UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE EDUCAÇÃO E SAÚDE

UNIDADE ACADÊMICA DE EDUCAÇÃO

Curso de Graduação em Licenciatura em Matemática

José Francisco dos Santos Oliveira

CLASSIFICAÇÃO DE GRUPOS DE ORDEM ≤ 11

Cuité-PB

2016

José Francisco dos Santos Oliveira

CLASSIFICAÇÃO DE GRUPOS DE ORDEM ≤ 11

TCC apresentado ao curso de Graduação em Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande em cumprimento às exigências do Componente Curricular Trabalho Acadêmico Orientado, para obtenção do grau de Licenciado em Matemática.

Orientador: Marciel Medeiros de Oliveira

Cuité-PB

2016

FICHA CATALOGRÁFICA ELABORADA NA FONTE
Responsabilidade Jesiel Ferreira Gomes – CRB 15 – 256

O48c Oliveira, José Francisco dos Santos.

Classificação de grupos de ordem ≤ 11. / José Francisco dos Santos Oliveira. – Cuité: CES, 2016.

56 fl.

Monografia (Curso de Licenciatura em Matemática) – Centro de Educação e Saúde / UFCG, 2016.

Orientador: Marciel Medeiros de Oliveira.

1. Grupos finitos. 2. Ordem de grupos. 3. Grupos gerados. I. Título.

Biblioteca do CES CDU 512

José Francisco dos Santos Oliveira

CLASSIFICAÇÃO DE GRUPOS DE ORDEM ≤ 11:

TCC apresentado ao curso de Graduação em Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande em cumprimento às exigências do Componente Curricular Trabalho Acadêmico Orientado, para obtenção do grau de Licenciado em Matemática.

Marciel Medeiros de Oliveira (Orientador) - UFCG Cuité

Aluízio Freire da Silva Junior(Examinador) - UFCG Cuité

Jussiê Ubaldo da Silva (Examinador) - UFCG Cuité

Cuité-PB, 25 de maio de 2016

Agradecimentos

Agradeço primeiramente a Deus, pelo dom da vida, por todas as oportunidades e por se fazer pequeno o suficiente somente para que eu possa alcançá-Lo pois a minha mente humana não é capaz de compreendê-Lo em sua totalidade.

Agradeço a toda minha família, por toda compreensão e toda ajuda de forma direta ou indiretamente para chegar até aqui.

Ao Subprojeto - PIBID/Matemática, em nome do Coordenador de Área o Professor Alecxandro Alves Vieira pelo direcionamento, incentivo e oportunidade de participar diretamente nas salas de aula.

Agradeço a todos os meus colegas de turma, do curso, do CES pela importância no decorrer deste curso.

Agradeço aos Professores Aluízio Freire da Silva Junior e Jussiê Ubaldo da Silva, pela disponibilidade de estarem presentes na banca examinadora deste trabalho. Como também aos meus ex-Professores, a todo o corpo docente do Curso de Licenciatura em Matemática do Centro de Educação e Saúde (CES), da Universidade Federal de Campina Grande (UFCG), Campus - Cuité, aos recepcionistas Vital e Jardel e em especial ao Professor Marciel Medeiros de Oliveira, pela confiança, disponibilidade e por tudo que fez para que essa fase fosse concluída.

Dedicatória

Aos meus pais Rita Pereira dos Santos
e Sebastião Francisco de Oliveira e irmãos.

"Treine enquanto eles dormem, estude enquanto eles se divertem, persista enquanto eles descansam, e então, viva o que eles sonham."

Provérbio japonês

Resumo

Este trabalho é um estudo sobre classificação, a menos de isomorfismo, de grupos finitos por meio de resultados importantes da álgebra como o Teorema de Lagrange, de Cauchy e o pequeno Teorema de Fermat, satisfazendo a condição de que sejam gerados por dois elementos a e b tal que $ba = a^s b$, Além de promover uma maior e melhor compreensão de alguns resultados da teoria de grupos. Para isso, se faz necessário um bom entendimento de parte dos principais resultados da teoria de grupos a nível de graduação, citamos então os resultados suficientes com as suas respectivas demonstrações.

Palavras-chave: Grupos finitos, Ordem de grupos, Grupos gerados.

Abstract

This work is a study of classification , less than isomorfismo, of nite groups generated by two elements a and b that satisfy the relation $ba = a^s b$. Beyond Promoting greater and better understanding of some results of group theory.For it , it is necessary a good understanding of some of the main results of that theory the level of graduation then we quote the enough results with your respective demonstrations .

Keywords: Finite groups , order groups , generated groups.

Sumário

Classificação de Grupos de ordem ≤ 11

Introdução

Ao estudar a teoria de grupos, busca-se o conhecimento e a determinação de suas estruturas e esse foi também um objetivo deste trabalho, além de classificar grupos finitos gerados por dois elementos a e b que satisfazem uma relação do tipo $ba = a^s b$, o que nos requer um conhecimento de resultados sobre teoria de grupos a nível de graduação.

Este trabalho foi dividido em três capítulos, onde no primeiro estão as preliminares; uma revisão dos conceitos e resultados básicos de grupos ou seja, a base para o terceiro capítulo.

No capítulo segundo, damos ênfase aos grupos gerados por dois elementos satisfazendo a relação $ba = a^s b$, ode oferece resultados de suma importância para que a conclusão do terceiro cítulo fosse possível.

No último capíto, é a parte onde classificamos todos os grupos de ordem menor que ou iguais a 11, a menos de isormorfismo, utilizando dos resultados dos capítulos anteriores.

Capítulo 1

Grupos

Neste capítulo vamos apresentar alguns conceitos elementares da teoria dos grupos, os quais, são essenciais para a compreensão dos próximos capítulos.

Definição 1.1 *Seja G um conjunto não vazio e $*$ uma operação em G. Dizemos que $(G, *)$ é um* ***grupo*** *se valem as seguintes propriedades:*

i) $(a * b) * c = a * (b * c)$, $\forall a, b, c \in G$

ii) Existe $e \in G$ *tal que* $a * e = e * a = a, \quad \forall a \in G$

iii) Para cada $a \in G$*, existe* $a' \in G$ *tal que* $a * a' = a' * a = e$.

Se, além disso, a operação $*$ for comutativa, ou seja, $a * b = b * a \ \forall a, b \in G$, dizemos que $(G, *)$ é um ***grupo comutativo*** (ou abeliano).

Observação 1.1 *1) Por simplicidade, usaremos apenas G ao invés de $(G, *)$ para denotar um grupo, ficando subentendido a operação. Também usaremos ab, ao invés de $a * b$ para denotar a operado com b.*

2) O grupo G possui um único elemento neutro.

3) Para cada $a \in G$, seu inverso $a' \in G$ é único.

4) Operações no grupo. Em todos os grupos citados acima, as operações de multiplicação e adição mencionadas, são as usuais de cada conjuno.

Usaremos a notação multiplicativa. Todavia, tudo pode ser adaptada para a notação aditiva.

Demonstraremos aqui as propriedades (2), (3) e (4) da observação acima:

Demonstração 1.1 *(2) De fato, se e e $e^{'}$ são elementos neutros de G, então;*

$$e = e \cdot e^{'} \text{ pois } e^{'} \text{ é elemento neutro,}$$
$$= e^{'} \text{ pois } e \text{ é elemento neutro.}$$

(3) De fato, seja a pertencente a G, e sejam b e $b^{'} \in G$ dois elementos inversos de a, temos:

$$b = b \cdot e = b \cdot (a \cdot b^{'}) \text{ pois } b^{'} \text{ é inverso de } b$$
$$= (b \cdot a) \cdot b^{'} = e \cdot b^{'} = b^{'} \text{ pois } b \text{ é inverso de } a.$$

(4) Dado $a \in G$, um elemento $b \in G$ é, por definição, o inverso de a ou vice-versa, quando

$$a \cdot b = b \cdot a = e.$$

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

■

São exemplos de grupos

(1) $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ grupos aditivos abelianos com a soma usual.

(2) $\mathbb{R} - \{0\}$, $\mathbb{Q} - \{0\}$, $\mathbb{C} - \{0\}$, grupos abelianos com a multiplicação usual.

(3) $(M_{m\times n}(\mathbb{Z}))$, $(M_{m\times n}(\mathbb{R}))$, $(M_{m\times n}(\mathbb{Q}))$, $(M_{m\times n}(\mathbb{C}))$, representam o grupo das matrizes de ordem nXm, abelianos , sob a adição usual.

Em cada grupo acima, as operações de adição e multiplicação são as usuais de cada conjunto.

(4) Seja $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}$, defina em ($\mathbb{Z}_m$ a soma $\overline{a}+\overline{b} = \overline{a+b}$; $\forall\ \overline{a}$ e $\overline{b} \in \mathbb{Z}_m$ temos que $(\mathbb{Z}_m, +)$ é grupo abeliano das classes de resto módulo m.

(5)O grupo $(S_n, \circ)$, das permutações de grau n, onde a notação

$$\begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$$

representa a função bijetiva definida por $f(1) = i_1$; $f(2) = i_2$; ...; $f(n) = i_n$ e $r_m r_n = r_m \circ r_n$.

(6) O grupo $(G \times H, \cdot)$, formado a partir dos grupos $(G, \diamond)$ e $(H, \circ)$ com elementos neutros iguais a e_G e e_H respectivamente. O produto cartesiano de G por H denotado por $(G \times H) = \{(g, h) \mid g \in G \text{ e } h \in H\}$,com a operação '$\cdot$' definida entre pares de elementos de $(G \times H)$ pela regra: $(g, h) \cdot (g', h') = (g \diamond g', h \circ h')\ \forall g, g' \in G; h, h' \in H$. Verica-se então que o grupo $(G \times H, \cdot)$ tem como elemento neutro $e = (e_G, e_H)$. Por exemplo, como $(\mathbb{Z}_2, +)$ é um grupo, temos que

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$$

é um grupo abeliano, de elemento neutro igual a $e = (\overline{0}, \overline{0})$.

Observação 1.2 *$(G_1 \times G_2)$ é abeliano quando G_1 e G_2 o são.*

(7)Grupo dos quatérnios Q_3, dado por

$$Q_3 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$$

Com $i \in \mathbb{C}$ tal que $i^2 = -1$

1.1 Subgrupos

Estudaremos aqui um subconjunto H de um grupo G, onde o estudo de G torna-se-á mais factível, usando resultados obtidos sobre H de forma a conseguir informações interessantes de G.

Definição 1.2 *Seja G um grupo e H um subconjunto não vazio de G. Dizemos que H é um* ***subgrupo*** *de G, denotado por $H \leq G$, se valem:*
i) $x.y \in H, \forall x, y \in H$;
ii) $x^{-1} \in H, \forall x \in H$

Definição 1.3 *Seja G um grupo e $H \subset G$ não vazio seja um subgrupo de G, é necessário e suficiente que:*

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

Observação 1.3 *Se G é um grupo e $H \leq G$. Então valem:*
1) $e \in H$, onde e é o elemento neutro de G.
2) O subgrupo H com operação de G, é por si só um grupo.

São exemplos de subgrupos

(1)$\{e\}$ e G são subgrupos de um grupo G, denominados subgrupos triviais.

(2) Para cada $n \in \mathbb{Z}$, o conjunto $H = n\mathbb{Z}$ de todos os múltiplos de n,

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}\ ,$$

é um subgrupo de $\mathbb{Z}$.

(3) Considere G um grupo arbitrário. O subconjunto $Z(G) = \{x \in G \mid xg = gx, \forall\ g \in G\}$, é um subgrupo de G denominado centro de G.

Primeiro, temos que $Z(G) \neq \varnothing$ pois, claramente, $e \in Z(G)$. Sejam a e $b \in Z(G)$ e $x \in G$. Assim

$$(ab^{-1})x = (ab^{-1})xe = ab^{-1}xbb^{-1}$$

(4) O subgrupo de S_4, denotado por D_4, o qual representa o grupo das simetrias de um quadrado, onde:

$$D_4 = \{a_0 = e, a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$$

com;

$$a_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},\ a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},\ a_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$

$$a_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},\ a_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},\ a_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$a_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix},\ a_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Observa-se que D_4 não é abeliano, notando que:

$$a_1 * a_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } a_4 * a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

ou seja, $a_1 * a_4 \neq a_4 * a_1$.

Subgrupo gerado por um subconjunto

Vamos considerar as seguintes notações:

Sejam H e K subgrupos de G, definimos $HK = \{hk \mid h \in H \text{ e } k \in K\}$ e $H^{-1} = \{h^{-1} | h \in H\}$.

Tomando S um subconjunto não-vazio do grupo G, faça $\langle S\rangle = \{a_1a_2...a_n | n \in \mathbb{N}, a_i \in S \text{ ou } a_i \in S^{-1}\}$. Se S possuir um número finito de elementos, ou seja, $S = \{a_1, a_2, ..., a_n\}$ utilizaremos $\langle a_1, a_2, ..., a_n\rangle$ para designar

$\{\langle a_1, a_2, ..., a_n\rangle\}$. Observemos que, se $r \in \mathbb{N}$, escreveremos g^{-r}, para denotar o elemento $(g^{-1})^r$, com $g \in G$. Portanto, se $g \in G$, temos que: $\langle g\rangle = \{..., (g^{-1})^2, g^{-1}, e, g, g^2, ...\} = \{g^t | t \in \mathbb{Z}\}$.

Proposição 1.1 *Sejam G um grupo e S um subconjunto não vazio de G. Então $\langle S\rangle$ é subgrupo de G.*

Demonstração 1.2 *Devemos provar que:*

1) $\forall\ x$ e $y \in \langle S\rangle$, temos $xy \in \langle S\rangle$.

2) $\forall\ x \in \langle S\rangle$, temos $x^{-1} \in \langle S\rangle$.

Sejam $x, y \in \langle S\rangle$. Temos

$x = a_1a_2...a_n$, com $a_i \in S$ ou $a_i \in S^{-1}, \forall\ i$

$y = b_1b_2...b_m$, com $b_j \in S$ ou $b_j \in S^{-1}, \forall\ j$

Logo, $xy = a_1a_2...a_nb_1b_2...b_m$ e $x^{-1} = a_n^{-1}a_{n-1}^{-1}...a_2^{-1}a_1^{-1}$ estão também em $\langle S\rangle$. ■

Definição 1.4 *Sejam G um grupo e S subconjunto não vazio de G, então $\langle S\rangle$ é o subgrupo gerado por $\langle S\rangle$.*

Definição 1.5 *A ordem de um grupo finito G é o número de elementos do conjunto G, denotada por $|G|$. Sendo α um elemento do grupo G, a ordem de α é a ordem do subgrupo gerado por α e denotada por $O(\alpha)$.*

Proposição 1.2 *Sejam G um grupo e $\alpha \in G$ e $\langle\alpha\rangle$ o subgrupo gerado por α, então, são equivalentes as seguintes condições:*

(i) A ordem $|\langle\alpha\rangle|$ é finita.

(ii) Existe $k \geq 1$ tal que $\alpha^k = e$

Assim, se denotarmos por n a ordem de α, temos

$\{k \geq 0; \alpha^k = e\} = \{o, n, 2n, ...\}$

$e\ \langle\alpha\rangle = \{e, \alpha, ..., \alpha^{n-1}\}$.

Demonstração 1.3 *(i)* $\rightarrow$ *(ii) Como* $\langle\alpha\rangle = \{\alpha^m; m \in \mathbb{Z}\}$, *e como,por hipótese, o subgrupo* $\langle\alpha\rangle$ *tem ordem finita, existem* p *e* $q \in \mathbb{Z}$, $p \neq q$ *tais que* $\alpha^p = \alpha^q$. *Sem perda de generalidade, podemos supor que* $p > q$. *Como* $\alpha^p = \alpha^q$, *então* $\alpha^{p-q} = e$ *e portanto existe* $k > 0$ *tal que* $\alpha^k = e$. *(ii)* $\Rightarrow$ *(i)Consideramos o inteiro* $r = min\{k \geq 1; \alpha^k = e\}$. *Queremos mostrar que* $r = n$. *Para isto, basta apenas provar que* $\langle\alpha\rangle = \{e, \alpha, ..., \alpha^{n-1}\}$ *e os elementos* $e, \alpha, ..., \alpha^{n-1}$ *são distintos.* ■

1.2 Homomorfismo e Isomorfismo de Grupos

Um conceito de grande importância para o nosso estudo de grupos é a parte de homomorfismo e isomorfismo, uma vez que torna-se uma ferramenta indispensável neste sentido. Aqui, relacionaremos dois grupos com intuito de adquirir informações algébricas do segundo através de propriedades algébricas do primeiro e vice-versa. A noção de isomorfismo de grupos é de grande valia, uma vez que nos fornece um modo de verificar se dois grupos são essencialmente os mesmos, ou seja, possuem propriedades algébricas iguais.

Definição 1.6 *Sejam* $(G_1, *)$ *e* $(G_2, \cdot)$ *grupos. Definimos um* ***homomorfismo*** *de* G_1 *em* G_2, *como sendo uma função que satisfaz:*

$$f(x * y) = f(x) \cdot f(y)$$

para quaisquer $x, y \in G_1$.

São exemplos de homomorfismo

(i) $e : G_1 \longrightarrow G_2$, $e(g) = e_{G_2}$ (homomorfismo trivial)

(ii) $Id : (G_1, \cdot) \longrightarrow (G_1, \cdot)$, $Id\,(g) = g$ (identidade)

Proposição 1.3 *Seja $f : G_1 \longrightarrow G_2$ um homomorfismo de grupos. Então,*

(1) $f(e_1) = e_2$, e_1 e e_2 elementos neutros de G_1 e G_2, respectivamente.

(2) $f(a^{-1}) = f(a)^{-1}$, $\forall\ a \in G_1$.

Definição 1.7 *Seja $f : G_1 \to G_2$ um homomorfismo. Definimos:*

*i) O **núcleo** de f, denotado por $Ker\ f$, como sendo $Ker\ f = \{x \in G_1 \mid f(x) = e_2\}$*

*ii) A **imagem** de f, denotada por $Im\ f$, como sendo $Im\ f = \{f(x) |\ x \in G_1\}$.*

Proposição 1.4 *(1) $Im(f) = \{f(a) : a \in G_1\}$ é um subgrupo de G_2 – a imagem de f.*

(2) $Kerf = \{x \in G_1 | f(x) = e_{G_2}\}$ é um subgrupo normal de G_1 chamado núcleo do homomorfismo f.

Demonstração 1.4 *(1) Sendo $f(e_1) = e_2$, então, $Im(f) \neq \varnothing$. Agora, dados $x e\ y \in Im(f)$, existem a e $b \in G_1$ tais que $f(a) = x$ e $f(b) = y$. Por isso,*

$$x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1}),$$

de maneira que $x \cdot y^{-1} \in Im(f)$ e $Im(f) < G_2$

(2) Temos que Ker de $f \subset G_1$, pois $f(e_{G_1}) = e_{G_2} \Longrightarrow e_{G_1} \in Kerf$ e $Kerf \neq \varnothing$. Além disso, $\forall\ a$ e $b \in Kerf$, temos $f(a) = f(b) = e_{G_2}$, então;

$$f(a) * b^{-1} = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b)^{-1}$$
$$= e_{G_2} \cdot (e_{G_2})^{-1} = e_{G_2} \cdot e_{G_2} = e_{G_2}$$

Logo, $a * b^{-1} \in Kerf$*, e pela proposição 1.3, concluímos que* $Kerf < G_1$*. Mas,* $\forall\ a \in G_1$ *e* $\forall\ k \in Kerf$*, temos:*

$$f(a * k * a^{-1}) = f(a) * f(k) * f(a^{-1}) = f(a) * e_{g_2} * f(a^{-1})$$
$$= f(a * a^{-1}) = f(e_{G_1}) = e_{G_2}$$

Isto é, $a * k * a^{-1} \in Kerf$ *que implica que* $Kerf \triangleleft G_1$*.* ■

Observação 1.4 *O resultado das proposição 1.3 e 1.4 parte (1), podem ser traduzidas em "um homomorfismo de grupos preserva não somente as operações do grupo, mas também a identidade de* G_1 *e o inverso de cada elemento* $a \in G_1$*"*

Proposição 1.5 *sejam* $f : G_1 \longrightarrow G_2$ *e* $g : G_1 \longrightarrow G_2$ *homomorfismo de grupos. Então,* $g \circ f$ *é um homomorfismo.*

Demonstração 1.5 *De fato,* $\forall\ a, b \in G_1$ *temos que:*
$(g \circ f)(a * b) = g(f(a * b)) = g(f(a) \cdot f(b) = g(f(a)) \cdot g(f(b)) = (g \circ f(a)) \cdot (g \circ f(b))$. ■

Definição 1.8 *Um homomorfismo de grupos* $f : G_1 \longrightarrow G_2$ *bijetivo é dito um* ***isomorfismo*** *. De forma singular, um isomorfismo* $f : G \longrightarrow G$ *denomina-se um* ***automorfismo*** *de* G*.*

Um **isomorfismo** f é um **automorfismo** se $G_1 = G_2$, dizemos que G_1 e G_2 são isomorfos se $f : G_1 \longrightarrow G_2$ um isomorfismo e escrevemos $G_1 \simeq G_2$.

Proposição 1.6 *Se* $f : G_1 \longrightarrow G_2$ *é um* ***isomorfismo*** *, então* $f^{-1} : G_2 \longrightarrow G_1$ *também é um* ***isomorfismo****.*

Demonstração 1.6 *Basta mostrar que* $f^{-1} : G_2 \longrightarrow G_1$ *é um* ***homomorfismo****. Dados que* a_2 *e* $b_2 \in G_2$*, exitem* a_1 *e* $b_1 \in G_1$ *tais que*

$f(a_1) = a_2 \Leftrightarrow f^{-1}(a_2) = a_1$ *e* $f(b_1) = b_2 \Leftrightarrow f^{-1}(b_2) = b_1$ *por isso*

$f^{-1}(a_2 \cdot b_2) = f^{-1}(f(a_1) \cdot f(b_1)$

$= f^{-1}(f(a_1 \cdot b_1))$

$= a_1 \cdot b_1$

$= f^{-1}(a_2) \cdot f^{-1}(b_2)$

o que mostra que f^{-1} *é um homomorfismo.* ■

Definição 1.9 *Um homomorfismo* $f : G_1 \longrightarrow G_2$ *é dito um* ***monomorfismo*** *se f é injetora,* ***epimorfismo*** *se f é sobrejetora.*

Proposição 1.7 *Se f é sobrejetivo, então* $ker\,(f) = \{e\} \Leftrightarrow f$ *é um isomorfismo.*

Proposição 1.8 *Se* $f : G_1 \longrightarrow G_2$ *é um isomorfismo, então* $f^{-1} : G_1 \longrightarrow G_2$ *também é.*

Proposição 1.9 *Seja* $f : G_1 \longrightarrow G_2$ *um isomorfismo. Então, temos que;*

$$O(f(x)) = O(x),\ \forall\ x \in G$$

O conjunto dos autumorfismos e automorfismos internos de G, serão denotados respectivamente por $Aut(G)$ e$I(G)$; assim:

$$I(G) = \{I_g | g \in G\} \subseteq Aut(G)$$

Proposição 1.10 *Seja a função* $I_g : G \longrightarrow G$ *definida por* $I_g(x) = g \cdot x \cdot g^{-1}$*, temos que*

(i) $(I_g)^{-1} = I_{g^{-1}}$

(ii) $I_{g_1} \circ I_{g_2} = I_{g_1 g_2}$

Proposição 1.11 *Seja G um grupo abeliano, então, $\forall\ g \in G$ temos que;*

$$I_g(x) = g \cdot x \cdot g^{-1} = (g \cdot g^{-1}) \cdot x = e \cdot x = x$$

1.3 Grupos Cíclicos

Sejam G e $a \in G$. Denotemos por $< a >$, o subconjunto de G dado por $< a >= \{a^n \mid n \in \mathbb{Z}\}$.

Proposição 1.12 *Se G é um grupo e $a \in G$. Então $< a >$ é um subgrupo de G.*

Demonstração 1.7 *Sejam $x, y \in < a >$, então $x = a^r$ e $y = a^s$, onde r e s são inteiros. Daí, $x.y = a^r.a^s = a^{r+s} \in < a >$. E mais, se $x \in < a >$, então $x = a^r \Rightarrow x^{-1} = (a^r)^{-1} = a^{-r} \in < a >$. Logo, $< a >$ é subgrupo de G.*

Observação 1.5 *O grupo $< a >$ de G é chamado de subgrupo de G* ***gerado por*** *$a \in G$.*

Definição 1.10 *Seja G um grupo. Dizemos que G é* ***cíclico*** *se existir $a \in G$ tal que $< a >= G$. Quando existir $a \in G$ tal que $< a >= G$ o elemento a é chamado um* ***gerador*** *de G.*

Exemplo 1.1 *1) O grupo $(\mathbb{Z}, +)$ é cíclico, pois*

$$< 1 >= \{n.1 \mid n \in \mathbb{Z}\} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\} = \mathbb{Z}.$$

2) O grupo $(\mathbb{Q}, +)$ não é cíclico.

Proposição 1.13 *Todo grupo cíclico é abeliano.*

Demonstração 1.8 *Considerando G um grupo cíclico e $a \in G$ tal que;*

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Dados x_1 e $x_2 \in G$, com $x_1 = a^{n_1}$ e $x_2 = a^{n_2}$, onde n_1 e $n_2 \in \mathbb{Z}$,

$$x_1 \cdot x_2 = a^{n_1} \cdot a^{n_2} = a^{((n_1)+(n_2))} = a^{((n_2)+(n_1))} = a^{n_2} \cdot a^{n_1} = x_2 \cdot x_1.$$

Ou seja, temos que G é abeliano. ■

A recíproca da proposição anterior não é válida, pois, conforme feito anteriormente, o grupo $G = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ não é cíclico. (exemplo clássico de um grupo abeliano que não é cíclico.)

Teorema 1.1 *Todo subgrupo de um grupo cíclico é cíclico.*

Demonstração 1.9 *Considerando $G = \langle a \rangle$ um grupo cíclico e H um subgrupo de G. Se $H = \{e\}$, temos $H = \langle e \rangle$. Se $H \neq \{e\}$, então existe um $b \in H$, com $b \neq e$. Como $b \in G$, $b = a^k$ para algum $k \in \mathbb{Z}_*$. Mas, sendo $H < G, a^k \in H$. Por isso,*

$$X = \{n \in \mathbb{N} : a^n \in H\} \neq \varnothing.$$

Pelo Princípio da Boa Ordem, existe $m \in X$, com $m = minX$. Vamos mostrar que $H = \langle a^m \rangle$. Como $a^m \in H$, então $\langle a^m \rangle \subset H$. Consideremos, pois $h \in H$. Desde que $H < G$, então $h = a^n$ para algum $n \in \mathbb{Z}$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que

$$n = mq + r, \text{ com } 0 \leq r < m.$$

Logo, $a^n = a^{mq} \cdot a^r$, isto é,

$$a^r = a^n \cdot (a^m)^{-q}.$$

Como $a^m \in H$, *segue que* $(a^m)^{-q} \in H$. *Além disso, sendo que* a^n *e* $(a^m)^{-q}$ *elementos de* H, *temos que* $a^n \cdot (a^m)^{-q} \in H$, *isto é,* $a^r \in H$. *Mas, desde que* $m = minX$, *devemos necessariamente ter* $r = 0$. *Por conseguinte,* $n = mq$ *e*

$h = a^n = (a^m)^q \in \langle a^m \rangle$, *Assim,* $H \subset \langle a^m \rangle e$, *portanto,* $H = \langle a^m \rangle$.

■

Proposição 1.14 *Seja* $G = \langle g \rangle = \{..., g^{-1}, e, g, g^{-2}, ...\}$ *um grupo cíclico de ordem infinita. Então:*
(i) $f : (\mathbb{Z}, +) \to (G, \cdot)$, *dada por* $f(z) = g^z$, *é um isomorfismo.*
(ii) O elemento g^z *gera* G *se, e somente se* $z = 1$ *ou* $z = -1$.

Demonstração 1.10 *(i)* $\forall$ z_1 *e* $z_2 \in \mathbb{Z}$, *temos que;*
$f(z_1 + z_2) = g^{z_1+z_2} = g^{z_1} \cdot g^{z_2} = f(z_1) \cdot f(z_2)$ *Portanto,* f *é um homomorfismo.*
Além disso, a função f *é claramente uma bijeção e consequentimente um isomorfismo.*
(ii) Ja vimos em (i) que $f : z \mapsto g^z$ *é um isomorfismo. Logo,* g^z *gera* G *se , e somente se,* z *gera* $\mathbb{Z}$. *Mas os únicos elementos que geram* $\mathbb{Z}$ *são* $z = 1$ *e* $z = -1$. ■

Corolário 1.1 *Todo grupo cíclico finito de ordem* m *é isomorfo ao grupo aditivo* $(\mathbb{Z}_m, +)$ *das classes de resto módulo* m.

1.4 Homomorfismos e automorfismos de grupos cíclicos

Proposição 1.15 *Sejam* G *e* G' *dois grupos,* $a \in G$ *e* $b \in G'$.
(i) Se $O(a) < \infty$ *então existe um homomorfismo* $f : \langle a \rangle \longrightarrow G'$ *tal*

que $f(a) = b$ *se, e somente se* $O(b)$ *divide* $O(a)$*. Quando existir, o homomorfismo* f *é único e definido por* $f(a^r) = (b^r) \forall\ r \in \mathbb{N}$.

(ii) Se $O(a) = \infty$ *e* $(O(b)\, qualquer)$ *então existe um único homomorfismo* $f : \langle a \rangle \longrightarrow G$ *tal que* $f(a) = b$*. Tal homomorfismo* f *é dado por* $f(a^r) = (b^r) \forall\ r \in \mathbb{Z}$

Demonstração 1.11 *Se temos que* $O(a) < \infty$ *e* $O(b)$ *não divide* $O(a)$*, não existe homomorfismo* $f : \langle a \rangle \longrightarrow G$*, tal que* $f(a) = b$.

Se $O(a) = \infty$ *ou se* $O(a) < \infty$ *e* $O(b)$ *divide* $O(a)$*, considere a função* $f : \langle a \rangle \longrightarrow G$*, definida por* $f(a^r) = (b^r)$*. Então no caso onde* $O(a) < \infty$ *um mesmo elemento* $\phi \in \langle a \rangle$ *pode ter duas representações* $\phi = a^r$ *e* $\phi = a^s$*; Porém, para que* f *seja uma função bem definida, devemos verificar que o valor* $f(\phi)$ *independe desta representação, ou seja, devemos verificar que* r *e* s *são dois inteiros tais que* $a^r = a^s \Rightarrow b^r = b^s$*. Com efeito, sejam* $\phi = a^r$ *e* $\phi = a^s$ *duas representações de* ϕ*. Temos que* $a^{r-s} = e$*, logo* $r - s$ *é múltiplo de* $O(a)$ *e ,como por hipótese,* $O(b)$ *divide* $O(a)$ *temos que* $r - s$ *é múltiplo de* $O(b)$ *e consequentimente que* $b^{r-s} = e$ *o que implica em* $b^r = b^s$ *portanto,* f *está bem definida neste caso.*

Se $O(a) = \infty$*, temos que;*

$a^r = a^s \Leftrightarrow a^{r-s} = e \Leftrightarrow r - s = 0 \Leftrightarrow r = s$*, isto é, todo elemento* $\phi \in \langle a \rangle$ *tem uma única representação. Logo, se* $O(a) = \infty$ f *é realmente uma função, independente qualquer que seja* $O(b)$*.* ■

1.5 Classes Laterais e Teorema de Lagrange

A base da teoria dos grupos finitos, com objetivo de compreender melhor a conjectura de que para cada subgrupo H de um grupo finito G, a ordem de H é sempre um divisor da ordem de G. Seja G um grupo finito e H um subgrupo de G. Sobre essa grupo vamos considerar a relação de equivalência $\equiv_E (modH)$ dada para quaisquer a e $b \in G$ por

$$a \equiv_E b(modH) \rightarrow a^{-1}b \in H.$$

Proposição 1.16 *A relação $\equiv_E (modH)$ citada acima é de equivalência. Além disso, a classe de equivalência de um elemento $g \in G$, relativa a esta relação é dada por $\{g \cdot h \mid h \in H\}$.*

Demonstração 1.12 *Consideremos a, b, $c \in G$. ($\equiv_E$ é reflexiva) Como $a^{-1}a = e \in H$, então $a \equiv_E a(modH)$, ou seja, $\equiv_E$ é reflexiva.*

($\equiv_E$ é simétrica) Se $a \equiv_E b(modH)$, então $a^{-1}b \in H$. Assim,

$$(a^{-1}b)^{-1} \in H \rightarrow b^{-1}a \in H \rightarrow b \equiv_E a(modH)$$

de modo que $\equiv_E$ é simétrica.

($\equiv_E$ é transitiva) Se $a \equiv_E b(modH)$ $b \equiv_E c(modH)$ então, $a^{-1}b = h_1 \in H$ e $b^{-1}c = h_2 \in H$. Desse modo,

$$(a^{-1}b)(b^{-1}c) = h_1h_2 \in H \Rightarrow a^{-1}c \in H \Rightarrow a \equiv_E c(modH).$$

assim, $\equiv_E$ é transitiva e, por isso, é de equivalência.

Por outro lado, dado $g \in G$, seja $\overline{g}$ a classe de equivalência de g relativa à relação $\equiv_E$. Por definição, $\overline{g} = \{x \in G \mid g \equiv_E x\}$. Logo, para $x \in G$,

$$x \in \overline{g} \Leftrightarrow g \equiv_E x \Leftrightarrow g^{-1}x \in H$$

isto é, $g^{-1}x = h \in H$*, ou melhor,* $x = gh \in \{gh \mid h \in H\}$*. Isto nos diz que* $\overline{g} \subset \{gh \mid h \in H\}$*. Agora, se* $x \in \{gh \mid h \in H\}$*, então existe* $h \in H$ *tal que* $x = gh$*, ou seja* $g^{-1}x = h$*. Por conseguinte,* $g \equiv_E x(modH)$ *e, assim,* $x \in \overline{g}$*. Logo,* $\{gh \mid h \in H\} \subset \overline{g}$*, mostrando que* $\overline{g} = \{gh \mid h \in H\}$*.* ■

Vamos denotar aqui a classe $\overline{g}$ de um elemento $g \in G$ segundo a relação $\equiv_E (modH)$ por gH, a qual chamaremos de classe lateral à esquerda de H em G determinada por g. Assim,

$$gH = \{gh \mid h \in H\}$$

Analogamente, prova-se que a relação $\equiv_D (modH)$ sobre G dada, para quaisquer a, $b \in G$, por

$$a \equiv_D b(modH) \Leftrightarrow ab^{-1} \in H$$

é de equivalência e, para cada $g \in G$ a classe de equivalência de g segundo esta relação é $\overline{g} = \{hg \mid h \in H\}$, a qual vamos denotar por Hg,

$$Hg = \{hg \mid h \in H\}$$

e chamaremos classe lateral à direita de H em H determinada por g

Observação 1.6 *As seguintes proposições apresentam-se com classes laterais à esquerda, porém tanto faz à direita ou à esquerda. Portanto, seja* G *um grupo e* H *um subgrupo de* G*.*

Proposição 1.17 *A união de todas as classes laterais de* H *em* G *é igual a* G*.*

Proposição 1.18 *Temos que* $aH = bH \Longleftrightarrow a^{-1}b \in H, \forall\ a, b \in G$*.*

Proposição 1.19 *Sejam aH e bH duas classes laterais qualquer de H em G, então $aH \cap bH = \varnothing$ ou $aH = bH$.*

Demonstração 1.13 *A função*

$$\Psi : H \longrightarrow aH$$

$$h \longmapsto ah$$

$\forall\ h \in H$ *é claramente uma bijeção pois:*

(i) $\psi(h_1) = \psi(h_2)$

(ii) Dado $ah \in aH$*, fica claro que* ah *é a imagem de* h *por* ψ

Exemplos de classes laterais

(i) Sejam o grupo multiplicativo $G = \{-1, 1, -i, i\}$, e o subgrupo $H = \{-1, 1\}$ de G, então:

$(-1) \cdot H = \{(-1) \cdot 1, (-1) \cdot (-1)\} = \{-1, 1\} = H \cdot (-1)$

$1 \cdot H = \{1 \cdot 1, 1 \cdot (-1)\} = \{1, -1\} = H \cdot 1$

$(-i) \cdot H = \{(-i) \cdot 1, (-i) \cdot (-1)\} = \{-i, i\} = H \cdot (-i)$

$i \cdot H = \{i \cdot 1, i \cdot (-1)\} = \{i, -i\} = H \cdot i$

(ii) Sejam $G = (\mathbb{Z}_6, +)$ e seu subgrupo $H = \{\overline{0}, \overline{3}\}$, então:

$\overline{0} + H = \{\overline{0} + \overline{0}, \overline{0} + \overline{3}\} = \{\overline{0}, \overline{3}\} = H + \overline{0}$

$\overline{1} + H = \{\overline{1} + \overline{0}, \overline{1} + \overline{3}\} = \{\overline{1}, \overline{4}\} = H + \overline{1}$

$\overline{2} + H = \{\overline{2} + \overline{0}, \overline{2} + \overline{3}\} = \{\overline{2}, \overline{5}\} = H + \overline{2}$

$\overline{3} + H = \{\overline{3} + \overline{0}, \overline{3} + \overline{6}\} = \{\overline{3}, \overline{0}\} = H + \overline{3}$

$\overline{4} + H = \{\overline{4} + \overline{0}, \overline{4} + \overline{3}\} = \{\overline{4}, \overline{1}\} = H + \overline{4}$

$\overline{5} + H = \{\overline{5} + \overline{0}, \overline{5} + \overline{3}\} = \{\overline{5}, \overline{2}\} = H + \overline{5}$

Teorema 1.2 ***(Teorema de Lagrange)***

Seja G um grupo finito e H um subgrupo de G. Então $|G| = |H|(G : H)$ e a ordem e o índice de H dividem G.

Demonstração 1.14 *Considerando que* $(G : H) = \alpha$, *e* $\{a_1H, ..., a_\alpha H\}$ *todas as classes laterais de* H *em* G. *Como cada uma dessas classes possue* $|H|$ *elementos,(da proposição anterior) e* $a_1H \cup ...a_\alpha H = G$, *com* $a_iH \cup ...a_jH \neq \varnothing$ *(proposições 1.4 e 1.6), temos que* $|G| = \alpha|H| \Longrightarrow |G| = |H|(G : H)$.

Deste teorema, temos os seguintes corolários:

Corolário 1.2 *Seja* G *um grupo finito e* $\alpha \in G$. *Então a ordem de* α *divide a ordem de* G.

Corolário 1.3 *(Pequeno Teorema de Fermat) Seja* p *um número primo. Então:*
$a^{p-1} \equiv 1 mod p, \forall\ a \in \mathbb{Z} \setminus p\mathbb{Z}$

Corolário 1.4 *Seja* G *um grupo de ordem prima. Então* G *é cíclico.*

Demonstração 1.15 *Seja* $\alpha \in G \setminus e$ *e considere* $\langle\alpha\rangle$ *o subgrupo gerado por* α. *pelo Teorema de Lagrange,* $|\langle\alpha\rangle|$ *divide* $|G|$ *e portanto* $|\langle\alpha\rangle| = p = |G|$,*logo* $G = \langle\alpha\rangle$ ■

Teorema 1.3 *Seja* $(G, \cdot)$ *um grupo cíclico finito de ordem* n, *onde* g *é um gerador, então:*
$g^n = e$ *e* $G = \{g, g^2, ..., g^{n-1}, g^n = e\}$, *com* $g^i \neq g^j$, $\forall i \neq j$; $i, j \leq n$.

Corolário 1.5 *Seja* $(G, \cdot)$ *um grupo cíclico finito de ordem* n, *onde* g *é um gerador, então* n *é o menor inteiro positivo tal que* $g^n = e$.

Teorema 1.4 *Seja* $(G, \cdot)$ *um grupo cíclico finito de ordem* n , *onde* g *é um gerador e* $k \in \mathbb{Z}$, *então* $g^k = e$ *se, e somente se* $n \mid k$.

Proposição 1.20 *Considere o grupo $(G, \cdot)$ onde e é o elemento neutro, se um elemento h de G tem ordem n, então $h^k = e$.* ■

Demonstração 1.16 *Se O(h)= n e $h^k = e$, então usando o Lema de Euclides podemos escrever $k = nq + r \leq r \leq n$. Logo, $e = h^k = (h^n)^q \cdot h^r \Longrightarrow h^r = e$, e portanto r = 0, pois $r < n$ e n é a ordem de h.*

■

Lema 1.1 *Seja G um grupo e considere $\alpha \in G, \alpha \neq e$.*

(i) $O(\alpha) = 2$ se e somente se $\alpha = \alpha^{-1}$

(ii) Se $O(\alpha) = 2, \forall\ \alpha \neq e$, então G é um grupo abeliano.

Lema 1.2 *Todo grupo de ordem par possui pelo menos um elemento de ordem 2.*

Teorema 1.5 *(Teorema de Cauchy). Cosidere G um grupo finito de ordem n e p um número primo que divide n. Então, G contém um elemento de ordem p.*

Proposição 1.21 *Considere G um grupo abeliano e α, $\beta \in G$ com ordens finitas. Se $MDC(O(\alpha), O(\beta)) = 1$, então $O(\alpha\beta) = O(\alpha)O(\beta)$.*

Demonstração 1.17 *Iniciaremos demonstrando que, se G é um grupo e α e $\beta \in G$ tal que $\alpha\beta = \beta\alpha$ com $O(\alpha) = n$ e $O(\beta) = m$, então,$O(\alpha\beta) \mid MMC(n, m)$.*

De fato:

Tomando $O(\alpha\beta) = p \Longrightarrow (\alpha\beta)^p = e$, e se $(\alpha\beta)^k = e \Longrightarrow p \mid k$. Como $\alpha\beta = \beta\alpha \Longrightarrow (\alpha\beta)^P = \alpha^P\beta^P = e$, e além disso, $(\alpha\beta)^{mn} = \alpha^{mn}\beta^{mn} = (\alpha^n)^m(\beta^m)^n = e$.

Seja $MMC(n, m) = l \Longrightarrow n|l$ e $m|l$ pois $l = n \cdot n_1 = m \cdot m_1$.

Mas, $\alpha\beta^l = \alpha^l\beta^l = \alpha^{n\cdot n_1}\beta^{m\cdot m_1} = (\alpha^n)_1^n(\beta^m)_1^m = e \Longrightarrow p|l$*, isto é,* $O(\alpha\beta)|MMC(n,m)$*. Considerando então que* $MDC(m,n) = 1 \Longrightarrow l = MMC(n,m) = nm \Longrightarrow O(\alpha\beta)|nm$ *e existem* $x, y \in \mathbb{Z}$*, tais que:*

$$mx + ny = 1. \text{ (1)}$$

Então: $(\alpha\beta)^{mx+ny} = \alpha^{mx+ny}\beta^{mx+ny} = \alpha^{mx}\underbrace{\alpha^{ny}\beta^{mx}}\beta^{ny} = \alpha\beta \Longrightarrow (\alpha^{mx}\beta^{ny})^p = (\alpha\beta)^p = e \Longrightarrow \alpha^{pmx}\beta^{pny} = e \Longrightarrow \alpha^{pmx} = \beta^{-pny} \Longrightarrow (\alpha^{pmx})^n = e = \beta^{-pn^2y} \Longrightarrow m|pn^2y$ *mas de (1) temos que* $(n^2y, m) = 1 \Longrightarrow m|p$*.*

Também temos que $n|pmx$*, mas de (1) temos que* $(mx, n) = 1 \Longrightarrow n|p$*.*

Conclui se que $m|p$ *e* $n|p \Longrightarrow mn|p$*, logo:*

$p|mn$ *e* $mn|p \Longrightarrow p = mn$*, isto é,* $O(\alpha\beta) = mn$*.* ■

Proposição 1.22 *Seja* G *um grupo abeliano com* a *e* b *elementos de* G *de ordens finitas. Então existe* $c \in G$ *tal que* $O(c) = MMC(O(a)O(b))$*.*

Proposição 1.23 *Se* G *é um grupo abeliano e* $r := sup\{O(g)|g \in G\}$ *é finito, então* $O(x)$ *divide* r *para cada* $x \in G$*.*

Demonstração 1.18 *Suponhamos que* $r = sup\{O(g)|g \in G\}$ *é finito etomemos* $y \in G$ *tal que* $O(Y) = r$*. Se existir* $x \in G$ *tal que* $O(x)$ *não divide* r*, tem-se* $r := MMC(O(x)O(y)) > r$ *e pela proposição 1.10, existe um elemento* $c \in \langle x, y\rangle \subseteq G$ *tal que* $O(c) = s > r$*, um absurdo, uma vez que* r *é o supremo do conjunto.* ■

1.6 Subgrupos Normais e Grupos Quocientes

Estabelece-se nesta parte, condições sobre um subgrupo H de um grupo G, para verificar se a operação de G induz de maneira natural

uma operação sobre o conjunto das clases laterais à esquerda de H em G. veremos com mais clareza no decorrer da seção.

Definição 1.11 *Um subgrupo H de um grupo G é um subgrupo normal de G, escrevemos $H \triangleleft G$, se*

$$aha^{-1} \in H, \forall\ a \in G\ e\ \forall\ h \in H.$$

Proposição 1.24 *Seja G um grupo, então:*

(i) $N \triangleleft G \Leftrightarrow Ng = gN, \forall\ g \in G$

(ii) $N_1, N_2 \triangleleft G \rightarrow N_1 \cap N_2 \triangleleft G.$

(iii) $K < G\ e\ N \triangleleft G \rightarrow KN = \{k \cdot n | k \in K, n \in N\} < G.$

(iv) $N_1 \triangleleft G, N_2 \triangleleft G \rightarrow N_1 \cdot N_2 \triangleleft G.$

(v) $K < G, N \triangleleft G \rightarrow K \cap N \triangleleft K.$

Exemplos de subgrupos normais

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

(ii) $Z(G) \triangleleft G$ tal que $Z(G) = \{x \in G | xg = gx, \forall\ g \in G\}$

Proposição 1.25 *Se N é um subgrupo de um grupo G, onde $(G : N) = 2$, então $N \triangleleft G$.*

Demonstração 1.19 *Como $(G : N) = 2$, existem em G duas classes laterais diferentes; N e $G - N$ e, dado $a \in G$, exitem as seguintes possibilidades; $aN = Na = N$. Por outro lado, $a \in G - N$ então $aN = G - N = Na$.*

Verificamos que, se $(G : N) = 2$, temos $aN = Na, \forall\ a \in G$ e, pelo item (i) da proposição 1.13, conclui-se que $N \triangleleft G$. ■

Grupos Quocientes

Definição 1.12 *Se G é um grupo e H subgrupo normal de G. O grupo de suas classes laterais, com a operação induzida de G é chamado de* ***grupo quociente*** *de G por H, denotado por G/H.*

Proposição 1.26 *Seja G um grupo e N um subgrupo normal de G;*

(i) Se G é abeliano, então G/N é abeliano.

(ii) Se G é cíclico, então G/N é cíclico.

Proposição 1.27 *A ordem do grupo quociente G/H é o índice de H em G, ou seja $|G/H| = (G : H)$.*

Capítulo 2

Grupos Finitos Gerados por dois Elementos

Os grupos cíclicos, gerados por um elemento, são de mais simples classificação. Em compensação, classificar grupos gerados por dois elementos pode ser de grande complicação. Vamos aqui, restringir nosso estudo aos grupos finitos gerados por dois elementos a e b ou seja, $G = \langle a, b\rangle$ satisfazendo uma relação $ba = a^s b$. Obteremos resultados que serão de grande ajuda para classificar os grupos de ordem ≤ 11.
Consederemos, primeiro , o grupo S_3 das permutações de grau 3.
Veja:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \ \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \ \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \ \delta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \ \epsilon = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Vemos que S_3 é um grupo de ordem 6, onde

$$\begin{cases} S_3 = \langle \alpha, \beta \rangle \\ \alpha^3 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^2\beta \end{cases}$$

Então, mostraremos que se G é um grupo qualquer de ordem 6 no qual possue elementos A e B tais que:

$$\begin{cases} G = \langle A, B \rangle \\ A^3 = e \\ B^2 = e \\ BA = A^2B \end{cases},$$

Daí, existe um isomorfismo entre S_3 e G. Logo, a menos de isormorfismos, o grupo S_3 é caracterizado como sendo o grupo de ordem 6 gerado por dois elementos α e β satisfazendo as relações:

$$\begin{cases} \alpha^3 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^2\beta \end{cases}$$

Precisamos, pois, sobre um grupo gerado por dois elementos , determinar a natureza dos homomorfismos definido para esse grupo que satisfaça a relação $ba = a^s b$.

Proposição 2.1 *A relação* $ba = a^s b$ *equivale a* $I_b(a) = a^s$.

Demonstração 2.1 $ba = a^s b \iff bab^{-1} = a^s bb^{-1} \iff bab^{-1} = a^s e \iff bab^{-1} = a^s \iff I_b(a) = a^s$. ■

Teorema 2.1 *sejam G um grupo finito e $a, b \in G$ e satisfazendo $ba = a^s b$ e seja G' um grupo qualquer e $\alpha, \beta \in G$. Tomando $s \geq 1$ e sejam $n, m \geq 1$ inteiros tais que;*

$$a^n = e \text{ e } b^m \in \langle a \rangle \, (*).$$

Então:

a) $b^t \cdot a^r = a^{rs^t} \cdot b^t \ \forall \ r, t \in \mathbb{N}$, *e*

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

b) Se os inteiros me n são escolhidos minimalmente satisfazendo $(*)$, então o grupo $\langle a, b \rangle$ tem ordem igual a nm.

c) Se os inteiros m e n são escolhidos minimalmente, e se u é um inteiro tal que $b^m = a^u$, então existe um homomorfismo $f : \langle a, b \rangle \longrightarrow G$, se $f\langle a \rangle = \alpha$ e $f\langle b \rangle = \beta$ se, e somente se

$$\beta\alpha = \alpha^s\beta, \ \alpha^n = e, \ \beta^m = \alpha^u$$

Demonstração 2.2 *Primeiramente, observamos que, G sendo um grupo finito, os inteiros n e m existem de fato.*

a) Devemos mostrar que $b^t \cdot a^r = a^{rs^t} \cdot b^t$, o que equivale a $I_b^t(a) = a^{rs^t}$. Por indução sobre t temos;

Se $t = 1$

$$I_b(a^r) = (I_b(a))^r = (a^s)^r = a^{rs}.$$

Se $t \geq 2$ e supondo que o resultado é válido para $t-1$, temos

$$I_b(a^r) = I_b \circ I_b^{t-1}(a^r)$$

Se vale para $t-1 \Longrightarrow I_b^{t-1}(a^r) = a^{rs^{t-1}}$,*então*

$$I_b \circ I_b^{t-1}(a^r) = I_b\left(I_b^{t-1}(a^r)\right) = I_b\left(a^{rs^{t-1}}\right) = \left(I_b(a)\right)^{rs^{t-1}} = (a^s)^{rs^{t-1}} = a^{rss^{t-1}} = a^{rs^t}.$$

podemos então, concluir que qualquer elemento de $\langle a, b\rangle$ *pode ser escrito da forma* $a^v b^w$ *com* $v, w \in \mathbb{N}$. *Agora, a conclusão* $b^w \in \langle a\rangle$ *permite escrever este elemento* $a^v b^w$ *na forma* $a^{v'} b^j$ *com* $v' \in \mathbb{N}$ *e* $0 \leq j \leq m-1$; *a condição* $a^n = e$ *permite que se escreva o elemento* $a^{v'} b^j$ *na forma* $a^i b^j$ *com* $0 \leq i \leq n-1$ *e* $0 \leq j \leq m-1$ *portanto temos;*

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

b) Agora, suponhamos que n *e* m *são de fato minimais satisfazendo* $(*)$ *. Para vermos que* $\langle a, b\rangle$ *tem ordem* mn *,é suficiente verificarmos 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* $j = l$.

Suponhamos que, sem perda de generalidade, $l \leq j$. *Multiplicando ambos os lados da igualdade* $a^i b^j = a^k b^l$ *por* a^{-i} *pela esquerda e* b^{-l} *pela direita, temos que* $b^{j-l} = a^{k-i} \in \langle a\rangle$ *com* $0 \leq j-l \leq j \leq m-1$. *Portanto, pela minimalidade de* m *, temos* $j - l = 0$. *Assim* $l = j$ *e, consequentimente,* $a^{k-i} = e$; *pela minimalidade de* n *obtemos também* $i = k$.

c)$(\Longrightarrow)$*Supondo que existe um homomorfismo* $f : \langle a, b\rangle \longrightarrow G'$ *tal que* $f(a) = \alpha$ *e* $f(b) = \beta$. *Como* $ba = a^s b$, *temos;*

$$\beta\alpha = f(b)\, f(a) = f(ba) = f(a^s b) = (f(a))^s\, f(b) = \alpha^s \beta.$$

Como $a^n = e$, *temos* $\alpha^n = f(a)^n = e$ *e como* $b^m \in = \langle a\rangle$, *temos que* $b^m = a^u$, *com* $u \in \mathbb{N}$, *logo:*

$$b^m = a^u \Longrightarrow \beta^m = \alpha^u$$

($\Longleftarrow$) Considerando que $\beta\alpha = \alpha^s\beta$, $\alpha^n = e$ *e* $\beta^m = \alpha^u$. *Naturalmente, podemos aplicar a parte (a) ao grupo* G' *e a* α, β, *obtendo que* $\beta^t \cdot \alpha^r = \alpha^{rs^t} \cdot \beta^t \ \forall\ r$ *e* $t \in \mathbb{N}$. *É suficiente, então, verificar que a função* $f : \langle a, b\rangle \longrightarrow G'$ *definida por* $f\left(a^i b^j\right) = \alpha^i\beta^j$ *para* $0 \leq i \leq n-1$ *e* $0 \leq j \leq m-1$ *é um homomorfismo. Ora,* f *está bem definida, uma vez que* m *e* n *foram escolhas minimais. Agora, escrevendo* $j + l = pm + v$ *com* $0 \leq v \leq m-1$ *e escrevendo* $i+ks^j+pu = qn+w$ *com* $0 \leq w \leq n-1$ *para* $i, j, k, l \in \mathbb{N}$.

Temos:

$f\left(a^i b^j \cdot a^k b^l\right) = f\left(a^i \cdot b^j a^k \cdot b^l\right) = f\left(a^i \cdot a^{ks^j} b^j \cdot b^l\right) = f\left(a^{i+ks^j} b^{j+l}\right)$
$= f\left(\left(a^{i+ks^j} b^{pm+v}\right)\right) = f\left(\left(a^{i+ks^j} b^{pm} b^v\right)\right) = f\left(\left(a^{i+ks^j} a^{pu} b^v\right)\right) = f\left(a^w b^v\right) =$
$\alpha^w\beta^v = \alpha^{i+ks^j}\alpha^{pu}\beta^v = \alpha^{i+ks^j}\beta^{pm}\beta^v = \alpha^{i+ks^j}\beta^{j+l} = \alpha^i\alpha^{ks^j}\beta^j\beta^l =$
$\alpha^i\beta^j \cdot \alpha^k\beta^l = f\left(a^i b^j\right) \cdot \left(a^k b^l\right)$ ■

Teorema 2.2 *Sejam* m, n *e* s *números inteiros positivos.*

(i) Existe um grupo G *de ordem* mn *que possui elementos* a, b *tais que*

$$\begin{cases} G = \langle a, b\rangle \\ a^n = e \\ b^m = a^u \\ ba = a^s b \end{cases},$$

se, e somente se $s^m \equiv 1(mod n)$ *e* $u\,(s-1) \equiv 0(mod n)$.

(ii)Quando existir um grupo de ordem mn *satisfazendo as condições acima, ele é único a menos de isomorfismo.*

Demonstração 2.3 *(i)($\Longrightarrow$) Do Teorema 2.1, temos que* $b^m a = a^{s^m} b^m$. *Como* $b^m \in \langle a\rangle$,*temos que* b^m *comuta com* a, *o que implica em* $ab^m = a^{s^m} b^m$. *Podemos multiplicar ambos os lados por* a^{-1} *á esquerda e por*

b^{-m} á direita, donde obtemos:

$a^{-1}ab^mb^{-m} = a^{-1}a^{s^m}b^mb^{-m} \Longrightarrow eb^{m-m} = a^{s^m-1}b^{m-m} \Longrightarrow e = a^{s^m-1}$

Portanto, $s^m - 1$ é um múltiplo da ordem de a pelo Teorema 2.1 parte a) logo, $s^m \equiv 1(modn)$.

Ainda pela primeira parte do Teorema 2.1, $ba^u = a^{us}b$ Como $a^u \in \langle b \rangle$, temos que a^u comuta com b, o que implica em $a^ub = a^{us}b$; Podemos multiplicar ambos os lados por a^{-u} á esquerda e por b^{-1} á direita, donde obtemos;

$ebb^{-1} = a^{us-u}e \Longrightarrow e = a^{u(s-1)}$

Portanto, $u\,(s-1)$ é um múltiplo da ordem de a pelo Teorema 2.1 parte a); logo, $u\,(s-1) \equiv 0(modn)$.

($\Longleftarrow$) A volta da demonstração será aqui omitida, uma vez que se faz necessário conhecimentos prévios de produto semidireto de dois grupos.

(ii) Considere, agora, um grupo G' de ordem mn que possui dois elementos α e β tais que;

$$\begin{cases} G = \langle \alpha, \beta \rangle \\ \alpha^n = \alpha^u \\ \beta^m = e \\ \beta\alpha = \alpha^s\beta \end{cases}$$

Temos que $\mid G \mid = \mid G' \mid = mn$, logo, a aplicação $f : G \longrightarrow G'$ que foi definida por $f\left(a^ib^j\right) = \alpha^i\beta^j$ para $0 \leq i \leq n-1$ e $0 \leq j \leq m-1$ é uma bijeção e , da última parte do Teorema 2.1 podemos concluir que f é um isomorfismo. ■

Teorema 2.3 *Seja n, m e s números inteiros positivos e $u = 0$, o teorema 2.1 pode se resumir a:*

a) Existe um grupo G de ordem nm que possui elementos a, b tais que

$$\begin{cases} G = \langle a, b \rangle \\ a^n = e \\ b^m = e \\ ba = a^s b \end{cases},$$

se, e somente se, $s^m \equiv 1 (mod n)$.

b) Quando existir um grupo de ordem nm tal que satisfaça as condições acima, este é único a menos de isomorfismo.

Capítulo 3

Classificação dos grupos de ordem ≤ 11

Utilizaremos aqui os principais resultados obtidos nos capítulos anteriores e, a partir disso, classificar os grupos de ordem menor ou igual a 11, finalizando assim este trabalho.

Grupo de ordem 1

Temos que o único grupo dessa ordem é o $G = \{e\}$ e o único elemento de um grupo dessa ordem é o neutro.

Grupos de ordem p, com p = 2, 3, 5, 7 ou 11

Temos que, pelo corolário 1.4, todo grupo de ordem p, com p primo, é cíclico e simples. Portanto, se G é um grupo de ordem p prima então $G \simeq \mathbb{Z}_p$, pelo corolário 1.1

Grupo de ordem 4

Consideremos os grupos a seguir de ordem 4:

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} \text{ e } \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$$

Vamos mostrar que esses dois grupos são os únicos grupos de ordem 4, a menos de isomorfismos. Lembrando que esses grupos não são isomorfos

devido $\mathbb{Z}_4$ possuir elementos de ordem 4 e $\mathbb{Z}_2 \times \mathbb{Z}_2$ não. Seja G um grupo de ordem 4, se esse grupo possui um elemento de ordem 4, pelo corolário 1.1 temos que $G \simeq \mathbb{Z}_4$; caso contrário, pelo teorema de Lagrange, todos os seus elementos diferentes do elemento neutro são de ordem 2, uma vez que a ordem dos elementos deve dividir a ordem do grupo. Logo, pelo Lema 1.1, G é um grupo abeliano.

Como $\mid G \mid = 4$, descreveremos $G = \{e, a, b, c\}$ onde, $O(a) = O(b) = O(c) = 2$ com todos distintos.

Procuraremos então em sua tabela de multiplicação, o resultado das possíveis multiplicações de seus elementos. Ora:

$ab \neq e$, se não, $a = b^{-1}$, um absurdo já que $O(b) = 2$ implica $b^{-1} = b$;

$ab \neq a$ pois $ab = a \iff b = e$, absurdo;

$ab \neq b$ pois $ab = b \iff a = e$, absurdo;

Portanto, $ab = c$ e como o grupo é abeliano, $ba = c$.

Como também:

$ac \neq e$, se não, $a = c^{-1}$, um absurdo já que $O(c) = 2$ implica $c^{-1} = c$;

$ac \neq a$ pois $ac = a \iff c = e$, absurdo;

$ac \neq c$ pois $ac = c \iff a = e$, absurdo;

Portanto, $ac = b$ e como o grupo é abeliano, $ca = b$.

de forma semelhante, temos: $bc = a = cb$. Seja f a seguinte função:

$$\begin{aligned} f : \mathbb{Z}_2 \times \mathbb{Z}_2 &\to G \\ \left(\overline{0}, \overline{0}\right) &\mapsto e \\ \left(\overline{0}, \overline{1}\right) &\mapsto a \\ \left(\overline{1}, \overline{0}\right) &\mapsto b \\ \left(\overline{1}, \overline{1}\right) &\mapsto c \end{aligned}$$

Tendo que $\mathbb{Z}_2 \times \mathbb{Z}_2$ e G possuem elementos distintos, notamos que a função f é uma bijeção.

De fato, pois:

$$f\left[\left(\overline{0},\overline{0}\right)+\left(\overline{1},\overline{0}\right)\right]=f\left(\overline{1},\overline{0}\right)=a=e\cdot a=f\left(\overline{0},\overline{0}\right)\cdot f\left(\overline{1},\overline{0}\right)$$
$$f\left[\left(\overline{0},\overline{0}\right)+\left(\overline{0},\overline{1}\right)\right]=f\left(\overline{0},\overline{1}\right)=b=e\cdot b=f\left(\overline{0},\overline{0}\right)\cdot f\left(\overline{0},\overline{1}\right)$$
$$f\left[\left(\overline{0},\overline{0}\right)+\left(\overline{1},\overline{1}\right)\right]=f\left(\overline{1},\overline{1}\right)=c=e\cdot c=f\left(\overline{0},\overline{0}\right)\cdot f\left(\overline{1},\overline{1}\right)$$
$$f\left[\left(\overline{1},\overline{0}\right)+\left(\overline{0},\overline{1}\right)\right]=f\left(\overline{1},\overline{1}\right)=c=a\cdot b=f\left(\overline{1},\overline{0}\right)\cdot f\left(\overline{0},\overline{1}\right)$$
$$f\left[\left(\overline{1},\overline{0}\right)+\left(\overline{1},\overline{1}\right)\right]=f\left(\overline{0},\overline{1}\right)=b=a\cdot c=f\left(\overline{1},\overline{0}\right)\cdot f\left(\overline{1},\overline{1}\right)$$
$$f\left[\left(\overline{1},\overline{0}\right)+\left(\overline{1},\overline{0}\right)\right]=f\left(\overline{0},\overline{0}\right)=e=a\cdot a=f\left(\overline{1},\overline{0}\right)\cdot f\left(\overline{1},\overline{0}\right)$$
$$f\left[\left(\overline{0},\overline{1}\right)+\left(\overline{0},\overline{1}\right)\right]=f\left(\overline{0},\overline{0}\right)=e=b\cdot b=f\left(\overline{0},\overline{1}\right)\cdot f\left(\overline{0},\overline{1}\right)$$
$$f\left[\left(\overline{0},\overline{1}\right)+\left(\overline{1},\overline{0}\right)\right]=f\left(\overline{1},\overline{1}\right)=c=b\cdot a=f\left(\overline{0},\overline{1}\right)\cdot f\left(\overline{1},\overline{0}\right)$$
$$f\left[\left(\overline{0},\overline{1}\right)+\left(\overline{1},\overline{1}\right)\right]=f\left(\overline{1},\overline{0}\right)=a=b\cdot c=f\left(\overline{0},\overline{1}\right)\cdot f\left(\overline{1},\overline{1}\right)$$
$$f\left[\left(\overline{1},\overline{1}\right)+\left(\overline{1},\overline{1}\right)\right]=f\left(\overline{0},\overline{0}\right)=e=c\cdot c=f\left(\overline{1},\overline{1}\right)\cdot f\left(\overline{1},\overline{1}\right)$$

Devido $\mathbb{Z}_2 \times \mathbb{Z}_2$ ser abeliano, temos que:

$f\left[\left(\overline{a},\overline{b}\right)+\left(\overline{c},\overline{d}\right)\right]=f\left[\left(\overline{c},\overline{d}\right)+\left(\overline{a},\overline{b}\right)\right], \forall \left(\overline{a},\overline{b}\right),\left(\overline{c},\overline{d}\right)\in \mathbb{Z}_2\times\mathbb{Z}_2$

Contudo, temos que a função f é um homomorfismo e, logo, um isomorfismo. Portanto, a menos de isomorfismo, $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ são os únicos grupos de ordem 4.

Grupo de ordem 6

Vimos anteriormente que $\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e S_3 são grupos de ordem 6 onde não são isomorfos uma vez que $\mathbb{Z}_6$ é um grupo abeliano e S_3 não é. Vamos mostrar agora que esses são os únicos grupos de ordem 6 a menos de isomorfismos.

Tomenos então um grupo G qualquer de ordem 6.

Pelo teorema 1.5, temos que G possue um elemento α, com $\mid \alpha \mid = 3$

e um elemento β onde $\mid \beta \mid = 2$ daí, α, $\alpha^2 \in G$, $\beta \in G$ como também os elementos $\alpha\beta$ e $\alpha^2\beta$. Devido $\mid G \mid = 6$, vemos que $G = \{e, \alpha, \alpha^2, \beta, \alpha\beta, \alpha^2\beta\}$, daí;

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

Vendo que $\mid \langle \alpha \rangle \mid = 3$, então $(G : \langle \alpha \rangle) = 2$, portanto $\langle \alpha \rangle \triangleleft G$, assim $\beta\alpha\beta^{-1} = \beta\alpha\beta \in \langle \alpha \rangle \Rightarrow \beta\alpha\beta = \alpha$ ou $\beta\alpha\beta = \alpha^2$ então $\beta\alpha = \alpha\beta$ ou $\beta\alpha = \alpha^2\beta$.

Temos, disso tudo, que existem duas possibilidades:

$$(i) \begin{cases} \mid G \mid = 6 = 3 \cdot 2 \\ G = \langle \alpha, \beta \rangle \\ \alpha^3 = e \\ \beta^2 \ = e \\ \beta\alpha = \alpha\beta \end{cases},$$

$$(ii) \begin{cases} \mid G \mid = 6 = 3 \cdot 2 \\ G = \langle \alpha, \beta \rangle \\ \alpha^3 = e \\ \beta^2 \ = e \\ \beta\alpha = \alpha^2\beta \end{cases}$$

Pela parte (ii) do Teorema 2.2, temos em cada um dos casos, no máximo um grupo, a menos de isomorfismo, satisfazendo as condições. Devemos então saber se existem de fato tais grupos. Existem sim, basta tomar $G = \mathbb{Z}_6$ para o caso (i) e $G = S_3$ no caso (ii).

Observemos que $\mathbb{Z}_2 \times \mathbb{Z}_3$ também satisfaz o caso (i) e, pela unicidade, temos que $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Grupo de ordem 8

Consideremos os grupos de ordem 8 a seguir:

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ e } D_4$$

Esses grupos não são isomorfos entre si e são compostos pelos seguintes elementos:

$$\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\},$$

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

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 =$$
$$\{(\overline{0}, \overline{0}, \overline{0}), (\overline{0}, \overline{0}, \overline{1}), (\overline{0}, \overline{1}, \overline{1}), (\overline{1}, \overline{1}, \overline{1}), (\overline{1}, \overline{0}, \overline{0}), (\overline{1}, \overline{1}, \overline{0}), (\overline{1}, \overline{0}, \overline{1}), (\overline{0}, \overline{1}, \overline{0})\}$$

$$D_4 = \{a_0 = e, a_1, a_2, a_3, a_4a_5, a_6, a_7\}$$

com;

$$a_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, a_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix},$$
$$a_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, a_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, a_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$
$$a_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, a_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Observa-se que D_4 não é abeliano, notando que:

$$a_1 * a_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ e } a_4 * a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

ou seja, $a_1 * a_4 \neq a_4 * a_1$.

Observemos que

$\circ$ $\mathbb{Z}_8$ possui 4 elementos de ordem 8, $\left(\overline{1}, \overline{3}, \overline{5}, \overline{7}\right)$, e que $\mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e D_4 não possuem tais elementos, o que nos garante a afirmação do não isomorfismo entre $\mathbb{Z}_8$ e o restante dos grupos citados.

$\circ$ $\mathbb{Z}_4 \times \mathbb{Z}_2$ possui 4 elementos de ordem 4 $\left(\left(\overline{1}, \overline{0}\right), \left(\overline{1}, \overline{1}\right), \left(\overline{3}, \overline{0}\right), \left(\overline{3}, \overline{1}\right)\right)$, enquanto que , $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ possui apenas elementos de ordem 2 e que D_4 só possui 2 elementos de ordem 4 daí, podemos afirmar que $\mathbb{Z}_4 \times \mathbb{Z}_2$ não é isomorfo a nenhum dos grupos citados.

$\circ$ $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ tem ao todo, 8 elementos de ordem 2 e D_4 apenas 5 desses elementos, assim, esses dois grupos são não isomorfos.

Denotaremos agora o grupo Q_3, o grupo dos quatérnios que, juntamente com os 4 grupos citados anteriormente, são os únicos de ordem 8, a menos de isomorfismos assim, Q_3 que é dado por;

$$Q_3 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}$$

Com $i \in \mathbb{C}$ tal que $i^2 = -1$ e

$$A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e,\ C = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ D = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix},\ E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ F = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ G = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

$$H = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix},$$

Devemos observar que $\mid Q_3 \mid = 8$, pois todos os seus elementos são distintos, vejamos:

$$C^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A$$

$$C^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = D$$

$$C^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

$$E^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A$$

$$E^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = F$$

$$E^4 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$$

$$CE = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = G$$

$$EC = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = H$$

$$C^3E = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = H$$

Logo:

$$\begin{cases} \mid Q_3 \mid = 8 \\ Q_3 = \langle A, B \rangle \\ C^4 = e \\ E^2 = C^2 \\ EC = C^3E \end{cases},$$

Portanto, pela parte (b) do teorema 2.3, temos que Q_3 tem características das relações acima. Ainda notamos que Q_3 não é isomorfo aos grupos $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ e precisamos verificar que D_4 e Q_3 também não são, notando que Q_3 tem apenas 1 elemento de ordem 2 enquanto D_4 possui 5 elementos com essa ordem. Isto está claro quando, tomando um grupo G de ordem 8, pelo Teorema de Lagrange, as ordens possíveis para os elementos de $G - \{e\}$ são 2, 4 e 8.

(Caso 1) G possui um elemento de ordem 8.

Seja $\delta \in G$ tal que $O(\delta) = 8$; logo $G = \langle \delta \rangle$ e $G \cong \mathbb{Z}_8$.

(Caso 2) G não tem nenhum elemento em que sua ordem seja 8.

Logo, as ordens possíveis dos elementos de G diferentes de e são 2 e 4. Aqui, dividiremos o caso 2 em duas partes:

(Caso 2.1) G não possui nenhum elemento de ordem 4.

Assim, todos os elementos de G diferentes do elemento neutro, são de ordem 2 e, portanto, o grupo G é abeliano. Agora, seja $a \neq e$, como $O(a) = 2$ temos que $H = \langle a \rangle$ é um subgrupo de G. Tome $b \in G - H$; então $K = \{e, a, b, ab\}$ é também um subgrupo de G. Tome $c \in G - K$; temos:

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

Logo, a função abaixo é um isomorfismo de grupos.

$$\varphi; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$$
$$\left(\overline{i}, \overline{j}, \overline{k}, \right) \mapsto a^i b^j c^k$$

(Caso 2.2) G possui um elemento de ordem 4.

Considere $a \in G$ um elemento de ordem 4 e seja $H = \langle a \rangle$. Tome $b \in G - H$ e considere o subgrupo H de G gerado por a e por b, ou seja, $H = \langle a, b \rangle$, com b não pertence ao subgrupo H, temos que $\mid H \mid > 4$ e, pelo Teorema de Lagrange, $\mid H \mid$ divide 8; portanto $H = G = \langle a, b \rangle = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$.

Temos que b^2 não pertence a H pois, b^2 não pertence a $\{b, ab, a^2b, a^3b\}$, também temos ba não pertence a $\{e, a, a^2, a^3\}$, provando assim que:

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

Vejamos agora as possibilidades para u e s $\in \{o, 1, 2, 3\}$. Primeiramente, $O(bab^{-1}) = O(a) = 4$ assim, $s = 1$ ou $s = 3$. Mas, b^2 não pertence a $\{a, a^3\}$, pois caso contrário a $O(b^2) = 4$ o que implica em $O(b)$ seria um multiplo de 4 e consequentimente $O(b) = 8$ (absurdo pois, por hipótese, G não possui elementos de ordem 8) ou que $O(b) = 4$ (absurdo, pois nesse caso teríamos $O(b^2) = 2$.

Portanto, $u = 0$ ou $u = 2$ e como ja foi visto $s = 1$ ou $s = 3$.

Considerando $u = 0$, temos dois casos correspondentes a $s = 1$ e $s = 3$:

$$(iii)\begin{cases} \mid G \mid = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = e \\ ba = ab \end{cases},$$

$$(iv)\begin{cases} \mid G \mid = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = e \\ ba = a^3b \end{cases},$$

Daí, pela segunda parte do Teorema 2.2, em cada um dos casos, vamos ter no máximo um grupo, a menos de isomorfismo, satisfazendo as condições indicadas. Podemos nos perguntar se existem tais grupos, de fato? Veremos a seguir que esses grupos existem.

Basta apenas tomar $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ no caso (iii) e $G = D_4$ no caso (iv).

Considerando $u = 2$, temos dois casos correspondentes a $s = 1$ e $s = 3$:

$$(v)\begin{cases} \mid G \mid = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = a^2 \\ ba = ab \end{cases},$$

$$(vi)\begin{cases} \mid G \mid = 8 \\ G = \langle a, b \rangle \\ a^4 = e \\ b^2 = a^2 \\ ba = a^3 b \end{cases},$$

Então, pela segunda parte do Teorema 2.2, em cada um dos casos, vamos ter no máximo um grupo, a menos de isomorfismo, satisfazendo as condições indicadas.Veremos a seguir que esses grupos também existem. Basta apenas tomar $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ no caso (v) e $G = Q_3$ no caso (vi). Portanto,

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_4 \text{ e } Q_3$$

a menos de isomorfismo, são os únicos cinco grupos de ordem 8.

Grupo de ordem 9

Tomenos, a seguir, os seguintes grupos:

$$\mathbb{Z}_9 \text{ e } \mathbb{Z}_3 \times \mathbb{Z}_3$$

que são de ordem 9. Eles não são isomorfos pois, $\mathbb{Z}_9$ possui elementos de ordem 9, enquanto que $\mathbb{Z}_3 \times \mathbb{Z}_3$ não possui tais elementos. Esses dois grupos são compostos pelos elementos seguintes:

$$\mathbb{Z}_9 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\}$$

$$\mathbb{Z}_3 \times \mathbb{Z}_3 =$$
$$\{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2}), (\overline{2}, \overline{0}), (\overline{2}, \overline{1}), (\overline{2}, \overline{2})\}$$

Vamos mostrar agora que esses dois grupos são os únicos grupos, a menos de isomorfismos, de ordem 9.

Consideremos um grupo G que não seja cíclico e, pelo Teorema de Lagrange, todos seus elementos diferentes do neutro, tem ordem 3. Sejam então, $e \neq \alpha \in G$ e $\beta \in G - \langle\alpha\rangle$. Então, $\langle\alpha\rangle = \{\alpha, \alpha^2, \alpha^3\} \in G$ e $\langle\beta\rangle = \{\beta, \beta^2, \beta^3\} \in G$ e $\alpha^i \neq \beta^j, \forall\ i,\ j \in \{1, 2\}$. Daí, por razões elementares, temos que

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

Portanto,

$$\begin{cases} \mid G \mid = 9 \\ G = \langle\alpha, \beta\rangle \\ \alpha^3 = e \\ \beta^3 = e \end{cases},$$

Mas quem é o produto $\beta\alpha$? Temos que $\beta\alpha$ não pertence a $\{e, \alpha, \alpha^2, \beta, \beta^2\}$. Analisaremos os casos restantes:

$\beta\alpha = \alpha\beta, \beta\alpha = \alpha^2\beta, \beta\alpha = \alpha\beta^2, \beta\alpha = \alpha^2\beta^2$, Observando ainda que, pela segunda parte do Teorema 2.2, temos no máximo um grupo a menos de isomorfismo em cada um dos casos.

(a) Caso $\beta\alpha = \alpha\beta$, basta tomar $G = \mathbb{Z}_3 \times \mathbb{Z}_3$.

(b) Caso $\beta\alpha = \alpha^2\beta$ não existe tal grupo, observando a primeira parte do Teorema 2.2, onde $2^3 = 8 \ncong 1 mod 3$.

(c) Caso $\beta\alpha = \alpha\beta^2$ Também não existe este grupo, pois, tomando $A = \beta^2$ e $B = \alpha$, teríamos $G = \langle A,\ B\rangle$ com $A^3 = e, B^3 = e, BA = \alpha\beta^2 = \beta\alpha = A^2B$, um absurdo pois, $2^3 = 8 \ncong 1(mod 3)$.

(d) Caso $\beta\alpha = \alpha^2\beta^2$ não existe, pois senão, teríamos $(\alpha\beta)^2 = \alpha\beta\alpha\beta = \alpha\alpha^2\beta^2\beta = e$, um absurdo, quando sabemos que $\alpha\beta$ tem ordem 3.

Portanto, a menos de isomorfismo, $\mathbb{Z}_9$ e $\mathbb{Z}_3 \times \mathbb{Z}_3$são os únicos grupos de

ordem 9.

Grupo de ordem 10

Seja G um grupo qualquer de ordem 10.

Pelo Teorema de Cauchy,G possui um elemento α onde $O(\alpha) = 5$ e um elemento β tal que $O(\beta) = 2$. Daí:

$$G = \{e, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta, \alpha^4\beta\} = \langle \alpha, \beta \rangle$$

Surge então a questão: Qual o produto $\beta\alpha$?

Ora, por razões elementares, $\beta\alpha$ não pertence a $\{e, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta\}$ então, pelo Teorema 2.2 $\beta\alpha \neq \alpha^2\beta$ pois $2^2 = 4 \ncong 1(mod5)$, e que $\beta\alpha \neq \alpha^3\beta$ pois $3^2 = 9 \ncong 1(mod5)$ Restam então duas possibilidades:

$$(1) \begin{cases} \mid G \mid = 10 = 5 \cdot 2 \\ G = \langle \alpha, \beta \rangle \\ \alpha^5 = e \\ \beta^2 = e \\ \beta\alpha = \alpha\beta \end{cases}, \qquad (2) \begin{cases} \mid G \mid = 10 = 5 \cdot 2 \\ G = \langle \alpha, \beta \rangle \\ \alpha^5 = e \\ \beta^2 = e \\ \beta\alpha = \alpha^4\beta \end{cases},$$

Daí, pela segunda parte do Teorema 2.2, teremos no máximo um grupo, a menos de isomorfismo, que satisfaça as condições. Para notar que tais grupos existem de fato, basta então, tomar $G = \mathbb{Z}_10$ no caso (1) e no caso (2) $G = D_5$ (grupo das simetrias espaciais do pentágono regular que consiste da identidade, das rotações de ângulos $2\pi/5, 4\pi/5, 5\pi/5, 8\pi/5$

e das reflexões espaciais em torno das cinco bissetrizes). É fácil notar que o grupo $\mathbb{Z}_2 \times \mathbb{Z}_5$ também consegue satisfazer as condições do caso (1) e então, portanto, pela unicidade estabelecida na segunda parte do Teorema 2.2 temos que $\mathbb{Z}_2 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{10}$.

Desta forma, conclui-se que :

$$\mathbb{Z}_{10} \text{ e } G = D_5$$

são os únicos grupos de ordem 10, a menos de isomorfismo.

Conclusão

A álgebra é de fundamental importância na matemática e em diversas outras áreas diferentes , como na Física com suas aplicações, em várias sub áreas da própria matemática como na Álgebra Computacional, na compreensão da construção de determinados conjuntos, Conseguimos com isso notar a importância dessa desta área e a sua contribuição no avanço de outras grandes áreas da ciência. No processo de construção desse trabalho foi possível compreender de forma mais aprofundada e detalhada o caminho para a classicação de grupos, a importância do Teorema de Lagrange, Fermat e Cauchy no decorrer desse estudo e das estruturas algébricas. Alcançamos o objetivo deste de classificar os grupos de ordem ≤ 11 e, por tudo isso, esse trabalho pôde ser concluído.

Referências Bibliográficas

[1] COELHO, Flávio U. LOURENÇO, Mary L. *Um Curso de Álgebra Linear*. São Paulo, Editora da Universidade de São Paulo, 2001.

[2] EVES, Howard. *Introdução à história da matemática.* tradução: Hygino H. Domingues. - Campinas, SP, Editora da UNICAMP, 2004.

[3] STEINBRUCH, Alfredo. *Álgebra Linear I.* 2ª ed. São Paulo, Pearson Makron Books, 1987.

[4] FRALEIGH, J. B. *A First Course in Abstract Algebra,* 5th Edition, Seventh Edition, 2002.

[5] HYGINO, D.; GELSON, I. *Álgebra Moderna,* 4ª ed. São Paulo: editora atual, 2003.

[6] GARCIA, A.; YVES, L. *elementos de álgebra,* Rio de Janeiro: IMPA, 1988.

[7] GONÇALVES, A. *Introdução à Algebra,* 5ª ed. Rio de Janeiro: IMPA, 2011.

[8] VIEIRA, V.L. *Álgebra Abstrata para Licenciatura,* 1ª ed. São Paulo - SP, Editora co-edição, 2013.