Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

GRUPOS COM UM SUBGRUPO MAXIMAL ABELIANO

Deyfila da Silva Lima

Brasília
10 de março de 2023

Deyfila da Silva Lima

GRUPOS COM UM SUBGRUPO MAXIMAL ABELIANO

Dissertação apresentada ao Programa de Pós-Gradução em Matemática do Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de Mestra em Matemática.

Orientador: Prof. Dr. Raimundo de Araújo Bastos Júnior

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Grupos com um subgrupo maximal abeliano

por

Deyfila da Silva Lima*

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

MESTRA EM MATEMÁTICA

Brasília, 10 de março de 2023.

Comissão Examinadora:

Prof. Dr. Raimundo de Araújo Bastos Júnior - MAT/UnB (Orientador)

Prof. Dr. Carmine Monetta – Università di Salerno (Membro)

Prof. Dr. Ricardo Nunes de Oliveira – UFG (Membro)

* A autora foi bolsista da CAPES durante a elaboração desta dissertação.

Agradecimentos

Agradeço primeiramente a Deus por todas as conquistas até aqui e por nunca me abandonar apesar das minhas falhas.

À minha mãe que é a inspiração de todas as minhas lutas e conquistas.

Ao meu padrasto Elivan que me escolheu como sua filha e sempre me apoiou em todas as minhas escolhas.

À minha irmã que apesar de ser chata nos presenteou com o nosso príncipe Ravi.

Ao meu namorado Jean que me deu todo incentivo e apoio para finalizar essa etapa.

As minhas amigas Tatiane e Jucineia que sempre me proporcionaram palavras de apoio e incentivo.

As minhas amigas Joyce e Henrylla que foram fundamentais para a minha permanência em Brasília.

Ao Tharles, Guilherme e Maria por toda ajuda na construção dessa pesquisa.

Em especial ao Professor Raimundo Bastos por ter aceito me orientar. Por toda paciência e dedicação.

Aos professores Carmine Monetta e Ricardo Nunes de Oliveira por terem aceito fazer parte da minha banca e por todas as contribuições para versão final deste trabalho.

Por fim, agradeço a CAPES e a DPG pelo apoio financeiro.

RESUMO

O objetivo deste trabalho é investigar/descrever propriedades estruturais de grupos (finitos ou infinitos) a partir de restrições sobre seus subgrupos.

Palavras Chaves: Critérios de Solubilidade. Grupos Finitos. Comutadores.

ABSTRACT

The goal of this work is to investigate/describe structural properties of groups (finite or infinite) under some restrictions on their subgroups.

Keywords: Solubility Criteria. Finite Groups. Commutators.

Lista de símbolos

Símbolo	**Significado**
$A \subseteq G$	A é subconjunto de G.
$A \subset G$	A é subconjunto de G com $A \neq G$.
$A \leq G$	A é um subgrupo de G.
$A < G$	A é um subgrupo próprio de G.
$N \trianglelefteq \trianglelefteq G$	N é um subgrupo subnormal de G.
$\|G : H\|$	Índice do subgrupo H em G.
$[x, y]$	Comutador de x e y.
$N \trianglelefteq G$	N é um subgrupo normal de G.
$N \cdot \trianglelefteq G$	N é um subgrupo normal minimal de G.
$M \lessdot G$	M é um subgrupo maximal de G.
$M \lessdot_c G$	M é um subgrupo cíclico maximal de G.
$\frac{G}{N}$	Grupo quociente de G por N.
$H \simeq G$	H é isomorfo a G.
$C_G(H)$	Centralizador de H em G.
$N_G(H)$	Normalizador de H em G.
$G' = [G, G]$	Subgrupo derivado de G.
$P \times Q$	Produto direto.
$P \rtimes Q$	Produto semidireto.
$Z(G)$	Centro do grupo de G.
$S \oplus V$	Soma direta.
$\langle a \rangle$	Grupo gerado pelo elemento a.
$o(a)$	Ordem do elemento a.
$\Phi(G)$	Subgrupo de Frattini de G.
$\pi(G)$	Conjunto dos primos que comparecem na fatoração de $\|G\|$.
$Syl_p(G)$	Conjunto dos p-subgrupos de Sylow de G.
$\|G\|$	Ordem do grupo G.
(m, n)	O mdc entre m e n.
x^y	Conjugado de x por $y, y^{-1}xy$.
$[x, y]$	Comutador dos elementos x e y (nessa ordem), $x^{-1}y^{-1}xy$.
π	Conjunto não vazio de primos.
$Syl_\pi(G)$	π-subgrupo de Sylow de G.

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

Neste trabalho, nosso objetivo é investigar propriedades estruturais de grupos a partir de restrições sobre certos subgrupos (maximais). Em linhas gerais, investigamos as seguintes duas questões:

- Como a existência de um dado subgrupo abeliano pode influenciar na estrutura de um grupo?
- O que podemos dizer acerca de grupos nos quais os subgrupos cíclicos maximais são ainda subgrupos maximais?

Todos os teoremas e exemplos aqui apresentados foram baseados nos trabalhos de Brodie [1], Segal [5], Robinson [9], Gupta [10] e Juriaans e Rogério [13].

Os dois primeiros teoremas apresentados nesse trabalho investigam a estrutura de um dado grupo a partir da existência de um subgrupo maximal e abeliano. O resultado a seguir é uma caracterização de p-grupos finitos que possuem um subgrupo maximal cíclico.

Proposição A. *Um grupo de ordem p^n tem um subgrupo maximal cíclico se, e somente se, for de um dos seguintes tipo:*

a) Um grupo cíclico de ordem p^n.

b) O produto direto de um grupo cíclico de ordem p^{n-1} e o outro de ordem p.

c) $\langle x, a \mid x^p = 1 = a^{p^{n-1}},\ a^x = a^{1+p^{n-2}} \rangle$, $n \geq 3$.

d) O grupo diedral D_{2^n}, $n \geq 3$.

e) O grupo quatérnion generalizado Q_{2^n}, $n \geq 3$.

f) O grupo semidiedral $\langle x, a \mid x^2 = 1 = a^{2^{n-1}},\ a^x = a^{2^{n-2}-1} \rangle$, $n \geq 3$.

O resultado a seguir é um critério de solubilidade para um grupo finito a partir da existência de um subgrupo maximal abeliano.

Teorema B. *(Herstein) Seja G um grupo finito admitindo um subgrupo maximal abeliano H. Então G é solúvel.*

O próximo resultado descreve propriedades do subgrupo derivado e da ordem de um grupo que possui um subgrupo normal abeliano cujo quociente é cíclico. Mais precisamente,

Teorema C. *Sejam G um grupo e A um subgrupo normal abeliano de G. Suponhamos que existe $x \in G$, tal que $G/A = \langle Ax \rangle$. Então*

(1) (Spiegel, [14]) $\{[a, x] \mid a \in A\} \leq G$.

(2) $G' = \{ [a, x] \mid a \in A\}$.

(3) A aplicação

$$\begin{aligned} \Gamma : A &\longrightarrow G' \\ a &\longmapsto [a, x] \end{aligned}$$

é um epimorfismo.

(4) O $\ker(\Gamma) = A \cap Z(G)$. *Em particular,*

$$\frac{A}{A \cap Z(G)} \simeq G'.$$

(5) Seja A um subgrupo maximal de um p-grupo não abeliano G. Suponhamos que A é abeliano. Então

(5.1) $Z(G) \leq A$.

(5.2) $|G| = p \cdot |Z(G)| \cdot |G'|$.

A Proposição A e os Teoremas B e C já são bastante conhecidos, mas optamos por incluir as suas demonstrações por uma questão de completude e evidenciar a importância/influência dos subgrupos maximais/abelianos na estrutura do seu grupo.

Agora estamos interessados em investigar a estrutura de grupos que são $\mathcal{M}_c$-grupos. Fixemos a seguinte definição. Dizemos que um grupo G é um $\mathcal{M}_c$-grupo se, e somente se, as seguintes duas condições são satisfeitas:

- Todo subgrupo cíclico maximal é maximal em G.
- G contém pelo menos um subgrupo cíclico maximal próprio.

No contexto de grupos finitos: Juriaans e Rogério classificaram todos os $\mathcal{M}_c$-grupos. Mais precisamente,

Teorema D. *(Juriaans e Rogério). Seja G um grupo finito. Então G é um $\mathcal{M}_c$- grupo se, e somente se, um dos seguintes vale:*

(1) G é cíclico ou $G \simeq C_p \times C_p \times C_n$, onde p é um primo que não divide n.

(2) $G \simeq C_n \times Q_8$ *com* n *ímpar.*

(3) Existem primos $q < p$*, uma sequência exata* $1 \to Z(G) \to G \to C_p \rtimes C_q \to 1$ *e* $Z(G) \leq \langle x \rangle$ *para qualquer* $\langle x \rangle \lessdot_c G$*.*

Aqui, começaremos estudando uma caracterização de grupos cíclicos infinitos em termos dos seus subgrupos (próprios) devido a Fedorov (veja [9, Exercício 14.5.5]).

Teorema E. *(Fedorov). Seja* G *um grupo infinito. Então* $G \simeq C_\infty$ *(cíclico infinito) se, e somente se, todos os subgrupos não triviais de* G *tem índice finito.*

No contexto dos $\mathcal{M}_c$-grupos infinitos a teoria é muito mais complicada e, até agora, não existe uma classificação completa para tais grupos. Aqui estudaremos os seguintes resultados de Juriaans e Rogério acerca de $\mathcal{M}_c$-grupos infinitos:

Teorema F. *(Juriaans e Rogério). Seja* G *um* $\mathcal{M}_c$*-grupo infinito.*

(1) Se G *é solúvel, então* G *é cíclico infinito.*

(2) Então $G' = G''$*.*

(3) Se G *é residualmente finito, então* G *é cíclico infinito.*

Observe que os itens (1) e (3) do Teorema F nos fornecem novas "caracterizações" para grupos cíclicos infinito em termos de $\mathcal{M}_c$-grupos. Cabe destacar que nem sempre um $\mathcal{M}_c$-grupo infinito é cíclico (infinito). Por exemplo, os grupos que ficaram conhecidos como Monstro de Tarski são $\mathcal{M}_c$-grupos infinitos. Tais grupos são 2-gerado, simples, infinito de expoente p, para primo "suficientemente grande".

O trabalho foi dividido em 5 Capítulos e a sua estrutura em linhas gerais é a seguinte:

- Capítulo 1: Neste capítulo apresentaremos alguns tópicos básicos da Teoria dos Grupos que serão necessários para o desenvolvimento desse trabalho. Na seção 1.1 definiremos subgrupos normais, grupo quociente e morfismos de grupos e apresentamos os Teoremas dos Índices, de Poincaré, da Correspondência e dos Isomorfismos. Na seção 1.2 apresentaremos alguns subgrupos clássicos os quais serão de grande utilidade na prova dos principais resultados deste texto. Também apresentaremos os Teoremas de Sylow. E por fim, na seção 1.3 faremos uma breve síntese sobre extensões de grupos.

- Capítulo 2: Neste capítulo, faremos um breve estudo dos grupos cíclicos, abelianos, solúveis, nilpotentes, supersolúveis e policíclicos, destacando alguns resultados básicos que nos serão fundamentais nos capítulos finais. Na última seção faremos uma comparação entre tais classes.

- Capítulo 3: Neste capítulo, estudaremos grupos que admitem um subgrupo maximal. Na seção 3.1 apresentaremos uma classificação de grupos, cuja ordem é uma potência de número primo que possuem um subgrupo cíclico o qual é maximal. Utilizaremos este resultado para provarmos o Teorema que caracteriza os grupos nilpotentes finitos que são $\mathcal{M}_c$-grupos. Na seção 3.2, apresentaremos um teorema de caracterização de grupos finitos que possuem um subgrupo maximal e abeliano, para a demonstração de tal resultado usaremos grupos de Frobenius, assim trazemos a definição e algumas propriedades de grupos de Frobenius. Na última seção nos ocuparemos de uma importante subclasse dos grupos solúveis chamados de grupos "abeliano-por-cíclico". A Proposição A e os Teorema B e C serão demonstrados neste capítulo.

- Capítulo 4: Aqui apresentaremos a prova do Teorema D. Iremos investigar a estrutura dos $\mathcal{M}_{\boldsymbol{c}}$-grupos. Na primeira seção, definiremos e exibiremos alguns exemplos e propriedades dos $\mathcal{M}_{\boldsymbol{c}}$-grupos e a seção 4.2 iremos caracterizar os $\mathcal{M}_{\boldsymbol{c}}$-grupos finitos.

- Capítulo 5: Na primeira seção deste capítulo, definiremos e apresentaremos algumas propriedades de FC-grupos. Na seção 5.2 apresentaremos o Teorema de Schur e Fedorov e na seção 5.3 iremos classificar algumas famílias de $\mathcal{M}_{\boldsymbol{c}}$-grupos infinitos.

Capítulo 1

Preliminares

Neste capítulo faremos uma revisão de alguns conceitos e resultados da Teoria dos Grupos que serão importantes para as demonstrações dos nossos resultados principais. No intuito de consolidar a notação que será utilizada ao longo deste trabalho, facilitando a compreensão dos lemas, proposições e teoremas abordados nos capítulos subsequentes. Em geral, não apresentaremos as demonstrações destes resultados, entretanto elas podem ser encontradas em [2, Capítulo 5], [3, Capítulo 6] e [9, Capítulo 1].

1.1 Subgrupos Normais, Grupo Quociente e Morfismos de Grupos

Definição 1.1.1. *Dizemos que um subgrupo $N \leq G$ é um subgrupo normal se $Ng = gN$, para todo $g \in G$.*

Notação: $N \trianglelefteq G$.

A partir de um subgrupo normal N induzimos uma operação natural sobre as classes laterais: $xN \cdot yN = xyN$. O conjunto $\{xN \mid x \in G\}$ com a operação mencionada é um grupo.
Notação: $G/N = \{xN \mid x \in G\}$.

Definição 1.1.2. *Seja $N \trianglelefteq G$, o índice de N em G é definido por $|G : N| := |G/N| = |\{gN \mid g \in G\}|$.*

Observação 1.1.1. *$\{1\}$ e G são sempre subgrupos normais em G.*

Definição 1.1.3. *A ordem do grupo G é o número de elementos em G e será denotada por $|G|$. Se α é um elemento do grupo G, a ordem de α é a ordem do subgrupo gerado por α que será denotada por $o(\alpha) = |\langle\alpha\rangle|$.*

Proposição 1.1.1. *Seja $N \leq G$ com $|G : N| = 2$, então $N \trianglelefteq G$.*

Definição 1.1.4. *Sejam $(K, *), (L, \circ)$ grupos. Dizemos que uma aplicação $\varphi : K \to L$ é um homomorfismo (de grupos) se $\varphi(x * y) = \varphi(x) \circ \varphi(y)$, para todo $x, y \in K$.*

Exemplo 1.1.1.

1. *Se* $N \trianglelefteq G$, *então* $\pi : G \to G/N$ *dada por* $g \mapsto gN$ *é um homomorfismo (projeção).*

2. *O* $det : GL_n(n, \mathbb{F}) \to \mathbb{F}^*$ *onde* $A^\alpha = detA$ *e* $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$. *Aqui* $\mathbb{F}$ *é um corpo.*

Teorema 1.1.1. *(Primeiro Teorema do Isomorfismo). Sejam* G, H *grupos e* $\varphi : G \longrightarrow H$ *um homomorfismo de grupos. Então*

$$\frac{G}{Ker(\varphi)} \simeq Im(\varphi).$$

Exemplo 1.1.2. *A projeção* $\pi : G \to G/N$ *é um epimorfismo cujo núcleo é* $\ker(\pi) = N$.

Corolário 1.1.1. *(Segundo Teorema do Isomorfismo). Sejam* G *um grupo,* $H \leq G$ *e* $N \trianglelefteq G$, *então* $N \cap H, N \trianglelefteq NH$ *e* $\dfrac{HN}{N} \simeq \dfrac{H}{H \cap N}$.

Corolário 1.1.2. *(Terceiro Teorema do Isomorfismo). Sejam* G *um grupo,* $H \trianglelefteq G, N \trianglelefteq G$ *e* $H \leq N$. *Então,*

$$\frac{G}{N} \simeq \frac{G/H}{N/H}.$$

Teorema 1.1.2. *(Teorema da Correspondência). Se* G *é um grupo e* $N \trianglelefteq G$, *então existe uma correspondência biunívoca entre os subgrupos de* G *que contém* N *e os subgrupos de* $\dfrac{G}{N}$. *Por esta correspondência, os subgrupos normais de* G *que contém* N *correspondem a subgrupos normais de* $\dfrac{G}{N}$ *e vale a recíproca.*

Proposição 1.1.2. *(Teorema dos índices). Sejam* H, K *subgrupos de um grupo* G. *Suponhamos que* $H \leq K \leq G$. *Então:* $|G : H| = |G : K| \cdot |K : H|$.

Teorema 1.1.3. *(Lema de Poincaré) Sejam* H, K *subgrupos de um grupo* G. *Então*

$$|G : H \cap K| \leq |G : H| \cdot |G : K|.$$

Ademais, se $(|G : H|, |G : K|) = 1$, *então* $|G : H \cap K| = |G : H| \cdot |G : K|$.

1.2 Subgrupos "Clássicos"

Nesta seção definiremos alguns subgrupos especiais que serão utilizados na construção do nosso trabalho, assim consolidando a notação a ser usada no texto. Vejamos as definições:

1) Se $x, g \in G$ o conjugado de x por g será $x^g = g^{-1}xg$.

2) Se $x \in G$, a classe de conjugação de x é o subconjunto:

$$x^G = \{x^g \mid g \in G\}.$$

3) Se $x \in G$, o centralizador de x em G é o subgrupo formado pelos elementos em G que comutam com x, indicado por:

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

4) Se $H \subseteq G$, o centralizador de H em G é o subgrupo:

$$C_G(H) = \{g \in G \mid h^g = h, \ \forall\ h \in H\} = \bigcap_{h \ \in \ H} C_G(h).$$

5) O centro do grupo G é o subgrupo formado pelos elementos de G que comutam com todos os outros elementos de G e é indicado por $Z(G) = C_G(G)$.

6) Se $H \leq G$, definimos o normalizador de H em G como sendo o subgrupo

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

Note que $H \trianglelefteq N_G(H) \leq G$.

7) Se $x, y \in G$, definimos o comutador de x e y como sendo:

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

Observe que x e y comutam se, e somente se, o comutador é $[x, y] = 1$.

8) Definimos o subgrupo derivado

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

Lembrando que se $X \subset G$, o subgrupo gerado por X será:

$$\langle X \rangle = \{x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \ldots \cdot x_n^{\alpha_n} \mid n \in \mathbb{N},\ x_i \in X,\ \alpha_i = \pm 1\}.$$

9) Se $H, K \subset G$ definimos $[H, K] = \langle [h, k] \mid h \in H, k \in K \rangle$. Note que $G' = [G, G]$.

10) Um grupo K é dito ser de torção quando $o(x) < \infty, \forall\ x \in K$.

Proposição 1.2.1. *Seja G um grupo.*

a) $|x^G| = |G : C_G(x)|$.

b) (Equações das Classes) Suponhamos que G é finito. Então existem $g_1, \cdots, g_r \in G$ tais que

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

1.2.1 Teoremas de Sylow

Um dos Teoremas fundamentais da Teoria dos grupos finitos é o Teorema de Sylow que nos dá uma "recíproca" do Teorema da Lagrange.

Teorema 1.2.1. *Sejam G um grupo finito e p um primo. Escreva $|G| = p^a m$, onde o inteiro m não é divisível por p.*

(1) Todo p-subgrupo de G está contido em um subgrupo de ordem p^a. Em particular, como 1 é um p-subgrupo, p-subgrupos de Sylow sempre existem.

(2) Se n_p é o número de p-subgrupos de Sylow, $n_p \equiv 1 \mod p$.

(3) Todos os p-subgrupos de Sylow são conjugados em G.

1.3 Extensões

Definição 1.3.1. *Sejam A, B, C grupos e $f : A \longrightarrow B$ e $g : B \longrightarrow C$ homomorfismos de grupos. Se f é injetiva, g sobrejetiva e $Im(f) = Ker(g)$, a sequência*

$$1 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 1$$

é chamada de sequência exata curta. Em particular,

$$\frac{B}{Im(f)} \simeq C.$$

Exemplo 1.3.1. *Se $N \trianglelefteq G$, então*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{\pi} G/N \longrightarrow 1$$

é uma sequência exata, por

$$\begin{aligned} i \ : \ N &\longrightarrow G \\ x &\longmapsto x \end{aligned}$$

$$\begin{aligned} \pi \ : \ G &\longrightarrow G/N \\ x &\longmapsto xN \end{aligned}$$

onde i é a função inclusão e π é a projeção canônica. Nesse caso, dizemos que G é uma extensão de N por G/N.

Exemplo 1.3.2. *O grupo D_4 é extensão de C_2 por $C_2 \times C_2$.*

De fato, consideremos $D_4 = \langle a, b \mid a^4 = b^2 = 1,\ bab = a^{-1} \rangle$. Tomemos $N = \langle a^2 \rangle$. Daí, $D_4/N = \langle aN, bN \rangle \simeq C_2 \times C_2$.

Exemplo 1.3.3. *O grupo D_p é extensão de C_p por C_2.*

Com efeito, consideremos $D_p = \langle a, b \mid a^p = b^2 = 1,\ bab = a^{-1} \rangle$, com p primo. Tomemos $N = \langle a^p \rangle \simeq C_p$. Daí, $D_p/N \simeq C_2$.

Exemplo 1.3.4. *O grupo $G = \langle a, b \mid a^5 = b^4 = 1, a^b = a^{-1} \rangle$ é extensão de C_2 por D_5. Tomemos $N = \langle b^2 \rangle$. Daí, $G/N \simeq D_5$.*

Classes de Grupos

Ao longo do texto será interessante descrever certas classes de grupos a partir de extensões.

Definição 1.3.2. *Dadas duas classes de grupos* $\mathcal{X}_1$ *e* $\mathcal{X}_2$*, podemos definir a classe* $\mathcal{X}_1$*-por-*$\mathcal{X}_2$ *como sendo todos os grupos* G *nos quais existe um subgrupo normal* N *no qual* $N \in \mathcal{X}_1$ *e* $G/N \in \mathcal{X}_2$*.*

Definição 1.3.3. *Dizemos que um grupo* G *é abeliano-por-cíclico se existe um subgrupo normal de* G*, tal que* N *é abeliano e* G/N *é cíclico.*

Exemplo 1.3.5.

1. *Todos os grupos que aparecem na Proposição A são abeliano-por-cíclico.*

2. *O grupo* $A_4 = \langle (1\,2)(3\,4), (1\,3)(2\,4), (1\,2\,3) \rangle$ *é abeliano-por-cíclico.*

Definição 1.3.4. *Dizemos que um grupo* G *é policíclico-por-finito se tiver um subgrupo policíclico normal de índice finito. Ou seja, se houver um subgrupo normal de índice finito que admita uma série subnormal com fatores cíclicos.*

Definição 1.3.5. *Dizemos que um grupo* G *é central-por-finito se o índice* $|G : Z(G)|$ *é finito.*

Exemplo 1.3.6. *Todo grupo finito é central-por-finito.*

Capítulo 2

Entre Nilpotentes e Solúveis

Neste capítulo faremos um breve estudo sobre alguns resultados básicos necessários para a compreensão dos resultados principais dos capítulos posteriores. Apresentaremos algumas definições e propriedades relevantes sobre grupos cíclicos, abelianos, solúveis, nilpotentes, supersolúveis e policíclicos. O leitor interessado em mais detalhes pode consultar [2, Capítulo 7], [5, Capítulo 1], [9, Capítulo 5] e [12, Capítulo 6].

2.1 Grupos Cíclicos

Definição 2.1.1. *Seja G um grupo, dizemos que G é um grupo cíclico se G é gerado por um único elemento, isto é, se existe $a \in G$ tal que $G = \langle a \rangle$.*

Vejamos alguns exemplos de grupos cíclicos:

Exemplo 2.1.1.

1. *O grupo aditivo dos números inteiros é um grupo cíclico infinito. De fato, $\mathbb{Z}$ é gerado por 1 ou por -1 e estes são seus únicos geradores.*

2. *Para todo número inteiro n, o Grupo aditivo $\mathbb{Z}_n$ dos Inteiros módulo n é cíclico, pois $\mathbb{Z}_n = \langle \bar{1} \rangle$.*

3. *O grupo multiplicativo $\mathbb{C}^*$, tal que, $\langle i \rangle = \{i, -i, 1, -1\}$ é cíclico gerado por i.*

4. *Dado $n \geq 2$. Consideremos $C_n = \{x \mid x^n = 1\} \leq \mathbb{C}^*$.*

Observação 2.1.1. *Se G é um grupo cíclico, então o gerador de G, isto é, o elemento $a \in G$ tal que $G = \langle a \rangle$, em geral, não é único. Por exemplo, $\mathbb{Z}_4 = \langle \bar{1} \rangle$ e $\mathbb{Z}_4 = \langle \bar{3} \rangle$.*

Proposição 2.1.1. *Se G é um grupo cíclico, então todo subgrupo H de G também é cíclico.*

Proposição 2.1.2. *Seja $G = \langle x \rangle$ um grupo de ordem n. Se d é um divisor de n, então existe um único subgrupo H de G de ordem igual a d. Este subgrupo é $H = \langle a^{n/d} \rangle$.*

Proposição 2.1.3. *Temos que $C_n \times C_m$ é cíclico se, e somente se, n e m são coprimos.*

2.2 Grupos Abeliano Finito

Definição 2.2.1. *Um grupo G é chamado de grupo abeliano se a operação for comutativa, ou seja,*

$$ab = ba \text{ para todo } a, b \in G.$$

Exemplo 2.2.1.

1. $(\mathbb{Z}, +)$ *é um grupo abeliano, pois*

$$x + y = y + x, \text{ para todo } x, y \in \mathbb{Z}.$$

2. $(\mathbb{Q}^*, \cdot)$ *é um grupo abeliano, pois*

$$xy = yx, \text{ para todo } x, y \in \mathbb{Q}^*.$$

Proposição 2.2.1. *Se um grupo G é cíclico então G é abeliano.*

Observação 2.2.1. *A recíproca da Proposição 2.2.1 é falsa, ou seja, nem todo grupo abeliano é um grupo cíclico. Por exemplo, o Grupo de Klein,*

$$K = \{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

é abeliano, mas não é cíclico.

Teorema 2.2.1. *(Teorema Fundamental dos Grupos Abelianos Finitamente Gerados). Seja G um grupo abeliano finitamente gerado. Então existem únicos inteiros $\tau_1, \dots, \tau_t > 1$ e $r \geq 0$ tais que*

$$G \simeq \frac{\mathbb{Z}}{\tau_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{\tau_t\mathbb{Z}} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r \text{ vezes}}$$

sendo que $\tau_1 | \tau_2 | \cdots \tau_{t-1} | \tau_t$.

2.3 Grupos Solúveis

Nesta seção iremos estudar brevemente grupos solúveis e grupos nilpotentes. Estes grupos surgem da generalização da propriedade comutativa.

Definição 2.3.1. *Seja G um grupo. Consideremos*

$$S : 1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

Uma série para G.

1) *Dizemos que G é solúvel se cada fator G_{i+1}/G_i é abeliano, $0 \leq i \leq n-1$. (uma série com tal descrição é chamada de série abeliana).*

2) *Dizemos que G é policíclico se cada fator G_{i+1}/G_i é cíclico, $0 \leq i \leq n-1$. (uma série com tal descrição é chamada de série cíclica).*

3) Dizemos que G é nilpotente se $G_i \trianglelefteq G$ $(1 \leq i \leq n)$ e cada fator $G_{j+1}/G_j \leq Z(G/G_j)$, tal que $(0 \leq j \leq n-1)$. (uma série com tal descrição é chamada de série central).

O resultado a seguir nos mostra que os grupos solúveis é fechado para a formação de subgrupos e formação de grupos quocientes.

Proposição 2.3.1. *Sejam G um grupo, $H \leq G$ e $N \trianglelefteq G$.*

a) Se G é solúvel, então H é solúvel.

b) Se G é solúvel, então G/N é solúvel.

Demonstração. Tomemos uma série genérica para G.

$$S : 1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G.$$

a) Suponhamos que S é uma série abeliana para G, isto é, G_{i+1}/G_i é abeliano, tal que, $0 \leq i \leq n-1$. Consideremos a seguinte sequência finita de subgrupos: $\{G_i \cap H\}_{i=0}^{n}$ e seja $H_i = G_i \cap H$. Como $H_i \trianglelefteq H_{i+1}$. Assim,

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

Portanto, o grupo quociente H_{i+1}/H_i é abeliano, pois é subgrupo de um grupo abeliano. Logo, H é solúvel.

b) Suponhamos que S é uma série abeliana para G. Consideremos a seguinte sequência de subgrupos para $G/N : \{NG_i/N\}_{i=0}^{n}$. Pelo Teorema dos Isomorfismos, temos

$$\frac{(NG_{i+1})/N}{(NG_i)/N} \simeq \frac{NG_{i+1}}{NG_i}.$$

Consequentemente, $NG_i/N \trianglelefteq NG_{i+1}/N$. Mais ainda,

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

Como G_{i+1}/G_i é abeliano $(0 \leq i \leq n-1)$, segue que a sequência $\{NG_i/N\}_{i=0}^{n}$ forma uma série abeliana para G/N. Logo, G/N é solúvel.

■

Proposição 2.3.2. *Sejam N um subgrupo normal de um grupo G e H um subgrupo de G.*

a) Se N e G/N são solúveis, então G é solúvel.

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

Demonstração. a) Suponhamos que $\{N_i\}_{i=0}^{r}$ e $\{H_i/N\}_{j=0}^{s}$ são séries abelianas para N e G/N, respectivamente. Assim, $N_0 = 1, Nr = N, H_0/N = N/N, H_s = G$ e, consequentemente, N_{i+1}/N_i abeliano $(i = 0, \cdots, r)$ e $\dfrac{H_{i+1}/N}{H_i/N}$ é abeliano $(i = 0, ..., s)$. Mais ainda, cada um dos fatores, pelo Teorema dos Isomorfismos:

$$\frac{H_{i+1}/N}{H_i/N} \simeq \frac{H_{i+1}}{H_i}$$

é abeliano. Assim, $1 = N_0 \trianglelefteq \cdots \trianglelefteq N = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$ é uma série abeliana para G. Daí, G é solúvel.

b) Sem perda de generalidade suponhamos que $G = NH$. Agora, notemos que

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

é solúvel. Assim, pelo item *a*) $G = NH$ é solúvel.

■

2.3.1 Grupos Nilpotentes

Para a demonstração do Teorema 4.2.3, usaremos o fato do grupo G ser nilpotente, sendo assim indispensável o estudo dessa classe para o entendimento da presente pesquisa. Abordaremos aqui, algumas propriedades dos grupos nilpotentes.

Para conveniência do leitor, reapresentamos a definição de grupos nilpotentes.

Definição 2.3.2. *Dizemos que G é nilpotente se $G_i \trianglelefteq G$ $(1 \leq i \leq n)$ e cada fator $G_{j+1}/G_j \leq Z(G/G_j)$, tal que $(0 \leq j \leq n-1)$. (uma série com tal descrição é chamada de série central).*

Proposição 2.3.3. *Sejam n um inteiro positivo e p um primo. Suponhamos que $|G| = p^n$. Então*

a) $Z(G) \neq 1$.

b) G é nilpotente.

Observação 2.3.1. *Usando as notações da Definição 2.3.1*

i) Se G é um grupo nilpotente, então $Z(G) \neq 1$.

ii) Notemos que todo grupo nilpotente é, em particular, solúvel. Basta observar que cada fator $G_{j+1}/G_j \leq Z(G/G_j)$. Assim, cada fator G_{j+1}/G_j é abeliano $(0 \leq j \leq n-1)$.

Exemplo 2.3.1.

1. *Todo grupo abeliano é nilpotente.*

2. *Todo p-grupo finito é nilpotente.*

3. *Todo grupo nilpotente é solúvel.*

4. *Os grupos S_3, A_4 e S_4 são solúveis e não são nilpotentes. Pois, os centros dos respectivos grupos são triviais.*

5. *A_5 não é solúvel.*

Definição 2.3.3. *(Subnormalidade) Seja H um subgrupo de G. Dizemos que H é um subgrupo subnormal de G se existe uma sequência finita de subgrupos $\{H_j\}_{j=0}^{n}$, tal que*

$$H = H_0 \trianglelefteq H_1 \trianglelefteq \ldots \trianglelefteq H_n = G.$$

Notação: $H \trianglelefteq \trianglelefteq G$.

Definição 2.3.4. *Seja G um grupo. Definimos o subgrupo de Frattini como sendo*

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

Teorema 2.3.1. *(Caracterização dos Grupos Nilpotentes Finitos). Seja G um grupo finito. As seguintes afirmações são equivalentes:*

(1) G é nilpotente.

(2) Todo subgrupo de G é subnormal.

(3) Se $H < G$, então $H < N_G(H)$.

(4) Todo subgrupo maximal de G é normal e existe $p \in \pi(G)$ tal que $|G : M| = p$.

(5) Todo p-subgrupo de Sylow de G é normal.

(6) $G' \leq \Phi(G)$.

(7) O grupo G é o produto direto dos seus p-subgrupos de Sylow.

Em alguns casos é pertinente reescrever a definição de grupo nilpotente em termos de certos subgrupos comutadores.

Lema 2.3.1. *O grupo G admite uma série central $\{G_i\}_{i=0}^{n}$ se, e somente se $[G_i, G] \leq G_{i-1}$, com $1 \leq i \leq n$.*

A proposição a seguir nos mostra que as classes dos grupos nilpotentes é fechada para subgrupos e formação de grupos quocientes.

Proposição 2.3.4. *Sejam G um grupo, $H \leq G$ e $N \trianglelefteq G$.*

a) Se G é nilpotente, então H é nilpotente.

b) Se G é nilpotente, então G/N é nilpotente.

Observação 2.3.2. *Notemos que a Proposição 2.3.2, em geral, não é válida para grupos nilpotentes. Por exemplo, $N = \langle (123) \rangle \trianglelefteq S_3$, sendo que $H = \langle (1\ 2) \rangle \simeq S_3/N$ são cíclicos (portanto nilpotentes), mas $S_3 = HN$ não é nilpotente.*

2.3.2 Grupos Supersolúveis Finitos

Definição 2.3.5. *Dizemos que um grupo G é supersolúvel se existe uma série $G = G_0 \geq G_1 \geq \cdots \geq G_n = 1$, onde $G_i \trianglelefteq G$, tal que $1 \leq i \leq n$ e cada fator G_{j+1}/G_j é cíclico, tal que $0 \leq j \leq n-1$.*

Exemplo 2.3.2.

1. *O grupo $G = S_3$ é supersolúvel. Tome a série*

$$1 \overset{3}{\trianglelefteq} C_3 \overset{2}{\trianglelefteq} S_3.$$

2. *O grupo $D_p = \langle a, b \mid a^p = b^2 = 1,\ bab = a^{-1}\rangle$, com p primo é supersolúvel. Tome a série*

$$1 \overset{p}{\trianglelefteq} C_p \overset{2}{\trianglelefteq} D_p.$$

3. *O grupo $G = S_4$ não é supersolúvel. Pois,*

$$1 \overset{4}{\trianglelefteq} K \overset{3}{\trianglelefteq} A_4 \overset{2}{\trianglelefteq} S_4$$

que é a "maior" série (normal) de S_4 e K, (onde K é o grupo de Klein) não é cíclico.

Observação 2.3.3. *Os números apresentados acima do símbolo de normalidade representa o índice entre os grupos.*

Observação 2.3.4. *Todo grupo supersolúvel é solúvel mas nem todo grupo solúvel é supersolúvel.*

Por exemplo, o grupo $G = A_4$ é solúvel, pois temos a série

$$1 \overset{4}{\trianglelefteq} K \overset{3}{\trianglelefteq} A_4.$$

Dado que $\dfrac{K}{1} \simeq K \simeq C_2 \times C_2$ é abeliano e não é cíclico. Portanto, não é supersolúvel.

Veremos nas Proposições 2.3.5 e 2.3.6 que a classe de grupos supersolúveis é fechada para subgrupos, quocientes e produto direto (de um número finito de grupos).

Proposição 2.3.5. *Seja G um grupo supersolúvel finito.*

a) Se $H \leq G$, então H é supersolúvel.

b) Se $N \trianglelefteq G$, então G/N é supersolúvel.

c) Se $N \cdot\!\trianglelefteq G$, então existe um primo p tal que $|N| = p$.

d) Se $M \lessdot G$, então existe um primo p tal que $|G : M| = p$.

Demonstração.

a) Seja H um subgrupo qualquer de G. Como G é supersolúvel, então existe uma série

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

tal que $G_i \trianglelefteq G$ e G_{i+1}/G_i é cíclico para todo $i = 0, 1, \cdots, n-1$. Consideremos $H_i = H \cap G_i$. Então:

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

implicando que H_{i+1}/H_i é cíclico. Além disso, temos $H_i = H \cap G_i \trianglelefteq H$ (pois $G_i \trianglelefteq G$) para todo i. Desse modo, H é supersolúvel.

b) Considere $\bar{N}_i = NG_i/N$. Temos que $\bar{N}_i \trianglelefteq G/N$ e $\bar{N}_i \leq \bar{N}_{i+1}$ para todo i. Daí

$$\frac{\bar{N}_{i+1}}{\bar{N}_i} = \frac{NG_{i+1}/N}{NG_i/N} \simeq \frac{NG_{i+1}}{NG_i} = \frac{(NG_i)G_{i+1}}{NG_i} \simeq \frac{G_{i+1}}{(NG_i) \cap G_{i+1}} \simeq \frac{G_{i+1}/G_i}{((NG_i) \cap G_{i+1})/G_i}$$

implicando que $\dfrac{\bar{N}_{i+1}}{\bar{N}_i}$ é cíclico. Portanto, G/N é supersolúvel.

c) Seja N um subgrupo normal minimal de G. Temos que G é supersolúvel, então temos a série

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

onde $G_i \trianglelefteq G$ e G_{i+1}/G_i é cíclico. Seja k o menor inteiro tal que $G_k \cap N \neq 1$. Isto implica que $G_{k-1} \cap N = 1$. Ademais, $G_k \cap N \trianglelefteq G$ e $1 \neq G_k \cap N \leq N$ o que acarreta que $G_k \cap N = N$. No qual $N \leq G_k$. Assim,

$$N \simeq \frac{NG_{k-1}}{G_{k-1}} \leq \frac{G_k}{G_{k-1}}$$

é cíclico. Logo, $|N| = p$ para algum primo p.

d) Sabemos pelo item c) que um normal minimal N de G tem ordem $|N| = q$, para algum primo q. Façamos indução sobre $|G|$. Temos que G/N é um grupo supersolúvel de ordem $< |G|$. Dado $M \lessdot G$, pode acontecer

Caso (1): Se $N \subseteq M$, então

$$\frac{M}{N} \lessdot \frac{G}{N}.$$

Daí, $|G/N : M/N| = p$, para algum primo p. Assim, $|G : M| = |G/N : M/N| = p$.

Caso (2): Se $N \nsubseteq M$, então $G = MN$, visto que $M \lessdot G$. Como $|N| = q$ primo, segue que $N \cap M = 1$. Assim, $|G| = |G : N||N| = |M||N|$ e, consequentemente, $|G : M| = |N| = q$, primo.

■

Observação 2.3.5. *Não é verdade que se $N \trianglelefteq G$ e $\dfrac{G}{N}$ forem supersolúveis, implica que G é supersolúvel.*

Como vimos A_4 não é supersolúvel, porém K e $\dfrac{A_4}{K}$ são supersolúveis.

Proposição 2.3.6. *Sejam G, H, K grupos.*

a) Se H, K são supersolúveis e $G = H \times K$, então G é supersolúvel.

b) Se G é nilpotente finito, então G é supersolúvel.

Demonstração. a) Temos que

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H$$

e

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_m = K$$

são séries normais cíclicas para H e K, respectivamente. Para $G = H \times K$, consideremos:

$$1 \trianglelefteq H_1 \times \{1\} \trianglelefteq \cdots \trianglelefteq H_n \times \{1\} = H \times \{1\} \trianglelefteq H \times K_1 \trianglelefteq \cdots \trianglelefteq H \times K_m = H \times K = G.$$

Notemos que

$$\frac{H_{j+1} \times \{1\}}{H_j \times \{1\}} \simeq \frac{H_{j+1}}{H_j} \times \frac{\{1\}}{\{1\}} \simeq \frac{H_{j+1}}{H_j}$$

é cíclico, $0 \leq j \leq n-1$ e

$$\frac{H \times K_{j+1}}{H \times K_j} \simeq \frac{H}{H} \times \frac{K_{j+1}}{K_j} \simeq \frac{K_{j+1}}{K_{j+1}}$$

é cíclico $0 \leq j \leq m-1$. Logo, $G = H \times K$ é supersolúvel.

b) Faremos Indução sobre $|G|$. Sabemos que G com ordem p primo é cíclico e, consequentemente, supersolúvel. Suponhamos que todos os grupos nilpotentes de ordem $< |G|$ são supersolúveis.

Como G é nilpotente, temos que $Z(G) \neq 1$. Temos que existe $p \in \pi(G)$ tal que p divide $|Z(G)|$. Daí, existe $H \leq Z(G)$ tal que $|H| = p$. Em particular, $H \trianglelefteq G$. Como $|G/H|$ é nilpotente e tem ordem $< |G|$, temos que G/H é supersolúvel. Assim, existe uma série normal cíclica:

$$\frac{H}{H} = \frac{H_0}{H} \trianglelefteq \frac{H_1}{H} \trianglelefteq \cdots \trianglelefteq \frac{H_r}{H} = \frac{G}{H}.$$

Agora, como $1 \trianglelefteq H \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$ é uma série normal cíclica para G. Logo, G é supersolúvel.

∎

Proposição 2.3.7. *Sejam G um grupo finito e $p = máx\ \pi(G)$.*

a) Se todos os subgrupos maximais tem índice primo, para algum primo $q \in \pi(G)$, então $P \in Syl_p(G)$ é um subgrupo normal de G.

b) Suponhamos adicionalmente que G é supersolúvel. Então existe um subgrupo normal H de G com ordem, exatamente, p.

Demonstração. a) Consideremos P um p-grupo de Sylow de G e suponhamos que $P \ntrianglelefteq G$. Desse modo, $N_G(P)$ é um subgrupo próprio de G e, desta maneira, existe $M \lessdot G$ tal que $N_G(P) \leq M$. Por hipótese, $|G : M| = q$, para algum primo $q \in \pi(G)$. Note que P é também um p-subgrupo de Sylow do subgrupo M e temos ainda $N_M(P) = N_G(P)$. Pelo Teorema de Sylow,

$$n_p = |G : N_G(P)| \equiv 1 \pmod p \quad e\ \tilde{n}_p = |M : N_M(P)| \equiv 1 \pmod p.$$

Por outro lado, $|G : N_G(P)| = |G : M||M : N_M(P)|$ e podemos escrever $n_p = \tilde{n}_p q$. Das congruências acima, provenientes do Teorema de Sylow, concluímos que $q \equiv 1 \pmod p$. Desta forma, p divide $q-1$ e temos $p \leq q$. Absurdo, pois $p = máx\{\pi(G)\}$.

b) Pela Proposição 2.3.5 *c*) e *d*), os subgrupos maximais de um grupo supersolúvel têm índice primo e os normais minimais tem ordem prima. Daí, pelo item *a*), $P \trianglelefteq G$, sendo que $P \in Sylp(G)$. Com isso, é suficiente tomar um normal minimal N em G que esteja contido em P.

■

Lema 2.3.2. *Seja N um subgrupo normal de um grupo G. Se N é cíclico e G/N é supersolúvel, então G é supersolúvel.*

Demonstração. Se G/N é supersolúvel, por definição existe uma série normal cíclica $\{N\} = \bar{G}_0 \leq \bar{G}_1 \leq \cdots \leq \bar{G}_n = G/N$, ou seja, $\bar{G}_i \trianglelefteq G/N$, com $0 \leq i \leq n$ e G_{i+1}/G_i é cíclico para $0 \leq i \leq n$. Pelo Teorema da correspondência, para cada $i \in \{0, 1, \cdots, n\}$, existe $G_i \trianglelefteq G$ com $G_i \geq N$ tal que $\bar{G}_i = G_i/N$ e assim,

$$N = G_0 \leq G_1 \leq \cdots \leq G_n = G.$$

Pelo teorema do Isomorfismo,

$$\frac{\bar{G}_{i+1}}{\bar{G}_i} = \frac{G_{i+1}/N}{G_i/N} \simeq \frac{G_{i+1}}{G_i},$$

para $0 \leq i \leq n-1$. Logo $\dfrac{G_{i+1}}{G_i}$ é cíclico para cada $i \in \{0, 1, \cdots, n-1\}$. Assim, consideramos a série $S : \{1\} \leq N = G_0 \leq G_1 \leq \cdots \leq G_n = G$. Portanto, S é uma série normal de G, onde todos os fatores são cíclicos, isto é, G é supersolúvel. ■

2.3.3 Grupos Policíclicos: Grupos solúveis satisfazendo MÁX

Para a comodidade do leitor reapresentaremos a definição de grupo policíclico.

Definição 2.3.6. *Dizemos que um grupo é policíclico se admite uma série (subnormal) cujos fatores são cíclicos.*

Proposição 2.3.8. *Grupos policíclicos são solúvel.*

Proposição 2.3.9. *Grupos abelianos finitamente gerados são policíclicos.*

Demonstração. Seja G um grupo abeliano finitamente gerado por $a_1, a_2, \cdots, a_n$. Tomemos $G_i = \langle a_1, \ldots, a_i \rangle$, tal que, $1 \leq i \leq n+1$. Então, G_i está contido em G_{i+1} e G_i é normal em G_{i+1}, já que G é abeliano. Os quocientes G_{i+1}/G_i são gerados por a_iG_i. Portanto, G_{i+1}/G_i é cíclico e os G_i formam uma série policíclica para G. ■

Proposição 2.3.10. *Subgrupos de grupos policíclicos são policíclicos.*

Demonstração. Seja $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$ uma série policíclica para um grupo G e seja H um subgrupo de G. Definamos $H_i = G_i \cap H$. Tomemos $a \in H_i$ e $b \in H_{i+1}$, temos que $a, b \in H$, e além disso, $a \in G_i$ e $b \in G_{i+1}$. Como $G_i \trianglelefteq G_{i+1}$, segue que $b^{-1}ab \in G_i$. Logo, $H_i \trianglelefteq H_{i+1}$. Pelo Teorema dos Isomorfismos,

$$H_{i+1}/H_i = (G_{i+1} \cap H)/(G_i \cap H) = (G_{i+1} \cap H)/(G_i \cap (G_{i+1} \cap H))$$

$$H_{i+1}/H_i \simeq (G_{i+1} \cap H)G_i/G_i = H_{i+1}G_i/G_i$$

que é um subgrupo do grupo cíclico G_{i+1}/G_i. Logo, H_{i+1}/H_i é cíclico. Assim,

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_n = G$$

é uma série policíclica para H. Portanto H é policíclico. ■

As condições de finitude envolvendo cadeias (condição de cadeia ascendente e/ou descendente) são frequentes no estudo de estruturas algébricas. Nessa subseção mostraremos que os grupos solúveis satisfazendo $M\acute{A}X$ são, exatamente, os grupos policíclicos.

Definição 2.3.7. *Sejam G um grupo e $C = \{H_i\}_{i=1}^{\infty}$ um conjunto de subgrupos de*

1) Dizemos que C é uma cadeia ascendente (de subgrupos) se

$$H_1 \leq H_2 \leq H_3 \leq \cdots$$

2) Dizemos que C é uma cadeia ascendente estacionária se existir um inteiro positivo n, tal que, $H_i = H_n$, para todo $i \geq n$.

Exemplo 2.3.3.

1. *Qualquer cadeia ascendente de subgrupos em um grupo finito é estacionária.*

2. *Qualquer cadeia ascendente no grupo aditivo dos inteiros $\mathbb{Z}$ é estacionária.*

3. *Seja p um primo. O Grupo de Prüfer C_{p^∞} possui cadeias ascendentes não estacionárias.*

De fato,

1. O resultado é uma consequência do Teorema de Lagrange.

2. Como todo subgrupo H não trivial de $\mathbb{Z}$ é da forma $m\mathbb{Z}$, para algum número inteiro $m \neq 0$, segue que o índice de H em G é dado por $[\mathbb{Z} : H] = [\mathbb{Z} : m\mathbb{Z}] = m$. Segue do Teorema dos índices que toda cadeia ascendente em $\mathbb{Z}$ é estacionária.

3. É suficiente construir uma cadeia ascendente não estacionária para o Prüfer. De fato, tomemos a seguinte cadeia própria infinita: $C = \{H_i\}_{i=1}^{\infty}$ dada por

$$H_i = \{x \in \mathbb{C} | x^{p^i} = 1\}.$$

Definição 2.3.8. *Dizemos que um grupo G satisfaz condição maximal se qualquer cadeia ascendente em G é estacionária. Para simplificar a escrita: dizemos que G satisfaz MÁX.*

Definição 2.3.9. *Dizemos que um grupo G satisfaz MÁX-C se toda cadeia ascendente de subgrupos cíclicos é estacionária. Ou seja, $\{C_i\}_{i=1}^{\infty}$, sendo que $C_i \leq G$ é cíclico, $C_i \leq C_{i+1}$ para todo $i \geq 1$, temos que existe $k \in \mathbb{N}$ tal que*

$$C_n = C_k,$$

para todo $n \geq k$.

Exemplo 2.3.4.

1. *Todo grupo finito satisfaz MÁX-C.*

2. *O grupo aditivo dos inteiros $\mathbb{Z}$ satisfaz MÁX-C. Logo, todos os grupos cíclicos satisfazem MÁX-C.*

3. *Seja p um primo. O grupo de Prüfer C_{p^∞} não satisfaz MÁX-C.*

4. *O grupo $\mathbb{Q}$ não satisfaz MÁX-C.*

Lema 2.3.3. *G satisfaz MÁX se e somente se cada subgrupo de G é finitamente gerado.*

Demonstração. Por contraposição, suponhamos que existe um subgrupo H de G que não é finitamente gerado. Daí, construa a seguinte cadeia de subgrupos:

- Tomemos $1 \neq h_1 \in H_1$. Como H não é finitamente gerado, segue que

$$1 < \langle h_1 \rangle < H;$$

- Tomemos $h_2 \in H \setminus \langle h_1 \rangle$. Como H não é finitamente gerado, segue que
$$1 < \langle h_1 \rangle < \langle h_1, h_2 \rangle < H;$$
...
- Tomemos $h_{n+1} \in H \setminus \langle h_1, \cdots, h_n \rangle$. Como H não é finitamente gerado, segue que
$$\langle h_1, \cdots, h_n \rangle < h;$$
...

Assim, podemos construir uma cadeia não estacionária própria em H.

Reciprocamente, seja $H_1 \leq H_2 \leq H_3 \leq \cdots$ uma cadeia ascendente de subgrupos de G. Então
$$\bigcup_{i=1}^{\infty} H_i$$
é um subgrupo de G e, consequentemente, H é finitamente gerado. Seja $H = \langle h_1, \cdots, h_t \rangle$, com $h_j \in H_{n_j}$. Se $n = máx\{n_j | 1 \leq j \leq t\}$, então $h_i \in H_n$ para todo $i \in \{1, \cdots, t\}$ e temos $H_n = H$. Logo, $H_n = H_{n+1} = \cdots = H$. ■

Lema 2.3.4. *Seja K um subgrupo normal de G. Então G satisfaz MÁX-C se, e somente se, K e G/K satisfazem MÁX-C.*

Demonstração. Temos por hipótese que K é um subgrupo de G, segue que todos os subgrupos de K são finitamente gerados, logo K satisfaz *MÁX-C*. Agora, vamos mostrar que todos os subgrupos de G/K são finitamente gerados. Tomemos arbitrariamente $\bar{N} \leq G/K$, assim, temos pelo Teorema da Correspondência, um subgrupo $N \leq G$ tal que $\bar{N} = N/K$. Como N é subgrupo de G, temos que N é finitamente gerado, e consequentemente, $\bar{N}$ é finitamente gerado. Como a escolha foi arbitrária, temos que G/K satisfaz *MÁX-C*.

Agora, dada $C_1 \leq C_2 \leq C_3 \leq \cdots$ uma cadeia ascendente de subgrupos cíclicos em G. Como K e G/K satisfazem *MÁX-C*, temos que existe um número inteiro positivo n de tal sorte que
$$C_j \cap K = C_n \cap K \text{ e } C_jK = C_nK,$$
para todo $j \geq n$. Seja $\{A_i\}_{i=1}^{\infty}$ tal que $A_i = C_i \cap K$ e $\{B_i\}_{i=1}^{\infty}$ tal que $B_i = C_iK$, dado $i \geq n$, usando as igualdades acima e a Lei de Dedekind temos,
$$C_i = C_i \cap (C_iK) = C_i \cap (C_nK) = C_n(C_i \cap K) = C_n(C_n \cap K) = C_n.$$
Portanto, a cadeia acima é estacionária e concluímos a prova. ■

Corolário 2.3.1. *Todo grupo policíclico satisfaz MÁX-C.*

Demonstração. Seja G um grupo policíclico. Temos que G admite uma série (subnormal) cíclica. Pelo Lema 2.3.4, G satisfaz *MÁX-C*. ■

Agora, vamos estudar grupos solúveis que satisfazem *MÁX-C*. Primeiro vamos caracterizar grupos abelianos que satisfazem *MÁX-C*.

Lema 2.3.5. *Seja A um grupo abeliano. Então A é policíclico se, e somente se, A satisfaz MÁX-C.*

Demonstração. $(\Longrightarrow)$: Segue do Corolário 2.3.1.

$(\Longleftarrow)$: Temos que A é finitamente gerado. Assim, $A = \langle a_1, \cdots, a_n \rangle$. É suficiente considerar a série:

$$1 \trianglelefteq \langle a_1 \rangle \trianglelefteq \langle a_1, a_2 \rangle \trianglelefteq \cdots \trianglelefteq \langle a_1, \cdots, a_n \rangle.$$

Daí, A é policíclico. ■

Proposição 2.3.11. *Seja G um grupo solúvel. Então G satisfaz MÁX-C se, e somente se, G é policíclico.*

Demonstração. $(\Longrightarrow)$: Faremos a nossa prova por indução sobre o comprimento derivado $\mathrm{dl}(G)$. Temos que o resultado é válido se $\mathrm{dl}(G) = 1$, pois G é abeliano e o resultado segue do Lema 2.3.5. Agora, suponhamos que todos os grupo solúveis que satisfazem *MÁX-C* com comprimento derivado $\leq d - 1$ são policíclicos. Dado G um grupo solúvel com $\mathrm{dl}(G)$. Temos que G/G' é abeliano e $\mathrm{dl}(G') \leq d - 1$. Assim, ambos são policíclicos. Assim, podemos construir duas séries cujos fatores são cíclicos

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G'$$

e

$$\frac{G'}{G'} = \frac{K_0}{G'} \trianglelefteq \frac{K_1}{G'} \trianglelefteq \frac{K_2}{G'} \trianglelefteq \cdots \trianglelefteq \frac{K_m}{G'} = \frac{G}{G'}.$$

Agora, ajustando ambas as séries, obtemos uma nova série com cíclica para G:

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G' = K_0 \trianglelefteq K_1 \trianglelefteq \cdots \trianglelefteq K_m = G.$$

$(\Longleftarrow)$: Segue do Corolário 2.3.1. ■

2.3.4 Comparando as Classes de Grupos

Consideremos as seguintes classes dos grupos finitos:

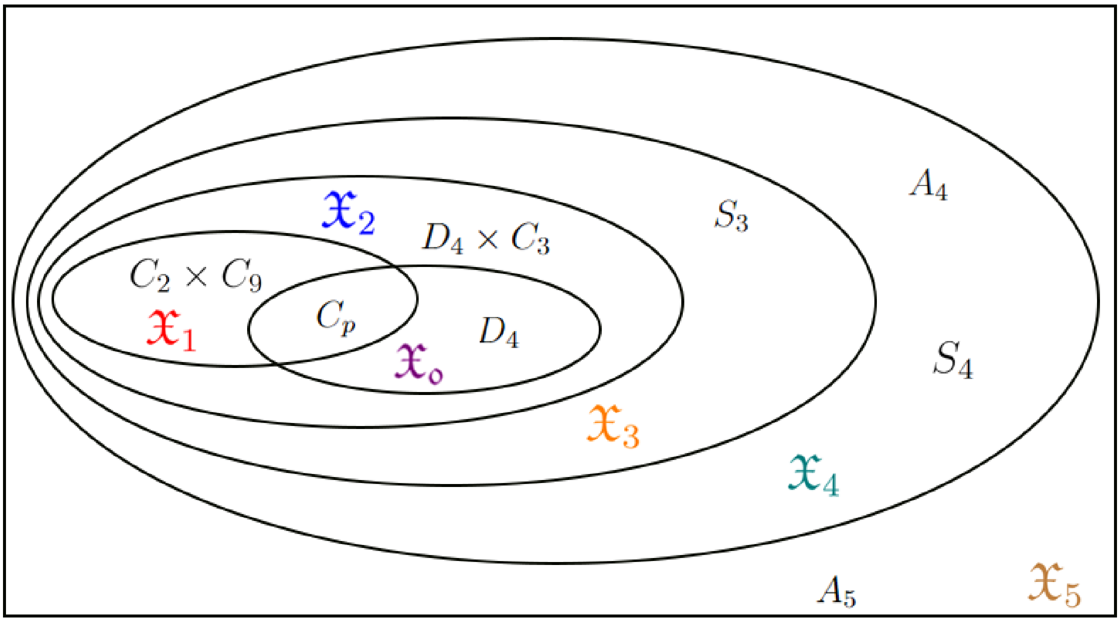
- $\mathfrak{X}_0$ = classe dos p-grupos finitos.
- $\mathfrak{X}_1$ = classe dos grupos abelianos finitos.
- $\mathfrak{X}_2$ = classe dos grupos nilpotentes finitos.
- $\mathfrak{X}_3$ = classe dos grupos supersolúveis finitos.
- $\mathfrak{X}_4$ = classe dos grupos solúveis finitos.
- $\mathfrak{X}_5$ = classe dos grupos finitos.

Daí, podemos expressar as seguintes inclusões entre as classes envolvidas:

- $\mathfrak{X}_o \subset \mathfrak{X}_2$.
- $\mathfrak{X}_1 \subset \mathfrak{X}_2 \subset \mathfrak{X}_3 \subset \mathfrak{X}_4 \subset \mathfrak{X}_5$.

Vejamos as relações das classes dos grupos na figura 2.1.

Figura 2.1: Comparando Classes de Grupos 1



Fonte: Autoria Própria

No diagrama acima evidenciamos alguns grupos que pertencem a uma dada classe e não à outra. Vejamos:

- S_3 é solúvel e não nilpotente.
- D_4 é um p-grupo nilpotente e não é abeliano.
- S_3 é supersolúvel e não é nilpotente.
- A_4 é solúvel e não é supersolúvel.
- $D_4 \times C_3$ é nilpotente e não é p-grupo.
- A_5 é um grupo finito não solúvel.

Capítulo 3

Grupos Finitos com um Subgrupo (Maximal) Abeliano

Neste capítulo investigaremos a propriedades de um grupo finito a partir da estrutura dos seus subgrupos maximais. O Capítulo é dividido em três seções. Na primeira delas, 3.1 apresentaremos uma classificação de p-grupos finitos que possuem um subgrupo cíclico que é maximal. Utilizaremos fortemente este resultado para provarmos o Teorema 4.2.1 (veja Capítulo 4). Na segunda seção, 3.2 deste capítulo apresentando um teorema de caracterização de grupos finitos que possuem um subgrupo abeliano e maximal. Usaremos tais resultados no capítulo 4. Finalizaremos obtendo características de um dado grupo supondo somente a existência de um subgrupo normal abeliano. Para o estudo deste capítulo usaremos como base os textos [11] e [9, Capítulo 5].

3.1 p-Grupos com um Subgrupos Maximais Cíclicos

Antes do nosso primeiro resultado principal incluímos o seguinte fato elementar. Sua demonstração será incluída para conveniência do leitor.

Lema 3.1.1. *Sejam $m \in \mathbb{N}$ e x, y elementos em um grupo G nilpotente de classe ≤ 2. Então*

$$(xy)^m = x^m y^m [y, x]^{\binom{m}{2}}.$$

Demonstração. Faremos indução sobre m. Primeiramente vamos mostrar que $[y^m, x] = [y, x]^m$. Para $m = 1$ é imediato. Suponhamos que a identidade seja válida para algum m. Assim,

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

Agora, voltaremos a nossa demonstração. Prosseguiremos novamente com indução sobre m. Temos que é válido para $m = 1$. Suponhamos que o resultado seja válido para algum m, lembrando que cada $[x, y] \in Z(G)$, temos que $y^m x = [y, x]^m x y^m$. Logo,

$$\begin{aligned}
(xy)^{m+1} &= (xy)^m xy = x^m y^m [y,x]^{\binom{m}{2}} xy \\
&= x^m (y^m x) y [y,x]^{\binom{m}{2}} = x^m [y,x]^m x y^m y [y,x]^{\binom{m}{2}} \\
&= x^m x y^m y [y,x]^m [y,x]^{\binom{m}{2}} = x^{m+1} y^{m+1} [y,x]^{m+\binom{m}{2}} \\
&= x^{m+1} y^{m+1} [y,x]^{\binom{m+1}{2}}
\end{aligned}$$

uma vez que $\binom{m+1}{2} = \binom{m}{2} + m$. ■

O seguinte resultado aparece na Introdução com o nome de **Proposição A**.

Proposição 3.1.1. *Um grupo de ordem p^n tem um subgrupo maximal cíclico se, e somente se, for de um dos seguintes tipo:*

a) Um grupo cíclico de ordem p^n.

b) O produto direto de um grupo cíclico de ordem p^{n-1} e o outro de ordem p.

c) $\langle x, a \mid x^p = 1 = a^{p^{n-1}},\ a^x = a^{1+p^{n-2}} \rangle$, $n \geq 3$.

d) O grupo diedral $D_{2^n}, n \geq 3$.

e) O grupo quatérnion generalizado $Q_{2^n}, n \geq 3$.

f) O grupo semidiedral $\langle x, a \mid x^2 = 1 = a^{2^{n-1}},\ a^x = a^{2^{n-2}-1} \rangle$, $n \geq 3$.

Demonstração. Seja $G = p^n$. Suponhamos que $N = \langle a \rangle$ é um subgrupo maximal cíclico de G, assim N é normal em G e $|G : N| = p$. Agora, seja $G/N = \langle xN \rangle$, temos que $G = \langle x, a \rangle$, daí $|a| = p^{n-1}$ e $x^p \in N$. Se G é abeliano e $x^p = b^p$, tal que $b \in N$, então $(xb^{-1})^p = 1$ e $G = \langle xb^{-1} \rangle \times N$, caso contrário $x^p = a^i$ onde $(i, p) = 1$, e $G = \langle x \rangle$. Assim, se G é abeliano é do tipo a) ou b).

Suponhamos que G é não abeliano, daí $n > 2$.

O elemento x induz um automorfismo em N que deve ter ordem p, daí $a^x = a^m$ onde $m^p \equiv 1 \bmod p^{n-1}$ e $1 < m < p^{n-1}$. Agora, pelo Teorema de Fermat $m^{p-1} \equiv 1 \bmod p$, então segue que $m \equiv 1 \bmod p$.

Por enquanto vamos assumir que p é ímpar. Consideremos $m = 1 + kp^i$ onde $(p, k) = 1$ e $0 < i < n - 1$. Agora,

$$m^p = (1 + kp^i)^p = 1 + kp^{i+1} + \frac{p-1}{2} k^2 p^{2i+1} + \frac{(p-1)(p-2)}{6} k^3 p^{3i+1} + \cdots ,$$

o que mostra que $m^p \equiv 1 + kp^{i+1} \bmod p^{i+2}$. Mas $m^p \equiv 1 \bmod p^{n-1}$ de modo que $kp^{i+1} + lp^{i+2} = l'p^{n-1}$ com l e l' inteiros. Como $i + 1 \leq n - 1$ e $(p, k) = 1$, segue-se que $i + 1 = n - 1$ e $i = n - 2$. Portanto $m = 1 + kp^{n-2}$. Agora existe um k' tal que $kk' \equiv 1 \bmod p$ e $a^{x^{k'}} = a^{(1+kp^{n-2})^{k'}} = a^{1+p^{n-2}}$, indicando que podemos substituir x por $x^{k'}$ e assumir que $m = 1 + p^{n-2}$. Resta discutir a posição de x^p em N. Agora $(x^p)^x = x^p$ implicando que $|x^p|$ divide p^{n-2} e $x^p \in \langle a^p \rangle$, digamos $x^p = b^p$ onde $b \in N$. Também G

é nilpotente de classe 2 desde $[a, x] = a^{p^{n-2}}$. Portanto, $(xb^{-1})^p = x^p b^{-p} = 1$ pelo Lema 3.1.1 já que $[b^{-1}, x]^p = 1$. Substituindo x por xb^{-1}, podemos supor que $x^p = 1$, de modo que que G é do tipo c).

De agora em diante seja $p = 2$. Certamente m é ímpar, igual a $2k+1$. De $m^2 \equiv 1 \bmod 2^{n-1}$, segue que $k(k+1) \equiv 0 \bmod 2^{n-3}$ e $k \equiv 0$ ou $-1 \bmod 2^{n-3}$. Existem, portanto, duas formas possíveis: $m = 2^{n-2}l + 1$, onde l é ímpar e $m = 2^{n-2}l - 1$. No primeiro caso, substituindo x por uma potência adequada, podemos supor que $m = 2^{n-2} + 1$, enquanto no segundo l é par e podemos tomar $m = 2^{n-1} - 1$ ou l é ímpar e podemos tomar $m = 2^{n-2} - 1$. Há portanto, três casos a examinar.

Suponhamos que $m = 2^{n-1} - 1$, de modo que $a^x = a^{-1}$. Como $(x^2)^x = x^2$, o elemento x^2 tem ordem 1 ou 2 em N, o que mostra que $x^2 = 1$ ou a^{2n-2} e $G \simeq D_{2^n}$ ou $G \simeq Q_{2^n}$ respectivamente. Agora, assuma que $m = 2^{n-2} + 1$. Como x^2 não pode gerar N, temos $x^2 = a^{2r}$ para algum r. Definindo $b = a^{r(2^{n-3}-1)}$, calculamos que

$$(xb)^2 = x^2 b^2 [b, x] = a^{2r} a^{r(2^{n-2}-2)} a^{r(2^{n-3}-1)2^{n-2}} = a^{r2^{2n-5}}.$$

Se $n \geq 4$ esta potência de a é igual a 1 e G é do tipo (c). No entanto, se $n = 3$, então $a^x = a^{-1}$ e $x^2 = 1$ ou a^2, de modo que $G \simeq D_8$ ou Q_8.

Finalmente, seja $m = 2^{n-2} - 1$. Se $x^2 = a^{2r}$, então $a^{2r} = (a^{2r})^x = a^{2r(2^{n-2}-1)}$, caso em que $2r \equiv 0 \bmod 2^{n-2}$ e $x^2 = 1$ ou a^{2n-2}. Se $x \neq 1$, então $(xa^{-1})^2 = a^{2^{n-2}} a^{-2} a^{-(2^{n-2}-2)} = 1$ e G é do tipo f). ∎

3.2 Grupos com um Subgrupo Maximal Abeliano

Na demonstração do teorema principal desta seção usaremos o Teorema de Frobenius-Thompson, para isso faremos uma breve síntese sobre os Grupos de Frobenius que serão importantes na demonstração do Teorema de Herstein.

Definição 3.2.1. *(Grupo de Frobenius) Seja H um subgrupo de G. Dizemos que G é um grupo de Frobenius com respeito ao subgrupo H se $H \cap H^x = \{1\}$ para todo $x \in G \setminus H$.*

Definição 3.2.2. *Seja G um grupo de Frobenius com respeito ao subgrupo H. Definimos o núcleo de Frobenius de G por*

$$M := G \setminus \bigcup_{x \in G} (H \setminus 1)^x$$

onde M um subconjunto normal de G tal que $G = HM$ e $H \cap M = 1$. Além disso, dizemos que H é o complemento de Frobenius de G.

Exemplo 3.2.1.

1. *O grupo $A_4 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 2\ 3) \rangle$ é grupo de Frobenius, com $H = \langle (1\ 2\ 3) \rangle$ e $M = K$, onde K é o grupo de Klein.*

2. *O grupo $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3)\}$ é grupo de Frobenius, com $H = \langle (1\ 2) \rangle$ e $M = \langle (1\ 2\ 3) \rangle$.*

3. *Consideremos o grupo $D_4 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$. Note que D_4 não é um grupo de Frobenius com relação a nenhum de seus subgrupos pois as suas duas cópias do grupo de Klein e o cíclico de ordem 4 são normais em D_4 e as cinco cópias de C_2 são subnormais em D_4. Em geral, o grupo diedral D_n é um grupo de Frobenius se, e somente se, n é ímpar.*

Proposição 3.2.1. *Seja G um grupo de Frobenius finito com complemento H e o núcleo M. Denotemos $|G : H| = n$, então*

a) *$N_G(H) = H$ e H possui n conjugados em G.*

b) *M é um subconjunto normal de G com $|M| = n$.*

c) *$C_M(h) = \{1\}, \forall\, h \in H \setminus \{1\}$.*

d) *$C_H(m) = \{1\}, \forall\, m \in M \setminus \{1\}$.*

e) *$C_G(m) \subset M, \forall\, m \in M \setminus \{1\}$.*

f) *$Z(G) = \{1\}$.*

g) *$|H|$ divide $n - 1$ e em particular $mdc(|H|, n) = 1$.*

O Teorema a seguir é bastante importante e profundo e sua demonstração foge dos nossos objetivos imediatos. A demonstração pode ser consultada em [9, 8.5.5 Capítulo 8 e 10.5.6 Capítulo 10].

Teorema 3.2.1. *(Frobenius-Thompson). Seja G um grupo finito de Frobenius com complemento H e núcleo K. Então K é um subgrupo nilpotente.*

O Teorema a seguir corresponde ao Teorema B da Introdução.

Teorema 3.2.2. *(Herstein) Seja G um grupo finito admitindo um subgrupo maximal abeliano H. Então G é solúvel.*

Demonstração. Temos que $H \leq N_G(H) \leq G$. A nossa prova será dividida em dois casos.

1) Se $N_G(H) > H$. Então $N_G(H) = G$, pela maximalidade de H. Logo, $H \trianglelefteq G$ e G/H é de ordem prima (pela maximalidade de H). Portanto, G/H é cíclico e em particular G/H é solúvel, como H é abeliano, também é solúvel. Daí G é solúvel.

2) Se $N_G(H) = H$.

2.1) Consideremos $W_x = H \cap H^x \neq \{1\}$, para $x \in G \setminus H$. Faremos indução sobre a ordem de G. Tomemos $w \in W_x \setminus \{1\}$ e defina $A := C_G(w) \supset H$. Como $x \notin H = N_G(H)$, então $H \neq H^x$. Note também que como $w \in W_x$, temos que $w = c^x$, tal que $c \in H$ e dado $h^x \in H^x$, temos $h^x w = h^x c^x = x^{-1}hcx = x^{-1}chx = c^x h^x = wh^x$, ou seja, $h^x \in C_G(w)$. Assim, $H^x \leq C_G(w) = A \supset H$. Portanto, $C_G(w) = A = G$, o que implica que w está no centro de G. Logo, $\langle w \rangle \trianglelefteq G$. Portanto, $H/\langle w \rangle$ é um maximal em $G/\langle w \rangle$. Assim, $H/\langle w \rangle$ é abeliano. Note ainda que $|G/\langle w \rangle| < |G|$, pela nossa hipótese $G/\langle w \rangle$ é solúvel e G também é solúvel.

2.2) Agora, seja $W_x = H \cap H^x = \{1\}$, para $x \in G \setminus H$. Nestas condições estamos na hipótese de G ser um grupo de Frobenius. Seja K o núcleo de Frobenius de G. Assim, Pelo Teorema de Frobenius-Thompson, temos que $K \trianglelefteq G$ e $G = KH$ e K é nilpotente, e em particular, K é solúvel, e como H é abeliano, logo solúvel segue que G é solúvel.

■

3.3 Grupos Abeliano-por-cíclico

A existência de um subgrupo normal abeliano pode influenciar bastante a estrutura de um grupo. Aqui nos ocuparemos de uma importante subclasse dos grupos solúveis chamados de grupos "abeliano-por-cíclico" (veja a seção 1.3 de Extensões no Capítulo 1).

O resultado a seguir descreve propriedades do subgrupo derivado e a ordem de um grupo abeliano-por-finito.

Teorema 3.3.1. *Sejam G um grupo e A um subgrupo normal abeliano de G. Suponhamos que existe $x \in G$, tal que $G/A = \langle Ax \rangle$. Então*

(1) (Spiegel) $\{[a,x] \mid a \in A\} \leq G$.

(2) $G' = \{\ [a,x]\ \mid\ a \in A\}$.

(3) A aplicação

$$\begin{aligned} \Gamma : A &\longrightarrow G' \\ a &\longmapsto [a,x] \end{aligned}$$

é um epimorfismo.

(4) O $\ker(\Gamma) = A \cap Z(G)$. Em particular,

$$\frac{A}{A \cap Z(G)} \simeq G'.$$

(5) Seja A um subgrupo maximal de um p-grupo não abeliano G. Suponhamos que A é abeliano. Então

(5.1) $Z(G) \leq A$.

(5.2) $|G| = p \cdot |Z(G)| \cdot |G'|$.

Demonstração. (1) Denotamos $H = \{[a,x] \mid a \in A\}$. Com efeito,

- Temos que $H \neq \emptyset$, pois $[a,x] \in H$.
- Existe elemento neutro: basta considerar $1 = [1,x]$.

- Existe elemento inverso para cada elemento $[a, x]$: de fato,

$$[a, x]^{-1} = [a^{-1}, x] \in H.$$

Com isso, concluímos que $H \leq G$.

(2) É suficiente mostrarmos que cada conjugado de $[a, x]$ é ainda um elemento de H. Com efeito, dado $g \in G$: existem $a_1 \in A$ e $i \in \mathbb{Z}$ tais que $g = a_1 x^i$. Daí,

$$[a, x]^g = [a, x]^{a_1 x^i} = \left([a, x]^{a_1}\right)^{x^i} = [a, x]^{x^i} = [a^{x^i}, x^{x^i}] = [\tilde{a}, x] \in H,$$

para algum $\tilde{a} \in A$. Agora, vejamos que $G' = H$. De fato, é suficiente mostrarmos que $[x, y] \in H$, pois $H \leq G'$. Dados $x, y \in G$, tomemos $x = a_1 x^i$ e $y = a_2 x^j$. Temos que

$$\begin{aligned}
[x, y] &= [a_1 x^i, a_2 x^j] \\
&= [a_1, a_2 x^j]^{x^i} [x^i, a_2 x^j] \\
&= ([a_1, x^j][a_1, a_2]^{x^j})[x^i, x^j][x^i, a_2] \\
&= [a_1, x^j][x^i, a_2] \in H. \\
&= [a_1, x^j][a_2, x^i]^{-1} \in H.
\end{aligned}$$

Portanto, $G' = \{\ [a, x] \mid a \in A\}$.

(3) Por construção temos que Γ é sobrejetiva. Vamos mostrar que a aplicação de fato é um epimorfismo. Dados $a, a_1 \in A$, temos

$$\begin{aligned}
\Gamma(a a_1) &= [a a_1, x] \\
&= [a, x]^{a_1} [a_1, x] \\
&= [a, x][a_1, x] \\
&= \Gamma(a) \cdot \Gamma(a_1).
\end{aligned}$$

(4) Por construção $\ker(\Gamma) \leq A$. Agora, tomemos $\alpha \in \ker(\Gamma)$. Daí,

$$[\alpha, x] = 1.$$

Logo, $x \in C_G(\alpha)$ e consequentemente, $\alpha \in Z(G)$. Portanto, $\ker(\Gamma) \leq A \cap Z(G)$.

Por outro lado, se $\tilde{a} \in A \cap Z(G)$, então $\Gamma(\tilde{a}) = [\tilde{a}, x] = 1$. Logo, $\tilde{a} \in \ker(\Gamma)$. Portanto, $\ker(\Gamma) = A \cap Z(G)$. Finalmente, pelo Teorema do Isomorfismo

$$\frac{A}{A \cap Z(G)} \simeq G'.$$

(5.1) Suponhamos que $Z(G) \nleq A$. Com isso, pela maximalidade de A, temos que $G = AZ(G)$. Notemos que $C_G(A) = G$ se, e somente se, $A \leq Z(G)$. Assim, $Z(G) = G$. De fato, temos que $A \leq C_G(A)$ e $Z(G) \leq C_G(A)$. Logo, $G = AZ(G) \leq C_G(A) \leq G$. Temos que $C_G(A) = G$. Assim, $A \leq Z(G)$. Portanto, $AZ(G) = Z(G) = G$, um absurdo.

(5.2) Pelo item anterior, $Z(G) \leq A$. Daí, pelo Teorema dos Índices temos que

$$\begin{aligned}|G| &= |G : A| \cdot |A| \\ &= |G : A| \cdot |A : A \cap Z(G)| \cdot |A \cap Z(G)| \\ &= p \cdot |G'| \cdot |Z(G)|.\end{aligned}$$

■

Observação 3.3.1. *i) O item (5.2) exprime um fenômeno que ocorre para todos os grupos da Proposição A. Por outro lado, existem grupos que não estão contemplados na Proposição A cuja ordem pode ser expressa em termos da mesma expressão (por exemplo, A_4).*

ii) O item (2) do Teorema anterior é um caso particular do resultado [14, Teorema B].

Exemplo 3.3.1.

1. *Seja $n \geq 3$. Considere o grupo $G = S_n$. Temos que $|Z(G)| = 1$ e $|G'| = |A_n| = n!/2$. Daí,*
$$n! = |G| = 2 \cdot |Z(G)| \cdot |G'|.$$

2. *Tome o grupo $G = A_4$. Temos que $|Z(G)| = 1$, $|G'| = 4$. Daí,*
$$12 = |G| = 3 \cdot |Z(G)| \cdot |G'|.$$

3. *Seja o grupo $G = D_{2^n}$. Temos que $|Z(G)| = 2$, $|G'| = 2^{n-2}$. Daí,*
$$2^n = |G| = 2 \cdot |Z(G)| \cdot |G'|.$$

4. *Considere o grupo $G = Q_{2^n}$. Temos que $|Z(G)| = 2$, $|G'| = 2^{n-2}$. Daí,*
$$2^n = |G| = 2 \cdot |Z(G)| \cdot |G'|.$$

Considerações Finais do Capítulo 3

Impor restrições sobre os subgrupos maximais é um procedimento padrão em Teoria dos Grupos. Um resultado bem conhecido nessa direção é o Teorema de Schmidt que caracteriza grupos finitos nos quais todos os subgrupos maximais são nilpotentes e o grupo em si não é (veja [9, Teorema 9.1.9]). Nesse capítulo estamos assumindo que certos subgrupos maximais são abeliano (ou cíclico). Pensando nessa direção parece razoável destacar os seguintes fatos/teoremas:

i) Existem grupos não solúveis nos quais todos os seus subgrupos maximais são solúveis. Por exemplo, $G = A_5$ é um grupo não solúvel e todos os seus subgrupos maximais são solúveis.

ii) Um famoso Teorema devido a Thompson assegura que se G é um grupo finito com um subgrupo maximal M nilpotente de ordem ímpar, então G é, necessariamente, solúvel.

Observação 3.3.2. *A hipótese de M ser ímpar no item ii) é essencial, por exemplo, $G \simeq PSL(2, 17)$.*

Em conexão com o Teorema 3.3.1 (5.2) é possível verificar que "muitos" grupos solúveis (e não solúveis) satisfazem a expressão para a ordem em termos de $|Z(G)|$ e $|G'|$. Parece aceitável a seguinte questão:

Questão 3.3.1. *Caracterizar todos os grupos solúveis finitos G tais que sua ordem é dada por:*

$$|G| = p \cdot |Z(G)| \cdot |G'|,$$

para algum p.

Capítulo 4

$\mathcal{M}_c$-grupos Finitos

Agora, estamos interessados em investigar a estrutura de grupos que são $\mathcal{M}_c$-grupos. Primeiramente, estabeleceremos algumas propriedades gerais de grupos com tal propriedade e classificaremos o caso finito. Neste capítulo usamos como principal referência [13].

4.1 Propriedades e Exemplos de $\mathcal{M}_c$-grupos

Definição 4.1.1. *Sejam G um grupo e M um subgrupo cíclico de G. O subgrupo M é chamado cíclico maximal se para todo $H < G$ cíclico tal que $M \leq H$, temos $M = H$. Notação: $M \lessdot_c G$.*

Nesta seção os seguintes grupos D_4, S_3, Q_8, D_p, K, A_4 e S_4 e denotam os grupos:

- $D_4 = \langle a, b \mid a^4 = b^2 = 1,\ bab = a^{-1} \rangle$;
- $S_3 = \langle a, b \mid a^3 = b^2 = 1,\ bab = a^{-1} \rangle$;
- $Q_8 = \langle a, b \mid a^4 = 1, b^2 = a^2,\ bab^{-1} = a^{-1} \rangle$;
- $D_p = \langle a, b \mid a^p = b^2 = 1,\ bab = a^{-1} \rangle$, com p primo;
- $K = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$;
- $A_4 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 2\ 3) \rangle$;
- $S_4 = \langle (1\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 2\ 3), (1\ 2\ 3\ 4) \rangle$.

Na tabela a seguir, temos os subgrupos maximais e subgrupos cíclicos maximais dos respectivos grupos.

Tabela 4.1: Subgrupos Maximais e Cíclicos Maximais

Grupo	Subgrupos Maximais	Subgrupos Cíclicos Maximais
D_4	$\langle a\rangle$, $\langle a^2, b\rangle$ e $\langle ba, a^2\rangle$	$\langle a\rangle$, $\langle b\rangle$, $\langle ba\rangle$, $\langle ba^2\rangle$ e $\langle ba^3\rangle$
S_3	$\langle a\rangle$, $\langle b\rangle$, $\langle ab\rangle$ e $\langle a^2b\rangle$	$\langle a\rangle$, $\langle b\rangle$, $\langle ab\rangle$ e $\langle a^2b\rangle$
Q_8	$\langle a\rangle$, $\langle b\rangle$ e $\langle ab\rangle$	$\langle a\rangle$, $\langle b\rangle$ e $\langle ab\rangle$
D_p	$\langle a\rangle$, $\langle ba^i\rangle$, $i \in \{1, \cdots, p\}$	$\langle a\rangle$, $\langle ba^i\rangle$, $i \in \{1, \cdots, p\}$
K	$\langle(1\,2)(3\,4)\rangle$, $\langle(1\,3)(2\,4)\rangle$ e $\langle(1\,4)(2\,3)\rangle$	$\langle(1\,2)(3\,4)\rangle$, $\langle(1\,3)(2\,4)\rangle$ e $\langle(1\,4)(2\,3)\rangle$
A_4	$\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle$ e K	$\langle(1\ 2\ 3)\rangle, \langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle$, $\langle(1\,2)(3\,4)\rangle$, $\langle(1\,3)(2\,4)\rangle$ e $\langle(1\,4)(2\,3)\rangle$
S_4	D_4, S_3 *e* A_4	$\langle(1\ 2)\rangle$, $\langle(1\ 2\ 3)\rangle$ e $\langle(1\ 4\ 2\ 3)\rangle$

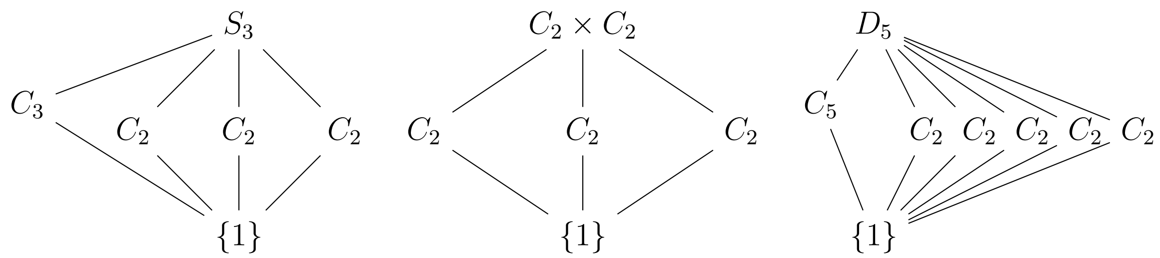
Fonte: Autoria Própria

Definição 4.1.2. *Dizemos que um grupo G é um $\mathcal{M}_c$-grupo se, e somente se, as seguintes duas condições são satisfeitas:*

1) Todo subgrupo cíclico maximal é maximal em G.

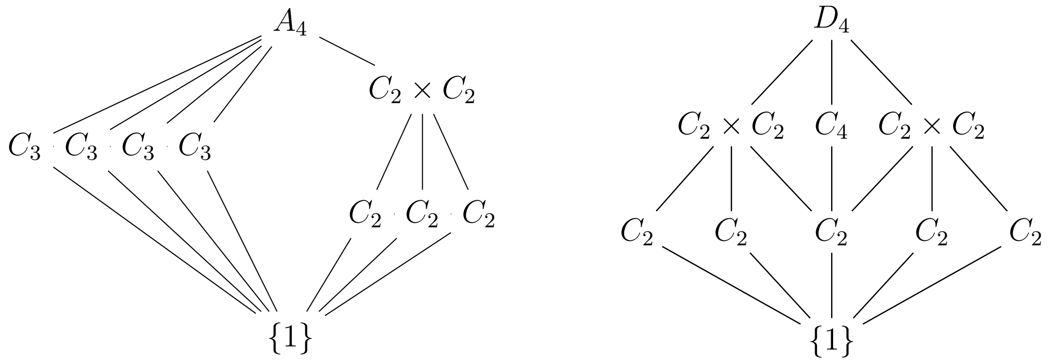
2) G contém pelo menos um subgrupo cíclico maximal próprio.

Exemplo 4.1.1. *Os grupos S_3, Q_8, K e D_p são $\mathcal{M}_c$-grupos.*



Fonte: Autoria Própria

Exemplo 4.1.2. *Os grupos D_4, A_4 e S_4 não são $\mathcal{M}_c$-grupos.*



Fonte: Autoria Própria

Lema 4.1.1. *Se G é um $\mathcal{M}_c$-grupo, então G é 2-gerado.*

Demonstração. Tomemos C cíclico maximal (que é maximal em G). Daí,

$$G = \langle C, y \rangle,$$

$\forall\ y \in G \backslash C$. Portanto, G é 2-gerado. ■

Observação 4.1.1. *Em geral, a recíproca do Lema 4.1.1 é falsa. Por exemplo, $G = D_4$ é 2-gerado, porém não é $\mathcal{M}_c$-grupos.*

Lema 4.1.2. *Sejam G um $\mathcal{M}_c$-grupo e $N \trianglelefteq G$. Suponha que G satisfaz uma das seguintes condições:*

(1) G tem MÁX-C.

(2) G/N é finito.

Então G/N é um $\mathcal{M}_c$-grupo. Ademais, se G é finito, então é solúvel.

Demonstração. (1) A nossa demonstração será feita por contradição. Suponhamos primeiramente que G tem *MÁX-C*. Agora, vamos definir $\bar{G} := G/N$ e seja^{-}: $G \to \bar{G}$ a projeção canônica. Tome $x \in G$ onde $\langle \bar{x} \rangle$ é um subgrupo cíclico maximal, ou seja, $\langle \bar{x} \rangle \lessdot_c \bar{G}$ mas $\langle \bar{x} \rangle$ não é maximal em $\bar{G}$. Logo, existe z arbitrário em G tal que $\langle \bar{x} \rangle < \langle \bar{x}, \bar{z} \rangle \neq \bar{G}$. Por hipótese, temos que G é um $\mathcal{M}_c$-grupo então podemos escolher y, arbitrário em G de modo que $x \in \langle y \rangle \lessdot G$. Mas, temos que $\langle \bar{x} \rangle \lessdot_c \bar{G}$, logo $\langle \bar{y} \rangle = \langle \bar{x} \rangle$ e consequentemente $\bar{z} \notin \langle \bar{y} \rangle$. Assim, temos que $G = \langle y, z \rangle$ e logo $\bar{G} = \langle \bar{y}, \bar{z} \rangle$, o que é uma contradição. Portanto, $\langle \bar{x} \rangle \lessdot \bar{G}$.

(2) Suponhamos que G/N é finito e tome z arbitrário em G, onde $\langle z \rangle$ é um subgrupo cíclico maximal de G, ou seja, $\langle z \rangle \lessdot_c G$. Observamos que se $N \nleq \langle z \rangle$, então pela maximalidade $G = N\langle z \rangle$, logo G/N é cíclico e, portanto, G/N é um $\mathcal{M}_c$-grupo. Agora, se $N \leq \langle z \rangle$, então N é cíclico e em particular policíclico. Logo, G é um grupo policíclico-por-finito e então pelo Corolário 2.3.1 G tem *MÁX-C*. Assim, pelo Lema 2.3.4 G/N satisfaz *MÁX-C*. Portanto, G/N é um $\mathcal{M}_c$-grupo.

Agora, se G é finito e um $\mathcal{M}_c$-grupo, então G tem um subgrupo maximal H abeliano. E pelo Teorema 3.2.2 G é solúvel.

■

Lema 4.1.3. *Seja G um $\mathcal{M}_c$-grupo não abeliano.*

(1) Se $\langle x\rangle \lessdot G$, então $C_G(x) = \langle x\rangle$.

(2) Seja A um subgrupo abeliano de G cujos geradores têm ordem finita em G (isto é, $A \leq Tor(G)$). Então A é cíclico.

Demonstração. (1) Suponhamos que este não é o caso, ou seja, $C_G(x) \neq \langle x\rangle$. Assim, podemos escolher y arbitrário, tal que $y \in C_G(x) - \langle x\rangle$ e, portanto, pela maximalidade, temos que $G = \langle x, y\rangle$, então G seria abeliano.

(2) Seja a um gerador arbitrário de A, como G é $\mathcal{M}_c$-grupo por hipótese, existe $x \in G$ tal que $\langle x\rangle \lessdot_c G$ de modo que $a \in \langle x\rangle$. Suponha que A não é cíclico, então podemos escolher $y \in A - \langle x\rangle$. Assim, teríamos que $G = \langle x, y\rangle$. Note que $a \in C_G(x) = \langle x\rangle$ e $a \in C_G(y)$, pois $y \in A$. Logo, $a \in Z(G)$ e consequentemente, $A \leq Z(G)$. Como $y \in A$, G seria abeliano. O que é uma contradição. Portanto, A é cíclico. ■

Lema 4.1.4. *Um $\mathcal{M}_c$-grupo não abeliano finito é supersolúvel.*

Demonstração. Seja G um contra-exemplo minimal. Seja G um $\mathcal{M}_c$-grupo não abeliano finito que não é supersolúvel. Como G é um $\mathcal{M}_c$-grupo finito, então pelo (Lema 4.1.2), G é solúvel. Agora, tomemos N o menor termo não trivial da série derivada de G. Assim, pelo (Lema 4.1.3), N é cíclico, e pela escolha de G, temos que G/N é supersolúvel. Daí, pelo (Lema 2.3.2) G também é supersolúvel, o que é uma contradição. ■

4.2 Caracterização de $\mathcal{M}_c$-grupos Finitos

Para simplificar a escrita do Teorema principal optamos por considerar alguns casos particulares. No resultado a seguir estudaremos p-grupos que são $\mathcal{M}_c$-grupos.

Teorema 4.2.1. *Seja G um p-grupo finito. Se G é um $\mathcal{M}_c$-grupo então G é isomorfo ao Q_8, C_{p^n} ou $C_p \times C_p$ para algum primo p.*

Demonstração. Por hipótese, temos que $|G| = p^n$. Suponhamos que $\langle a\rangle$ é um subgrupo cíclico maximal de G, como G é um $\mathcal{M}_c$-grupo, então $\langle a\rangle$ é maximal em G, isto é, $|\langle a\rangle| = p^{n-1}$. Logo, temos um p-grupo que possui um subgrupo cíclico que é maximal em G. Portanto, pelo Teorema 3.1.1, temos as seguintes possibilidades para G:

(1) $G \simeq C_{p^n}$.

(2) $G \simeq C_{p^{n-1}} \times C_p$.

(3) $\langle a, b \mid a^p = 1 = a^{p^{n-1}},\ a^b = a^{1+p^{n-2}1}\rangle$, $n \geq 3$.

(4) O grupo diedral $D_{2^n} = \langle a, b \mid a^{2^n} = 1 = b^2, a^b = a^{-1}\rangle$, $n \geq 3$.

(5) O grupo quatérnion generalizado $Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2,\ x^y = x^{-1}\rangle$, $n \geq 3$.

(6) O grupo semidiedral $\langle a, b \mid a^{2^{n-1}} = 1 = b^2,\ a^b = a^{2^{n-2}-1}\rangle$, $n > 3$.

Agora, para concluirmos a prova deste teorema, verificaremos quais dos grupos acima são $\mathcal{M}_c$-grupos.

- Se G cíclico é um $\mathcal{M}_c$-grupo.

- Seja H do tipo (2). Temos $H = C_{p^{n-1}} \times C_p = \langle x, y \mid x^{p^{n-1}} = 1 = y^p,\ x^y = x\rangle$, $n \geq 2$. Como $\langle x\rangle \bigcap \langle y\rangle = \{1\}$ e $\langle x\rangle, \langle y\rangle \trianglelefteq H$, pois H é abeliano, teremos

$$H = \langle x\rangle \times \langle y\rangle = \{1, x, \cdots, x^{p^{n-1}-1}, xy, \cdots, xy^{p-1}, \cdots, x^{p^{n-1}-1}y, \cdots, x^{p^{n-1}-1}y^{p-1}\}.$$

  * Se $p^{n-1} > p$, ou seja, $n > 2$, então $\langle y\rangle \lessdot_c G$ e $\langle y\rangle$ não é maximal. De fato, como $y \notin \langle x\rangle$, basta mostrarmos que $y \notin \langle x^i y^j\rangle$. Se $y \in \langle x^i y^j\rangle$, com $1 \leq i \leq p^{n-1} - 1$ e $1 \leq j \leq p - 1$, então $y = (x^i y^j)^t = x^{it} y^{jt}$. Portanto, $x^{it} = y^{1-jt}$ e como $\langle x\rangle \bigcap \langle y\rangle = \{1\}$, segue que $x^{it} = 1 = y^{1-jt}$. Assim, temos
  i) $p^{n-1} | it$;
  ii) $p | 1 - jt$.
  De ii) temos que para $m \in \mathbb{Z}$

$$1 - jt = pm \Longrightarrow 1 = pm + jt \Longrightarrow (p, t) = 1.$$

  Em i) temos que $p^{n-1}|i$, um absurdo, pois $i < p^{n-1}$. Portanto, $\langle y\rangle$ não está contido em nenhum cíclico de H, isto é, $\langle y\rangle \lessdot_c H$. Por outro lado, $\langle y\rangle < \langle x^p\rangle\langle y\rangle$ e assim $\langle y\rangle$ não é subgrupo maximal em H. Portanto, para $n > 2$, H não é um $\mathcal{M}_c$-grupo.

  * Se $n = 2$, $H = C_p \times C_p$ e como mostramos na Tabela 4.1 H é um $\mathcal{M}_c$ - grupo. Portanto, $H \simeq G$.

- Seja H um grupo tipo (3). Temos que H é não abeliano , pois $a^b = a^{1+p^{n-2}} \neq a$. Suponhamos que H é um $\mathcal{M}_c$-grupo, então pelo Lema 4.1.3 (2), todo subgrupo abeliano de H é cíclico. Consideremos o subgrupo $A = \langle a^p\rangle\langle b\rangle$ de H, como $(a^p)^b = (a^b)^p = (a^{1+p^{n-2}})^p = a^{p+p^{n-1}} = a^p$, segue que A é abeliano, logo cíclico. Mas isso não pode ocorrer, pois existem dois subgrupos cíclicos distintos em A de ordem p, que são: $\langle a^{p^{n-2}}\rangle$ e $\langle b\rangle$. Portanto H não pode ser $\mathcal{M}_c$-grupo.

- Seja H do tipo (4). Então, $H = D_{2^n} = \langle a, b \mid a^{2^n} = 1 = b^2, a^b = a^{-1}\rangle$, $n \geq 3$. Como $\langle a\rangle \trianglelefteq H$, pois $|H : \langle a\rangle| = 2$, segue que

$$H = \langle a\rangle\langle b\rangle = \{1, a, a^2, \cdots, a^{2^n-1}, b, ab, \cdots, a^{2^n-1}b\}.$$

  Temos que cada involução $\langle a^i b\rangle \lessdot_c H$. Em particular, $\langle b\rangle \lessdot_c H$. Por outro lado, $\langle b\rangle$ não é maximal em H, pois $\langle b\rangle < \langle b, a^2\rangle < H$.

- Seja H do tipo (5). Então, $H = Q_{2^n} = \langle x, y \mid x^{2^{n-1}} = 1, x^{2^{n-2}} = y^2,\ x^y = x^{-1}\rangle$, $n \geq 3$. Como $\langle x\rangle \trianglelefteq H$ (pois $|H : \langle x\rangle| = 2$), temos

$$H = \langle x\rangle\langle y\rangle = \{1, x, \cdots, x^{n^{n-1}-1}, y, xy, \cdots, x^{2^{n-1}-1}y\}.$$

  Observamos que os elementos y, x^iy, com $1 \leq i \leq 2^{n-1} - 1$ têm ordem 4. De fato, a relação $x^iy = yx^{-i}$, com $1 \leq i \leq 2^{n-1} - 1$ obtida no item anterior, nos diz que $(x^iy)^2 = y^2$, e isso implica que $(x^iy)^4 = (y^2)^2 = 1$, com $1 \leq i \leq 2^{n-1} - 1$. Portanto, $o(y) = o(x^iy) = 4$ para todo $1 \leq i \leq 2^{n-1} - 1$. Agora notemos que

  * Se $n > 3$, então $\langle y\rangle \lessdot_c H$ mas $\langle y\rangle$ não é maximal em H. De fato, Suponhamos que $y \in \langle x^iy\rangle$, para todo $i \neq 2^{n-2}$. Como $|\langle y\rangle| = |\langle x^iy\rangle|$, segue que $\langle y\rangle = \langle x^iy\rangle$, isso implica que $x^iy = y^t$ para algum t inteiro, isto é, $x^i = y^{t-1}$. Mas $\langle x\rangle \cap \langle y\rangle = \{1, y^2\}$, então $x^i = 1$ ou $x^i = y^2$. Se $x^i = 1$, então $2^{n-1}|i$ um absurdo já que $1 \leq i \leq 2^{n-1} - 1$; e como suponhamos $i \neq 2^{n-2}$, temos que $x^i \neq y^2$. E com isso concluímos que $\langle y\rangle \lessdot_c H$. Agora, note que $y^x = x^{-1}yx = (x^2)^{-1}y \notin \langle y\rangle$, portanto $\langle y\rangle \ntrianglelefteq H$, e como H é nilpotente segue que $\langle y\rangle$ não é maximal em H e por isso temos que H não é um $\mathcal{M}_c$-grupo;
  * Se $n = 3$, mostramos na Tabela 4.1 que $H = Q_{2^3}$ é um $\mathcal{M}_c$-grupo.

- Seja H do tipo (6). Então, $H = \langle a, b \mid a^{2^{n-1}} = 1 = b^2,\ a^b = a^{2^{n-2}-1}\rangle$, $n > 3$. Notemos que H não é abeliano, pois $a^b = a^{2^{n-2}-1} \neq a$. Suponhamos que H seja um $\mathcal{M}_c$-grupo e considere o subgrupo $A = \langle a^{2^{n-2}}\rangle\langle b\rangle$, como $|A| = 2^2$, segue que A é abeliano, donde cíclico pelo Lema 4.1.3 (2), o que é um absurdo, pois $\langle x^{2^{n-2}}\rangle$ e $\langle y\rangle$ são dois subgrupos de ordem 2 em A. Portanto, H não é um $\mathcal{M}_c$-grupo.

Portanto, $G \simeq C_p \times C_p$ ou $G \simeq Q_8$ ou cíclico C_{p^n}. ■

Para a demonstração dos próximos resultados usaremos o fato de que subgrupos maximais de um grupo supersolúvel tem índice primo, como foi mostrado no capítulo 2. Iremos também usar o fato de que se um grupo quatérnion generalizado é um $\mathcal{M}_c$-grupo, então é isomórfico a Q_8, o grupo quatérnion de ordem 8.

Observação 4.2.1. *Com intuito de simplificar o enunciado dos resultados a seguir, denotaremos por $\mathfrak{X}$ a classe composta pelos seguintes grupos*

Proposição 4.2.1. *Seja G um $\mathcal{M}_c$-grupo nilpotente finito. Então*

a) G é cíclico ou $G \backsimeq C_p \times C_p \times C_n$, onde p é um primo que não divide n.

b) $G \backsimeq C_n \times Q_8$ com n ímpar.

Demonstração. Sejam $\pi(G) = \{p_1, \cdots, p_k\}$ e $M \lessdot G$. Sem perda de generalidade, podemos assumir que M é cíclico. Como G é nilpotente finito, temos que

$$|G : M| = p_1,$$

com M cíclico. Daí, $P_i \in Syl_{p_i}(G)$, $2 \leq i \leq k$ é cíclico. Pela Caracterização dos Grupos Nilpotentes Finitos temos que $G \simeq P_1 \times P_2 \times \cdots \times P_k$, sendo que $P_i \in Syl_{P_i}(G)$. Pela observação acima podemos reescrever

$$G = P_1 \times C_n, \tag{4.1}$$

sendo que $P_1 \in Syl_{p_1}(G)$ e $n = \dfrac{|G|}{|P_1|}$.

Como $\dfrac{G}{C_n} \simeq P_1$ pelo Lema 4.1.3 P_1 é um $\mathcal{M}_c$-grupo. Logo, pelo Teorema 4.2.1 temos que

$$P_1 \simeq C_p \times C_p \text{ ou } P_1 \simeq Q_8 \text{ ou } P_1 \simeq C_{p^n}. \tag{4.2}$$

Portanto, por (4.1) e (4.2)

$$G = P_1 \times C_n \simeq C_p \times C_p \times C_n, \text{ com } (n,p) = 1$$

ou

$$G = P_1 \times C_n \simeq Q_8 \times C_n$$

tal que n é ímpar ou G é cíclico porque

$$G = P_1 \times C_n \simeq C_{p_1}^{k_1} \times C_n.$$

■

Proposição 4.2.2. *Seja G um grupo finito. Se $G \in \mathfrak{X}$ então G é um $\mathcal{M}_c$-grupo.*

Demonstração. a) Se G é cíclico, tal que $G = C_n$, então pela Proposição 2.1.2 G é um $\mathcal{M}_c$ - grupo. Suponhamos que $G \backsimeq C_p \times C_p \times C_n$, onde p é um primo que não divide n. Pela Proposição 2.1.3 temos que $G \backsimeq C_p \times C_{pn}$. Ainda mais, todos os subgrupos cíclicos maximais de $C_p \times C_{pn}$ são maximais, pois $|G : C_{pn}| = p$. Logo, $C_p \times C_{pn}$ é um $\mathcal{M}_c$-grupo. Portanto, G é um $\mathcal{M}_c$-grupo.

b) Suponhamos que $G \backsimeq C_n \times Q_8$. Sabemos que existem cópias de C_4 em Q_8 e cópias de C_n em G. Então, pela Proposição 2.1.3 existe uma cópia de $C_n \times C_4 \backsimeq C_{4n}$. Notemos que $|G : C_{4n}| = \dfrac{8n}{4n} = 2$, o que implica que G é um $\mathcal{M}_c$-grupo.

■

Na prova do nosso próximo teorema, iremos usar o seguinte resultado:

Teorema 4.2.2 (Hölder-Burnside-Zassenhaus)**.** *Se G é um grupo finito cujos subgrupos Sylow são cíclicos, então G tem uma apresentação*

$$G = \langle a, b \mid a^m = b^n = 1,\ a^b = a^r \rangle,$$

onde $r^n \equiv 1 \ (mod\ m)$, m é ímpar, $0 \leq r < m$ e m $n(r-1))$ são coprimos. Por outro lado, em um grupo com tal representação, todos os subgrupos Sylow são cíclicos.

Não faremos a demonstração, pois foge do nosso objetivo, todavia a mesma pode ser encontrada em [9, Teorema 10.1.10].

Proposição 4.2.3. *Seja G um grupo não nilpotente. Então G é um $\mathcal{M}_c$-grupo se, e somente se, existe uma sequência exata*

$$1 \to Z(G) \to G \to C_p \rtimes C_q \to 1$$

sendo que p e q são primos $(p > q)$ e $Z(G) \leq \langle x \rangle$ para todo $\langle x \rangle \lessdot_c G$.

Demonstração. Suponhamos que todos os subgrupos Sylow de G sejam cíclicos. O Teorema 4.2.2, nos diz que

$$G = \langle a, b \mid a^m = b^n = 1, \ a^b = a^r \rangle,$$

onde $r^n \equiv 1 \pmod{m}, 0 \leq r < m$, m é ímpar e $mdc(m, \ n(r-1)) = 1$. Seja $b \in \langle t \rangle \lessdot_c G$ e seja $\langle t \rangle \cap \langle a \rangle = \langle a^s \rangle$. Segue-se que $a^{s(r-1)} = 1$ e, portanto, $m|s$. Então provamos que $\langle b \rangle = \langle t \rangle \lessdot_c G$. Portanto, como G é supersolúvel, $\langle b \rangle$ tem índice primo e assim $m = p$ é um primo. Mas $G = \langle a \rangle \rtimes \langle b \rangle$ e então $C_G(a) = \langle a, Z(G) \rangle$. Assim, existe $y \in G$ tal que $C_G(a) \leq \langle y \rangle < G$. No entanto, isso implicaria que $y \in C_G(a)$ e assim $C_G(a)$ tem índice primo q, digamos. Mas então temos $q = [\langle b \rangle : Z(G)]$. Logo, $G/Z(G)$ é um grupo isomórfico a $C_p \rtimes C_q$ e assim $q|(p-1)$. Se $\langle x \rangle \lessdot_c G$, já que G é não abeliano, $\langle x, Z(G) \rangle$ é um subgrupo próprio. Portanto, como G é um $\mathcal{M}_c$-grupo, temos que ter $Z(G) \leq \langle x \rangle$.

Reciprocamente, pela definição de sequência exata, temos que $Z(G) \trianglelefteq G$ e $\dfrac{G}{Z(G)} \backsimeq C_p \rtimes C_q$. E mais, todos os subgrupos de $C_p \rtimes C_q$ são cópias de C_p e C_q. Logo, são cíclicos maximais e portanto $C_p \rtimes C_q$ é um $\mathcal{M}_c$-grupo. Logo, temos que $\dfrac{G}{Z(G)}$ também é um $\mathcal{M}_c$-grupo. Como $\langle x \rangle \lessdot_c G$ e $Z(G) \leq \langle x \rangle$, já que G é não abeliano, temos $\langle x, Z(G) \rangle$ é um subgrupo próprio. Portanto G é um $\mathcal{M}_c$-grupo. ∎

Combinando as Proposições 4.2.1, 4.2.2 e 4.2.3 temos o Teorema principal do Capítulo 4.

Teorema 4.2.3. *Seja G um grupo finito. Então G é um $\mathcal{M}_c$-grupo se, e somente se, um dos seguintes vale:*

(1) G é cíclico ou $G \backsimeq C_p \times C_p \times C_n$, onde p é um primo que não divide n.

(2) $G \backsimeq C_n \times Q_8$ com n ímpar.

(3) Existem primos $q < p$, uma sequência exata $1 \to Z(G) \to G \to C_p \rtimes C_q \to 1$ e $Z(G) \leq \langle x \rangle$ para qualquer $\langle x \rangle \lessdot_c G$.

Exemplo 4.2.1. *Seja $G = \langle a, b \mid a^5 = b^4 = 1, \ a^b = a^{-1} \rangle$. De acordo com o Teorema 4.2.3, temos que G é um $\mathcal{M}_c$-grupo. De fato, pois pelo item (3) Temos a sequência exata*

$$1 \to \langle b^2 \rangle \to \langle a \rangle \rtimes \langle b \rangle \to \langle a \rangle \rtimes \langle b^2 \rangle \to 1$$

e $\langle b^2 \rangle \leq \langle b \rangle$ e $\langle b \rangle \lessdot_c G$.

Exemplo 4.2.2. *O Teorema 4.2.3 nos mostra que a classe de $\mathcal{M}_c$-grupos é fechada em relação a formação de subgrupos, porém não é com relação a produtos direto e semidireto. Vejamos:*

1. *S_3 e Q_8 são $\mathcal{M}_c$-grupos, mas $G = C_8 \rtimes S_3$ não é um $\mathcal{M}_c$-grupo.*

2. *C_7 e S_3 são $\mathcal{M}_c$-grupos, mas $G = C_7 \times S_3$ não é um $\mathcal{M}_c$-grupo.*

4.3 Aplicação: Grupos Unicamente Cobertos

A tentativa de classificar grupos com uma propriedade específica através de seus subgrupos é um tema frequente na Teoria dos Grupos. Muitos matemáticos contribuíram nestes estudos. Cabe destacar os trabalhos de [7, Neumann], [6, Cohn] e [8, Tomkinson].

Aqui apresentaremos a definição e algumas propriedades de grupos unicamente cobertos estabelecidos por [1].

Definição 4.3.1. *Sejam G um grupo e $S = \{H_i \mid H_i \leq G, i \in I\}$ uma família de subgrupos de G, sendo que I é um um conjunto de índices.*

1) *Dizemos que S é uma cobertura de G se*

$$G = \bigcup_{i \,\in\, I} H_i$$

2) *Dizemos que S é uma cobertura irredundante de G se*

$$G = \bigcup_{i \,\in\, I} H_i$$

e

$$H_i \not\subseteq \bigcup_{j \,\in\, I \setminus \{i\}} H_j,$$

para todo $i \in I$.

Exemplo 4.3.1.

1. $S_3 = \langle \sigma \rangle \cup \langle \tau \rangle \cup \langle \sigma\tau \rangle \cup \langle \sigma^2\tau \rangle$.

2. $Q_8 = \langle a \rangle \cup \langle ab \rangle \cup \langle b \rangle$.

3. $A_4 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \cup \langle (1\ 2\ 3) \rangle \cup \langle (1\ 2\ 4) \rangle \cup \langle (1\ 3\ 4) \rangle \cup \langle (2\ 3\ 4) \rangle = \langle (1\,2)(3\,4) \rangle \cup \langle (1\,3)(2\,4) \rangle \cup \langle (1\,4)(2\,3) \rangle \cup \langle (1\,2\,3) \rangle \cup \langle (1\,2\,4) \rangle \cup \langle (1\,3\,4) \rangle \cup \langle (2\,3\,4) \rangle$.

4. $D_p = \langle \sigma \rangle \cup \langle \tau \rangle \cup \langle \sigma\tau \rangle \cup \cdots \cup \langle \sigma^{p-1}\tau \rangle$.

5. $C_2 \times C_2 = \langle a \rangle \cup \langle b \rangle \cup \langle ab \rangle$.

Observação 4.3.1. *Seja G um grupo finito. Suponhamos que $\langle x_1\rangle, \cdots, \langle x_r\rangle$ são todos os subgrupos cíclicos maximais de G. Então $\{\langle x_1\rangle, \cdots, \langle x_r\rangle\}$ é uma cobertura irredundante de G.*

Demonstração. De fato,

$$G = \bigcup_{i\,=\,1}^{r} \langle x_i\rangle.$$

Pelo Teorema de Lagrange, todo subgrupo cíclico está contido em, pelo menos, um subgrupo cíclico maximal. Por outro lado,

$$K = \bigcup_{j\,\neq\,i} \langle x_j\rangle \neq G,$$

visto que $x_i \notin K$. ■

Definição 4.3.2. *Um grupo finito G é unicamente coberto quando possui exatamente uma cobertura irredundante por subgrupos próprios.*

Observação 4.3.2. *Em particular, se G é unicamente coberto, então a única cobertura possível é a dada por subgrupos cíclicos maximais, dada por*

$$G = \bigcup_{i=1}^{r}\langle x_j\rangle,$$

sendo que $\{\langle x_1\rangle, \ldots, \langle x_r\rangle\}$ são todos os subgrupos cíclicos maximais de G.

Exemplo 4.3.2. *Os grupos $Q_8, C_2 \times C_2$ e S_3 são unicamente cobertos.*

Cabe destacar uma conexão entre grupos finitos unicamente cobertos e $\mathcal{M}_c$-grupos.

Proposição 4.3.1. *Um grupo G é um $\mathcal{M}_c$ - grupo se, e somente se, é unicamente coberto.*

Demonstração. Tomemos $\{\langle x_1\rangle, \ldots, \langle x_r\rangle\}$ o conjunto de todos os subgrupos cíclicos maximais de G.

Suponhamos que G é um $\mathcal{M}_c$-grupo. Dado $G = \bigcup_{i\,=\,1}^{m} H_i$ uma cobertura irredundante qualquer. Então para todo $i \in \{1, \cdots, r\}$ existe $j_i \in \{1, \cdots, m\}$ tal que $x_i \in H_{j_i}$. Daí, temos que

$$\langle x_i\rangle \leq H_{j_i} < G,$$

o que implica que $\langle x_i\rangle = H_{j_i}$ (maximalidade do subgrupo $\langle x_i\rangle$). Portanto, $r = m$ e

$$\bigcup_{i=1}^{r} H_{j_i} = G,$$

tal que, $\{j_1, \cdots, j_r\} = \{1, \cdots m\}$. Daí, a única cobertura para G é $\bigcup_{i\,=\,1}^{r} \langle x_i\rangle$.

Reciprocamente, usando a contrapositiva, suponhamos que G não é um $\mathcal{M}_c$-grupo. Daí, existe $x_i \in G$ e $M \lessdot G$ tais que $\langle x_i \rangle \leq M$ e M não é cíclico. Sem perda de generalidade, podemos supor que $i = 1$. Daí, G admite as seguintes coberturas irredundantes:

$$\bigcup_{i=1}^{r} \langle x_i \rangle = G = M \cup \langle x_2 \rangle \cup \cdots \cup \langle x_r \rangle.$$

■

Em particular, podemos parafrasear as Proposições 4.2.1, 4.2.2 e 4.2.3 no contexto de grupos unicamente cobertos:

Proposição 4.3.2. *Um grupo G nilpotente é unicamente coberto se, e somente se, um dos seguintes vale:*

a) G é cíclico ou $G \simeq C_p \times C_p \times C_n$, onde p é um primo que não divide n.

b) $G \simeq C_n \times Q_8$ com n ímpar.

Proposição 4.3.3. *Seja G um grupo não nilpotente. Então G é unicamente coberto se, e somente se, existe uma sequência exata*

$$1 \to Z(G) \to G \to C_p \rtimes C_q \to 1$$

sendo que p e q são primos $(p > q)$ e $Z(G) \leq \langle x \rangle$ para todo $\langle x \rangle \lessdot_c G$.

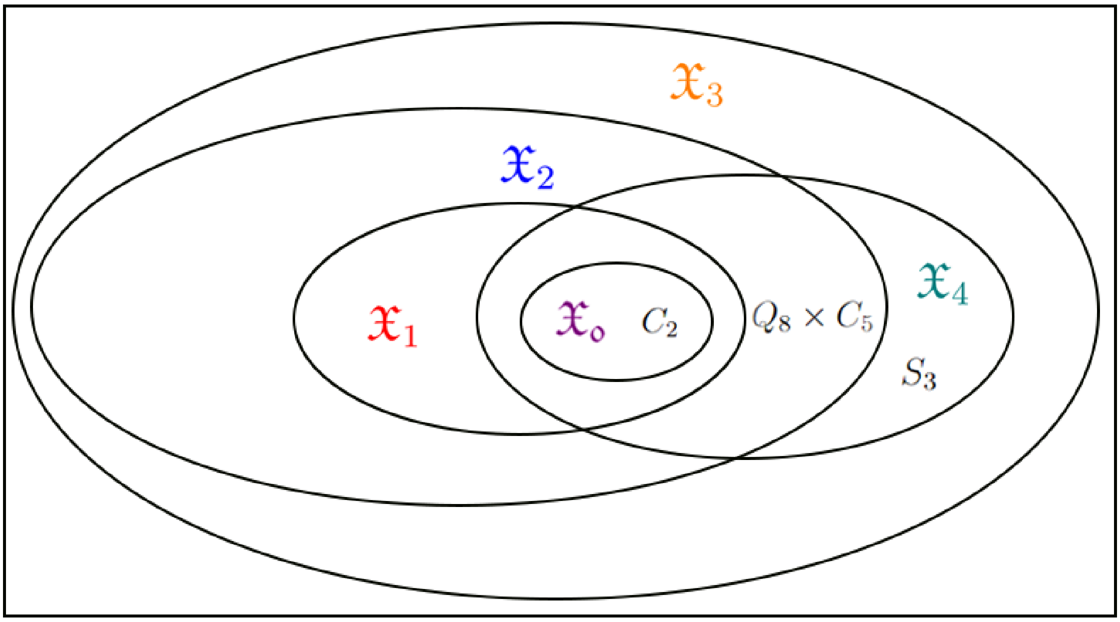
Tais resultados foram estudados originalmente por [1, Brodie].

$\mathcal{M}_c$-grupos e outras subclasses de grupos solúveis

Agora, para finalizarmos essa seção, observemos como a classe dos grupos aqui apresentados se relacionam.

- $\mathfrak{X}_0$ = classe dos grupos cíclicos finitos;
- $\mathfrak{X}_1$ = classe dos grupos abelianos finitos;
- $\mathfrak{X}_2$ = classe dos grupos nilpotentes finitos;
- $\mathfrak{X}_3$ = classe dos grupos supersolúveis finitos;
- $\mathfrak{X}_4$ = classe dos grupos $\mathcal{M}_c$-grupos finitos.

Figura 4.1: Comparando Classes de Grupos 2



Fonte: Autoria Própria

Daí, $\mathcal{M}_c$-grupos formam uma subclasse dos grupos supersolúveis.

Capítulo 5

Grupos Infinitos

Aqui investigaremos propriedades estruturais de grupos infinitos a partir de certas suposições sobre certos subgrupos cíclicos. Inicialmente, apresentaremos um breve resumo sobre FC-grupos. Em seguida apresentamos o Teorema de Schur e, como aplicação, demonstramos o Teorema de Fedorov que nos dá uma caracterização de grupos cíclicos infinitos. Na última seção veremos algumas propriedades de $\mathcal{M}_c$-grupos infinitos. E, no final, mencionaremos os Monstros de Tarski que nos mostram que $\mathcal{M}_c$-grupos infinitos podem ser bastante complexos.

5.1 FC-grupos: Definições e Propriedades

Definição 5.1.1. *Um grupo G é dito FC-grupo se x^G é finito para qualquer $x \in G$. Ademais, se existir $k \in \mathbb{N}$ tal que $|x^G| \leq k$ para todo $x \in G$, então G é chamado de BFC-grupo.*

Exemplo 5.1.1.

1. *Todo grupo abeliano é FC-grupo.*
2. *Todo grupo finito é FC-grupo.*

Proposição 5.1.1. *Se $|G : Z(G)| < +\infty$, então G é BFC-grupo.*

Demonstração. Suponhamos que $|G : Z(G)| = n$. Se $x \in G$, então $Z(G) \leq C_G(x) \leq G$, logo $|x^G| = |G : C_G(x)| \leq n$. Consequentemente $|x^G| \leq n$, para todo $x \in G$. Portanto, G é um BFC-grupo. ∎

Proposição 5.1.2. *G é um FC-grupo se, e somente se, $\dfrac{G}{C_G(x^G)}$ for finito para qualquer $x \in G$.*

Demonstração. Suponhamos que G é um FC-grupo. Tomemos $x^G = \{x_1, x_2, \cdots, x_n\}$. Então

$$|x^G| = |x_i^G| = |G : C_G(x_i)| = |G : C_G(x)| = n.$$

Pelo Lema de Poincaré, temos que

$$|G : C_G(x^G)| = \left|G : \bigcap_{i=1}^{n} C_G(x_i)\right| < +\infty.$$

Portanto, $\dfrac{G}{C_G(x^G)}$ é finito.

Reciprocamente, tomemos $x \in G$, $C_G(x^G) \leq C_G(x) \leq G$. Logo,

$$|x^G| = |G : C_G(x)| \leq |G : C_G(x^G)| < \infty.$$

Portanto, G é um FC-grupo. ■

Definição 5.1.2. *Um grupo G é dito residualmente finito se, dado $1 \neq g \in G$, existe um $N \trianglelefteq G$ tal que $g \notin N$ e G/N é finito.*

Teorema 5.1.1. *(Baer). Se G é um FC-grupo, então $G/Z(G)$ é um grupo de torção residualmente finito.*

Demonstração. Temos que o $Z(G)$ é a interseção de todos os centralizadores de G. Como cada um dos últimos tem índice finito, $G/Z(G)$ é residualmente finito. Temos que G é um FC-grupo, logo $|G : C_G(x)| = k < +\infty$, para algum inteiro positivo k. Agora, seja $x \in G$ tomemos um transversal $\{t_1, \cdots, t_k\}$ de $C_G(x)$ em G. Considere $H = \cap_{i=1}^{k} C_G(t_i)$, pelo Lema de Poincaré,

$$|G : H| = |G : \bigcap_{i=1}^{k} C_G(t_i)| \leq \prod_{i=1}^{k} |G : C_G(t_i)| = n < +\infty$$

para algum inteiro positivo n, de onde o mesmo acontece com seu núcleo H. Assim, $x^m \in H$ para algum inteiro positivo m, assim, $x^m t_i = t_i x^m$, $1 \leq i \leq k$. Segue que x^m centraliza cada t_i. Como t_i e $C_G(x)$ geram G, temos que $x^m \in Z(G)$. Portanto $G/Z(G)$ é de torção. ■

5.2 Teoremas de Schur e Fedorov

O objetivo dessa será apresentar uma demonstração do célebre Teorema de Schur e, como aplicação direta, demonstraremos o Teorema de Fedorov. A demonstração que apresentamos aqui foi inteiramente baseada no livro do John Dixon [4, Capítulo 5].

Lema 5.2.1. *Seja G um grupo com $|G : Z(G)| = n$. Então o subgrupo comutador G' é finitamente gerado. Mais ainda, G' é gerado por, no máximo, n^2 geradores.*

Demonstração. Chamemos $I := \{1, 2, \ldots, n\}$. Tomemos $\tau = \{t_1, t_2, \ldots, t_n\}$ um transversal de $Z(G)$ em G. Dados x, $y \in G$, existem índices i, $j \in I$ e elementos z_1, $z_2 \in Z(G)$ tais que $x = z_1 t_i$, $y = z_2 t_j \in G$. Note que

$$\begin{aligned}[x, y] &= [z_1 t_i, z_2 t_j] = (z_1 t_i)^{-1}(z_2 t_j)^{-1}(z_1 t_i)(z_2 t_j) \\ &= t_i^{-1} z_1^{-1} t_j^{-1} z_2^{-1} z_1 t_i z_2 t_j = t_i^{-1} t_j^{-1} t_i t_j = [t_i, t_j],\end{aligned}$$

pois z_1, $z_2 \in Z(G)$. Logo, $G' = \langle [x, y] \,|\, x, y \in G \rangle = \langle [t_i, t_j] \,|\, i, j \in I \rangle$. ■

O próximo resultado mostra que, se o centro de um grupo G tiver índice n, então a $(n+1)$-ésima potência de qualquer comutador (em G) pode ser reescrita como o produto de n comutadores.

Lema 5.2.2. *Seja um grupo G com $|G : Z(G)| = n$. Então, $[x, y]^{n+1} = [x, y^2][x^y, y]^{n-1}$ para todo $x, y \in G$.*

Demonstração. Como $G/Z(G)$ tem ordem n, segue que $[x, y]^n \in Z(G)$ para todo x, $y \in G$. Então,

$$\begin{aligned}[x, y]^{n+1} &= [x, y]^n[x, y] = [x, y]^n x^{-1}y^{-1}xy \\ &= x^{-1}y^{-1}x[x, y]^n y = x^{-1}y^{-1}x[x, y][x, y]^{n-1}y \\ &= x^{-1}y^{-2}xy[x, y]^{n-1}y = x^{-1}y^{-2}xy^2y^{-1}[x, y]^{n-1}y \\ &= [x, y^2][x^y, y]^{n-1}.\end{aligned}$$

■

Lema 5.2.3. *Seja um grupo G com $|G : Z(G)| = n$. Então, todo elemento do subgrupo comutador G' pode ser escrito como um produto de, no máximo, n^3 comutadores.*

Demonstração. Suponhamos que existe um elemento $\alpha \in G'$ o qual pode ser escrito como um produto de $n^3 + 1$ comutadores e não menos, isto é,

$$\alpha = c_1c_2 \dots c_{n^3+1},$$

sendo que $c_i = [x_i, y_i]$. Por outro lado, pelo Lema 5.2.1, existem no máximo n^2 comutadores em G. Mais ainda, existem pelo menos um comutador, digamos $[x, y]$, que ocorre mais de n vezes nesse produto. Daí, podemos reescrever α da seguinte forma

$$\alpha = [x, y]^{n+1}c'_{n+2}c'_{n+3} \dots c'_{n^3+1},$$

sendo que cada um dos c'_j é um comutador conjugado a um dos comutadores (originais) c_i sob alguma potência de $[x, y]$. Pelo Lema 5.2.2,

$$\alpha = [x, y^2][x^y, y]^{n-1}c'_{n+2}c'_{n+3} \dots c'_{n^3+1}$$

e, consequentemente, α é um produto de n^3 comutadores, absurdo. ■

Agora estamos em condicões de demonstrar o Teorma de Schur.

Teorema 5.2.1. *(Schur) Seja G um grupo central-por-finito. Suponha que $|G : Z(G)| = n$. Então, o subgrupo comutador G' é finito.*

Demonstração. Pelo Lema 5.2.1, existem, no máximo, n^2 comutadores distintos. Ademais, pelo Lema 5.2.3, cada elemento $\alpha \in G'$ pode ser escrito como um produto de, no máximo, n^3 comutadores, digamos

$$\alpha = c_1c_2 \dots c_{n^3}.$$

Assim, $|G'| \leqslant (n^2)^{n^3} = n^{2n^3}$. ■

Agora podemos demonstrar o Teorema de Fedorov [9, Exercício 14.5.5]. O próximo resultado é o Teorema E da Introdução.

Teorema 5.2.2. *(Fedorov). Seja G um grupo infinito. Então $G \simeq C_\infty$ (cíclico infinito) se, e somente se, todos os subgrupos não triviais de G tem índice finito.*

Demonstração. Se $G \simeq C_\infty$, então $1 \neq H \leq G$ é dado por $H = \langle x^m \rangle$ para algum $m \in \mathbb{N}$.

Reciprocamente, seja $1 \neq x \in G$. Como $1 \neq \langle x \rangle \leq G$ temos por hipótese que $|G : \langle x \rangle| = n < +\infty$. Agora, tomemos $\{t_1, \cdots, t_n\}$ um transversal de $\langle x \rangle$ em G de modo que $t_i \neq 1$, para todo i. Logo, $G = \dot{\bigcup\limits_i} \langle x \rangle t_i = \langle x, t_1, \cdots, t_n \rangle$. Note que, $\langle x \rangle \subset C_G(x)$. Portanto, $|G : C_G(x)| \leq |G : \langle x \rangle| = n < +\infty$. Analogamente, para todo $t_i \in \{t_1, \cdots, t_n\}$, temos $1 \neq \langle t_i \rangle < G$ e $\langle t_i \rangle \subset C_G(t_i)$. Logo, $|G : C_G(t_i)| < |G : \langle t_i \rangle| < +\infty$ para todo i.

Agora, sendo $Z(G) = \bigcap\limits_{y \in \{x, t_i\}} C_G(y)$, segue do Lema de Poincaré que $|G : Z(G)| < +\infty$ e portanto, G' é finito.

Afirmação: G é livre de torção, ou seja, todo elemento, exceto a identidade tem ordem infinita. De fato, seja $1 \neq a \in G$, de modo que a ordem de a é finita, então teríamos que $|G| = |G : \langle a \rangle||\langle a \rangle| < \infty$ o que é um absurdo. Portanto, temos que $G' = 1$. Logo, G é abeliano finitamente gerado e livre de torção. Daí $G = H_1 \times \cdots \times H_n$ com $H_i \simeq C_\infty$, tal que $n = 1$. Pois, caso contrário, se $n > 1$, tomando $H = H_1 \times \cdots \times H_{n-1}$, teríamos que $G/N \simeq H_n$. Assim, H é um subgrupo de índice infinito em G o que é um absurdo. Portanto, $n = 1$ e $G \simeq C_\infty$. ■

O Teorema de Fedorov pode ser visto como uma caracterização de grupos cíclicos infinitos. Na próxima seção veremos algumas caracterizações em termos de $\mathcal{M}_c$-grupos.

5.3 $\mathcal{M}_c$-grupos infinitos

Agora, nesta seção, iremos classificar algumas famílias de $\mathcal{M}_c$-grupos infinitos.

Teorema 5.3.1. *(Robinson, Wehrfritz) . Suponha que G é um grupo solúvel finitamente gerado. Se G é não nilpotente, então ele tem uma imagem finita que é não nilpotente.*

A demonstração do resultado supracitado não será feita aqui mas pode ser encontrada em [9, 15.5.3].

A próxima proposição corresponde ao item (1) do Teorema F da Introdução.

Proposição 5.3.1. *Seja G um $\mathcal{M}_c$-grupo solúvel infinito. Então G é cíclico infinito.*

Demonstração. Primeiramente, vamos provar que G é policíclico. Suponhamos que G é não nilpotente, logo pelo Teorema 5.3.1, G contém um subgrupo normal N, de modo que G/N é finito e não nilpotente. Note que, se $\langle x \rangle$ é um subgrupo cíclico maximal de G, então temos que N está contido em $\langle x \rangle$, logo temos que G é policíclico. Portanto, todo subgrupo maximal de G tem índice finito. Ademais, todo subgrupo cíclico de G está contido em um subgrupo cíclico de índice finito, logo G é um FC-grupo. Como G é policíclico e FC-grupo, temos que G é central-por-finito e pelo Teorema 5.2.1, $|G'|$ é finito e portanto $G' = 1$, ou seja, G é livre de torção. Logo, G é abeliano e, portanto $G \simeq C_\infty$. ■

A próxima proposição corresponde ao item (2) do Teorema F da Introdução.

Proposição 5.3.2. *Seja G um $\mathcal{M}_c$-grupo infinito. Então $G' = G''$.*

Demonstração. Suponhamos, por contradição, que $G' \neq G''$ e seja $\langle x \rangle$ um subgrupo cíclico maximal de G. Temos que G/G'' não é abeliano, assim G'' está contido em $\langle x \rangle$, pois caso contrário, se $G'' \nleq \langle x \rangle$, pela maximalidade $G = G''\langle x \rangle$, assim G/G'' seria cíclico, mas já vimos que não é o caso. E portanto, G é solúvel, e pelo Proposição 5.3.1 é abeliano. Daí $G' = G'' = 1$ uma contradição. ∎

Aqui trataremos dos casos em que os grupos são residualmente finitos.

Proposição 5.3.3. *Seja G um grupo residualmente finito. Então*

$$\bigcap_{\substack{N \trianglelefteq G \\ |G:N| < +\infty}} N = 1.$$

Demonstração. Suponhamos que G é residualmente finito. Seja $1 \neq g \in G$. Como G é residualmente finito temos que exitem F um grupo finito e um homomorfismo $\phi : G \to F$, tal que $g \notin Ker(\phi)$. Como $Ker(\phi) \trianglelefteq G$ podemos concluir que

$$g \notin \bigcap_{\substack{N \trianglelefteq G \\ |G:N| < +\infty}} N.$$

Pela arbitrariedade da escolha de g podemos concluir que

$$\bigcap_{\substack{N \trianglelefteq G \\ |G:N| < +\infty}} N = 1.$$

∎

Teorema 5.3.2. *Seja G um $\mathcal{M}_c$-grupo infinito. Se G é residualmente finito, então G é cíclico infinito.*

Demonstração. Tomemos N um subgrupo normal de índice finito de G. Pela Proposição 5.3.2 $G' = G''$. Daí

$$\left(\frac{G}{N}\right)' = \frac{G'N}{N} = \frac{G''N}{N} = \left(\frac{G}{N}\right)''.$$

Por indução, para todo $n \geq 2$, temos

$$\frac{G^{(n)}N}{N} = \left(\frac{G}{N}\right)^{(n)} = \left(\frac{G}{N}\right)' = \frac{G'N}{N}.$$

Como G/N é finito e $\mathcal{M}_c$-grupo. Daí pelo Lema 4.1.2, G/N é solúvel e existe $n \in N$ tal que

$$\frac{G'N}{N} = \left(\frac{G}{N}\right)^{(n)} = \frac{N}{N} \Longrightarrow G' \leq N.$$

Como tomemos N arbitrário, segue pela Propriedade que

$$G' \leq \bigcap_{\substack{N \trianglelefteq G \\ |G:N| < +\infty}} N = 1.$$

Daí, G é abeliano e pela Proposição 5.3.1 $G \simeq C_\infty$. ■

5.4 Monstros de Tarski são $\mathcal{M}_c$-grupos?

Para cada p primo, $p > 10^{75}$, existe um p-grupo simples, 2-gerado infinito no qual todo subgrupo próprio é cíclico (de ordem p). Em particular, tais grupos são chamados de Monstros de Tarski. Portanto, cada Monstro de Tarski é um $\mathcal{M}_c$-grupo.

Nem todo $\mathcal{M}_c$-grupo infinito é cíclico. Na verdade, eles podem ser bastante complicados. Nesse contexto cabe destacar a seguinte pergunta devida ao lógico polonês Alfred Tarski:

Conjectura 5.4.1. *(A. Tarski) Existem um primo p e um grupo infinito G tal que todos os subgrupos próprios (e não triviais) são cíclicos com p elementos?*

Alexander Yu. Ol'shansky [15], mostrou que a Conjectura acima é verdadeira para primos suficientemente grandes:

Teorema 5.4.1. *(A. Yu. Ol'shansky) Seja $p > 10^{75}$. Existe um grupo infnito $G = G(p)$ tal que todos os subgrupos próprios e não triviais de G são cíclicos de ordem p.*

Observação 5.4.1. *Esses grupos ficaram conhecidos na literatura como Monstros de Tarski. Outras propriedades desses grupos:*

i) G é um grupo simples e não abeliano.

ii) Tais grupos são 2-gerado.

iii) Tais grupos tem expoente $exp(G) = p$.

Mais ainda, eles são contra-exemplos para questões famosas em Teoria dos Grupos, por exemplos: "Problemas de Burnside". Veja mais detalhes e referências em [10].

Considerações Finais do Capítulo 5

Observação 5.4.2. *Sabemos que todo Monstro de Tarski é um $\mathcal{M}_c$-grupo. Uma pergunta natural feita pelos autores de [13], é o seguinte: Qual seria uma condição suficiente para um $\mathcal{M}_c$-grupo infinito G ser um Monstro de Tarski?*

Definição 5.4.1. *Dizemos que $G \neq \{1\}$ é localmente graduado se todo subgrupo finitamente gerado (não trivial) admite um subgrupo próprio de índice finito.*

Exemplo 5.4.1.

1. *Todo grupo residualmente finito é localmente graduado.*

2. *O grupo $\mathbb{Q}$ é localmente graduado e não é residualmente finito.*

Pergunta: Seja G um $\mathcal{M}_c$-grupo localmente graduado. Então $G \simeq C_\infty$?

Considerações Finais

Nosso trabalho envolveu estudar propriedades estruturais de um dado grupo a partir de restrições sobre certos subgrupos abelianos. O estudo foi majoritariamente direcionado para os grupos finitos, salvo o Capítulo 5.

Ao longo do trabalho sugiram algumas questões associadas aos teoremas/definições expostas:

Q_1) O que podemos dizer de grupos finitos nos quais cada subgrupo maximal é um $\mathcal{M}_c$-grupo e G não é? (minimais não $\mathcal{M}_c$-grupos)

Observação: Todos os subgrupos de A_4 são $\mathcal{M}_c$-grupos, mas ele não é.

Q_2) (Juriaans e Rogério) Qual seria uma condição suficiente para um $\mathcal{M}_c$-grupo G ser um Monstro de Tarski?

Q_3) Se G é um $\mathcal{M}_c$-grupo localmente graduado. Então $G \simeq C_\infty$?

Q_4) Quais são os grupos solúveis finitos G tais que sua ordem é dada por:

$$|G| = p \cdot |Z(G)| \cdot |G'|,$$

para algum p?

Observação: Todos os grupos que aparecem na Proposição A da Introdução também satisfazem a relação acima.

Bibliografia

[1] Brodie. M. A. Uniquely covered groups. In *Algebra Colloquium*, volume 10, pages 101–108. Springer, 2003.

[2] Garcia. A. and Lequain. Y. *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada, 2001.

[3] Gonçalves. A. *Introdução à álgebra*, volume 7. Instituto de Matemática Pura e Aplicada, 1979.

[4] Dixon. J. D. *Problems in group theory*. Dover, 2007.

[5] Segal. D. *Polycyclic groups*, volume 82. Cambridge University Press, 2005.

[6] Cohn. John. H. E. On n-sum groups. *Mathematica Scandinavica*, pages 44–58, 1994.

[7] Neumann. Bernhard. H. Groups covered by permutable subsets. *Journal of the London Mathematical Society*, 1(2):236–248, 1954.

[8] Tomkinson. M. J. Groups as the union of proper subgroups. *Mathematica Scandinavica*, pages 191–198, 1997.

[9] Robinson. D. J.S. *A Course in the Theory of Groups*, volume 80. Springer, 1996.

[10] Gupta. N. On groups in which every element has finite order. *The American Mathematical Monthly*, 96(4):297–308, 1989.

[11] Herstein. I. N. A remark on finite groups. *Proceedings of the American Mathematical Society*, 9(2):255–257, 1958.

[12] Milne. J. S. *Group Theory*, volume 4. 2021.

[13] Juriaans. S.O. and Rogério. J. R. On groups whose maximal cyclic subgroups are maximal. In *Algebra Colloquium*, volume 17, pages 223–227. World Scientific, 2010.

[14] Eugene Spiegel. Calculating commutators in groups. *Math. Mag.*, 49(4):192–194, 1976.

[15] Ol'shanskii. A. Y. Groups of bounded period with subgroups of prime order. *Algebra i Logika*, 21(5):553–618, 1982.