Quais são os grupos simples de ordem menor que 60?

Lucimeire Alves de Carvalho
Isabella Maciel Torres

Atena Editora
Ano 2023

Quais são os grupos simples de ordem menor que 60?

Lucimeire Alves de Carvalho
Isabella Maciel Torres

Atena Editora
Ano 2023

CIÊNCIAS EXATAS E DA TERRA E ENGENHARIAS

Editora chefe
Profª Drª Antonella Carvalho de Oliveira
Editora executiva
Natalia Oliveira
Assistente editorial
Flávia Roberta Barão
Bibliotecária
Janaina Ramos
Projeto gráfico
Camila Alves de Cremo
Ellen Andressa Kubisty
Luiza Alves Batista
Nataly Evilin Gayde
Imagens da capa
iStock
Edição de arte
Luiza Alves Batista

CIÊNCIAS EXATAS E DA TERRA E ENGENHARIAS

Quais são os grupos simples de ordem menor que 60?

Diagramação: Natália Sandrini de Azevedo
Correção: Mariane Aparecida Freitas
Indexação: Amanda Kelly da Costa Veiga
Revisão: As autoras
Autoras: Lucimeire Alves de Carvalho
Isabella Maciel Torres

Dados Internacionais de Catalogação na Publicação (CIP)

C331 Carvalho, Lucimeire Alves de
Quais são os grupos simples de ordem menor que 60? / Lucimeire Alves de Carvalho, Isabella Maciel Torres. – Ponta Grossa - PR: Atena, 2023.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-65-258-1494-0
DOI: https://doi.org/10.22533/at.ed.940230707

1. Teoria dos grupos. 2. Grupos simples. I. Carvalho, Lucimeire Alves de. II. Torres, Isabella Maciel. III. Título.
CDD 512.7

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora
Ponta Grossa – Paraná – Brasil
Telefone: +55 (42) 3323-5493
www.atenaeditora.com.br
contato@atenaeditora.com.br

DECLARAÇÃO DAS AUTORAS

As autoras desta obra: 1. Atestam não possuir qualquer interesse comercial que constitua um conflito de interesses em relação ao conteúdo publicado; 2. Declaram que participaram ativamente da construção dos respectivos manuscritos, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final do manuscrito para submissão.; 3. Certificam que o texto publicado está completamente isento de dados e/ou resultados fraudulentos; 4. Confirmam a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhecem terem informado todas as fontes de financiamento recebidas para a consecução da pesquisa; 6. Autorizam a edição da obra, que incluem os registros de ficha catalográfica, ISBN, DOI e demais indexadores, projeto visual e criação de capa, diagramação de miolo, assim como lançamento e divulgação da mesma conforme critérios da Atena Editora.

DECLARAÇÃO DA EDITORA

A Atena Editora declara, para os devidos fins de direito, que: 1. A presente publicação constitui apenas transferência temporária dos direitos autorais, direito sobre a publicação, inclusive não constitui responsabilidade solidária na criação dos manuscritos publicados, nos termos previstos na Lei sobre direitos autorais (Lei 9610/98), no art. 184 do Código Penal e no art. 927 do Código Civil; 2. Autoriza e incentiva os autores a assinarem contratos com repositórios institucionais, com fins exclusivos de divulgação da obra, desde que com o devido reconhecimento de autoria e edição e sem qualquer finalidade comercial; 3. Todos os e-book são *open access, desta forma* não os comercializa em seu site, sites parceiros, plataformas de *e-commerce,* ou qualquer outro meio virtual ou físico, portanto, está isenta de repasses de direitos autorais aos autores; 4. Todos os membros do conselho editorial são doutores e vinculados a instituições de ensino superior públicas, conforme recomendação da CAPES para obtenção do Qualis livro; 5. Não cede, comercializa ou autoriza a utilização dos nomes e e-mails dos autores, bem como nenhum outro dado dos mesmos, para qualquer finalidade que não o escopo da divulgação desta obra.

DEDICATÓRIA

Dedico essa conquista ao meu filho Henry, que mudou a minha perspectiva sobre a minha vida profissional e que certamente foi o acontecimento mais marcante da minha vida.

AGRADECIMENTOS

Agradeço primeiramente a Deus pela oportunidade de estar tão próxima da realizaçao de um sonho. Aos meus pais Jozimaura Souza Maciel e Pedro Araujo Torres por todo carinho e dedicação prestados. À toda minha família, de maneira especial Isadora, por todo apoio. Agradeço também ao meu esposo Túlio, que sempre me incentivou a não desistir.

Agradeço aos meus orientadores Lucimeire e Bruno por tamanho conhecimento transmitido e por toda atenção e motivação. Agradeço aos meus colegas por toda experiência compartilhada, de forma especial, agradeço à Ana Caroline que me ajudou durante todo esse percurso, provavelmente eu não estaria aqui neste momento sem seu apoio e lembretes.

Finalmente agradeço a todos os professores aos quais tive a honra de conhecer e conviver, levarei comigo lembranças, aprendizados e conselhos.

SUMÁRIO

RESUMO

Neste trabalho serão estudados conceitos importantes dentro da álgebra moderna, especificamente da teoria de grupos, que possibilitem construir uma base de conhecimentos prévios para que se alcance o objetivo do trabalho: Encontrar os grupos simples de ordem menor que 60. Um grupo *G* é dito simples se seus únicos subgrupos normais são os triviais, isto é, o grupo trivial formado pelo elemento neutro e o próprio *G.* Com base nesta definição e a ajuda dos Teoremas de Sylow iremos obter a classificação desejada.

PALAVRAS-CHAVE: Grupo. Subgrupo. Subgrupo Normal. Grupo Simples. p-grupos. Teoremas de Sylow.

ABSTRACT

In this work we will study important concepts of modern Algebra, specifically Group Theory, in order to construct the necessary knowledge to realize the objective of this work: finding the simple groups of order less than 60. *a* group *G* is called simple if its only normal subgroups are the trivial ones, that is, the identity subgroup and the whole group *G.* We will obtain our classification starting from this definition with the help of Sylow's theorems.

KEYWORDS: Group. Subgroup. Normal subgroup. Simple group. p-groups. Sylow's Theorems.

NOTAÇÕES

Seja (G,*) um grupo. Denotaremos apenas por G o grupo (G,*).

$\mathbb{Z}$: O conjunto dos números inteiros.

$\mathbb{Q}$: O conjunto dos números racionais.

e: elemento neutro.

a^{-1}: elemento inverso.

$\mathbb{Z}_n$: conjunto de classes módulo n.

$H \leq G$: H subgrupo de G.

$H \lhd G$: H subgrupo normal de G.

|G|: ordem de G.

$o(g_1)$: ordem do elemento g_1.

$Z(G)$: Centro de G.

$a \equiv b \ mod \ H$: a congruente a b mod H.

INTRODUÇÃO

O conceito de grupos é uma das ferramentas mais utilizadas na Matemática moderna. Seu conceito torna-se fundamental em vários campos da Ciência, a saber, na teoria quântica dos campos, nas estruturas atômica e molecular, na cristalografia, bem como na álgebra abstrata.

A teoria de Grupos surgiu ligada a tentativa de soluçõess de equaçõess polinomiais, de forma especial equaçõess de grau maior que 4, questionada por diversos matemáticos na história inclusive por Lagrange no século XVIII. No entanto, foi Évariste Galois (1811-1832) que revolucionou o campo da Álgebra ao introduzir o conceito de grupo solúvel, cujo objetivo era mostrar que a solubilidade dessas equaçõess por radicais dependia do fato de seu grupo ser solúvel ou não.

Tendo em vista a relevância da teoria de Grupos, iniciada por Galois, e aplicada até os dias atuais, vemos a importância de fazer um estudo geral de todos os conceitos básicos dessa grande área da Matemática.

A teoria de grupos está dividida em áreas e subáreas e os interesses são muitos. Vários problemas já foram apontados e alguns, solucionados dando assim destaque a muitos outros matemáticos e físicos.

De acordo com o Teorema de Lagrange, " se *G* é um grupo finito e H um subgrupo de G, então a ordem de *G* é igual ao produto da ordem de H pelo indice de H em *G"*. Este teorema é um dos resultados mais utilizados para embasar nosso trabalho, visto que como consequência dele temos que a ordem de qualquer subgrupo de *G* divide a ordem de *G.*

Aliados ao Teorema de Lagrange, veremos os Teoremas de Sylow. Sylow (1832-1918) foi um importante matemático e trouxe bastantes contribuiçõess para a Matemática, e especialmente no campo da Álgebra Abstrata. Sylow encontrou resultados que possibilitam conhecer as estruturas dos grupos quanto aos seus subgrupos.

Um dos problemas encontrados na teoria de Grupos é a classificação de Grupos simples finitos e vários são os resultados nesse sentido. Um grupo *G* é dito simples se os seus únicos subgrupos normais forem os triviais, ou seja, não há neste grupo subgrupos normais que não a identidade ou o próprio *G.* Foi proposto neste trabalho buscar meios a partir de conhecimentos já desenvolvidos até o momento no campo da Álgebra, de encontrar todos os grupos simples de ordem menor que 60, especificamente chegaremos a conclusão de que até a ordem 59, os grupos simples são apenas aqueles de ordem prima. O trabalho limitou-se a ordem 60 pois temos por exemplo o grupo A5 que é simples e não tem ordem prima mas sim ordem igual a 60. Detalhadamente faremos classificaçãoo destes grupos ,de modo a se tornar compreensível a futuros leitores.

No Capítulo 1, foram listados alguns dos conceitos e resultados acerca de grupos, subgrupos e classes laterais, bem como Homomorfismos e Isomorfismos, parte essencial

para este estudo. Foram também apresentados alguns exemplos a fim de que os conceitos fossem melhor fixados.

No Capitulo 2, foram apresentados e demonstrados os Teoremas de Sylow, estes por sua vez, possuem extrema importancia para que se alcance o principal objetivo deste trabalho: Classificar os grupos de ordem menor que 60.

Por fim, no Capítulo 3 mostramos os resultados obtidos a partir de toda a análise bibliográfica. Foram construídos lemas, e usados métodos a fim de que a classificaçãoo se tornasse possível. Assim foi feita a classificação de todos os grupos de ordem menor que 60 classificando-os em grupos simples ou não-simples. Para todos os casos mostramos de forma específica os teoremas e proposiçõess necessárias para que se classificasse determinado grupo.

Todo o trabalho será feito de modo que se conclua que, sendo G um grupo de ordem menor que 60, apenas aqueles cuja ordem seja um número primo serão simples, ou seja, todos os grupos de ordem não-prima, possuem subgrupos normais além dos triviais.

CAPÍTULO 1

TEORIA BÁSICA DOS GRUPOS

1 | NOÇÕES PRELIMINARES

Numerosos sao os resultados e aplicacões dos grupos, não apenas na Matematica, mas também em outras ciências como a Física, que utiliza-se das simetrias. A teoria de grupos se preocupa com o estudo de estruturas algébricas. Tendo em vista sua relevância, o objetivo deste capítulo é, então, apresentar definições, exemplos, teoremas e resultados acerca de Grupos que servirão de base para este trabalho.

Definição 1. Um conjunto não-vazio G é um grupo, se em G é definido uma operação binária, a qual denominamos *, tal que em G valem as seguintes propriedades:

(I) $a,b \in G$ implica que $a * b \in G$;

(II) a,b e $c \in G$ implica que $a * (b * c) = (a * b) * c$;

(III) Existe um elemento $e \in G$ tal que $\forall a \in G$, temos: $a * e = e * a = a$;

(IV) Para todo $a \in G$ existe $a^{-1} \in G$ tal que: $a * a^{-1} = a^{-1} * a = e$.

O item (I) se refere ao fechamento do conjunto, ou seja, operando quaisquer elementos deste com a operação definida, o resultado também encontra-se neste conjunto; o item (II) diz respeito a associatividade.

O item (III) nos aponta a existência de um elemento neutro, podendo também ser chamado de identidade, denotado geralmente por e, e finalmente o item (IV) garante a existência de um elemento inverso para qualquer elemento do conjunto, sabendo que ao operar um elemento com o seu inverso a operação resulta no elemento neutro do conjunto. Observaremos ao longo deste trabalho que para $a, b \in G$ nem sempre $a * b = b * a$.

Todavia quando isto ocorre, especificamente, este grupo é chamado de grupo **comutativo** ou **abeliano** em homenagem ao matemático norueguês Niels H. Abel (1802-1829).

Geralmente um grupo é expresso por $(G, *)$, lê-se: "grupo G, munido da operaçao $*$", entretanto, quando não causar ambiguidade usaremos G ao invés de $(G, *)$ para denotar um grupo com a operação $*$. Daqui para frente usaremos a notação multiplicativa $a \cdot b = ab$ em vez de $a * b$. Denotaremos por a^{-1} o elemento inverso de um elemento a e o elemento neutropor e. Na notação multiplicativa, pode-se denominar o elemento neutro por identidade.

Lema 1.1. *Se G é um grupo, então:*

(a) o elemento neutro de G é único;

(b) para qualquer $a \in G$ existe um único inverso de a, ou seja, a^{-1} é único;

(c) $\forall\ a \in G$, $(a^{-1})^{-1} = a$;

(d) para quaisquer $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demonstração. (a) Neste enunciado queremos mostrar que se dois elementos e e f pertencentes a G possuem a propriedade $a = a \cdot e = e \cdot e\ a = a \cdot f = f \cdot a$ para todo $a \in G$ então $e = f$.

Como $e \cdot a = a$, para todo $a \in G$ então, em particular $e \cdot f = f$. Por outro lado, para todo $b \in G$ temos $b \cdot f = b$ logo $e \cdot f = e$. Unindo então as informações temos que $f = e \cdot f = e$ conclui-se logo que $e = f$.

Em (b) queremos mostrar que se dado $a \in G$, se existem $x, y \in G$ tais que $x \cdot a = a \cdot x = e$ e $y \cdot a = a \cdot y = e$ então $x = y$.

Suponha que para a, x, y em G, $a \cdot x = e$ e $a \cdot y = e$ torna-se evidente que $a \cdot x = a \cdot y$. Neste ponto da demonstração não se sabe ainda o número de elementos $b \in G$ tal que $b \cdot a = e$ sabendo apenas que existe pelo menos um. Então existe $b \in G$ tal que $b \cdot a = e$. Desta forma $b \cdot (a \cdot x) = b \cdot (a \cdot y)$; usando a associatividade do grupo teremos :

$$x = e \cdot x = (b \cdot a) \cdot x = b \cdot (a \cdot x) = b \cdot (a \cdot y) = (b \cdot a) \cdot y = e \cdot y = y.$$

Logo $x = y$. Analogamente podemos mostrar que $x \cdot a = y \cdot a$ em um grupo G implica $x = y$. Isto quer dizer então que vale a lei do cancelamento para um elemento se este aparece do mesmo lado em ambos os membros da equação.

Em (c) queremos verificar que $\forall\ a \in G$, $(a^{-1})^{-1} = a$. Note que,

$$a^{-1} \cdot (a^{-1})^{-1} = e = e \cdot a^{-1}\, a$$

disso obtemos a seguinte equação $a^{-1} \cdot (a^{-1})^{-1} = a^{-1}\, a$. Cancelando a^{-1} à esquerda temos que $(a^{-1})^{-1} = a$

A fim de provar o item (d) vamos operar $ab \cdot b^{-1}a^{-1}$. Veja que,

$$ab \cdot b^{-1}a^{-1} = a \cdot (bb^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = e,$$

assim, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Exemplo 1.1.1. O conjunto dos números inteiros $\mathbb{Z}$ munido da operação de adição usual é um grupo. Em notaçao $(\mathbb{Z}; +)$.

Tomemos a, b e $c \in \mathbb{Z}$, temos que:

(I) $a + b \in \mathbb{Z}$, entao $(\mathbb{Z}; +)$ é fechado;

(II) $(a + b) + c = a + (b + c)$, pois a soma nos inteiros é associativa;

(III) Note que, para qualquer $a \in \mathbb{Z}$, $0 + a = a + 0 = a$, logo 0 é o elemento neutro de $(\mathbb{Z}, +)$;

(IV) Para todo $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$ e $a + (-a) = 0$.

Logo, $(\mathbb{Z}; +)$ é um grupo.

Exemplo 1.1.2. O conjunto dos números racionais $\mathbb{Q} - \{0\}$ munido da operação multiplicação é um grupo. Em notação $(\mathbb{Q} - \{0\} , \cdot)$

Tome $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}$ logo o conjunto $(\mathbb{Q} - \{0\} , \cdot)$ é fechado.

É óbvio que em $(\mathbb{Q} - \{0\} ; \cdot)$ vale a associatividade, e o elementro neutro no produto é 1, além disso se $\frac{a}{b} \in \mathbb{Q} - \{0\}$, temos que $\frac{a}{b} \cdot \frac{b}{a} = 1$.

Logo, $(\mathbb{Q} - \{0\}, \cdot)$ é um grupo.

2 | CONGRUÊNCIAS

Definição 2. Dados os conjuntos A e B, o *produto cartesiano* de A por B, denotado $A \times B$ (lê-se: A cartesiano B), é o conjunto formado por todos os pares ordenados (a, b), onde $a \in A$ e $b \in B$, isto é

$$A \times B = \{(a, b) \mid \forall a \in A, \forall b \in B \}.$$

Definição 3. Dados os conjuntos A e B, uma *relação* R de A em B, denotada $R : A \to B$ (lê-se: R de A em B), é qualquer subconjunto do produto cartesiano $A \times B$.

Definição 4. Uma relação R sobre um conjunto não-vazio E é denominado relação de equivalêcia sobre E se, e somente se, R é reflexiva, simétrica e transitiva, ou seja, R deve cumprir as seguintes propriedades:

(I) *se* $x \in E$, então xRx.

(II) se $x, y \in H$ e xRy então yRx.

(III) *se* $x, y, z \in$ H e xRy, yRz então xRz.

Lema 1.2. *A relação congruência módulo m, define uma relação de equivalência sobre o conjunto dos números inteiros.*

Demonstração. De fato, como $m \mid 0$, temos que $m \mid (a - a)$ logo $a \equiv a \ mod \ m$ para todo $a \in \mathbb{Z}$. Agora, se $a \equiv b \ mod \ m$ então $m \mid (a - b)$ e, portanto $m \mid (b - a) = -(a - b)$; logo $b \equiv a \ mod \ m$. Por fim, se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$ então $m \mid (b - a)$ e $m \mid (b - c)$. Logo, $m \mid (a - b) + (b - c)$, ou seja, $m \mid (a - c)$ o que mostra que $a \equiv c \ mod \ m$.

Definição 5. Seja m um inteiro positivo fixo. Se a é um inteiro qualquer então a classe residual módulo m de a, denotada por $\bar{a}$, consiste do conjunto formado por todos os inteiros que são congruentes ao inteiro a módulo m, isto é,

$$\bar{a} = \{x \in \mathbb{Z} : x \equiv a \ (mod \ m)\} = \{ x \in \mathbb{Z} : m \mid x - a\} = \{a + km : k \in \mathbb{Z}\}$$

O conjunto formado por todas as classes residuais módulo m, é denotado por $\mathbb{Z}_m$, ou seja,

$$\mathbb{Z}_m = \{\bar{a} : a \in \mathbb{Z}\}$$

Proposição 1.1. *Seja m um inteiro positivo fixo e sejam* $\bar{a}$ *e* $\bar{b}$ *as classes residuais módulo m de dois inteiros quaisquer de a* e *b. Então:*

1. $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \ (mod\ m)$.

2. $\bar{a} \cap \bar{b} = \emptyset$ ou $\bar{a} = \bar{b}$.

Demonstração. 1. Devemos mostrar que $\bar{a} \subset \bar{b}$ e $\bar{b} \subset \bar{a}$. Tome $x \in \bar{a}$, então $x \equiv a \ mod\ m$. Por hipótese, $a \equiv b \ mod\ m$ assim, por transitividade $x \equiv b \ mod\ m \Rightarrow b \equiv x \ mod\ m$ logo $x \in \bar{b}$. De modo análogo prova-se que se $x \in \bar{b} \rightarrow x \in \bar{a}$. Reciprocamente, como $a \equiv a \ mod\ m$ e $b \equiv b \ mod\ m$ temos que $a \in \bar{a}$ e $b \in \bar{b}$, se $\bar{a} = \bar{b}$ entao, em particular $a \in \bar{a} \Rightarrow a \in \bar{b} \Rightarrow a \equiv b \ mod\ m$.

2. Suponha que exista $x \in \bar{a} \cap \bar{b}$, assim $x \equiv a \ mod\ m$ e $x \equiv b \ mod\ m$ logo, $a \equiv b \ mod\ m$ o que gera pelo item 1) que $\bar{a} = \bar{b}$. Assim, $\bar{a} \cap \bar{b} = \emptyset$ ou $\bar{a} = \bar{b}$.

Proposição 1.2. *O conjunto* $\mathbb{Z}_m$ *tem exatamente m elementos.*

Demonstração. Vamos mostrar que $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m\text{-}1}\}$ e que $\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m\text{-}1}\}$ tem exatamente *m* elementos.

1) É fácil ver que $\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m\text{-}1}\} \subset \mathbb{Z}_m$.

2) Seja $\bar{a} \in \mathbb{Z}_m$, com $a \in \mathbb{Z}$. Pelo algoritmo da divisão de a por m, existem inteiros q e r tais que $a = mq + r$, $0 \leq r \leq m - 1$. Assim $a - r = mq$, onde $m \mid a - r$. Logo $a \equiv r (mod\ m)$ e, pela proposição anterior, temos $\bar{a} = \bar{r}$. Como $0 \leq r \leq m - 1$ então $\bar{a} = \bar{r} \in \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m\text{-}1}\}$. Portanto, $\mathbb{Z}_m \subset \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m\text{-}1}\}$.

De (1) e (2) concluímos que $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m\text{-}1}\}$.

3) Suponha $\bar{r} = \bar{s}$, onde $r, s \in \mathbb{Z}$ tais que $0 \leq r < s \leq m - 1$. Pela proposição anterior temos que $r \equiv s (mod\ m)$. Assim, $s \equiv r (mod\ m)$ e $m \mid s - r$. O que é absurdo, pois $0 < s - r < m$. Portanto, $\{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m\text{-}1}\}$ tem m elementos.

Adição e Multiplicação em $\mathbb{Z}_m$

Seja m um inteiro positivo fixo. Vamos definir as operações de de adição e multiplicação no conjunto $\mathbb{Z}_m$ das classes residuais modulo m.

Sejam $\bar{a}, \bar{x}, \bar{b}, \bar{y}, \in \mathbb{Z}_m$. Temos que se $\bar{a} = \bar{x}$ e $\bar{b} = \bar{y}$, então $a \equiv x \ (mod\ m)$ e $b \equiv y \ (mod\ m)$; logo $a + b \equiv x + y \ (mod\ m)$ e $ab \equiv xy \ (mod\ m)$ e consequentemente, $\overline{a+b} = \overline{x+y}$ *e* $\overline{ab} = \overline{xy}$.

Note que até o momento os grupos apresentados ja são bastante conhecidos, assim como suas propriedades,em ambos os casos tínhamos grupos com infinitos elementos. Veremos agora um exemplo em que o grupo tem uma quantidade finita de elementos, e que

sua estrutura possui características distintas de qualquer outra estrutura algébrica, veja:

Exemplo 1.2.1. O conjunto aditivo de classes módulo n é um grupo $G : (\mathbb{Z}_n, +)$

É fácil notar que para esta operação $\mathbb{Z}_n$ é fechado, pois realizando a soma entre quaisquer $\bar{a}$, $\bar{b} \in \mathbb{Z}_n$ ou $\overline{a+b}$ já está listado em $\mathbb{Z}_n$ ou é côngruo a algum elemento, já que cada elemento representa uma classe módulo n. Podemos ver também que esta operação é associativa e comutativa.

$$\bar{a} + \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} + \bar{a}$$

Existe $\bar{0}$ tal que para todo $\bar{a} \in \mathbb{Z}_n$, $\bar{a}+ \bar{0}= \bar{0}+\bar{a}= \bar{a}$, logo $\bar{0}$ é o elemento neutro de $(\mathbb{Z}_n+)$.

Para que $(\mathbb{Z}_n, +)$ seja grupo precisamos encontrar a^{-1} para cada elemento $\bar{a}$ de $\mathbb{Z}_n$.

Para todo $\bar{a} \in$ Z, tome o elemento: $\overline{n-a}$. Pela associatividade e comutatividade do conjunto, podemos notar que:

$$\bar{a}+ \overline{n-a} = \overline{a+n-a}= \bar{n}=\bar{0}$$

Assim, $\overline{n-a}$ é o oposto de $\bar{a}$ para todo $\bar{a} \in \mathbb{Z}$.

Conclui-se então que $(\mathbb{Z}_n, +)$ é grupo para todo n natural com $n > 1$.

Nota-se que para todos os exemplos dados anteriormente os grupos eram abelianos, definiremos agora um exemplo muito importante de um grupo não-abeliano.

3 | GRUPO SIMÉTRICO

Seja X um conjunto, uma permutação de X é um bijeção $X \to X$. O grupo simétrico de X, é o conjunto $G = Sym(X)$ de todas as permutações de X com a operação composição.

É importante lembrar que a composição entre duas funções $f, g : X \to X$ é a função $fg = f \circ g$ definida assim: $(f \circ g)(x) := f\,(g(x))$. A função $f : X \to X$ tal que $f(x) = x$ para todo $x \in X$ é chamada identidade e será denotada por *id.*

Se $X = \{1, ..., n\}$ usa-se a notação S_n para denotar $Sym(X)$.

Exemplo 1.3.1. Seja $X = \{1, 2, 3\}$ assim $G = S_3$. Para descrever uma permutação f de X precisamos das imagens dos elementos 1, 2 e 3, isto é, dos elementos $f(1)$, $f(2)$, $f(3)$. Usa-se geralmente a notação:

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$$

S_3 possui 6 permutações, a saber:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

As permutações listadas compreendem todos os elementos de S_3. Vamos provar agora que é grupo.

Demonstração. O fechamento e a associatividade são óbvios. Sabe-se também que a identidade é o elemento neutro, restando provar que para todo elemento de $G = S_3$, existe elemento inverso em S_3. Sejam

$$\psi_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \psi_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \psi_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\ \psi_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\psi_5=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \psi_6=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \text{ elementos de } S_3$$

Operando $\psi_1 \cdot \psi_1$ isto resulta no elemento neutro. Operando ψ_2^2 temos

$$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

que é o elemento neutro. O mesmo acontece com ψ_3^2 e ψ_5^2.

Operando agora os elem ntos restantes, temos que :

$$\psi_4 \cdot \psi_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

Mostrando assim que todo elemento em S_3 possui inverso logo S_3 é grupo.

Ordem do Grupo e de seus elementos

Definição 6. A ordem de um grupo finito G corresponde à quantidade de elementos que este possui e é denotada por $|G|$.

Definição 7. Seja G um grupo, a ordem de um elemento $a \in G$ denotada por $o(a)$ é o menor inteiro positivo n, tal que:

$$a^n = e$$

onde e é o elemento neutro/identidade do grupo.

Exemplo 1.3.2. Note que no exemplo anterior, $o(\psi_1) = 1$, $o(\psi_2) = o(\psi_3) = o(\psi_5) = 2$ restando descobrir a ordem dos elementos ψ_4 e ψ_6.

$$\psi_4\cdot\psi_4=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$\psi_4^3=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

disso temos que $o(\psi_4 = 3)$. Fazendo o mesmo processo com ψ_6 teremos,

$$\psi_6\cdot\psi_6=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\psi_6^3=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

o que nos mostra que $o(\psi_6) = 3$.

Já foi verificado anteriormente que $(\mathbb{Z}_n, +)$ é grupo para todo n natural com $n > 1$, vejamos então um exemplo que trata sobre a ordem dos elementos de $\mathbb{Z}_6$:

Exemplo 1.3.3. Seja G: $(\mathbb{Z}_6, +)$, o grupo aditivo de classes módulo 6, podendo ser denotado por: $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. O elemento neutro deste grupo é $\bar{0}$.

Para descobrir a ordem de cada elemento do grupo devemos operá-lo com ele mesmo repetidas vezes até que se obtenha $\bar{0}$. Veja:

$\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}+\bar{1}=\overline{1+1+1+1+1+1}=\bar{6}=\bar{0}$

$\bar{2}+\bar{2}+\bar{2}=\bar{6}=\bar{0}$

$\bar{3}+\bar{3}=\bar{6}=\bar{0}$

$\bar{4}+\bar{4}+\bar{4}=\bar{12}=\bar{0}$

$\bar{5}+\bar{5}+\bar{5}+\bar{5}+\bar{5}+\bar{5}=\bar{30}=\bar{0}$

Assim $o(\bar{1})=6$, $o(\bar{2})=3$, $o(\bar{3})=2$, $o(\bar{4})=3$, $o(\bar{5})=6$,

Note que, nos exemplos acima podemos calcular a ordem de qualquer elemento de S_3 ou de $\mathbb{Z}_6$. Já nos exemplos 1.1.1 e 1.1.2 fora a identidade, não existem nesses grupos nenhum elemento de ordem finita.

4 | SUBGRUPOS

Definição 8. Um subconjunto H de um grupo G é dito um subgrupo de G e denotado por $H \leq G$ se, com a mesma operação definida em G, o próprio H forma um grupo. É fácil ver que se G é grupo então $G \leq G$ e $\{e\} \leq G$ esses subgrupos são denominados **subgrupos triviais.**

Lema 1.3. *Um subconjunto não-vazio H de um grupo G será um subgrupo de G se, e somente se,*

(1) H é fechado;

(2) $\forall a \in H$, $a^{-1} \in H$, *ou seja, todo elemento de H possui elemento inverso também pertencente a H.*

Demonstração. As afirmações (1) e (2) são verdadeiras uma vez que H é grupo. Reciprocamente temos de verificar que se valem (1) e (2) então $H \leq G$.

Temos que H é fechado, e que todo elemento possui inverso em H, restando provar que $e \in H$ e que vale a associatividade.

Tome $a \in H$. Sabemos que $a^{-1} \in H$. Operando os dois elementos temos $a \cdot a^{-1} = e$ que pertence a H já que este é fechado. Logo $e \in H$.

Como os elementos de H estão em G vale a associatividade também em H.

Vamos provar agora que a partir de dois subgrupos de um dado grupo G podemos

gerar novos subgrupos.

Teorema 1.3. *Se H_1 e H_2 são subgrupos de um grupo de um grupo G, então $H_1 \cap H_2 \leq H_1$ e $H_1 \cap H_2 \leq H_2$. Em particular, se H_1 e H_2 são dois subgrupos distintos de G, com $|H_1| = |H_2| = p$, então $H_1 \cap H_2 = \{e\}$.*

Demonstração. De fato, tome $x, y \in H_1 \cap H_2$ então:

$$x \in H_1 \Rightarrow x^{-1} \in H_1$$

$$x \in H_2 \Rightarrow x^{-1} \in H_2$$

$$y \in H_1 \Rightarrow y^{-1} \in H_1$$

$$y \in H_2 \Rightarrow y^{-1} \in H_2$$

Como $xy^{-1} \in H_1$ e $xy^{-1} \in H_2$ pelo fechamento dos subgrupos, então $xy^{-1} \in H_1 \cap H_2$

Exemplo 1.4.1. Seja *G* um grupo. Então

$$Z(G) = \{a \in G : ax = xa \ \forall x \in G\}$$

é um subgrupo de *G* e *Z(G)* é denominado centro do grupo *G.*

Demonstração. Sabe-se que $e \in Z(G)$ pois $xe = ex = x$, $\forall x \in G$. Dados $a, b \in Z(G)$, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, para todo $x \in G$. Logo, $ab \in Z(G)$ o que nos mostra que *Z(G)* é fechado. Tomando $a \in Z(G)$, então $ax = xa$, $\forall x \in G$. Além disso, $a^{-1}(ax) = a^{-1}(xa) \Rightarrow x = (a^{-1}x)a \Rightarrow xa^{-1} = (a^{-1}x)aa^{-1} = a^{-1}x$, ou seja, $xa^{-1} = a^{-1}x$, $\forall x \in G$ e portanto, $a^{-1} \in Z(G)$. Concluindo assim que *Z(G)* é subgrupo de *G.* A comutatividade de *Z(G)* sai da própria definição do conjunto, pois se os elementos que estão em *Z(G)* comutam com todos os elementos de *G* em particular eles comutam entre si.

Definição 9. Seja *p* um primo. Um grupo *G* (não necessariamente finito) no qual todo elemento tem sua ordem igual a uma potência de *p* é chamado de *p*-grupo.

Em particular, *p*-grupos finitos são os grupos cuja ordem é uma potência de *p.*

4.1 Grupos Ciclicos

Seja *G* um grupo qualquer e $a \in G$. É possível mostrar que o conjunto das potências de *a*, $\langle a \rangle = \{a^i \mid i = 0, \pm 1, \pm 2, ...\}$ é um subgrupo de *G*, e será denominado o **subgrupo cíclico** gerado por *a.* Se para um certo $a \in G$ temos $G = \langle a \rangle$, então *G* é dito um grupo cíclico. Os grupos cíclicos são exemplos de grupos abelianos, por isso sua importância. Mas a recíproca não é verdadeira.

Exemplo 1.4.2

$$\mathbb{Z} = \langle 1 \rangle \quad \text{e} \quad \mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$$

Exemplo 1.4.3. $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$

Note que *H* é sub grupo cíclico de S_3.

4.2 Classes Laterais e Teorema de Lagrange

Definição 10. Se G é um grupo e $H \leq G$, para $a, b \in G$ diz-se que a é congruente a b mod H, indicando por $a \equiv b \bmod H$ se $ab^{-1} \in$ H.

Lema 1.4. *A relação $a \equiv b$ mod H é uma relação de equivalência.*

Demonstração. Para que a relação de congruência entre a e b seja de equivalência temos de verificar se valem as seguintes afirmações: Para todos $a, b, c \in G$ valem:

(1) $a \equiv a$ mod H ;

(2) $a \equiv b$ mod H implica $b \equiv a$ mod H ;

(3) $a \equiv b$ mod H , $b \equiv c$ mod H implica $a \equiv c$ mod H .

(1) Como $H \leq G$ então $e \in G$. Logo, para todo $a \in$ G, temos $aa^{-1} = e \in$ H, assim, $a \equiv a \, mod H$.

(2) Por definição se $a \equiv b$ mod H então $ab^{-1} \in$ H. Observe que $(ab^{-1})^{-1} = ba^{-1}$.

Como $H \leq G$, se $ab^{-1} \in H$, $ba^{-1} \in H$. Assim como $ba^{-1} \in H$ então $b \equiv a \, mod \, H$.

(3) Se $a \equiv b \, mod \, H$ e $b \equiv c \, mod \, H$, então $ab^{-1} \in H$ e $bc^{-1} \in H$ pois $H \leq G$, logo é fechado assim, $ab^{-1}bc^{-1} = ac^{-1} \in H$. Logo da definição temos que $a \equiv c \, mod \, H$.

Definição 11. Se H é um subgrupo de G, $a \in G$, então $Ha = \{ha \mid h \in H\}$, o conjunto. Ha é denominado **classe lateral à direita de H em G.**

De forma análoga podemos definir a classe lateral à esquerda de H em G denotada por aH.

Lema 1.5. Para todo $a \in$ G,

$$Ha = \{x \in G \mid a \equiv x \, mod \, H\}$$

Demonstração. Seja $[a] = \{x \in G \mid a \equiv x \, mod \, H\}$, mostraremos inicialmente que $Ha \subseteq [a]$. De fato, para $h \in H$ temos $a(ha)^{-1} = aa^{-1}h^{-1} = h^{-1}$, que está em H pois H é subgrupo de G. Pela definição de congruência $mod \, H$ isto implica que ha $\in [a]$ $\forall h \in H$, entao $Ha \subseteq [a]$.

Tomando agora $x \in [a]$, sabe-se que $ax^{-1} \in H$ pela definição de congruência.

Sabemos que $(ax^{-1})^{-1} \in H$ e ainda que $(ax^{-1})^{-1} = xa^{-1} = h$ para algum $h \in H$. Multiplicando os dois membros da equação por a pela direita teremos $x = ha$, logo $x \in Ha$. Desta forma $[a] \subseteq Ha$ concluimos então que se $Ha \subseteq [a]$ e $[a] \subseteq Ha$, $Ha = [a]$

Este lema nos diz que Ha é a **classe de equivalência** de a em G, o que da proposição 1.1 gera que duas quaisquer classes laterais à direita de H em G ou são idênticas ou não tem elementos em comum.

Lema 1.6. *Existe uma correspondência bijetora entre duas quaisquer classes laterais à direita de H em G.*

Demonstração. Associando um elemento $ha \in Ha$, com $h \in H$ e $a \in G$, ao elemento $hb \in Hb$ com $b \in G$ é fácil ver que esta aplicação é sobrejetora. Podemos afirmar que a

aplicação tambem é injetora, pois para $h_1b = h_2b$, com $h_1, h_2 \in H$ pela lei do cancelamento em G, teremos que $h_1 = h_2$, e assim $h_1a = h_2a$.

Este lema diz que o tamanho das classes laterais de H em G são iguais. Assim no caso em que G é finito, o tamanho de G seria um múltiplo do tamanho de H.

Corolário 1.4. *Seja G um grupo e H um subgrupo de G. Todas as classes laterais à esquerda e à direita de H em G, possuem o tamanho de H.*

Demonstração. Basta notar que uma das classes laterais é o próprio $He = H$, pelo lema anterior como existe uma bijeção entre quaisquer classes laterais o mesmo vale para $He = H$. O que indica que $|He| = |H| = |Ha|$, para qualquer $a \in G$.

Corolário 1.5. *A união de todas as classes laterais de H em G é o próprio G.*

Demonstração. Sabemos que podemos obter uma classe lateral para cada elemento de G pois como H é subgrupo de G, $e \in H$. Pelo lema 1.5 duas classes laterais de H em G ou são iguais ou são disjuntas, ou seja, sem intersecções. Desta forma, o conjunto de todas as classes laterais de G acabam por resultar no próprio G.

Definição 12. O conjunto formado por todas as classes laterais de H em G é denotado por $G/H = \{Ha_1, Ha_2, Ha_3, ..., Ha_n\}$, com $a_1, a_2, a_3, ... , a_n \in G$.

Definição 13. Se H é um subgrupo de G, o índice de H em G é o número de classes laterais à direita ou a esquerda de H em G, sendo indicado por $i_G(H)$ ou $(G : H)$.

Subgrupos Normais e Grupos Quocientes

Definição 14. Um subgrupo H *é* dito um **subgrupo normal** de G se para todo $g \in G$ e $h \in H$, $ghg^{-1} \in H$.

Está é uma das definições mais importantes de todo o trabalho, isto por que, neste trabalho classificamos os grupos quanto a existência de subgrupos normais não-triviais. Observe que se o grupo for abeliano, os seus subgrupos também serão. Como consequência todo subgrupo H de um grupo abeliano G, é normal em G, pois por definição $H \triangleleft G$ se para todo $G \in G$ e $h \in H$, $ghg^{-1} \in H$, porém $ghg^{-1} = gg^{-1}h = h \in H$. Logo $H \triangleleft G$.

Definição 15. Seja G um grupo. Se os únicos subgrupos normais de G forem os triviais, isto é, G e $\{e\}$, então G é denominado como grupo simples.

Lema 1.7. N *é subgrupo normal de G se, e somente se,* $gNg^{-1} = N$ *para todo* $G \in G$

Demonstração. Se $gNg^{-1} = N$ para todo $g \in$ G, é facil ver que $gNg^{-1} \subset N$. Logo N é normal em G. Suponhamos agora que N seja normal em G, desta forma como $g^{-1}Ng \subset N$, $N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$ portanto $N = gNg^{-1}$

Um teorema interessante sobre subgrupos normais é:

Teorema 1.6. (Subgrupos de índice 2 no Grupo). *Se um grupo N de G tem índice 2,* $(G : N) = 2$*, então N é normal em G.*

Demonstração. Se $N \leq G$ e $(G : N) = 2$, então N possui duas classes laterais a direita de G, uma delas é N_e. Assim, para um $a \in G$, temos Na também é uma classe lateral a direita de N. Mas se o produto de duas quaisquer classes laterais a direita de N ainda for uma classe lateral a direita de N, então N é normal em G. Mas $NeNa = NNa = Na \Rightarrow N$ é normal em G.

Lema 1.8. *O subgrupo H de G é subgrupo normal de G se, e somente se, toda classe lateral à direita de H em G, é uma classe lateral à esquerda de H em G.*

Lema 2.10 demonstrado em [4]. Este lema é de extrema importância para a demonstração do resultado que veremos no corolário que se segue.

Corolário 1.7. *Se H é um subgrupo normal de G, então NaNb = Nab.*

Demonstração. Se $H \lhd G$ *e* $a, b \in G$ pelo Lema anterior, $aH = Ha$, e portanto, ao operar duas classes Ha e Hb, temos

$$HaHb = H(aH)b = H(Ha)b = HHab = Hab$$

assim, $(Ha)(Hb) = Hab$.

Motivados por esta propriedade, naturalmente podemos então definir, no caso em que H é normal em G, um produto entre classes laterais de G/H, ou seja, dados duas classes laterais Ha e Hb em G/H, definimos o produto dessas duas classes por $HaHb = Hab$. Com esta operação observamos que valem as seguintes propriedades:

1. Para todos $X, Y \in G/H$ implica $XY \in G/H$. De fato, se $X = Ha$, $Y = Hb$, com a, b G, então

$$XY = HaHb = Hab \in G/H.$$

Assim o conjunto G/H é fechado com essa operação.

2. Sejam $X, Y, Z \in G/H$ e $Z = Hc$, então $X(Y Z) = (XY)Z$. De fato, $X(Y Z) = Ha(HbHc) = Ha(Hbc) = Habc = H(ab)c = (HaHb)Hc = (XY)Z$. Assim vale a associatividade.

3. Considere o elemento $H = He \in G/H$. Se $X = Ha$, com $a \in G$ então

$$XH = HaHe = Hae = Ha = X.$$

Assim $H = He$ é o elemento neutro.

4. Sendo $X = Ha \in G/H$ com $a \in G$, $Ha^{-1} \in G/H$, e

$$HaHa^{-1} = Haa^{-1} = He = H.$$

Como já vimos, um conjunto com essas características é um grupo.

Definição 16. Se G é um grupo, H um subgrupo normal de G, então G/H também será denominado de grupo quociente ou grupo fator de G por H.

O centro de um grupo sempre é normal no grupo, uma vez que é formado pelos elementos do grupo que comutam com todos os elementos. A partir da definição acima, temos um interessante resultado relacionado ao quociente de um grupo por seu centro. Este

próximo resultado tem muita relevância quando o grupo em questão é um *p*-grupo, pois o mesmo garante que o centro de um p-grupo nunca é trivial.

Proposição 1.8. Seja G um grupo e seja $Z(G)$ seu centro. Se o quociente $G/Z(G)$ é cíclico, então $Z(G) = G$. Em particular, o índice de $Z(G)$ em G nunca é igual a um número primo.

Demonstração. Seja $\bar{z}$ um gerador do grupo $G/Z(G)$. então, $\forall g \in G$, $\exists i$ tal que $\bar{g} = \bar{z}^i$, logo tal que $G = z^i h$ com $h \in Z(G)$. Se $g_1 = z^{i_1} h_1$ e $g_2 = z^{i_2} h_2$ são dois elementos quaisquer de G, temos

$$g_1 g_2 = z^{i_1} h_1 z^{i_2} h_2 = z^{i_1+i_2} h_1 h_2 = z^{i_2} h_2 z^{i_1} h_1 = g_2 g_1$$

pois h_1 e h_2 comutam com qualquer elemento de G. Concluindo assim que o grupo é abeliano, logo $Z(G) = G$.

Lema 1.9. *Seja p um número primo. Então todo grupo G de ordem p^2 é abeliano.*

Demonstração. Como $Z(G) \leq G$, então $|Z(G)|$ divide $|G|$. Portanto se $|G| = p^2$, temos que $|Z(G)| \in \{1, p, p^2\}$, por outro lado sabemos pela Proposição 1.8 que o centro de um grupo não pode ter índice no grupo igual a um primo, logo $|Z(G)| \neq p$. Como a ordem de G é um número primo, G é um p-grupo, logo seu centro nunca é trivial, ou seja, $|Z(G)| \neq 1$ e portanto, $|Z(G)| = p^2$, sendo então G abeliano.

Teorema 1.9. (Teorema de Lagrange). *Seja G um grupo e H um subgrupo de G . Então* $|G| = |H| \cdot (G : H)$. *Em particular a ordem e o índice de H em G dividem a ordem de G.*

Demonstração. Suponha $(G : H) = r$ e seja $G/H = \{H_{a_1}, H_{a_2}, H_{a_3}, ..., H_{a_r}\}$. Pelo corolário 1.5

$$G = \{H_{a_1} \cup H_{a_2} \cup H_{a_3} \cup ... \cup H_{a_r}\} \text{ onde } H_{a_i} \cap H_{a_j} = \emptyset$$

Pelo corolário 1.4 sabemos que todas as classes laterais à direita de H tem o tamanho de H, ou seja $|H|$. Assim

$$|G| = |H_{a_1}| + |H_{a_2}| + ... + |H_{a_r}| = |H| + |H| + |H| + ... + |H| \text{ (r vezes)}$$

Logo $|G| = r \cdot |H| \Rightarrow |G| = (G : H) \cdot |H|$, como consequência temos que $|H|$ divide $|G|$, e $(G : H)$ divide $|G|$.

5 | HOMOMORFISMO DE GRUPOS

Um homomorfismo é uma aplicação de um sistema algébrico em outro sistema algébrico semelhante que conserva a estrutura. Tornamos isto preciso para grupos na definição a seguir.

Definição 17. Uma aplicaçao ψ de um grupo $(G, \cdot)$ em um grupo $(\bar{G}, *)$ é dita um homomorfismo se, para todo $a, b \in G$ temos,

$$\psi(a \cdot b) = \psi(a) * \psi(b)$$

Quando a aplicação acima é uma bijeção, dizemos que ela é um **isomorfismo**, ou que os grupos $(G, \cdot)$ e $(\bar{G}, *)$ são isomorfos.

Propriedades elementares

Seja $f : (G, \cdot) \to (G, x)$ um homomorfismo de grupos. Então:

1) $f(e_G) = e_G$.

De fato, $f(e_G) = f(e_G \cdot e_G) = f(e_G) \times f(e_G)$.

2) $f(x^{-1}) = f(x)^{-1}$.

De fato, $e_G = f(e_G) = f(x \cdot x^{-1}) = f(x) \times f(x^{-1})$

3) $kerf := \{x \in G \mid f(x) = e_G\}$ é um subgrupo normal de G chamado núcleo do homomorfismo f .

Demonstração. Primeiramente, vejamos que ker $f \leq G$. Dados $x, y \in \ker f$, temos:

$$f(x \cdot y) = f(x) \times f(y) = e_G \times e_G = e_G,$$

$$f(x^{-1}) = f(x)^{-1} = e_G{}^{-1} = e_G ;$$

portanto $ker\ f \leq$ G. Para provar que ker $f \triangleleft G$ devemos mostrar que:

$$gxg^{-1} \in ker\ f, \forall g \in G\ e\ \forall x \in ker\ f.$$

De fato, temos

$$f(gxg^{-1}) = f(g) \times f(x) \times f(g^{-1}) = f(g) \times e_G \times f(g)^{-1} = f(g) \times f(g)^{-1} = e_G.$$

Lema 1.10. *Seja $\rho : (G, \cdot) \to (\bar{G}, *)$ um homomorfismo de grupos. Então $Im(\rho) = \rho(G) \leq \bar{G}$.*

Demonstração. De fato, sejam $x, y \in \rho(G)$ então existem $g_1, g_2 \in G$ tais que $X = \rho(g_1)$ e $y = \rho(g_2)$. Pelo fato de ρ ser homomorfismo, temos

$$x * y = \rho(g_1) * \rho(g_2) = \rho(g_1 \cdot g_2)$$

logo $x * y \in \rho(G)$. Note também que, se $x = \rho(g_1)$, $G^{-1} \in G$ e $\rho(g_1{}^{-1}) = \rho(g_1)^{-1} = x^{-1}$, assim $x^{-1} \in \rho(G)$. Deste modo a imagem $\rho(G)$ é subgrupo de $\bar{G}$

Nesta demonstraçao, vimos que se ρ é um homomorfismo de G em $\bar{G}$ a imagem de ρ sempre é um subgrupo do grupo $\bar{G}$.

Teorema 1.10. (Teorema dos Isomorfismos). *Seja $f : (G, \cdot) \to (G, x)$ um homomorfismode grupos. Então,*

1. A função induzida

$$\bar{f} : \frac{G}{ker\ f} \longrightarrow f(G)$$

$$g ker\ f \mapsto f(G)$$

é um isomorfismo.

2. As seguintes funções

$\{$*Subgrupos de G que contém ker f*$\} \longleftrightarrow^{1-1} \{$*subgrupos de f* $(G)\}$

$$H \mapsto f(H)$$

$$f^{-1}(\mathcal{H}) \leftarrow \mathcal{H}$$

são bijeções, inversas uma da outra. Além disso, estas bijeções levam subgrupos normais, isto é:

a) $H \triangleleft G \Rightarrow f(H) \triangleleft f(G)$.

b) $\mathcal{H} \triangleleft f(G) \Rightarrow f^{-1}(\mathcal{H}) \triangleleft G$.

Demonstração. Primeiramente, deve-se verificar que $\bar{f}$ é bem definida, ou seja, $g\ker f = g'\ker f$ entao temos que $f(g) = f(g')$. Porém, $g\ker f = g'\ker f$ implica que $g = g' \cdot k$, para algum $k \in \ker f$ e, portanto,

$$f(g) = f(g' \cdot k) = f(g') \times f(k) = f(g') \times e_G = f(g')$$

Agora, $\bar{f}$ é claramente uma função sobrejetora e, para $g, g_1 \in G$, obtemos $\bar{f}(g\ker f \cdot g_1\ker f) = \bar{f}((gg_1)\ker f) = f(g \cdot g_1) = f(g) \times f(g_1) = \bar{f}(g\ker f) \times \bar{f}(g_1\ker f)$; assim $\bar{f}$ é um homomorfismo. Agora,

$$\ker \bar{f} = \{g\ker f \mid f(g) = e_G\} = \{g\ker f \mid g \in \ker f\} = \ker f\ ;$$

assim $\ker \bar{f} = \{e_G/\ker f\}$, ou seja, a função f é injetiva.

Temos que $f^{-1}(f(H)) = H(\ker f)$, $\forall H \leq G$, e que $f(f^{-1}(\mathcal{H})) = \mathcal{H} \cap f(G)$, $\forall \mathcal{H} \leq \mathcal{G}$. Daí $H \supseteq \ker f$ então $f^{-1}(f(H)) = He$, se $\mathcal{H} \subseteq f(G)$ então $f(f^{-1}(\mathcal{H})) = \mathcal{H}$. Obtemos então que as duas funções definidas em 2 são inversas uma da outra, restando mostrar que as funções levam subgrupos normais em subgrupos normais:

a) Dados $y \in f(G)$ e $x \in f(H)$ quaisquer, devemos mostrar que $yxy^{-1} \in f(H)$. Temos $y = f(g)$ e $x = f(h)$, com $g \in G$ e $h \in H$, logo $yxy^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1})$; como, por hipótese, $H \triangleleft G$, temos $ghg^{-1} \in H$ e portanto $yxy^{-1} \in f(H)$.

b) Dados $g \in G$ e $\alpha \in f^{-1}(\mathcal{H})$ quaisquer, devemos mostrar que $g\alpha g^{-1} \in f^{-1}\mathcal{H}$. Temos

$$f(g\alpha g^{-1}) = f(g)f(\alpha)f(g)^{-1} \text{ e } f(\alpha) \in \mathcal{H};$$

Por hipótese, $\mathcal{H} \triangleleft f(G)$, logo temos que $f(g\alpha g^{-1}) \in \mathcal{H}$ e portanto obtemos $g\alpha g^{-1} \in f^{-1}(\mathcal{H})$.

CAPÍTULO 2

TEOREMAS DE SYLOW

Antes de enunciar e provar os teoremas de Sylow se faz necessária a análise de alguns tipos de aplicaçoes que possibilitarão que se chegue em resultados concretos nas demonstrações posteriores, assim veremos a definição e alguns resultados acerca das representações de um grupo por permutações. Todos os conceitos e definições neste capítulos enunciados podem ser encontrados em [2].

1 | REPRESENTAÇÃO DE UM GRUPO POR PERMUTAÇÕES

Até o momento em nosso estudo de grupos, estudamos alguns exemplos de grupos tais como grupo das permutações, grupos dos restos módulo m, etc. Quando se tinha por objetivo encontrar alguma propriedade em G, o trabalho consistia em trabalhar dentro do próprio grupo, e de seus elementos, seus subgrupos.

A partir de agora dados dois grupos G e $\mathcal{G}$ e se $\rho : G \to \mathcal{G}$ é um homomorfismo, procuraremos propriedades de G via homomorfismo em $\mathcal{G}$, ou seja a ideia consiste em estudar as propriedades de G por meio de um outro grupo capaz de transportar suas propriedades pelo homomorfismo, e é o que veremos no estudo de um grupo via representações por permutações.

Definição 18. Sejam G um grupo, C um conjunto e $P(C)$ o grupo de permutações de C. Uma *Representação de G no grupo de permutações de C é um homomorfismo* $\rho : G \to P(C)$, isto é, uma função $\rho(g_1g_2) = \rho(g_1) \cdot \rho(g_2)$. Diz-se também que o grupo G opera sobre o conjunto C.

Dado um grupo G, podemos considerar G como um conjunto, neste caso, a fim de evitar confusões, será utilizado o símbolo G_0 para designar o conjunto G.

Exemplo 2.1.1. Seja G um grupo e seja $C = G_0$. Considere:

$$\begin{aligned} \mathrm{I} : G &\to P(G_0) \\ g &\to \mathrm{I}_g : G_0 \to G_0 \\ a &\to gag^{1} \end{aligned}$$

Sabemos que I é um homomorfismo, logo uma representação de G no grupo de permutações do conjunto G_0.

Definição 19. Seja $x \in C$. A órbita de x é o conjunto

$$D(x) := \{y \in C \mid y \sim x\} = \{\rho(g)(x) \mid g \in G\}.$$

O estabilizador de x é o conjunto de elementos de G que deixam o elemento x fixo, isto é

$$E(x) := \{g \in G \mid \rho(g)(x) = x\}$$

Teorema 2.1. *Seja:* $\rho : G \to P(C)$ *uma representação do grupo* G *no grupo de permutações do conjunto* C *. Seja* $x \in C$*. Então a aplicação abaixo é uma bijeção:*

$$\psi : D(x) \to \{\text{classes laterais à esquerda de } E(x) \text{ em } G\}$$
$$\rho(g)(x) \to gE(x)$$

Em particular, no caso de G *ser um grupo finito, temos que* $|D(x)| = (G : E(x))$ *e que* $|D(x)|$ *divide* $|G|$*.*

Demonstração. Precisamos verificar inicialmente que a aplicação ψ é bem definida, ou seja para $y \in D(x)$, $\psi(y)$ não depende da escolha do elemento $g \in G$ utilizado para obter y a partir de x. Sejam $g_1, g_2 \in G$ tais que $\rho(g_1)(x) = \rho(g_2)(x)$; aplicando $\rho(g_2^{-1})$ em ambos os lados e sabendo que ρ é homomorfismo, obtemos $\rho(g_2^{-1}g_1)(x) = x$; assim temos que $g_2^{-1}g_1 \in E(x)$, logo $g_1 \in g_2E(x)$ e $g_1E(x) = g_2E(x)$.

Agora, a aplicação ψ é sobrejetora pois, se $gE(x)$ é uma classe lateral a` esquerda de $E(x)$ em G, então temos que $gE(x) = \psi(y)$ com $y = \rho(g)(x)$.

Para verificar que ψ é injetora tomemos $y_1 = \rho(g_1)(x)$ e $y_2 = \rho(g_2)(x)$ dois elementos de $D(x)$ tais que $\psi(y_1) = \psi(y_2)$, ou seja, tais que $g_1E(x) = g_2E(x)$. Construindo desta forma, temos $g_1^{-1}g_2 \in E(x)$, logo $\rho(g_1^{-1}g_2)(x) = x$, ou seja $\rho(g_1^{-1}) \cdot g_2)(x) = x$ e portanto, temos

$$y_2 = \rho(g_2)(x) = \rho(g_1) \cdot \rho(g_1^{-1}) \cdot \rho(g_2)(x) = \rho(g_1)(x) = y_1$$

Exemplo 2.1.2. Seja G um grupo e seja C= {subgrupos de G} . Considere a aplicação:

$$I : G \to P(C)$$

A órbita $D(H) = \{Ig(H) \mid g \in G\} = \{gHg^{-1} \mid g \in G\}$ de um subgrupo H se chama a classe de conjugação de H. Os elementos de $D(H)$ se chamam subgrupos conjugados de H. Note-se que temos $D(H) = \{H\}$ se, e somente se H for subgrupo normal de G . O estabilizador $E(H) = \{g \in G \mid Ig(H) = H\} = \{g \in G \mid gHg^{-1} = H\}$ se chama o *normalizador de H em G,* e será denotado por $N_G(H)$.

Teorema 2.2. Se G é um grupo tal que $|G| = p^n$, onde p é um número primo e $n \geq 1$, então $Z(G) \neq e$.

Demonstração. Seja $a \in G$. Como $N(a)$ é um subgrupo de G, pelo Teorema de Lagrange, $|N(a)|$ divide $|G|$, logo $|N(a)| = p^{n_a}$, onde $0 \leq n_a \leq n$. Pela proposição anterior, $a \in Z(G)$ se, e somente se, $n_a = n$. Seja $z = |Z(G)|$. Consideremos a equação de classe de G.

$|G| = \sum \frac{|G|}{|N(a)|}$ onde a soma é nas classes de conjugação distintas.

$$p^n = \sum_{n_a = n} \frac{|G|}{|N(a)|} + \sum_{n_a < n} \frac{|G|}{|N(a)|}$$

$$p^n = z + \sum_{n_\alpha < n} \frac{|G|}{|N(a)|}$$

Como p divide p^n e divide cada parcela do tipo p^{n-n_α} , com $n_\alpha < n$, obtemos que p divide z. Logo $z \geq p$ e $Z(G) \neq e$

2 | TEOREMAS DE SYLOW

Peter L. M. Sylow (1832-1918) foi um matemático norueguês de bastante relevância para o desenvolvimento da teoria de grupos, ele foi responsavel por enunciar e provar teoremas que nos permitem classificar grupos em simples ou não, estes teoremas são conhecidos por teoremas de Sylow.

Por isso o objetivo deste capítulo será apresentar os 3 teoremas de Sylow.

2.1 Primeiro Teorema de Sylow

O Teorema de Lagrange nos garante que a ordem de qualquer subgrupo de um grupo G divide o a ordem de G. Entretanto, a recíproca não é garantida pelo teorema, ou seja, não podemos garantir, por exemplo, que um grupo de ordem 12 possua necessariamente subgrupo de ordem 6. Esta negativa pode ser verificada em A_4.

Uma iniciativa a recíproca pode ser dada pelo Lema:

Lema 2.1. (Cauchy). *Seja G um grupo abeliano finito e p um número primo que divide $|G|$. Então existe $x \in G$ de ordem p.*

Observe que se $x \in G$ tem ordem p, então o subgrupo $\langle x \rangle$ formado pelas potências de x tem ordem p. Esta observação juntamente com o lema acima, garante a existência de subgrupo de ordem p no caso em que o grupo em questão é abeliano. O primeiro Teorema de Sylow vai generalizar este resultado garantindo que, para qualquer grupo, não necessariamente abeliano, existe para cada potência de um primo p que dividem a ordem de G, um subgrupo com esta ordem.

Teorema 2.3. (1º Teorema de Sylow). *Seja p um número primo e G um grupo de ordem $p^m b$ com $(p, b) = 1$. Então, para cada $n \in \mathbb{N}$, $0 \leq n \leq m$, existe um subgrupo H de G com $|H| = p^n$.*

Demonstração. Fazemos uma prova por indução sobre $|G|$. Se $|G| = 1$, nada há para fazer. Se $|G| > 1$, supomos, como hipótese de indução, que o teorema vale para todos os grupos de ordem menor que $|G|$; queremos mostrar que o teorema vale também para o grupo $|G|$. Caso 1: Se existe um subgrupo próprio H de G tal que p^n divida a ordem de H. Neste caso, pela hipótese de indução, temos que H, e portanto a fortiori G, possui um subgrupo de ordem p^n. Caso 2: Se não existe um subgrupo próprio H de G tal que p^n divida a sua ordem. Neste caso, considere a equação das classes de conjugação:

$$|G| = |Z(G)| + \sum_{x_a \notin Z(G)} |C|(x_a)| = |Z(G)| + \sum_{x_a \notin Z(G)} (G : Z(x_a))$$

para $x_a \notin Z(G)$, temos $Z(G) \subsetneq G$, logo, por hipótese, p^n não divide $|Z(x_a)|$, e portanto p divide $(G : Z(x_a))$. Como p divide $|G|$, obtemos então que p divide $|Z(G)|$. Como $Z(G)$ é um grupo abeliano existe, pelo lema de Cauchy, um elemento $y \in Z(G)$ de ordem p. Como $y \in Z(G)$, é claro que $\langle y\rangle \triangleleft G$, de modo que podemos considerar o grupo quociente $G/\langle y\rangle$. Naturalmente, $|G/\langle y\rangle| < |G|$ e p^{n-1} divide $|G/\langle y\rangle|$. Logo, pela hipótese de indução, o grupo $G/\langle y\rangle$ possui um subgrupo K' de ordem p^{n-1}. Considere o homomorfismo canonico $\phi: G \leftarrow G/\langle y\rangle$ e tome $K = \phi^{-1}(K')$. Então K é um subgrupo de G e $|K| = |ker\phi||K'| = |\langle y\rangle||K'| = p^n$.

Definição 20. Sejam G um grupo finito, p um número primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que tem ordem p^m são chamados de **p-Sylow** subgrupos de G.

Agora, vamos nos preparar para apresentar e demonstrar o 2º Teorema de Sylow, onde é garantido que todos os p-Sylows subgrupos são conjugados entre si além de apresentar uma ideia da quantidade deles. Para demonstrar o resultado precisamos de um pequeno lema, enunciado abaixo.

Teorema 2.4. *Seja G um grupo finito, H um p-Sylow subgrupo e K um q-Sylow subgrupo de G com* $(p, q) = 1$, , $|H| = p^m$ e $|K| = q^n$ *então*

$$H \cap K = \{e\}$$

Demonstração. De fato, se houvesse um elemento $g \in G$, $g \neq e$ com $g \in H \cap K$ então $o(g)|p^m$ e $o(g)|q^n$, gerando um absurdo pelo fatos de $(p, q) = 1$.

Lema 2.2. *Sejam G um grupo finito e p um número primo. Sejam S um p-Sylow subgrupo de G e P um p-subgrupo qualquer de G. Então* $P \cap N_G(S) = P \cap S$.

2.2 Segundo Teorema de Sylow

Teorema 2.5. (Segundo Teorema de Sylow). *Sejam G um grupo finito, p um número primo e* n_p *o número de p-Sylow subgrupos de G. Então:*

a) Todos os p-Sylow subgrupos de G são conjugados entre si. Em particular, um p-Sylow subgrupo S de G é normal em G se, e somente se, S é o subgrupo de G. Neste caso, S é um subgrupo característico de G. único p-Sylow

b) Se P é um p-Sylow subgrupo de G, existe um p-Sylow subgrupo S de G tal que $P \subseteq S$.

c) Se S é um p-Sylow subgrupo, temos $n_p = (G : N_G(S))$.

Demonstração. Seja S um p-Sylow subgrupo de qualquer G. Considere o conjunto $C = \{\text{conjugados de } S\} = \{gSg^{-1};\ g \in G\}$. Por definição, o conjunto C é a órbita de S na representação por conjugações $I : G \to P(D)$ onde denotamos $D = \{\text{subgrupos de } G\}$;

portanto, pelo teorema 2.1 temos

$$|C| = (G : N_G(S)).$$

Claramente, basta mostrar que se P é um p-Sylow subgrupo qualquer de G, então o subgrupo P está contido num conjugado S em G. Considere a seguinte representação de P:

$$I : P \to P(C)$$
$$a \to I_a : C \to C$$
$$gSg^{-1} \to agSg^{-1}a^{-1}$$

Sejam $D_1, ..., D_k$ as órbitas distintas desta representação e para cada D_i escolha um representante $S_i = g_iSg^{-1}$ dentro de D_i. É fácil ver que $|C| = \Sigma_{i=1}^{k} |D_i|$; além disto, pelo teorema 2.1, temos $|D_i| = (P : E(S_i)) = (P : P \cap N_G(S_i))$ e, pelo lema 2.2, temos $(P : P \cap N_G(S_i)) = (P : P \cap S_i)$. Portanto temos

$$|C| = \sum_{i=1}^{k} (P : P \cap S_i)$$

Das duas expressões obtidas para $|C|$, tiremos que

$$(G : N_G(S)) = \sum_{i=1}^{k} (P : P \cap S_i)$$

Vamos apresentar agora, o terceiro Teorema de Sylow. Dado um primo p que divide a ordem de G, o Teorema reduz as possibilidades para valores de n_p, ou seja, ele auxilia em alguns casos na busca da quantidade de p-Sylows subgrupos.

2.3 Terceiro Teorema de Sylow

Teorema 2.6. *Sejam p um número primo e G um grupo finito de ordem $p^m b$, com $(p, b) = 1$. Seja n_p o número de p-Sylow subgrupos de G. Então:*

$$\begin{cases} n_p \text{ divide } b \\ n_p \equiv 1 \text{ módulo } p \end{cases}$$

Demonstração. Seja S um p-Sylow subgrupo de G, naturalmente temos que $(G : N_G(S))$ divide $(G : S) = b$. Agora, consideramos a expressão para $(G : N_G(S))$ estabelecida no decorrer da prova do segundo Teorema de Sylow. Tomando $P = S$ nesta expressão, obtemos

$$(G : N_G(S)) = \sum_{i=1}^{k} (S : S \cap S_i)$$

onde $S_1,..., S_K$ sao representantes das distintas órbitas de $D_1,..., D_k$ da representação seguinte

$$I : S \to P(C),$$

Onde C é o conjunto dos p-Sylow subgrupos de G. Evidentemente, podemos tomar, $S_i = S$; com esta escolha obtemos

$$(G : N_G(S)) = (S : S \cap S_i) + \sum_{i=1}^{k} (S : S \cap S_i) \equiv 1 \bmod p$$

Pelo segundo Teorema de Sylow, sabemos que $n_p = (G : N_G(S))$. Portanto, obtemos os resultados desejados sobre n_p.

CAPÍTULO 3

RESULTADOS OBTIDOS/CLASSIFICAÇÃO DOS GRUPOS SIMPLES DE ORDEM MENOR QUE 60

Toda a analise bibliográfica até o momento foi feita visando a classificação de grupos de ordem menor que 60 em simples ou não. Para a classificação dos grupos faremos uso dos teoremas de Sylow, Cauchy, Lagrange e de resultados que surgiram a partir destes. Vejamos o primeiro lema que trata de grupos de ordem p, onde p é primo. A medida que um teorema possibilitar classificar determinada ordem, a mesma será desconsiderada de outras classificações que forem feitas posteriormente,não excluindo a possibilidade de uma mesma ordem pode ser classificada de mais de uma forma.

Lema 3.1. *Seja G grupo finito e p um número primo. Se* $|G| = p$*, então G é um grupo simples.*

Demonstração. Pelo Teorema de Lagrange sabemos que a ordem do subgrupo divide a ordem do grupo, então os únicos subgrupos possíveis para estes grupos são os triviais, portanto são grupos simples.

Em particular se G é um grupo tal que $|G| \in \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 39, 41, 43, 47, 53, 57, 59\}$ então G é grupo simples.

Agora que todo grupo de ordem prima já foi classificado como simples, nosso objetivo será classificar os grupos de ordens não-primas menores que 60. Desta forma de modo a facilitar o trabalho vejamos todas as ordens não primas e suas decomposições:

$4 = 2^2$	$18 = 2 \cdot 3^2$	$30 = 2 \cdot 3 \cdot 5$	$42 = 2 \cdot 3 \cdot 7$	$52 = 2^2 \cdot 13$
$6 = 2 \cdot 3$	$20 = 2^2 \cdot 5$	$32 = 2^5$	$44 = 2^2 \cdot 11$	$54 = 2 \cdot 3^3$
$8 = 2^3$	$22 = 2 \cdot 11$	$33 = 3 \cdot 11$	$45 = 3^2 \cdot 5$	$55 = 5 \cdot 11$
$9 = 3^2$	$24 = 2^3 \cdot 3$	$34 = 2 \cdot 17$	$46 = 2 \cdot 23$	$56 = 2^3 \cdot 7$
$10 = 2 \cdot 5$	$25 = 5^2$	$35 = 5 \cdot 7$	$48 = 2^4 \cdot 3$	$58 = 2 \cdot 29$
$12 = 2^2 \cdot 3$	$26 = 2 \cdot 13$	$36 = 2^2 \cdot 3^2$	$49 = 7^2$	
$14 = 2 \cdot 7$	$27 = 3^3$	$38 = 2 \cdot 19$	$50 = 2 \cdot 5^2$	
$16 = 2^4$	$28 = 2^2 \cdot 7$	$40 = 2^3 \cdot 5$	$51 = 3 \cdot 17$	

A seguir serão apresentados resultados e lemas que possibilitarão a classificação dos grupos das ordens citadas acima.

Lema 3.2. *Seja G é um grupo e p primo. Se* $|G| = p^2$*, então G possui subgrupo normal de ordem p.*

Demonstração. Se G é grupo com $|G| = p^2$, então pelo Lema 1.9, o grupo G é

abeliano, como consequência, todo subgrupo de G é normal em G. Pelo 1º Teorema de Sylow, G possui subgrupo de ordem p, sendo portanto normais em G.

Desta forma, os grupos G com as ordens 4, 9, 25, 49 não são simples.

Lema 3.3. *Seja G um grupo de ordem $2p^k$ com p primo e $k \geq 1$ natural, então G não é um grupo simples.*

Demonstração. Se $|G| = 2p^k$, com $k \in \mathbb{N}$, pelo 1º Teorema de Sylow existe um subgrupo H de ordem p^k. Assim $(G : H) = 2$ e pelo Teorema 1.6 sabemos que $H \triangleleft G$.

Assim, se $|G| \in \{6, 8, 10, 14, 16, 18, 22, 26, 32, 34, 38, 46, 50, 54, 58\}$ então G não é simples.

Lema 3.4. *Seja G um grupo com $|G| = pq$, onde p e q são primos distintos, então G não é um grupo simples.*

Demonstração. Seja G um grupo de ordem pq, com p e q primos distintos, suponha sem perda de generalidade que $p < q$.

Como n_q divide p, $n_q \in 1, p$. Como $n_q \equiv 1 \ mod \ q$ e $p < q$ temos que, $p \not\equiv 1 \ mod \ q$ assim $n_q = 1$. Logo temos um único q-Sylow subgrupo, sendo este normal em G.

Podemos concluir que se $|G| \in \{15, 21, 33, 35, 51, 55\}$ então G não é simples.

Lema 3.5. *Se G é grupo e $|G| = pqr$ com p, q e r primos distintos, então G não é grupo simples.*

Demonstração. Suponha $|G| = pqr$ com p, q e r primos distintos. Suponha também, sem perda de generalidade, que $p < q < r$. Então pelo 3º Teorema de Sylow temos que,

$$n_p \in \{1, q, r, qr\}; \ n_q \in \{1, r, pr\}; \ n_r \in \{1, pq\}$$

Se n_p, n_q, ou n_r for igual a um, nada mais há para provar. Vamos supor então que $n_p = q$, $n_q = r$ e $n_r = pq$. Assim temos q *p-Sylow* subgrupos distintos, que, pelo Teorema 1.3 , a instersecção entre eles é apenas a identidade. Da mesma forma, é trivial a intersecção dos *r q-Sylow* subgrupos e dos pq *r-Sylow* subgrupos.

Agora, pelo Teorema sabemos que também é trivial a intersecção de Sylow subgrupos de ordens distintas. Assim,pela proposição 2.4 a expressão

$$(p - 1)q + (q - 1)r + (r - 1)pq + 1$$

descreve a quantidade de elementos distintos necessários para a construção destes subgrupos. Observe que,

$$(p - 1)q + (q - 1)r + (r - 1)pq + 1 =$$

$$pq - q + qr - r + rpq - pq + 1 =$$

$$rpq + qr + pq - pq - r - q + 1 =$$

$$rpq + r(q - 1) - q + 1$$

mas $q - 1 > 1$, então

$$rpq + r(q-1) - q + 1 > rpq + r - q + 1$$

mas $r - q > 0$, então

$$rpq + r(q-1) - q + 1$$

mas $rpq + 1 > rpq$ e $|G| = rpq$. Portanto n_p, n_q, ou n_r é igual a um, pois se não o fosse, os elementos ultrapassariam os de G, assim, pelo Segundo Teorema de Sylow, esse subgrupo será normal em G. O que implica que G não será simples. Desta forma grupos finitos de ordem pqr com p, q e r primos distintos não são simples.

Com isto, podemos afirmar, por exemplo, que os grupos com ordens 30 e 42 não são simples.

Lema 3.6. *Seja G um grupo e* $|G| = p^n q$, *com p e q primos e* $(p, q) = 1$. *Se* $p^n < q$ *então G possui um subgrupo normal de ordem q.*

Demonstração. Se $p^n < q$, pelo 3º Teorema de Sylow sabemos que $n_q \mid p^n$, o que implica $n_q \in \{1, p, ..., p^n\}$ como $n_q \equiv 1 \ mod\ q$ e $p^n < q$ temos que $n_q = 1$ logo pelo 2º Teorema de Sylow sabemos que este q-Sylow subgrupo é normal em G.

Assim se G é um grupo tal que $|G| \in \{20, 28, 44, 52\}$, G não é simples.

Lema 3.7. *Seja G um grupo com* $|G| = p^k$, *com p primo e k > 1, então existe algum subgrupo de G normal não trivial.*

Demonstração. Como $|G| = p^k$, temos que G é um *p-grupo.* Se G é abeliano, pelo 1º Teorema de Sylow, existe um subgrupo de ordem p, assim este subgrupo será normal em G. Agora, se G não é abeliano, sabemos pelo Teorema 2.2, que seu centro é um subgrupo normal com $Z(G) \neq \{e\}$. Note que $|Z(G)| \neq p^k$ uma vez que G não é abeliano, assim, $Z(G) \neq G$. Logo, em todo caso G possui subgrupo normal não trivial.

Disso temos que se $|G| = 27$ então G não é simples.

Por meio da utilização das representações de um grupo podemos classificar os grupos de ordem 24, 36 e 48.

Note que se $f : G \to G$ é um homomorfismo de grupos, então $ker\ f \triangleleft G$. Especificamente, se temos um conjunto C, um grupo G, e $\rho : G \to P(C)$ uma representação de G como grupo das permutações do conjunto C, então $ker\ \rho$ é um subgrupo normal de G, o objetivo então, será encontrar uma condição tal que $ker\rho \neq \{e\}$.

Se $|P(C)| = |C|! < |G|$, então $|\rho(G)| = |G/ker\ \rho| < |G|$ e $ker\ \rho \neq \{e\}$. Assim, se um inteiro m divide $|G|$ e não divide $|C|!$, então $ker\rho \neq \{e\}$.

Lema 3.8. *Seja G um grupo tal que* $|G| \in \{24, 36, 48\}$ *então G não é simples.*

Demonstração. Faremos a demonstração para o caso 36, e de maneira análoga pode-se obter os casos 24 e 48.

Seja G um grupo tal que $|G| = 36 = 2^2 \cdot 3^2$, sabemos pelo terceiro Teorema de Sylow que $n_3 | 4$ e $n_3 \equiv 1 \ mod\ 3$ logo $n_3 \in \{1, 4\}$ Se $n_3 = 1$ então G possui subgrupo normal de ordem

9, por outro lado se $n_3 = 4$ temos 4 subgrupos de ordem 9. Digamos H_1, H_2, H_3, H_4.

Seja $C = \{H_1, H_2, H_3, H_4\}$. Defina,

$$\rho : G \to P(C)$$

$$g \to \rho_g : C \to C$$

$$H_i \to gH_ig^{-1}$$

ρ é uma representação de G, então $ker\ \rho\ G$. Note que, $|P(C)| = |C|! = 4! < |G| = 36$. Como

$$G/ker\rho \cong \rho(G) < P(C)$$

se $ker\ \rho = \{e\}$ chegaríamos que $|G| < |P(C)| = 24$ o que seria um absurdo. Assim, $ker\ \rho$ não é trivial e é normal em G, logo G não é simples.

Classificação dos grupos de ordens 12, 40, 45 e 56

Até o momento os lemas construídos não englobaram a classificação de grupos G tal que $|G| \in \{12, 40, 45, 56\}$. Essa classificação se fará a seguir:

Lema 3.9. *Seja G um grupo finito e* $|G| \in \{12, 40, 45, 56\}$ *então G não é simples.*

Demonstração. Para a demonstração deste lema demonstraremos de forma específica cada um dos casos, que se seguem.

Grupos de ordem 12

Seja G um grupo com $|G| = 12 = 2^2 \cdot 3$. Pelo 3º Teorema de Sylow temos que, $n_2 \in \{1, 3\}$ e $n_3 \in \{1, 4\}$. Se $n_3 = 1$ então pelo 2º Teorema de Sylow existe um subgrupo K normal em G de ordem 3. Se $n^3 = 4$ teremos 4 subgrupos de ordem 3, sendo a única interseção entre eles {e}, ou seja, são necessários $4 \cdot 2$ elementos distintos para compor estes subgrupos, sobrando exatamente 4 elementos. Pelo 1º Teorema de Sylow existe um subgrupo H com $|H| = 4$, então ele é único pois se não o fosse a quantidade de elementos ultrapassariam a ordem de G além disso esse subgrupo é necessariamente normal em G. Portanto grupos de ordem 12 não são simples.

Grupos de ordem 40

Seja G um grupo com $|G| = 40 = 2^3 \cdot 5$. Pelo 3º Teorema de Sylow temos que $n^2 = \{1, 5\}$ e $n_5 = 1$. Desta forma, como existe somente um 5-Sylow subgrupo, pelo 2º Teorema de Sylow, ele é normal em G. Assim, os grupos de ordem 40 não são simples.

Grupos de ordem 45

Seja G um grupo com $|G| = 45 = 3^2 \cdot 5$. Pelo 3º Teorema de Sylow temos que $n_3 = 1$ e $n_5 = 1$. Desta forma, existe somente um 3-Sylow subgrupo, e também um único 5-Sylow subgrupo, sendo ambos normais em G como afirma o 2º Teorema de Sylow. Portanto, grupos de ordem 45 não são simples.

Grupos de ordem 56

Seja G um grupo com $|G| = 56 = 2^3 \cdot 7$. Pelo 3º Teorema de Sylow temos que $n_2 \in \{1,$

7} e $n_7 \in \{1, 8\}$. Suponha que $n_7 = 8$, então teremos 8 grupos distintos, cuja única interseção é o elemento neutro, então serão necessários $8 \cdot 6 = 48$ elementos distintos para construir esses grupos, além disso sabemos pelo 1º Teorema de Sylow que existe um subgrupo H com $|H| = 2^3$, como sobraram exatamente oito elementos, então este subgrupo é único, pois se não o fosse a quantidade de elementos ultrapassaria $|G|$, além disso esse subgrupo por ser único necessariamente é normal em G pelo 2º Teorema de Sylow. Então subgrupos de ordem 56 não são simples.

A partir de todos os lemas construídos até o momento pode-se chegar ao seguinte Teorema:

Teorema 3.1. *Seja G um grupo finito e* $|G| < 60$*, então G só será simples se* $|G| = p$ *sendo p primo.*

Demonstração. A demonstração segue diretamente dos lemas supracitados.

CONCLUSÃO

Tendo em vista que os temas tratados neste presente trabalho são obstantes a grade curricular do curso de Licenciatura, pode se observar que este trabalho foi de significativa importância para o aprofundamento do saber matemático.

Toda a parte de noções preliminares contidas neste estudo eram componentes curriculares na disciplina de Álgebra Moderna I, a qual possibilitou conhecer e analisar grupos, subgrupos, homomorfismos conteúdos estes que possibilitaram chegar a diversos resultados.

Conhecendo-se os Teoremas de Sylow, uma gama de novas propriedades a cerca de grupos puderam ser descobertas, uma vez que eles trazem resultados a cerca dos subgrupos de um dado grupo. Utilizando-se dos Teoremas de Sylow e de conhecimentos prévios, foi possível construir métodos para classificar todos os grupos finitos de ordem menor que 60, todos os métodos devidamente demonstrados, chegando então a conclusão de que apenas serão grupos simples, aqueles cuja ordem forem um número primo.

REFERÊNCIAS

1. DOMINGUES,HyginoH.e.IEZZI,Gelson. **Álgebra Moderna.** 4 ed. Urbana, São Paulo: Atual , 2003.

2. GARCIA, Arnaldo; LEQUAIN, Yves. **Elementos de Álgebra.** 5 ed. Rio de Janeiro: Impa, 2008.

3. GARONZI, Martino. **Notas de Aula de Álgebra 2**. Disponível em: <http://www.mat.unb.br/martino/doc/AAnotealg2glued.pdf> . Acesso em: 25 out. 2019.

4. HERSTEIN, I.N. **Topics in Algebra .** 2 ed. New York: Wiley, 1975.

5. OTMAN, Joseph J. **An Introduction to the theory of Groups.** 4 ed. Urbana, USA: Spinger, 1994.

6. VILLELA, Maria Lucia Torres. **Grupos.** Disponível em: <http://www.professores.uff.br/marco/wp-content/uploads/sites/37/2017/08/grupos- mod2.pdf> . Acesso em: 5 set. 2019.

Quais são os grupos simples de ordem menor que 60?

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2023

Quais são os grupos simples de ordem menor que 60?

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2023