UNIVERSIDADE DO ESTADO DE SANTA CATARINA
CENTRO DE CIÊNCIAS TECNOLÓGICAS - CCT
CURSO DE LICENCIATURA EM MATEMÁTICA

MAISA DAMAZIO FRANCO

CLASSIFICAÇÃO DE ALGUNS GRUPOS DE ORDEM FINITA

JOINVILLE - SC
2012

MAISA DAMAZIO FRANCO

CLASSIFICAÇÃO DE ALGUNS GRUPOS DE ORDEM FINITA

Trabalho de Graduação apresentado ao Curso de Licenciatura em Matemática do Centro de Ciências Tecnológicas, da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Licenciatura em Matemática.

Orientadora: Prof.ª Dr. Elisandra Bär de Figueiredo

JOINVILLE - SC
2012

F825c

Franco, Maisa Damazio

Classificação de alguns grupos de ordem finita / Maisa Damazio Franco. - 2012.

74 p.: il

Bibliografia: f. 74

Trabalho de Conclusão de Curso (Graduação) - Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Curso de Licenciatura em Matemática. Joinville, 2012.

Orientadora: Elisandra Bar de Figueiredo

1. Grupos finitos. Ordem de grupos. Teorema de Lagrange. Teoremas de Sylow. I. Figueiredo, Elisandra Bar de. II. Universidade do Estado de Santa Catarina - Curso de Licenciatura em Matemática. III. Classificação de alguns grupos de ordem finita.

CDD: 512.2

MAISA DAMAZIO FRANCO

CLASSIFICAÇÃO DE ALGUNS GRUPOS DE ORDEM FINITA

Trabalho de Graduação apresentado ao Curso de Licenciatura em Matemática do Centro de Ciências Tecnológicas, da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Licenciatura em Matemática.

BANCA EXAMINADORA

Orientadora: _____
Profª. Dra. Elisandra Bär de Figueiredo
Universidade do Estado de Santa Catarina

Membro: _____
Prof. Ms. Marnei Luis Mandler
Universidade do Estado de Santa Catarina

Membro: _____
Prof. Ms. Rodrigo de Lima
Universidade do Estado de Santa Catarina

Joinville, 28 de junho de 2012.

AGRADECIMENTOS

Primeiramente, eu gostaria de agradecer a Deus por me manter sempre calma e com fé, na esperança de que tudo sempre dará certo. Agradeço imensamente a professora Elisandra Bär de Figueiredo que fez de tudo para me ajudar na conclusão deste trabalho, me ensinando, orientando e tranquilizando, e além disso me fez gostar muito de Álgebra por ser uma excelente e dedicada professora. Agradeço também ao professor Rodrigo de Lima por aceitar fazer parte da minha banca e por me inspirar a sempre procurar conhecer e estudar coisas novas. E ao professor Marnei Luis Mandler que acompanhou toda a minha jornada acadêmica, como professor de várias matérias e como chefe de departamento, sempre me incentivando e mostrando como ser um verdadeiro professor que ama a sua profissão e se dedica integralmente aos alunos. Muito obrigada a todos os professores, por terem sido verdadeiros exemplos.

A minha querida família. Minha mãe Rosana D. Franco que sempre está ao meu lado em todos os momentos me acompanhando em tudo, me apoiando e fazendo todo o possível para me ajudar no que for preciso, sendo uma verdadeira mãe e amiga. Ao meu pai Luiz Carlos D. Franco que também incentiva as minhas decisões, me guia sempre para as escolhas certas e me deu a oportunidade de me dedicar integralmente aos estudos. Enfim devo a vocês tudo o que sou hoje e tudo o que eu conquistei, obrigada pela educação, dedicação e amor que vocês sempre me deram. Ao meu amado namorado Evandro Machado, que me acompanha desde o início do curso, que me faz sorrir quando estou triste, teve paciência durante os finais de semana de estudos e por todo o amor e carinho que me dedica. E a toda a minha família que sempre espera e acredita no melhor de mim.

Agradeço aos meus amigos de faculdade, em especial a Cintia Préve que compartilhou comigo todos os momentos desde o começo, trabalhos, dificuldades, tristezas, mas principalmente as alegrias e os finais de semana de estudos, sempre me ajudando e me lembrando de tudo o que eu esqueço. Aos meus amigos Joice Dörner, Marcelo Possamai, Priscila Gadotti, Fernando El Haje e Mayara Possamai, por alegrarem os meus dias e dividirem inúmeras histórias.

Obrigada a todos que fizeram, e fazem parte da minha vida.

RESUMO

FRANCO, Maisa Damazio. **Classificação de alguns grupos de ordem finita**. 2012. 74f. Trabalho de Conclusão do Curso de Licenciatura em Matemática - Universidade do Estado de Santa Catarina, Joinville, 2012.

No estudo da teoria de grupos busca-se conhecer e determinar a estrutura de cada grupo. Nesse sentido é importante classificar os tipos de grupos distintos que existem, para transferir as propriedades obtidas de um para outro dentro da mesma classe. Neste trabalho foram classificados os grupos de ordem menor que 12 usando como ferramenta o Teorema de Lagrange. Além disso, são apresentadas algumas recíprocas do Teorema de Lagrange, entre estas o 1° Teorema de Sylow.

Palavras-chave: Grupos finitos. Ordem de grupos. Teorema de Lagrange. Teoremas de Sylow.

ABSTRACT

FRANCO, Maisa Damazio. Classification of some groups of finite order. 2012. 74f. Trabalho de Conclusão do Curso de Licenciatura em Matemática - Universidade do Estado de Santa Catarina, Joinville, 2012.

When studying theory of groups one seeks to know and determine the structure of each group. For that it's important do classify the existing types of groups, so that properties obtained from one can be transferred to another within the same class. In this work, groups of order 12 or less were classified using Lagrange's theorem as a tool. Besides that, some converses to Lagrange's theorem are presented, including Sylow's 1^{st} theorem.

Key-words: Finite groups. Order of groups. Lagrange's theorem. Sylow's theorems.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{R}$	Conjunto dos números reais
$\|G\|$	Ordem do Grupo G
$o(a)$	Ordem do elemento a
$\overline{a}$	Classe de equivalência do elemento a
aH	Classe lateral à esquerda
Ha	Classe lateral à direita
G/H	Conjunto quociente de G por H
$\mathbb{Z}_m$	Classe de equivalência de $\mathbb{Z}$ módulo m
S_n	Grupo de permutações
D_n	Grupo diedral
R_n	Grupo de rotações
$S_\triangle$	Grupo das simetrias de um triângulo equilátero
Q_3	Grupo dos quatérnios
$G_1 \times G_2 \times \ldots \times G_n$	Produto direto dos grupos $G_1, G_2, \ldots, G_n$
$H < G$	H é subgrupo de G
$H \triangleleft G$	H é subgrupo normal de G
$Ker(f)$	Núcleo de f
$\langle S \rangle$	Grupo gerado pelo conjunto S
$\langle a \rangle$	Grupo gerado pelo elemento a
$G \simeq J$	G é isomorfo a J
$\#H$	Cardinalidade de H
$Z(G)$	Centro de G
$Aut(G)$	Grupo dos automorfismos internos de G
$\mathcal{I}_g$	Automorfismo interno
$(G : H)$	Índice do subgrupo H em G
$C(a)$	Classe de conjugação do elemento a
C_a	Cardinalidade do conjunto $C(a)$

SUMÁRIO

INTRODUÇÃO

Na disciplina de Álgebra estuda-se, na teoria de grupos finitos, o Teorema de Lagrange que garante que a ordem de qualquer subgrupo sempre divide a ordem do grupo. Surge a pergunta natural sobre a sua recíproca: se para qualquer divisor da ordem do grupo existe um subgrupo com tal ordem. Os Teoremas de Cauchy e o 1° Teorema de Sylow apresentam resultados nessa linha. Os Teoremas de Sylow formam uma parte fundamental da teoria de grupos, fornecendo informações detalhadas sobre o número de subgrupos de ordem fixa que um dado grupo finito contém.

Outro tema importante para o desenvolvimento da Álgebra é a classificação de grupos finitos, a qual permite separá-los em classes disjuntas tais que as propriedades deduzidas para um grupo particular de uma dada classe possam ser transferidas para todos os grupos dessa classe, e apenas para estes, com uma simples mudança de notação. Assim é suficiente analisar uma quantidade finita de grupos.

Com o Teorema de Lagrange é possível classificar grupos de ordem baixa, mas é inviável para grupos com ordens maiores. Para tal são importantes os resultados dos Teoremas de Sylow.

Este trabalho está dividido da seguinte forma: no Capítulo 1 serão apresentados alguns resultados preliminares que já foram vistos na disciplina de Álgebra e que são de suma importância para a compreensão dos estudos propostos; no Capítulo 2 serão apresentados resultados da teoria de grupos que são a base para este trabalho; no Capítulo 3 serão classificados os grupos de ordem menor ou igual a 11 e os grupos de ordem $2p$ com $p > 2$ um número primo, utilizando como principal ferramenta o Teorema de Lagrange; no Capítulo 4, serão vistas algumas recíprocas do Teorema de Lagrange; e finalmente serão apresentadas as conclusões e sugestões que complementariam este trabalho.

Capítulo 1

RESULTADOS PRELIMINARES

Para a melhor compreensão deste trabalho, apresentar-se-á neste capítulo alguns resultados preliminares da Álgebra, a fim de que se possa aprofundar os estudos de grupos tendo as bases necessárias. Este primeiro capítulo será referenciado na obra de Domingues e Iezzi (1979).

1.1 RELAÇÕES

Os tipos de relações que serão utilizadas neste trabalho são: Relações binárias e Relações de equivalência.

Definição 1.1.1 *Dados dois conjuntos E e F, não vazios, chama-se* **produto cartesiano** *de E por F o conjunto formado por todos pares ordenados (x, y) com $x \in E$ e $y \in F$. Ou seja:*

$$E \times F = \{(x, y) / \ x \in E \ \ e \ \ y \in F\}.$$

Definição 1.1.2 *Chama-se* **relação binária** *de E em F todo subconjunto R de $E \times F$. Ou seja:*

$$(R \text{ é relação de } E \text{ em } F) \iff \ R \subset E \times F.$$

Os conjuntos E e F são denominados conjunto de partida e conjunto de chegada da relação R respectivamente. Ou seja, toda relação binária é um conjunto de pares ordenados. Para indicar que $(a, b) \in R$, usa-se a notação aRb.

Observação 1.1.3 *Quando $E = F$ diz-se que $R \subset E^2 = E \times E$ é uma relação sobre E.*

Definição 1.1.4 *Chama-se* **domínio** *de R o subconjunto de E definido por*

$$D(R) = \{x \in E / \ \exists y \in F : \ xRy\}.$$

Definição 1.1.5 *Chama-se* **imagem** *de R o subconjunto de F definido por*

$$Im(R) = \{y \in F/\ \exists x \in E :\ xRy\}.$$

Definição 1.1.6 *Sejam R uma relação de E em F e S uma relação de F em G. Chama-se* **relação composta** *de R e S a seguinte relação, indicada por $S \circ R$, de E em G :*

$$S \circ R = \{(x, z) \in E \times G/\ \exists y \in F :\ (x, y) \in R \text{ e } (y, z) \in S\}.$$

Definição 1.1.7 *Seja R uma relação de E em F. Chama-se* **relação inversa** *de R, e indica-se por R^{-1}, a seguinte relação de F em E :*

$$R^{-1} = \{(y, x) \in F \times E/\ (x, y) \in R\}.$$

Seja R uma relação sobre E. Então, R pode apresentar as seguintes propriedades:

1. **Reflexiva:** se para todo $x \in E$ tem-se que xRx.
2. **Simétrica:** se para todo $x,\ y \in E$ tem-se que $(xRy \ \Rightarrow\ yRx.)$
3. **Transitiva:** se para todo $x,\ y,\ z \in E$ tem-se que $(xRy \text{ e } yRz \ \Rightarrow\ xRz.)$
4. **Antissimétrica:** se para todo $x,\ y \in E$ tem-se que $(xRy \text{ e } yRx \Rightarrow\ x = y.)$

Definição 1.1.8 *Uma relação R sobre E é chamada* **relação de equivalência** *sobre E se R é reflexiva, simétrica e transitiva.*

Definição 1.1.9 *Seja R uma relação de equivalência sobre E. Dado $a \in E$ chama-se* **classe de equivalência** *determinada por a, módulo R o subconjunto $\overline{a}$ de E formado pelos elementos x tais que xRa, ou seja,*

$$\overline{a} = \{x \in E/\ xRa\}.$$

Definição 1.1.10 *O conjunto de todas classes de equivalência módulo R será indicado por E/R e chamado* **conjunto quociente** *de E por R.*

Exemplo 1.1.11 *A relação*

$$xRy \Longleftrightarrow x \equiv y(mod\ \ m)$$

é uma relação de equivalência do conjunto dos números inteiros em que o conjunto quociente é

$$\mathbb{Z}/_{\equiv} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}.$$

Este conjunto é usualmente denotado por $\mathbb{Z}_m$ e chamado de conjunto das classes de restos módulo m. Algumas vezes, quando não houver problema de ambiguidade, para simplificar a notação será utilizado apenas $a \in \mathbb{Z}_m$ para representar a classe $\overline{a}$.

Observação 1.1.12 *Duas classes de equivalência são iguais ou são disjuntas.*

Definição 1.1.13 *Seja E um conjunto não vazio. Diz-se que uma classe $\mathcal{F}$ de subconjuntos não vazios de E é uma* **partição** *de E se:*

(i) dois membros quaisquer de $\mathcal{F}$ ou são iguais ou são disjuntos;

(ii) a união dos membros de $\mathcal{F}$ é igual a E.

Proposição 1.1.14 *Se R é uma relação de equivalência sobre um conjunto E, então E/R é uma partição de E.*

1.2 APLICAÇÕES

Definição 1.2.1 *Seja f uma* **relação** *de E em F. Diz-se que f é uma aplicação de E em F se:*

(i) $D(f) = E$;

(ii) dado $a \in D(f)$, existe um único $b \in F$ tal que $(a, b) \in f$.

Observação 1.2.2 *Se $f : E \to F$ é uma aplicação e F é um conjunto numérico ($F \subset \mathbb{C}$), é usual chamar f de* **função**. *Às vezes, porém, usa-se a palavra função para designar uma aplicação qualquer.*

Definição 1.2.3 *Seja $f : E \to F$ uma aplicação.*

- *Diz-se que f é uma aplicação* **injetora** *ou* **1-1** *se dois elementos diferentes quaisquer de E tem imagens diferentes. Ou seja, se para quaisquer x_1, $x_2 \in E$, tais que $x_1 \neq x_2$, for válido $f(x_1) \neq f(x_2)$. Ou equivalentemente f é 1-1 se $x_1, x_2 \in E$ e $f(x_1) = f(x_2)$, então $x_1 = x_2$.*

- *Diz-se que f é uma aplicação* **sobrejetora** *se $Im(E) = F$, ou seja, se para todo $y \in F$ existir $x \in E$, tal que $y = f(x)$.*

- *Diz-se f é uma aplicação* **bijetora** *se f for injetora e sobrejetora.*

Teorema 1.2.4 *Seja $f : E \to F$ uma aplicação. Então, f^{-1} é uma aplicação se, e somente se, f é bijetora.*

Definição 1.2.5 *Sejam $f : E \to F$ e $g : F \to G$ duas aplicações. Chama-se* **composta** *de f e g a aplicação (indicada por $g \circ f$) de E em G definida da seguinte maneira:*

$$(g \circ f)(x) = g(f(x)),\ \forall\ x \in E.$$

Proposição 1.2.6 *Se $f : E \to F$ e $g : F \to G$ são injetoras, então $g \circ f$ é injetora.*

Proposição 1.2.7 *Se $f : E \to F$ e $g : F \to G$ são sobrejetoras, então $g \circ f$ é sobrejetora.*

1.3 OPERAÇÕES

Definição 1.3.1 *Sendo E um conjunto não vazio, toda aplicação $f : E \times E \to E$ recebe o nome de* **operação** *sobre E (ou em E) ou* **lei de composição interna** *sobre E (ou em E).*

Notação: Uma operação f sobre E associa a cada par $(x, y) \in E \times E$ um elemento de E que será denotado por $x * y$. Assim, $x * y$ é uma forma de indicar $f(x, y)$. Diz-se também que E é um conjunto munido da operação $*$. O elemento $x*y$ é chamado composto de x e y pela operação $*$.

Outras notações usuais para indicar uma operação sobre E :

- *Notação aditiva:* neste caso o símbolo da operação é $+$, a operação é chamada *adição*, o composto $x + y$ é chamado *soma* e os termos x e y são as parcelas.
- *Notação multiplicativa:* neste caso o símbolo da operação é $\cdot$ ou a simples justaposição dos elementos, a operação é chamada *multiplicação*, o composto $x \cdot y$ ou xy é chamado *produto* e os termos x e y são os fatores.

Seja . uma lei de composição interna em E. Esta lei pode apresentar as seguintes propriedades:

1. **Propriedade associativa**

   Diz-se que . satisfaz a propriedade associativa se

   $$x.(y.z) = (x.y).z,$$

   quaisquer que sejam $x,\ y,\ z \in E$.

2. **Propriedade comutativa**

   Diz-se que . satisfaz a propriedade comutativa se

   $$x.y = y.x,$$

   quaisquer que sejam $x,\ y \in E$.

3. **Elemento neutro**

   Se existe $e \in E$ tal que $e.x = x$, para todo $x \in E$, diz-se que e é um elemento neutro à esquerda.

   Se existe $e \in E$ tal que $x.e = x$, para todo $x \in E$, diz-se que e é um elemento neutro à direita.

   Se e é elemento neutro à esquerda e à direita para a operação $\cdot$, diz-se simplesmente que e é elemento neutro para essa operação.

   Proposição 1.3.2 *Se a operação $\cdot$ sobre E tem um elemento neutro e, então ele é único.*

   Demonstração: De fato, se $e,\ e' \in G$ são elementos neutros, então

$$e = e.e', \quad \text{pois } e' \text{ é neutro}$$
$$e' = e.e', \quad \text{pois } e \text{ é neutro}$$

   logo $e = e'$. ■

4. **Elementos simetrizáveis**

   Seja $\cdot$ uma operação sobre E que tem elemento neutro e. Dizemos que $x \in E$ é um elemento simetrizável para esta operação se existir $x' \in E$ tal que

$$x'.x = e = x.x'.$$

   O elemento x' é chamado simétrico de x.

   Quando a operação é uma adição, o simétrico de x também é chamado oposto de x e indicado por $-x$.

   Quando a operação é uma multiplicação, o simétrico de x também é chamado inverso de x e indicado por x^{-1}.

Proposição 1.3.3 *Seja $\cdot$ uma aplicação sobre E que é associativa e tem elemento neutro e.*

(i) Se um elemento $x \in E$ é simetrizável, então o simétrico de x é único.

(ii) Se $x \in E$ é simetrizável, então seu simétrico também é e $(x')' = x$.

(iii) Se $x,\ y \in E$ são simetrizáveis, então $x \cdot y$ é simetrizável e $(x \cdot y)' = y' \cdot x'$.

Demonstração:

(i) De fato, sejam $a \in E$, e $b, b' \in E$ dois elementos simétricos de a, então

$$\begin{aligned} b = b \cdot e &= b \cdot (a \cdot b'), \quad \text{pois b' é simétricos de a} \\ b &= (b \cdot a) \cdot b' \quad \text{pela associatividade} \\ b &= e \cdot b', \quad \text{pois b é simétrico de a} \\ b &= b' \end{aligned}$$

logo o simétrico de a é único.

(ii) Tem-se que $x \cdot x' = e = x' \cdot x$ e quer-se obter o simétrico y de x' que é o único elemento que satisfaz:

$$x' \cdot y = e = y \cdot x'$$

Como $y = x$ satisfaz esta equação e como o simétrico é único, então $(x')' = x$.

(iii) Deseja-se mostrar que existe $z \in E$ tal que $(x \cdot y) \cdot z = e = z \cdot (y \cdot x)$, no caso z é o simétrico de $(x \cdot y)$. Tem-se

$$\begin{aligned} (x \cdot y) \cdot z = e \quad &\Leftrightarrow \quad x' \cdot ((x \cdot y) \cdot z) = x' \cdot e \\ &\Leftrightarrow \quad (x' \cdot x) \cdot (y \cdot z) = x' \\ &\Leftrightarrow \quad e \cdot (y \cdot z) = x' \\ &\Leftrightarrow \quad y \cdot z = x' \\ &\Leftrightarrow \quad y' \cdot (y \cdot z) = y' \cdot x' \\ &\Leftrightarrow \quad (y' \cdot y) \cdot z = y' \cdot x' \\ &\Leftrightarrow \quad z = y' \cdot x' \end{aligned}$$

■

1.3.4 Tábua de uma operação

Num conjunto finito E com uma lei de composição interna $\cdot$ pode-se representar a operação dos elementos numa tabela de dupla entrada chamada **Tábua da Operação** $*$ em E. A construção desta tábua está descrita a seguir.

Seja $E = \{a_1,\ a_2,\ \cdots,\ a_n\}\ \ (n \geq 1)$ um conjunto de n elementos, com $n \geq 1$. Uma operação sobre E é uma aplicação $f : E \times E \to E$ que associa a cada par (a_i, a_j) o elemento $f(a_i, a_j) = a_i \cdot a_j := a_{ij}$.

Pode-se representar o elemento a_{ij}, correspondente ao par (a_i, a_j), numa tabela de dupla entrada, construída como segue:

(1°) Marca-se na linha fundamental e na coluna fundamental os elementos do conjunto E, como ilustra a Tabela 1.1. Chama-se de i-ésima linha aquela que começa com a_i e j-ésima coluna a que é encabeçada por a_j.

Tabela 1.1: Linha e coluna fundamental da tábua de uma operação

$\cdot$	a_1	a_2	$\cdots$	a_i	$\cdots$	a_j	$\cdots$	a_n
a_1								
a_2								
$\vdots$								
a_i								
$\vdots$								
a_j								
$\vdots$								
a_n								

Fonte: Domingues e Iezzi (1979, p.64)

(2°) Dado um elemento a_i na coluna fundamental e um elemento a_j na linha fundamental, na interseção da linha i com a coluna j marcamos o composto $a_{ij} = a_i * a_j$, como na Tabela 1.2.

Tabela 1.2: Tábua de uma operação

$\cdot$	a_1	a_2	$\cdots$	a_i	$\cdots$	a_j	$\cdots$	a_n
a_1	a_{11}	a_{12}	$\cdots$	a_{1i}	$\cdots$	a_{1j}	$\cdots$	a_{1n}
a_2	a_{21}	a_{22}	$\cdots$	a_{2i}	$\cdots$	a_{2j}	$\cdots$	a_{2n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$		$\vdots$
a_i	a_{i1}	a_{i2}	$\cdots$	a_{ii}	$\cdots$	a_{ij}	$\cdots$	a_{in}
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$		$\vdots$
a_j	a_{j1}	a_{j2}	$\cdots$	a_{ji}	$\cdots$	a_{jj}	$\cdots$	a_{jn}
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$		$\vdots$
a_n	a_{n1}	a_{n2}	$\cdots$	a_{ni}	$\cdots$	a_{nj}	$\cdots$	a_{nn}

Fonte: Domingues e Iezzi (1979, p.64)

Capítulo 2

TEORIA BÁSICA DOS GRUPOS

Neste capítulo serão apresentados resultados da teoria de grupos que são necessários para atingir os objetivos deste trabalho, sendo algumas demonstrações omitidas, por serem resultados clássicos. Estes resultados são referenciados em Domingues e Iezzi (1979) e Garcia e Lequain (2008).

2.1 GRUPOS

Definição 2.1.1 *Um conjunto G não vazio com uma operação*

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\mapsto a \cdot b \end{aligned}$$

é um **grupo** *se satisfaz as seguintes condições:*

(i) **Associatividade**

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \quad \forall \quad a, b, c \in G$$

(ii) **Elemento neutro**

$$\exists \quad e \in G \ / \ e \cdot a = a \cdot e = a, \quad \forall \quad a \in G$$

(iii) **Elemento inverso (elemento simetrizável)**

$$\forall a \in G, \exists \quad b \in G \ / \ a \cdot b = b \cdot a = e$$

Este elemento b é chamado de simétrico de a e denotado por a^{-1} se a operação for multiplicativa (não necessariamente a multiplicação usual) e por $-a$ se a operação for uma adição (não necessariamente usual).

O grupo G é **abeliano** ou **comutativo** se $a \cdot b = b \cdot a$, para todo $a, b \in G$.

Definição 2.1.2 *Se o conjunto G for finito com n elementos, diz-se que o* **grupo** G *é* **finito** *com ordem n e escreve-se $|G| = n$.*

Notação: Se G munido da operação $\cdot$ é um grupo, denota-se $(G, \cdot)$.

2.2 EXEMPLOS DE GRUPOS

Nesta seção serão apresentados alguns exemplos de grupos que serão referenciados neste e nos próximos capítulos.

Exemplo 2.2.1 *Grupo aditivo dos inteiros $(\mathbb{Z}, +)$ (abeliano).*

Exemplo 2.2.2 *Grupo aditivo dos racionais $(\mathbb{Q}, +)$ (abeliano).*

Exemplo 2.2.3 *Grupo aditivo dos reais $(\mathbb{R}, +)$ (abeliano).*

Exemplo 2.2.4 *Grupo aditivo dos complexos $(\mathbb{C}, +)$ (abeliano).*

Exemplo 2.2.5 *Grupo multiplicativo dos racionais $(\mathbb{Q}^*, \cdot)$ (abeliano).*

Exemplo 2.2.6 *Grupo multiplicativo dos reais $(\mathbb{R}^*, \cdot)$ (abeliano).*

Exemplo 2.2.7 *Grupo multiplicativo dos complexos $(\mathbb{C}^*, \cdot)$ (abeliano).*

Exemplo 2.2.8 *Grupo aditivo das matrizes $m \times n$ denotado por $(M_{m\times n}(K), +)$, com $K = \mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C}$ (abeliano).*

Exemplo 2.2.9 *$(GL_n(K), \cdot)$, com $K = \mathbb{Q},\ \mathbb{R},\ \mathbb{C}$ é o grupo linear racional, real ou complexo de grau n conforme $K = \mathbb{Q},\ \mathbb{R}$ ou $\mathbb{C}$ (não comutativo se $n > 1$), chamado de grupo das matrizes inversíveis.*

Exemplo 2.2.10 *Grupo aditivo de classes de restos $(\mathbb{Z}_m, \oplus)$. Este é um grupo abeliano finito com $|\mathbb{Z}_m| = m$, em que $\overline{a} \oplus \overline{b} = \overline{a + b}$, sendo $\mathbb{Z}_m$ definido no Exemplo 1.1.11.*

De fato, pode-se provar que a operação $\oplus$ independe dos representantes, a propriedade associativa é consequência da associatividade dos números inteiros, o elemento neutro deste conjunto é a classe $\overline{0}$ e o elemento simétrico (oposto) de $\overline{a} \in \mathbb{Z}_m$ é o elemento $\overline{m - a}$.

Exemplo 2.2.11 *Grupo multiplicativo abeliano de classes de restos$(\mathbb{Z}_m^*, \odot)$, em que $\overline{a} \odot \overline{b} = \overline{ab}$ e $|\mathbb{Z}_m^*| = m - 1$.*

Neste caso também prova-se que a operação $\odot$ independe do representante, além disso a propriedade associativa é consequência da associatividade dos números inteiros e o elemento neutro deste conjunto é a classe $\overline{1}$, porém o elemento simétrico (inverso) de $\overline{a} \in \mathbb{Z}_m$ não existe para qualquer valor de m, por exemplo em $\mathbb{Z}_4$ o elemento $\overline{2}$ não possui simétrico para operação $\odot$, pois

- $\overline{1} \odot \overline{2} = \overline{2}$,
- $\overline{2} \odot \overline{2} = \overline{0}$,
- $\overline{3} \odot \overline{2} = \overline{2}$

logo, $(\mathbb{Z}_4^*, \odot)$ não é grupo. Para solucionar este problema tem-se o seguinte resultado:

Proposição 2.2.12 $(\mathbb{Z}_m^*, \odot)$ *é um grupo se, e somente se, m for um número primo.*

Assim, o simétrico de $\overline{a} \in \mathbb{Z}_m$, com m sendo um número primo, é $\overline{x} \in \mathbb{Z}_m$ tal que $ax + my = 1$, para algum $y \in \mathbb{Z}$.

Exemplo 2.2.13 $(S(E), \circ)$ - *Grupo de permutações sobre E.*

Seja E um conjunto não vazio e $S(E)$ o conjunto de todas bijeções de E. Com a operação de composição de funções $S(E)$ é um grupo, chamado grupo das permutações sobre E. Tal grupo só é comutativo quando E é formado por 1 ou 2 elementos.

No caso particular em que $E = \{1,\ 2,\ \cdots,\ n\}$, $n \geq 1$, tem-se um importante grupo finito denotado neste caso por $(S_n, \circ)$ e chamado grupo simétrico de grau n cuja ordem é $|S_n| = n!$. A notação usual de um elemento de S_n é:

$$f = \begin{pmatrix} 1 & 2 & \cdots & r & \cdots & n \\ i_1 & i_2 & \cdots & i_r & \cdots & i_n \end{pmatrix},$$

onde $f(r) = i_r,\ \ r \in \{1,\ 2,\ \cdots,\ n\}$.

Em particular para $n = 3$ tem-se

$$\begin{aligned} S_3 \ = \ & \left\{ f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \right. \\ & \left. g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}. \end{aligned}$$

cuja tábua é

Exemplo 2.2.14 $(S_\triangle, \circ)$ - *Grupo das simetrias de um triângulo equilátero formado pelos elementos*

$$S_\triangle = \{id,\ R_{\frac{2\pi}{3}},\ R_{\frac{4\pi}{3}},\ R_1,\ R_2,\ R_3\}$$

que estão representados na Figura 2.1 e descritos na sequência.

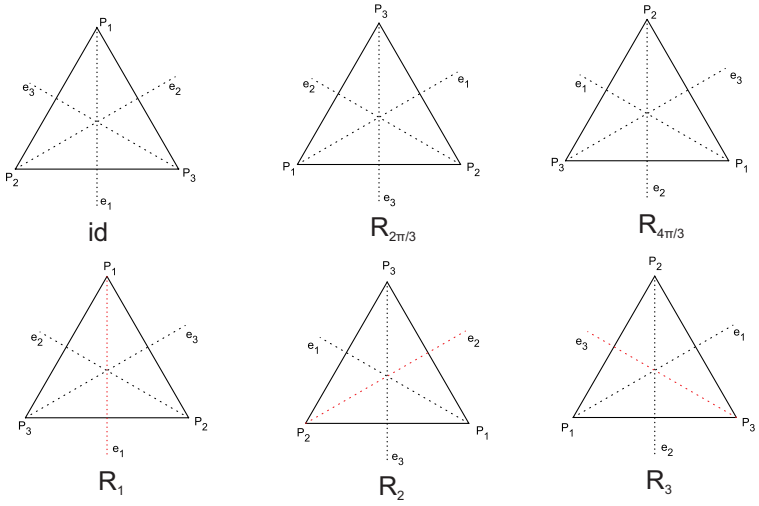
Sejam $P_1\ P_2\ P_3$ um triângulo equilátero com centro de gravidade na origem 0 do espaço e ainda e_1, e_2, e_3 as retas do espaço que passam pelas medianas do triângulo. Então, as transformações que preservam o triângulo são:

Tabela 2.1: Tábua do Grupo Simétrico S_3

$\circ$	f_0	f_1	f_2	g_1	g_2	g_3
f_0	f_0	f_1	f_2	g_1	g_2	g_3
f_1	f_1	f_2	f_0	g_3	g_1	g_2
f_2	f_2	f_0	f_1	g_2	g_3	g_1
g_1	g_1	g_2	g_3	f_0	f_1	f_2
g_2	g_2	g_3	g_1	f_2	f_0	f_1
g_3	g_3	g_1	g_2	f_1	f_2	f_0

Fonte: Domingues e Iezzi (1979, p.84)

Figura 2.1: Transformações espaciais que preservam o triângulo equilátero



Fonte: Produção do próprio autor

- $id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}$: as rotações planas centradas em 0, no sentido anti-horário, de ângulos zero, $\dfrac{2\pi}{3}$ e $\dfrac{4\pi}{3}$ respectivamente.
- R_1, R_2, R_3: as rotações espaciais de ângulo π com eixos e_1, e_2, e_3 respectivamente.

A tábua de $S_\triangle$ está apresentada na Tabela 2.2.

Exemplo 2.2.15 $(R_n, \circ)$ - *Grupo de Rotações de um polígono regular de n lados.*

Considera-se um polígono regular de n vértices, em que o centro do polígono está no ponto 0 do espaço e que o eixo x contenha um de seus vértices, o qual será indicado como ponto 1. Os vértices consecutivos serão indicados por $2, 3, \ldots, n$ respectivamente no sentido anti-horário, como na Figura 2.2.

Assim, as operações que transformam o polígono nele mesmo, são as rotações em torno da origem no sentindo anti-horário segundo os ângulos de:

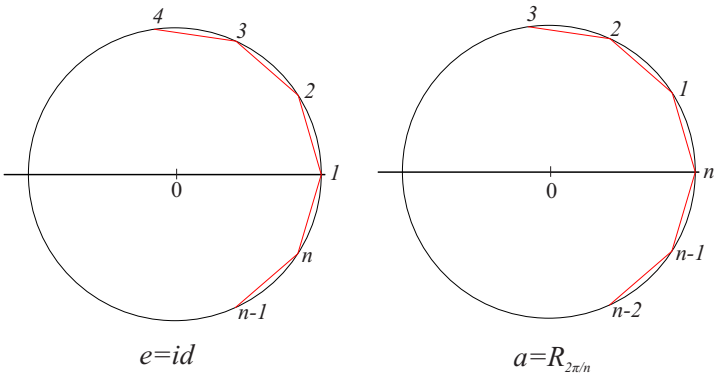
$$0, \frac{2\pi}{n}, 2 \cdot \frac{2\pi}{n}, \cdots, (n-1) \cdot \frac{2\pi}{n} \quad \text{radianos.}$$

Tabela 2.2: Tábua do Grupo das simetrias do triângulo equilátero $S_{\triangle}$

	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
id	id	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	R_1	R_2	R_3
$R_{\frac{2\pi}{3}}$	$R_{\frac{2\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	R_3	R_1	R_2
$R_{\frac{4\pi}{3}}$	$R_{\frac{4\pi}{3}}$	id	$R_{\frac{2\pi}{3}}$	R_2	R_3	R_1
R_1	R_1	R_3	R_2	id	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$
R_2	R_2	R_1	R_3	$R_{\frac{2\pi}{3}}$	id	$R_{\frac{4\pi}{3}}$
R_3	R_3	R_2	R_1	$R_{\frac{4\pi}{3}}$	$R_{\frac{2\pi}{3}}$	id

Fonte: Produção do próprio autor

Figura 2.2: Polígono regular de n lados - Grupo de Rotações



Fonte: Produção do próprio autor

Indicando por e a primeira dessas rotações e por a a segunda, como na Figura 2.2, então o conjunto dessas n rotações é composto pelos elementos

$$R_n = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Exemplo 2.2.16 $(D_n, \circ)$ - *Grupo Diedral de grau n: grupo de simetrias espaciais de um polígono regular de n lados.*

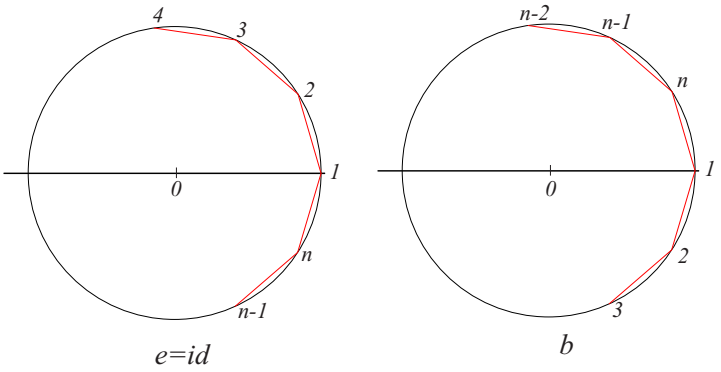
Como no Exemplo 2.2.15 considera-se o polígono de n vértices num referencial cartesiano com um vértice sobre o eixo x o qual será denotado por 1, esta posição inicial do polígono, como na Figura 2.2, será o elemento neutro do grupo D_n, a será a rotação de um ângulo de $\dfrac{2\pi}{n}$ radianos em torno da origem (Figura 2.2) e b a reflexão em torno do eixo-x, conforme a Figura 2.3.

O conjunto

$$D_n = \{e,\ a,\ a^2,\ \cdots,\ a^{n-1},\ b,\ ab,\ a^2b,\ \cdots,\ a^{n-1}b\}$$

cujos elementos são as rotações de R_n , estas rotações seguidas da reflexão b é o Grupo Diedral das simetrias do polígono de n lados.

Figura 2.3: Polígono regular de n lados - Grupo Diedral



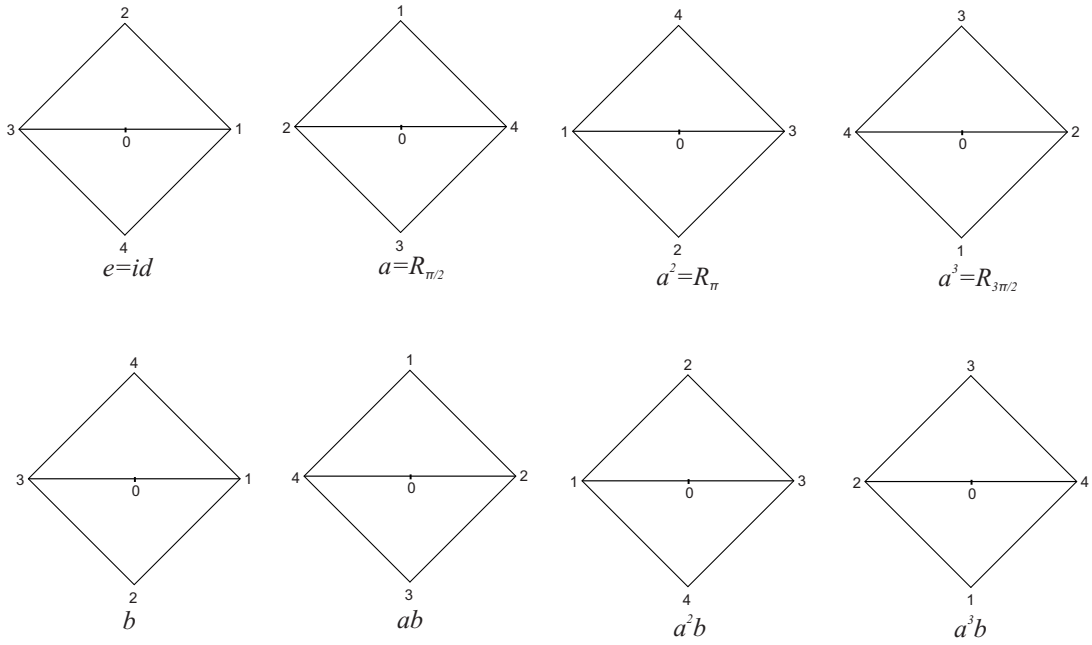
Fonte: Produção do próprio autor

Exemplo 2.2.17 $(D_4, \circ)$ - *grupo diedral de grau 4: grupo das simetrias do quadrado formado pelos elementos*

$$D_4 = \{e,\ a,\ a^2,\ a^3,\ b,\ ab,\ a^2b,\ a^3b\}$$

que estão representados na Figura 2.4.

Figura 2.4: Transformações espaciais que preservam o quadrado



Fonte: Produção do próprio autor

A tábua de D_4 é dada pela Tabela 2.3 e por ela observa-se que D_4 é de fato um grupo com elemento neutro e e este grupo não é abeliano.

Tabela 2.3: Tábua do Grupo D_4

$\circ$	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

Fonte: Produção do próprio autor

Exemplo 2.2.18 *Sejam* $(G, *)$ *e* $(J, \triangle)$ *grupos. No conjunto* $G \times J$ *defina a seguinte relação:*

$$(a, b) \odot (x, y) := (a * x,\ b \triangle y).$$

Então, $(G \times J, \odot)$ *é um grupo chamado* **produto direto** *de* G *por* J.

De fato, $\odot$ é uma lei de composição interna em $G \times J$ que satisfaz a propriedade associativa, pois G e J são grupos, o elemento neutro desta operação é (e_G, e_J) e o simétrico (inverso) do elemento $(x, y) \in G \times J$ é (x^{-1}, y^{-1}), em que x^{-1} é o simétrico de x em G e y^{-1} é o simétrico de y em J.

De modo análogo define-se o grupo produto direto de n parcelas, isto é,

$$(G_1 \times G_2 \times \cdots \times G_n, \odot)$$

sendo cada G_i, $i = 1, 2, \cdots, n$, um grupo. Se cada parcela for um grupo finito, então o produto direto será finito e

$$|G_1 \times G_2 \times \cdots \times G_n| = |G_1||G_2| \cdots |G_n|.$$

Além disso, se cada grupo for abeliano o grupo produto direto também será abeliano.

Como casos particulares de produto direto tem-se:

1. $\mathbb{Z} \times \mathbb{Z}$ com a operação sendo a adição definida por $(a, b) \oplus (x, y) = (a + x,\ b + y)$, o elemento neutro é $(0, 0)$ e o elemento simétrico de (a, b) é $(-a, -b)$.

2. $\mathbb{Z}_n \times \mathbb{Z}_m$ com a operação sendo a adição definida por $(\overline{a}, \overline{b}) \oplus (\overline{x}, \overline{y}) = (\overline{a + x},\ \overline{b + y})$, o elemento neutro é $(\overline{0}, \overline{0})$ e o elemento simétrico de $(\overline{a}, \overline{b})$ é $(\overline{n - a}, \overline{m - b})$. Além disso, $|\mathbb{Z}_n \times \mathbb{Z}_m| = nm$.

2.3 SUBGRUPOS

Definição 2.3.1 *Seja $(G,.)$ um grupo. Um subconjunto não vazio H de G é um* **subgrupo** *de G (que será denotado por $H < G$) quando o conjunto H é um grupo com a operação de G. Ou seja:*

(i) $h_1.h_2 \in H, \ \forall \ \ h_1, h_2 \in H.$

(ii) $(h_1.h_2).h_3 = h_1.(h_2.h_3), \ \forall \ \ h_1, h_2, h_3 \in H.$

(iii) $\exists \ \ e_H \in H \ / \ e_H.h = h.e_H, \forall \ \ h \in H.$

(iv) Para cada $h \in H$, existe $k \in H$ tal que $h.k = k.h = e_H$.

Observação 2.3.2 *A condição (ii) é sempre válida, pois ela é válida para todos os elementos de G.*

Observação 2.3.3 *O elemento neutro de H dado por e_H é necessariamente igual ao elemento neutro de G.*

Observação 2.3.4 *Seja $h \in H$, então o inverso de h em H é igual ao inverso de h em G em símbolos temos $(h_H^{-1} = h_G^{-1})$.*

Proposição 2.3.5 *Seja H um subconjunto não vazio do grupo G. Então, H é um subgrupo de G se, e somente se, a condição seguinte é satisfeita:*

$$\forall \ \ a, b \in H, a.b^{-1} \in H,$$

sendo b^{-1} o inverso de b em G.

Demonstração:

($\Rightarrow$) Supondo $H < G$, então por definição H é grupo com a operação herdada de G, e pelas observações acima $e_H = e_G$ e $h_H^{-1} = h_G^{-1}$. Assim, dados $a, b \in H$ tem-se que $b^{-1} \in H$ e assim $ab^{-1} \in H$

($\Leftarrow$) Supondo que para quaisquer $a, b \in H$ tem-se $ab^{-1} \in H$. Então, como $H \neq \emptyset$ existe $a \in H$ e pela hipótese $e_G = aa^{-1} \in H$ e consequentemente $a^{-1} = e_G a^{-1} \in H$. Assim, para $a, b \in H$ tem-se que $b^{-1} \in H$ e pela hipótese

$$ab = a(b^{-1})^{-1} \in H.$$

Além disso, como $H \subset G$ tem-se que a propriedade associativa continua válida em H. Portanto, $H < G$. ∎

Exemplo 2.3.6 *São exemplos de subgrupos:*

(i) Se G é um grupo com neutro e, então $\{e\}$ e G são subgrupos de G (chamados de subgrupos triviais).

(ii) $(2\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$. De maneira geral se n é um inteiro qualquer, $(n\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$.

De fato, sejam $h_1, h_2 \in n\mathbb{Z}$. Então, existem $n_1, n_2 \in \mathbb{Z}$ tais que $h_1 = nz_1$ e $h_2 = nz_2$, assim

$$h_1 - h_2 = nz_1 - nz_2 = n(z_1 - z_2) = nz \text{ com } z \in \mathbb{Z}.$$

Logo, $h_1 - h_2 \in n\mathbb{Z}$ e pela Proposição 2.3.5 $n\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$.

(iii) $\{id, R_1\}$ e $\{id, R_{\frac{2\pi}{3}}, R_{\frac{4\pi}{3}}\}$ são subgrupos de $S_\triangle$.

(iv) O grupo das rotações de um polígono regular de n lados, R_n, é subgrupo do grupo diedral D_n de ordem $2n$ obtido desse mesmo polígono.

(v) Se G é um grupo com $H < G$ e $K < G$, então $H \cap K < G$.

De fato, dados $a, b \in H \cap K$, então $a \in H$ e $a \in K$, ainda $b \in H$ e $b \in K$. Pela Proposição 2.3.5, basta provar que $ab^{-1} \in H \cap K$. Como $b \in H$ e $b \in K$ sendo H e K subgrupos de G, então existe $b^{-1} \in H$ e $b^{-1} \in K$, logo

- $ab^{-1} \in H$, pois $a \in H$ e $b^{-1} \in H$,
- $ab^{-1} \in K$, pois $a \in K$ e $b^{-1} \in K$.
  Assim, $ab^{-1} \in H \cap K$ logo $H \cap K$ é subgrupo de G.

Proposição 2.3.7 *$H < (\mathbb{Z}, +)$ se, e somente se, $H = n\mathbb{Z}$ para algum $n \in \mathbb{N}$.*

Demonstração:

($\Rightarrow$) Seja H um subgrupo qualquer de $\mathbb{Z}$. Se $H = \{0\}$, então $H = 0\mathbb{Z}$. Se $H \neq \{0\}$, então escolhendo $n = min\{x \in H | x > 0\}$ tem-se que $H = n\mathbb{Z}$. De fato, como $n \in \mathbb{N}$, tem-se que $n\mathbb{Z} \subset H$. Por outro lado, dado $h \in H$, pelo algoritmo de Euclides existem $q, r \in \mathbb{Z}$ tais que $h = qn + r$ com $0 \leq r < n$. Como h e n pertencem a H e H é subgrupo, então $r = h - qn \in H$. Pela minimalidade de n segue que $r = 0$ e $h = qn$, ou seja, $h \in n\mathbb{Z}$. Logo $H = n\mathbb{Z}$.

($\Leftarrow$) Provado no Exemplo 2.3.6 (ii). ∎

2.4 HOMOMORFISMOS DE GRUPOS

Nesta seção será estudado o homomorfismo de grupos, o que é muito importante para a classificação dos mesmos, pois encontra-se aplicações que preservam as operações.

Definição 2.4.1 *Dados dois grupos* $(G,*)$ *e* $(J,\triangle)$*, diz-se que uma aplicação* $f: G \to J$ *é um homomorfismo de* G *em* J *se, para todo* $x, y \in G$, $f(x*y) = f(x)\triangle f(y)$.

Observação 2.4.2 *Sejam* $(G,*)$ *e* $(J,\triangle)$ *grupos. Então,*

- *um homomorfismo do grupo* G *nele próprio,* $f: G \to G$*, é chamado* **endomorfismo** *de* G.
- *um homomorfismo* $f: G \to J$ *injetor é chamado* **monomorfismo** *de* G *em* J.
- *um homomorfismo* $f: G \to J$ *sobrejetor é chamado* **epimorfismo** *de* G *em* J.
- *um homomorfismo* $f: G \to J$ *bijetor é chamado* **isomorfismo** *de* G *em* J.

Definição 2.4.3 *Se existe um isomorfismo de grupos* $f: G \to J$*, diz-se que* G *e* J *são isomorfos e denota-se por* $G \simeq J$.

Exemplo 2.4.4 *Seja* $n \in \mathbb{N}$ *fixo. Então,* $\varphi_n : (\mathbb{Z},+) \to (\mathbb{Z},+)$*, dada por,* $\varphi_n(z) = nz$ *é monomorfismo, pois dados* $a, b \in \mathbb{Z}$

$$\varphi_n(a+b) = n(a+b) = na + nb = \varphi_n(a) + \varphi_n(b)$$

e para todo $x, y \in \mathbb{Z}$

$$\varphi_n(x) = \varphi_n(y) \quad \Leftrightarrow \quad nx = ny \quad \Leftrightarrow \quad x = y.$$

Definição 2.4.5 *Sejam* $(G,*)$ *e* $(J,\triangle)$ *grupos e* $f: G \longrightarrow J$ *um homomorfismo. Chama-se* **núcleo** *de* f *e denota-se por* $ker(f)$ *o seguinte subconjunto de* G*:*

$$ker(f) = \{x \in G / \ f(x) = e\}$$

sendo e *o elemento neutro de* J.

Proposição 2.4.6 *Seja* $f: (G,\cdot) \to (J,*)$ *um homomorfismo de grupos. Então:*

(i) $f(e_G) = e_J$

(ii) $f(x^{-1}) = f(x)^{-1}$

(iii) $Im(f) = \{y \in J \ \mid \ y = f(g) \text{ para algum } g \in G\}$ *é um subgrupo de* J.

(iv) Se B *é um subgrupo de* J*, então* $f^{-1}(B)$ *é um subgrupo de* G *contendo* $ker(f)$ *e* $f(f^{-1}(B)) = B \cap Im(f)$*. Em que* f^{-1} *é a aplicação inversa de* f.

(v) Sejam $f: (G,\cdot) \to (J,*)$ *e* $h: (J,*) \to (B,\times)$ *dois homomorfismos de grupos. Então a composição* $h \circ f: (G,.) \to (B,\times)$ *é um homomorfismo.*

(vi) $ker(f) < G$.

Demonstração:

(i) $f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G) \Rightarrow f(e_G) = e_J$

(ii)
$$\begin{cases} f(x^{-1}) * f(x) = f(x^{-1}.x) = f(e_G) = e_J \\ f(x) * f(x^{-1}) = f(x.x^{-1}) = f(e_G) = e_J \end{cases}$$

Portanto $f(x^{-1}) = (f(x))^{-1}$

(iii) Tem-se
$$y, z \in \ Im(f) \Rightarrow \exists\ x_1, x_2 \in G : \ y = f(x_1),\ z = f(x_2).$$

Logo,
$$y * z^{-1} = f(x_1) * (f(x_2))^{-1} = f(x_1) * f(x_2^{-1}) = f(x_1.x_2^{-1}).$$

Como $x_1.x_2^{-1} \in G$, segue que $y * z^{-1} \in Im(f)$ e pela Proposição 2.3.5, $Im(f) < J$.

(iv) Sejam $a, b \in f^{-1}(B)$. Então, $f(a), f(b) \in B$ e $f(a) * f(b)^{-1} \in B$. Como,

$$f(a) * f(b)^{-1} = f(a) * f(b^{-1}) = f(a.b^{-1}) \in B,$$

então $a.b^{-1} \in f^{-1}(B)$, donde $f^{-1}(B) < G$.

Seja $x \in Ker(f)$. Então, $f(x) = e_J \in B$ e consequentemente $x \in f^{-1}(B)$. Donde $Ker(f) \subset f^{-1}(B)$. Além disso, $f(f^{-1}(B)) = Im(f) \cap B$.

(v) Dados $x, y \in G$ então
$(h \circ f)(x \cdot y) = h(f(x \cdot y)) = h(f(x) * f(y)) = h(f(x)) \times h(f(y)) = (h \circ f)(x) \times (h \circ f)(y)$.

(vi) Sejam $x, y \in Ker(f)$. Então,

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = ee^{-1} = e \Rightarrow xy^{-1} \in Ker(f).$$

Portanto, $ker(f) < G$.

■

Exemplo 2.4.7 *Os grupos S_3 e $S_\triangle$ são isomorfos.*

De fato, considerando a seguinte relação f:

$$\begin{aligned} f : S_3 &\to S_\triangle \\ id &\mapsto id \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = f_1 &\mapsto R_{\frac{2\pi}{3}} \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = f_2 &\mapsto R_{\frac{4\pi}{3}} \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = g_3 &\mapsto R_3 \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = g_2 &\mapsto R_2 \\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = g_1 &\mapsto R_1 \end{aligned}$$

Tem-se que f é bijetora e também um homomorfismo, logo é um isomorfismo, analisando as Tabelas 2.1 e 2.2 pode-se observar que são equivalentes, o que explicita que $S_3 \simeq S_\triangle$.

2.5 GRUPOS CÍCLICOS

Nesta seção serão estudados os grupos cíclicos, que são de grande importância para a classificação de grupos. Será visto mais adiante que com os grupos cíclicos pode-se classificar imediatamente os grupos de ordem prima.

Definição 2.5.1 *Seja G um grupo multiplicativo. Dado $a \in G$ define-se a potência m-ésima de a, para todo inteiro m, como num dos segintes casos*

- *se $m = 0 : a^0 = e$ (elemento neutro de G)*
- *se $m \geq 1 : a^m = a^{m-1} \cdot a$*
- *se $m < 0 : a^m = (a^{-m})^{-1}$, sendo $(a^{-m})^{-1}$ o inverso de a^{-m}*

Em particular num grupo aditivo o análogo à potência é o múltiplo:

Definição 2.5.2 *Seja G um grupo aditivo. Se $a \in G$ e $m \in \mathbb{Z}$, o múltiplo m-ésimo de a é o elemento de G denotado por $m \cdot a$ e definido por*

- *se $m = 0 : 0 \cdot a = e$ (elemento neutro de G)*
- *se $m \geq 1 : m \cdot a = (m-1) \cdot a + a$*

- *se* $m < 0 : m \cdot a = -(-m \cdot a)$ *sendo* $(-m \cdot a)$ *é o oposto de* $m \cdot a$

Proposição 2.5.3 *Seja* G *um grupo multiplicativo. Se* m *e* n *são números inteiros e* $a \in G$*, então:*

(i) $a^m \cdot a^n = a^{m+n}$

(ii) $a^m \cdot a^n = a^n \cdot a^m$

(iii) $a^{-m} = (a^m)^{-1}$

(iv) $(a^m)^n = a^{mn}$

Analogamente, para grupos aditivos temos o resultado:

Proposição 2.5.4 *Seja* G *um grupo aditivo. Se* m *e* n *são números inteiros e* $a \in G$*, então:*

(i) $ma + na = (m + n)a$

(ii) $ma + na = na + ma$

(iii) $(-m)a = -(ma)$

(iv) $n(ma) = (nm)a$

A ideia de demonstração das propriedades anteriopres podem ser encontradas no livro de Domingues e Iezzi (1979) p. 108.

Proposição 2.5.5 *Se* S *é um subconjunto não-vazio do grupo* G*, então o conjunto*

$$\langle S \rangle = \{a_1^{n_1} a_2^{n_2} \dots a_k^{n_k} / \ k \in \mathbb{N}^*, \ n_i \in \mathbb{Z}, \ a_i \in S\}$$

é um subgrupo de G*.*

A demonstração encontra-se na obra de Domingues e Iezzi (1979) p. 112.

Definição 2.5.6 *Sejam* G *um grupo e* S *um subconjunto não-vazio de* G*. O conjunto* $\langle S \rangle$*, definido na Proposição 2.5.5, é chamado* **subgrupo gerado** *por* S*.*

Exemplo 2.5.7 *Observa-se, pela Tabela 2.1, que*

$$S_3 = \{f_0, \ f_1, \ f_1^2, \ g_1, \ f_1 \circ g_1, \ f_1^2 \circ g_1\} = \langle f_1, \ g_1 \rangle$$

e pela Tabela 2.2

$$S_\triangle = \{id, R_{\frac{2\pi}{3}}, R_{\frac{2\pi}{3}}^2, R_1, R_{\frac{2\pi}{3}} \circ R_1, R_{\frac{2\pi}{3}}^2 \circ R_1\} = \langle R_{\frac{2\pi}{3}}, \ R_1 \rangle.$$

Definição 2.5.8 *Um grupo G é* **cíclico** *quando ele pode ser gerado por um elemento, isto é, quando $G = \langle g \rangle$, para algum $g \in G$.*

Exemplo 2.5.9 *São Exemplos de Grupos Cíclicos:*

(i) $(\mathbb{Z}, +) = \langle 1 \rangle$, *pois*

$$\mathbb{Z} = \{ \cdots, \ 1 \cdot (-2), \ 1 \cdot (-1), \quad 1 \cdot 0, \quad 1 \cdot 1, \quad 1 \cdot 2, \quad 1 \cdot 3, \quad \cdots \}$$

(ii) $(\mathbb{Z}_5^*, \odot) = \langle \overline{2} \rangle$, *pois* $\mathbb{Z}_5^* = \{\overline{1}, \quad \overline{2}, \quad \overline{3}, \quad \overline{4}\}$ *e*

$$\overline{2}^{\,0} = \overline{1}; \quad \overline{2}^{\,1} = \overline{2}; \quad \overline{2}^{\,2} = \overline{4}; \quad \overline{2}^{\,3} = \overline{8} = \overline{3}.$$

O próximo resultado indica uma interessante propriedade satisfeita para todos os grupos cíclicos.

Proposição 2.5.10 *Se G é um grupo cíclico, então G é abeliano.*

Demonstração: Se G é um grupo cíclico, então existe $g \in G$ e modo que

$$G = \langle g \rangle = \{g^n / \ n \in \mathbb{Z}\}.$$

Assim, dados $a, b \in G$ existem $n, m \in \mathbb{Z}$ tais que $a = g^n$ e $b = g^m$, logo

$$ab = g^n g^m = g^{n+m} = g^{m+n} = g^m g^n = ba.$$

Portanto, G é abeliano. ■

Proposição 2.5.11 *Todo subgrupo de um grupo cíclico também cíclico.*

Demonstração: Seja $(G, .)$ um grupo cíclico e H um subgrupo de G. Então, existe $a \in G$ tal que $G = \langle a \rangle$

Se $H = \{e\}$, então $H = \langle e \rangle$ com e sendo neutro de G. Se $H \neq \{e\}$, então existe $x \in H - \{e\}$. Como $x \in H \subset G = \langle a \rangle$, então existe $n \in \mathbb{Z}$ tal que $x = a^n$.

Seja b a menor potência positiva de a em H, isto é, $b = a^l \in H$ e l é o menor inteiro não nulo tal que $a^l \in H$. Será provado que $H = \langle b \rangle = \langle a^l \rangle$.

Tem-se que se $a^l \in H$, então $\langle a^l \rangle \subset H$, falta provar então que $H \subset \langle a^l \rangle$.

Seja $x \in H$, então basta provar que $x = (a^l)^m$ para algum $m \in \mathbb{Z}$. Como $H \subset G = \langle a \rangle$, existe $t \in \mathbb{Z}$ tal que $x = a^t$. Pelo algoritmo de Euclides, tem-se $t = lq + r$ com $q \in \mathbb{Z}$

e $0 \leqslant r < l$, então,

$$\begin{aligned} x = a^t &= a^{lq+r} = a^{lq}a^r \\ &\Rightarrow (a^{lq})^{-1}x = a^r \\ &\Rightarrow a^{-lq}x = a^r \\ &\Rightarrow (a^l)^{-q}x = a^r \end{aligned}$$

Como $a^l \in H$ e $x \in H$, então $(a^l)^{-q} \in H$, sendo H subgrupo tem-se que

$$a^r = (a^l)^{-q}x \in H.$$

Assim $a^r \in H$ e $0 \leqslant r < l$. Como l é o menor inteiro positivo com $a^l \in H$, então $r = 0$ e

$$x = (a^l)^q e = (a^l)^q \subset \langle a^l \rangle.$$

Portanto, $H = \langle a^l \rangle$, ou seja, H é cíclico.

■

Definição 2.5.12 *Dado um elemento a de um grupo multiplicativo G com elemento neutro e, se*

$$a^m = e \quad \Leftrightarrow \quad m = 0,$$

diz-se que o elemento a tem **período zero** *ou* **ordem zero** *e que o grupo $\langle a \rangle$ é um* **grupo cíclico infinito.**

Definição 2.5.13 *Seja G um grupo com elemento neutro e e seja $a \in G$. O menor número inteiro $h > 0$ tal que $a^h = e$ chama-se* **período** *ou* **ordem** *do elemento a. Notação $o(a) = h$.*

Proposição 2.5.14 *Seja a um elemento de um grupo multiplicativo G, com elemento neutro e. Se a ordem de a é $h > 0$, então $\langle a \rangle$ é um grupo finito de ordem h dado por $\langle a \rangle = \{e,\ a,\ a^2,\ \cdots,\ a^{h-1}\}$.*

Demonstração: Por definição de grupo gerado, tem-se que $\{e, a, a^2, \ldots, a^{h-1}\} \subset \langle a \rangle$. Por outro lado, seja $a^m \in \langle a \rangle$. Pelo algoritmo de Euclides, tem-se que existem $q, r \in \mathbb{Z}$ com $0 \leqslant r < h$ tal que

$$a^m = a^{hq+r} = a^{hq}.a^r = (a^h)^q.a^r = e^q.a^r = a^r,$$

ou seja, $a^m \in \{e, a, a^2, \ldots, a^{h-1}\}$. Portanto, $\langle a \rangle = \{e, a, a^2, \ldots, a^{h-1}\}$.

Falta provar que $|\langle a \rangle| = h$. Suponha que existam $r, s \in \mathbb{Z}$ com $0 \leqslant r < s \leqslant h-1$ tais que $a^r = a^s$. Então, $a^{s-r} = e$, o que é um absurdo, pois como $0 < s - r < h$, teríamos $o(a) = s - r < h$. Portanto, $|\langle a \rangle| = h$. ■

Definição 2.5.15 *Seja $G = \langle a \rangle$ um grupo cíclico, com neutro e. Diz-se que G é um* **grupo cíclico finito** *se o período do elemento a for um número natural $h > 0$. Desta forma,*

$$G = \{e,\ a,\ a^2,\ \cdots,\ a^{h-1}\}.$$

Proposição 2.5.16 *Seja a um elemento de um grupo G com ordem $h > 0$. Então,*

$$a^m = e \iff h|m, \tag{2.5.1}$$

sendo e o elemento neutro de G.

Demonstração:

($\Rightarrow$) Tem-se por hipótese que $a^m = e$. Então, pelo algoritmo de Euclides $m = hq+r$ com $q \in \mathbb{Z}$ e $0 \leq r \leq h-1$ e

$$e = a^m = a^{hq+r} = (a^h)^q.a^r = e^q.a^r = a^r$$

logo $e = a^r,\ 0 \leq r \leq h-1$. Como $o(a) = h$, tem-se que $r = 0$ e $m = hq$ ou seja $h|m$.

($\Leftarrow$) Tem-se por hipótese que $h|m$, então $m = hq$ com $q \in \mathbb{Z}$. Logo $a^m = a^{hq} = (a^h)^q = e^q = e$ portanto $a^m = e$. ■

Exemplo 2.5.17 *Seja $f : G \to J$ um homomorfismo de grupos. Se $o(x) < \infty$, então $o(f(x))$ divide $o(x)$.*

De fato, sendo $n = o(x)$, tem-se $x^n = e_G$, então

$$e_J = f(e_G) = f(x^n) = f(x)^n.$$

Portanto, pela Proposição 2.5.16 $o(f(x))$ divide n.

Teorema 2.5.18 *Seja $G = \langle a \rangle$ um grupo cíclico infinito, com elemento neutro e. Então:*

(i) G possui dois e apenas dois geradores.

(ii) G é isomorfo ao grupo aditivo dos números inteiros.

Demonstração:

(i) Se $G = \langle a \rangle$, então $G = \langle a^{-1} \rangle$. Seja $b \in G$ tal que $G = \langle b \rangle$. Então, existem $n, m \in \mathbb{Z}$ tais que

$$a = b^n = (a^m)^n = a^{mn}$$

donde $a^{1-mn} = e$. Como G é um grupo cíclico infinito, segue que $1 - mn = 0$, ou seja, $mn = 1$ e $m = n = 1$ ou $m = n = -1$. Assim, os únicos geradores de G são a e a^{-1}.

(ii) A relação $f : (\mathbb{Z}, +) \longrightarrow (G, \cdot)$ dada por $f(z) = a^z$, é um isomorfismo, pois f é bijetora, e ainda $f(z + w) = a^{z+w} = a^z.a^w$. Logo, $(\mathbb{Z}, +) \simeq (G, \cdot)$.

■

Por este teorema todo grupo cíclico infinito é isomorfo a $(\mathbb{Z}, +)$, ou seja, a menos de isomorfismos $(\mathbb{Z}, +)$ é o único grupo cíclico infinito.

Teorema 2.5.19 *Seja $G = \langle a \rangle = \{e,\ a,\ a^2,\ \cdots,\ a^{n-1}\}$ um grupo cíclico de ordem finita igual a n. Então, G é isomorfo a $(\mathbb{Z}_n, \oplus)$.*

Demonstração: Note que a relação $f : (\mathbb{Z}_n, \oplus) \longrightarrow (G, \cdot)$ definida por $f(\overline{r}) = a^r$ é um isomorfismo. Logo, $(\mathbb{Z}_n, \oplus) \simeq (G, \cdot)$. ■

Por este teorema, a menos de isomorfismos, $(\mathbb{Z}_n, \oplus)$ é o único grupo cíclico de ordem n.

2.6 CLASSES LATERAIS

Nesta seção serão apresentadas as classes laterais, que tem aplicação direta no Teorema de Lagrange.

Definição 2.6.1 *Seja H um subgrupo de um grupo $(G, .)$. Dado $a \in G$ denotaremos por aH e chamaremos de* **classe lateral à esquerda**, *módulo H, o subconjunto*

$$aH = \{ax/\ x \in H\} \subset G.$$

Analogamente, denotaremos por Ha e chamaremos de **classe lateral à direita**, *módulo H, o subconjunto*

$$Ha = \{xa/\ x \in H\} \subset G.$$

Se G é um grupo comutativo temos que $aH = Ha$, para todo $a \in G$ e todo subgrupo H.

Observação 2.6.2 *Se $a \in H$, então $aH = H = Ha$.*

Proposição 2.6.3 *Seja H um subgrupo de G. Então, $aH = bH$ se, e somente se, $a^{-1}b \in H$.*

Demonstração:
($\Rightarrow$)

$$aH = bH \quad \Rightarrow \quad \exists h \in H : eb = ah \quad \Rightarrow \quad a^{-1}b = h \in H.$$

($\Leftarrow$)

$$a^{-1}b \in H \quad \Rightarrow \quad \exists h \in H : a^{-1}b = h \quad \Rightarrow \quad b = ah \ \text{ e } \ a = bh^{-1}.$$

Logo, se $x \in aH$, então existe $h_1 \in H$ tal que $x = ah_1$ e

$$x = ah_1 = (bh^{-1})h_1 = b(h^{-1}h_1) \in bH,$$

pois $H < G$. Portanto, $aH \subset bH$. Analogamente obtém-se que $bH \subset aH$ e consequentemente $aH = bH$. ■

Proposição 2.6.4 *Seja H um subgrupo de $(G, *)$. Então que o conjunto das classes laterais à esquerda, módulo H, forma uma partição em G e os conjuntos desta partição são equipotentes entre si, ou seja, tem a mesma cardinalidade. Um resultado análogo é válido para classes laterais à direita.*

Demonstração: Seja $\mathcal{P} = \bigcup_{a \in G} aH$. Então, $G = \bigcup_{a \in G} aH$.

Suponha que $x \in aH \cap bH$. Então, existem $h_1, h_2 \in H$ tais que $x = ah_1$ e $x = bh_2$. Assim,

$$ah_1 = bh_2 \Rightarrow h_1 = a^{-1}bh_2 \Rightarrow a^{-1}b = h_1(h_2)^{-1} \in H,$$

pois $H < G$. Pela Proposição 2.6.3 tem-se que $aH = bH$. Logo, ou $aH = bH$ ou $aH \cap bH = \emptyset$. Portanto, $\mathcal{P}$ é uma partição de G.

Além disso, observa-se que para qualquer $a \in G$ a aplicação $f : H \longrightarrow aH$ dada por $f(h) = ah$ é bijetora. Logo, $\#(aH) = |H|$ para todo $a \in G$, donde $\#(aH) = \#(bH)$ para quaisquer $a, b \in G$. ■

Definição 2.6.5 *A cardinalidade do conjunto das classes laterais à esquerda é o* **índice** *de H em G, e será denotado por $(G : H)$.*

Teorema 2.6.6 (Teorema de Lagrange) *Sejam G um grupo finito e H um subgrupo de G. Então, $|G| = |H|(G : H)$, em particular, a ordem e o índice de H dividem a ordem de G.*

Demonstração: Seja $\mathcal{P}$ partição de G formada pelas classes laterais à esquerda. Como G é finito existe uma quantidade finita de elementos nesta partição, suponha que a quantidade de elementos de $\mathcal{P}$ é $(G : H) = k$, ou seja,

$$\mathcal{P} = \{a_1H, \ldots, a_kH\}$$

sendo todas as classes distintas. Pela Proposição 2.6.4 todas as classes tem a mesma cardinalidade de H, ou seja,

$$\#(a_1H) = \ldots = \#(a_kH) = |H|$$

$$\therefore |G| = k.|H|$$

$$\Longrightarrow |G| = |H|(G : H)$$

■

Corolário 2.6.7 *Seja G um grupo finito e seja $\alpha \in G$. Então, a ordem de α divide a ordem de G.*

Demonstração: De fato, $o(\alpha) = |\langle\alpha\rangle|$ e pelo Teorema de Lagrange (Teorema 2.6.6) $|\langle\alpha\rangle|$ divide $|G|$. ■

Corolário 2.6.8 *Seja G um grupo de ordem prima. Então, G é cíclico.*

Demonstração: Seja $a \in G$. Pelo Corolário 2.6.7, $o(a)||G|$. Como $|G|$ é um número primo, segue que ou $o(a) = 1$ ou $o(a) = |G|$. Se $o(a) = 1$, então a é o elemento neutro de G. Se $o(a) = |G|$, então $\langle a\rangle = G$, ou seja, G é cíclico. ■

Proposição 2.6.9 *Seja G um grupo finito e sejam $K < H < G$. Então,*

$$(G : K) = (G : H)(H : K)$$

Demonstração: Pelo Teorema de Lagrange:

$$H < G \Longrightarrow |G| = |H|(G : H) \tag{2.6.2}$$

$$K < H \Longrightarrow |H| = |K|(H : K) \tag{2.6.3}$$

Substituindo (2.6.3) em (2.6.2), temos

$$|G| = |K|(H : K)(G : H) \tag{2.6.4}$$

e ainda

$$K < G \Longrightarrow |G| = |K|(G : K) \tag{2.6.5}$$

Comparando (2.6.5) e (2.6.4) tem-se que

$$(G : K) = (G : H)(H : K) \tag{2.6.6}$$

■

Definição 2.6.10 *Um subgrupo H de um grupo G é chamado* **subgrupo normal** *(e denotado por $H \triangleleft G$) se, para todo $x \in G$, tem-se $xH = Hx$. Ou seja, a classe lateral à esquerda módulo H, determinada por x é igual à classe lateral à direita, módulo H, determinada por x, para qualquer $x \in G$.*

Exemplo 2.6.11 *São exemplos de subgrupos normais:*

(i) $\{e\}, G$ são subgrupos normais de G.

(ii) Se $(G : H) = 2$, então $H \triangleleft G$. De fato se $(G : H) = 2$, então existem duas classes laterais distintas, H e H^c. Logo,

- se $x \in H$, então $xH = H = Hx$
- se $x \notin H$, então $xH = H^c = Hx$.

(iii) Se G é um grupo abeliano, então todo subgrupo de G é normal em G. A recíproca é falsa em geral como contra-exemplo tem-se o grupo do quatérnios, apresentado no Capítulo 3.

(iv) Seja G um grupo. Se todo elemento de G, exceto o neutro e, tem ordem 2, então G é abeliano e consequentemente todos seus subgrupos são normais.

De fato, dados $a, b \in G - \{e\}$, tem-se que $ab,\ ba \in G$ e

$$o(a) = o(b) = o(ba) = o(ab) = 2.$$

Logo,

$$ab = e(ab)e = b^2(ab)a^2 = b(ba)(ba)a = b(ba)^2a = bea = ba,$$

ou seja, $ab = ba$ para todo $a, b \in G$, donde G é abeliano. Pelo item (iii) todo subgrupo de G é normal.

(v) Se $f : (G) \longrightarrow (J, *)$ é um homomorfismo de grupos, então $ker(f) \triangleleft G$.

De fato, dado $y \in xKer(f)$, existe $a \in Ker(f)$ tal que $y = xa$. Logo, $y = xax^{-1}x$ e

$$f(xax^{-1}) = f(x) * f(a) * f(x^{-1}) = f(x) * e_J * f(x)^{-1} = e_J$$

ou seja, $xax^{-1} \in Ker(f)$ e consequentemente $y \in Ker(f)x$.

Assim, $xKer(f) \subset Ker(f)x$. Analogamente prova-se que $xKer(f) \supset Ker(f)x$. Portanto, $Ker(f) \triangleleft G$.

Capítulo 3

DETERMINAÇÃO DE ALGUNS GRUPOS

Neste capítulo deseja-se classificar os grupos de ordem menor ou igual a 11.

Já sabe-se que o único grupo de ordem 1 é o grupo que contém apenas o elemento neutro $\{e\}$. Além disso, para os grupos de ordem prima, isto é,para $p = 2, 3, 5, 7$ ou 11, tem-se pelo Corolário 2.6.8 que G é cíclico, e pelo Teorema 2.5.19, obtém-se que $G \simeq \mathbb{Z}_p$.

Na primeira seção deste capítulo, serão apresentados resultados importantes para a classificação dos grupos gerados por dois elementos em particular os grupos de ordem $6, 8, 9$ e 10.

3.1 GRUPOS FINITOS GERADOS POR DOIS ELEMENTOS

Definição 3.1.1 *Seja $(G, \cdot)$ um grupo. Um* **automorfismo** *de G é um isomorfismo $f : G \longrightarrow G$. O conjunto dos automorfismos de G será denotado por $Aut(G)$.*

Exemplo 3.1.2 *Tem-se que $\mathcal{I}_g : G \longrightarrow G$, dada por $\mathcal{I}_g(x) = gxg^{-1}$, é um homomorfismo bijetivo e portanto um automorfismo de G, chamado de* **automorfismo interno** *associado ao elemento $g \in G$.*

De fato, tem-se

1. $\mathcal{I}_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \mathcal{I}_g(x)\mathcal{I}_g(y)$
2. $\mathcal{I}_g(x) = \mathcal{I}_g(y) \Leftrightarrow gxg^{-1} = gyg^{-1} \Leftrightarrow x = y$
3. $z \in G \Rightarrow g^{-1}zg \in G$ e $\mathcal{I}_g(g^{-1}zg) = g(g^{-1}zg)g^{-1} = z$.

Portanto, $\mathcal{I}_g$ é um automorfismo.

O conjunto dos automorfismos internos de G será denotado por $\mathcal{I}(G)$, assim

$$\mathcal{I}(G) := \{\mathcal{I}_g \ / \ g \in G\} \subseteq Aut(G).$$

Proposição 3.1.3 *$(\mathcal{I}(G), \circ)$ é um subgrupo normal de $(Aut(G), \circ)$.*

Demonstração:

1. $\mathcal{I}(G)$ é subgrupo de $Aut(G)$, pois dados $\mathcal{I}_a$ e $\mathcal{I}_b \in \mathcal{I}(G)$, tem-se que

   (a) $(\mathcal{I}_a \circ \mathcal{I}_b)(x) = \mathcal{I}_a(\mathcal{I}_b(x)) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \mathcal{I}_{ab}(x) \in \mathcal{I}(G)$;

   (b) sendo e o elemento neutro de G, então $\mathcal{I}_e$ é o elemento neutro de $\mathcal{I}(G)$, pois $(\mathcal{I}_e \circ \mathcal{I}_a)(x) = \mathcal{I}_{ea}(x) = \mathcal{I}_a(x)$;

   (c) $(\mathcal{I}_b)^{-1} = \mathcal{I}_{b^{-1}}$, pois $\mathcal{I}_b \circ \mathcal{I}_{b^{-1}} = \mathcal{I}_{bb^{-1}} = \mathcal{I}_e$.

   Assim,

   $$(\mathcal{I}_a \circ \mathcal{I}_{b^{-1}})(x) = \mathcal{I}_a(b^{-1}xb) = ab^{-1}xba^{-1} = (ab^{-1})x(ab^{-1})^{-1} = \mathcal{I}_{ab^{-1}}(x),$$

   ou seja, $\mathcal{I}_a \circ \mathcal{I}_b^{-1} \in \mathcal{I}(G)$ e pela Proposição 2.3.5 $\mathcal{I}(G) < Aut(G)$.

2. $\mathcal{I}(G)$ é normal a $Aut(G)$, pois escolhendo $f \in Aut(G)$ seja $h \in f \circ \mathcal{I}(G)$. Então, existe $\mathcal{I}_g \in \mathcal{I}(G)$ tal que $h = f \circ \mathcal{I}_g$ e

   $$\begin{aligned} h(x) &= (f \circ \mathcal{I}_g)(x) = f(\mathcal{I}_g(x)) = f(gxg^{-1}) = f(g)f(x)f(g^{-1}) \\ &= f(g)f(x)f(g)^{-1} = \mathcal{I}_{f(g)}(f(x)) = (\mathcal{I}_{f(g)} \circ f)(x) \end{aligned}$$

   donde, $h = \mathcal{I}_{f(g)} \circ f$ e $h \in \mathcal{I}(G) \circ f$ para qualquer $f \in Aut(G)$. Assim, $f \circ \mathcal{I}(G) \subset \mathcal{I}(G) \circ f$. Analogamente prova-se a outra inclusão. Portanto, $\mathcal{I}(G) \lhd Aut(G)$.

■

Teorema 3.1.4 *Seja $s \geq 1$ um inteiro e seja G um grupo finito com $a, b \in G$ satisfazendo $ba = a^s b$ (equivalentemente, $\mathcal{I}_b(a) = a^s$). Além disso, considere $n, m \geq 1$ inteiros tais que*

$$a^n = e, \quad b^m \in \langle a \rangle. \tag{3.1.1}$$

Então,

(a) (i) $b^t.a^r = a^{rs^t}.b^t$, *para todo* $r, t \in \mathbb{N}$, *e*

$$\langle a, b \rangle = \{a^i b^j / \ 0 \leq i \leq n-1 \ \ e \ \ 0 \leq j \leq m-1\}.$$

(ii) Se os inteiros n, m são escolhidos minimalmente satisfazendo a equação (3.1.1), então o grupo $\langle a, b\rangle$ tem ordem igual a mn.

(b) Sejam J um grupo e $c, d \in J$. Se os inteiros m, n são escolhidos minimalmente, e se u é um inteiro tal que $b^m = a^u$, então existe um homomorfismo $f : \langle a, b\rangle \longrightarrow J$ com $f(a) = c$ e $f(b) = d$ se, e somente se,

$$dc = c^s d, \quad c^n = e_J, \quad d^m = a^u.$$

Demonstração:

(a)(i) Como G é um grupo finito, então m, n realmente existem, pois $a^{o(a)} = e$ e $b^{o(b)} = e \in \langle a\rangle$. Para mostrar que $b^t.a^r = a^{rs^t}b^t$, basta verificar que $\mathcal{I}_{b^t}(a^r) = a^{rs^t}$, pois $\mathcal{I}_{b^t}(a^r) = b^t.a^r.(b^t)^{-1}$.

A demonstração será com por indução em t. Se $t = 0$ tem-se que $\mathcal{I}_e(a^r) = a^r$. Para $t = 1$ segue que

$$\begin{aligned}
\mathcal{I}_b(a^r) &= ba^rb^{-1} \\
&= baaa\cdots ab^{-1} \\
&= ba(b^{-1}b)a(b^{-1}b)a\cdots a(b^{-1}b)ab^{-1} \\
&= (bab^{-1})^r = (a^sbb^{-1})^r = (a^s)^r = a^{rs}
\end{aligned}$$

Supondo o resultado válido para k com $1 < k < t - 1$, tem-se

$$\begin{aligned}
\mathcal{I}_{b^t}(a^r) &= b^t.a^r.(b^t)^{-1} \\
&= b.b^{t-1}.a^r.(b.b^{t-1})^{-1} \\
&= b.b^{t-1}.a^r.(b^{t-1})^{-1}.b^{-1} \\
&= b\mathcal{I}_{b^{t-1}}b^{-1} \\
&= ba^{rs^{t-1}}b^{-1}, \text{ pela hipótese de indução} \\
&= \mathcal{I}_b(a^{rs^{t-1}}) = (a^{rs^{t-1}})^s, \text{ pelo caso em que t = 1} \\
&= a^{rs^{t-1}s} = a^{rs^t}
\end{aligned}$$

Além disso,

$$\langle a, b\rangle = \{a^lb^k/\ l, k \in \mathbb{Z}\} \cup \{b^pa^q/p, q \in \mathbb{Z}\}$$

e pelo fato de G ser um grupo finito, todos os elementos de $\langle a, b\rangle$ podem ser escritos como potências de números naturais, ou seja,

$$\langle a, b\rangle = \{a^lb^k/\ l, k \in \mathbb{N}\} \cup \{b^pa^q/p, q \in \mathbb{N}\}.$$

Ainda como foi provado acima, todo elemento do tipo $b^p a^q$ pode ser escrito como $a^{qs^p} b^p$. Logo, qualquer elemento de $\langle a, b\rangle$ é da forma $a^v b^w$, com $v, w \in \mathbb{N}$.

Agora pela condição $b^m \in \langle a\rangle$, para algum $m \geq 1$, tem-se que

$$a^v b^w = a^v b^m b^j = a^u b^j, \text{ com } 0 \leq j \leq m-1$$

além disso, $a^n = e$, para algum $n \geq 1$, assim

$$a^u = a^{tn+i} = a^i, \text{ com } 0 \leq i \leq n-1$$

e consequentemente

$$a^v b^w = a^i b^j, \text{ com } 0 \leq i \leq n-1 \text{ e } 0 \leq j \leq m-1.$$

Portanto,

$$\langle a, b\rangle = \{a^i b^j / \ 0 \leq i \leq n-1 \ \text{ e } \ 0 \leq j \leq m-1\}.$$

(ii) Falta provar que $\#\langle a, b\rangle = mn$, para tal, é suficiente verificar que se $0 \leq i, k \leq n-1$, $0 \leq j, l \leq m-1$ e $a^i b^j = a^k b^l$, então $i = k$ e $j = l$

Supondo que $l \leq j$ e multiplicando ambos os lados da igualdade por a^{-i} à esquerda e por b^{-l} à direita, obtém-se

$$b^{j-l} = a^{k-i} \in \langle a\rangle \text{ com } 0 \leq j-l \leq j \leq m-1,$$

portanto, pela minimalidade da escolha de m, tem-se que $j - l = 0$, ou seja, $j = l$ e consequentemente $a^{k-i} = e$ e pela minimalidade de n, segue que $k = i$.

(b) ($\Rightarrow$) Supondo que existe um homomorfismo $f : \langle a, b\rangle \longrightarrow J$ tal que $f(a) = c$ e $f(b) = d$. Como $ba = a^s b$, tem-se

$$dc = f(b)f(a) = f(ba) = f(a^s b) = (f(a))^s f(b) = c^s d.$$

Além disso, como $a^n = e_G$ e $b^m = a^u$ para algum $u \in \{0, 1, \cdots, n-1\}$ tem-se que

* $c^n = (f(a))^n = f(a^n) = f(e_G) = e_J$.
* $d^m = (f(b))^m = f(b^m) = f(a^u) = (f(a))^u = c^u$.

($\Leftarrow$) Sejam $c, d \in J$ tais que

$$dc = c^s d, \ c^n = e_J \ \text{ e } \ d^m = c^u,$$

com $m, n \geq 1$ escolhidos minimalmente.

Pela parte (a) aplicada a J e $a, c, d \in J$ tem-se que

$$d^t c^r = c^{rs^t} d^t, \text{ para todo } r, t \in \mathbb{N}.$$

Considera a relação $f : \langle a, b\rangle \longrightarrow J$ definida por $f(a^i b^j) = c^i d^j$.

Como m, n foram escolhidos minimalmente, foi provado para o item (ii) da parte (a) que para $0 \leq i, k \leq n-1$ e $0 \leq j, l \leq m-1$ tais que $a^i b^j = a^k b^l$, então $i = k$ e $j = l$ e consequentemente

$$f(a^i b^j) = c^i d^j \quad \text{e} \quad f(a^k b^l) = c^k d^l = c^i d^j,$$

ou seja, f está bem definida.

E ainda f é homomorfismo pois,

$$\begin{aligned} f((a^i b^j)(a^k b^l)) &= f(a^i (b^j a^k) b^l) = f(a^i (a^{ks^j} b^j) b^l) = f(a^{i+ks^j} b^{j+l}) \\ &= f(a^{i+ks^j} b^{mp} b^v) = f(a^{i+ks^j} a^{up} b^v) = f(a^w b^v) \\ &= c^w d^v = c^{i+ks^j} c^{pu} d^v = c^{i+ks^j} d^{pm} d^v = c^{i+ks^j} d^{j+l} \\ &= c^i (c^{ks^j} d^j) d^l = (c^i d^j)(c^k d^l) = f(a^i b^j) f(a^k b^l). \end{aligned}$$

■

Observação 3.1.5 *Se no Teorema 3.1.4 souber-se que a ordem do grupo $\langle a, b\rangle$ é nm, então pela da parte (a), os inteiros n e m são minimais e em particular, $o(a) = n$.*

Teorema 3.1.6 *Sejam $n, m, s, u \geq 0$ inteiros.*

(i) Se G é um grupo de ordem nm que possui elementos a, b tais que

$$G = \langle a, b\rangle, \quad a^n = e, \quad b^m = a^u, \quad ba = a^s b, \tag{3.1.2}$$

então, $s^m \equiv 1 (mod\ n)$ e $u(s-1) \equiv 0 (mod\ n)$.
Reciprocamente, se $s^m \equiv 1 (mod\ n)$ e $u(s-1) \equiv 0 (mod\ n)$, então existe um grupo G de ordem nm que possui dois elementos a, b satisfazendo as condições (3.1.2).

(ii) Quando existir um grupo de ordem nm satisfazendo as condições (3.1.2) ele é único a menos de isomorfismos.

Demonstração:

(i) Seja G um grupo de ordem mn que possui elementos a, b que satisfazem a hipótese. Então, será provado que $s^m \equiv 1 (mod\ n)$ e $u(s-1) \equiv 0 (mod\ n)$.

Pelo Teorema 3.1.4, tem-se que $b^m a = a^{s^m} b^m$ e como por hipótese $b^m \in \langle a \rangle$, então existe $u \in \mathbb{N}$ com $0 \leq u \leq n-1$, tal que $b^m = a^u$, assim

$$b^m a = a^u a = a^{u+1} = aa^u = ab^m$$

logo,

$$ab^m = a^{s^m} b^m.$$

Operando em ambos os lados a^{-1} obtém-se $b^m = a^{s^m - 1} b^m$ e ainda operando b^{-m} segue que $e = a^{s^m - 1}$.

Logo pela Proposição 2.5.16, $s^m - 1$ é um múltiplo da ordem de a, assim $s^m \equiv 1 (mod\ n)$.

Novamente pelo Teorema 3.1.4 tem-se que $ba^u = a^{us} b$ e como por hipótese $a^u = b^m \in \langle b \rangle$ segue que

$$a^u b = b^m b = bb^m = ba^u$$

e assim $a^u b = a^{us} b$. Operando em ambos os lados a^{-u} à esquerda e b^{-1} à direita, obtém-se que $e = a^{u(s-1)}$. Logo, pela Proposição 2.5.16 $u(s-1)$ é um múltiplo da ordem de a, donde $u(s-1) \equiv 0 (mod\ n)$.

A recíproca não será provada, pois este resultado envolveria produto semidireto de grupos que não foram estudados por falta de tempo, além desse resultado não ser necessário para a classificação dos grupos de ordem menor que 12.

(ii) Seja J um grupo de ordem mn que possui as mesmas características de G, ou seja, existem α, β tais que

$$J = \langle \alpha, \beta \rangle,\ \alpha^n = e,\ \beta^m = \alpha^u,\ \beta\alpha = \alpha^s \beta.$$

Como G e J têm ordem mn, então existe uma bijeção $f : G \longrightarrow J$ definida por $f(a^i b^j) = \alpha^i \beta^j$, com $0 \leq i \leq n-1$ e $0 \leq j \leq m-1$ e pelo Teorema 3.1.4 f é um isomorfismo. Portanto, $G \simeq J$ o que garante a unicidade a menos de isomorfismos.

■

3.2 GRUPOS DE ORDEM 4

Tem-se que $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})$, com a adição, são grupos de ordem 4. Eles não são isomorfos, pois pelo Exemplo 2.5.17, se existisse um isomorfismo $f : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$, então $o(f(x)) | o(x)$ em particular $o(f(\overline{1})) | o(\overline{1})$, mas $o(\overline{1}) = 4$ e a ordem dos elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$ é 1 ou 2, logo teria-se um absurdo.

Seja G um grupo de ordem 4 com elemento neutro e. Se G possui um elemento de ordem 4, então G é cíclico, e pelo Teorema 2.5.19 é isomorfo a $\mathbb{Z}_4$.

Se G não possui elemento de ordem 4, então pelo Teorema de Lagrange, todos os elementos, exceto e tem ordem 2, logo pelo Exemplo 2.6.11 G é um grupo abeliano.

Escrevendo $G = \{e, a, b, c\}$, pode-se encontrar a tabela de multiplicação desse grupo. Pois:

* Apenas o neutro tem ordem 1, pois se $o(a) = 1$, então $a = e$. Absurdo!

* $ab \neq a$, pois caso contrário, tem-se que $b = e$. Absurdo!

* $ab \neq b$, pois caso contrário, tem-se que $a = e$. Absurdo!

* $ab \neq e$, pois caso contrário, $a = b'$ o que é um absurdo visto que sendo b um elemento de ordem 2, então $b = b'$.

Portanto, $ab = c$ e $ba = c$, pois G é abeliano. Assim tem-se que

$$ac = b = ca \quad \text{e} \quad bc = a = cb,$$

e pelas tabelas a seguir pode-se ver que $\mathbb{Z}_2 \times \mathbb{Z}_2$ é isomorfo ao G, considerando a aplicação

$$\begin{aligned} (0,0) &\longrightarrow e \\ (1,0) &\longrightarrow a \\ (0,1) &\longrightarrow b \\ (1,1) &\longrightarrow c \end{aligned}$$

Tabela 3.1: Tábua do Grupo G

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Fonte: Produção do próprio autor

Assim, a menos de isomorfismos $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ são os únicos grupos de ordem 4.

3.3 GRUPOS DE ORDEM 6

Tem-se que $(\mathbb{Z}_6, +)$ e S_3 são grupos de ordem 6. Eles não são isomorfos, pois $\mathbb{Z}_6$ é abeliano enquanto S_3 não é.

Tabela 3.2: Tábua do Grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$

	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$

Fonte: Produção do próprio autor

Nesta seção será provado, que a menos de isomorfismos, $\mathbb{Z}_6$ e S_3, são os únicos grupos de ordem 6.

Seja G um grupo qualquer de ordem 6 com neutro e.

(i) Sabe-se que o grupo G possui um elemento α de ordem 3, pois:

- Se G é cíclico gerado por um elemento γ, então $\alpha = \gamma^2$ é tal que $o(\alpha) = 3$, pois $\alpha^3 = \gamma^6 = e$ e ainda $\alpha = \gamma^2 \neq e$, $\alpha^2 = \gamma^4 \neq e$, pois $\langle\gamma\rangle = G$ e assim $o(\gamma) = 6$.
- Se G não é cíclico, então por absurdo supõe-se que não exista um elemento em G que tenha ordem 3. Neste caso, pelo Teorema de Lagrange, todo elemento diferente de e tem ordem 2. Assim G é abeliano e, tomando dois elementos $a, b \in G$, tem-se que $H = \{e, a, b, ab\}$ é subgrupo de G com ordem 4, o que é um absurdo, pois $|H|$ não divide 6 e contradiz o Teorema de Lagrange.

(ii) O grupo G possui pelo menos um elemento β de ordem 2 e $G = \langle\alpha, \beta\rangle$, pois:

- Se G é cíclico gerado por um elemento γ, então $\beta = \gamma^3$, é tal que $o(\beta) = 2$, pois $\beta = \gamma^3 \neq e$, $\beta^2 = \gamma^6 = e$. Tem-se que $\gamma^3 \notin \langle\gamma^2\rangle = \{e, \gamma^2, \gamma^4\}$, assim $o(\langle\gamma^2, \gamma^3\rangle) > 3$, mas pelo Teorema de Lagrange $o(\langle\gamma^2, \gamma^3\rangle)$ divide 6, então $o(\langle\gamma^2, \gamma^3\rangle) = 6$, portanto $G = \langle\gamma^2, \gamma^3\rangle = \langle\alpha, \beta\rangle$.
- Se G não é cíclico, seja α um elemento de G tal que $o(\alpha) = 3$ (que existe por (i)). Então tomando $\beta \notin \langle\alpha\rangle = \{e, \alpha, \alpha^2\}$ os elementos: $e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta$ são distintos, pois:
  - $\alpha\beta = e \Rightarrow \beta = \alpha^{-1}$. Absurdo, pois $o(\beta) = 2$ logo, $\beta^{-1} = \beta$.
  - $\alpha\beta = \alpha \Rightarrow \beta = e$. Absurdo, pois desse modo $\beta \in \langle a\rangle$.
  - $\alpha\beta = \alpha^2 \Rightarrow \beta = \alpha$. Absurdo!
  - $\alpha\beta = \beta \Rightarrow \alpha = e$. Absurdo!
  - $\alpha\beta = \alpha^2\beta \Rightarrow \alpha = e$. Absurdo!
  - $\alpha^2\beta = e \Rightarrow \alpha\beta = \alpha^{-1} = \alpha^2 \Rightarrow \beta = \alpha$. Absurdo!
  - $\alpha^2\beta = \alpha \Rightarrow \alpha\beta = e$. Absurdo!
  - $\alpha^2\beta = \alpha^2 \Rightarrow \beta = e$. Absurdo!

* $\alpha^2\beta = \beta \Rightarrow \alpha^2 = e$. Absurdo!

logo

$$G = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\} \text{ e } G = \langle \alpha, \beta \rangle$$

Obtém-se então que

$$\begin{cases} |G| &= 6 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^3 &= e \\ \beta^2 &= e \end{cases}.$$

Entretanto ainda não foi explicitado o produto $\beta\alpha$. Tem-se que $\beta\alpha \notin \{e, \alpha, \alpha^2, \beta\}$, pois:

* $\beta\alpha = e \Rightarrow \beta = \alpha^{-1} = \alpha^2$. Absurdo!

* $\beta\alpha = \alpha \Rightarrow \beta = e$. Absurdo!

* $\beta\alpha = \alpha^2 \Rightarrow \beta = \alpha$. Absurdo!

* $\beta\alpha = \beta \Rightarrow \alpha = e$. Absurdo!

logo, $\beta\alpha = \alpha\beta$ ou $\beta\alpha = \alpha^2\beta$. Assim surgem duas possibilidades:

$$\begin{cases} |G| &= 6 = 3.2 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^3 &= e \\ \beta^2 &= e \\ \beta\alpha &= \alpha\beta \end{cases} \quad \text{ou} \quad \begin{cases} |G| &= 6 = 3.2 \\ G &= \langle \alpha, \beta \rangle \\ \alpha^3 &= e \\ \beta^2 &= e \\ \beta\alpha &= \alpha^2\beta \end{cases}.$$

Portanto, pelo item (ii) do Teorema 3.1.6 temos, a menos de isomorfismos, apenas um grupo em cada caso. No primeiro caso $G \simeq \mathbb{Z}_6$, pois é abeliano e o isomorfismo é definido por $\alpha \leftrightarrow \overline{2}$ e $\beta \leftrightarrow \overline{3}$. No segundo caso $G \simeq S_3$, como pode ser observado pela Tabela 2.1, S_3 satisfaz estas condições com o isomorfismo definido por $\alpha \leftrightarrow f_1$ e $\beta \leftrightarrow g_1$.

3.4 GRUPOS DE ORDEM 8

Tem-se que $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, com a soma, e D_4 são grupos de ordem 8, que não são isomorfos, pois D_4 não é abeliano, $\mathbb{Z}_8 = \langle 1 \rangle$ tem elemento de ordem 8, enquanto os outros não tem, e por fim,

$\mathbb{Z}_4 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1), (3,0), (3,1)\}$ é tal que

$$o(0,0) = 1 \ ; \ o(0,1) = 2$$

$$o(1,0) = 4 \ ; \ o(1,1) = 4$$

$$o(2,0) = 2 \ ; \ o(2,1) = 2$$

$$o(3,0) = 4 \ ; \ o(3,1) = 4$$

ou seja, $\mathbb{Z}_4 \times \mathbb{Z}_2$ possui elementos com ordem 4, enquanto

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$ possui apenas elementos com ordem 1 ou 2, pois

$$o(0,0,0) = 1 \text{ e } o(a,b,c) = 2 \ \forall \ a,b,c \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus (0,0,0).$$

Será provado nesta seção que, a menos de isomorfismos, existe apenas mais um grupo de ordem 8, chamado grupo dos quatérnios e denotado por Q_3. Os elementos de Q_3 são:

$$\begin{aligned} Q_3 \ = \ & \left\{ e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, AB = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \right. \\ & \left. A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, A^3 = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, A^2B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, A^3B = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\}. \end{aligned}$$

Com $i \in \mathbb{C}$ e $i^2 = -1$. Q_3 é um grupo com a operação multiplicação de matrizes, e tomando A, B como acima, é fácil verificar que

$$\begin{cases} |Q_3| &= 8 \\ Q_3 &= \langle A, B \rangle \\ A^4 &= id \\ B^2 &= A^2 \\ BA &= A^3B \end{cases}.$$

Assim a tábua do Q_3 é:

Tabela 3.3: Tábua do Grupo Q_3

.	e	A	A^2	A^3	B	AB	A^2B	A^3B
e	e	A	A^2	A^3	B	AB	A^2B	A^3B
A	A	A^2	A^3	e	AB	A^2B	A^3B	B
A^2	A^2	A^3	e	A	A^2B	A^3B	B	AB
A^3	A^3	e	A	A^2	A^3B	B	AB	A^2B
B	B	A^3B	A^2B	AB	A^2	A	e	A^3
AB	AB	B	A^3B	A^2B	A^3	A^2	A	e
A^2B	A^2B	AB	B	A^3B	e	A^3	A^2	A
A^3B	A^3B	A^2B	AB	B	A	e	A^3	A^2

Fonte: Produção do próprio autor

Pelo item (ii) do Teorema 3.1.6, tem-se que Q_3 é caracterizado unicamente pelas

relações acima. Q_3 não é isomorfo a $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, pois não é comutativo. Então, basta verificar que D_4 e Q_3 não são isomorfos. Os elementos de D_4 têm as seguintes ordens:

$$o(e) = 1,\ o(a) = 4$$

$$o(a^2) = 2,\ o(a^3) = 4$$

$$o(b) = 2,\ o(ab) = 2$$

$$o(a^2b) = 2,\ o(a^3b) = 2$$

enquanto Q_3 tem apenas um elemento de ordem 2, pois:

$$o(e) = 1,\ o(A) = 4$$

$$o(A^2) = 2,\ o(A^3) = 4$$

$$o(B) = 4,\ o(AB) = 4$$

$$o(A^2B) = 4,\ o(A^3B) = 4$$

Portanto, D_4 e Q_3 não são isomorfos, o que também pode ser verificado pelas Tabelas 2.3 e 3.3.

Agora basta provar que todos os outros grupos de ordem 8, são isomorfos aos grupos citados acima.

Seja G um grupo qualquer de ordem 8, com neutro e. Pelo Teorema de Lagrange, as possíveis ordens dos elementos, diferentes de e, são $2, 4$ e 8.

(i) Se G possui um elemento de ordem 8:
Seja γ um elemento de ordem 8, então $G = \langle\gamma\rangle$ e pelo Teorema 2.5.19 $G \simeq \mathbb{Z}_8$.

(ii) Se G não possui nenhum elemento de ordem 8, então pelo Teorema de Lagrange, as possíveis ordens dos, elementos exceto o neutro, são 2 e 4.

(a) Supondo que G não possui nenhum elemento de ordem 4 então todos seus elementos tem ordem 2, e assim G é abeliano. Além disso,

- Se $a \neq e$, então $H = \{e, a\}$ é subgrupo de G;
- Se $b \in G - H$, então $K = \{e, a, b, ab\}$ é subgrupo de G;
- Se $c \in G - K$, então $J = \{e, a, c, ac\}$ e $L = \{e, b, c, bc\}$ são subgrupos de G. E ainda $ac \neq ab, ac \neq bc, ab \neq bc$ pois caso contrário, $b = c$ ou $a = b$ ou $a = c$ o que é um absurdo.

Note que $abc \notin \{e, a, b, c, ab, ac, bc\}$, pois $o(c) = o(b) = o(a) = 2$ e:

* $abc = e \Rightarrow ab = c^{-1} \Rightarrow ab = c$. Absurdo!

* $abc = a \Rightarrow bc = e \Rightarrow b = c^{-1} = c$. Absurdo!

* $abc = b \Rightarrow ac = e \Rightarrow a = c^{-1} = c$. Absurdo!
* $abc = c \Rightarrow ab = e \Rightarrow a = b^{-1} = b$. Absurdo!
* $abc = ab \Rightarrow c = e$. Absurdo!
* $abc = ac \Rightarrow b = e$. Absurdo!
* $abc = bc \Rightarrow a = e$. Absurdo!

Assim

$$G = \{e, a, b, c, ab, ac, abc, bc\} = \{a^i b^j c^k / \ i, j, k \in \{0, 1\}\}.$$

Neste caso é fácil ver que G é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, pois

$$f : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow G$$

definida por

$$f(\overline{i}, \overline{j}, \overline{k}) = a^i b^j c^k$$

é um isomorfismo.

(b) Supondo que G possui um elemento de ordem 4, seja $a \in G$ tal que $o(a) = 4$, assim $H = \langle a \rangle$ é um subgrupo de G. Tomando $b \in G$ tal que $b \notin H$, então o subgrupo $K = \langle a, b \rangle$ tem ordem maior que 4, pois $H \subsetneq K$ e pelo Teorema de Lagrange $|K|$ divide 8, logo

$$K = G = \langle a, b \rangle = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

E ainda, tem-se que $b^2 \in H$, pois $b^2 \notin \{b, ab, a^2b, a^3b\}$. De fato

* $b^2 = b \Rightarrow b = e$. Absurdo!
* $b^2 = ab \Rightarrow b = a$. Absurdo!
* $b^2 = a^2b \Rightarrow b = a^2$. Absurdo!
* $b^2 = a^3b \Rightarrow b = a^3$. Absurdo!

Além disso, $ba \notin \{e, a, a^2, a^3, b\}$, pois caso contrário

* $ba = e \Rightarrow b = a^{-1}$. Absurdo!
* $ba = a \Rightarrow b = e$. Absurdo!
* $ba = a^2 \Rightarrow b = a$. Absurdo!
* $ba = a^3 \Rightarrow b = a^2$. Absurdo!

Assim as propriedades encontradas foram

$$\begin{cases} |G| = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = a^u, \quad \text{para algum } u \in \{0,1,2,3\} \\ ba = a^s b, \quad \text{para algum } s \in \{1,2,3\} \end{cases}.$$

Analisando as possibilidades para u e s, tem-se que $o(bab^{-1}) = o(a) = 4$, pois

$$\begin{aligned} (bab^{-1})^n &= (bab^{-1})(bab^{-1})(bab^{-1})\dots(bab^{-1}) \\ &= ba(b^{-1}b)a(b^{-1}b)a(b^{-1}b)\dots(b^{-1}b)ab^{-1} \\ &= ba^n b^{-1}. \end{aligned}$$

Assim se $s = 2$, então $bab^{-1} = a^2$ donde $(bab^{-1})^2 = a^4 = e$ o que é um absurdo. Logo $s = 1$ ou $s = 3$. Tem-se também que $b^2 \notin \{a, a^3\}$, pois G não possui elementos de ordem 8. Logo $u = 0$ ou $u = 2$.

Se $u = 0$ tem-se dois casos para $s = 1$ e $s = 3$

$$\begin{cases} |G| = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = e \\ ba = ab \end{cases} \quad \text{e} \quad \begin{cases} |G| = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = e \\ ba = a^3 b \end{cases}.$$

Pelo item (ii) do Teorema 3.1.6 cada caso tem no máximo um grupo que satisfaz as condições, a menos de isomorfismos, no primeiro caso $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$, pois G é abeliano e o isomorfismo é definido por $a \leftrightarrow (1,0)$ e $b \leftrightarrow (0,1)$. No segundo caso, $G \simeq D_4$, como pode-se observar na Tabela 2.3, D_4 satisfaz estas condições.

Se $u = 2$, tem-se dois casos, para $s = 1$ e $s = 3$

$$\begin{cases} o(G) = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = a^2 \\ ba = ab \end{cases} \quad \text{e} \quad \begin{cases} o(G) = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = a^2 \\ ba = a^3 b \end{cases}.$$

Pelo item (ii) do Teorema 3.1.6 cada caso tem no máximo um grupo que satisfaz as condições, a menos de isomorfismos, no primeiro caso $G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ pois G é abeliano e o isomorfismo é definido por $a \leftrightarrow (1,1)$ e $b \leftrightarrow (1,0)$. No segundo caso $G \simeq Q_3$, como pode-se observar na Tabela 3.3 e o isomorfismo é definido por $a \leftrightarrow A$ e $b \leftrightarrow B$.

Portanto, a menos de isomorfismos, existem apenas cinco grupos de ordem 8.

3.5 GRUPOS DE ORDEM 9

Tem-se que $\mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$ são grupos de ordem 9. Eles não são isomorfos pois, $\mathbb{Z}_9$ tem elemento de ordem 9 e $\mathbb{Z}_3 \times \mathbb{Z}_3$ não.

Nesta seção será provado que a menos de isomorfismos $\mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$ são os únicos grupos de ordem 9.

Seja G um grupo não cíclico de ordem 9, com neutro e. Pelo Teorema de Lagrange, como G não é cíclico, todos os seus elementos, exceto e, tem ordem 3, pois caso contrário teriam ordem 1 o que é um absurdo. Neste caso, pode-se escolher $a \neq e$ tal que $a \in G$ e $b \in G$ tal que $b \in G - \langle a \rangle$. Assim

$$G = \langle a, b \rangle = \{e, a, a^2, b, ab, a^2b, b^2, ab^2, a^2b^2\}$$

em que todos os elementos são distintos, por raciocínio análogo ao da seção anterior. Portanto,

$$\begin{cases} o(G) &= 9 \\ G &= \langle a, b \rangle \\ a^3 &= e \\ b^3 &= e \end{cases}.$$

É claro que $ba \notin \{e, a, a^2, b, b^2\}$ pois:

* $ba = e \Longrightarrow b = a^{-1}$. Absurdo!
* $ba = a \Longrightarrow b = e$. Absurdo!
* $ba = a^2 \Longrightarrow b = a$. Absurdo!
* $ba = b \Longrightarrow a = e$. Absurdo!
* $ba = b^2 \Longrightarrow a = b$. Absurdo!

Falta analisar $ba = ab$, $ba = a^2b$, $ba = ab^2$ e $ba = a^2b^2$. Pelo Teorema 3.1.6 em cada caso existe no máximo um grupo que satisfaz as propriedades. Agora basta verificar se existem tais grupos,

(i) Caso $ba = ab$, então $G \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$. Com o isomorfismo definido por $a \leftrightarrow (1, 0)$ e $b \leftrightarrow (0, 1)$.

(ii) Caso $ba = a^2b$, com $s = 2, n = 3, m = 3$, pelo item (i) do Teorema 3.1.6, este grupo não existe, pois $2^3 = 8 \not\equiv 1 (mod\ 3)$.

(iii) Caso $ba = ab^2$, não pode existir, pois tomando $\alpha = b^2$ e $\beta = a$, tem-se

$$\beta\alpha = ab^2 = ba = b^3ba = b^4a = \alpha^2\beta,$$

ou seja $\beta\alpha = \alpha^2\beta$, o que é um absurdo, pois pelo item (i) do Teorema 3.1.6 $2^3 = 8 \not\equiv 1(mod\ 3)$.

(iv) Caso $ba = a^2b^2$. Este grupo também não existe, pois então

$$(ab)^2 = a(ba)b = aa^2b^2b = a^3b^3 = e$$

o que é um absurdo, sendo que ab tem ordem 3.

Assim os únicos grupos de ordem 9 a menos de isomorfismos são $\mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$.

3.6 GRUPOS DE ORDEM 10

Seja G um grupo qualquer de ordem 10, com neutro e. Pelo Teorema de Lagrange, os elementos de G, exceto e, podem ter ordem 2, 5 e 10.

Se G possui um elemento de ordem 10, então G é cíclico e é isomorfo a $(\mathbb{Z}_{10}, \oplus)$.

Além disso pode-se enunciar duas importantes afirmações:

(i) G possui um elemento de ordem 5.
De fato, se $\alpha \in G$ é um elemento de ordem 10, então $o(\alpha^2) = 5$, ou seja, $\alpha^2 \in G$ é um elemento de ordem 5. No caso em que G não possui um elemento de ordem 10, suponha que ele também não possui elemento de ordem 5, então todos os seus elementos, exceto e, tem ordem 2 e G é abeliano. Sejam $a, b \in G - \{e\}$ tais que $b \in G - \langle a\rangle$ (existe tal elemento b, pois $|G| = 10$ e $|\langle a\rangle| = 2$). Logo

$$H = \langle a, b\rangle = \{e, a, b, ab\}$$

é um subgrupo de G, gerado por a e b, que possui ordem 4 o que contradiz o Teorema de Lagrange. Logo G possui um elemento de ordem 5.

(ii) G possui um elemento de ordem 2.
De fato, se G é cíclico gerado por α, então $o(\alpha^5) = 2$, ou seja, α^5 é um elemento de ordem 2. Se G não é cíclico, pela parte (i) G possui um elemento a de ordem 5. Seja $b \in G - \langle a\rangle$. Então $o(b) = 2$, pois caso contrário $o(b) = 5$ e o subgrupo $\langle b\rangle \cap \langle a\rangle$ tem ordem igual a 1, pois $\langle b\rangle \cap \langle a\rangle \subsetneq \langle a\rangle$ e $|\langle a\rangle| = 5$. Assim

$$e, a, a^2, a^3, a^4, b, b^2, b^3 \text{ e } b^4$$

são os elementos distintos de G e ainda ab e a^2b pertencem a G e são distintos destes, pois

* $ab = a^i \Rightarrow\ b = a^{i-1},\ 0 \leqslant i \leqslant 4$. Absurdo!
* $ab = b^i \Rightarrow\ a = b^{i-1},\ 0 \leqslant i \leqslant 4$. Absurdo!
* $a^2b = a^i \Rightarrow\ b = a^{i-2},\ 0 \leqslant i \leqslant 4$. Absurdo!
* $a^2b = b^i \Rightarrow\ a^2 = b^{i-1},\ 0 \leqslant i \leqslant 4$. Absurdo!

Desta forma G teria pelo menos 11 elementos distintos, o que é um absurdo. Logo, a ordem de b é 2 e consequentemente

$$G = \langle a, b\rangle = \{e, a, a^2, a^3, a^4, b, ab, a^2b, a^3b, a^4b\}.$$

Além disso, $ba \notin \{e, a, a^2, a^3, a^4, b\}$, pois $b \in G - \langle a\rangle$ e ainda

(a) $ba \neq a^2b$, pois pelo Teorema 3.1.6 item (i), com $s = 2, m = 2, u = 5$ e $n = 5$ tem-se que $2^2 = 4 \not\equiv 1(mod\ 5)$.

(b) $ba \neq a^3b$, pois com $s = 3, m = 2, u = 5$ e $n = 5$ tem-se que $3^2 = 9 \not\equiv 1(mod\ 5)$.

Logo, restam duas possibilidades:

$$\begin{cases} |G| &= 10 = 5.2 \\ G &= \langle a, b\rangle \\ a^5 &= e \\ b^2 &= e \\ ba &= ab \end{cases} \quad \text{e} \quad \begin{cases} |G| &= 10 = 5.2 \\ G &= \langle a, b\rangle \\ a^5 &= e \\ b^2 &= e \\ ba &= a^4b \end{cases}.$$

Pelo item (ii) do Teorema 3.1.6 existe no máximo um grupo que satisfaz essas condições. No primeiro caso $G \simeq \mathbb{Z}_{10}$ com isomorfismo definido por $a \leftrightarrow \overline{2}$ e $b \leftrightarrow \overline{5}$. No segundo caso $G \simeq D_5$ (grupo das simetrias espaciais no pentágono regular), como pode ser observado no Exemplo 2.2.16 D_5 satisfaz estas condições.

3.7 GRUPOS DE ORDEM 2P COM P $>$ 2 PRIMO

Seja G um grupo, com neutro e, cuja ordem é $2p$ com $p > 2$ um número primo. Sabe-se que existem pelo menos dois grupos com ordem $2p$ para $p > 2$, a saber o grupo das classes de restos $(\mathbb{Z}_{2p}, \oplus)$ e o grupo diedral D_p, sendo que D_p satisfaz as condições do Exemplo 2.2.16.

Se p for um número primo, então estes são os únicos grupos de ordem $2p$, a menos de isomorfismos.

De fato, sendo p primo, pelo teorema de Lagrange, os elementos de G, exceto e, tem ordem 2, p e $2p$. Se G tiver um elemento de ordem $2p$, então G é cíclico, logo isomorfo a $\mathbb{Z}_{2p}$. Se G não for cíclico, então G possui um elemento de ordem p, pois caso contrário todos os seus elementos teriam ordem 2 e para $a, b \in G - \{e\}$ tal que $b \in G - \langle a \rangle$ o subgrupo de G gerado por a e b teria ordem 4 o que é um absurdo, pois $4 \nmid (2p)$. Além disso, se $a \in G$ tem ordem p e $b \in G$ é tal que

$$b \in G - \langle a \rangle,$$

então $o(b) = 2$, pois se $o(b) \neq 2$, então $o(b) = p$ e

$$e, a, a^2, \ldots, a^{p-1}, b, b^2, \ldots, b^{p-1}$$

são $2p - 1$ elementos distintos de G e pode-se notar que ab e a^2b são elementos de G que diferem destes (análise análoga a feita para grupos de ordem 10) donde G teria pelo menos $2p + 1$ elementos, o que é um absurdo.

Assim, se G é um grupo de ordem $2p$ com $p > 2$ um número primo, então existem em G um elemento a de ordem p, e um elemento b de ordem 2. Portanto,

$$G = \{e, a, a^2, \ldots, a^{p-1}, b, ab, a^2b, \ldots, a^{p-1}b\}.$$

Além disso, $ba \notin \{e, a, a^2, \ldots, a^{p-1}, b\}$, pois $b \in G - \langle a \rangle$, e ainda $ba = ab$ ou $ba = a^{p-1}b$, pois nos demais casos teria-se uma contradição do item (i) do Teorema 3.1.6. De fato, para $2 \leq i \leq p - 2$, $(p - i)^2 \not\equiv 1 (mod\ p)$ com $s = p - i, m = 2, u = p$ e $n = p$. Assim tem-se duas possibilidades:

$$\begin{cases} |G| = 2p \\ G = \langle a, b \rangle \\ a^p = e \\ b^2 = e \\ ba = ab \end{cases} \quad \text{e} \quad \begin{cases} |G| = 2p \\ G = \langle a, b \rangle \\ a^p = e \\ b^2 = e \\ ba = a^{p-1}b \end{cases}.$$

Pelo item (ii) do Teorema 3.1.6 existe um único grupo que satisfaz cada uma destas possibilidades. No primeiro caso, o grupo é abeliano, logo $G \simeq \mathbb{Z}_{2p}$ com o isomorfismo definido por $a \longleftrightarrow \overline{2}$ e $b \longleftrightarrow \overline{p}$ (pode-se provar que $o(ab) = 2p$, logo G é cíclico). No

segundo caso $G \simeq D_p$, pois pode-se notar que D_n satisfaz

$$\begin{cases} |D_n| &= 2n \\ D_n &= \langle a, b \rangle \\ a^n &= e \\ b^2 &= e \\ ba &= a^{n-1}b \end{cases} .$$

Assim se p é um número primo ímpar, então $\mathbb{Z}_{2p}$ e D_p são os únicos grupos de ordem $2p$ exceto isomorfismos.

Com este resultado tem-se uma recíproca para o Teorema de Lagrange para a classe de grupos de ordem $2p$ com $p > 2$ primo, ou seja, se $n \mid |G|$ e $n < |G|$ então existe um subgrupo H de G tal que $|H| = n$.

No próximo capítulo serão apresentados outros resultados nesta linha.

Capítulo 4

RECÍPROCAS DO TEOREMA DE LAGRANGE

Pelo Teorema de Lagrange tem-se que a ordem de qualquer subgrupo H de G sempre divide a ordem de G.

Neste capítulo busca-se apresentar algumas recíprocas deste resultado, ou seja, se $m \mid |G|$ existe $K < G$ tal que $|K| = m$? Os Teoremas de Cauchy e de Sylow apresentam resultados nesta linha.

4.1 GRUPOS QUOCIENTES

Teorema 4.1.1 *Seja H um subgrupo normal do grupo G e considere o conjunto das classes laterais à esquerda, módulo H, denotado por G/H e definido por*

$$G/H = \{aH/\ a \in G\}.$$

Nesse conjunto considere a relação induzida de G, dada por

$$(aH) \odot (bH) = (ab)H, \qquad \textit{para todo} \quad a, b \in G.$$

Então, $(G/H, \odot)$ é um grupo chamado **grupo quociente** *de G por H.*

Demonstração: Seja $x \in (aH) \odot (bH)$. Então, existem $h_1, h_2 \in H$ tais que $x = (ah_1)(bh_2)$. Como $H \triangleleft G$, existe $h_3 \in H$ de modo que,

$$x = a(h_1 b)h_2 = a(bh_3)h_2 = (ab)(h_3 h_2) \in (ab)H.$$

Por outro lado, dado $y \in (ab)H$ existe $h \in H$ tal que $y = (ab)h$. Como $H \triangleleft G$ o

elemento neutro de G, pertence a H, logo

$$y = (ab)h = (ae)(bh) \in (aH) \odot (bH).$$

Portanto, $\odot$ está bem definida. Além disso,

$$\begin{aligned}[(aH) \odot (bH)] \odot (cH) &= (ab)H \odot (cH) = (ab)cH = a(bc)H \\ &= aH \odot ((bc)H) = (aH) \odot [(bH) \odot (cH)],\end{aligned}$$

o elemento neutro é o próprio H e $a^{-1}H$ é o simétrico de aH, para todo $aH \in G/H$. ■

Exemplo 4.1.2 *Seja $H \triangleleft G$. Então $\varphi : G \to G/H$, dada por $\varphi(g) = gH$ é um epimorfismo chamado projeção canônica.*

De fato, tem-se que

- $f(a.b) = (ab)H = (aH) \odot (bH) = f(a) \odot f(b)$.
- $a = b \Longrightarrow a^{-1}b = e \in H \Longrightarrow aH = bH \Longrightarrow f(a) = f(b)$.
- $gH \in G/H \Longrightarrow g \in G$ *e* $f(g) = gH$.

Proposição 4.1.3 *Seja G um grupo qualquer. Então, o subconjunto*

$$Z(G) = \{x \in G/\ xg = gx, \forall g \in G\} \tag{4.1.1}$$

é subgrupo normal de G. Este subgrupo $Z(G)$ é chamado de centro de G, e ainda G é abeliano se, e somente se $Z(G) = G$.

Demonstração: De fato, dados $y, z \in Z(G)$. Então, $yg = gy$ e $zg = gz$ para todo $g \in G$. Assim,

$$g(yz^{-1}) = (gy)z^{-1} = (yg)z^{-1} = y(gz^{-1}) = y(zg^{-1})^{-1} = y(g^{-1}z)^{-1} = y(z^{-1}g) = (yz^{-1})g.$$

logo, $yz^{-1} \in Z(G)$, e pela Proposição 2.3.5, $Z(G)$ é subgrupo de G.

E ainda dado $g \in G$ tem-se

$$gZ(G) = \{gx/\ x \in Z(G)\} = \{xg/\ x \in Z(G)\} = Z(G)g,$$

ou seja, $Z(G) \triangleleft G$.

Além disso, se G for comutativo, então para quaisquer $x, y \in G$ tem-se $xy = yx$, ou seja, $x, y \in Z(G)$, donde $Z(G) = G$. ■

Proposição 4.1.4 *Seja G um grupo e seja $Z(G)$ seu centro. Se $G/Z(G)$ é cíclico, então $Z(G) = G$. Em particular, o índice de $Z(G)$ em G nunca é igual a um número primo.*

Demonstração: Se $G/Z(G)$ é cíclico, então existe $a \in G$ tal que

$$G/Z(G) = \langle aZ(G)\rangle = \langle \overline{a}\rangle.$$

Assim, dado $x \in G$, existe $n \in \mathbb{Z}$ tal que $\overline{x} = \overline{a}^{\,n}$ ou seja,

$$xZ(G) = (aZ(G))^n = a^n Z(G).$$

Logo, pela Proposição 2.6.3, $x^{-1}a^n \in Z(G)$, ou seja, existe $y \in Z(G)$ tal que

$$x^{-1}a^n = y, \quad \text{ou ainda,} \quad x = a^n y^{-1}.$$

Assim, para $x, u \in G$ existem $m, n \in \mathbb{Z}$ e $y_1, y_2 \in Z(G)$ tais que $x = a^m y_1^{-1}$ e $u = a^n y_2^{-1}$. Donde

$$xu = (a^m y_1^{-1})(a^n y_2^{-1}) = y_2^{-1}(a^m y_1^{-1})a^n = y_2^{-1}a^m(a^n y_1^{-1}) = (y_2^{-1}a^n)(a^m y_1^{-1}) = (a^n y_2^{-1})(a^m y_1^{-1}) = ux.$$

Portanto, G é abeliano e consequentemente $Z(G) = G$.

Se $(G : Z(G))$ é um número primo p, então pelo Corolário 2.6.8 o conjunto quociente $G/Z(G)$ é cíclico, pois $(G : Z(G)) = |G/Z(G)|$ logo, pelo resultado acima $G = Z(G)$ e pelo Teorema de Lagrange

$$|G| = (G : Z(G))|Z(G)|$$

donde

$$(G : Z(G)) = 1$$

o que é um absurdo. ■

Teorema 4.1.5 *Sejam H e K dois subgrupos de um grupo G. Considere o conjunto HK definido por*

$$HK := \{hk/\ h \in H \quad e \quad k \in K\} \tag{4.1.2}$$

Tem-se

(i) $H \cup K \subset HK \subset \langle H \cup K\rangle$;

(ii) $\langle H \cup K\rangle = HK \iff HK$ *é subgrupo de* G.

Demonstração:

(i) Sendo e o elemento neutro de G, tem-se

$$x \in H \cup K \Rightarrow x \in H \text{ ou } x \in K \Rightarrow x * e \in HK \text{ ou } e * x \in HK \Rightarrow x \in HK.$$

Logo $H \cup K \subset HK$ e ainda

$$y = hk \in HK \Rightarrow hk \in \langle H \cup K \rangle := \{x_1^{n_1} x_2^{n_2} \dots x_t^{n_t} / x_i \in H \cup K, n_i \in \mathbb{Z}\} \Rightarrow HK \subset \langle H \cup K \rangle.$$

(ii) ($\Longrightarrow$) Sejam $x = h_1 k_1$ e $y = h_2 k_2$ elementos de HK. Então

$$xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_2 k_2^{-1} h_2^{-1} \in \langle H \cup K \rangle.$$

Como por hipótese $\langle H \cup K \rangle = HK$, segue que $xy^{-1} \in HK$, donde HK é subgrupo de G.
($\Longleftarrow$) Pelo item (i) $HK \subset \langle H \cup K \rangle$, então basta provar que $\langle H \cup K \rangle \subset HK$.
Dado $z \in \langle H \cup K \rangle$, então existem $x_1, x_2, \dots, x_t \in H \cup K$ e $n_1, n_2, \dots, n_t \in \mathbb{Z}$, tais que

$$z = x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}.$$

Como $x_i \in H$ ou $x_i \in K$, então $x_i^{n_i} \in H$ ou $x_i^{n_i} \in K$ e como HK é subgrupo de G por hipótese, segue que $x_i^{n_i} x_j^{n_j} \in HK$ e donde $z \in HK$. Portanto $\langle H \cup K \rangle = HK$.

■

Corolário 4.1.6 *Sejam H, K dois subgrupos de G. Então,*

$$HK \text{ é um subgrupo de } G \Longleftrightarrow HK = KH.$$

Demonstração: Pelo teorema anterior tem-se

$$HK \text{ é subgrupo de } G \iff HK = \langle H \cup K \rangle = \langle K \cup H \rangle = KH.$$

■

Corolário 4.1.7 *Sejam H e K dois subgrupos de G. Se H ou K for normal em G, então HK é um subgrupo de G.*

Demonstração: Sem perda de generalidade se $H \triangleleft G$, então $xH = Hx$ para todo $x \in G$, em particular para $x \in K$, logo $KH = HK$ e pelo corolário anterior HK é um subgrupo de G. ■

Exemplo 4.1.8 *Seja $f : G \to J$ um homomorfismo de grupos. Se H é um subgrupo de G, então $f(H)$ é um subgrupo de J e $f^{-1}(f(H)) = Hker(f)$. Nota-se que a igualdade $f^{-1}(f(H)) = Hker(f)$ implica que $f^{-1}(f(H))$ é um subgrupo de G, pois $ker(f)$ é um subgrupo normal de G.*

De fato,

- $x \in f^{-1}(f(H)) \iff f(x) \in f(H) \iff x \in H \iff x = x \cdot e_G \in Hker(f)$.

- $y \in Hker(f) \quad \Rightarrow \quad y = hx : \ h \in H, x \in ker(f) \quad \Rightarrow \quad f(y) = f(hx) = f(h)f(x) = f(h)e_J = f(h) \quad \Rightarrow \quad f(y) \in f(H) \quad \Rightarrow \quad y \in f^{-1}(f(H))$.

Teorema 4.1.9 *Seja $f : (G, .) \to (J, *)$ um homomorfismo de grupos. Então, A função induzida*

$$\sigma : \frac{G}{ker(f)} \to f(G)$$
$$xker(f) \mapsto f(x)$$

é um isomorfismo. Além disso, $f = \varphi \circ \sigma$, em que φ é a projeção canônica definida no Exemplo 4.1.2.

Demonstração:

(i) σ é uma aplicação, pois para $a, b \in G$, tem-se

$$aker(f) = bker(f) \Rightarrow a = b.k \text{ para algum } k \in ker(f)$$

logo

$$f(a) = f(b.k) = f(b) * f(k) = f(b) * e_J = f(b)$$

(ii) σ é um homomorfismo, pois dados $g, h \in G$, tem-se

$$\sigma(gker(f) \odot hker(f)) = \sigma((g.h)ker(f)) = f(g.h) = f(g) * f(h) = \sigma(gker(f)) * \sigma(hker(f)).$$

(iii) σ é bijetora, pois

$$\begin{aligned} \sigma(gker(f)) = \sigma(hker(f)) &\iff f(g) = f(h) \\ &\iff f(g) * (f(h))^{-1} = e_J \\ &\iff f(g) * f(h^{-1}) = e_J \\ &\iff f(g.h^{-1}) = e_J \\ &\iff g.h^{-1} \in ker(f) \end{aligned}$$

então pela Proposição 2.6.3, $gker(f) = hker(f)$. Assim σ é injetora e como σ é definida sobrejetora, então σ é bijetora.

■

Corolário 4.1.10 *Seja $f : G \to J$ um homomorfismo de grupos e seja H um subgrupo de G. Então, a função*

$$\frac{H}{H \cap ker(f)} \to f(H)$$

$$h(H \cap ker(f)) \mapsto f(h)$$

é um isomorfismo.

Demonstração: Considere o homomorfismo f restrito apenas ao subgrupo H e seja $K = H \cap ker(f)$. Como $K \subset ker(f)$ e $ker(f) \triangleleft G$, então $K \triangleleft G$ e em particular $K \triangleleft H$. Assim, pelo teorema acima a relação $h(H \cap ker(f)) \mapsto f(h)$ é um isomorfismo. ■

Corolário 4.1.11 *Sejam $H \triangleleft G$ e $K < G$. Então,*

$$\frac{K}{H \cap K} \simeq \frac{KH}{H}.$$

Demonstração: Como $H \triangleleft G$, pelos Corolários 4.1.6 e 4.1.7, tem-se que $KH < G$ e $KH = HK$. Além disso,

$$H \triangleleft G \text{ implica } H \triangleleft KH$$

e consequentemente pode-se considerar o grupo quociente KH/H. Seja $\varphi : KH \to KH/H$ o homomorfismo canônico definido no Exemplo 4.1.2 e seja $\varphi|_K$ sua restrição ao subgrupo $K < KH$, isto é,

$$\begin{array}{rccc} \varphi|_K : & K & \to & \dfrac{KH}{H} \\ & k & \mapsto & kH. \end{array}$$

Assim,

$$ker(\varphi|_K) = \{k \in K / \ kH = H\} = H \cap K.$$

Além disso, dado $x \in KH/H$, tem-se que existem $k \in K$ e $h \in H$ tais que $x = (kh)H$. Logo,

$$x = (kh)K = kH = \varphi|_K(k),$$

ou seja, $\varphi|_K$ é sobrejetora. Aplicando o Teorema 4.1.9 para $\varphi|_K$ obtém-se o resultado. ■

Corolário 4.1.12 *Sejam $K < H < G$ com $K \triangleleft G$ e $H \triangleleft G$. Então,*

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

Demonstração: Considere a relação

$$\begin{array}{rccc} \psi : & \dfrac{G}{K} & \to & \dfrac{G}{H} \\ & gK & \mapsto & gH. \end{array}$$

Então,

1. Se $aK = bK$, então, pela Proposição 2.6.3, existe $k \in K$ tal que $b^{-1}a = k$, ou seja, $a = bk$, assim
$$\psi(aK) = aH = bkH = bH = \psi(bK),$$
pois $k \in K \subset H$. Donde ψ está bem definida.

2. ψ é homomorfismo, pois $\psi((ab)K) = (ab)H = (aH) \odot (bH) = \psi(aK)\psi(bK)$, pelo Teorema 4.1.1.

3. Pela definição ψ é sobrejetor e, além disso,
$$ker(\psi) = \{aK/\ \psi(aK) = H\} = \{aK/\ a \in H\} = H/K.$$

Assim, aplicando o Teorema 4.1.9 para ψ segue o resultado. ■

O próximo resultado é conhecido como Teorema de Cauchy para grupos abelianos e ele apresenta uma recíproca parcial para o Teorema de Lagrange e sua demonstração é uma aplicação do grupo quociente.

Teorema 4.1.13 (Teorema de Cauchy para grupos abelianos) *Seja $(G, \cdot)$ um grupo abeliano finito. Se p é um natural primo que divide a ordem de G, então existe $a \in G$, com $a \neq e$, tal que $a^p = e$, ou seja, G possui um subgrupo com ordem p.*

Demonstração: Por indução sobre a ordem de G será mostrado que existe $a \in G$, com $a \neq e$, tal que $a^p = e$.

Se $|G|$ não tem subgrupos diferentes de $\{e\}$ e G, então G é cíclico de ordem prima, o único divisor primo de $|G|$ é $|G|$ e G tem $|G| - 1$ elementos com ordem $|G|$.

Supondo que exista $N < G$, tal que $N \neq \{e\}$ e $N \neq G$, então $1 < |N| < |G|$ (hipótese de indução). Seja p um número primo tal que $p|\ |G|$.

Se p divide $|N|$, como N é abeliano, então pela hipótese de indução existe $a \in N \subset G$, tal que $a \neq e$ e $a^p = e$.

Se p não divide $|N|$, então $p|(G : N)$, pois pelo Teorema de Lagrange $|G| = |N|(G : N)$. Como G é abeliano, então $N \triangleleft G$ e pode-se considerar o grupo quociente G/N.

Como $|G/N| = (G : N) = \frac{|G|}{|N|}$, então $p \mid |G/N|$ e $|G/N| < |G|$. Pela hipótese de indução, existe $Nb \in G/N$ tal que $Nb \neq N$ e $(Nb)^p = N$. Como $Nb \neq N$, então $b \notin N$, mas $N = (Nb)^p = Nb^P$, ou seja $b^p \in N$. Assim $e = (b^p)^{|N|} = b^{p|N|} = (b^{|N|})^p$.

Seja $a = b^{|N|}$, então $a \neq e$, pois caso contrário $b^{|N|} = e$ e $mdc(p, |N|) = 1$ pois p é primo que não divide $|N|$.Assim existem $c, d \in \mathbb{Z}$ tais que $1 = c|N| + dp$, logo

$$Nb = (Nb)^1 = (Nb)^{c|N|+dp} = (Nb)^{c|N|} \odot (Nb)^{dp} = (Nb^{|N|})^c \odot (b^pN)^d = N^cN^d = NN = N$$

o que é um absurdo, pois $Nb \neq e$.

Portanto $a = b|N| \in G$ é o elemento procurado.

■

Exemplo 4.1.14 *Todo grupo abeliano de ordem $2p$ com $p > 2$ um número primo é cíclico.*

De fato, seja $(G, .)$ um grupo abeliano com $|G| = 2p$, com $p > 2$ um número primo. Pelo Teorema 4.1.13 existem $a, b \in G$ tais que $o(a) = 2$ e $o(b) = p$. Note que $o(ab) = 2p$. Pois

$$(ab)^{2p} = a^{2p}b^{2p} = (a^2)^p(b^p)^2 = e^p e^2 = e,$$

sendo e o elemento neutro de G. Por outro lado, seja $n \geq 1$ tal que

$$e = (ab)^n$$

então $a^n = b^{-n} \in \langle a \rangle \cap \langle b \rangle$. Pelo Teorema de Lagrange $|\langle a \rangle \cap \langle b \rangle|$ divide $|\langle a \rangle| = 2$ e divide $|\langle b \rangle| = p$, logo $|\langle a \rangle \cap \langle b \rangle| = 1$ e consequentemente

$$\langle a \rangle \cap \langle b \rangle = \{e\}.$$

Portanto, $a^n = e$ e $b^n = e$. Logo $2|n$ e $p|n$, ou seja, n é múltiplo de $2p$. Desse modo o menos inteiro positivo tal que $(ab)^n = e$ é $2p$, donde $o(ab) = 2p$. Como $\langle ab \rangle \subset G$ e $|\langle ab \rangle| = |G| < \infty$ segue que $G = \langle ab \rangle$, ou seja, G é cíclico. Este fato também foi provado na seção 3.7 onde foi usado o Teorema de Lagrange.

4.2 A EQUAÇÃO DE CLASSE

Definição 4.2.1 *Sejam $(G, \cdot)$ um grupo e $a, b \in G$. Diz-se que b é* **conjugado** *de a se existe $x \in G$ tal que $b = x^{-1}ax$. Escreve-se $a \sim b$ e chama-se $\sim$ de conjugação.*

Proposição 4.2.2 *A conjugação é uma relação de equivalência em $(G, \cdot)$.*

Demonstração: Para mostrar que a conjugação é uma relação de equivalência, basta verificar que satisfaz as propriedades reflexiva, simétrica e transitiva.

- Reflexiva: $a \sim a$.
  De fato, pois $a = e^{-1}ae$.

- Simétrica: $b \sim a \Rightarrow a \sim b$.
  De fato, pois se $b \sim a$, então existe $x \in G$ tal que $b = x^{-1}ax$ logo $a = (x^{-1})^{-1}bx^{-1}$, com $x^{-1} \in G$ pois G é grupo.

- Transitiva: $b \sim a$ e $a \sim c \Rightarrow b \sim c$.
  De fato, pois se $b \sim a$, então existe $x \in G$ tal que $b = x^{-1}ax$, e ainda se $a \sim c$ existe

$y \in G$ tal que $a = y^{-1}cy$. Assim $b = x^{-1}y^{-1}cyx \Rightarrow b = (yx)^{-1}cyx$, com $yx \in G$, pois G é grupo.

■

Definição 4.2.3 *Seja $(G, \cdot)$ um grupo e $\sim$ a conjugação. Para cada $a \in G$ define-se a* **classe de conjugação** *de a por*

$$C(a) = \{b \in G / b \sim a\} = \{x^{-1}ax / x \in G\}.$$

Exemplo 4.2.4 *Em qualquer grupo $(G, \cdot)$, tem-se que $C(e) = \{e\}$.*

Exemplo 4.2.5 *Se $(G, \cdot)$ é um grupo abeliano, então $C(a) = \{a\}$ para todo $a \in G$.*

De fato, $C(a) = \{x^{-1}ax / x \in G\} = \{ax^{-1}x / x \in G\} = \{a\}$.

Proposição 4.2.6 *Seja $(G, \cdot)$ um grupo finito e $\sim$ a conjugação. Se $C_a = \#C(a)$, então*

$$|G| = \sum C_a,$$

onde a soma é feita nas classes distintas.

Demonstração: Como a conjugação é uma relação de equivalência em G, tem-se que pela Proposição 1.1.14 a união das classes é uma partição de G, ou seja:

- $C(a) \cap C(b) \neq \emptyset \Leftrightarrow C(a) = C(b) \Leftrightarrow a \sim b$.
- $G = \cup C(a)$.

Assim, a união é disjunta nas classes disjuntas, logo $|G| = \#C(a) = \sum C_a$. ■

Definição 4.2.7 *Seja $(G, .)$ um grupo e $a \in G$. Chama-se* **normalizador** *de a o conjunto*

$$N(a) = \{x \in G / ax = xa\}.$$

Proposição 4.2.8 *Seja $(G, \cdot)$ um grupo. $N(a)$ é um subgrupo de G, para todo $a \in G$.*

Demonstração: Sejam $x, y \in N(a)$, então $ax = xa$ e $ay = ya$. Basta provar que $xy^{-1} \in N(a)$.

De fato,

$$\begin{aligned} a(xy^{-1}) &= (xx^{-1})(ax)y^{-1} \\ &= (xx^{-1})(xa)y^{-1} \\ &= x(x^{-1}x)ay^{-1} \\ &= xay^{-1} \\ &= x(y^{-1}y)ay^{-1} \\ &= (xy^{-1})ayy^{-1} \\ &= (xy^{-1})a. \end{aligned}$$

Portanto, $N(a)$ é subgrupo de G. ■

Teorema 4.2.9 *Seja $(G, \cdot)$ um grupo finito. Então, para cada $a \in G$,*

$$C_a = \frac{|G|}{|N(a)|} = (G : N(a)).$$

Demonstração: Para provar a igualdade será construída uma bijeção entre o conjunto das classes à direita de $N(a)$ em G, e o conjunto $C(a)$, ou seja $f : G/N(a) \longrightarrow C(a)$, provando que $|G/N(a)| = |C(a)| = C_a$.

Seja $f : \{N(a)x/x \in G\} \longrightarrow \{x^{-1}ax/x \in G\}$ definida por $f(N(a)x) = x^{-1}ax$. Verificando que f é uma função bijetora:

- Boa definição e injetora:

$$\begin{aligned} N(a)x = N(a)y &\Leftrightarrow xy^{-1} \in N(a) \text{ pela Proposição 2.6.3} \\ &\Leftrightarrow (xy^{-1})a = a(xy^{-1}) \\ &\Leftrightarrow y^{-1}ay = x^{-1}ax \\ &\Leftrightarrow f(N(a)y) = f(N(a)x). \end{aligned}$$

- Sobrejetora: A função f é definida sobrejetora.

Assim f é uma bijeção e $C_a = |G/N(a)| = (G : N(a))$. ■

Corolário 4.2.10 (Equação de classe) *Seja $(G, \cdot)$ um grupo finito. Então,*

$$|G| = \sum \frac{|G|}{|N(a)|},$$

onde a soma é feita nas classes de conjugação distintas.

Demonstração: Pela Proposição 4.2.6 $|G| = \sum C_a$ e pelo Teorema 4.2.9 $C_a = \dfrac{|G|}{|N(a)|}$. Logo, $|G| = \sum \dfrac{|G|}{|N(a)|}$. ■

Proposição 4.2.11 *Seja $(G,\cdot)$ um grupo e seja $a \in G$. Então, $a \in Z(G)$ se, e somente se, $N(a) = G$. Se G é um grupo finito, então $a \in Z(G)$ se, e somente se, $|N(a)| = |G|$.*

Demonstração:

$$\begin{aligned} a \in Z(G) &\Leftrightarrow ax = xa, \text{ para todo } x \in G \\ &\Leftrightarrow \text{ para todo } x \in G,\ x \in N(a) \\ &\Leftrightarrow G \subset N(a) \\ &\Leftrightarrow G = N(a) \end{aligned}$$

A segunda afirmação é direta, pois se $G = N(a)$, então $|G| = |N(a)|$. ∎

4.3 TEOREMA DE SYLOW

Nesta seção serão estudados os Teoremas de Sylow que são muito importantes para a classificação de grupos finitos, pois garantem a existência de subgrupos de um grupo finito com ordens especiais (recíproca do Teorema de Lagrange). Para isso serão importantes os subgrupos cuja ordem são da forma p^n, para algum primo p que divide a ordem do grupo, motivando a seguinte definição.

Definição 4.3.1 *Seja p um natural primo. Um grupo finito $(G,\cdot)$ é chamado um* **p-grupo** *se, e somente se, $|G| = p^n$, para algum $n \in \mathbb{N}$.*

Teorema 4.3.2 *Se $(G,\cdot)$ é um grupo tal que $|G| = p^n$, onde p é um natural primo e $n \geq 1$, então $Z(G) \neq \{e\}$.*

Demonstração: Seja $a \in G$. Como $N(a)$ é subgrupo de G, então pelo Teorema de Lagrange $|N(a)|$ divide $|G|$, ou seja, $|N(a)| = p^k$, com $0 \leq k \leq n$. Pela Proposição 4.2.11 $a \in Z(G)$ se, e somente se $|N(a)| = |G|$, ou seja $k = n$ e pela equação de classe de G tem-se que

$$\begin{aligned} |G| &= \sum \frac{|G|}{|N(a)|} \\ p^n &= \sum_{k=n} \frac{|G|}{|N(a)|} + \sum_{k<n} \frac{|G|}{|N(a)|} \end{aligned}$$

Se $k = n$, então $|G| = |N(a)|$ e $a \in Z(G)$. Assim, $\sum \frac{|G|}{|N(a)|} = |Z(G)| = z$. Logo

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

como p divide $\sum \frac{|G|}{|N(a)|}$ e p divide p^n, então p divide z. Logo, $z \geq p$ e $Z(G) \neq \{e\}$. ∎

Corolário 4.3.3 *Se $(G,\cdot)$ é um grupo de ordem p^2, onde p é primo, então G é abeliano.*

Demonstração: G é abeliano se, e somente se $G = Z(G)$, mas como $Z(G)$ é subgrupo de G, basta provar que $|G| = |Z(G)| = p^2$.
Pelo Teorema 4.3.2 $Z(G) \neq \{e\}$, então pelo Teorema de Lagrange $|Z(G)| = p$ ou $|Z(G)| = p^2$. Supondo por absurdo que $|Z(G)| = p$, então existe $a \in G$, tal que $a \notin Z(G)$, assim $|Z(G)| \subsetneq N(a)$. Pela Proposição 4.2.11 $Z(G) \subsetneq N(a) \subsetneq G$, mas $N(a)$ é subgrupo de G e $N(a) \subsetneq G$, então pelo Teorema de Lagrange $|N(a)| = p$ ou $|N(a)| = 1$, o que é um absurdo.
Logo, $|Z(G)| = p^2$. ∎

Teorema 4.3.4 (Teorema de Cauchy) *Seja $(G,\cdot)$ um grupo finito. Se p é um natural primo e divide a ordem de G, então G tem elemento de ordem p.*

Demonstração: Para encontrar $a \in G$ com $a \neq e$ tal que $a^p = e$, será feita a indução sobre a ordem de G.

Se $|G| = 1$ não há nada a fazer, pois $G = \{e\}$. Supondo que o resultado seja válido para grupos T, com $1 \leq T < G$. Será mostrado que vale para G.

Se G possui apenas subgrupos triviais, isto é, G e $\{e\}$. Tem-se que $|G| = p$, pois se $|G| = p^n$ com $n > 1$, então pelo Teorema 4.3.2 $Z(G) \neq \{e\}$, logo G teria um subgrupo não-trivial. Como $G = p$, pelo Teorema de Lagrange, para todo $a \in G$, $o(a) = 1$ ou $o(a) = p$, ou seja, se $a \neq e$, então $a^p = e$.

Se G possui subgrupos não-triviais, então serão analisados dois casos:

Caso 1. Seja H subgrupo não-trivial de G, tal que p divide $|H|$. Então, $1 < |H| < |G|$ e pela hipótese de indução existe $a \in H$ com $a \neq e$ tal que $a^p = e$.

Caso 2. Para qualquer subgrupo não-trivial H de G, p não divide H.
Sempre que $a \notin Z(G)$, então $\{e\} \subsetneq N(a) \subsetneq G$ e p não divide $|N(a)|$. Pela equação da classe de G, tem-se

$$\begin{aligned} |G| &= \sum \frac{|G|}{|N(a)|} \\ &= \sum_{N(a)=G} \frac{|G|}{|N(a)|} + \sum_{N(a)\neq G} \frac{|G|}{|N(a)|} \\ &= |Z(G)| + \sum_{N(a)\neq G} \frac{|G|}{|N(a)|}. \end{aligned}$$

Como p divide $|G| = |N(a)|(G : N(a))$ (pelo Teorema de Lagrange) e p não divide $|N(a)|$, então p divide $(G : N(a))$ ou seja p divide $\sum \frac{|G|}{|N(a)|}$. Logo p divide $|Z(G)|$ e por hipótese p não divide a ordem dos subgrupos próprios de G, então $Z(G) = G$ logo G é abeliano pela Proposição 4.1.1 e pelo Teorema 4.1.13 G tem elementos de ordem p.

■

Para garantir a existência de subgrupos de um grupo finito com ordens especiais, serão necessários os estudos dos Teoremas de Sylow vistos a seguir.

Definição 4.3.5 *Seja $(G, \cdot)$ um grupo finito. Seja p um natural primo. Um subgrupo H de G é chamado um* **p-Sylow** *subgrupo de G se $|H| = p^m$, onde p^m divide $|G|$, mas p^{m+1} não divide $|G|$.*

Exemplo 4.3.6 *Seja $(G, \cdot)$ um grupo cíclico de ordem 10 gerado por a. Então, $H = \langle a^5 \rangle$ é o único 2-Sylow subgrupo de G, e $N = \langle a^2 \rangle$ é o único 5-Sylow subgrupo.*

Exemplo 4.3.7 *Em $(S_3, \circ)$, $H = \langle g_1 \rangle$ é um 2-Sylow subgrupo de S_3 e $K = \langle f_1 \rangle$ é um 3-Sylow subgrupo de S_3.*

Definição 4.3.8 *Seja H um subgrupo de $(G, .)$. Chama-se* **normalizador** *de H o conjunto*

$$N(H) = \{x \in G / x^{-1}Hx = H\}.$$

Proposição 4.3.9 *$N(H)$ é subgrupo de G.*

Demonstração: De fato, dados $x, y \in N(H)$ então $x^{-1}Hx = H$ e $y^{-1}Hy = H$. Logo

$$(xy^{-1})^{-1}H(xy^{-1}) = yx^{-1}Hxy^{-1} = yHy^{-1}$$

e se $y^{-1}Hy = H$, então $yHy^{-1} = H$.

Assim, $xy^{-1} \in N(H)$ e pela Proposição 2.3.5 $N(H) < G$. ■

Teorema 4.3.10 *Seja $(G, .)$ um grupo finito e seja p um natural primo tal que $p^m \mid |G|$ e $p^{m+1} \nmid |G|$. Então,*

(i) **1° Teorema de Sylow:** *G tem subgrupo de ordem p^m*

(ii) **2° Teorema de Sylow:** *Os p-Sylow subgrupos de G são conjugados, isto é, se H e K são p-Sylow subgrupos de G, então existe $a \in G$ tal que $K = a^{-1}Ha$.*

Além disso, o número n_p de p-Sylow subgrupos de G é $n_p = \dfrac{|G|}{|N(P)|}$, onde P é qualquer p-Sylow subgrupo. Em particular, n_p divide $|G|$.

(iii) **3° Teorema de Sylow:** $n_p \equiv 1 (mod\ p)$.

Será apresentada a demonstração apenas da primeira parte que ressalta a recíproca de Lagrange. A segunda e a terceira parte exploram a quantidade de p-subgrupos porém não houve tempo para estudar estes resultados.

Teorema 4.3.11 (1º Teorema de Sylow) *Seja $(G,.)$ um grupo finito e seja p um natural primo tal que $p^m \mid |G|$ e $p^{m+1} \nmid |G|$. Então, G tem subgrupo de ordem p^m*

Demonstração:

Será feita indução sobre a ordem de G. Se $|G| = 1$, o teorema é válido. Supondo o resultado válido para grupos T, com $1 \leq |T| < G$. Provar-se á o resultado para G.

Se G possui subgrupo H tal que $p^m|H$ e $p^{m+1} \nmid H$, então pela hipótese de indução H tem subgrupo de ordem p^m.

Supondo que p^m não divide a ordem dos subgrupos próprios de G. Neste caso $m \geq 1$, pois se $m = 0$, então $p^m = 1$ e 1 divide a ordem dos subgrupos. Pela equação de classe de G,

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} \frac{|G|}{|N(a)|}.$$

Como para todo $a \notin Z(G)$, $p^m| \ |G|$ e $p^m \nmid \ |N(a)|$, então p divide $\frac{|G|}{|N(a)|}$, logo p divide $|Z(G)|$. Pelo Teorema 4.3.4, existe $b \in Z(G)$, com $b \neq e$ tal que $b^p = e$. Seja $K = \langle b \rangle$ então $|K| = p$ e K é subgrupo normal de G, pois $b \in Z(G)$ e para todo $g \in G$ tem-se

$$g^{-1}bg = g^{-1}gb = b.$$

E ainda

$$\begin{aligned} g^{-1}b^r g &= g^{-1}bbb\ldots bg \\ &= g^{-1}b(gg^{-1})b(gg^{-1})b(gg^{-1})\cdots b(gg^{-1})bg \\ &= (g^{-1}bg)(g^{-1}bg)(g^{-1}bg)\cdots(g^{-1}bg) \\ &= bbbb\cdots bb \\ &= b^r \subset K, \text{ para todo } r \in \mathbb{N}. \end{aligned}$$

Então, considerando o grupo quociente G/K, tem-se

$$|G/K| = \frac{|G|}{|K|} = \frac{|G|}{p} < |G|.$$

Como $p^m| \ |G|$ e $p^{m+1} \nmid \ |G|$, tem-se $p^{m-1}| \ |G/K|$ e $p^m \nmid \ |G/K|$. Por hipótese de indução, G/K tem um subgrupo F com $|F| = p^{m-1}$.

Seja $H = \{x \in G/ \ Kx \in F\}$. Então H é um subgrupo de G, $K \subset H$ e $f(H) = F$, isto é $F = \{Kx/ \ x \in H\} = H/K$, onde $f : G \longrightarrow G/K$ é definida por $f(x) = Kx$.

De fato, se $x \in K$, então $Kx = K \in F$, assim pela definição de H tem-se que $x \in H$, donde $K \subset H$.

Sejam $x, y \in H$. Pela definição de H tem-se que $Kx, Ky \in F$. Como F é um subgrupo de G/K, então $K(xy) = KxKy \in F$ e $Kx^{-1} = (Kx)^{-1} \in F$, assim $xy \in H$ e $x^{-1} \in H$.

Logo, H é subgrupo de G. Portanto

$$p^{m-1} = |F| = |H/K| = \frac{|H|}{|K|} = \frac{|H|}{p}.$$

Então $|H| = p^m$ e H é o p-Sylow subgrupo de G procurado.

■

Como consequência do 1° Teorema de Sylow temos que se G for um grupo de ordem 15, então existem subgrupos $H,\ K$ de G tais que $|H| = 3$ e $|K| = 5$. Além disso, pelo 2° e 3° Teorema de Sylow tem-se que

- $n_3 = \dfrac{|G|}{|N(H)|} = \dfrac{15}{|N(H)|}$ e $n_3 = 1 + 3s$, para algum $s \in \mathbb{N}$;
- $n_5 = \dfrac{|G|}{|N(K)|} = \dfrac{|15|}{|N(K)|}$ e $n_5 = 1 + 5s$, para algum $s \in \mathbb{N}$.

Como $H < N(H) < G$ e $K < N(K) < G$ segue que

- $|H| \backslash |N(H)|$ e $|N(H)| \backslash |G|$
- $|K| \backslash |N(K)|$ e $|N(K)| \backslash |G|$

Assim, $n_3 = 1$ e $n_5 = 1$ e consequentemente $N(H) = G$ e $N(K) = G$, donde H e G são subgrupos normais de G. Logo, pelo Corolário 4.1.10 segue que

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Pelo Teorema de Cauchy (Teorema 4.3.4) tem-se que existem $a, b \in G$ tais que $H = \langle a \rangle$ e $K = \langle b \rangle$. Então, $H \cap K = \{e\}$ e, portanto, $|HK| = 15$ e $G \simeq HK$.

Pode-se provar que, a menos de isomorfismos, os grupos de ordem 15 são isomorfos a $(\mathbb{Z}_{15}, \oplus)$. Para tal precisa-se dos produtos semidiretos de dois grupos.

Ainda como consequência do 1° Teorema de Sylow temos que se G for um grupo de ordem 12, então existem subgrupos $H,\ K$ de G tais que $|H| = 3$ e $|K| = 4$.

De fato, pois $|G| = 12 = 3.2^2$

- $3|\ |G|$ e $3^2 \nmid |G| \Longrightarrow \exists K < G\ :\ |K| = 3.$
- $2^2|\ |G|$ e $2^3 \nmid |G| \Longrightarrow \exists H < G\ :\ |K| = 4.$

Porém para terminar a classificação de todos os grupos de ordem 12 seriam necessários o 2° e 3° Teorema de Sylow e o estudo de produtos semidiretos de grupos.

CONCLUSÃO

Neste trabalho foram vistos alguns resultados já estudados na graduação durante a disciplina de Álgebra que foram de grande importância para os estudos que se prosseguiram.

Utilizando como principal ferramenta o Teorema de Lagrange, pode-se classificar grupos de ordem menor que 12 e grupos de ordem $2p$ com $p > 2$ primo, mas para grupos finitos com ordem maiores era inviável continuar a classificação do mesmo modo, portanto foram estudados os Teoremas de Sylow, que oferecem ferramentas para a classificação de grupos finitos com ordens maiores.

O 1° Teorema de Sylow apresenta uma recíproca parcial do Teorema de Lagrange garantindo a existência de subgrupos finitos com ordem p^m sendo p um número natural primo tal que $p^m | \, |G|$ e $p^{m+1} \nmid \, |G|$. Além disso, aparecem os Teoremas de Cauchy que garantem que se p é um número natural primo que divide a ordem de G, então G possui um elemento de ordem p e consequentemente um subgrupo com ordem p.

Seria interessante para a complementação destes estudos, o aprofundamento em produto direto, produto semi-direto de grupos, além do 2° e 3° Teorema de Sylow que não foram vistos neste trabalho por falta de tempo. Com estes resultados seria viável a classificação de mais grupos finitos tornando os estudos dos Teoremas de Sylow mais exemplificados.

REFERÊNCIAS

DOMINGUES, H; IEZZI, G. **Álgebra moderna**. São Paulo: Atual, 1979.

GARCIA, A; LEQUAIN, Y. **Elementos de Álgebra**. 2. ed. Rio de Janeiro: IMPA, 2008.

GONÇALVES, A. **Introdução à álgebra**. Rio de Janeiro: IMPA, 1999.

HERNSTEIN, I. N. **Tópicos em álgebra**. São Paulo: Editora da Universidade e Polígono, 1970.

LANG, S. **Álgebra para graduação**. Rio de Janeiro: Editora Ciência Moderna, 2008.

MARTIN, P. A. **Grupos, Corpos e Teoria de Galois**. São Paulo: Editora Livraria da Física, 2010.

MONTEIRO, L. H. J. **Elementos de álgebra**. Rio de Janeiro: Livros técnicos e Científicos editora, 1969.

VILLELA, M. L. T, **Grupos**: Parte 2 - Complementos da Teoria dos Grupos. Agosto de 2007. 53f. Notas de aula.