Universidade Federal de Minas Gerais
Instituto de Ciências Exatas
Departamento de Matemática

Grupos satisfazendo as condições $(\mathcal{A}, n)$ e $(\mathcal{N}, n)$

Willian Vieira de Paula

Orientadora:

Ana Cristina Vieira

Dissertação apresentada ao Departamento de Matemática da Universidade Federal de Minas Gerais, como parte dos requisitos para obtenção do título de Mestre na área de Matemática.

UFMG - Belo Horizonte
2007

Dedicado a meus pais, José Francisco e Maria da Penha

Agradecimentos

Primeiramente a Deus, por tudo. Agradeço imensamente aos meus pais, José Francisco e Maria de Penha, por tudo que fizeram por mim.

Minha irmã Rose, meus irmãos mais velhos Elin e Markim, muito obrigado pela ajuda, confiança e atenção. Minhas cunhadas Del e Marli e minhas sobrinhas Mayara e Maryelle.

Agradeço a minha namorada Meyr, por todo o amor e dedicação, e por ter sido a companhia mais presente em minha vida nestes anos de mestrado, mesmo estando longe.

A professora Ana Cristina Vieira, pelo apoio e orientação que me ajudaram a concluir este trabalho.

Meus queridos professores da UFV Marinês Guerreiro e Olímpio Miyagaki.

Gostaria de agradecer especialmente aos amigos Heleno, Perigoso, Ná e Perigosinho, Raquel, Rutyele, Tarcísio e Viviane pelas valiosas dicas para a apresentação.

Aos amigos de Viçosa, especialmente Wally, Adriano, Alessandro, André, Fábio e Geraldo. E a todos os amigos que fiz na UFV, UnB, UEG, UFMG e PUC-Minas. Enfim, agradeço a todos cujos nomes não aparecem aqui, mas cuja amizade foram fundamentais para que eu pudesse trilhar este caminho.

All you need is love

Lennon e McCartney

Resumo

Neste trabalho caracterizamos grupos finitos não solúveis que satisfazem a condição $(\mathcal{N}, 21)$. Damos também a caracterização dos grupos que satisfazem a condição $(\mathcal{A}, n)$, utilizando para isto alguns resultados de Teoria de Grafos.

Abstract

In this work we give the characterization of insoluble finite groups satisfying the condition $(\mathcal{N}, 21)$. We also give the characterization of groups satisfying the condition $(\mathcal{A}, n)$, using some results of Graph Theory.

Sumário

Lista de Símbolos

$\mathcal{A}$	Classe dos grupos abelianos
$\mathcal{N}$	Classe dos grupos nilpotentes
$\mathcal{CPF}$	Classe dos grupos cujo centro tem índice finito
$\mathcal{PE}$	Classe dos PE-grupos
$\mathcal{Z}(G)$	Centro do grupo G
$[x, y] = x^{-1}y^{-1}xy$	Comutador de x e y
$G \cong H$	G e H são isomorfos
$\|G\|$	Ordem do grupo G
$[G : H]$	O índice de H em G
$C_G(H)$	O centralizador de H em G
$N_G(H)$	O normalizador de H em G
$H \leq G$	H é subgrupo de G
$H \lhd G$	H é subgrupo normal de G
$H\ car\ G$	H é subgrupo característico de G
$\langle X \rangle$	Subgrupo gerado por X
$Syl_p(G)$	O conjunto dos p-subgrupos de Sylow de G
$\mathcal{Z}^*(G)$	Hipercentro de G
$\Gamma(G)$	Grafo associado ao grupo G
$A \times B$	Produto direto dos grupos A e B
S_n	Grupo simétrico de grau n
A_n	Grupo alternado de grau n
$M_n(R)$	Anel das matrizes sobre um anel R
I_n	Matriz identidade de ordem n
$Aut(G)$	O grupo de automorfismos de G
$CR(G)$	O CR-radical sem centro de G
$Sol(G)$	O radical solúvel de G
$H \hookrightarrow G$	H está isomorficamente imerso em G

Introdução

Considere um grupo que não satisfaça alguma propriedade, como, por exemplo, ser abeliano. No entanto pode ser que este grupo possua elementos que geram um subgrupo que satisfaz esta propriedade. A pergunta que guia nosso trabalho é a seguinte: *Qual o número mínimo de elementos que devemos tomar em um grupo para garantir que dois deles gerem um subgrupo que esteja em uma determinada classe?*

Ao denotar por $\mathcal{X}$ uma classe qualquer de grupos (abelianos, nilpotentes, CPF-grupos, etc.) e considerar um inteiro $n > 0$, dizemos que um grupo G satisfaz a condição $(\mathcal{X}, n)$ se, em qualquer subconjunto com $n+1$ elementos de G, existem dois elementos distintos que geram um subgrupo que pertence a classe $\mathcal{X}$.

Em 1976, B. H. Neumann [11] mostrou que G é um grupo satisfazendo a condição $(\mathcal{A}, n)$ se, e somente se, G é central-por-finito, ou seja, seu centro $Z(G)$ tem índice finito. Em 1987, L. Pyber [12] apresentou um limite para o índice $[G : Z(G)]$, quando G satisfaz a condição $(\mathcal{A}, n)$.

Em 1992, M. Tomkinson [16] mostrou que se G é a união de n subgrupos, cada um dos quais sendo nilpotente de classe c, então $[G : Z_k(G)] \leq (n!)!$, onde $k = c(r + c^{log2r})$ e $r = (n!)!$, com $Z_k(G)$ o k-ésimo termo da série central superior de G. Como uma consequência disto, Tomkinson mostrou que G é uma união finita de subgrupos nilpotentes se, e somente se, algum termo $Z_m(G)$ da série central superior de G tem índice finito. Além disso, demonstrou o seguinte resultado: *Se G é um grupo solúvel finitamente gerado satisfazendo a condição $(\mathcal{N}, n)$, então* $[G : \mathcal{Z}^*(G)] < n^{n^4}$, onde $\mathcal{Z}^*(G)$ denota o hipercentro de G.

Em 1994, G. Endimioni [3] estudou grupos finitos satisfazendo a condição $(\mathcal{N}, n)$. No seu artigo, ele mostrou o seguinte resultado: *Um grupo finito satisfazendo a condição $(\mathcal{N}, n)$, para $n \leq 20$, é necessariamente solúvel.*

Uma questão se torna pertinente: *para quais valores de n podemos dizer que um grupo finito satisfazendo a condição $(\mathcal{N}, n)$ é uma união de n subgrupos nilpotentes?* Em seu trabalho de 2004, A. Abdollahi e A. Hassanabadi [1] caracterizaram grupos finitos não solúveis satisfazendo a condição $(\mathcal{N}, 21)$ mostrando que estes são tais que $\dfrac{G}{Z^*(G)} \cong A_5$. Como uma consequência, garantiram que um grupo finito não solúvel satisfaz a condição $(\mathcal{N}, 21)$ se, e somente se, é uma união de 21 subgrupos nilpotentes.

Nesta dissertação estudamos grupos que satisfazem as condições $(\mathcal{A}, n)$ e $(\mathcal{N}, n)$ e damos uma caracterização dos grupos que satisfazem $(\mathcal{A}, n)$ e $(\mathcal{N}, 21)$.

O Capítulo 1 contém alguns pré-requisitos para os capítulos seguintes. Basicamente fazemos neste capítulo um apanhado geral sobre os conceitos de grupos solúveis e grupos nilpotentes e também listamos algumas propriedades importantes de alguns grupos finitos, além de apresentar os problemas a serem estudados nos capítulos seguintes e falarmos um pouco mais sobre grupos que satisfazem a condição $(\mathcal{X}, n)$.

No Capítulo 2 estudamos grupos que satisfazem a condição $(\mathcal{A}, n)$ e caracterizamos quais os grupos que satisfazem esta condição, utilizando para isto alguns resultados sobre teoria dos grafos, com destaque para o Teorema de Ramsey. Damos também exemplos de grupos que satisfazem e não satisfazem a condição $(\mathcal{A}, n)$, para certos valores de n.

No Capítulo 3 inicialmente apresentamos o resultado de Endimioni que diz que todo grupo que satisfaz a condição $(\mathcal{N}, n)$, para $n \leq 20$ é solúvel, e em seguida damos a caracterização dos grupos não-solúveis que satisfazem a condição $(\mathcal{N}, 21)$.

Finalizamos a dissertação com alguns comentários e resultados com os quais nos deparamos durante a elaboração deste trabalho, que podem ser considerados a continuidade dos assuntos aqui tratados.

Capítulo 1

Resultados Preliminares

Neste capítulo introduzimos as principais definições e resultados sobre grupos a serem utilizados no decorrer da dissertação, indicando as referências para a demonstração de alguns deles.

Começamos com o conceito de classe. Consideramos intuitivamente que uma *classe* $\mathcal{X}$ é uma coleção de objetos, chamados *elementos*, em que podemos determinar quando um elemento x é membro de $\mathcal{X}$ ($x \in \mathcal{X}$) ou não é membro de $\mathcal{X}$ ($x \notin \mathcal{X}$). Uma *classe de grupos* $\mathcal{X}$ é uma classe cujos elementos são grupos com alguma propriedade em comum, que satisfaz as seguintes condições:

1. $\mathcal{X}$ contém um grupo de ordem 1;

2. se $G \in \mathcal{X}$ e $W \cong G$, então $W \in \mathcal{X}$.

Por exemplo, todos os grupos abelianos formam uma classe, que denotaremos por $\mathcal{A}$. Observamos que a classe dos grupos abelianos é fechada, ou seja, se A é um grupo em $\mathcal{A}$ então qualquer subgrupo de A também está na classe $\mathcal{A}$. Uma classe de grupos importante no decorrer deste trabalho é a classe dos CPF-grupos, que definimos a seguir.

Definição 1.1 *Um grupo G cujo centro tem índice finito é chamado de* central-por-finito*. Denotamos por $G \in \mathcal{CPF}$ e diremos que G é um CPF-grupo.*

Exemplos imediatos de CPF-grupos são os grupos finitos.

Note que se G é um grupo finitamente gerado por $\{x_1, \ldots, x_n\}$ para o qual o centralizador de todo elemento $x \in G$ é de índice finito, ou seja, $[G : C_G(x)] < \infty$, para todo $x \in G$, então $G \in \mathcal{CPF}$. Realmente, desde que $\mathcal{Z}(G) = \bigcap_{k=1}^{n} C_G(x_k)$, este fato segue do resultado a seguir:

Proposição 1.2 *Seja G um grupo e H, K são subgrupos de G tais que $[G : H] < \infty$ e $[G : K] < \infty$. Então $[G : H \cap K] \leq [G : H]\,[G : K]$.*

Demonstração: Defina a seguinte aplicação entre classes laterais

$$x(H \cap K) \longmapsto (xH, xK).$$

Observamos que esta aplicação está bem definida e é injetiva pois se tomarmos $x, y \in G$, então

$$\begin{aligned} x(H \cap K) = y(H \cap K) \quad &\Leftrightarrow \quad y^{-1}x \in H \cap K \Leftrightarrow \\ y^{-1}x \in H \text{ e } y^{-1}x \in K \quad &\Leftrightarrow \quad xH = yH \text{ e } xK = yK \Leftrightarrow \\ (xH, xK) = (yH, yK). & \end{aligned}$$

Pela injetividade da aplicação, temos

$$[G : H \cap K] \leq [G : H]\,[G : H]\,.$$

∎

Introduzimos na próxima seção duas classes de grupos importantes neste trabalho: as classes dos grupos solúveis e dos grupos nilpotentes.

1.1 Grupos Solúveis e Nilpotentes

Um dos conceitos mais antigos da Teoria de Grupos é o de grupo solúvel, introduzido por Evariste Galois quando estudava o problema de resolver equações algébricas por meio de radicais [10].

Definição 1.3 *Um grupo G é* solúvel *se contém uma cadeia de subgrupos*

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

tal que cada subgrupo G_{i-1} é normal em G_i e o grupo quociente $\dfrac{G_i}{G_{i-1}}$, $1 \leq i \leq n$, é abeliano.

Uma cadeia de subgrupos de G com esta propriedade chama-se uma *série subnormal abeliana* de G e os quocientes respectivos chamam-se *fatores* da série. Se G é solúvel, o comprimento de sua menor série derivada é chamado *comprimento derivado* de G.

É fácil ver que todo grupo abeliano é solúvel. Um exemplo de grupo não-abeliano que é solúvel é o grupo simétrico

$$S_3 = \left\langle x, y;\; x^2 = 1;\; y^3 = 1;\; xy = y^{-1}x \right\rangle.$$

De fato, se $H = \langle y \rangle$, então H tem ordem 3 e, portanto, é normal em G. Além disso, $\dfrac{S_3}{H}$ é cíclico, portanto abeliano. Logo $1 \subset H \subset G$ é uma série subnormal abeliana de S_3.

Dados dois elementos x, y em um grupo G, o *comutador* de x e y é o elemento $[x, y] = x^{-1}y^{-1}xy \in G$. Definimos indutivamente o *elemento comutador de comprimento* $n \geq 2$ por

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

onde $[x_1] = x_1$ e $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$.

Analogamente, dados dois subconjuntos não vazios H e K de um grupo G, definimos o *subgrupo comutador* de H e K por

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

De maneira análoga com os elementos comutadores de comprimento n, definimos o subgrupo comutador de ordem n denotado por $[H,\ _n K]$.

O subgrupo $G' = [G, G]$ é chamado *subgrupo derivado* de G. Definimos indutivamente a *série derivada* de G da seguinte forma:

$$\begin{aligned} G^{(0)} &= G, \\ G^{(1)} &= \left[G^{(0)}, G^{(0)}\right] = G' \text{ e} \\ G^{(n)} &= \left[G^{(n-1)}, G^{(n-1)}\right], \text{ para } n \geq 2. \end{aligned}$$

Observação 1.4 *Se H, K são subgrupos de G, valem as seguintes propriedades* [10]*:*

1. $[H, K] = [K, H]$*;*
2. *Se $H \subset G$, então $H^{(n)} \subset G^{(n)}$, para todo $n \in \mathbb{N}$;*
3. *$G^{(n)}$ car G, para todo inteiro não-negativo n. Em particular, $G^{(n+1)} \lhd G^{(n)}$;*
4. *Seja $H \lhd G$. Então $\dfrac{G}{H}$ é abeliano se, e somente se, $G' \subset H$. Em particular, $\dfrac{G^{(n)}}{G^{(n+1)}}$ é abeliano.*
5. *Se $H \subset K$ e ambos sï¿½o normais em G entï¿½o:*

$$\frac{K}{H} \subset \mathcal{Z}\left(\frac{G}{H}\right) \text{ se, e somente se, } [K, G] \subset H.$$

O próximo resultado dá uma caracterização de solubilidade em termos da série derivada de um grupo.

Teorema 1.5 *Um grupo G é solúvel se, e somente se, sua série derivada termina, isto é, se existe um inteiro positivo n tal que $G^{(n)} = \{1\}$.*

Demonstração: Suponha que existe $n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$, então

$$\{1\} = G^{(n)} \subset \cdots \subset G^{(0)} = G$$

é uma série subnormal abeliana de G. Portanto, G é solúvel.

Reciprocamente, se G é solúvel então contém uma série subnormal abeliana

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

Assim $\dfrac{G_i}{G_{i+1}}$ é abeliano e, pela Observação 1.4, temos com isso que $G_i' \subset G_{i+1}$, com $0 \leq i \leq n-1$. Em particular, $G' \subset G_1$. Suponha, por indução, que $G^{(k)} \subset G_k$, para algum inteiro positivo k. Então

$$G^{(k+1)} = \left[G^{(k)}, G^{(k)}\right] \subset [G_k, G_k] = G_k' \subset G_{k+1}.$$

Segue, por indução, que $G^{(i)} \subset G_i$, $0 \leq i \leq n$. Em particular, $G^{(n)} \subset G_n = \{1\}$.

■

Note na demonstração acima que se G for solúvel, então nenhuma série subnormal abeliana pode ser mais curta que a série derivada, isto é, o comprimento derivado de G é igual ao comprimento de sua série derivada.

Seja G um grupo solúvel e $H \leq G$. Pela Observação 1.4, temos $H^{(i)} \subset G^{(i)}$, para todo inteiro não-negativo i. Pelo Teorema 1.5, existe um inteiro positivo n tal que $G^{(n)} = \{1\}$, portanto $H^{(n)} = \{1\}$. Logo H é solúvel. Isto mostra que subgrupos de grupos solúveis são solúveis.

Se G é solúvel e $H \lhd G$, considere o homomorfismo canônico $\phi : G \to \dfrac{G}{H}$. Temos $\phi(G') = (\phi(G))'$. Suponha $\phi(G^{(n)}) = (\phi(G))^{(n)}$, então

$$\phi(G^{(n+1)}) = \phi(G^{(n)\prime}) = (\phi(G^{(n)}))' = ((\phi(G))^{(n)})' = (\phi(G))^{(n+1)},$$

segue por indução que, para todo inteiro $i \geq 0$,

$$\phi(G^{(i)}) = (\phi(G))^{(i)} = \left(\frac{G}{H}\right)^{(i)}.$$

Com este resultado em mente, vamos demonstrar o:

Teorema 1.6 *Seja H um subgrupo normal de um grupo G. Então G é solúvel se, e somente se, ambos H e $\dfrac{G}{H}$ são solúveis.*

Demonstração: Suponha que G é solúvel e seja $n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$, então $H^{(n)} = \{1\}$. Considere o homomorfismo canônico $\phi : G \to \frac{G}{H}$, como anteriormente. Assim,

$$\left(\frac{G}{H}\right)^{(n)} = \phi(G^{(n)}) = \phi\left(\{1\}\right) = \{1\},$$

isto mostra que $\dfrac{G}{H}$ é solúvel.

Reciprocamente, se $\dfrac{G}{H}$ é solúvel então existe um inteiro positivo n tal que

$$\left(\frac{G}{H}\right)^{(n)} = \phi(G^{(n)}) = \{1\},$$

portanto $G^{(n)} \subset Ker\phi = H$. E se H é solúvel, existe $m \in \mathbb{N}$ tal que $H^{(m)} = \{1\}$. Logo,

$$G^{(m+n)} = (G^{(n)})^{(m)} \subset H^{(m)} = \{1\},$$

e, pelo Teorema 1.5, concluímos que G é solúvel.

■

Este teorema nos diz que a classe dos grupos solúveis é fechada quanto à formação de quocientes. Como consequência obtemos mais exemplos de grupos solúveis, como os p-grupos finitos.

Corolário 1.7 *Todo p-grupo finito é solúvel.*

Demonstração: Seja G um p-grupo finito, isto é, $|G| = p^n$, para algum $n \geq 1$. Vamos utilizar indução sobre n.

Se $n = 1$, então $|G|$ é um número primo, com isso G é abeliano, portanto solúvel.

Seja $n > 1$. Se G for abeliano, então G é solúvel. Agora suponha por indução que todo p-grupo de ordem menor que $|G|$ é solúvel. Se G não é abeliano então $\mathcal{Z}(G) \neq G$ e, como G um p-grupo, temos que $\mathcal{Z}(G)$ é um subgrupo não trivial de G. Além disso, $\mathcal{Z}(G)$ é solúvel, pois é abeliano e, como $\left|\dfrac{G}{\mathcal{Z}(G)}\right| < |G|$, segue pela hipótese de indução que $\dfrac{G}{\mathcal{Z}(G)}$ é solúvel. Logo, pelo Teorema 1.6, concluímos que G é solúvel.

■

Um resultado clássico sobre grupos solúveis é o Teorema de Burnside, enunciado a seguir, obtido em 1904. A demonstração pode ser encontrada em [6].

Teorema 1.8 (Burnside) *Todo grupo finito de ordem $p^\alpha q^\beta$, onde p e q são primos, $\alpha, \beta \in \mathbb{N}$, é solúvel.*

Uma outra classe importante de grupos que faz parte deste trabalho é a classe dos grupos nilpotentes, que denotaremos por $\mathcal{N}$.

Definição 1.9 *Um grupo G é* nilpotente *se contém uma série de subgrupos*

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

tal que G_{i-1} é normal em G e $\dfrac{G_i}{G_{i-1}} \subset \mathcal{Z}\left(\dfrac{G}{G_{i-1}}\right)$, *para* $1 \leq i \leq n$.

Uma série de G com esta propriedade é chamada *série central* de G.

É fácil ver que todo grupo nilpotente é solúvel. Daremos agora um exemplo de um grupo solúvel que não é nilpotente. Para isto, vamos precisar do lema a seguir.

Lema 1.10 *O centro de um grupo nilpotente é não-trivial.*

Demonstração: Seja G um grupo nilpotente. Pela definição observamos que G_1 está contido no centro de G. Se for $G_1 = \{1\}$, então G_2 está contido no centro de G, e assim sucessivamente. Como a série central termina em G resulta que, para algum inteiro i teremos $G_{i-1} = \{1\}$ com $G_i \neq \{1\}$. Como G_i está contido no centro de G, segue que este é não-trivial.

■

Como o centro de S_3 é trivial segue, pelo Lema 1.10, que S_3 não é nilpotente, apesar de ser solúvel. Mais geralmente, S_n não é solúvel, para todo $n \geq 5$, enquanto S_4 é solúvel apesar de não ser nilpotente [13].

Damos agora duas caracterizações alternativas de nilpotência, que relacionam a propriedade de um grupo ser nilpotente a certos tipos de comutadores.

Definimos a *série central superior* de um grupo G por

$$\{1\} = \mathcal{Z}_0(G) \subset \mathcal{Z}_1(G) \subset \cdots \subset \mathcal{Z}_n(G) \subset \cdots$$

onde $\mathcal{Z}_0(G) = \{1\}$, $\mathcal{Z}_1(G) = \mathcal{Z}(G)$ e $\mathcal{Z}_i(G)$ é definido indutivamente como sendo o único subgrupo de G tal que

$$\frac{\mathcal{Z}_i(G)}{\mathcal{Z}_{i-1}(G)} = \mathcal{Z}\left(\frac{G}{\mathcal{Z}_{i-1}(G)}\right),$$

para $i \geq 2$.

Definimos a *série central inferior* de G como

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

onde $\gamma_1(G) = G$ e $\gamma_i(G) = [\gamma_{i-1}(G), G]$, quando $i \geq 2$.

Note que se G é nilpotente então as séries $\gamma_i(G)$ e $\mathcal{Z}_i(G)$ terminam em $\{1\}$ e G, respectivamente. Reciprocamente, se existe $m \in \mathbb{N}$ tal que $\gamma_m(G) = \{1\}$ (ou existe $k \in \mathbb{N}$ tal que $\mathcal{Z}_k(G) = G$), então G é nilpotente. Neste caso, o comprimento da série central superior concide com o comprimento da série central inferior, e este comprimento é chamado de *classe de nilpotência* de G.

Seja

$$D_4 = \left\langle a, b; a^4 = 1, b^2 = 1, ab = ba^{-1} \right\rangle$$

o grupo diedral de ordem 8. Assim, $\mathcal{Z}_0(D_4) = \{1\}$, $\mathcal{Z}_1(D_4) = \mathcal{Z}(D_4) = \langle a^2 \rangle$ e $\mathcal{Z}_2(D_4) = D_4$. Além disso, $\gamma_1(D_4) = D_4$, $\gamma_2(D_4) = \langle a^2 \rangle$ e $\gamma_3(D_4) = \{1\}$. Neste exemplo, a série central inferior coincide com a série central superior

$$\{1\} \subset \left\langle a^2 \right\rangle \subset D_4,$$

portanto D_4 é nilpotente de classe 2.

Seja G um grupo e $H \leq G$. Note que $\gamma_1(H) = H \subset G = \gamma_1(G)$. Além disso se $i \geq 2$, então $\gamma_i(H) = [\gamma_{i-1}(H), H] \subset [\gamma_{i-1}(G), G] = \gamma_i(G)$. Se G é nilpotente, isto é, existe $m \in \mathbb{N}$ tal que $\gamma_m(G) = \{1\}$, então $\gamma_m(H) = \{1\}$, donde H é nilpotente. Concluímos que todo subgrupo de um grupo nilpotente é também nilpotente.

Além disso, vale o seguinte resultado:

Lema 1.11

1. *Todo grupo quociente de um grupo nilpotente é nilpotente.*

2. *O produto direto de grupos nilpotentes é nilpotente.*

Demonstração: Se G é nilpotente e $N \lhd G$, então $\mathcal{Z}_i(G)$ se projeta em $\mathcal{Z}_i\left(\dfrac{G}{N}\right)$ e daí $\mathcal{Z}_n\left(\dfrac{G}{N}\right) = \dfrac{G}{N}$, para algum n e, portanto, $\dfrac{G}{N}$ é nilpotente. Isto mostra o item 1. O item 2 segue por indução e do seguinte fato: o centro de um produto direto é o produto direto dos centros de cada fator.

■

A série central superior de um grupo G apresenta as seguintes características:

Lema 1.12 *Seja G um grupo. Então*

1. $\mathcal{Z}_m\left(\dfrac{G}{\mathcal{Z}_n(G)}\right) = \dfrac{\mathcal{Z}_{m+n}(G)}{\mathcal{Z}_n(G)}$, *para quaisquer inteiros positivos m e n;*

2. *se $\dfrac{G}{\mathcal{Z}_n(G)}$ é nilpotente, para algum inteiro positivo n, então G é nilpotente.*

Demonstração: A demonstração da parte 1 pode ser encontrada em [13]. Para a parte 2, se $\dfrac{G}{\mathcal{Z}_m(G)}$ é nilpotente, então existe um inteiro positivo m tal que $\mathcal{Z}_m\left(\dfrac{G}{\mathcal{Z}_n(G)}\right) = \dfrac{G}{\mathcal{Z}_n(G)}$ e, pelo item 1, temos

$$\frac{\mathcal{Z}_{m+n}(G)}{\mathcal{Z}_n(G)} = \frac{G}{\mathcal{Z}_n(G)},$$

portanto $\mathcal{Z}_{m+n}(G) = G$. Logo G é nilpotente.

■

O próximo resultado é análogo ao Corolário 1.7.

Proposição 1.13 *Todo p-grupo finito é nilpotente.*

Demonstração: Seja G um p-grupo finito, cuja série central superior é dada por

$$\{1\} = \mathcal{Z}_0(G) \subset \mathcal{Z}_1(G) \subset \cdots \subset \mathcal{Z}_n(G) \subset \cdots$$

Por definição, $\dfrac{\mathcal{Z}_{i+1}(G)}{\mathcal{Z}_i(G)} = \mathcal{Z}\left(\dfrac{G}{\mathcal{Z}_i(G)}\right)$, para todo $i \in \mathbb{N}$. Suponha que G não seja nilpotente, ou seja, para todo $i \in \mathbb{N}$, $\mathcal{Z}_i(G) \neq G$, então $\dfrac{G}{\mathcal{Z}_i(G)}$ é um p-grupo (não trivial), portanto seu centro é não trivial, o que implica que $\dfrac{\mathcal{Z}_{i+1}(G)}{\mathcal{Z}_i(G)}$ também é não trivial. Logo, para todo $i \in \mathbb{N}$, temos $\mathcal{Z}_i(G) \subsetneq \mathcal{Z}_{i+1}(G)$, isto é, não aparecem fatores repetidos na série central superior.

Como G é finito, então existe $k \in \mathbb{N}$ tal que $\mathcal{Z}_k(G) = G$, uma contradição. Portanto, G deve ser nilpotente, o que conclui a demonstração.

■

Teorema 1.14 *Seja G um grupo finito. Então G é nilpotente se, e somente se, G é o produto direto de seus subgrupos de Sylow.*

Demonstração: Se G é o produto direto de seus subgupos de Sylow, então G é nilpotente, pela Proposição 1.13 e pelo ítem 2 do Lema 1.11.

Reciprocamente, suponha que G é nilpotente e seja P um p-subgrupo de Sylow de G. Suponha que $N_G(P)$ é um subgrupo próprio de G. Então

$$\{1\} = \mathcal{Z}_0(G) \subset N_G(P) \subset \mathcal{Z}_n(G) = G$$

e existe $i \in \mathbb{N}$ tal que $\mathcal{Z}_i(G) \subset N_G(P)$ e $\mathcal{Z}_{i+1} \not\subseteq N_G(P)$. Tome $x \in \mathcal{Z}_{i+1}(G) \backslash N_G(P)$. Pelo item 5 da Observação 1.4, temos

$$[\mathcal{Z}_{i+1}(G), G] \subset \mathcal{Z}_i(G).$$

Assim, para cada $n \in N_G(P)$, existe $y \in \mathcal{Z}_i(G) \subset N_G(P)$ tal que $xnx^{-1} = ny \in N_G(P)$, logo $(N_G(P))^x \subset N_G(P)$. Portanto, $x \in N_G(N_G(P))$, isto é, existe um elemento que pertence $N_G(N_G(P))$ mas não pertence a $N_G(P)$, ou seja, $N_G(P) \subsetneq N_G(N_G(P))$. Isto é um absurdo, pois se P é um p-subgrupo de Sylow de (qualquer grupo) G, então $N_G(P) = N_G(N_G(P))$ [10]. Logo, $N_G(P) = G$, isto é, todo p-subgrupo de Sylow de G é normal em G. Assim, pelo Teorema de Sylow, existe exatamente um p-subgrupo de Sylow de G, para cada primo p. Portanto, o produto dos p-subgrupos de Sylow de G é direto, igual a G.

■

Observe que se G é nilpotente, $|G| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, onde os p_i são primos distintos e $P_1 \in Syl_{p_1}(G), \ldots, P_n \in Syl_{p_n}(G)$, então $G = P_1 \times \ldots \times P_n$.

Um outro critério de nilpotência é o seguinte [10]:

Teorema 1.15 *Seja $N \leq \mathcal{Z}(G)$. Se N e $\dfrac{G}{N}$ são nilpotentes então G é nilpotente.*

Um conceito fundamental neste trabalho é o de *hipercentro* de um grupo.

Definição 1.16 *Definimos o* hipercentro *de G por $\mathcal{Z}^*(G) = \bigcup_{k \geq 0} Z_k(G)$.*

Observe que se G é um grupo finito, então $\mathcal{Z}^*(G) = \mathcal{Z}_m(G)$, para algum inteiro positivo n. Além disso, se $H \leq G$, então $\mathcal{Z}^*(G) \cap H \leq \mathcal{Z}^*(H)$. Portanto, se $\mathcal{Z}^*(G) \leq H$ então, $\mathcal{Z}^*(G) \leq \mathcal{Z}^*(H)$.

Outros resultados que serão utilizados neste trabalho são os relacionados aos chamados grupos de Engel. Seja G um grupo, dizemos que $g \in G$ é um *elemento de Engel à direita* se, para cada $x \in G$, existe um inteiro positivo $n = n(g, x)$ tal que $[g,_n x] = 1$. Analogamente, $g \in G$ é um *elemento de Engel à esquerda* se, para cada $x \in G$, existe um inteiro positivo $n = n(g, x)$ tal que $[x,_n g] = 1$.

Os conjuntos dos elementos de Engel à direita e à esquerda são denotados por $R(G)$ e $L(G)$, respectivamente.

Definição 1.17 *Dado um grupo G, se $G = R(G)$ ou $G = L(G)$, chamamos G de grupo de Engel.*

O próximo resultado é interessante pois relaciona os elementos de Engel ao hipercentro de um grupo finito.

Teorema 1.18 (Baer) *Se G é um grupo finito, então $R(G) = \mathcal{Z}^*(G)$.*

O Teorema de Baer é mais geral do que como está apresentado aqui. Na verdade, o grupo G não precisa ser finito. De fato, o Teorema de Baer garante que se G é um grupo que satisfaz a condição de maximalidade (ou seja, toda cadeia de subgrupos de G possui um elemento maximal), então $R(G)$ coincide com o hipercentro de G. A demonstração pode ser encontrada em [13] (página 374).

Um corolário imediato deste teorema é que grupos finitos nilpotentes são grupos de Engel. Porém, grupos de Engel não são necessariamente nilpotentes [5]. O próximo resultado, cuja demonstração pode ser encontrada em [13] (página 372), dá uma condição suficiente para que um grupo de Engel seja nilpotente.

Teorema 1.19 (Zorn) *Todo grupo de Engel finito é nilpotente.*

1.2 Alguns Grupos Importantes

Vamos introduzir nesta seção algumas notações e ressaltar alguns resultados a respeito de alguns grupos que desempenham papel de destaque no decorrer deste trabalho. Começaremos dando as definições de alguns grupos lineares, considerando que R é um anel comutativo com unidade.

Definição 1.20

1. $GL(n, R) = \{A \in M_n(R);\ \det A \neq 0\}$;
2. $SL(n, R) = \{A \in M_n(R);\ \det A = 1\}$;
3. $PGL(n, R) = \dfrac{GL(n, R)}{\mathcal{Z}(GL(n, R))}$;
4. $PSL(n, R) = \dfrac{SL(n, R)}{\mathcal{Z}(SL(n, R))}$.

Para os grupos acima definidos, vale que $\mathcal{Z}(GL(n, R)) = \{aI_n;\ a \in R\}$ e $\mathcal{Z}(SL(n, R)) = \{aI_n;\ a^n = 1\}$. Os grupos $1, 2, 3$ e 4 são chamados respectivamente de Grupo Linear Geral, Grupo Especial Linear, Grupo Projetivo Geral Linear e Grupo Projetivo Especial Linear.

Se R for um corpo finito com q elementos, denotamos os grupos em $1, 2, 3$ e 4 por $GL(n, q)$, $SL(n, q)$, $PGL(n, q)$, $PSL(n, q)$, respectivamente. Neste caso vale o seguinte:

Proposição 1.21

1. $|GL(n, q)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$;

2. $|SL(n,q)| = \frac{|GL(n,q)|}{q-1} = |PGL(n,q)|$;

3. $|PSL(n,q)| = \frac{|GL(n,q)|}{(q-1)d}$, *onde* $d = mdc\{n, q-1\}$.

Demonstração: Ver [13].

$\blacksquare$

Observamos que $|SL(2,5)| = 120 = 2^3 \cdot 3 \cdot 5$ e $SL(2,5)$ possui $5, 10$ e 6 p-subgrupos de Sylow, para $p = 2, 3$ e 5, respectivamente [8].

O próximo resultado descreve a estrutura dos subgrupos de Sylow do grupo $SL(2, p^n)$, para p primo.

Teorema 1.22 *Seja r um número primo. Um r-subgrupo de Sylow de $SL(2, p^m)$ é:*

1. *cíclico, se $r \neq 2$ e $r \neq p$.*

2. *o grupo dos quatérnios generalizados, se $r = 2$ e $r \neq p$.*

3. *abeliano elementar, se $r = p$.*

Demonstração: Ver [8], página 196.

$\blacksquare$

Vamos destacar algumas propriedades dos grupos alternados A_n. O Teorema de Jordan garante que A_n é simples, quando $n \neq 1, 2$ e 4 [13]. Nestes casos temos $\mathcal{Z}(A_n) = 1$, logo estes grupos são não-nilpotentes, de acordo com o Lema 1.10.

Observação 1.23 *No decorrer deste trabalho, usamos algumas propriedades do grupo alternado A_5. Afirmamos que A_5 é o único grupo simples de ordem 60 e valem as seguintes propriedades [8]:*

1. *A_5 possui um total de 21 p-subgrupos de Sylow distintos, para $p = 2, 3$ ou 5;*

2. *A_5 é coberto pelos seus 21 p-subgrupos de Sylow, ou seja, $A_5 = \bigcup_{i=1}^{21} P_i$.*

Sejam $x_1, \ldots, x_{21}$ elementos distintos da identidade pertencentes a $P_1, \ldots, P_{21}$, respectivamente. Cada p-subgrupo de Sylow P_i é abeliano e $P_i \cap P_j = 1$, se $i \neq j$. Então $C_{A_5}(x_i) = P_i$ e assim $\mathcal{Z}(\langle x_i, x_j \rangle) = P_i \cap P_j = 1$, para $i \neq j$. Então $\langle x_i, x_j \rangle$ não pode ser nilpotente, pois contradiria o Lema 1.10. Isto mostra que o conjunto $\{x_1, \ldots, x_{21}\}$ não possui nenhum subconjunto com dois elementos que gera um subgrupo nilpotente de A_5.

Vamos encerrar esta seção dando uma caracterização do grupo $PSL(2,5)$ como consequência do seguinte fato, cuja demonstração pode ser encontrada em [13], página 74.

Teorema 1.24 (Jordan-Dickson) *Se ou $n > 2$ ou $n = 2$ e $q > 2$, então $PSL(n,q)$ é simples.*

Por este teorema temos que $PSL(2,5)$ é um grupo simples e, de acordo com a Proposição 1.21, o grupo $PSL(2,5)$ tem ordem 60, no entanto o único grupo simples de ordem 60 é A_5. Portanto, $PSL(2,5) \cong A_5$.

1.3 O CR-Radical e o Radical Solúvel

Os conceitos e resultados desta seção serão utilizados nas demonstrações de alguns resultados do Capítulo 3.

Definição 1.25 *Um subgrupo normal H de um grupo G é dito um* subgrupo normal minimal *em G se, para todo $K \leq H$, temos $K \ntriangleleft G$.*

Se H for um subgrupo normal minimal de um grupo G, então H não pode ter subgrupos característicos. De fato, se K *car* H, dado $g \in G$ defina $\phi_g : H \to H$ por $h^{\phi_g} = h^g$. Então $\phi_g \in Aut(H)$ e como K é subgrupo característico de H, segue que $K^{\phi_g} \subseteq K$, ou seja, $g^{-1}kg \in K$, para todo $g \in G$ e todo $k \in K$, isto é, $K \lhd G$, o que contradiz a minimalidade de H.

Definição 1.26 *O* radical solúvel *de um grupo G, denotado por $Sol(G)$, é o maior subgrupo normal solúvel de G.*

Entendemos que S é o maior subgrupo normal de G se, caso N seja um subgrupo normal de G, então $N \subset S$.

Definição 1.27 *Um grupo G é dito* semi-simples *se não possui subgrupos normais abelianos não triviais.*

Observação 1.28 *Note que se G é um grupo e $S = Sol(G)$, então $\dfrac{G}{S}$ é semi-simples. De fato, seja $\bar{A} \lhd \dfrac{G}{S}$, com $\bar{A}$ abeliano. Pelo Teorema da Correspondência, existe um subgrupo abeliano $A \leq G$ tal que $S \leq A \lhd G$. Mas assim S é um subgrupo do subgrupo solúvel A. Pela maximalidade de S, segue que $A = S$.*

Definição 1.29 *O CR*-radical sem centro *de um grupo G é o produto de todos os subgrupos normais minimais não-abelianos de G, denotado por $CR(G)$. Caso o grupo G não possua subgrupos normais não-abelianos, consideramos $CR(G) = 1$.*

O próximo resultado mostra como é a estrutura do CR-radical de um grupo finito G.

Proposição 1.30 *O CR-radical sem centro de um grupo finito G é o produto direto de subgrupos simples normais não-abelianos.*

Demonstração: Seja $C = CR(G)$, então $C = \prod N$, onde N é subgrupo normal minimal não-abeliano de G. Vamos mostrar que cada N é um produto direto de subgrupos simples não-abelianos.

Suponha que N não é simples e dentre os subgrupos normais de N escolha um que seja minimal simples, que vamos chamar de K. Considere o subgrupo de N dado por $\left\langle K^{\theta}; \theta \in Aut(N) \right\rangle$. Por construção, este subgrupo é característico em N e é não trivial. Como N não possui subgrupos característicos não-triviais, este subgrupo deve ser o próprio N.

Devemos observar que $K^{\theta} \lhd N$, para qualquer $\theta \in Aut(N)$. Além disso, K^{θ} não possui subgrupos característicos, pela minimalidade de K. Queremos mostrar que N é o produto direto de alguns destes K^{θ}, isto é, devemos mostrar que existe um subconjunto $\Omega \subset Aut(N)$ tal que $N = \displaystyle\prod_{\theta_i \in \Omega} K^{\theta_i}$.

Consideremos S o conjunto de todos os subconjuntos de automorfismos α_i de N tais que $\langle K^{\alpha_i}; \{\alpha_i\} \in S\rangle = \prod_{\{\alpha_i\}\in S} K^{\alpha_i}$ (produto direto), isto é, $K^{\alpha} \cap \left\langle K^{\beta}; \beta \neq \alpha \right\rangle = 1$, para todo $\alpha \in S$. Observamos que $S \neq \emptyset$, pois um conjunto com um único automorfismo $\{\alpha\}$ está em S. Além disso, S é parcialmente ordenado por inclusão.

Se $\{S_i\}_{i\in I}$ é uma *cadeia* em S, isto é, I é um conjunto de índices e

$$S_{i_0} \subset S_{i_1} \subset \dots, \text{ onde } S_{i_j} \in S \text{ e } i_j \in I,$$

então $\bigcup_{i\in I} S_i \in S$. Pelo Lema de Zorn, S tem um elemento maximal M (subconjunto de $Aut(N)$). Considere $L = \langle K^{\mu}; \mu \in M\rangle$ e note que este é um produto direto, desde que $M \in S$.

Se $\lambda \in Aut(N)\backslash M$ então $M \cup \{\lambda\} \notin S$, pela maximalidade de M. Assim, $K^{\lambda} \cap L \neq 1$.

Tomando $x \in K^{\lambda} \cap L$ e $\phi \in Aut(K^{\lambda})$, temos que $x^{\phi} \in K^{\lambda} \cap L$, o que implica que $K^{\lambda} \cap L$ é um subgrupo característico de K^{λ}. Com isso, $K^{\lambda} \cap L = K^{\lambda}$ e assim $K^{\lambda} \subseteq L \subseteq N$. Mas lembre que $N = \left\langle K^{\theta}; \theta \in Aut(N) \right\rangle$. Deste modo, os demais elementos de N estão em L, ou seja, $L = N$ e N é um produto direto, como queríamos.

■

1.4 Grupos Satisfazendo $(\mathcal{X}, n)$

A principal definição neste trabalho é a seguinte:

Definição 1.31 *Dado um inteiro $n > 0$ e uma classe de grupos $\mathcal{X}$, dizemos que G satisfaz $(\mathcal{X}, n)$ se, em qualquer subconjunto com $n+1$ elementos de G, for possível escolher dois elementos x e y tais que o subgrupo $\langle x, y\rangle$ pertence a $\mathcal{X}$.*

Note que se G satisfaz $(\mathcal{X}, n)$ e H é um subgrupo de G tal que $|H| \geq n+1$, então H satisfaz $(\mathcal{X}, n)$.

Observação 1.32 *Seja G um grupo e suponha que*

$$G = \bigcup_{i=1}^{n} H_i,$$

onde $H_i \in \mathcal{X}$. Note que em qualquer subconjunto com $n+1$ elementos de G, existem dois elementos que pertencem a um mesmo grupo H_k, $1 \leq k \leq n$, portanto G satisfaz $(\mathcal{X}, n)$. Ou seja, se um grupo G é coberto por n grupos que pertencem a uma classe $\mathcal{X}$, então G satisfaz $(\mathcal{X}, n)$.

Exemplo 1.33 *De acordo com a Observação 1.23, temos que $A_5 = \bigcup_{i=1}^{21} P_i$, onde P_i são os subgrupos de Sylow de A_5. Como cada P_i é um p-grupo finito segue da Proposição 1.13 que A_5 é coberto por 21 grupos nilpotentes, portanto A_5 satisfaz a condição $(\mathcal{N}, 21)$.*

Exemplo 1.34 *O grupo A_4 é coberto por seus 5 subgrupos de Sylow [4], portanto A_4 satisfaz a condição $(\mathcal{N}, 5)$.*

Seja G um grupo que satisfaz a condição $(\mathcal{X}, n)$, onde $\mathcal{X}$ é fechada para formação de subgrupos e quocientes. Seja $N \lhd G$ e considere o subconjunto

$$\{x_1N, \ldots, x_{n+1}N\}$$

de $\frac{G}{N}$. Assim, para $i, j \in \{1, \ldots, n+1\}$, com $i \neq j$, vale que $\langle x_iN, x_jN \rangle = \langle x_i, x_j \rangle N$ pertence a classe $\mathcal{X}$, pois $\langle x_i, x_j \rangle \in \mathcal{X}$. Portanto, $\frac{G}{N}$ satisfaz a condição $(\mathcal{X}, n)$.

Nos próximos capítulos vamos estudar algumas condições que devem cumprir certos grupos de modo que satisfaçam as condições $(\mathcal{A}, n)$ e $(\mathcal{N}, n)$.

Capítulo 2

Grupos Satisfazendo $(\mathcal{A}, n)$

Vamos estudar neste capítulo grupos (não necessariamente finitos) que satisfazem a condição $(\mathcal{A}, n)$.

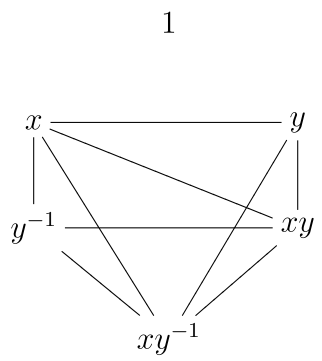
O objetivo deste capítulo é mostrar que um grupo G satisfaz a condição $(\mathcal{A}, n)$, para um inteiro não-negativo n apropriado se, e somente se, $G \in \mathcal{CPF}$. Para chegar a este objetivo vamos precisar inicialmente de alguns resultados sobre grafos de grupos, apresentados a seguir.

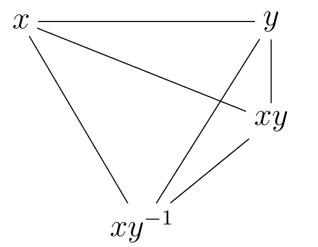
2.1 Grafos e PE-Grupos

Seja G um grupo e $\Gamma(G)$ um grafo associado a G, cujos vértices são elementos de G e para o qual dois vértices $g, h \in G$ estão conectados por uma aresta se h e g não comutam, isto é, $[h, g] \neq 1$. Definimos a *ordem de um grafo* como o número de elementos em seu conjunto de vértices, caso este seja finito.

Definição 2.1 *Se um subgrafo de* $\Gamma(G)$ *possui todos os vértices conectados, dizemos que este é um* subgrafo completo*.*

Note, por exemplo, que o grafo $\Gamma(G)$ de um grupo abeliano G não contém arestas, portanto não contém subgrafos completos. Por outro lado, seja $S_3 = \langle x, y; x^2 = 1, y^3 = 1, xy = y^{-1}x \rangle$. Então o subgrafo com vértices x, y, xy e xy^{-1} é completo, pois estes elementos não comutam entre si.





O grafo de S_3 Um subgrafo completo de S_3

Vamos introduzir agora alguns conceitos e demonstrar alguns resultados importantes. Começamos introduzindo a classe dos PE-grupos, que foram utilizados para responder a seguinte pergunta, formulada por *Paul Erdös* em 1975 [11]:

Se G é um grupo para o qual $\Gamma(G)$ não contém subgrafos infinitos completos, então existe um limite finito para a ordem dos subgrafos completos de $\Gamma(G)$?

Definição 2.2 *Um grupo G para qual o seu grafo associado $\Gamma(G)$ não contém subgrafos infinitos completos é chamado de PE-grupo. Denotamos a classe dos PE-grupos por $\mathcal{PE}$.*

Vejamos como relacionar os PE-grupos com o problema a respeito da condição $(\mathcal{A}, n)$.

Lema 2.3 *Se um grupo G satisfaz $(\mathcal{A}, n)$, então G é um PE-grupo.*

Demonstração: Basta observar que em qualquer subconjunto de G com $n + 1$ elementos existem dois deles que comutam, portanto não estão conectados. Com isso, é impossível formar subgrafos infinitos em que todos os vértices estejam conectados, isto é, é impossível formar subgrafos infinitos completos.

$\blacksquare$

Queremos saber quais grupos satisfazem a condição $(\mathcal{A}, n)$, para algum n.

O próximo resultado é bem conhecido da Teoria dos Grafos e será aplicado na próxima seção, mas antes de enunciá-lo, devemos introduzir alguma terminologia.

Uma *coloração* dos elementos de um conjunto X com c cores é uma partição de X em c classes, chamadas de *cores*. Em particular, consideramos $[X]^k$ o conjunto de todos os k-subconjuntos de X, ou seja, subconjuntos com k elementos. Dada uma c-coloração de $[X]^k$, dizemos que $Y \subset X$ é *monocromático* se todos os elementos de $[Y]^k$ tem a mesma cor, isto é, pertencem a uma mesma classe de uma c-partição de $[X]^k$.

Por exemplo, seja

$$X = \{1, 2, 3, 4\}.$$

Se $k = 2$, consideremos os 2-subconjuntos de X:

$$A_1 = \{1, 2\}, A_2 = \{1, 3\}, A_3 = \{1, 4\}, A_4 = \{2, 3\}, A_5 = \{2, 4\}, A_6 = \{3, 4\}.$$

Então $[X]^2 = \{A_1, A_2, \ldots, A_6\}$. Consideremos uma 2-coloração de $[X]^2$:

$$\{A_1, A_3, A_5\} \cup \{A_2, A_4, A_6\}.$$

Deste modo, temos que $Y = \{1, 2, 4\} \subset X$ é monocromático, pois

$$[Y]^2 = \{\{1, 2\}, \{1, 4\}, \{2, 4\}\},$$

mas $Z = \{1, 2, 3\}$ não é monocromático.

Seguindo a terminologia acima, o Teorema de Ramsey [2] pode ser enunciado da seguinte maneira:

Teorema 2.4 *Para todo inteiro positivo r, existe um inteiro positivo n tal que dado qualquer n-conjunto X, toda 2-coloração de $[X]^2$ produz um r-subconjunto $Y \subset X$ monocromático. Mais que isto, esta afirmação permanece verdadeira para uma c-coloração de $[X]^k$, com c e k arbitrários.*

Agora, a versão *infinita* para este resultado.

Teorema 2.5 (Ramsey) *Sejam c, k inteiros positivos e X um conjunto infinito. Se $[X]^k$ é colorido com c cores, então X tem um subconjunto infinito monocromático.*

Demonstração: A demonstração é feita por indução sobre k, com c fixo. Se $k = 1$ então X, por ser infinito e colorido com c cores, possui uma cor com infinitos elementos.

Vamos supor que a afirmação o teorema é verdadeira para valores menores que k, onde $k > 1$. Seja $[X]^k$ colorido com c cores. Vamos construir uma sequência infinita $X_0, X_1, \ldots$ de subconjuntos infinitos de X e escolher elementos $x_i \in X_i$, em que para todo i, valem as seguintes propriedades:

1. $X_{i+1} \subset X_i \backslash \{x_i\}$;

2. todos os k-subconjuntos $\{x_i\} \cup Z$, onde $Z \in [X_{i+1}]^{k-1}$, têm a mesma cor, que associamos a x_i.

Começando com $X_0 = X$, seja $x_0 \in X_0$ um elemento arbitrário. Assim X_0 é infinito e, escolhendo um subconjunto infinito X_i e $x_i \in X_i$, para algum i, façamos uma c-coloração de $[X \backslash \{x_i\}]^{k-1}$, dando a cada conjunto Z a cor de $\{x_i\} \cup Z$, da c-coloração de $[X]^k$.

Pela hipótese de indução, $X_i \backslash \{x_i\}$ tem um subconjunto infinito monocromático, que escolhemos para ser X_{i+1}. Observe que esta escolha satisfaz (1) e (2).

Tomamos então $x_{i+1} \in X_{i+1}$ arbitrário e repetimos o processo. Como c é finito, uma das c cores está associada a infinitos destes elementos x_i, que formam um subconjunto monocromático de X.

■

O Teorema de Ramsey pode ser aplicado ao considerarmos X um grafo infinito $\Gamma(G)$ associado a um grupo infinito G de modo que, para qualquer 2-coloração de $[\Gamma(G)]^2$, $\Gamma(G)$ contém um subgrafo infinito monocromático. Mais sobre a Teoria Ramsey para grafos pode ser encontrado em [2].

2.2 FC-Grupos e CPF-Grupos

Vamos agora introduzir a classe dos FC-grupos. Em seguida apresentamos alguns resultados sobre a classe dos CPF-grupos, que foi apresentada no Capítulo 1.

Definição 2.6 *Dizemos que G é um FC-grupo se todos os elementos de G tem um número finito de conjugados. Escrevemos $G \in \mathcal{FC}$.*

Assim, $G \in \mathcal{FC}$ se, para qualquer $x \in G$, tem-se que sua classe de conjugação $cl(x) = \{x^g; g \in G\}$ é um conjunto finito.

Lembramos que o tamanho da classe de conjugação de um elemento $x \in G$ coincide com o índice $[G : C_G(x)]$ do centralizador de x em G. Observamos ainda que $\mathcal{Z}(G) = \bigcap_{x \in G} C_G(x)$, segue que se G for central-por-finito então $[G : C_G(x)] < \infty$, para todo $x \in G$. Isto mostra que $\mathcal{CPF} \subset \mathcal{FC}$.

Também é verdade que se $G \in \mathcal{FC}$ e é finitamente gerado, então $G \in \mathcal{CPF}$. Realmente, se $G = \langle x_1, \ldots, x_n \rangle$, então, pela Proposição 1.2, segue $[G : \mathcal{Z}(G)] \leq [G : C_G(x_1)] \cdots [G : C_G(x_n)] < \infty$. Note que se $G \notin \mathcal{FC}$, então G é um grupo infinito.

Lema 2.7 *Se G é um PE-grupo, então G é um FC-grupo.*

Demonstração: Suponha que G não é um FC-grupo, ou seja, G contém um elemento g que tem uma classe de conjugação infinita. Vamos mostrar que $G \notin \mathcal{PE}$.

Seja $T \subset G$ um subconjunto infinito com a seguinte característica: se tomarmos em T dois elementos distintos, eles formam conjugados distintos de $g \in G$, ou seja, se $t_1, t_2 \in T$ e $t_1 \neq t_2$ então $g^{t_1} \neq g^{t_2}$.

Considere a restrição $\Gamma(T)$ do grafo $\Gamma(G)$ a T. Considerando a 2-coloração de $[\,\Gamma(T)]^2$ dada por $C(T) \cup N(T)$, onde $C(T)$ é formado pelos 2-subconjuntos de elementos conectados e $N(T)$ por aqueles que não estão conectados, então, pelo Teorema 2.5, duas situações podem acontecer: ou $\Gamma(T)$ contém um subgrafo infinito completo (e isto terminaria a demonstração, pois deste modo $G \notin \mathcal{PE}$) ou $\Gamma(T)$ contém um subgrafo infinito independente U, isto é, um conjunto infinito de vértices sem qualquer aresta.

Ocorrendo a segunda situação, temos que os elementos de $U \subset G$ comutam uns com os outros, pois não estão ligados por arestas. Considere o conjunto $gU = \{gu; u \in U\}$. Se $u, v \in U$ são elementos distintos, então

$$\begin{aligned}
[gu, gv] &= (gu)^{-1}(gv)^{-1}gugv \\
&= u^{-1}g^{-1}v^{-1}g^{-1}gugv \\
&= u^{-1}g^{-1}v^{-1}ugv \\
&= u^{-1}g^{-1}uv^{-1}gv
\end{aligned}$$

$$= \quad (g^u)^{-1}g^v \neq 1, \text{ pois } g^u \neq g^v \text{ já que } u, v \in U \subset T.$$

Assim, quaisquer dois elementos distintos em gU não comutam e, portanto, $\Gamma(gU)$ é um subgrafo infinito completo de $\Gamma(G)$. Deste modo, $G \notin \mathcal{PE}$, completando a demonstração.

■

Lema 2.8 *Seja $G \in \mathcal{FC}$ e suponha que G contém um subgrupo abeliano A de índice finito. Então $G \in \mathcal{CPF}$.*

Demonstração:

O grupo G pode ser gerado a partir de um subconjunto Q dos geradores de A e de um conjunto finito R formado pelos representantes das classes laterais de A em G. Se $S = Q \cup R$, então

$$\mathcal{Z}(G) = C_G(S) = C_G(Q) \cap C_G(R).$$

Como $Q \subseteq A$ e A é abeliano, segue que $A \subseteq C_G(Q)$. Por hipótese, A tem índice finito, o que implica que $[G : C_G(Q)]$ é finito. Como $G \in \mathcal{FC}$, então, para cada $r \in R$, $C_G(r)$ tem índice finito. Agora, observamos que $C_G(R) = \bigcap_{r \in R} C_G(r)$ e como R é finito, pela Proposição 1.2 concluímos que $[G : C_G(R)]$ também é finito. Logo $[G : \mathcal{Z}(G)]$ é finito, isto é, $G \in \mathcal{CPF}$.

■

É claro que se $G \in \mathcal{CPF}$, então $\mathcal{Z}(G)$ é um subgrupo abeliano de G índice finito.

Corolário 2.9 *Se $G \in \mathcal{FC} \backslash \mathcal{CPF}$ e G contém um subgrupo de índice finito A, então A não é abeliano.*

Demonstração: Se A fosse abeliano, pelo teorema anterior teríamos que $G \in \mathcal{CPF}$, o que contradiz a hipótese do corolário.

■

2.3 CPF-Grupos e a Condição $(\mathcal{A}, n)$

Inicialmente observamos que se G é um grupo tal que $[G : \mathcal{Z}(G)] = n$, então G satisfaz $(\mathcal{A}, n)$. De fato, seja $Z = \mathcal{Z}(G)$ e suponha que $[G : Z] = n$ e seja X um subconjunto de G com $n + 1$ elementos, assim existem elementos distintos $g, h \in X$ tais que $Zg = Zh$. Isto implica que $gh^{-1} \in Z$, isto é, existe $z \in Z$ tal que $g = zh$. Assim,

$$gh = zhh = hzh = hg.$$

Portanto g e h comutam, mostrando que G satisfaz $(\mathcal{A}, n)$.

Vimos até agora que PE-grupos e CPF-grupos são FC-grupos. No entanto, se $G \in \mathcal{FC} \backslash \mathcal{CPF}$, então $G \notin \mathcal{PE}$, como mostraremos mais adiante. Para isto, precisaremos do seguinte resultado:

Lema 2.10 *Seja $G \in \mathcal{FC} \backslash \mathcal{CPF}$. Assuma que G contém duas sequências finitas de n elementos*

$$(a_1, a_2 \ldots, a_n) \ \ e \ \ (b_1, b_2 \ldots, b_n)$$

tais que:

1. *se $i \neq j$ então $[a_i, a_j] \neq 1$;*

2. *se $i \neq j$ então $[a_i, b_j] = 1$;*

3. *$[a_i, b_i] \neq 1$, para todo i;*

4. *$[b_i, b_j] = 1$, para todo i, j.*

Então G contém dois elementos adicionais a_{n+1} e b_{n+1} tais que as propriedades acima continuam valendo para as sequências de comprimento $n + 1$

$$(a_1, a_2 \ldots, a_n, a_{n+1}) \ \ e \ \ (b_1, b_2 \ldots, b_n, b_{n+1}).$$

Demonstração: Faça

$$A = C_G(\{a_1, a_2, \ldots, a_n, b_1, \ldots, b_n\}) = \bigcap \left(C_G(a_i) \cap C_G(b_j)\right).$$

Como $G \in \mathcal{FC}$, temos que $[G : A] < \infty$. Mas como $G \notin \mathcal{CPF}$, pelo Corolário 2.9, A não é abeliano. Asim, podemos tomar dois elementos de A, digamos $a, b \in A$ tais que $[a, b] \neq 1$.

Colocamos $a_{n+1} = ab_1b_2 \cdots b_n$ e $b_{n+1} = b$. Então, para $i \in \{1, \ldots, n\}$, temos

1') $[a_i, a_{n+1}] = a_i^{-1}b_n^{-1} \ldots b_2^{-1}b_1^{-1}a^{-1}a_iab_1b_2 \ldots b_n = a_i^{-1}b_i^{-1}a_ib_i = [a_i, b_i] \neq 1$, pois a e todos os $b_j \neq b_i$ comutam com os a_i.

2') $[a_{n+1}, b_i] = b_n^{-1} \ldots b_2^{-1}b_1^{-1}a^{-1}b_i^{-1}ab_1b_2 \ldots b_nb_i = 1$, pois a e todos os b_j comutam com os b_i, e a_i comuta com b.

3') $[a_{n+1}, b_{n+1}] = b_n^{-1} \ldots b_2^{-1}b_1^{-1}a^{-1}b^{-1}ab_1b_2 \ldots b_nb = (b_1 \ldots b_n)^{-1}[a, b](b_1 \ldots b_n) = [a, b] \neq 1$, pois a e $b = b_{n+1}$ não comutam, mas b comuta com todos os b_i.

4') $[b_i, b_{n+1}] = 1$, pois $b_{n+1} = b$ comuta com todos os b_i.

■

Corolário 2.11 *Se $G \in \mathcal{FC} \backslash \mathcal{CPF}$ então $G \notin \mathcal{PE}$.*

Demonstração: A partir do Lema 2.10 construímos indutivamente uma sequência infinita $(a_1, a_2, \ldots)$ de elementos de G que não comutam dois a dois, começando de um par (a, b) de elementos em G que não comutam. Com isso, o grafo deste subconjunto de G é infinito e completo, isto é, G não é um PE-grupo.

■

Apresentamos agora o resultado deste capítulo.

Teorema 2.12 *Se o grupo G satisfaz $(\mathcal{A}, n)$ então $G \in \mathcal{CPF}$.*

Demonstração:

Suponha que G satisfaça $(\mathcal{A}, n)$, então pelo Lema 2.3 temos $G \in \mathcal{PE}$. Assim, pelo Lema 2.7 segue que $G \in \mathcal{FC}$. Se $G \notin \mathcal{CPF}$, pelo Corolário 2.11, teríamos que $G \notin \mathcal{PE}$, uma contradição.

Portanto, $G \in \mathcal{CPF}$.

■

No início desta seção comentamos que se um grupo G é central-por-finito, com $[G : \mathcal{Z}(G)] = n$, então o grupo satisfaz a condição $(\mathcal{A}, n)$. Assim, poderíamos enunciar o Teorema 2.12 da seguinte forma: $G \in \mathcal{PE}$ *se, e somente se* $G \in \mathcal{CPF}$ (basta observar a demonstração do Teorema 2.12, os Lemas 2.3 e 2.7 e o Corolário 2.11). Este resultado responde afirmativamente o problema de Paul Erdös, já que se o centro de G tem índice n então $\Gamma(G)$ não possui subgrafos completos de ordem maior que n.

É fácil ver também que poderíamos enunciar o Teorema 2.12 como:

$G \in \mathcal{CPF}$ *se, e somente se, existe um inteiro positivo* n *tal que* G *satisfaz* $(\mathcal{A}, n)$.

Em particular vale que todo grupo finito satisfaz a condição $(\mathcal{A}, n)$, para algum inteiro positivo n.

Deve ficar claro também que o inteiro n não precisa coincidir com o índice do centro do grupo, isto é, podemos ter um grupo $G \in \mathcal{CPF}$ que não satisfaz uma condição $(\mathcal{A}, n)$, dependendo do inteiro n escolhido. O próximo resultado dá um exemplo de um caso destes.

Lema 2.13 *O grupo* $SL(2,5)$ *não satisfaz a condição* $(\mathcal{A}, 21)$.

Demonstração: Suponha que $P_1, \ldots, P_5 \in Syl_2\left(SL(2,5)\right)$, $Q_1, \ldots, Q_{10} \in Syl_3\left(SL(2,5)\right)$ e $R_1, \ldots, R_6 \in Syl_5\left(SL(2,5)\right)$. Pelo Teorema 1.22, temos que P_i é isomorfo ao grupo dos quatérnios de ordem 8, para todo $i = 1, \ldots, 5$. Além disso, pela Proposição 1.21 temos $|\mathcal{Z}\left(SL(2,5)\right)| = 2 = |\mathcal{Z}\left(P_i\right)|$. Portanto $\mathcal{Z}\left(SL(2,5)\right) = \mathcal{Z}(P_i)$. Sejam

$$x_i \in P_i \backslash \mathcal{Z}(P_i), \text{ para } i = 1, \ldots, 5;$$

$$y_j \in Q_j \backslash \{1\}, \text{ para } j = 1, \ldots, 10;$$

$$z_k \in R_k \backslash \{1\}, \text{ para } k = 1, \ldots, 6.$$

Afirmamos que quaisquer dois elementos distintos no subconjunto de $SL(2,5)$ com 21 elementos

$$\{x_1,\ldots,x_5,y_1,\ldots,y_{10},z_1,\ldots,z_6\}$$

não comutam. De fato, observando que $\dfrac{SL(2,5)}{\mathcal{Z}(SL(2,5))} = \dfrac{SL(2,5)}{\mathcal{Z}\left(P_i\right)} \cong A_5$, suponha que a afirmação é falsa, isto é, suponha que existam dois elementos distintos no conjunto acima que comutam. Então existiriam dois elementos no conjunto

$$\{x_1\mathcal{Z}\left(P_i\right),\ldots,x_5\mathcal{Z}\left(P_i\right),y_1\mathcal{Z}\left(P_i\right),\ldots,y_{10}\mathcal{Z}\left(P_i\right),z_1\mathcal{Z}\left(P_i\right),\ldots,z_6\mathcal{Z}\left(P_i\right)\}$$

que comutariam. Mas este é um subconjunto de $\dfrac{SL(2,5)}{\mathcal{Z}\left(P_i\right)}$, que como acabamos de ver é isomorfo a A_5, e que possui dois elementos que geram um grupo nilpotente, contrariando a Observação 1.23 (isto já garante que $SL(2,5)$ não satisfaz $(\mathcal{A},20)$). Portanto, a afirmação é verdadeira.

Como P_1 é isomorfo a um grupo dos quatérnios de ordem 8 e $x_1 \in P_1 \backslash \mathcal{Z}\left(P_1\right)$, então existe um elemento $x \in P_1 \backslash \mathcal{Z}(P_1)$ tal que $x_1x \neq xx_1$. Pelo mesmo motivo acima, quaisquer dois elementos distintos em

$$\{x,x_2,\ldots,x_5,y_1,\ldots,y_{10},z_1,\ldots,z_6\}$$

não comutam. Assim, quaisquer dois elementos distintos no subconjunto de $SL(2,5)$ com 22 elementos

$$\{x,x_1,\ldots,x_5,y_1,\ldots,y_{10},z_1,\ldots,z_6\}$$

também não comutam, o que garante que $SL(2,5)$ não satisfaz $(\mathcal{A},21)$.

■

Mesmo sendo $SL(2,5)$ um grupo central-por-finito, ele não satisfaz a condição $(\mathcal{A},21)$. Mas, como observado no início desta seção, $SL(2,5)$ satisfaz $(\mathcal{A},60)$, pois $\mathcal{Z}(SL(2,5))$ tem índice 60.

É importante observar também que se um grupo satisfaz a condição $(\mathcal{A},n)$ não implica que $[G:\mathcal{Z}(G)] = n$. Por exemplo, seja $Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$ o grupo dos quatérnios de ordem 8. Temos $Q_8 = \langle i\rangle \cup \langle j\rangle \cup \langle k\rangle$, assim Q_8 é coberto por três grupos abelianos e, pela Observação 1.32, segue que o grupo Q_8 satisfaz a condição $(\mathcal{A}, 3)$, no entanto não é verdade que $[Q_8 : \mathcal{Z}(Q_8)] = 3$. Vale a pena observar que Q_8 não satisfaz a condição $(\mathcal{A}, 2)$, pois se escolhermos quaisquer pares de elementos dois a dois distintos no subconjunto $\{i, j, k\} \subset Q_8$, o subgrupo gerado por estes é o próprio Q_8, que não é abeliano.

Antes de encerrar este capítulo, vamos mostrar que o comprimento derivado de um grupo solúvel que satisfaz $(\mathcal{A}, n)$ é no máximo igual a uma função que depende apenas do valor de n. Precisamos antes do seguinte resultado.

Lema 2.14 *Seja G um grupo que satisfaz a condição $(\mathcal{A}, n)$ $(n > 1)$ e seja N um subgrupo normal não-abeliano de G. Então o grupo quociente $\dfrac{G}{N}$ satisfaz a condição $(\mathcal{A}, n-1)$.*

Demonstração: Suponha, por contradição, que $\dfrac{G}{N}$ não satisfaz $(\mathcal{A}, n-1)$, isto é, dentre os elementos do subconjunto

$$\{x_1N, \ldots, x_nN\}$$

de $\dfrac{G}{N}$, vale $[x_iN, x_jN] \neq N$, para índices distintos $i, j \in \{1, \ldots, 21\}$. Portanto $[x_i, x_j] \notin N$, para todos $i \neq j$.

Sejam a, b dois elementos distintos em N e considere o subconjunto

$$X = \{ax_1, \ldots, ax_n, bx_1\}$$

com $n+1$ elementos de G. Por hipótese, existem dois elementos distintos em X que comutam. Suponha que $ax_iax_j = ax_jax_i$, onde $i, j \in \{1, \ldots, n\}$ e $i \neq j$. Então $x_iax_j = x_jax_i$, com isso temos

$$x_iax_j = x_jax_i \Rightarrow x_iax_i^{-1}x_ix_j = x_jax_j^{-1}x_jx_i.$$

Como $a \in N$ e N é normal em G, segue que $x_iax_i^{-1} = n_1$ e $x_jax_j^{-1} = n_2$, onde $n_1, n_2 \in N$. Portanto

$$n_1x_ix_j = n_2x_jx_i \Rightarrow x_i^{-1}x_j^{-1}x_ix_j = n_2^{-1}n_1 \Rightarrow [x_i, x_j] \in N,$$

absurdo. Por isto podemos assumir que o único par de elementos distintos em X que comuta é ax_1, bx_1. Portanto, para todo $a, b \in N$, temos que $ax_1bx_1 = bx_1ax_1$, o que implica que $ax_1b = bx_1a$. Em particular, se $b = 1$ então $ax_1 = x_1a$, para todo $a \in N$. Analogamente, se $a = 1$ então $bx_1 = x_1b$, para todo $b \in N$. Com isso, temos

$$bax_1 = bx_1a = ax_1b = abx_1,$$

portanto, $ba = ab$, para todos $a, b \in N$, assim N é abeliano, uma contradição.

■

Teorema 2.15 *Seja G um grupo solúvel que satisfaz $(\mathcal{A}, n)$ e seja d o comprimento derivado de G. Se $n \in \{1, 2\}$, então $d = 1$. Se $n \geq 2$, então $d \leq 2n - 3$.*

Demonstração: é claro que se $n = 1$ então G é abeliano e assim $d = 1$. Suponha $n = 2$ e $x, y \in G$. Considerando o subconjunto de G com 3 elementos $\{x, y, xy\}$, então dois destes elementos devem comutar. Se x comuta com y implica que G é abeliano. Se x e xy comutam então temos

$$xxy = xyx \Rightarrow xy = yx.$$

Se y e xy comutam, temos

$$yxy = xyy \Rightarrow yx = xy.$$

Em todo caso temos que G é abeliano, portanto $d = 1$.

Vamos considerar $n \geq 2$ e mostrar a afirmação por indução sobre n. Vimos que a afirmação vale para $n = 2$, vamos considerar, portanto, que $n > 2$. Observe que neste caso $2 < 2n - 3$, com isso devemos assumir que $d > 2$. Então $G^{(d-2)} \neq 1$, portanto, $G^{(d-2)}$ não é abeliano, segue do Lema 2.14 que $\dfrac{G}{G^{(d-2)}}$ satisfaz a condição $(\mathcal{A}, n-1)$. Suponha, por indução, que a afirmação do teorema vale para $n - 1$, então o comprimento derivado de $\dfrac{G}{G^{(d-2)}}$ é no máximo $2(n-1) - 3$, portanto, $d - 2 \leq 2(n-1) - 3$, o que implica $d \leq 2n - 3$.

■

É fácil ver que se um grupo satisfaz a condição $(\mathcal{A}, n)$, então ele satisfaz a condição $(\mathcal{N}, n)$. Contudo a recíproca desta afirmação não é verdadeira, como veremos no próximo capítulo, onde estudaremos grupos que satisfazem $(\mathcal{N}, n)$.

Capítulo 3

Grupos Satisfazendo $(\mathcal{N}, n)$

Vimos no primeiro capítulo que todo grupo nilpotente é solúvel. Portanto, se um grupo G é não-solúvel, então ele não é nilpotente. Neste capítulo estudaremos grupos que satisfazem a condição $(\mathcal{N}, n)$ e o principal resultado dá uma caracterização de tais grupos finitos não-solúveis quando $n = 21$.

Recordamos que, para um primo p e um grupo finito G, dizemos que $a \in G$ é um *p-elemento* se $p \mid o(a)$. Dizemos que $a \in G$ é um *p'-elemento* se $p \nmid o(a)$. Analogamente, um subgrupo $H \leq G$ é dito um *p'-subgrupo* se $p \nmid |H|$.

Definição 3.1 *Um grupo finito G é dito p-*nilpotente*, para um número primo p se, dado Q o maior p'-subgrupo normal de G, tem-se que $\frac{G}{Q}$ é um p-grupo.*

Por exemplo, S_3 é 2-nilpotente, pois A_3 é o maior $2'$-subgrupo normal de S_3 e $\left|\frac{S_3}{A_3}\right| = 2$. No entanto, S_3 não é 3-nilpotente.

Proposição 3.2 *Seja G um grupo finito. Se G é nilpotente, então G é p-nilpotente, para todo primo p.*

Demonstração: Suponha que G é nilpotente, assim pelo Teorema 1.14 vale que $G = P_1 \times \cdots \times P_k$, onde $P_i \in Syl_{p_i}(G)$, para os números primos p_i, $i = 1, \ldots, k$. Seja p um primo que divide $|G|$. Digamos que $p = p_1$. Seja Q o maior subgrupo normal de G tal que p não divide $|Q|$. Assim, $\prod_{i=2}^{k} P_i \subset Q$. Com isso, $\left|\frac{G}{Q}\right| = p^{\alpha}$, para algum α. Portanto, G é p-nilpotente.

Se p não divide $|G|$, então o maior p'-subgrupo normal de G é o próprio G. Assim $\left|\frac{G}{Q}\right| = 1 = p^0$, com isso $\frac{G}{Q}$ é um p-grupo, portanto, G também é p-nilpotente neste caso. Logo G é p-nilpotente, para todo primo p.

$\blacksquare$

3.1 Grupos Satisfazendo $(\mathcal{N}, n)$, $n < 21$

O objetivo deste capítulo é responder a seguinte pergunta: *Quais são os grupos finitos não-solúveis que satisfazem a condição $(\mathcal{N}, n)$?* Nesta seção vemos o que acontece com um grupo que satisfaz $(\mathcal{N}, n)$, quando $n < 21$.

Definição 3.3 *Seja G um grupo finito. Dizemos que G é* quase p-nilpotente *se G não é p-nilpotente, mas todos os seus subgrupos próprios são p-nilpotentes.*

O primeiro resultado desta seção é o seguinte lema. A demonstração pode ser encontrada em [8], página 434.

Lema 3.4 *Sejam p um número primo e G um grupo finito quase p-nilpotente. Então:*

1. *G possui um único p-subgrupo de Sylow P.*
2. *$\frac{G}{P}$ é de ordem potência de um número primo $q \neq p$.*
3. *Os q-subgrupos de Sylow de G são cíclicos.*

Observação 3.5 *Note que nas condições do lema anterior se $Q \in Syl_q(G)$, então $G = PQ$, já que $\frac{G}{P}$ é q-grupo.*

Dado um inteiro positivo n, denotaremos por π_n o conjunto dos números primos p tais que $p < n$. Um elemento em g um grupo G é dito um π_n-*elemento* se os divisores primos de $o(g)$ pertencem ao conjunto π_n. Se nenhum divisor primo de $o(g)$ pertence a π_n, dizemos que g é um π_n'-*elemento*. Se todos elementos em um grupo G são π-elementos, dizemos que G é um π_n-*grupo*.

No caso que um grupo finito G que satisfaz $(\mathcal{N}, n)$, os conjuntos dos π_n-elementos e dos π'_n-elementos são subgrupos de G. Para demonstrar este fato, precisamos dos lemas a seguir.

Lema 3.6 *Seja n um inteiro positivo. Se G é um grupo finito tal que G é p-nilpotente, para todo $p \geq n$, então o conjunto dos π_n-elementos de G é um subgrupo de G.*

Demonstração: Seja A o conjunto dos π_n-elementos de G. Afirmamos que se $a, b \in A$ então $ab \in A$. De fato, suponha que $a, b \in A$ mas $ab \notin A$, isto é, existe um primo $p \geq n$ tal que $p \mid o(ab)$. Seja Q o maior p'-subgrupo normal de G. Como G é p-nilpotente, então $\dfrac{G}{Q}$ é p-grupo. Se $H = \langle a \rangle$, então p não divide $|H|$ e $p \mid [QH : Q] = [H : H \cap Q]$. No entanto, como $[H : H \cap Q] \mid |H|$, então p deveria dividir $|H|$, o que é uma contradição. Portanto, $ab \in A$ e isto mostra que A é subgrupo de G.

■

Lema 3.7 *Seja G um grupo finito que satisfaz $(\mathcal{N}, n)$, para $n > 0$. Se $\mathcal{Z}(G) = 1$, então G é um π_n-grupo.*

Demonstração: Dado um primo p tal que $p \mid |G|$, seja $P \in Syl_p(G)$. Considere H o subgrupo de G gerado por todos os p'-elementos de G. Então $G = PH$. Se $[P, H] = 1$, então $\mathcal{Z}(P) \leq \mathcal{Z}(G) = 1$, o que é um absurdo, pois P é p-grupo e por isso $\mathcal{Z}(P) \neq 1$. Portanto, existem um elemento $a \in P$ e um elemento $b \in H$ tais que $[a, b] \neq 1$. Considere o conjunto com $p + 1$ elementos

$$\left\{a, b, ab, a^2b, \ldots, a^{p-1}b\right\}.$$

Como a é um p-elemento e b é um p'-elemento, segue que $\langle a \rangle \cap \langle b \rangle = 1$. Portanto, se $\langle a, b \rangle$ fosse nilpotente, como $\langle a \rangle \in Syl_p(\langle a, b \rangle)$, teríamos $\langle a \rangle \lhd \langle a, b \rangle$ e, analogamente, $\langle b \rangle \lhd \langle a, b \rangle$. Então $[a, b] = 1$, absurdo. Como $\langle a^i b, a^j b \rangle = \langle a, b \rangle$, segue que nenhum par de elementos do conjunto acima gera um subgrupo nilpotente de G. Mas G satisfaz $(\mathcal{N}, n)$, logo devemos ter $p + 1 < n + 1$, ou seja, $p < n$.

■

Proposição 3.8 *Seja G é um grupo finito que satisfaz $(\mathcal{N}, n)$. Sejam A o conjunto dos π_n-elementos de G e B o conjunto dos π'_n-elementos de G. Então*

1. *A é um subgrupo (próprio) de G.*

2. *B é um subgrupo nilpotente (próprio) de G.*

Em particular, $G = A \times B$.

Demonstração:

Pelo Lema 3.6, basta mostrar que G é p-nilpotente, para todo primo $p \geq n$.

Sejam p um número primo e G um grupo finito de menor ordem que satisfaz $(\mathcal{N}, n)$ e que não é p-nilpotente. Desta forma, todos os subgrupos próprios de G são p-nilpotentes, ou seja, G é quase p-nilpotente.

Pelo Lema 3.4, G possui um único p-subgrupo de Sylow P, tal que $\left|\dfrac{G}{P}\right|$ é uma potência de um primo $q \neq p$. Além disso, os q-subgrupos de Sylow $Q_1, \ldots, Q_k$ de G são cíclicos.

Afirmamos que $k > 1$. De fato, suponha que Q é o único q-subgrupo de Sylow de G. De acordo com a Observação 3.5 temos que G é o produto direto de P e Q, o que implica que G é nilpotente, um absurdo. Assim, $k > 1$ e, pelo Teorema de Sylow, $k \mid p^{\alpha}$, portanto, $k \geq p \geq n$.

Sejam $x_1, \ldots, x_n$ os geradores dos n subgupos de Sylow $Q_1, \ldots, Q_n$, respectivamente, e seja x_{n+1} um elemento de $\mathcal{Z}(P) \backslash \{1\}$. Como G satisfaz $(\mathcal{N}, n)$, então devem existir inteiros distintos i, j tais que $\langle x_i, x_j \rangle$ é nilpotente. Suponha que $j < n + 1$. Como x_i, x_j são geradores de Q_i e Q_j, respectivamente, segue que Q_i e Q_j seriam dois q-subgrupos de Sylow distintos de $\langle x_i, x_j \rangle$. Mas $\langle x_i, x_j \rangle$ é nilpotente, por isso tem um único q-subgrupo de Sylow. Portanto devemos ter $j = n + 1$.

Consideramos, a partir de agora, o grupo $\langle x_i, x_{n+1} \rangle$ de H. Como H é nilpotente, então $\langle x_i \rangle \in Syl_q(H)$ e $\langle x_{n+1} \rangle \in Syl_p(H)$, além de $\langle x_i \rangle \lhd H$ e $\langle x_{n+1} \rangle \lhd H$. Portanto H é o produto direto de $\langle x_i \rangle$ e $\langle x_{n+1} \rangle$ e desde que estes grupos têm ordens relativamente primas, vamos mostrar que os elementos x_i e x_{n+1} comutam entre si. De fato, temos

$$[x_i, x_{n+1}] = x_i^{-1} x_{n+1}^{-1} x_i x_{n+1} \in \langle x_{n+1} \rangle \cap \langle x_n \rangle = \{1\}.$$

Como $x_{n+1} \in \mathcal{Z}(P_i) \setminus \{1\}$ e, pela Observação 3.5, $G = PQ_i$, então $C_G(x_{n+1}) = G$, logo $\langle x_{n+1} \rangle \lhd G$.

O grupo quociente $\bar{G} = \dfrac{G}{< x_{n+1} >}$ é de ordem estritamente menor que a ordem de G e satisfaz $(\mathcal{N}, n)$, então, por hipótese, temos que $\bar{G}$ é p-nilpotente. Seja $\bar{K}$ o maior p'-subgrupo normal de $\bar{G}$, então $\bar{K}$ é um p-grupo, portanto $|G| = p^{\alpha} q^{\lambda}$. Então $\bar{K} \in Syl_q(\bar{G})$, que implica que $\bar{G}$ possui um único q-subgrupo de Sylow, pela normalidade de $\bar{K}$.

Mas $\bar{G}$ possui também um único p-subgrupo de Sylow $\bar{P}$, pois $\bar{P} = \dfrac{P}{\langle x_{n+1} \rangle} \in Syl_p\left(\bar{G}\right)$, onde P é o único p-subgrupo de Sylow de G. Resulta do Teorema 1.14 que $\bar{G}$ é nilpotente. Mas $\langle x_{n+1} \rangle$ está contido no centro de G, então, pelo Teorema 1.15, segue que G é nilpotente, o que é uma contradição. Isto mostra o item 1.

Para o item 2, suponha que G é um grupo finito que satisfaz $(\mathcal{N}, n)$. Temos, pelo Lema 3.7, que $\dfrac{G}{\mathcal{Z}^*(G)}$ é um π_n-grupo, portanto o conjunto B dos π_n'-elementos está contido no grupo nilpotente $\mathcal{Z}^*(G)$, portanto, $\langle a, b \rangle$ é nilpotente, onde $a, b \in B$. Suponha que $ab \notin B$, isto é, suponha que exista um número primo p tal que $p \mid o(ab)$. Pela Proposição 3.2, $\langle a, b \rangle$ é p-nilpotente e, por um raciocínio análogo ao feito na demonstração do Lema 3.6, concluímos que B é um subgrupo (nilpotente) de G

■

Note que se G é um grupo finito satisfazendo a condição $(\mathcal{N}, 3)$ então G é nilpotente e, portanto, solúvel. De fato, nas hipóteses da Proposição 3.8, temos $\pi_3 = \{2\}$ e com isso temos que o conjunto A dos π_3-elementos é um 2-grupo e, portanto, nilpotente. Pela Proposição 3.8 temos B é nilpotente e assim, segue do Lema 1.11, que G é nilpotente.

Observe também que se G satisfaz $(\mathcal{N}, 4)$ então G é solúvel. Neste caso, temos $\pi_4 = \{2, 3\}$ e assim $|A| = 2^{\alpha} 3^{\beta}$. Logo, pelo Teorema 1.8, A é solúvel. Assim $G = A \times B$ é solúvel. No entanto, G não é necessariamente nilpotente. Para isto, observe que o grupo $S_3 = \{1, x, y, y^{-1}, xy, xy^{-1}\}$ satisfaz $(\mathcal{N}, 4)$, pois um subconjunto com 5 elementos de S_3 ou contém 1 e, neste caso, o subgrupo gerado por 1 e por um outro elemento qualquer neste conjunto é cíclico, portanto nilpotente; ou não contém o 1, e assim temos que y e y^2 pertencem a este conjunto, e com isso $\langle y, y^2 \rangle = \langle y \rangle$, que novamente é cíclico, logo nilpotente. Porém, S_3 não é nilpotente, como visto no Capítulo 1.

Na verdade, vale o seguinte resultado:

Proposição 3.9 *Todo grupo finito que satisfaz a condição* $(\mathcal{N}, n)$*, para* $n \leq 20$*, é solúvel.*

A demonstração desta proposição é feita supondo que o grupo G é não-solúvel de ordem minimal, portanto um grupo simples minimal. A partir da classificação de todos os grupos com esta característica, dada em [15], pode ser mostrado que nenhum destes grupos satisfaz a condição $(\mathcal{N}, 20)$. Esta demonstração pode ser encontrada em [3].

Observamos que um grupo que satisfaz a condição $(\mathcal{N}, 21)$ pode não ser solúvel, um exemplo disto é o grupo A_5, que é coberto por 21 grupos nilpotentes (ver Observação 1.23) e não é solúvel. Na próxima seção será dada uma condição necessária e suficiente para que um grupo finito não-solúvel possa satisfazer a condição $(\mathcal{N}, 21)$.

3.2 Grupos Não-Solúveis que Satisfazem $(\mathcal{N}, 21)$

Começamos com o seguinte fato, cuja demonstração pode ser encontrada em [1].

Proposição 3.10 *O único grupo simples finito não-abeliano que satisfaz a condição* $(\mathcal{N}, 21)$ *é* A_5*.*

Precisamos também dos seguintes lemas:

Lema 3.11 *Sejam* $M_1, \ldots, M_t$ *grupos finitos simples e não-abelianos. Então* $M_1 \times \cdots \times M_m$ *não satisfaz a condição* $(\mathcal{N}, 21^t - 1)$*.*

Demonstração: Observe que o grupo M_i não pode ser solúvel, portanto pela Proposição 3.9 não pode satisfazer $(\mathcal{N}, 20)$, isto é, existem subconjuntos $X_i \subset M_i$ com 21 elementos tais que nenhum par de elementos de X_i gera um subgrupo nilpotente, para todo $i \in \{1, \ldots, t\}$.

Considere o conjunto $X = X_1 \times \cdots \times X_t$. Sejam

$$a = (a_1, \ldots, a_t) \text{ e } b = (b_1, \ldots, b_t)$$

dois elementos distintos de X, isto é, para algum $i \in \{1, \ldots, t\}$ tem-se que $a_i \neq b_i$. Como $a_i, b_i \in X_i$, temos que $K = \langle a_i, b_i \rangle$ é não-nilpotente. Como K é um grupo finito, segue pelo Teorema 1.19 que K não é um grupo de Engel. Portanto, existem elementos $x, y \in K$ tais que $[x,_n y] \neq 1$, para todo $n \in \mathbb{N}$. Suponha que

$$x = a_i^{\delta_1} b_i^{\delta_2} \cdots a_i^{\delta_{r-1}} b_i^{\delta_r} \text{ e } y = a_i^{\gamma_1} b_i^{\gamma_2} \cdots a_i^{\gamma_{s-1}} b_i^{\gamma_s},$$

onde $\delta_p, \gamma_q \in \{0, 1, -1\}$, para todo $p \in \{1, \ldots, r\}$ e $q \in \{1, \ldots, s\}$.

Suponha por contradição que $\langle a, b \rangle$ é nilpotente (portanto um grupo de Engel, pelo Teorema 1.19). Tome $\bar{x}, \bar{y} \in \langle a, b \rangle$ da seguinte forma:

$$x = a^{\delta_1} b^{\delta_2} \cdots a^{\delta_{r-1}} b^{\delta_r} \text{ e } y = a^{\gamma_1} b^{\gamma_2} \cdots a^{\gamma_{s-1}} b^{\gamma_s}.$$

Assim, deve existir um inteiro positivo m tal que $[\bar{x},_m \bar{y}] = 1$,. No entanto,

$$[\bar{x},_m \bar{y}] = ([x_1,_m y_1], \ldots, [x_t,_m y_t]),$$

onde

$$x_j = a_j^{\delta_1} b_j^{\delta_2} \cdots a_j^{\delta_{r-1}} b_j^{\delta_r} \text{ e } y_j = a_j^{\gamma_1} b_j^{\gamma_2} \cdots a_j^{\gamma_{s-1}} b_j^{\gamma_s},$$

para todo $j \in \{1, \ldots, t\}$. Logo, $[x,_m y] = [x_i,_m y_i] = 1$, o que é uma contradição. Consequentemente, nenhum par de elementos distintos do conjunto com 21^t elementos X gera um grupo nilpotente. Portanto, $M_1 \times \ldots \times M_t$ não satisfaz $(\mathcal{N}, 21^t - 1)$.

■

Lema 3.12 *O grupo simétrico S_5 não satisfaz a condição $(\mathcal{N}, 21)$.*

Demonstração: Um subgrupo gerado por qualquer par de elementos distintos do subconjunto de S_5 com 22 elementos $\{(3\ 4\ 5), (2\ 3\ 4), (2\ 3\ 4\ 5), (1\ 4\ 5), (2\ 3\ 5\ 4), (2\ 3\ 5), (2\ 4\ 5), (1\ 2\ 3), (1\ 2\ 3\ 4), (1\ 2\ 4\ 5\ 3), (1\ 2\ 4\ 3\ 5), (1\ 2\ 5), (1\ 3\ 4), (1\ 3\ 4\ 5), (1\ 3\ 5), (1\ 3\ 2\ 4\ 5), (1\ 4\ 2), (1\ 5\ 4\ 3\ 2), (1\ 5\ 3\ 2), (1\ 5\ 4\ 2), (1\ 5\ 2\ 4\ 3),$

(1 5 3 2 4)} é não-nilpotente. Basta observar que o centro do subgrupo gerado por qualquer par de elementos deste conjunto é trivial, com isso a afirmação decorre do Lema 1.10. Pode se verificar que o centro de cada um destes subgrupos é trivial utilizando o software *GAP*.

■

Lema 3.13 *Seja G um grupo finito não-solúvel satisfazendo $(\mathcal{N}, 21)$ e $S = Sol(G)$, isto é, S é o maior subgrupo normal solúvel de G. Então:*

1. $\dfrac{G}{S} \cong A_5$;
2. *para todo $a \in S$, $x \in G \backslash S$, tem-se que $\langle a, x\rangle$ é nilpotente;*
3. $\mathcal{Z}^*(G) = \mathcal{Z}^*(S)$.

Demonstração:

Para demonstrar o item 1, suponha $\bar{G} = \dfrac{G}{S}$. Então $\bar{G}$ é semi-simples, pela Observação 1.28 e $\bar{G} \neq \bar{1}$, pois G é não-solúvel (portanto $G \neq S$).

Seja $\bar{R} = CR(\bar{G})$. Afirmamos que $\bar{R} \neq \bar{1}$. De fato, suponha que $\bar{R} = \bar{1}$, isto é, o produto de subgrupos normais minimais não-abelianos de $\bar{G}$ é $\bar{1}$, portanto $\bar{G}$ não possui subgrupos normais não-abelianos. Como $\bar{G}$ é semi-simples, segue que $\bar{G}$ também não possui subgrupos normais abelianos. Logo $\bar{G}$ é simples. Observamos que $\bar{G} = \dfrac{G}{S}$ não é abeliano, pois se fosse, seria solúvel, e como S é solúvel, teríamos G solúvel, uma contradição. Mas $\bar{R}$ é um subgrupo normal não abeliano de $\bar{G}$ e, como $\bar{G}$ não possui subgrupos normais não abelianos, pela simplicidade de $\bar{G}$ deveríamos ter $\bar{R} = \bar{G}$, o que é absurdo. Isto demonstra a afirmação.

Pela Proposição 1.30, $\bar{R}$ é o produto direto de grupos simples normais não-abelianos, istgo é

$$\bar{R} = \bar{K}_1 \times \cdots \times \bar{K}_t;$$

onde $\bar{K}_i \lhd \bar{G}$, e $\bar{K}_i$ é grupo simples não-abeliano.

Por hipótese, G satisfaz $(\mathcal{N}, 21)$, logo o grupo quociente $\bar{G}$ satisfaz $(\mathcal{N}, 21)$, o que implica que o subgrupo $\bar{R}$ também satisfaz $(\mathcal{N}, 21)$. Com isso, se $t > 1$ então $\bar{R}$ satisfaz $(\mathcal{N}, 21^t - 1)$. No entanto, pelo Lema 3.11, $\bar{R}$ não satisfaz $(\mathcal{N}, 21^t - 1)$.

Então $t = 1$, assim $\bar{R} = \bar{K_1}$, isto é, $\bar{R}$ é simples não-abeliano e satisfaz $(\mathcal{N}, 21)$. Pela Proposição 3.10, temos que o único grupo nestas condições é A_5, assim $\bar{R} \cong A_5$.

Agora, considere o homomorfismo

$$\begin{array}{rcccl} \phi & : & \bar{G} & \longrightarrow & Aut(\bar{R}) \\ & & \bar{g} & \longmapsto & \phi_{\bar{g}} \; : \; \begin{array}{l} \bar{R} \to \bar{R} \\ \bar{r} \mapsto \bar{r}^{\bar{g}} \end{array} \end{array}$$

Dessa forma, $Im\phi \leq Aut(\bar{R}) \cong Aut(A_5)$ e como $Aut(A_5) \cong S_5$ [14], segue que $Im\phi \hookrightarrow S_5$.

Observe que

$$Ker\phi = \{\bar{g} \in \bar{G}; \phi_{\bar{g}} = \bar{1}\} = \{\bar{g} \in \bar{G}; \bar{g}\bar{r} = \bar{r}\bar{g}, \text{ para todo } \bar{r} \in \bar{R}\} = C_{\bar{G}}(\bar{R}).$$

Desde que $C_{\bar{G}}(\bar{R}) = 1$ e, pelo Primeiro Teorema do Isomorfismo $\dfrac{\bar{G}}{Ker\phi} \cong Im\phi$, temos $A_5 \hookrightarrow \bar{G} \hookrightarrow S_5$ e assim $\bar{G} \cong A_5$ ou $\bar{G} \cong S_5$. Mas o Lema 3.12 implica que $\bar{G} \cong A_5$.

Para o item 2, segue da Observação 1.23 que A_5 possui 21 subgrupos de Sylow. Assim, pelo item 1, podemos considerar $Q_1, \ldots, Q_{21}$ os distintos subgrupos de Sylow de $\dfrac{G}{S}$. Para cada $i \in \{1, \ldots, 21\}$, seja $x_iS \in Q_i \backslash \bar{1}$. Novamente, pela Observação 1.23, nenhum par de elementos distintos em $\{x_1S, \ldots, x_{21}S\}$ gera um grupo nilpotente.

Fixando $k \in \{1, \ldots, 21\}$, dado $a \in S$, considere os elementos

$$x_k, x_1, \ldots, x_{k-1}, ax_k, x_{k+1}, \ldots, x_{21}.$$

Para $k, j \in \{1, \ldots, 21\}$, com $j \neq k$, temos $\langle ax_k, x_j \rangle$ não é nilpotente pois $\langle ax_k, x_j \rangle S = \langle x_k, x_j \rangle S$.

Como G satisfaz $(\mathcal{N}, 21)$, então $\langle x_k, ax_k \rangle = \langle a, x_k \rangle$ é nilpotente, para todo $k \in \{1, \ldots, 21\}$. Desde que $\dfrac{G}{S} = \displaystyle\bigcup_{i=1}^{21} Q_i$ (Observação 1.23), segue que $\langle a, x \rangle$ é nilpotente para todo $x \in G \backslash S$ e todo $a \in S$.

Finalmente, note que se S é finito, então $\mathcal{Z}^*(S) = \mathcal{Z}_m(S)$, para algum $m \in \mathbb{N}$. Sejam $a \in \mathcal{Z}_m(S)$ e $b \in S$. Vamos mostrar que $\langle a, b \rangle$ é nilpotente. Seja $T = \langle a, b \rangle$. Primeiramente, sabemos que

$$\frac{T}{T \cap \mathcal{Z}_m(S)} \cong \frac{T\mathcal{Z}_m(S)}{\mathcal{Z}_m(S)}$$

e temos $\dfrac{T}{T \cap \mathcal{Z}_m(S)}$ cíclico, pois $T = \langle a, b\rangle$ e $a \in \mathcal{Z}_m(S)$ ou seja, $\dfrac{T\mathcal{Z}_m(S)}{\mathcal{Z}_m(S)}$ é cíclico e $T \cap \mathcal{Z}_m(S) \leq \mathcal{Z}_m(T)$. Como

$$\frac{\dfrac{T}{T \cap \mathcal{Z}_m(S)}}{\dfrac{\mathcal{Z}_m(T)}{T \cap \mathcal{Z}_m(S)}} \cong \frac{T}{\mathcal{Z}_m(T)},$$

temos $\dfrac{T}{\mathcal{Z}_m(T)}$ cíclico e, portanto, T é nilpotente.

Com isso, mostramos que dado $a \in \mathcal{Z}^*(S)$, temos $\langle a, x\rangle$ nilpotente, para todo $x \in G$. Mas $\langle a, x\rangle$ é n-Engel à direita, assim $a \in R(G)$. Como $\langle a, x\rangle$ é finito, temos, pelo Teorema 1.18, $R(G) = \mathcal{Z}^*(G)$. Portanto, $\mathcal{Z}^*(S) \leq \mathcal{Z}^*(G)$ e, como $\mathcal{Z}^*(G) \leq \mathcal{Z}^*(S)$, então $\mathcal{Z}^*(G) = \mathcal{Z}^*(S)$.

■

Estamos prontos agora para demonstrar o resultado principal do capítulo.

Teorema 3.14 *Seja G um grupo finito não-solúvel. Então G satisfaz $(\mathcal{N}, 21)$ se, e somente se, $\dfrac{G}{\mathcal{Z}^*(G)} \cong A_5$.*

Demonstração: Suponha que G satisfaz $(\mathcal{N}, 21)$. Suponha que G é o contra-exemplo de menor ordem tal que $\dfrac{G}{\mathcal{Z}^*(G)} \ncong A_5$, isto é, se H é um grupo com as mesmas características de G e $|H| < |G|$ então $\dfrac{H}{\mathcal{Z}^*(H)} \cong A_5$. Seja $S = Sol(G)$. Afirmamos que $\mathcal{Z}(S) = 1$.

De fato, suponha $\mathcal{Z}(S) \neq 1$. Então $\dfrac{G}{\mathcal{Z}(S)}$ é um grupo finito, não solúvel e satisfaz $(\mathcal{N}, 21)$. Como $|\dfrac{G}{\mathcal{Z}(S)}| < |G|$, temos

$$\frac{\dfrac{G}{\mathcal{Z}(S)}}{\mathcal{Z}^*(\dfrac{G}{\mathcal{Z}(S)})} \cong A_5 \tag{3.1}$$

e o radical solúvel de $\dfrac{G}{S}$ é $\dfrac{S}{\mathcal{Z}(S)}$, Pelo Lema 3.13,

$$\left(\mathcal{Z}^* \frac{G}{\mathcal{Z}(S)}\right) = \mathcal{Z}^*\left(Sol\left(\frac{G}{\mathcal{Z}(S)}\right)\right) = \mathcal{Z}^*\left(\frac{S}{\mathcal{Z}(S)}\right).$$

Por outro lado, temos

$$\mathcal{Z}^*\left(\frac{S}{\mathcal{Z}(S)}\right) = \frac{\mathcal{Z}^*(S)}{\mathcal{Z}(S)} = \frac{\mathcal{Z}^*(G)}{\mathcal{Z}(S)}. \tag{3.2}$$

De (3.1) e (3.2) temos

$$A_5 \cong \frac{\dfrac{G}{\mathcal{Z}(S)}}{\mathcal{Z}^*\left(\dfrac{G}{\mathcal{Z}(S)}\right)} = \frac{\dfrac{G}{\mathcal{Z}(S)}}{\dfrac{\mathcal{Z}^*(G)}{\mathcal{Z}(S)}} \cong \frac{G}{\mathcal{Z}^*(G)},$$

o que é uma contradição. Portanto $\mathcal{Z}(S) = 1$ e isso implica $\mathcal{Z}^*(S) = 1$.

Agora seja $x \in G\backslash S$ de forma que $x^2 \in S$. Para todo $b \in S$, temos $bx \in G\backslash S$. Realmente, se $bx \in S$ teríamos $x \in S$.

Note que $(bx)^2 = bxbx = bx^2x^{-1}bx \in S$.

Pelo Lema 3.13 temos $\langle bx, a\rangle$ nilpotente, para todo $a \in S$. Como $\langle (bx)^2, a\rangle \subset \langle bx, a\rangle$ segue que, para todo $a \in S$, o subgrupo $\langle (bx)^2, a\rangle$ é nilpotente, e como este subgrupo é finito, concluímos que $(bx)^2$ é um elemento de Engel à direita de S. Pelo Teorema 1.18, temos $(bx)^2 \in \mathcal{Z}^*(S) = 1$, portanto $(bx)^2 = 1$, para todo $b \in S$.

Como $b \in S$ e $x \in G\backslash S$, pelo Lema 3.13, $\langle b, x\rangle$ é nilpotente. Assim $\langle b, x^2\rangle \subset \langle b, x\rangle$ é nilpotente e finito. Da mesma forma que no parágrafo anterior concluímos que $x^2 = 1$. Portanto, $D = \langle b, x\rangle$ é um grupo diedral finito nilpotente, logo um 2-grupo, o que implica que b é um elemento de ordem potência de 2. Com isso, S é um 2-grupo, mas como vimos anteriormente, $\mathcal{Z}(S) = 1$, implicando $S = 1$. Assim, pelo Lema 3.13, temos $\mathcal{Z}^*(G) = 1$ e, portanto,

$$\frac{G}{\mathcal{Z}^*(G)} = \frac{G}{S} \cong A_5,$$

uma contradição. Logo,

$$\frac{G}{\mathcal{Z}^*(G)} \cong A_5.$$

Reciprocamente, suponha que $\dfrac{G}{\mathcal{Z}^*(G)} \cong A_5$. Pela Observação 1.23, temos

$$\frac{G}{\mathcal{Z}^*(G)} = \bigcup_{i=1}^{21} \frac{P_i}{\mathcal{Z}^*(G)},$$

onde $\dfrac{P_1}{\mathcal{Z}^*(G)}, \ldots, \dfrac{P_1}{\mathcal{Z}^*(G)}$ são os subgrupos de Sylow de $\dfrac{G}{\mathcal{Z}^*(G)}$.

Como G é finito, temos então $\mathcal{Z}^*(G) = \mathcal{Z}_m(G)$, para algum m. Como $\mathcal{Z}_m(G) \subset P_i$, então $\mathcal{Z}_m(G) \leq \mathcal{Z}_m(P_i)$, para todo i. Agora $\dfrac{P_i}{\mathcal{Z}_m(G)}$ tem ordem prima e é finito, portanto é nilpotente. Assim,

$$\frac{\dfrac{P_i}{\mathcal{Z}_m(G)}}{\dfrac{\mathcal{Z}_m(P_i)}{\mathcal{Z}_m(G)}} \cong \frac{P_i}{\mathcal{Z}_m(P_i)}$$

é nilpotente e portanto, P_i é nilpotente, pelo Lema 1.12.

Seja $g \in G$. Então $g\mathcal{Z}^*(G) = x\mathcal{Z}^*(G)$, para $x \in P_i$, com isso $x^{-1}g \in \mathcal{Z}^*(G)$. Como vimos acima, $\mathcal{Z}^*(G) \leq \mathcal{Z}^*(P_i) \leq P_i$, portanto, $x^{-1}g \in P_i$, isto é, existe $h \in P_i$ tal que $x^{-1}g = h$, logo $g = xh \in P_i$, isto mostra que se $x \in G$, então x está necessariamente em algum dos grupos P_i, $i = 1, \ldots, 21$. Então,

$$G = \bigcup_{i=1}^{21} P_i.$$

Logo G satisfaz $(\mathcal{N}, 21)$.

■

Vejamos agora algumas consequências deste teorema. A primeira delas dá uma interessante caracterização do grupo A_5.

Corolário 3.15 *O único grupo finito, não-solúvel, sem centro que satisfaz a condição* $(\mathcal{N}, 21)$ *é* A_5.

Demonstração: Seja G um grupo finito, não-solúvel, sem centro que e satisfaz a condição $(\mathcal{N}, 21)$. Como $\mathcal{Z}(G) = 1$, segue que $\mathcal{Z}^*(G) = 1$. Assim, pelo Teorema 3.14, segue que

$$\frac{G}{\mathcal{Z}^*(G)} \cong G \cong A_5.$$

■

Observe que pelo Teorema 3.14 temos que A_n não satisfaz $(\mathcal{N}, 21)$, para $n > 5$, pois pela simplicidade de tais grupos temos $\mathcal{Z}^*(A_n) = 1$, e assim $\dfrac{A_n}{\mathcal{Z}^*(A_n)} \ncong A_5$.

Considere o grupo $SL(2,5)$. Vimos logo após a Observação 1.23 que

$$\frac{SL(2,5)}{\mathcal{Z}(SL(2,5))} = PSL(2,5) \cong A_5,$$

então

$$\mathcal{Z}\left(\frac{SL(2,5)}{\mathcal{Z}(SL(2,5))}\right) = 1,$$

pois $\dfrac{SL(2,5)}{\mathcal{Z}(SL(2,5))} = PSL(2,5)$ é simples. Como $SL(2,5)$ é finito, temos $\mathcal{Z}^*(SL(2,5)) = \mathcal{Z}(SL(2,5))$. Portanto,

$$\frac{SL(2,5)}{\mathcal{Z}^*(SL(2,5))} \cong A_5$$

e, pelo Teorema 3.14, segue que $SL(2,5)$ satisfaz a condição $(\mathcal{N}, 21)$, embora $SL(2,5)$ não satisfaça a condição $(\mathcal{A}, 21)$, pelo Lema 2.13.

Mais alguns exemplos: como $PSL(2,3) \cong A_4$, então $SL(2,3)$ satisfaz $(\mathcal{N}, 5)$, conforme o Exemplo 1.34. Além disso $PSL(4,2) \cong A_8$ e $PSL(2,9) \cong A_6$, portanto $SL(4,2)$ e $SL(2,9)$ não satisfazem $(\mathcal{N}, 21)$. As demonstraçï¿½es de tais isomorfismos podem ser encontradas em [8].

Vamos apresentar agora um interessante resultado sobre grupos que satisfazem $(\mathcal{N}, 21)$.

Corolário 3.16 *Um grupo finito não-solúvel satisfaz* $(\mathcal{N}, 21)$ *se, e somente se, é coberto por* 21 *subgrupos nilpotentes.*

Demonstração: Se G é um grupo finito, não-solúvel que satisfaz $(\mathcal{N}, 21)$, vimos na demonstração do Teorema 3.14 que ele é coberto por 21 subgrupos nilpotentes. Reciprocamente se G é coberto por 21 subgrupos nilpotentes então, claramente, G satisfaz $(\mathcal{N}, 21)$.

■

Considerações Finais

Apresentamos neste trabalho caracterizações de grupos que satisfazem a condição $(\mathcal{A}, n)$ e grupos não-solúveis que satisfazem $(\mathcal{N}, 21)$.

Vimos que se um grupo solúvel G satisfaz a condição $(\mathcal{A}, n)$, então podemos determinar um limite para o comprimento derivado de G que depende apenas de n (Teorema 2.15). Abdollahi e Hassanabadi [1] caracterizam os grupos não solúveis que satisfazem $(\mathcal{A}, 21)$, mostrando que um grupo G nestas condições é isomorfo a $Z(G) \times A_5$, isto é, um grupo não solúvel que satisfaz a condição $(\mathcal{A}, 21)$ é o produto direto um grupo abeliano (o centro do grupo) com o grupo A_5.

No caso em que G é um grupo solúvel e finitamente gerado que satisfaz $(\mathcal{N}, n)$, Tomkinson [16] determina um limite para a ordem de $\dfrac{G}{\mathcal{Z}^*(G)}$ que depende apenas de n, mostrando que $\left|\dfrac{G}{\mathcal{Z}^*(G)}\right| \leq n^{n^4}$.

Se G é um grupo finito semi-simples que satisfaz $(\mathcal{N}, n)$, então $|G| < c^{2n^2\left[log_{21}^{n}\right]}\,[log_{21}^{n}]!$, para alguma constante c [1]. Em particular, este resultado dá um limite para a ordem de um grupo solúvel finito sem centro que satisfaz $(\mathcal{N}, n)$. Como $\dfrac{G}{Sol(G)}$ é semi-simples (Observação 1.28), segue que $\left|\dfrac{G}{Sol(G)}\right| < c^{2n^2\left[log_{21}^{n}\right]}\,[log_{21}^{n}]!$, para alguma constante c. Combinando este resultado com aquele obtido por Tomkinson, temos que se G é um grupo finito que satisfaz $(\mathcal{N}, n)$, então $\left|\dfrac{G}{Fit(G)}\right| < n^{n^4} c^{2n^2\left[log_{21}^{n}\right]}\,[log_{21}^{n}]!$, para alguma constante c, onde $Fit(G)$ é o produto de todos os subgrupos normais nilpotentes de G.

No comentário que fizemos logo após a demonstração da Proposição 3.8, vimos que se $n \leq 3$ então todo grupo satisfazendo a condição $(\mathcal{N}, n)$ é nilpotente, vimos também que S_3 é um exemplo de um grupo não-nilpotente que satisfaz a condição $(\mathcal{N}, 4)$. Na verdade, o único grupo finito cujo centro é trivial e que satisfaz a condição

$(\mathcal{N}, 4)$ é S_3, de acordo com o seguinte resultado [1].

Teorema: *Seja G um grupo finito não-nilpotente. Então G satisfaz a condição $(\mathcal{N}, 4)$ se, e somente se $\dfrac{G}{\mathcal{Z}^*(G)} \cong S_3$.*

Abdollahi e Hassanabadi [1] também mostraram o seguinte resultado, como corolário do Teorema 3.14:

Teorema: *Seja G um grupo finito que satisfaz $(\mathcal{N}, 21)$. Se $CR(G)$ é não-trivial, então $G \cong \mathcal{Z}^*(G) \times A_5$.*

Isto é, um grupo finito que satisfaz $(\mathcal{N}, 21)$ é o produto direto de um grupo nilpotente com A_5, desde que o CR-radical sem centro do grupo seja não-trivial. A idéia da demonstração consiste em mostrar que $CR(G) \cong A_5$ e $CR(G) \cap \mathcal{Z}^*(G) = 1$, para se chegar ao produto direto. Conjectura-se que um grupo não solúvel que satisfaz a condição $(\mathcal{N}, 21)$ é um produto direto de um grupo nilpotente e um grupo isomorfo a A_5 e $SL(2, 5)$.

Utilizamos fortemente no Capítulo 2, alguns resultados de Teoria de Grafos para demonstrar o Teorema 2.12, que dá a caracterização dos grupos que satisfazem a condição $(\mathcal{A}, n)$. Para isto, associamos a um grupo G um grafo onde dois elementos $x, y \in G$ estão conectados se eles não comutam. Em 1981, Lennox e Wiegold [9] extenderam estes conceitos relacionados a grafos para caracterizar grupos que satisfazem a condição $(\mathcal{X}, n)$, para outras classes de grupos além da classe dos grupos abelianos. Para caracterizar os grupos que satisfazem $(\mathcal{N}, n)$, define-se que $x, y \in G$ estão conectados no grafo de G se $\langle x, y\rangle \notin \mathcal{N}$. Neste caso, um grupo G satisfaz a condição $(\mathcal{N}, n)$se, e somente se, $G \in \mathcal{FN}$, desde que G seja solúvel e finitamente gerado. Aqui, $\mathcal{FN}$ denota a classe dos grupos finito-por-nilpotente, onde G é *finito-por-nilpotente* se existe $H \lhd G$, com H finito e $\dfrac{G}{H}$ nilpotente.

Tais resultado servem de motivação para se dar continuidade aos assuntos tratados nesta dissertação, bem como para o aprofundamento do estudo da Teoria de Grupos em si, além de outras áreas, como Teoria de Grafos, aplicadas à Teoria de Grupos. A Teoria de Grafos é frequentemente utilizada em Teoria de Grupos (por exemplo apresentação de grupos, grafos de ciclo, grafos de Cayley, diagramas de isomorfismo, etc) e outras áreas da Álgebra, como álgebras de Lie (diagramas de Dynkin em Álgebras de Lie, por exemplo).

Referências Bibliográficas

[1] A. Abdollahi, A. M. Hassanabadi. *Finite groups with a certain number of elements pairwise generating a non-nilpotent subgroup*. Bull. of the Iranian Math. Soc. 30 No. 2, (2004), 1-20.

[2] R. Diestel. *Graph Theory*. 3d Edition, Springer-Verlag, 2005.

[3] G. Endimioni. *Groupes finis satisfaisant la condition* $(\mathcal{N}, n)$. C. R. Acad. Sci. Paris Ser. I. 319 (1994), 1245-1247.

[4] A. Garcia, Y. Lequain. *Álgebra: um curso de introdução*. IMPA, 1988.

[5] E. S. Golod. *Some problems of Burnside type*. Amer. Math. Soc. Trans. Ser. 2, Vol. 84 (1969), 83-84

[6] A. Gonçalves. *Tópicos em representação de grupos*. 9^o Colóquio Brasileiro de Matemática, 1973.

[7] D. Gorenstein. *Finite Groups*. 2nd Edition, Chelsea Publishing Company, 1968

[8] B. Huppert. *Endliche Gruppen I*. Springer-Verlag, 1967.

[9] J. C. Lennox, J. Wiegold. *Extensions of a problem of Paul Erdös on groups*. J. Austr. Math. Soc. Ser. A 31 (1981), 467-

[10] Francisco C. P. Milies. *Grupos nilpotentes*. Bienal da Sociedade Brasileira de Matemática, Departamento de Matemática-ICEx/UFMG, 2002 472.

[11] B. H. Neumann. *A problem of Paul Erdös on groups*. J. Austral. Math. Soc. Ser. A 21 (1976), 467-472.

[12] L. Pyber *The number of pairwise non-commuting and the index of the centre in a finite group*, J. London Math. Society, 35 (1987), 287-295.

[13] D. Robinson, *A Course in the Theory of Groups*. Second Edition, Springer-Verlag, 1996

[14] M. Suzuki. *Group theory I*. Springer-Verlag, 1982.

[15] J. G. Thompson. *Nonsolvable finite groups all of whose local subgroups are solvable.* Bulletin of American Mathematical Society, vol. 74 (1968), 383-437.

[16] M. J. Tomkinson. *Hypercentre-by-finite groups*. Publ. Math. Debrecen 40 (1992), 313-321.