposta acima foi reformulada, passando a ser apresntada da seguinte maneira:

Seja G um grupo finito e p um primo. Suponha que, para $x \in G$, o $Ind_{\langle a,x\rangle}(x)$ é uma potência de primo, para qualquer $a \in G$. É verdade que $Ind_G(x)$ é uma potência de primo?

Com resposta positiva, obteve-se, na verdade, um caso mais geral, cuja demonstração será um dos principais objetivos de nosso capítulo 2.

Um fato importante é o teorema clássico de Burnside que diz: se um grupo G contém um elemento x de índice potência de primo, então, G não é simples [[15], p. 131], pois, a partir do $Ind_G(x)$, para algum $x \in G$, permite verificar se G não é simples, ou seja, este resultado está relacionado diretamente com a classificação dos grupos finitos simples. Além disso, Kazarin deduziu que um elemento x nessas condições pertence a $S(G)$, o radical solúvel de G [22]. Daí resulta que x reside no segundo termo da série de Fitting

de G [5].

O objetivo principal deste trabalho é discorrer sobre as condições usadas para provar que: se $Ind_{\langle a,b,x\rangle}(x)$ é uma potência de primo para qualquer $a, b \in G$, então $Ind_G(x)$ é uma potência de primo.

O primeiro capítulo tem por finalidade abordar definições e resultados básicos de grupos finitos que servirão de base ao segundo capítulo.

No segundo capítulo, faremos um estudo relativamente aprofundado de elementos de um grupo cujos índices são potências de primos e, em seguida, daremos ênfase à motivação deste trabalho, o artigo de Alan R. Camina, Pavel Shumyatsky e Carmela Sica [4], que trata de elementos cujos índices dos centralizadores são potências de primos.

Finalmente, no Anexo, faremos uma breve abordagem histórica da Classificação dos Grupos Finitos Simples e da influência do Teorema da Ordem Ímpar nesta classificação.

Capítulo 1

Noções Básicas da Teoria dos Grupos Finitos

Neste capítulo vamos lembrar algumas notações, fatos e conceitos essenciais da teoria dos grupos. Devido as limitações óbvias de uma dissertação de mestrado, alguns resultados serão enunciados sem demonstrações. No entanto, demonstraremos alguns resultados fundamentais para o desenvolvimento do tema central deste trabalho. No decorrer desse capítulo, destacaremos ainda, temas importantes relacionados aos grupos finitos, como, por exemplo, os p-grupos, dando destaque aos Teoremas de Sylow, que são de referência constante em qualquer curso sobre teoria dos grupos. Além disso, cometaremos um pouco sobre grupos finitos solúveis e nilpotentes, destacando o subgrupo de Fitting e, finalmente, definiremos o π-número, apresentando algumas propriedades.

1.1 Ações de Grupos

Até o início do século XX, os grupos estudados foram quase todos considerados como grupos de permutações, de modo que seus elementos agiam de forma natural num conjunto. Conforme tornou-se mais abstrata, a teoria dos grupos, ficou envidente que a ideia de ações de grupos são muito úteis quando os elementos do grupo agem num conjunto. Nesta seção, desenvolvemos a teoria básica das ações de grupos enfatizando sua utilidade teórica nos grupos finitos.

Definição 1.1. *Seja G um grupo e X um conjunto não vazio. Uma* ***ação à esquerda*** *de G em X é uma aplicação*

$$\psi : G \times X \longrightarrow X,$$

que denotamos, por conveniência, $\psi((g,x)) = gx$*, tal que:*

i) $1_G x = x$*, para todo* $x \in X$*; e*

ii) $g_1(g_2x) = (g_1g_2)x$*, para todo* $g_1, g_2 \in G$ *e* $x \in X$*.*

Analogamente, uma ***ação à direita*** *de* G *em* X *é uma aplicação*

$$\varphi : X \times G \longrightarrow X,$$

que denotamos, por conveniência, $\psi((x,g)) = xg$*, tal que:*

i) $x1_G = x$*, para todo* $x \in X$*; e*

ii) $(xg_2)g_1 = x(g_1g_2)$*, para todo* $g_1, g_2 \in G$ *e* $x \in X$*.*

Em ambos os casos, dizemos que X é um G-conjunto.

Exemplo 1.1 (Ação por conjugação)**.** *Uma ação natural de um grupo* G *em si mesmo é a* ***ação por conjugação****, definida da seguinte forma:*

$$g \cdot x = x^g = gxg^{-1},$$

onde $x, g \in G$*.*

Uma outra maneira de um grupo G *agir, por conjugação, é no conjunto de seus subgrupos, ou seja, se* $H \leq G$*, definimos por:*

$$g \cdot H = H^g = gHg^{-1} = \{ghg^{-1} \mid h \in H \text{ e } g \in G\}.$$

Nos dois casos, é simples verificar que as condições i) e ii) da definicão 1.1 são satisfeitas,isto é, podemos demonstrar que as aplicações definidas acima são ações de grupos.

Em seguinda, definimos dois aspectos fundamentais de G-conjuntos.

Definição 1.2. *Seja* X *um* G*-conjunto e* $x \in X$*. Dizemos que, a* G*-órbita de* x *é:*

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

Muitas vezes denota-se a órbita $\mathcal{O}(x)$ por Gx. Normalmente, diremos órbita ao invés de G-órbita. As órbitas de X formam uma partição do conjunto$X$, na verdade, a relação $x \equiv y$, definida por "$y = gx$, para alguns $g \in G$ ", é uma relação de equivalência cujas classes de equivalência são as órbitas.

Definição 1.3. *Seja X um G-conjunto e $x \in X$. Dizemos que, o estabilizador de x em G, denotado por G_x, é o subgrupo*

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

Vejamos as órbitas e os estabilizadores nos G-conjuntos do exemplo 1.1.

Exemplo 1.2. *Seja G um grupo qualquer.*

1. *Na ação por conjugação de G em G, a G-órbita de $x \in G$ é a classe de conjugação de x, isto é, $\{gxg^{-1} \mid g \in G\}$ e o estabilizador de x em G consiste de todos $g \in G$ tal que $gxg^{-1} = x$, ou seja, $gx = xg$. Este subgrupo é chamado o **centralizador** de x em G, sendo denotado por*

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

2. *Na ação por conjugação de G em seu conjunto de subgrupos, a G-órbita de $H \leq G$ é apenas o conjunto de todos os conjugados de H em G, ou seja, $\{gHg^{-1} \mid g \in G\}$. O estabilizador de H em G é um subgrupo importante denominado, **normalizador** de H em G, isto é:*

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

Ambos, centralizadores e normalizadores, têm grande destaque em toda teoria dos grupos.

Teorema 1.1. *Se X é um G-conjunto e $x \in X$, então*

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

Demonstração. Se $x \in X$, denota-se $\frac{G}{G_x}$ a família de todos as classes laterais a esquerda de G_x em G. Definindo $f : \mathcal{O}(x) \longrightarrow \frac{G}{G_x}$, tal que, $f(ax) = aG_x$. Observe que f está bem definida, se $ax = bx$, para algum $b \in G$, então $b^{-1}ax = x$, $b^{-1}a \in G$, e $aG_x = bG_x$. A função f é injetiva, pois, se $aG_x = f(ax) = f(cx) = cG_x$, para algum $c \in G$, então $c^{-1}a \in G$, $c^{-1}ax = x$, e asim, $ax = cx$. E ainda, f é sobrejetiva, pois, para todo $a \in G$ tem-se $aG_x = f(ax)$. Portanto, f é bijetiva e $|\mathcal{O}(x)| = \left|\frac{G}{G_x}\right| = [G : G_x]$. ■

Corolário 1.1. *Seja G um grupo finito.*

i) *Se $x \in G$, então o número de conjugados de x em G é igual a $[G : C_G(x)]$.*

ii) *Se $H \leq G$, então o número de conjugados de H em G é igual a $[G : N_G(H)]$.*

Demonstração. Use os Exemplos 1.2 e 1.3. ■

Definição 1.4. *O **centro** de um grupo G, que denotamos por $Z(G)$, é o conjunto de todos $g \in G$ que comutam com qualquer elemento de G, ou seja:*

$$Z(G) = \{z \in G \mid zg = gz, \forall g \in G\}$$

Note também que, $x \in Z(G)$ se, e somente se, $\mathcal{O}(x) = \{x\}$. De fato, seja $\mathcal{O}(x)$ a classe de conjugação de $x \in G$. Temos que:

$$x \in Z(G) \Leftrightarrow xg = gx, \forall g \in G \Leftrightarrow g^{-1}xg = x, \forall g \in G \Leftrightarrow \mathcal{O}(x) = \{x\}.$$

A partir dessas ideias vamos apresentar, a seguir, o teorema conhecido como **Equação das Classes**.

Teorema 1.2 (Equação das Classes). *Suponhamos que G é um grupo finito e $x_i \in G$ com $i = 1, 2, \ldots, k$. Se $\mathcal{O}(x_1)$, $\mathcal{O}(x_2)$, $\ldots$, $\mathcal{O}(x_k)$ é uma lista completa das classes de conjugação de G cujas ordens são maiores do que 1. Tem-se:*

i) $G = Z(G) \overset{\bullet}{\bigcup} \left\{ \overset{\bullet}{\bigcup}_{i=1}^{k} \mathcal{O}(x_i) \right\}$ *(união disjunta).*

ii) $|G| = |Z(G)| + \sum_{i=1}^{k} |\mathcal{O}(x_i)| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]$.

Demonstração. **i)** Seja $\mathcal{C} = \{x_1, x_2, \ldots, x_n\}$ uma coleção completa de representantes das classes de conjugação da ação G em G. Como sabemos, G é a união disjunta das suas classes de conjugação. Assim,

$$G = \bigcup_{x_i \in \mathcal{C}} \mathcal{O}(x_i)$$

Da definição 1.4, temos que, os elementos do centro geram classes de conjugação unitárias. Por hipótese, seja $x_1, x_2, \ldots, x_k$ são representantes, respectivamente, de cada uma das classes de conjugação $\mathcal{O}(x_1), \mathcal{O}(x_2), \ldots, \mathcal{O}(x_k)$, cujas ordens são maiores que 1. Então,

$$G = \left\{ \dot{\bigcup_{\substack{x_i \in \mathcal{C} \\ x_i \in Z(G)}}} \mathcal{O}(x_i) \right\} \dot{\bigcup} \left\{ \dot{\bigcup_{\substack{x_i \in \mathcal{C} \\ x_i \notin Z(G)}}} \mathcal{O}(x_i) \right\} = Z(G) \dot{\bigcup} \left\{ \dot{\bigcup}_{i=1}^{k} \mathcal{O}(x_i) \right\}.$$

ii) Pela item i) os elementos de $G - Z(G)$ estão em classes de conjugação de mais de um elemento. Portanto, se G é abeliano, a equação se reduz a $|G| = |Z(G)|$, pois, nesse caso $G = Z(G)$. Por outro lado, se G é não-abeliano, temos que $G - Z(G) \neq \varnothing$. Por hipótese, $x_1, x_2, \ldots, x_k$ são representantes de cada uma das classes de conjugação cujas ordens são maiores que 1. Então, podemos escrever as classes de conjugação como $\mathcal{O}(x_1), \mathcal{O}(x_2), \ldots, \mathcal{O}(x_k)$. Logo,

$$|G - Z(G)| = \left| \dot{\bigcup}_{i=1}^{k} \mathcal{O}(x_i) \right| = \sum_{i=1}^{k} |\mathcal{O}(x_i)|,$$

ou seja,

$$|G| = |Z(G)| + \sum_{i=1}^{k} |\mathcal{O}(x_i)| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]. \qquad \blacksquare$$

As equações em *i*) e *ii*), acima, são chamadas **Equações das Classes** de G.

1.2 p-Grupos Finitos e os Teoremas de Sylow

Nesta seção, apresentamos alguns conceitos considerando grupos cuja ordem são potências de um número primo p. Esses grupos têm uma série de propriedades úteis, por exemplo, eles têm subgrupos normais para todos as ordens que dividem a ordem do grupo.

Um resultado importante que não podemos deixar de enunciar e demonstrar é o Teorema de Cauchy, ferramenta importante na caracterização dos p-grupos.

Sabe-se também que, no geral, a recíproca do Teorema de Lagrange não é verdadeira, porém, é verdadeiro para grupos que são potências de primo, isto é, para os subgrupos que são p-grupos. Este é o começo da teoria de Sylow e o ponto de partida para a teoria dos grupos finitos.

Iniciamente, faremos uma breve abordagem sobre o princípio do contra-exemplo minimal, ferramenta poderosa da teoria dos grupos finitos. Em seguinda, vamos conceituar algumas propriedades básicas de p-grupos finitos e demostrar os Teoremas de Sylow.

Observação 1.1. *Seja $\mathcal{P}(X)$ uma sentença aberta, onde X corresponde a um grupo finito. Por exemplo, para todo $H \subseteq X$, se $H \neq \varnothing$ e $ab^{-1} \in H$, para quaisquer $a, b \in H$. Então, $|H| \,|\, |X|$.*

Seja $\mathcal{G} = \{G \mid \mathcal{P}(G)$ é falso$\}$ a família dos contra-exemplos e $\mathcal{N} = \{|G| \mid G \in \mathcal{G}\}$ um subconjunto dos números naturais .

Se $\mathcal{G} = \varnothing$, então $\mathcal{N} = \varnothing$ e pelo princípio da boa ordenação de $\mathbb{N}$, existe $m \in \mathcal{N}$ que é o elemento mínimo de $\mathcal{N}$.

Considerando $\mathcal{X} = \{G \in \mathcal{G} \mid |G| = m\}$ a família dos contra-exemplos minimais. Tem-se:

i) *Se $G \in \mathcal{X}$ e $\langle 1_G \rangle \neq H \lneq G$, então $H \notin \mathcal{G}$, i. e., a sentença $\mathcal{P}(H)$ é verdadeira.*

ii) *Se $G \in \mathcal{X}$ e $\langle 1_G \rangle \neq N \lhd G$, então $\dfrac{G}{N} \notin \mathcal{G}$, i. e., a sentença $\mathcal{P}\left(\dfrac{G}{N}\right)$ é verdadeira.*

Definição 1.5. *Seja p um primo fixo. Um grupo G é chamado de p-grupo se todos os seus elementos tem ordem potência de p.*

O grupo trivial $\langle 1_G \rangle$ é um p-grupo para todo número primo p, pois $p^0 = 1$. No caso finito, a definição 1.5 pode ser substituído por: G é um p-grupo finito se, e somente se, $|G|$ é uma potência de p.

Isso decorre do Teorema de Cauchy que enuciamos a seguir. Mas primeiro, vejamos o seguinte lema:

Lema 1.1. *Se G é um grupo abeliano finito cuja ordem é divisível por um primo p, então G contém um elemento de ordem p.*

Demonstração. Considerando $|G| = pm$, onde $m \geq 1$. Vamos proceder por indução em m. Claro que, para $m = 1$ tem-se $|G| = p$, isto é, G é um p-grupo e por definição, G possui um elemento de ordem p. Agora, suponhamos que, $g \in G$ é um elemento de ordem $t > 1$. Se $p \mid t$ tem-se $1_G = g^t = g^{pk} = (g^k)^p$. Logo, $g^k \in G$ é de ordem p. Portanto, o lema está provado. Por outro lado, podemos assumir que a ordem de g não é divisível por p. No entanto, G é abeliano, assim, $\langle g \rangle$ é um subgrupo normal de G e $\dfrac{G}{\langle g \rangle}$ é um grupo abeliano de ordem $\dfrac{|G|}{\langle g \rangle} = \dfrac{pm}{t}$. Como $p \nmid t$, temos que o número inteiro $\frac{m}{t} < m$. Por indução, existe $\overline{y} \in \dfrac{G}{\langle g \rangle}$ de ordem p. Consideremos o homomorfismo canônico $\varphi : G \longrightarrow \dfrac{G}{\langle g \rangle}$, e assuma $y \in G$, tal que $\varphi(y) = \overline{y}$. Como $y^t = 1_G$, temos que $\varphi(y^t) = \varphi(1_G)$, ou seja, $\overline{y}^t = \overline{1_G}$ e, portanto, t é múltiplo da ordem de $\overline{y}$. Isto é, t é um múltiplo de p, digamos, $t = rp$ com $r \geq 1$. Então, y^r é um elemento de G de ordem p. ■

Teorema 1.3 (**Teorema de Cauchy**). *Se G é um grupo finito e p um número primo, tal que $p \mid |G|$, então G contém, pelo menos, um elemento de ordem p.*

Demonstração. Pelo Corolário 1.1 item (i). Se $x \in G$, então o número de conjugados de x é $[G : C_G(x)]$. Se $x \notin Z(G)$, então sua classe de conjugação tem mais de um elemento, assim, $|C_G(x)| < |G|$. Se $p \mid |C_G(x)|$, para tal x não central, segue do teorema. Por outro lado, podemos supor que, $p \nmid |C_G(x)|$ para todo x não central em G. No entanto, uma vez que, $|G| = [G : C_G(x)]|C_{G(x)}|$, podemos assumir que, $p \mid [G : C_G(x)]$

Considerando, agora a equação das classes, tem-se:

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

onde, cada um x_i é seleccionado a partir de cada classe de conjugação com mais de um elemento. Desde que, $|G|$ e todos $[G : C_G(x)]$ são divisíveis por p, segue que, $|Z(G)|$ é divisível por p. Mas, $Z(G)$ é abeliano e, assim, contém um elemento de ordem p, pelo lema 1.1. ■

Cauchy provou este resultado para os grupos de permutação, em 1845, como parte de uma série de artigos sobre as propriedades de permutações. Com toda as possibilidades, a primeira prova para grupos gerais foi dada por Jordan, em 1870.

Corolário 1.2. *Se G é um grupo finito e p um primo, então G é um p-grupo se, e somente se, $|G| = p^r$, para algum número inteiro não negativo r.*

Demonstração. Suponha que, G é um p-grupo finito cuja $|G|$ não é uma potência de p. Então, existe $q \neq p$, com q primo, tal que, $q \mid |G|$. Então, pelo teorema de Cauchy, existe um elemento de G de ordem q uma contradição, pois, G é um p-grupo. Por outro lado, se $|G|$ é potência de p, então, para todo $g \in G$, $|\langle g \rangle| \mid |G|$, pelo Teorema de Lagrange, temos que, $|\langle g \rangle|$ é uma potência de p e, portanto, G é um p-grupo. ■

Em seguida , mostraremos que a propriedade de ser p-grupo é preservada para os subgrupos, grupos quocientes e extensões.

Teorema 1.4. *Seja G um grupo e $K \trianglelefteq G$. Tem-se:*

i) *Se G é um p-grupo, então todos os subgrupos e quocientes de G são p-grupos.*

ii) *Se K e $\dfrac{G}{K}$ são ambos p-grupos, então G também é um p-grupo.*

Demonstração. i) A primeira parte, ligado a subgrupo, decorre da definição. Para a segunda parte, suponhamos que, $g \in G$ e $|\langle g \rangle| = p^r$, então pelas classes laterais tem-se $K = 1_G K = g^{p^r} K = (gK)^{p^r}$. Daí, a ordem de gK é divisor de p^r, e por isso a ordem de cada elemento de $\dfrac{G}{K}$ é potência de p.

ii) Se $g \in G$, então $(gK)^{p^r} = K$, para algum inteiro r pela segunda hipótese, daí $g^{p^r} \in K$. Mas, K é um p-grupo (a primeira hipótese), assim, $\left|\langle g^{p^r} \rangle\right| = p^s$ para algum inteiro não negativo s, de modo que a ordem de g é um divisor de p^{r+s}. O resultado segue, pois, isso vale para todo $g \in G$. ■

Teorema 1.5. *Seja G um p-grupo finito e $1_G \neq N \trianglelefteq G$. Então, $N \cap Z(G) \neq 1_G$. Em particular, o centro de um p-grupo não trivial é não trivial.*

Demonstração. Ver [9], p. 244. ■

Corolário 1.3. *Seja G um p-grupo finito. Então, qualquer subgrupo normal de G de ordem p é central em G.*

Demonstração. Claro que, $1_G < N \cap Z(G) \leq N$. Porém, pela hipótese e o Teorema 1.3, tem-se $|N \cap Z(G)| = p = |N|$. Assim, $N \cap Z(G) = N$, e portanto, $N \leq Z(G)$. ■

Teorema 1.6. *Se G é um grupo com a ordem p^r, então G é um p-grupo finito e tem subgrupos $G_0, ..., G_r$ satisfazendo:*

i) $G_0 = \langle 1_G \rangle$ *e* $G_r = G$, *para algum* $r > 0$;

ii) $G_i \lhd G$ *e* $G_{i-1} \lhd G_i$, *para* $i = 1, ..., r$;

iii) $|G_i| = p^i$, *para* $i = 1, ..., r$.

Demonstração. Ver [26], p.116. ■

No entanto, existe uma extensão do Teorema 1.6 que aplica-se quando K é um subgrupo maximal de G. Neste caso, K tem índice primo e é normal em G. A seguir, enunciaremos tal teorema.

Teorema 1.7. *Seja G é um p-grupo finito.*

i) *Se H é um subgrupo próprio de G. Então, $H < N_G(H)$.*

ii) *Todo subgrupo maximal de G é normal e tem índice p.*

Demonstração. i) (Indução sobre $|G|$). Se $|G| = p$ a afirmação é verdadeira, pois $H = 1_G < G = N_G(1)$. Suponhamos que $|G| > p$. Se $Z(G) \nleq H$ tem-se $H < HZ(G) \leq N_G(H)$, implicando em $H < N_G(H)$. Agora, vamos assumir que $Z(G) \leq H$. Como $1_G \neq Z(G)$, por indução, temos que $\dfrac{H}{Z(G)} < N_{\frac{G}{Z(G)}}\left(\dfrac{H}{Z(G)}\right) = \dfrac{N_G(H)}{Z(G)}$. Portanto, $H < N_G(H)$.

ii) Seja M um subgrupo maximal de G, por (i), $M < N_G(M) \leq G$, implicando que $N_G(M) = G$. Logo, $M \trianglelefteq G$. Agora, $\dfrac{G}{M}$ é um p-grupo, tal que o único subgrupo é o trivial e, portanto, $\left|\dfrac{G}{M}\right| = p$. ■

Sabemos que a recíproca do Teorema de Lagrange é falsa, isto é, se $m \mid |G|$ não podemos garantir que G tem um subgrupo de ordem m. Por exemplo, A_5 não tem subgrupo de ordem 15, ver [26], p.101. Mas há uma recíproca parcial se restringirmos m a potência de um primo, ou seja, se p^r é a maior potência de p dividindo $|G|$, então, veremos que

G contém um subgrupo de ordem p^r. Quaisquer dois desses subgrupos são conjugados, e o número deles podem ser contados a patir, de uma congruência. Começamos com o teorema principal, da existência, provado, primeiramente, pelo matemático norueguês, Ludwig Sylow (1832-1918), em 1872. Os resultados, a seguir, são fundamentais para a compreensão da estrutura de um grupo finito.

Teorema 1.8 (Teorema de Sylow I)**.** *Se G é um grupo finito com ordem $p^r m$, onde p é primo e $p \nmid m$, então G contém um subgrupo de ordem p^r.*

Demonstração. Usamos indução sobre $|G| = n$, não há nada para provar se $n = 1$. Suponhamos que, $n > 1$ e o resultado é válido para todo grupo de ordem $n \leq c - 1$. Considere, $c = |G| = p^r m$.

- Se $r = 0$, tem-se $H = \{1_G\}$ com ordem $1 = p^0$.
- Se $r \geq 1$, tem-se duas possibilidades:

  (1) $p \mid |Z(G)|$

  (2) $p \nmid |Z(G)|$

No caso (1), sabemos que existe $a \in Z(G)$, tal que, $|\langle a \rangle| = p$. Logo, $H = \langle a \rangle$ é subgrupo normal de G de ordem p. Assim, o grupo $\dfrac{G}{H}$ tem ordem $p^{r-1}m$. Mas, por hipótese de indução, tem-se que $\dfrac{G}{H}$ têm subgrupos $\dfrac{K_i}{H}$, pelo teorema da correspondência, K_i são subgrupos de G contendo H, tais que,

$$\left|\frac{K_i}{H}\right| = p^i,\ i \in \{1, 2, \ldots, r-1\}.$$

Assim,

$$|K_i| = |H|p^i = p^{i+1},\ i \in \{1, 2, \ldots, r-1\}.$$

Definindo, $H_0 = \{1_G\}$ e $H_i = K_{i-1}$, para $i \in \{1, 2, \ldots, r\}$.

No caso (2), olhando para a equação das classes:

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C_G(a)],$$

tem-se que existe $a \notin Z(G)$, tal que, $p \nmid [G : C_G(a)]$. Mas, $|G| = [G : C_G(a)]\,|C_G(a)|$ isto implica que $p \mid |C_G(a)|$, e como $|C_G(a)| < |G|$, pela hipótese de indução, $C_G(a)$ tem subgrupos H_i de ordem p^i para todo $i \in \{0, 1, \ldots, r\}$. Logo, como H_i é subgrupo de G. Daí, segue o resultado. ■

Definição 1.6. *Seja $|G| = p^r m$ com p primo e $p \nmid m$. Um subgrupo de G com ordem p^r é chamado um* ***Sylow p-subgrupo*** *de G. Um Sylow subgrupo é um Sylow p-subgrupo para algum primo p.*

Definição 1.7. *Se p é um primo. Então, um Sylow p-subgrupo P de um grupo G é um p-subgrupo maximal de G.*

Teorema 1.9 (Teorema de Sylow II)**.** *Seja G um grupo finito e p um primo. Então:*

i) *todo p-subgrupo de G está contido num Sylow p-subgrupo de G;*

ii) *todos os Sylow p-subgrupos de G são conjugados. Se P é um Sylow p-subgrupo de G e n_p é o número de Sylow p-subgrupos de G, temos $n_p = [G : N_G(P)]$;*

iii) *se n_p é o número de p-subgrupos de Sylow de G, temos $n_p \equiv 1 \pmod{p}$.*

Demonstração. i) Seja P um Sylow p-subgrupo de G e $\mathcal{X}$ denota o conjunto de subgrupos conjugado de P em G, isto é, $\mathcal{X} = \{g^{-1}Pg \,;\, g \in G\}$. Agora, seja R um p-subgrupo de G e suponha que, R age sobre $\mathcal{X}$, por conjugação, da seguinte maneira:

$$(g^{-1}Pg)x = x^{-1}(g^{-1}Pg)x = (gx)^{-1}P(gx), \text{ para } g \in G \text{ e } x \in R$$

Como R é um p-grupo, o teorema da Órbita-Estalizador, mostra que a ordem de uma órbita dessa ação é uma potência de p, possivelmente, $p^0 = 1$. Agora,

$$|\mathcal{X}| = [G : N_G(P)] \text{ e } p \nmid [G : N_G(P)].$$

A equação acima, é dada pelo Corolário 1.1 (ii), e a propriedade da não divisibilidade, segue do fato de P ser um Sylow p-subgrupo de G e $N_G(P)$. Daí, $p \nmid |\mathcal{X}|$ e, portanto, como $\mathcal{X}$ é uma união disjunta de suas órbitas, deve existir pelo menos uma órbita de ordem 1. Suponha que, $\{P_1\}$ é uma órbita de ação, definida acima, com ordem 1. Então, $x^{-1}P_1x = P_1$, para todo $x \in R$, então $P_1R = RP_1$ e $RP_1 \leq G$. Mas, $P_1 \lhd RP_1$, daí $|P_1| \leq |RP_1|$. Como,

$$\frac{RP_1}{R} \simeq \frac{P_1}{R \cap P_1},$$

temos que,

$$|RP_1|\,|R \cap P_1| = |R|\,|P_1| \text{ ou } |RP_1| = |P_1|\,[R : R \cap P_1],$$

pelo Teorerma de Lagrange. Como, P_1 e R são p-grupos, concluimos que, $|RP_1|$ é uma potência de p, e assim, RP_1 é um p-subgrupo de G. Por outro lado, P_1 é um Sylow p-subgrupo de G e, portanto, sua ordem é a maior potência possível de p. Daí,

$$|RP_1| = |P_1|,$$

isto é, $RP_1 = P_1$. Logo, $R \leq P_1$. Isso prova i), pois, R é um p-subgrupo arbitrário de G.

ii) Se R usando no item i) é um Sylow p-subgrupo de G, então, $|R| = |P_1|$, assim, $R = P_1$, onde P_1 é o conjugado de P em G pela ação definida. Isso prova ii), e também, mostra que $|\mathcal{X}| = n_p$.

iii) Suponhamos que, $\{P_2\}$ é uma segunda órbita com um único elemento da ação. Então, considerando $R = P_2$, concluimos que, $P_1 = P_2$, isto é, só existe uma órbita de um único elemento. Como todas as outras órbitas tem ordem que são potência máxima de p, segue que, $|\mathcal{X}| = n_p \equiv 1 \pmod{p}$. ■

Teorema 1.10 (Teorema de Sylow III)**.** *Suponha que $|G| = p^r m$, com $p \nmid m$, e P um Sylow p-subgrupo de G.*

i) $P \lhd G$ se, e somente se, P é o único Sylow p-subgrupo de G;

ii) $n_p \mid m$.

Demonstração. i) ($\Rightarrow$) Se P é o único Sylow p- subgrupo de G, então pelo teorema 1.9 item ii), todo conjugado de P é igual a P. Logo, $P \lhd G$.
($\Leftarrow$) Consequentimente, se $P \lhd G$ temos que, $N_G(P) = G$. Como $n_p = [G : N_G(P)] = [G : G] = 1$, podemos concluir que P é o unico Sylow p-subgrupo de G.

ii) Sabendo que, $P \leq N_G(P) \leq G$, temos que:

$$m = [G : P] = [G : N_G(P)][N_G(P) : P],$$

pelo teorema de Lagrange. Como $n_p = [G : N_G(P)]$, segue que, $n_p \mid m$. ■

Teorema 1.11 (Argumento de Frattini)**.** *Seja K um subgrupo normal de um grupo finito G. Se P é um Sylow p-subgrupo de K, para algum primo p, então $G = KN_G(P)$.*

Demonstração. Para $g \in G$, temos que:

$$g^{-1}Pg \subseteq g^{-1}Kg = K,$$

com $P \leq K \lhd G$. Daí, tanto P como $g^{-1}Pg$ são Sylow subgrupos de K, e assim, por Sylow II são conjugado em K. Portanto, exite $k \in K$, tal que:

$$k^{-1}(g^{-1}Pg)k = (gk)^{-1}P(gk) = P.$$

Isso mostra que $gk \in N_G(P)$ e, assim:

$$g \in N_G(P)k^{-1} \subseteq N_G(P)K \subseteq G.$$

O resultado segue, por este argumento, já que se aplica a todos $g \in G$. ■

1.3 Um Pouco da Teoria dos Grupos Solúveis e Nilpotentes

Nesta seção, definiremos os grupos solúveis e nilpotentes, subgrupos característicos e forneceremos alguns resultados básicos que serão utilizados ao longo de nosso trabalho.

Para obtermos a definição de grupos solúveis e nilpotentes, precisaremos antes da definição de alguns tipos de séries.

Definição 1.8. *Uma* ***série subnormal*** *de um grupo G é uma sequência de subgrupos $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1_G$, onde $G_{i+1} \lhd G_i$, para todo i. Os* ***grupos fatores*** *desta série são os grupos G_i/G_{i+1}, para $i = 1, \ldots, n-1$.*

Definição 1.9. *Uma* ***série de composição*** *é uma série subnormal $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1_G$, na qual, ou G_{i+1} é um subgrupo normal maximal de G_i, ou $G_{i+1} = G_i$, para todo i. Os grupos fatores desta série são chamados* ***fatores de composição****.*

Definição 1.10. *Uma* ***série normal*** *de um grupo G é uma série subnormal $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1_G$, onde $G_{i+1} \lhd G$, para todo i.*

Agora, vamos definir os grupos solúveis.

Definição 1.11. *Um grupo G é* ***solúvel*** *se possui uma série subnormal $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1_G$, onde cada grupo fator $\dfrac{G_i}{G_{i+1}}$ é abeliano.*

Uma cadeia de subgrupos de G com esta propriedade chama-se, *série subnormal abeliana* de G e os quocientes respectivos chamam-se, *fatores* da série.

Exemplo 1.3. *Todo grupo abeliano G é solúvel.*

De fato, a cadeia$\{1_G\} \subseteq G$ é uma série subnormal abeliana.

Exemplo 1.4. *Todo grupo de ordem 12 é solúvel.*

Pelo teorema de Sylow, tem-se $n_2|3$ e $n_2 \equiv 1 \pmod 2$. Por outro lado, tem-se $n_3|4$ e $n_3 \equiv 1 \pmod 3$. Portando, $n_2 = 1$ ou 3 e $n_3 = 1$ ou 4. Agora, dividiremos em dois casos:

1º Caso: Se $n_3 = 1$, então existe um 3-subgrupo normal N de G que é abeliano e $[G : N] = 2^2$. Logo, $\langle 1_G\rangle \subseteq N \subseteq G$ é uma série subnormal abeliana de G.

2º Caso: Se $n_3 = 4$, então G possui $4\cdot(3-1) = 8$ elementos de ordem três, logo, $n_2 = 1$ implicando que o 2-subgrupo H é normal em G. Como $\langle H\rangle = 2^2$ e $[G : H] = 3$ a cadeia $\langle 1_G\rangle \subseteq H \subseteq G$ é subnormal abeliana.

A seguir, enunciaremos um resultado importante a respeito desta classe de grupos.

Teorema 1.12 (Feit-Thompson-1963)**.** *Todo grupo de ordem ímpar é solúvel.*

Este teorema foi conjecturado por Miller-Burnside, em 1911, e foram necessárias 255 páginas para ser provado, motivo pelo qual sua demonstração não constará no presente trabalho.

Monstraremos, agora, alguns teoremas que podem auxiliar na determinação de grupos solúveis.

Teorema 1.13. *Todo subgrupo de um grupo solúvel é solúvel.*

Demonstração. Como G é solúvel, existe uma série subnormal abeliana:

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = 1_G,$$

onde $G_{i+1} \lhd G_i$ e $\dfrac{G_i}{G_{i+1}}$ é abeliano para $0 \leq i \leq n-1$.
Considere uma série normal de H, dada por

$$H = H_0 \geq (H \cap G_1) \geq \cdots \geq (H \cap G_n) = 1_G.$$

Pelo segundo teorema do isomorfismo, temos que

$$H \cap G_{i+1} = (H \cap G_i) \cap G_{i+1} \lhd H \cap G_i, \text{ para todo } i.$$

E ainda,

$$\frac{H \cap G_i}{H \cap G_{i+1}} = \frac{H \cap G_i}{H \cap G_i \cap G_{i+1}} \cong \frac{G_{i+1}(H \cap G_i)}{G_{i+1}} \leq \frac{G_i}{G_{i+1}},$$

e assim, H tem uma série subnormal abeliana. Portanto, H é grupo solúvel. ■

Teorema 1.14. *Todo quociente de um grupo solúvel é solúvel.*

Demonstração. Seja G um grupo solúvel e $H \lhd G$ um subgrupo solúvel de G. Considerando uma série subnormal de $\frac{G}{H}$, dada por

$$\frac{G}{H} = \frac{G_0 H}{H} \geq \frac{G_1 H}{H} \geq \cdots \geq \frac{G_n H}{H} = \frac{H}{H}.$$

Pelo segundo teorema do isomorfismo, temos que

$$\frac{G_{i+1}H}{H} \lhd \frac{G_i H}{H},$$

e

$$\frac{G_i H}{G_{i+1}H} = \frac{G_i(G_{i+1}H)}{G_{i+1}H} \simeq \frac{G_i}{G_i \cap G_{i+1}H}.$$

Pelo terceiro teorema do isomorfismo, temos

$$\frac{G_i}{G_i \cap G_{i+1}H} \simeq \frac{\frac{G_i}{G_{i+1}}}{\frac{G_i \cap G_{i+1}H}{G_{i+1}}},$$

e

$$\frac{G_i H}{G_{i+1}H} \simeq \frac{\frac{G_i H}{H}}{\frac{G_{i+1}H}{H}}$$

Daí, aplicando o primeiro e o segundo teorema do isomorfismo, segue que

$$\frac{\frac{G_i H}{H}}{\frac{G_{i+1}H}{H}} \simeq \frac{G_i H}{G_{i+1}H} \simeq \frac{G_i}{G_i \cap G_{i+1}H} \simeq \frac{\frac{G_i}{G_{i+1}}}{\frac{G_i \cap G_{i+1}H}{G_{i+1}}}.$$

Como esse último termo é abeliano, concluímos que, $\frac{G}{H}$ tem uma série subnormal abeliana e, portanto, $\frac{G}{H}$ é um grupo solúvel. ■

Teorema 1.15. *Se $H \lhd G$, tal que H e $\dfrac{G}{H}$ são solúvel, então G é solúvel.*

Demonstração. Como N é solúvel, existe uma série subnormal abeliana:

$$H = H_0 \geq H_1 \geq \cdots \geq H_k = 1_G,$$

onde $H_{i+1} \lhd H_i$ e $\dfrac{H_i}{H_{i+1}}$ é abeliano, para todo $0 \leq i \leq k-1$. Da mesma forma, como $\dfrac{G}{H}$ é solúvel, existe uma série subnormal abeliana:

$$\frac{G}{H} = \frac{G_0H}{H} \geq \frac{G_1H}{H} \geq \cdots \geq \frac{G_rH}{H} = \frac{H}{H},$$

onde $\dfrac{G_{i+1}H}{H} \lhd \dfrac{G_iH}{H}$ e $\dfrac{G_iH/H}{G_{i+1}H/H}$ é abeliano, para todo $0 \leq i \leq r-1$.

Facilmente podemos concluir que a seguinte série é subnormal abeliana:

$$G = G_0H \geq G_1H \geq \cdots \geq G_rH = H = H_0 \geq H_1 \geq \cdots \geq H_k = 1_G,$$

E portanto, G é um grupo solúvel. ■

Corolário 1.4. *Se H e K são grupos solúveis, então $H \times K$ é solúvel.*

Demonstração. Suponhamos, inicialmente, que $G = H \times K$ seja solúvel. Sendo assim, $H \simeq H \times 1_G$ e $K \simeq K \times 1_G$ são subgrupos normais de G. Logo, H e K são solúveis. Então, $H \lhd G$ e $\dfrac{G}{H} \simeq K$. Portanto, o resultado segue pelo teorema 1.15. ■

Dado um grupo G, se x e y são elementos de G, o **comutador** de x e y é o elemento $x^{-1}y^{-1}xy$, que denotamos por $[x, y]$. O significado de comutadores surge do fato que $[x, y] = 1$ se, e somente se, $xy = yx$, isto é, x e y comutam.

Definição 1.12. *Se $H, K \leq G$, então*

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

onde $[h, k]$ é o comutador $h^{-1}k^{-1}hk$.

Em particular, denominamos de *subgrupo derivado* ou *subgrupo comutador*, denotado por G', o subgrupo gerado por todos os comutadores, isto é:

$$G' = [G, G] = \langle [x, y] \mid x, y \in G \rangle.$$

Por outro lado, os subgrupos comutadores $G^{(i)}$, $i = 0, 1, 2, \ldots$, são definidos indutivamente por:

$$G^{(0)} = G$$

$$G^{(1)} = [G^{(0)}, G^{(0)}] = G'$$

$$G^{(i+1)} = [G^{(i)}, G^{(i)}]$$

Definição 1.13. *O subgrupo $G^{(i)}$, definido acima, chama-se* ***i-ésimo grupo derivado*** *de G e da sequência:*

$$G = G^{(0)} \supset G^{(1)} \supset \ldots \supset G^{(i)} \supset \ldots$$

que chamamos de ***sequência derivada*** *de G.*

A cadeia de subgrupo $G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \ldots$, formada tomando repetidamente subgrupos derivados, é uma sequência descendente chamada de *série derivada* de G. Note que, $G^{(i)} \lhd G$ e $\dfrac{G^{(i)}}{G^{(i+1)}}$ é um grupo abeliano. Por outro lado, se existir um menor número n, tal que $G^{(n)} = 1_G$, o chamaremos de *comprimento derivado* de G.

Veremos, a seguir, que o conhecimento de G' támbem permite saber quando um quociente é abeliano.

Lema 1.2. *Seja H um subgrupo normal de um grupo G. Então, o grupo quociente $\dfrac{G}{H}$ é abeliano se, e somente se, $G' \subset H$.*

Demonstração. Sejam $H \lhd G$ e $\dfrac{G}{H}$ um grupo abeliano. Então, para todo $x, y \in G$ temos que $(xH)(yH) = (yH)(xH)$, assim $x^{-1}y^{-1}xyH = H$, isto é, $[x, y] \in H$, mostrando que $G' \subset H$.

Reciprocamente, se $G' \subset H$, temos que:

$$(xH)(yH) = xyH = xy[y, x]H = yxH = (yH)(xH)$$

e, portanto $\dfrac{G}{H}$ é abeliano. ■

Lema 1.3. *Seja G um grupo. Se $K \trianglelefteq G$ e $K \leq H \leq G$, então $[G, H] \leq K$ se, e somente se, $\dfrac{H}{K} \leq Z\left(\dfrac{G}{K}\right)$.*

Demonstração. Suponha que, $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$. Seja $g \in G$ e $h \in H$, então $[g,h] = g^{-1}h^{-1}gh \in H$, pois, $K \trianglelefteq G$ e

$$(g^{-1}h^{-1}gh)K = (g^{-1}K)(h^{-1}K)(gK)(hK) = K,$$

já que,

$$hK, h^{-1}K \in \frac{H}{K} \leq Z\left(\frac{G}{K}\right).$$

Dessa forma, $[g,h] \in K$ e assim, $[G,H] \leq K$.

Agora, suponhamos que, $[G,H] \leq K$. Assim, $g^{-1}h^{-1}gh \in K$, para todo $g \in G$ e $h \in H$. Logo, $(g^{-1}h^{-1}gh)K = K$ e, daí $(gh)K = (hg)K$, ou seja, $(gK)(hK) = (hK)(gK)$, para todo $g \in G$ e $h \in H$. Portanto, $\frac{H}{K} \leq Z\left(\frac{G}{K}\right)$. ■

No próximo resultado, veremos como a série derivada é realmente uma ferramenta importante na caracterização dos grupos solúveis.

Teorema 1.16. *Seja $1_G = G_0 \rhd G_1 \rhd \ldots \rhd G_k = 1_G$ uma série com fatores abelianos em um grupo solúvel G. Então, $G^{(i)} \leq G_i$, para $0 \leq i \leq k$. Em particular, G é solúvel se, e somente se, existe um número $d \in \mathbb{N}$, tal que $G^{(d)} = 1_G$.*

Demonstração. A demonstração da primeira parte do lema será feita por indução sobre i. De fato, para $i = 0$, temos que $G = G^0 \leq G_0 = G$. Para o processo de indução, usaremos o fato de que se $\frac{G_i}{G_{i+1}}$ é um grupo abeliano, então $(G_i)' \leq G_{i+1}$. Suponha que, $G^{(i)} \leq G_i$ é verdadeiro, para algum i, mostraremos que $G^{(i+1)} \leq G_{i+1}$. Por hipótese, $\frac{G_i}{G_{i+1}}$ é abeliano, então $G^{(i+1)} = (G^{(i)})' \leq (G_i)' \leq G_{i+1}$, como queriamos mostrar. Consequentemente, se $i = k$, obtemos $G^{(k)} \leq G_k = 1_G$ e, portanto $G^{(k)} = 1_G$. Por outro lado, se $G^{(k)} = 1_G$ a série derivada é uma série subnormal abeliana de G, pois os fatores da série derivada são grupos abelianos. Logo, G possui uma série subnormal abeliana e, portanto G é solúvel. ■

A seguir, caracterizaremos os grupos solúveis em termos de seus fatores de composição.

Teorema 1.17. *Um grupo finito G é solúvel se, e somente se, todos os seus fatores de composição têm ordem prima. Em particular, um grupo simples é solúvel se, e somente se, tem ordem prima.*

Demonstração. Inicialmente, verificaremos o caso particular desse teorema. Sabemos que, $G' \lhd G$. Sendo assim, $G' = 1_G$ ou $G' = G$, pois G é simples. Como G é solúvel, segue que, $G' = 1_G$. Portanto, G é abeliano e simples, consequentemente, $|G| = p$, onde p é um número primo.

Agora, vejamos o caso geral:
($\Leftarrow$) Segue imediatamente pela definição.
($\Rightarrow$) Seja $\frac{G_i}{G_{i+1}}$ fator de composição. Assim, $\frac{G_i}{G_{i+1}}$ é solúvel e simples. Portanto, $\left|\frac{G_i}{G_{i+1}}\right| = p$, com p um número primo. ■

Os dois próximos resultados nos fornecem uma classe de grupos solúveis.

Teorema 1.18. *Todo p-grupo finito é solúvel.*

Demonstração. Seja G um contra exemplo minimal. A prova é feita, por indução, sobre $|G|$. Pelo Teorema 1.5, $Z(G) \neq \{1_G\}$. Portanto, $\frac{G}{Z(G)}$ é um p-grupo de ordem menor que $|G|$ e, assim é solúvel, por indução. Uma vez que, cada grupo abeliano é solúvel, $Z(G)$ é solúvel. Portanto, G é solúvel, pelo Teorema 1.15. ■

Teorema 1.19. *Se G é um grupo finito e $|G| = p^a q^b$, com p e q primos e $a, b \in N$, então G é solúvel.*

Demonstração. [3], p. 384-387 ■

Os teoremas de Sylow nos mostram que, a partir, do conhecimento de p-grupos obtemos informações sobre grupos finitos arbitrários. Além disso, a não simplicidade dos p-grupos sugere que a série normal pode ser uma ferramenta poderosa em seu estudo. Acontece que, os mesmos métodos que dão origem a teoremas relacionados a p-grupos também se aplicam a uma classe mais ampla, como os grupos nilpotentes, que podem ser considerados como p-grupos generalizados. No caso de serem finito, esses grupos têm muitas propriedades independentes de muita utilidade. Algumas dessas novas definições são "baseadas em série" que também proporcionam uma forma de "medida" à chamada "classe de nilpotência", que nos permite saber quão próximo um grupo nilpotente está de ser abeliano, e esta medida pode ser usada para estabelecer novos resultados. Um grupo abeliano G tem classe de nilpotência igual a 1, isto é:

$$[a,b] = a^{-1}b^{-1}ab = 1_G, \text{ para todo } a,b \in G.$$

Para grupos nilpotentes H de "classe n", temos que:

$$[...[a_0,a_1],a_2],...,a_n] = e, \text{ para todo } a_0,...,a_n \in H.$$

Iniciamente, definiremos uma classe de grupos que, de certa forma, está entre a classe dos grupos abelianos e a classe dos grupos solúveis e mostraremos alguns resultados fortes sobre a sua estrutura.

Definição 1.14. *Uma série normal de G:*

$$\langle 1_G \rangle = H_0 \lhd H_1 \lhd ... \lhd H_n = G,$$

é chamada uma série central de G, para cada i no intervalo de $0 \leq i \leq n-1$, se:

$$\frac{H_{i+1}}{H_i} \leq Z\left(\frac{G}{H_i}\right),$$

ou equivalentemente,

$$[H_{i+1}, G] \leq H_i.$$

Definição 1.15. *Dizemos que um grupo G é **nilpotente** se ele contém uma série de subgrupos $\{1_G\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$, tal que cada subgrupo G_{i-1} é normal em G e cada grupo quociente $\frac{G_i}{G_{i-1}}$ está contido no centro de $\frac{G}{G_{i-1}}$, $1 \leq i \leq n$. Neste caso, a série de subgrupos de G diz-se uma **série central** de G.*

Definição 1.16. *Seja $n \geq 0$. Um grupo G diz-se nilpotente de **classe de nilpotência** menor ou igual a n, denotado por $cl(G) \leq n$, se exitir em G uma série de subgrupos:*

$$\{1_G\} \subset G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

tal que cada subgrupo G_{i-1} é normal em G e cada quociente $\frac{G_i}{G_{i-1}}$ está contido no centro de $\frac{G}{G_{i-1}}$, onde $1 \leq i \leq n$.

Indicaremos por $\mathfrak{N}_c$ a *classe* dos grupos nilpotentes de classe menor ou igual a c.

Um grupo G é dito *nilpotente*, se ele é nilpotente com $cl(G) \leq n$ para algum n. Além disso, denotamos por:

$$\mathfrak{N} = \bigcup_{n=0}^{\infty} \mathfrak{N}_n$$

é a classe de todos os grupos nilpotentes. Nitidamente, tem-se $\mathfrak{N}_0 = \{\{1_G\}\}$ e $\mathfrak{N}_1$ é a classe dos grupos abelianos. Note que, a definição acima implica que G_1 está contido no centro de G. Se $G_1 = \{e\}$, então G_2 está contido no centro, e assim sucessivamente. Como a série central acaba, resulta imediatamente que todo grupo nilpotente tem centro não trivial.

Proposição 1.1. *Seja G um grupo nilpotente de classe c:*

i) *Se $H < G$, então H é nilpotente de $cl(G) \leq c$.*

ii) *Se $H \lhd G$, então $\dfrac{G}{H}$ é nilpotente de $cl(G) \leq c$.*

Demonstração. Seja

$$1_G = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_{c-1} \leq G_c = G$$

uma série central de G, com $G_i \lhd G$ e $\dfrac{G_i}{G_{i-1}} \leq Z\left(\dfrac{G}{G_{i-1}}\right)$, para todo $i = 1, 2, \ldots, n$.
i) Se $H \leq G$, então

$$1_G = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_{c-1} \leq H_c = H,$$

com $H_i = G_i \cap H$, é uma série de H, onde $H_i \lhd H$. E ainda,

$$\frac{H_i}{H_{i-1}} = \frac{H_i}{G_{i-1} \cap H_i} \simeq \frac{H_i G_{i-1}}{G_{i-1}} \leq \frac{G_i}{G_{i-1}}.$$

Logo, $\dfrac{H_i}{H_{i-1}} \leq Z\left(\dfrac{H}{H_{i-1}}\right)$.

ii) Se $H \lhd G$, então

$$\frac{H}{H} = \frac{G_0 H}{H} \leq \frac{G_1 H}{H} \leq \frac{G_2 H}{H} \leq \ldots \leq \frac{G_{c-1} H}{H} \leq \frac{G_c H}{H} = \frac{G}{H},$$

é uma série de $\dfrac{G}{H}$, com $\dfrac{G_i H}{H} \lhd \dfrac{G}{H}$.
E ainda,

$$\frac{\dfrac{G_i H}{H}}{\dfrac{G_{i-1} H}{H}} \simeq \frac{G_i H}{G_{i-1} H} = \frac{(G_{i-1} H) G_i}{G_{i-1} H} \simeq \frac{G_i}{G_i \cap G_{i-1} H}.$$

Como $G_{i-1} \leq G_{i-1} H \cap G_i$, vemos que $\dfrac{G_i}{G_i \cap G_{i-1} H} \simeq \dfrac{G_i}{G_{i-1}}$. Logo,

$$\frac{\frac{G_iH}{H}}{\frac{G_{i-1}H}{H}} \leq Z\left(\frac{\frac{G}{H}}{\frac{G_{i-1}H}{H}}\right)$$

Portanto, H e $\dfrac{G}{H}$ são nilpotentes de classes de nilpotência menor ou igual a c. ■

Daremos, agora, duas caracterizações de nilpotência, exploraremos as conexões entre a nilpotência e certos tipos de comutador.

Para isso, definimos o subgrupos característico $\gamma_i(G)$, indutivamente por:

$$\gamma_1(G) = G;\ \gamma_{i+1}(G) = [G, \gamma_i(G)],\ i = 1, 2, \ldots.$$

Claramente, $\gamma_{i+1}(G) \leq \gamma_i(G)$ e do lema 1.2, temos:

$$\frac{\gamma_{i+1}(G)}{\gamma_i(G)} \leq Z\left(\frac{G}{\gamma_i(G)}\right)$$

Precisaremos ainda de um outro subgrupo característico $\zeta_i(G)$, que definimos, se apoiando no conceito de *centro* de um grupo, indutivamente, da seguinte maneira, $\zeta_0(G) = 1_G$, $\zeta_1(G) = Z(G)$ e, em geral, $\zeta_{i+1}(G)$ é a pré-imagem em $Z\left(\dfrac{G}{\zeta_i(G)}\right)$, isto é, $\zeta_{i+1}(G)$ é o subgrupo de G, onde $\dfrac{\zeta_{i+1}(G)}{\zeta_i(G)} = Z\left(\dfrac{G}{\zeta_i(G)}\right)$.

Definição 1.17. *As sequências de subgrupos*

$$\{1_G\} = \zeta_0(G) \subset \zeta_1(G) \subset \cdots \subset \zeta_n(G) \subset \cdots$$

e

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \cdots \supset \gamma_n(G) \supset \cdots,$$

chamam-se ***série central superior*** *e* ***série central inferior*** *de G, respectivamente.*

No próximo resultado utilizamos a série central inferior e superior para caracterizar os grupos nilpotentes.

Teorema 1.20. *Seja G um grupo. São equivalentes:*

i) *G é nilpotente.*

ii) *Existe um inteiro positivo m, tal que $\zeta_m(G) = G$.*

iii) *Existe um inteiro positivo n, tal que $\gamma_n(G) = \{1_G\}$.*

Demonstração. [26], p. 221. ■

Claramente, vale que, se G é um grupo nilpotente, então as séries centrais superior e inferior de G têm o mesmo comprimento e como já definimos esse número é a **classe de nilpotência** de G.

O próximo resultado mostra a relação estreita entre a série central inferior e a superior.

Teorema 1.21. *Se $\zeta_s(G) = \zeta_s = G$, para alguns inteiros s, então $\gamma_{s+1} = \langle 1_G \rangle$ e*

$$\gamma_{r+1} \leq \zeta_{s-r}, \text{ para } r = 0, \cdots, s. \qquad (*)$$

Consequentemente, se o $\gamma_{s+1}(G) = \gamma_{s+1} = \langle 1_G \rangle$, para alguns inteiros s, então $\zeta_s = G$ e $(*)$ novamente se mantém.

Demonstração. Ver [26], Teorema 10.4, p.211. ■

A classe dos grupos nilpotentes contém a classe dos p-grupos finitos. Assim, vale a seguinte proporsição.

Proposição 1.2. *Todo p-grupo finito é nilpotente.*

Demonstração. Seja G um grupo, tal que $|G| = p^n$. Como $G > 1_G$, sabemos que, $Z(G) > 1_G$. Coloquemos $G_0 = 1_G$, $G_1 = Z(G)$. Se $G_k \trianglelefteq G$, define-se G_{k+1} por $\frac{G_{k+1}}{G_k} = Z\left(\frac{G}{G_k}\right)$. Como $\frac{G}{G_k}$ é um p-grupo finito, teremos que, se $\frac{G}{G_k} > 1_G$, então $\frac{G_{k+1}}{G_k} = Z\left(\frac{G}{G_k}\right) > 1_G$ e, daí $G_k < G_{k+1} \trianglelefteq G$. Depois de (no máximo) n passos temos $1 = G_0 \leq G_1 \leq \ldots \leq G_{n-1} \leq G_n = G$, com $G_k \trianglelefteq G$ e $\frac{G_{k+1}}{G_k} = Z\left(\frac{G}{G_k}\right)$ $k = 1, \ldots, n$. Portanto, G é nilpotente com $cl(G) \leq n$. ■

Proposição 1.3. *Se G e H são grupos nilpotentes, então $G \times H$ também é nilpotente.*

Demonstração. Considere que,

$$\gamma_i(G \times H) \leq \gamma_i(G) \times \gamma_i(H),$$

para todo i.

A prova será por indução sobre i. De fato, para $i = 1$, temos que:

$$\gamma_1(G \times H) = G \times H = \gamma_1(G) \times \gamma_1(H).$$

Agora, suponhanos que $\gamma_i(G \times H) \leq \gamma_i(G) \times \gamma_i(H)$ vale para um i qualquer, mostraremos que $\gamma_{i+1}(G \times H) \leq \gamma_{i+1}(G) \times \gamma_{i+1}(H)$. Vejamos:

$$\gamma_{i+1}(G \times H) = [\gamma_i(G \times H), G \times H] \leq [\gamma_i(G) \times \gamma_i(H), G \times H] \leq [\gamma_i(G), G] \times [\gamma_i(H), H,$$

isto é,

$$\gamma_{i+1}(G \times H) \leq \gamma_{i+1}(G) \times \gamma_{i+1}(H).$$

Logo, pelo Teorema 1.20, existe um inteiro positivo n, tal que

$$\gamma_n(G \times H) = \gamma_n(G) \times \gamma_n(H) = \{1_G\} \times \{1_H\}.$$ ■

Agora, estamos em condições de mostrar que o centro de um grupo nilpotente é razoavelmente grande, e intercepta todos os subgrupo normais do grupo.

Proposição 1.4. *Seja H um subgrupo normal não trivial de um grupo nilpotente G. Então, $H \cap Z(G) \neq \{1_G\}$. Consequentemente, um subgrupo normal minimal de um grupo nilpotente está contido no seu centro.*

Demonstração. Pelo Teorema 1.20, existe $n \in \mathbb{N}$, tal que $G = \zeta_n(G)$, daí existe $i \in \mathbb{N}$, tal que $H \cap \zeta_i(G) \neq \{1_G\}$ e $H \cap \zeta_{i-1}(G) = \{1_G\}$. Então, $[H \cap \zeta_i(G), G] \subset H \cap \zeta_{i-1}(G) = \{1_G\}$ e, portanto $H \cap \zeta_i(G) \subset H \cap Z(G)$. Consequentimente, temos que $H \cap Z(G) \neq \{1_G\}$. Além disso, $H \cap Z(G) \lhd G$ e H é minimal. Logo, $H \cap Z(G) = H$ e, portanto $H \subset Z(G)$. ■

A seguir, demonstraremos uma propriedade importante dos grupos nilpotentes, que será útil para descrever sua estrutura.

Proposição 1.5. *Seja H um subgrupo próprio de um grupo nilpotente. Então, $H \subsetneq N_G(H)$*

Demonstração. Seja $n \in \mathbb{N}$ o maior inteiro positivo, tal que $\zeta_n \leq H$. Escolha $a \in \zeta_{n+1}(G)$, com $a \notin H$. Como

$$\frac{\zeta_{n+1}(G)}{\zeta_n(G)} = Z\left(\frac{G}{\zeta_n(G)}\right),$$

segue que,

$$\zeta n(G)ah = (\zeta_n(G)a)(\zeta_n(G)h) = (\zeta_n(G)h)(\zeta_n(G)a) = \zeta_n(G)ha,$$

para todo $h \in H$. Logo, $xah = xha$, onde $x \in \zeta_n(G) \lneq H$ e, então

$$ah = ha \Longrightarrow aha^{-1} = h \in H.$$

Portanto, $a \in N_{G(H)}$. ■

Definição 1.18. *Diz-se que um grupo G tem a* ***propriedade do normalizador*** *se todo subgrupo próprio de G está estritamente contido no seu normalizador.*

Assim, acabamos de verificar que todo grupo nilpotente tem a propriedade do normalizador. Como consequência, tem-se o seguinte:

Corolário 1.5. *Todo subgrupo maximal de um grupo nilpotente é normal.*

Agora, nossa intenção é mostra que vale, para os grupos nilpotentes finitos, uma caracterização semelhante a que vale para grupos abelianos finitos.

Lembre-se que um subgrupo H de um grupo G diz-se *subnormal* se existe uma cadeia de subgrupos:

$$H = H_0 \subset H_1 \subset \cdots \subset H_n = G,$$

tal que $H_{i-1} \lhd H_i, onde 1 \leq i \leq n$.

Como consequência da proposição acima temos a seguinte afirmação:

Corolário 1.6. *Seja G um grupo nilpotente finito. Então, todo subgrupo de G é subnormal em G.*

Demonstração. Seja H um subgrupo de G. Definindo $H_0 = H$ e, indutivamente, $H_i = N_G(H_{i-1})$, para todo $i \geq 1$. Pela Proposição 1.6, segue que, se $H_{i-1} \neq G$, então $|H_{i-1}| \leq |H_i|$. Como G é nilpotente finito, deve existir um índice n tal que $H_n = G$. ■

Agora, estamos com condições de estabelecer um resultado de caracterização de grupos nilpotentes finitos.

Teorema 1.22. *Seja G um grupo finito. Então, as seguintes condições são equivalentes.*

i) *G é nilpotente.*

ii) *G tem a propriedade do normalizador.*

iii) *Todo subgrupo de Sylow de G é normal em G.*

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

v) *Todo subgrupo de G é subnormal.*

vi) *Todo subgrupo maximal de G é normal.*

Demonstração. Vamos provar inicialmente que i) $\Rightarrow$ ii) $\Rightarrow$ iii) $\Rightarrow$ iv) $\Rightarrow$ i).
i) $\Rightarrow$ ii). Provamos na Proposição 1.6.
ii) $\Rightarrow$ iii). Sejam P um Sylow p-subgrupo de G e $H = N_G(P)$. Se $H \neq G$, então por ii), temos que $H \subsetneq N_G(H)$. Por outro lado, se $x \in N_G(H)$, onde $P \subset H \lhd N_G(H)$, temos que $P^x \subset H$. Logo, P^x e P são Sylow p-subgrupo de H. Assim, existe um elemento $h \in H$ tal que $P^h = P^x$, donde $h^{-1}x \in N_G(P) = H$. Segue que $x \in H$ e, portanto $N_G(H) = H$, absurdo. Logo, $H = G$ implicando que $P \lhd G$.
iii) $\Rightarrow$ iv). Suponhamos que, $|G| = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$, onde p_i são primos distintos e $n_i > 0$, para todo i. Por iii) $P_1, P_2, \ldots, P_k$ são os Sylow p_i-subgrupos normais de G. Como $|P_i| = p_i^{n_i}$, temos que $P_i \cap P_j = \{1_G\}$, para $i \neq j$, logo $xy = yx$ para $x \in P_i$ e $y \in P_j$. E ainda, considere $P^* = P_1 \ldots P_{i-1}P_{i+1} \ldots P_k < G$ e que a ordem de todo elemento de P^* divide $p_1 \ldots p_{i-1}p_{i+1} \ldots p_k$. Consequentemente,

$$P_i \cap P^* = \{1_G\} \text{ e } P_1 \ldots P_{i-1}P_iP_{i+1} \ldots P_k = P_1 \times \ldots \times P_{i-1} \times P_i \times P_{i+1} \times \ldots \times P_k.$$

Portanto, $G = p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k} = |P_1 \ldots P_{i-1}P_iP_{i+1} \ldots P_k| = |P_1 \times \ldots \times P_{i-1} \times P_i \times P_{i+1} \times \ldots \times P_k|$
iv) $\Rightarrow$ i). Segue imediatamente pelas Proposições 1.2 e 1.3.
Agora, para terminar a demonstração vamos mostrar que i) $\Rightarrow$ v) $\Rightarrow$ vi) $\Rightarrow$ i).
i) $\Rightarrow$ v). Provamos no corolário 1.6.
v) $\Rightarrow$ vi). Seja H um subgrupo maximal de G. Como H é subnormal, temos que:

$$H = H_0 \leq H_1 \leq \ldots \leq H_n, \text{ onde } H_i \lhd H_{i+1}.$$

Como H é maximal, $H \lhd H_i$, daí, segue imediatamente que H é normal.
vi) $\Rightarrow$ i). Finalmente, mostraremos que, se vale vi), então todo Sylow p-subgrupo de G é normal o que, como vimos acima, implica na nilpotência de G. De fato, seja P um Sylow p-subgrupo de G. Se $N_G(P)$ é um subgrupo próprio de G, então deve estar contido em algum subgrupo maximal H de G que, por hipótese de vi), é normal. Isto significa que,

$N_G(H) = G$, o que é uma contradição, pois dado P um Sylow p-subgrupo de G e H um outro subgrupo. Se $N_G(P) \subset H$, então $H = N_G(H)$. De fato, seja $x \in N_G(H)$. Como $P \subset H \lhd N_G(H)$, temos que $P^x \subset H$. Como, P^x e P são Sylow p-subgrupo de H, existe um elemento $h \in H$ tal que $P^h = P^x$, donde $h^{-1}x \in N_G(P) = H$. Segue que, $x \in H$ e, assim, $N_G(H) = H$. Portanto, $P \lhd G$. ■

Nossa próxima condição relacionada a nilpotência diz respeito a comutar elementos cuja ordem não têm fatores comuns.

Teorema 1.23. *Um grupo finito G é nilpotente se, e somente se, sempre que $a, b \in G$ e $mdc(|a|, |b|) = 1$, então a e b comutam.*

Demonstração. Não há nada a provar, se G é um p-grupo. Por isso, suponhamos que, os números primos que dividem $|G|$ são $p_1, p_2, \ldots, p_s$, onde $s > 1$. Se G é nilpotente, então pelo Teorema 1.23, é um produto direto dos seus Sylow p_i-subgrupos, onde $1 \leq i \leq s$. Reordenando esses fatores, se necessário, vamos considerar que os fatores primos de $|a|$ são $p_1, \ldots, p_t$, e assim, por hipótese, os fatores primos de $|b|$ são $p_{t+1}, \ldots, p_s$. Agora, se $R_1 = P_1 \times \cdots \times P_t$ e $R_2 = P_{t+1} \times \cdots \times P_s$, temos que $G = R_1 \times R_2$, $a \in R_1$ e $b \in R_2$, e assim a e b comutam. Por outro lado, se para todos $a \in R_1$ e $b \in R_2$, a e b comutam, então R_1 e R_2 são subgrupos normais de G, onde $R_1 \cap R_2 = \{1_G\}$ e $R_1R_2 = G$. Logo, podemos concluir que $G \simeq R_1 \times R_2$, daí segue o teorema. ■

Trataremos, neste momento, do subgrupo de Fitting, com menos propriedades elementares, mas, as generalizações provaram ser úteis em trabalhos recentes sobre a classificação dos grupos simples finitos. O resultado abaixo foi provado por H. Fitting (1906-1938), em 1938.

Teorema 1.24 (Teorema de Fitting)**.** *Se J e K são subgrupos normais nilpotentes de um grupo G, com classes $cl(J) = r$ e $cl(K) = s$, respectivamente, então JK também é um subgrupo normal nilpotente de G com classe, no máximo, $cl(G) \leq r + s$.*

Demonstração. Seja G um grupo e $J \trianglelefteq G$, $H \trianglelefteq G$, tem-se $\gamma_{r+1}(J) = 1_G$ e $\gamma_{s+1}(K) = 1_G$. Então

$$\gamma_n(JK) = \underbrace{[JK, \ldots, JK]}_{n} = \prod [A_1, \ldots, A_n]$$

onde $(A_1, \ldots, A_n)$ percorre sobre todas as sequências de n $J's$ e $K's$. Desde que $\gamma_i(J)$ é característico em J, tem-se que $\gamma_i(J) \trianglelefteq G$, daí

$$[K, \gamma_i(J)] \leq \gamma_i(J), \text{ para todo } i$$

Assim, se i das entradas $A_1, \ldots, A_n$ são $J's$, e o restante $n - i$ são $K's$, tem-se

$$[A_1, \ldots, A_n] \leq \gamma_i(J) \bigcap \gamma_{n-i}(K).$$

Se tomarmos $n = r + s + 1$, então $i \geq r + 1$ ou $n - i \geq s + 1$. Portanto, $\gamma_n(JK) = 1_G$. ■

Consequentemente, obtem-se a seguinte definição.

Definição 1.19. *Para um grupo finito G, o produto de todos os subgrupos normais nilpotentes de G, isto é,*

$$\prod_{\substack{N \trianglelefteq G \\ N \in \mathfrak{N}}} N = \langle N \mid N \trianglelefteq G, N \in \mathfrak{N} \rangle$$

é chamado o ***subgrupo Fitting*** *de G, e denotamos por $F(G)$.*

Proposição 1.6. *Seja G um grupo e $x \in G$. Então $x \in F(G)$ se, e somente se, $\langle x^G \rangle$ é nilpotente*

Demonstração. ($\Leftarrow$) Seja $\langle x^G \rangle \in \mathfrak{N}$. Por definição, concluimos que $x \in \langle x^G \rangle \leq F(G)$.
($\Rightarrow$) Suponha que, $x \in F(G)$, assim, existem $N_1, N_2, \ldots, N_r \leq G$, com $N_i \in \mathfrak{N}$ e $x_i \in N_i$, $i = 1, 2, \ldots, r$, tais que $x = x_1 x_2 \ldots x_r \in N_1 N_2 \ldots N_r$, desde que $N_1 N_2 \ldots N_r \in \mathfrak{N}$. Daí, segue que, $\langle x^G \rangle \leq N_1 N_2 \ldots N_r$, e assim, $\langle x^G \rangle \in \mathfrak{N}$ ■

Além disso, o teorema de Fitting nos permite caracterizar $F(G)$ da seguinte maneira:

Proposição 1.7. *Para todo grupo G, vale que:*

$$F(G) = \{x \in G \mid \langle x^G \rangle \in \mathfrak{N}G\}$$

isto é, $F(G)$ é o conjunto dos elementos de G que geram um subgrupo normal nilpotente de G.

Demonstração. Basta usar a Proposição 1.7. ■

Definição 1.20. *Um grupo G é denominado um* ***grupo de Fitting****, se $F(G) = G$.*

Suponha que G é um grupo finito, p é primo e $P_1, \cdots, P_k$ é uma lista de seus Sylow p-subgrupos. Então, definimos:

$$O_p(G) = \bigcap_{i=1}^{k} P_i.$$

O subgrupo normal $O_p(G)$ é chamado o ***p-radical*** de G. Se G tem apenas um Sylow p-subgrupo P_1, então pelo Teorema 1.10 (Sylow III), temos que, $O_p(G) = P_1 \lhd G$. Mesmo, se G tem vários p-subgrupos de Sylow, ainda, temos $O_p(G) \lhd G$.

Teorema 1.25. *Se $p_1, \cdots, p_r$ são os números primos (distintos) que dividem $|G|$, então*

$$F(G) = O_{p_1}(G) \cdots O_{p_r}(G).$$

Demonstração. Para cada p_i os Sylow p_i-subgrupos de G são conjugados em G e, por isso, $O_{p_i}(G)$ é o núcleo de cada membro desta classe e, portanto, é normal em G. Como p-grupos são nilpotentes, tem-se $O_{p_i}(G) \leq F(G)$ para cada p_i divisor $|G|$. Agora, pelo Teorema de Fitting, mostra-se que:

$$\prod_{i=1}^{r} O_{p_i}(G) \subseteq F(G).$$

Por outro lado, se Q é um Sylow p_i-subgrupo de $F(G)$, então Q está contido em alguns Sylow p_i-subgrupo P de G (Teorema 6.9). Pelo argumento de Frattini, conclui-se que $Q \lhd G$, daí $Q \subseteq O_{p_i}(G)$, e assim, por $F(G) \subseteq \prod_{i=1}^{r} O_{p_i}(G)$. Daí, segue o resultado. ■

Pelo Teorema 1.25, $F(G)$ é o maior subgrupo normal nilpotente de G.

A seguir, caracterizaremos o radical solúvel de um grupo fornecendo alguns resultados valiosos para demostrar os resultados do capítulo 2.

Definição 1.21. *Para um grupo G, chamamos de* ***radical solúvel*** *o subgrupo gerado por todos os subgrupos normais solúveis de G, e denotamos por $R(G)$.*

Vale ressaltar, que para todo grupo G tem-se:

$$R(G) = \{x \in G \mid \langle x^G \rangle \text{ é solúvel}\},$$

isto é, $R(G)$ é o conjunto dos elementos em G que geram um subgrupo normal solúvel de G.

Definição 1.22. *Seja G um grupo. Dizemos que $y \in G$ é um elemento radical se para qualquer $x \in G$ o subgrupo gerado por x e y é solúvel. Denota-se por $S(G)$ o conjunto dos elementos radicais de G. Ou seja,*

$$S(G) = \{y \in G \mid \langle y, x\rangle \text{ é solúvel, para todo } x \in G\}.$$

Note que, qualquer que seja o grupo G, tem-se que $R(G) \subseteq S(G)$. De fato, se $y \in R(G)$, então para qualquer $x \in G$ o subgrupo gerado por x e y contém um subgrupo normal solúvel com quociente cíclico e, portanto é solúvel.

Teorema 1.26. *Seja G um grupo finito e $R(G)$ o radical solúvel de G. Então, $R(G)$ coincide com o conjunto de todos os $y \in G$ com a seguinte propriedade: para qualquer $x \in G$ o subgrupo gerado por x e y é solúvel.*

Demonstração. Ver [18]. ■

Esse importante resultado apresentado por Robert Guralnick, Boris Kunyavskiĭ, Eugene Plotkin e Aner Shalev, que surgiu, a partir de um famoso teorema de J. Thompson, demonstra que se G é finito, então $R(G) = S(G)$.

1.4 π-Número

Seja $\mathbb{P}$ o conjunto de todos os números primos e $\pi \subseteq \mathbb{P}$. Um número natural n é um π-número, se todo divisor primo p de n pertence a π. Observamos que 1 é um π-número para qualquer π. Divisores e produtos de π-números são π-números. Um elemento g de ordem finita de um grupo G é denominado um elemento periódico ou de torção. Um grupo G é periódico se todos elementos de G forem periódicos.

Definição 1.23. *Seja $\pi \subseteq \mathbb{P}$.*

(a) *Um elemento periódico g de um grupo G é dito um π-elemento se a ordem dele fôr um π-número.*

(b) *Um grupo G é um π-grupo se todo elemento de G fôr π-elemento.*

(c) *Um subgrupo S de um grupo G é um π- subgrupo de G se S fôr um π-grupo.*

Indicamos a classe dos π-grupos por $\mathfrak{B}_\pi$.

Para todo G e todo $\pi \subseteq \mathbb{P}$, indicamos por $\pi G = \mathfrak{B}_\pi G$ o conjunto dos π-subgrupos de G. Já, $m\pi G$ será o conjunto dos π-subgrupos maximais de G.

Observe que, $\{1_G\} \in \pi G$, para qualquer grupo G e qualquer $\pi \subseteq \mathbb{P}$. Se $\pi = \{p\}$ escrevemos pG e mpG, ao invés, de $\{p\}G$ e $m\{p\}G$.

Observação 1.2. *Seja G um grupo finito e $\pi \subseteq \mathbb{P}$. Então, G é um π-grupo se, e somente se, $|G|$ é um π- número.*

Demonstração.

($\Rightarrow$) Aplicando o Teorema de Sylow.

($\Leftarrow$) Aplicando o Teorema de Lagrange. ■

Observe também que, se o grupo G fôr finito, o conjunto mpG coincide com o conjunto Syl_pG dos Sylow p-subgrupos de G.

Observação 1.3. *As classes $\mathfrak{B}_\pi$ são fechadas a subgrupos, quocientes e quaisquer extensões. Com isto, queremos dizer que, para qualquer grupo G e $N \trianglelefteq G$, tem-se:*

i) *Se $G \in \mathfrak{B}_\pi$ e $N \leq G$, então $N \in \mathfrak{B}_\pi$ e $\dfrac{G}{N} \in \mathfrak{B}_\pi$.*

ii) *Se $N \in \mathfrak{B}_\pi$ e $\dfrac{G}{N} \in \mathfrak{B}_\pi$, então $G \in \mathfrak{B}_\pi$.*

Demonstração.

i) A primeira parte, ligado ao subgrupo, decorre da definição. Para a segunda parte, suponha $g \in G$ e a ordem de g um π-número, digamos r, então, pelas classes laterais, $N = 1_GN = g^rN = (gN)^r$. Daí a ordem de gN é um π-número e, portanto a ordem de cada elemento de $\dfrac{G}{N}$ é um π-número.

ii) Suponhamos que, G é um grupo qualquer e $N \trianglelefteq G$ com N, $\dfrac{G}{N} \in \mathfrak{B}_\pi$ e, seja $g \in G$, existe um π-número n com $(gN)^n = N$, isto é, $g^n \in N$. Agora, existe um π-número l com $(g^n)^l = 1_G$. Assim, $g^{nl} = 1_G$ com nl um π-número. Logo, $G \in \mathfrak{B}_\pi$ ■

Observação 1.4. *Seja $G \in \mathfrak{B}_\pi$ e $H \leq G$*

i) *Se $H < \infty$, então $|H|$ é um π-número*;

ii) *Se $|G : H| < \infty$, então $|G : H|$ é um π-número.*

Demonstração.

i) É claro pela Observação 1.2.

ii) Considerando:

$$R = \bigcap_{g \in G} H^g,$$

sabemos também que $\left|\frac{G}{R}\right| < \infty$. Como $\left|\frac{G}{R}\right|$ é π-grupo, veremos que:

$$|G : H| = \left|\frac{G}{R} : \frac{H}{R}\right|$$

é um π-número. ■

Capítulo 2

Sobre Elementos Cujos Índices dos seus Centralizadores são Potências de Primo

Neste capítulo vamos apresentar uma série de resultados para que um elemento x de um grupo tenha índice potência de primo em G. Para isto, considerando um elemento x de um grupo finito G denotaremos por $Ind_G(x)$ o índice do $C_G(x)$ em G, ou apenas, índice de x em G. O objetivo deste trabalho é mostrar dois teoremas apresentados por Alan R. Camina, Pavel Shumyatsky e Carmela Sica [4], em especial, o seguinte teorema, se $Ind_{\langle a,b,x\rangle}(x)$ é uma potência de primo para qualquer $a, b \in G$, segue que, $Ind_G(x)$ é uma potência de primo.

2.1 Sobre Elementos com Índices Potências de Primo

A influência do tamanho das classes de conjugação na estrutura de um grupo finito já foi considerado por muitos autores. Um desses autores foi Reinhold Baer, que apresentou a seguinte definição.

Definição 2.1. *Sejam G um grupo finito e $x \in G$. O índice de x em G é dado por $[G : C_G(x)]$ e denotamos por $Ind_G(x)$.*

Note que, pelo teorema da órbita-estabilizador o $Ind_G(x)$ é o tamanho da classe de conjugação que contém x e, portanto, indicada por $|x^G|$.

Talvez Ludvig Sylow tenha contribuído com os primeiros resultados, afirmando que, um grupo G cujo índices de x em G são potência de um primo dado, tem centro não-

trivial. Já William Burnside declara que se o índice de x em G é potência de primo, então o grupo é não-simples. Estes são dois resultados clássicos que dão informações sobre o grupo e algumas propriedades aritméticas do conjunto de índices.

Em 1990, Kazarin, provou a seguinte extensão para o resultado de Burnside:

Teorema 2.1. *Seja G um grupo finito e x um elemento de G, de tal forma que, $Ind_G(x) = p^b$, para algum p primo e b inteiro. Então, $\langle x^G \rangle$ é um subgrupo solúvel de G.*

Demonstração. Ver [22]. ■

Os lemas a seguir tratam de algumas propriedades sobre índices de subgrupos. Essas propriedades serão fundamentais para o entendimento de alguns resultados que apresentaremos neste capítulo.

Lema 2.1. *Seja S um subgrupo de G, e N um subgrupo normal de G, então $[N : N \cap S]$ é um divisor de $[G : S]$.*

Demonstração. Pelo Segundo Teorema do Isomorfismo, tem-se:

$$\frac{NS}{N} \simeq \frac{S}{N \cap S}.$$

Consequentemente,

$$\begin{aligned}[G : 1_G] &= [G : NS][NS : N][N : N \cap S][N \cap S : 1_G] = \\ &= [G : NS][S : N \cap S][N : N \cap S][N \cap S : 1_G] = \\ &= [G : NS][N : N \cap S][S : 1_G],\end{aligned}$$

isto implica que,

$$[G : S] = [G : NS][N : N \cap S],$$

como queriamos demostrar. ■

Lema 2.2. *Seja N um subgrupo normal de G. Então:*

i) *Se $x \in N$, então $Ind_N(x)$ divide $Ind_G(x)$;*

ii) *Se $x \in G$, então $Ind_{G/N}(x)$ divide $Ind_G(x)$.*

Demonstração.

i) Basta considerar que $C_N(x) = N \cap C_G(x)$ e usar o Lema 2.1.

ii) É claro que:

$$\frac{NC_G(x)}{N} \leq C_{\frac{G}{N}}(Nx).$$

Consequentemente, podemos deduzir, a partir, do Primeiro Teorema do isomorfismo que:

$$[G : NC_G(x)] = \left[\frac{G}{N} : \frac{NC_G(x)}{N}\right] = \left[\frac{G}{N} : C_{\frac{G}{N}}(Nx)\right]\left[C_{\frac{G}{N}}(Nx) : \frac{NC_G(x)}{N}\right].$$

Daí, $\left[\frac{G}{N} : Nx\right]$ é divisor de $[G : NC_G(x)]$ e este índice é divisor de $Ind_G(x) = [G : C_G(x)]$, desde que:

$$[G : C_G] = [G : NC_G(x)][NC_G(x) : C_G(x)].$$

Isso prova nossa afirmação. ■

Agora, vamos considerar a estrutura de um grupo que tem um elemento de índice potência de primo.

Lema 2.3. *Se a ordem do subgrupo normal N de G é divisível pelo número primo p, então N contém um elemento de ordem p cujo índice é primo com p.*

Demonstração. Decorre da nossa hipótese e do Teorema de Sylow que os Sylow p-subgrupos de N são diferentes de 1_G. Se S é um Sylow p-subgrupo de N, então S está contido em alguns Sylow p-subgrupo P de G. De $S = P \cap N$, deduz-se que S é um subgrupo normal de P. Cada subgrupo normal, diferente de 1_G, de um p-grupo contém um elemento central de ordem p. Consequentemente, existe um elemento t de ordem p em S e t pertence ao centro de P. Claramente, $C_G(t)$ contém P, isso implica que $[G : C_G(t)] = Ind_G(t)$ é primo com p. ■

Os próximos dois lemas e suas provas são atribuídos a H. Wielandt.

Lema 2.4 (Wielandt)**.** *Seja p um primo e $x \in G$. Se tanto a ordem de x como a ordem da classe de x são potências de p, então $x \in O_p(G)$.*

Demonstração. Seja x um elemento de G cuja ordem e índice são potências de p. Considere $P \in Syl_p(G)$. Claramente, podemos supor que $x \in P$. Além disso, $G = C_G(x)P$. Daí,

$$\langle x^G \rangle = \langle x^{C_G(x)P} \rangle = \langle x^P \rangle \leq P,$$

assim,

$$\langle x^G \rangle \trianglelefteq G, \langle x^G \rangle \leq O_p(G).$$

Então,

$$x \in \langle x^G \rangle \leq O_p(G).$$

■

Lema 2.5. *Seja G um grupo finito e x um elemento de índice potência de primo. Então x centraliza cada fator principal não abeliano de G.*

Demonstração. O principal teorema em Kazarin [5] diz que $\langle x^G \rangle$ é um subgrupo solúvel de G. Daí, segue o lema. ■

A seguir, apresentaremos a proposição que generaliza o resultado de Wielandt mencionado no Lema 2.4.

Proposição 2.1. *Seja G um grupo finito e x um elemento de G cujo índice é p^n, onde p é um primo e n é um número natural. Então*

$$[x^G, x^G] \subseteq O_p(G).$$

Demonstração. Seja G um contra-exemplo mínimo para a proposição. Uma vez que a condição da proposição são herdadas por grupos quocientes (Lema 2.1), podemos supor que $O_p(G) = 1_G$. Por isso, precisamos mostrar que $[x^G, x^G] = 1_G$. Primeiramente, suponhamos que $\langle x \rangle$ é subnormal em G, em seguida, $\langle x \rangle$ está contido no subgrupo de Fitting $F(G)$ de G, mas, uma vez que $F(G)$ é um p'-grupo, segue-se que x é central em $F(G)$. Como $\langle x^G \rangle$ está em $F(G)$, segue o resultado. Por outro lado, vamos assumir que $\langle x \rangle$ não é subnormal em G. Seja $N = \langle x^G \rangle$ e suponhamos que N é subgrupo próprio de G. Pela minimalidade de G, uma vez que $O_p(N) = 1_G$, temos que $[x^N, x^N] = 1_G$ e, portanto, x é central no seu fecho normal em N. No entanto, isso implica que $\langle x \rangle$ é subnormal em G, o que é uma contradição. Assim, podemos assumir que $N = G = \langle x^G \rangle$. Seja K um subgrupo normal

mínimo de G. Se considerarmos $\frac{G}{K}$, vemos que $\frac{G'}{K} = \frac{[x^G, x^G]K}{K} \subseteq O_p\left(\frac{G}{K}\right)$, por indução. Assumindo que K é central em G, temos $O_p(\frac{G}{K}) = \frac{O_p(G)K}{K}$ e, nesse caso, $O_p\left(\frac{G}{K}\right) = 1_G$. Assim, $G' < Z(G)$ e, portanto, G é nilpotente e o resultado é verdadeiro. Além disso, se K não é central em G e, portanto, não é centralizado por x, temos que K tem ordem divisível por p. Assim, K é um fator principal não-abeliano de G já que $O_p(G) = 1_G$. Mas isso é um absurdo pelo Lema 2.5. ■

Para um grupo G, os subgrupos característicos $F_k(G)$, $k \geq 0$ são definidos por $F_0(G) = 1_G$ e $F_{k+1}(G)$, e indutivamente por $\frac{F_{k+1}(G)}{F_k(G)} = F\left(\frac{G}{F_k(G)}\right)$.

Daí, podemos provar o seguinte teorema.

Teorema 2.2. *Seja G um grupo finito. Então, todos os elementos de índice potência de primo estão no $F_2(G)$.*

Demonstração. Seja $x \in G$, tal que $Ind_G(x) = p^a$ para algum primo p e a um número natural. Então, $[x^G, x^G] \subseteq O_p(G) \subseteq F(G)$. Daí, $\frac{F(G)\langle x\rangle}{F(G)}$ é um subgrupo nilpotente subnormal de $\frac{G}{F(G)}$. Assim, segue o teorema. ■

Se G é solúvel, o comprimento de Fitting de G é o menor inteiro k, tal que $G = F_k(G)$. Para qualquer k notamos que $F_k(G)$ tem comprimento de Fitting no máximo k e contém cada subgrupo normal de G com esta propriedade. Defini-se:

$$\mathcal{F}_k(G) = \{x \in G / x \in F_k(\langle x, g\rangle), \text{ para todo } g \in G\}.$$

Trivialmente, tem-se $F_k(G) \subseteq \mathcal{F}_k(G)$.

Teorema 2.3. *Seja G um grupo solúvel. Então, $\mathcal{F}_k(G) = F_k(G)$, para todos os $k \geq 0$.*

Demonstração. Ver [7]. ■

A partir do estudo de elementos de índice potência de primo, Alan R. Camina, Pavel Shumyatsky e Carmela Sica, levantaram a seguinte questão.

Conjectura 2.1. *Seja $x \in G$. Suponhamos que $Ind_{\langle a,x\rangle}(x)$ é uma potência de primo, para qualquer $a \in G$. Então, $Ind_G(x)$ é uma potência de primo.*

No entanto, verificou-se que a conjectura não vale. De fato, considerando um grupo abeliano V agindo sobre $A = \mathbb{S}_3$, o grupo simétrico de grau 3 e, assumindo que $G = VA$ e $x \in V$ é um elemento, tal que $C_A(x) = 1_G$. Temos que, $Ind_{\langle a,x\rangle}(x) = |a|$ é um primo, para cada $a \in A$, porém, $Ind_G(x) = 6$.

Deste modo, modificou-se a conjectura da seguinte maneira.

Conjectura 2.2. *Seja p um primo e $x \in G$. Suponha que $Ind_{\langle a,x\rangle}(x)$ é uma p-potência para qualquer $a \in G$. Então, $Ind_G(x)$ é um p-potência.*

Esse resultado, além de ser vedadeiro, deu origem a um teorema mais geral, que enunciaremos e demonstraremos. Mas, antes, é imprescindível admitir o seguinte lema.

Lema 2.6. *Sejam π um conjunto de números primos e x um elemento de G. Suponha que $Ind_{\langle a,x\rangle}(x)$ é um π-número para qualquer $a \in G$. Se Q é um π'-subgrupo de G, tal que $x \in N_G(Q)$, então $x \in C_G(Q)$.*

Demonstração. Seja $a \in Q$. Por hipótese, $Ind_{\langle a,x\rangle}(x) = [\langle a, x\rangle : C_{\langle a,x\rangle}(x)]$ é π-número. Por outro lado, é claro que $Ind_{\langle a,x\rangle}(x)$ é um π'-número, pois adimitindo que $x \in N_G(Q)$, tem-se $\langle a, x\rangle \leq Q$ e $C_{\langle a,x\rangle}(x) \leq Q$. Daí, pelo teorema de Lagrange:

$$|\langle a, x\rangle| = |C_{\langle a,x\rangle}(x)|[\langle a, x\rangle : C_{\langle a,x\rangle}(x)],$$

isto é, $\langle a, x\rangle$ é π'-subgrupo. Logo,$|\langle a, x\rangle : C_{\langle a,x\rangle}(x)| = 1$, ou seja, $\langle a, x\rangle = C_{\langle a,x\rangle}(x)$, para todo $a \in Q$. Portanto, $x \in C_G(Q)$. ■

É interessante notar que, se $Ind_G(x)$ é um π-número $Ind_H(x)$ não é necessariamente um π-número para cada subgrupo H. Seja M o grupo elementar de ordem 8 e A o grupo não-abeliano de ordem 21. Seja A agindo em M, de tal forma que o subgrupo de ordem 7 permuta as involuções em M transitivamente. Seja G a extensão de M por A. Escolhendo x para ser uma involução em M. Então, $Ind_G(x) = 7$, mas, existe um subgrupo não abeliano H de ordem de 24, de tal modo que $Ind_H(x) = 3$.

Durante a demostração do lema anterior, observamos que se fossemos capazes de mostrar que $\langle x\rangle \trianglelefteq G$ provariamos o lema usando o seguinte resultado.

Corolário 2.1. *Sejam M, N subgrupos normais de G e $M \cap N = 1_G$. Então, $mn = nm$, para todo $m \in M$ e $n \in N$.*

Demonstração. De fato, se $N \trianglelefteq G$ e $M \trianglelefteq G$, tem-se $N^g = N$ e $M^g = M$, para todo $g \in G$, em particular, $N^m = N$, isto é, $nm \in N$, para todo $m \in M$. Logo, $m^{-1}nm \in N$ e, assim, $n^{-1}m^{-1}nm \in N$. Analogamente, $n^{-1}m^{-1}nm \in M$, já que $M \trianglelefteq G$. Deste modo, $n^{-1}m^{-1}nm \in M \cap N = 1_G$. Portanto, $nm = mn$. ■

Agora, com o auxílio do Lema 2.6, podemos enunciar e demonstrar, a seguir, de forma rápida e elementar, o teorema que generalizou a Conjectura 2.2.

Teorema 2.4. *Seja π um conjunto de números primos. Seja $x \in G$ e suponha que $Ind_{\langle a,x\rangle}(x)$ é um π-número para qualquer $a \in G$. Então, $Ind_G(x)$ é um π-número.*

Demonstração. Seja G um contraexemplo de ordem mínima. Escolha um primo $q \notin \pi$ que divide $Ind_G(x)$. Seja Q um Sylow q-subgrupo do $C_G(x)$ e R um Sylow q-subgrupo de G, tal que $Q \leq R$. Se $a \in R \backslash Q$, segue-se que $Ind_{\langle a,x,Q\rangle}(x)$ é divisível por q, daí, por indução, $G = \langle a, x, Q\rangle$. Seja $Z = Z(R)$. É fácil de ver que $Z \cap Q \leq Z(G)$. Se $Z \cap Q = \{1_G\}$, escolha $1_G \neq a \in Z$. Agora, a igualdade $G = \langle a, x, Q\rangle$ mostra que $Z(Q) \leq Z(G)$. Assim, $M = O_q(G) \neq 1_G$. Por indução o resultado é válido para G/M. Defina, $H/M = C_{(G/M)}(xM)$. Se $[G : H]$ é um π-número, basta que se prove que $Ind_H(x)$ é um π-número. Podemos assumir que $G = H$. Se $H < G$, o resultado segue por indução. Sendo central em G/M, o elemento x normaliza cada Sylow q-subgrupo de G. Pelo Lema 2.7, podemos concluir que x centraliza cada Sylow q-subgrupo de G. Assim, $Ind_G(x)$ não é divisível por q, uma contradição. A prova está completa. ■

Mas, o resultado principal mencionado no artigo [4] e a motivação deste trabalho é o seguinte teorema.

Teorema 2.5. *Suponha que $Ind_{\langle a,b,x\rangle}(x)$ é uma potência de primo para qualquer $a, b \in G$. Então, $Ind_G(x)$ é uma potência de primo.*

A prova do teorema 2.5 já não é tão simples e imediato. Particularmente, utilizamos o resultado conhecido por Aschbacher e Guralnick [1], que afirma, cada grupo simples não abeliano é 2-gerado. Isto depende da classificação dos grupos finitos simples. Outra importante ferramenta utilizada na prova do Teorema 2.5 é o teorema de Flavell [7], que afirma: $x \in F_2(G)$ se, e somente se $x \in F_2(\langle a, x\rangle)$ para qualquer $a \in G$.

Com o objetivo de provar o Teorema Principal desse trabalho, iremos mostrar dois lemas importantes .

Lema 2.7. *Se $G = F(G)\langle x\rangle$, o Teorema 2.5 é confirmado.*

Demonstração. Suponha que $Ind_G(x)$ é divisível por dois primos distintos, p e q. Escolhendo um p-elemento a e um q-elemento b em $F(G)$, tal que $[a, x] \neq 1_G$ e $[b, x] \neq 1_G$, segue-se que $Ind_{\langle a,b,x\rangle}(x)$ é divisível por ambos p e q, uma contradição. ■

No próximo lema usaremos a notação $Ind_H(x)$ mesmo quando $x \notin H$.

Lema 2.8. *Seja G um grupo agindo sobre um grupo abeliano V, e seja x um elemento de V, tal que $Ind_{\langle a,b\rangle}(x)$ é um potência de primo, para qualquer $a, b \in G$. Então, $Ind_G(x)$ é uma potência de primo.*

Demonstração. Escolha um contra-exemplo, com G de ordem mínima e, suponha que o $Ind_G(x)$ é divisível por dois números primos diferentes. Nota-se, que nenhum subgrupo normal não trivial de G centraliza x. Se isso fosse falso existiria um subgrupo normal N de G, tal que $N \leq C_G(x)$. Considere a ação de G/N em $W = C_V(N)$. Então, a órbita de x sob a ação de G é a mesma órbita, sob a ação de G/N obtendo uma contradição, uma vez que, $|G/N| < |G|$. Em seguida, percebe-se que G não é simples, já que todos os grupos simples são 2- gerados. Seja D um subgrupo normal minimal de G. Desde que $D < G$ e D não centralizar x, o índice $Ind_D(x)$ é uma p-potência para algum primo p. Seja $q \neq p$ outro primo que divide $Ind_G(x)$. Escolha um Sylow q- subgrupo S em G. Desde que $Ind_{DS}(x)$ é divisível por ambos p e q, por indução implica que $G = DS$. Suponha, primeiramente, que $S/S \cap D$ não é cíclico e escreva $S = S_1S_2$, onde S_1 e S_2 são subgrupos máximais distintos de S contendo $S \cap D$. Desde que $|DS_1| < |DS|$, segue-se que $Ind_{DS_1}(x)$ é um potência de primo e, assim, x centraliza um Sylow q- subgrupo em DS_1. Portanto, existe $d_1 \in D$, tal que $S_1^{d_1} \leq C_G(x)$. Da mesma forma, existe $d_2 \in D$, tal que $S_2^{d_2} \leq C_G(x)$. Desde que $C_G(x)$ não contenha um subgrupo de ordem igual $|S|$ e $|S_1| = |S_2| = |S|/q$, podemos concluir, que $S_1^{d_1}$ e $S_2^{d_2}$ são Sylow q-subgrupos $C_G(x)$. Portanto, S_1 e S_2 são conjugados em G. Isto leva a uma contradição porque as imagens de S_1 e S_2 em G/D são normais e distintas. Portanto, $S/S \cap D$ é cíclico. Seja $a \in S$, tal que $G = D\langle a\rangle$. Suponha-se que $a \in C_G(x)$. Sabemos que $C_D(x)$ contém um Sylow q-subgrupo Q de D. Escolhendo Q de tal modo

que $a \in N_G(Q)$, temos que $Q\langle a\rangle$ é um Sylow q-subgrupo de G contido no $C_G(x)$ e, assim, $Ind_G(x)$ não é divisível por q, uma contradição. Daí, $a \notin C_G(x)$. Naturalmente, este argumento também mostra que nenhum conjugado de a está contido no $C_G(x)$. Suponha, agora, que a normaliza um q'-subgrupo não trivial R em D. Sem perda de generalidade, podemos supor que $R\langle a\rangle$ é 2-gerados. Daí $Ind_{R\langle a\rangle}(x)$ é uma potência de primo. Uma vez que $a \notin C_G(x)$, segue-se que $R \leq C_G(x)$. Por outro lado, nenhum conjugado de a está contido em $C_G(x)$. Segue-se que cada conjugado de R está contido em $C_G(x)$. Assim, o fecho normal da R está contido em $C_G(x)$, uma contradição. Conclui-se que a não pode normalizar um q'-subgrupo não trivial de D. Seja, agora, $r \neq q$ um divisor primo de $|D|$ e R um Sylow r-subgrupo em D. Pelo argumento de Frattini, existe $d \in D$, tal que ad normaliza R. Seja a_0 um gerador do Sylow q-subgrupo de $\langle ad\rangle$ e d_0 um gerador do Sylow q'-subgrupo de $\langle ad\rangle$. Sem perda de generalidade, podemos supor que $a = a_0$, ou seja, poderíamos escolher a_0 no lugar de a. Em seguida, a centraliza um q'-elemento $d_0 \in D$. Portanto, $d_0 = 1$. No entanto, neste caso, a normaliza R, uma contradição. ■

Lema 2.9. *Se $x \notin Z(F(G))$ o Teorema 2.5 é confirmado.*

Demonstração. Suponhamos que o lema é falso. Seja G um contra-exemplo de ordem mínima. Dado x de tal maneira que $|G|$ é tão pequena quanto possível, pelo principal resultado de Carmina [5], concluímos que, $x \in F_2(\langle a, x\rangle)$ para todo $a \in G$. Assim, pelo teorema de Flavell [7], $x \in F_2(G)$. Como $x \notin Z(F(G))$, segue-se que $x \notin C_G(F(G))$ [[7], Teorema 6.1.3]. Portanto, existe um número primo p e um p-elemento $a \in F(G)$, tal que $[a, x] \neq 1_G$. Por hipótese, existe um primo $q \neq p$, tal que nenhum Sylow q-subgrupo de G comute com x. Escolha um Sylow q-subgrupo S, tal que S contém um Sylow q-subgrupo de $C_G(x)$, digamos T. Pelo Lema 2.8 $S \cap F(G) \leq T$. Considere $H = \langle x, a, S\rangle$. Uma vez que a está em cada Sylow p-subgrupo, $Ind_H(x)$ é divisível por p e q e, portanto, não é uma potência de primo. Assim, por indução, $H = G$. Uma vez que $a \in F(G)$ e $x \in F_2(G)$, observamos que $G/F_2(G)$ é um q-grupo e, assim, G tem a altura de Fitting no máximo 3. Considere $K = \langle x, a, N_G(T)\rangle$. Como $x \in N_G(T)$, $K = \langle x, a, N_G(T)\rangle \leq F(G)N_G(T)$. Ainda mais, $T < N_S(T)$, segue-se que $K = F(G)N_G(T) = G$. Assim, T é normal em S e $F(G)T$ é normal em G. Escolha $b \in S \setminus T$. Pela hipótese, $Ind_{\langle a,b,x\rangle}(x)$ é um p-potência e, assim, x centraliza um conjugado de b, digamos b^z. Mas, então, $b^z \in F(G)T$ e, assim, $b \in F(G)T \cap S = T$ e isto é uma contradição. ■

Agora, o Teorema 2.5 pode ser facilmente provado a partir do Lema 2.8 e 2.9. Se $x \notin Z(F(G))$, o resultado segue do Lema 2.9. Se $x \in Z(F(G))$, então $\langle x^G \rangle$ é abeliano e o resultado segue do Lema 2.8.

Anexo

Em 1959, o jornal americano *New York Times*, surpreende toda sociedade matemática publicando um artigo intitulado: "**50-YEAR PROBLEM IN MATH IS SOLVED: Student, 26, Proves Finite Conjecture**".

O estudante era Jonh Griggs Thompson, aluno de doutorado da Universidade de Chicago nos Estados Unidos, e o problema que ele solucionou era a conjectura de Frobenius sobre automorfismos sem pontos fixos. Apesar do reporter não mencionar, começava, naquele momento, a era moderna da teoria dos Grupos Finitos. Sua tese de doutorado "*A proof that a finite group with a fixed-point-free automophism of prime order is nilpotent*", como o título propõe, Thompson prova que se α é um automorfismo de ordem prima de um grupo finito G tal que $\alpha(x) \neq x$ para todo $x \neq 1$, então G é nilpotente. Mas, não foi a solução desta conjectura o mais maravilhoso, mas a criação de uma nova técnica revolucionária que não se havia suspeitado de sua existência até esse momento.Thompson havia inventado a teoria local dos grupos finitos, que fundamentalmente resultaria na classificação dos grupos simples.

Definição 2.2. *Um grupo G é dito simples se seus únicos subgrupos normais são o trivial e o próprio grupo.*

Acontecendo a grandes distâncias, pode se dizer que, os grupos simples desempenham na teoria dos grupos finitos o mesmo papel que os números primos na teoria dos números. Lembre-se que um subgrupo N de um grupo G se diz normal, e escreve-se $N \lhd G$, se:

$$gN = Ng,$$

para todo $g \in G$. O conceito de subgrupo normal é essencial na teoria dos grupos, pois, permite definir um novo grupo :

$$Ng = \{ng/n \in Neg \in G\},$$

a partir, dos subconjuntos de G. Se G é finito, então a ordem deste novo grupo é $\left|\frac{G}{N}\right| = \frac{|G|}{|N|}$, como se pode observar a estrutura de $\frac{G}{N}$ está estritamente ligada á G. Se conhecemos os grupos N e $\frac{G}{N}$, obtemos informações valiosas que certamente irão nos ajudar a compreender melhor G. Dizemos, anteriormente, que os grupos simples são como os números primos, neste momento, diremos em que sentido. Se G é um grupo finito, entre os subgrupos normais de G podemos escolher N com a ordem tão grande quanto possível. Da maximalidade de N como normal, facilmente, segue-se que $S = \frac{G}{N}$ é simples. Repetindo esse processo, podemos encontrar um número de subgrupos:

$$1_G = N_k \lhd N_{k-1} \lhd \cdots \lhd N_1 \lhd N_0,$$

com quociente $S_i = \frac{N_i}{N_{i+1}}$ simples. O teorema de Jordan-Hölder ([25],p165) afirma que o conjunto destes grupo simples S_i está unicamente determinado por G, e que não depende da série escolhida. Então, todo grupo finito é construído a partir de grupos simples. Parece razoável acreditar que se quesermos compreender grupos finitos, deveremos começar entendendo os grupos simples. No entanto, precisava-se saber quais os grupos que não têm subgrupos normais. Alguns grupos simples já eram conhecidos simplesmente por não ter espaço para terem subgrupos, estes grupos eram formados por p elementos, onde p é um número primo. Esses grupos são cíclicos e como grupos simples não são muito interessantes. Os grupos finitos cujo fatores de composição são todos cíclicos são chamados de *solúveis* e foram descobertos por Abel e Galois no estudo da resolução de equações polinimiais por radicais. Os grupos solúveis, que estão ligados aos números primos, possuem propriedades aritméticas fascinantes.

Definição 2.3. *Um grupo finito G é solúvel se existem subgrupos $N_0, N_1, \cdots, N_{k+1}$ de G com:*

$$G = N_0 \geq N_1 \geq \cdots \geq N_{k+1} = 1_G$$

que satisfazem as seguintes condições:

i) *N_{i+1} é normal em N_i, para todo $i = 0, 1, 2, \cdots, k$;*

ii) *$\frac{N_i}{N_{i+1}}$ é um grupo cíclico de ordem p.*

O grupo S_5 das permutações de 5 elementos tem ordem $5! = 120$ e não é solúvel. Este fato está ligado à irresolubilidade de equações de 5^o grau por radicais. Esta foi a grande descoberta de Golais, que deu início à Teoria dos Grupos.

Os grupos finitos simples são as "partículas elementares"da teoria dos grupos finitos e sua classificação, terminada, em 1980, ocupa mais de 10000 páginas de trabalhos escritos ao longo de mais de um século. O teorema da Classificação estabelece que todo grupo finito simples pertence a uma das seguinte categorias.

1. Grupos cíclico de ordem prima;
2. Grupos alternados;
3. Grupos de tipo Lie;
4. Grupos esporádicos.

O Teorema da Ordem Ímpar foi o elemento crucial em todas as demonstrações dos teoremas da Classificação dos Grupos Simples, ele afirma que:

Todo grupo de ordem ímpar é solúvel.

Trata-se de um enuciado curto e simples cuja prova obtida, em 1962, por Walter Feit e John Thompson, ocupou 255 páginas do Pacific Journal of Mathematics. As técnicas introduzidas ao longo da demonstração foram fundamentais, em grande parte, no desenvolvimento posterior da teoria dos grupos finitos. A partir do Teorema Feit-Thompson, constatou-se que os grupos simples têm ordem ímpar e, portanto, contém involuções, ou seja, elementos de $x \neq 1_G$ com $x^2 = 1_G$, Esse foi o primeiro passo e, talvez, o maior, para classifica-los; o segundo, foi a ideia maravilhosa de Richard Brauer de classificação de grupos simples de acordo com o subgrupo:

$$C_G(x) = \{g \in G | xg = gx\}.$$

Além dos grupos cíclicos de ordem p, com p número primo, existe, o grupo alternado A_n das permutações pares de um conjunto com n elementos, que são grupos simples, para todo $n \geq 5$ (ver [25], 9.1.7–p.166). Mas, a família com maior número de grupos simples são os grupos $G(q)$ chamados de *tipo Lie*, associados a espaços vetoriais finitos de tamanho q e a certas geometrias. Galois já conhecia alguns destes grupos, tal como grupos projectivos

especiais de matrizes sobre o corpo de q elementos de determinante 1 sobre seu centro. No ínicio do século XX, quase todos os grupos de tipo Lie eram conhecidos como grupos clássicos análogos aos correspondentes sobre o corpo $\mathbb{C}$, e foram motivos de estudo, dentre outros, de Jordan ó Dickson, por volta dos anos 50. Porém, em 1861, Mathieu havia descoberto cinco grupos simples que não eram alternados e nem pertenciam à qualquer um dos grupos de tipo Lie. Estes grupos foram chamados *esporádicos*, estes constituiam um grande mistério, pois, não sabiam quantos mais existiam. Esta foi a questão fundamental da teoria dos grupos durante décadas. Após um século, Janko detectou outro grupo esporádico que havia permanecido oculto, apesar do seu tamanho ser relativamente pequeno, 175560 elementos. A partir do descoberta de Janko foram encontrados 26 grupos simples esporádicos, bem como, o maior grupo esporádico conhecido como "*o mostro*"que tem aproximadamente 10^{54} elementos.

Referências Bibliográficas

[1] Aschbacher, Michael, and R. Guralnick, *Some applications of the first cohomology group.*Journal of Algebra **90-2**, p. 446-460, 1984. 39

[2] Baer, Reinhold, *Group elements of prime power index.* Transactions of the American Mathematical Society **75-1**, p.20-47, 1953.

[3] Burnside, William, *Theory of Groups of Finite Order.* Messenger of Mathematics **23**, p.112 , 1909. 19

[4] Camina, Alan R., Pavel Shumyatsky, and Carmela Sica, *On elements of prime-power index in finite groups.* Journal of Algebra **323-2**, p.522-525, 2010. i, ii, 33, 39

[5] Camina, A. R., and R. D. Camina, *Implications of conjugacy class size.*J. Group Theory **1-3**, p.257-269, 1998. ii, 36, 41

[6] Camina, A. R., and R. D. Camina, *The influence of conjugacy class sizes on the structure of finite groups: A survey.*Asian-European Journal of Mathematics **4-04** , p.559-588, 2011.

[7] Flavell, Paul, *A characterisation of $F_2(G)$*, J. Algebra **55**, p.271-287, 2002. 37, 39, 41

[8] Flavell, Paul, *On the Fitting height of a soluble group that is generated by a conjugacy class.* Journal of the London Mathematical Society **66-1**, p.101-113, 2002.

[9] Garcia, A.; Lequain, Y., *Elementos de Algebra.* Rio de Janeiro: IMPA, 2002. 8

[10] Gordeev, N., Grunewald, F., Kunyavskiĭ, B., and Plotkin, E, *A description of Baer–Suzuki type of the solvable radical of a finite group.* Journal of Pure and Applied Algebra **213.2**, p. 250-258, 2009.

[11] Gordeev, N., Grunewald, F., Kunyavskiĭ, B., and Plotkin, E. ,*A commutator description of the solvable radical of a finite group*, Groups, Geometry, and Dynamics **2**, p. 85-120, 2008.

[12] Gordeev, N., Grunewald, F., Kunyavskii, B., and Plotkin, E., *From Thompson to Baer-Suzuki: a sharp characterization of the solvable radical*. Journal of Algebra **323-10**, p.2888-2904, 2010.

[13] Gordeev, N., Grunewald, F., Kunyavskii, B., and Plotkin, E., *On the number of conjugates defining the solvable radical of a finite group*. Comptes Rendus Mathematique **343-6**, p.387-392, 2006.

[14] Gordeev, N., Grunewald, F., Kunyavskiĭ, B., Plotkin, E., *On the number of conjugates defining the solvable radical of a finite group*. Comptes Rendus Mathematique **343-6**, p.387-392 , 2006.

[15] Gorenstein, D., *Finite Groups*, New York: Harper and Row, 1968. i

[16] Grunewald, Fritz, Boris Kunyavskii, and Eugene Plotkin, *Characterization of solvable groups and solvable radical*. International Journal of Algebra and Computation **23.05**, p. 1011-1062, 2013.

[17] Guralnick, R., Grunewald, F., Kunyavskii, B., Plotkin, E., and Shalev, A., *Thompson-like characterizations of the solvable radical*. Journal of Algebra **300-1**, p.363-375, 2006.

[18] Guralnick, R., Kunyavskiĭ, B., Plotkin, E., Shalev, A., *Thompson-like characterizations of the solvable radical*. Messenger of Mathematics **300-1**, p.363-375 , 2006. 30

[19] Gracián, Adolfo Quirós, and Gabriel Navarro, *John G. Thompson y los grupos finitos*. "LAS MEDALLAS FIELDS". La Gaceta de la RSME **9.1**, p.183-189, 2006.

[20] Houcine, Abderezak Ould,*A remark on the definability of the Fitting subgroup and the soluble radical*. Mathematical Logic Quarterly **59.1-2**, p.62-65, 2013.

[21] José Felipe Voloch e Laura Martignon (Entrevistadores), *Walter Feit comenta o Teorema da Ordem Ímpar e a classificação dos grupos simples*, Matemática Unversitária **07**, p.11-20, 1988.

[22] Kazarin, Lev Sergeevich, *Burnside's p^{α}-lemma*, Mathematical Notes **48**, p.749-751, 1990. i, 34

[23] Liu, Xiaolei, Yanming Wang, and Huaquan Wei, *Notes on the length of conjugacy classes of finite groups*. Journal of Pure and Applied Algebra **196-1**, p.111-117, 2005.

[24] Martinez, Elena Alemany, *Estructura de grupos finitos y propiedades aritméticas de los tamanos de clase de conjugación*. 2011.

[25] Robinson, Derek J. S., *An Introduction to Abstract Algebra*. New York: Walter de Gruyter Berlin, 2003. 44, 45

[26] Rose, Harvey E., *A Course on Finite Groups*. London: Springer- Verlag, 2009. 9, 23

[27] Rotman, Joseph J., *An Introduction to the Theory of Groups*. New York: Springer-Verlag, 4. ed., 1995.

[28] Shumyatsky, Pavel, *Finite groups and the fixed points of coprime automorphisms*. Proceedings of the American Mathematical Society **129-12**, p.3479-3484, 2001.