UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Pró-Reitoria de Pesquisa e Pós-Graduação
Departamento de Matemática Pura e Aplicada - CCENS

RELATÓRIO DE INICIAÇÃO CIENTÍFICA

Uma introdução à teoria de grupos com aplicações

Discente: *Gabriel de Souza Cruz*
Orientador: *Prof. Dr. Victor do Nascimento Martins (DMPA - UFES)*

SETEMBRO/2023

SUMÁRIO

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Pró-Reitoria de Pesquisa e Pós-Graduação
Departamento de Matemática Pura e Aplicada - CCENS

RESUMO

UMA INTRODUÇÃO À TEORIA DE GRUPOS COM APLICAÇÕES

Este trabalho possui o intuito de apresentar elementos primordiais da Teoria Básica de Grupos, trazendo as principais definições, teoremas e exemplos, apresentando de forma detalhada algumas características dessa estrutura. No escopo desse trabalho comentamos alguns resultados acerca de grupos específicos tais como os grupos cíclicos, grupos finitamente gerados, grupo das permutações e a classificação de grupo de ordem pequena, dentre outros. E por fim apresentamos o software GAP, que nos é útil para o estudo de estruturas algébricas, e mais especificamente, mostramos aplicações práticas do programa em relação aos fundamentos teóricos estudados, com o intuito de mostrar a relevância dessa ferramenta nos estudos e pesquisas de cunho algébrico.

Palavras-chave: Teoria de Grupos. Grupos finitos. Grupos cíclicos. GAP.

INTRODUÇÃO

A Teoria de Grupos surgiu como objeto de estudo das permutações e possuía o fundamento em realizar investigações acerca de equações polinomiais. Sabia-se que equações de até quarto grau eram solúveis por meio de radicais, a partir disso, estudos vinham em busca de analisar se equações de quinto grau eram também solúveis através de expressões radicias e esse objeto de estudo foi alvo de pesquisa de diversos matemáticos, onde em 1824, através de trabalhos dos matemáticos Lagrange, P. Ruffini e Abel comprovou-se que as equações de quinto grau não possuíam solução através de expressões radicais, mas a centralidade da temática ainda estava sem resposta, pois não se conseguia definir quando uma equação polinomial de quinto ou maior grau era ou não solúvel por meio de radicais. Tal resposta foi trazida a academia através de Liouville, no ano de 1843, quando apresentou trabalhos do matemático Évarist Galois que continham a solução, isto é, determinava quando uma equação de maior ou igual que o quinto grau era solúvel.

Por outro lado, uma linha de pesquisa em álgebra seguia uma característica bastante diferente, de modo que na Inglaterra, diversos pesquisadores matemáticos defendiam que a álgebra poderia tomar estruturações axiomáticas, visto que possuía alicerces bastante sólidos, assim como a Geometria. Nessa vertente ideológica, Arthur Cayley descreveu a primeira definição abstrata de **Grupo** em um trabalho no ano de 1854. Foi uma definição um pouco diferente da usada hoje, sendo elas equivalentes. A definição que usamos hoje foi descrita por Walther von Dyck, no ano de 1882, onde diz-se que um conjunto não vazio G, com uma operação * é um **Grupo** se esta operação for associativa, se existir elemento neutro para essa operação em G e se para todo elemento em G existir um elemento inverso. Se a operação ainda for comutativa, dizemos que o grupo é **abeliano**.

No presente trabalho, introduzimos a Teoria básica de Grupos e para isso dividimos o trabalho em 3 capítulos. No primeiro, trouxemos os principais resultados acerca da Teoria

de Grupos, que são as definições, Teoremas e exemplos acerca da temática, seguindo as referências [3] e [4].

No segundo capítulo trouxemos exemplos característicos do estudo da Teoria de Grupos, tais como: Grupos Cíclicos, Grupos Finitos Gerados por Dois Elementos a e b onde $ab = a^s b$, Grupo das Permutações e Classificação de Grupo de Ordem Pequena, mostrando algumas características específicas de cada estrutura, nesta seção utilizamos as referências [1] e [3].

No terceiro capítulo objetivamos apresentar uma aplicação de tal estrutura algébrica utilizando o software GAP, visualizando alguns tópicos fundamentais através de códigos descritos em seu sistema, pois por meio do GAP pode-se visualizar, de forma direta, resultados em tal estrutura, que por muitas vezes, são bastante abstratos. Nesse capítulo seguimos fielmente a referência [1].

CAPÍTULO 1

TEORIA BÁSICA DE GRUPOS

Como nosso primeiro capítulo queremos introduzir os conceitos primordiais que estão relacionados a teoria de Grupos, trazendo as principais definições voltadas a temática e também destacar alguns elementos chaves para desenvolvimento da parte teórica e prática pertencente ao escopo do trabalho, aqui serão retratados pontos importantíssimos que são a definição e exemplos de grupos, subgrupos, subgrupos normais, grupos quocientes e homomorfismos de grupos, trazendo algumas demonstrações dos principais teoremas e proposições acerca de tais tópicos. Tal capítulo traz conceitos descritos e desenvolvidos por grandes matemáticos tais como Galois, Abel, dentre outros. As principais referências para o desenvolvimento do capítulo são [3], [4].

1.1 Definição e exemplos

Um **grupo** G é um conjunto não vazio munido de uma operação

$$* : G \times G \to G$$

$$(a, b) \mapsto a * b,$$

satisfazendo as seguintes propriedades:

i) **Associatividade:**

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

ii) **Elemento neutro:**

Existe $e \in G$ tal que

$$e * a = a * e = a, \quad \forall\ a \in G$$

iii) Elemento inverso:
$\forall\ g \in G$ existe $g^{-1} \in G$ tal que

$$g * g^{-1} = e = g^{-1} * g$$

Proposição 1.1 *Seja G um grupo com a operação $*$, onde e é o elemento neutro, então:*

a) O elemento neutro é único;

b) O elemento inverso é único;

Demonstração:

a) Sejam e, e_1 elementos neutros de G, ou seja:
$e = e * e_1 = e_1 * e \quad$ e $\quad e_1 = e_1 * e = e * e_1$ logo $e = e_1$;

Observação 1.1 *É usual denotarmos o único elemento neutro de G por e.*

b) Sejam $g \in G$ e $g_1, g_2 \in G$ elementos inversos de g, daí
$g_1 = g_1 * e = g_1 * (g * g_2) = (g_1 * g) * g_2 = e * g_2 = g_2$;

Observação 1.2 *É usual denotarmos o único inverso de $g \in G$ por g^{-1}.*

■

Definição 1.1 *Um grupo G é denominado comutativo (ou abeliano) se*

$$g * h = h * g,\ \forall\ g, h \in G$$

Exemplo 1.1 *$(\mathbb{Z}, +)$ é um grupo abeliano infinito.*

Exemplo 1.2 *$(\mathbb{C}, +)$ e $(\mathbb{R}, +)$ são grupos aditivos abelianos.*

Exemplo 1.3 *Considere um conjunto G não vazio e defina*

$$G' = \{f : G \to G, f \text{ é bijetora}\}.$$

A operação que definiremos para G' será a composição de funções, isto é:

$$\begin{aligned} \circ : G' \times G' &\to G' \\ (g, f) &\mapsto g \circ f \end{aligned}$$

Temos que $(G', \circ)$ é um grupo onde seu elemento neutro é a aplicação identidade dada por

$$I_G : G \to G$$

$$x \mapsto x.$$

Esse grupo G' que acabamos de definir é chamado ***grupo das permutações do conjunto*** *G. Se $G = 1, 2, 3, ..., n$, denotamos das permutações de G por G_n e tal grupo possui $n!$ elementos.*

Usualmente, denotamos os elementos do grupo G_n da seguinte forma:

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

Vamos considerar o seguinte exemplo

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

Temos que $f(1) = 2, f(2) = 3, e f(3) = 1$. Podemos utilizar a notação cíclica (123), para representar essa permutação, onde o elemento seguinte é a imagem do anterior. Temos que o grupo G_n é formado pelos seguintes elementos:

$$e_G = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \; f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \; f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \; f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \; f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

1.1.1 Subgrupos

Considerando G um grupo e H um subconjunto não vazio de G. Diz-se que H é **subgrupo** de G se e só se H for um grupo com a operação herdada de G.

Proposição 1.2 *Seja $(G, *)$ um grupo com elemento neutro e, e H um subconjunto não vazio de G. H é subgrupo de G se, e somente se, são válidas as seguintes condições*

i) $e \in H$;

ii) $\forall h_1, h_2 \in H$ *tem-se* $h_1 * h_2 \in H$;

iii) $\forall h \in H$ *tem-se* $h^{-1} \in H$;

Demonstração:
($\Rightarrow$) De fato, segue imediatamente das definições de grupo, da unicidade do elemento neutro e da unicidade do inverso de cada elemento do grupo G.

($\Leftarrow$) Basta observar que a condição (ii) (H é fechado para a operação de G) mostra que a operação de G induz a operação em H e essa operação será também associativa já que a operação é associativa em G.

■

Se H for subgrupo do grupo G então denota-se $H \leq G$.

Exemplo 1.4 *Se G é grupo, então $\{e\}$ e G são subgrupos de G, ditos* ***subgrupos triviais****.*

Exemplo 1.5 *Seja $n \in \mathbb{Z}$. Temos que $(n\mathbb{Z}, +)$ é subgrupo de $(\mathbb{Z}, +)$.*

Exemplo 1.6 *Seja G um grupo e $x \in G$. Então $C_g(x) = \{y \in G : y * x = x * y\}$ é um subgrupo de G denominado* ***centralizador de*** *x* ***em*** *G.*

1.2 Classes laterais e Teorema de Lagrange

A priori, consideremos G um grupo e $H \leq G$. Nesta seção, iremos definir uma relação de equivalência em G que dependerá do subgrupo H fixado e estudaremos as classes de equivalência dessa relação.

Para cada par $x, y \in G$ dizemos que x é congruente a y módulo H se $x * y^{-1} \in H$, isto é,

$$x \equiv y(modH) \Leftrightarrow x * y^{-1} \in H.$$

A relação definida acima é uma relação de equivalência. De fato,

i) $x \equiv x(modH)$, para todo $x \in G$ pois $e = x * x^{-1} \in H$. Logo a relação é simétrica;

ii) Se $x \equiv y(modH)$ então $y \equiv x(modH)$, pois se $x * y^{-1} \in H$ então $x * y^{-1} = h_1 \in H$. Daí, $h_1^{-1} = y * x^{-1} = (x * y^{-1})^{-1} \in H$. Logo a relação é reflexiva;

iii) Se $x \equiv y(modH)$ e $y \equiv z(modH)$ então $x \equiv z(modH)$ pois, $x * y^{-1} \in H$ e $y * z^{-1} \in H$. Logo $(x * y^{-1}) * (y * z^{-1}) = (x * z^{-1}) \in H$ e daí que a relação é transitiva.

As classes de equivalência da relação definida acima são dadas por

$$\overline{x} = \{y \in G : y \equiv x(modH)\}.$$

Ou seja, se $y \in \overline{x}$ então $y * x^{-1} \in H$, isto é, $y * x^{-1} = h \in H$ e consequentemente $h * x = y$. Segue que

$$\overline{x} = \{h * x : h \in H\} = Hx,$$

onde Hx será denominada **uma classe lateral a direita de H em G** e de forma análoga constrói-se o conjunto $xH = \{x * h : h \in H\}$ denominado **uma classe lateral a esquerda de H em G**.

O conjunto quociente, que contém todas as classes laterais a direita da relação dada, será representado por

$$G/H = \{Hx : \ x \in G\}$$

e de forma análoga

$$G/H = \{xH : \ x \in G\}$$

descreve o conjunto para as classes laterais a esquerda.

Proposição 1.3 *Todas as classes laterais de H em G possuem a mesma cardinalidade de H.*

Demonstração:

Note que a função

$$f : H \to Hx$$
$$h \mapsto hx$$

é claramente sobrejetiva e tomando $h_1, h_2 \in H$ de modo que

$$h_1 * x = h_2 * x$$

logo

$$h_1 = h_2$$

e com isso temos que a função é também injetiva, ou seja, é bijetiva e daí $|H| = |Hx|$.

■

Dado um grupo G, dizemos que a **ordem** de G é n e escrevemos $|G| = n$ se G possui exatamente n elementos. Neste caso, dizemos que G é um grupo finito. No caso de grupos finitos um importante resultado, o Teorema de Lagrange, garante que qualquer subgrupo de um grupo finito tem ordem que divide a ordem do grupo.

Teorema 1.1 (Teorema de Lagrange) *Se G é um grupo finito e H é um subgrupo de G então $|H|$ é um divisor de $|G|$, ou seja, a ordem de H é um divisor da ordem de G.*

Demonstração:

Considerando G um grupo finito e definida sobre G a relação de equivalência $\equiv (modH)$ temos que o conjunto quociente G/H é finito, daí

$$G/H = n \qquad \text{e} \qquad G/H = \{Hx_1, Hx_2, ..., Hx_n\}$$

Observe que $G = Hx_1 \dot{\cup} Hx_2 \dot{\cup} ... \dot{\cup} Hx_n$ e com isso $|G| = |Hx_1| + |Hx_2| + ... + |Hx_n|$
Segue da proposição anterior que $|G| = n|H|$, e portanto segue o resultado.

■

1.3 Subgrupos normais e grupos quocientes

Sejam G um grupo e H um subgrupo de G. Para cada $g \in G$, define-se a função γ_g (**conjugação pelo elemento** $g \in G$) por

$$\gamma_g : G \to G$$
$$x \mapsto \gamma_g(x) = g^{-1} * x * g$$

Note que $\gamma_g(H) = \{\gamma_g(h) : h \in H\} = \{g^{-1} * h * g : h \in H\}$. Vamos denotar a conjugação de um elemento h por g por h^g, isto é

$$\gamma_g(h) = h^g = g^{-1} * h * g.$$

Daí faz sentido denotarmos por H^g ou $g^{-1} * H * g$ o conjunto $\gamma_g(H) = \{\gamma_g(h) : h \in H\}$.

Vejamos que H^g é um é um subgrupo de G:

i) $e = e^g \in H^g$;
   De fato, $\gamma_g(e) = g^{-1} * e * g = e$

ii) $h^g * h_1^g \in H^g, \ \forall \ h^g, h_1^g \in H^g$;
   De fato $h^g * h_1^g = (g^{-1} * h * g) * (g^{-1} * h_1 * g) = g^{-1} * (h * h_1) * g \in H^g$

iii) $(h^g)^{-1} \in H^g, \ \forall \ h^g \in H^g$;
   De fato, dado que $h^g \in H^g$ como $h \in H$, $h^{-1} \in H$ logo $(h^{-1})^g \in H^g$. Note que $(h^g) * (h^{-1})^g = (g^{-1} * h * g) * (g^{-1} * h^{-1} * g) = e$, ou seja, $(h^{-1})^g = (h^g)^{-1} \in H^g$

Observe que a função γ_g transforma subgrupos de G em subgrupos de G.

Definição 1.2 *Diz-se que um subgrupo H em G é* ***normal*** *se $\gamma_g(H) = H^g \subseteq H, \ \forall g \in G$.*

Note que $H^g \subseteq H$, para todo $g \in G$. Portanto, se H é um subgrupo normal de G, então $H^g = H$, para todo $g \in G$.

Se H é um subgrupo normal de G denotaremos "$H \trianglelefteq G$".

Exemplo 1.7 *$\{e\}$ e G são subgrupos normais do grupo G;*

Exemplo 1.8 *Se G é um grupo abeliano então qualquer subgrupo H de G é normal.*

Definição 1.3 *Diz-se que um grupo $G \neq \{e\}$ é **simples** se e só se os únicos subgrupos normais de G são $\{e\}$ e G.*

Proposição 1.4 *Seja G um grupo, então:*

i) $N \trianglelefteq G \Leftrightarrow Ng = gN, \forall g \in G$ *onde* $gN = \{gn : n \in \mathbb{N}\}$ *é uma classe lateral (à esquerda) de N em G;*

ii) $N, N_1 \trianglelefteq G \Rightarrow N \cap N_1 \trianglelefteq G$;

iii) $H \leq G$ *e* $N \trianglelefteq G \Rightarrow HN = \{h * n : h \in H, n \in N\}$ *é um subgrupo de G*;

iv) $N \trianglelefteq G, N_1 \trianglelefteq G \Rightarrow N * N_1 \leq G$;

v) $H \leq G, N \trianglelefteq G \Rightarrow H \cap N \trianglelefteq H$.

Demonstração:

i) Basta observar que $N^g = g^{-1} * N * g = N \Leftrightarrow Ng = gN, \forall g \in G$.

ii) Se x $\in N \cap N_1$ e $g \in G$ então $x \in N$ e $X \in N_1$. Assim , $x^g \in N^g = N$ e $x^g \in N_1^g = N_1$, ou seja, $x^g \in N \cap N_1$. Assim $(N \cap N_1)^g = N \cap N_1, \forall g \in G$.

iii) Seja $H \leq G$ e $N \trianglelefteq G$, queremos provar que $HN = \{h * n : h \in H, n \in N\}$ é um subgrupo de G.
De fato,

a) $e \in H$, $e \in N \Rightarrow e * e = e \in HN$.

b) Considerando h_0n_0 e $h_1n_1 \in HN \Rightarrow (h_0n_0)(h_1n_1) = h_0(h_1h_1^{-1})(n_0h_1)n_1 \Rightarrow (h_0n_0)(h_1n_1) = (h_0h_1)(h_1^{-1}n_0h_1)n_1$, e se denotarmos $h = h_0h_1, n = n_0^{h_1} * n_1$ teremos $h \in H, n_0^{h_1} * n_1 \in N^{h_1} = N$ e $n = n_0^{h_1} * n_1$, assim

$$(h_0n_0)(h_1n_1) = hn \in HN.$$

c) Tomando $r = hn \in HN \Rightarrow r^{-1} = n^{-1}h^{-1} = h^{-1}(h * n^{-1} * h^{-1})$, mas $h^{-1} \in H$ e $h * n^{-1} * h^{-1} = (n^{-1})^{h^{-1}} \in N^{h^{-1}} = N$, ou seja, $r^{-1} \in HN$.

iv) Basta observar que $\forall g \in G$ temos

$$(NN_1)^g = g^{-1} * (NN_1)g = (g^{-1}Ng)(g^{-1}N_1g) = N^gN_1^g$$

e como $N^g = N$ e $N_1^g = N_1, \forall g \in G$, segue que $(NN_1)^g = NN_1, \forall g \in G$.

v) Considerando $x \in H \cap N$ e $h \in H \Rightarrow x \in N$ e $x^h \in N^H = N$, como $x, h \in H$ segue imediatamente que $x^h \in H \cap N, \forall h \in H$.

■

Vamos utilizar a relação de equivalência definida anteriormente para trabalhar com o conjunto quociente daquela relação que poderemos, sob certa circunstância, muní-lo com estrutura de grupo. Este será chamado **grupo quociente**.

Seja G um grupo e $N \trianglelefteq G$. Sabe-se que

$$x, y \in G,\ x \equiv y(modN) \Leftrightarrow x * y^{-1} \in N$$

define uma relação de equivalência sobre G de modo que $G/N = \{\overline{g} : g \in G\}$ é o conjunto quociente de G por N e $\overline{g} = Ng = \{n * g : n \in N\}$ são as classes de equivalência da relação $\equiv (modN)$.

A proposição abaixo definirá uma operação no conjunto das classes G/N de modo que G/N seja um grupo com essa operação atribuída, sendo esse denominado **grupo quociente**.

Proposição 1.5 *Seja G um grupo e $N \trianglelefteq G$ então para quaisquer $x, y \in G$,*

$$\overline{x} * \overline{y} = \overline{x * y}$$

define uma operação no conjunto quociente G/N. Com essa operação, G/N é um grupo.

Demonstração:

Primeiramente provar-se-á que a operação está bem definida, isto é, não depende da escolha do representante da classe.

Dados $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$, queremos mostrar que $\overline{x * y} = \overline{a * b}$, ou seja, queremos mostrar que

$$(x * y) \equiv (a * b)(modN) \Leftrightarrow (x * y) * (a * b)^{-1} \in N \Leftrightarrow x * y * b^{-1} * a^{-1} \in N.$$

Mas note que, como $\overline{x} = \overline{a}$ e $\overline{y} = \overline{b}$ então

$$x * a^{-1} \in N, y * b^{-1} \in N.$$

Entretanto se $x * a^{-1} = n_0 \in N$ e $y * b^{-1} = n_1 \in N$ então temos

$$x * n_1 * a^{-1} = (n_0 * a) * (n_1) * a^{-1} = n_0 * (a * n_1 * a^{-1})$$

E como $n_0 \in N$ e $a * n_1 * a^{-1} \in N^{a^{-1}} = N$. Segue de imediato que

$$x * n_1 * a^{-1} = x * y * b^{-1} * a^{-1} = (x * y) * (a * b)^{-1} \in N$$

.

i) Elemento neutro de G/N;

Tomando e elemento neutro de G tem-se que $\overline{e} * \overline{x} = \overline{e * x} = \overline{x} = \overline{x * e} = \overline{x} * \overline{e}$, para todo $\overline{x} \in G/N$.

ii) Associatividade em G/N;

Considerando $\overline{g}, \overline{h}, \overline{i} \in G/N$ tem-se que $\overline{g} * (\overline{h * i}) = \overline{g * (h * i)} = \overline{(g * h) * i} = \overline{g * h} * \overline{i}$.

iii) Elemento inverso em G/N;

Considerando $\overline{x} \in G/N \Rightarrow \overline{x} * \overline{x^{-1}} = \overline{x * x^{-1}} = \overline{e} = \overline{x^{-1} * x} = \overline{x^{-1}} * \overline{x}$.

Portanto, G/N com a operação atribuída é um grupo.

■

1.4 Homomorfismos de grupos

Sejam $(G, \bullet)$ e $(G', *)$ grupos e $\gamma : G \to G'$ uma aplicação de G em G'. Dizemos que γ é um **homomorfismo** se

$$\gamma(x \bullet y) = \gamma(x) * \gamma(y), \ \forall \ x, y \in G.$$

Se o homomorfismo $\gamma : G \to G'$ for bijetivo então γ é um **isomorfismo**. Neste caso diz-se que G é **isomorfo** a G', denotando-se $G \simeq G'$. E um isomorfismo $\gamma : G \to G$ é denominado **automorfismo** de G. O conjunto de todos os automorfismos de G é denotado por Aut$G$.

Proposição 1.6 *Seja G um grupo e f_1, $f_2 \in AutG$ então*

i) $f_1 \circ f_2 \in AutG$;

ii) $f_1^{-1} \in AutG$, sendo f_1^{-1} a aplicação inversa de f_1.

Demonstração:

i) Basta mostrar que a composição de aplicações que estão em Aut$G$ descreve um homomorfismo. De fato,

$f_1 \circ f_2(x * y) = f_1(f_2(x * y)) = f_1(f_2(x) * f_2(y)) = f_1(f_2(x)) * f_1(f_2(y)) = f_1 \circ f_2(x) * f_1 \circ f_2(y)$,

logo $f_1 \circ f_2 \in$ Aut$G$, pois a composição de aplicações bijetivas é também bijetiva.

ii) Considerando que $f_1 \in \mathrm{Aut}G$ então $\forall x', y' \in G$ existem $x, y \in G$ de modo que $f_1(x) = x'$ e $f_1(y) = y'$. Como f_1 é bijetiva, então existe f_1^{-1} tal que

$$f_1^{-1}(x'*y') = f_1^{-1}(f_1(x)*f_1(y)) = f_1^{-1}(f_1(x*y)) = (f_1^{-1}\circ f_1)(x*y) = x*y = f_1^{-1}(x')*f_1^{-1}(y').$$

Portanto $f_1^{-1} \in \mathrm{Aut}G$.

■

Teorema 1.2 (Primeiro Teorema do Homomorfismo) *Sejam G e G' grupos com identidades e,e' respectivamente e $\gamma : G \to G'$ um homomorfismo. Então*

i) $Im(\gamma) = \gamma(G) = \{\gamma(g) : g \in G\}$ é um subgrupo de G';

*ii) $N(\gamma) = \{g \in G : \gamma(g) = e'\}$ é um subgrupo normal de G chamado **núcleo** do homomorfismo γ, e mais*

$$\gamma \text{ é injetiva} \iff N(\gamma) = \{e\};$$

iii) $G/N(\gamma) \simeq Im(\gamma)$.

Demonstração:

i) $e' = \gamma(e) \in \mathrm{Im}(\gamma)$ pois $e \bullet e = e \Rightarrow \gamma(e) * \gamma(e) \Rightarrow \gamma(e) = e^{'} \in \mathrm{Im}(\gamma)$, logo $\mathrm{Im}(\gamma) \neq \varnothing$.
Observe que $\gamma(g_1), \gamma(g_2) \in \mathrm{Im}(\gamma) \Rightarrow \gamma(g_1) * \gamma(g_2)^{-1} \in \mathrm{Im}(\gamma), \forall g \in G$.
E isto demonstra que $\mathrm{Im}(\gamma)$ é subgrupo de G, visto que satisfaz de forma sintática a definição de subgrupo.

ii) Note que $e \in N(\gamma)$, pois $\gamma(e) = e'$.

Dados $g_1, g_2 \in \mathrm{N}(\gamma)$, temos que

$$\gamma(g_1 \bullet g_2) = \gamma(g_1) * \gamma(g_2) = e' * e' = e' \Rightarrow g_1 \bullet g_2 \in N(\gamma).$$

Temos que se $g \in \mathrm{N}(\gamma)$ então

$$\gamma(g^{-1}) = \gamma(g)^{-1} = (e')^{-1} = e' \Rightarrow g^{-1} \in N(\gamma).$$

Considere $n \in N(\gamma)$ e $g \in G$, daí

$$\gamma(g^{-1} \bullet n \bullet g) = \gamma(g^{-1}) * \gamma(n) * \gamma(g) = \gamma(g^{-1}) * e' * \gamma(g) = e'$$

isto é, $g^{-1} \bullet n \bullet g \in \mathrm{N}(\gamma)$, para todo $n \in N(\gamma)$ e para todo $g \in G$.

Portanto $\mathrm{N}(\gamma)$ é um subgrupo normal de G.
Agora, se $g_1, g_2 \in G$

$$\gamma(g_1) = \gamma(g_2) \Leftrightarrow \gamma(g_1) * \gamma(g_2)^{-1} = e' \Leftrightarrow \gamma(g_1 \bullet g_2^{-1}) = e^{'} \Leftrightarrow g_1 \bullet g_2^{-1} \in N(\gamma),$$

e dai segue de imediato o item (ii) do Teorema 1.2.

iii) Consideremos $\overline{G} = G/\ \mathrm{N}(\gamma)$ e $N = \mathrm{N}(\gamma) \trianglelefteq G$ defina a função

$$\begin{aligned} \overline{\gamma} : \overline{G} &\to \mathrm{Im}\gamma \\ \overline{g} &\mapsto \gamma(g) \end{aligned}$$

Primeiramente, veremos que $\overline{\gamma}$ está bem definida, basta observar que

$$\overline{g} = \overline{h} \Rightarrow Ng = Nh,$$

e daí

$$g \bullet h^{-1} \in N \Rightarrow \gamma(g \bullet h^{-1}) = e' \Rightarrow \gamma(g) * \gamma(h)^{-1} = e',$$

ou seja, $\gamma(g) = \gamma(h)$.

A função é claramente sobrejetiva, pois $\mathrm{Im}\overline{\gamma} = \mathrm{Im}(\gamma)$.

Observe que $\overline{\gamma}$ é homomorfismo, pois

$$\overline{\gamma}(\overline{x} \bullet \overline{y}) = \overline{\gamma}(\overline{x \bullet y}) = \gamma(x \bullet y) = \gamma(x) * \gamma(y) = \overline{\gamma}(\overline{x}) * \overline{\gamma}(\overline{y}).$$

Note que

$$\overline{\gamma}(\overline{x}) = e^{'} \Rightarrow \gamma(x) = e^{'} \Rightarrow x \in N \Rightarrow \overline{x} = \overline{e},$$

ou seja, $\mathrm{N}(\overline{\gamma}) = \overline{e}$ e com isso $\overline{\gamma}$ é injetiva e portanto $\overline{G} \simeq \mathrm{Im}\gamma$.

■

CAPÍTULO 2

ALGUNS GRUPOS

Nesse capítulo apresentamos alguns grupos que são importantíssimos para o desenvolvimento teórico do presente trabalho, as principais estruturas descritas são os grupos cíclicos, grupos finitos definidos por dois elementos a e b com $ba = a^s b$, o grupo das permutações e a classificação de grupos de ordem pequena. São estruturas que envolvem maior grau de abstração em suas demonstrações, neste trecho do trabalho usamos grande parte dos elementos descritos no capítulo anterior para fundamentar as demonstrações dos teoremas vigentes sobre os temas abordados. Pela complexidade das temáticas aqui descritas, indicamos preferencialmente a leitura complementar das referências que aqui foram usadas, que são [1] e [3].

2.1 Grupos cíclicos

Seja G um grupo e $g \in G$, se $n \in \mathbb{Z}$ definimos g^n como

$$g^n = \begin{cases} e & se \quad n = 0 \\ g^{n-1} * g & se \quad n > 0 \\ (g^{-n})^{-1} & se \quad n < 0 \end{cases}$$

Se $m, n \in \mathbb{Z}$ valem as seguintes propriedades:

i) $g^m * g^n = g^{m+n}$

ii) $(g^m)^n = g^{mn}$

Denotando $< g >= \{g^n : n \in \mathbb{Z}\} \subset G$ então temos que $g^0 = e$, $(g^n)^{-1} = g^{-n}$ e $g^m * g^n = g^{m+n}$ segue de imediato que $< g >$ é um grupo abeliano. Tal grupo é denominado **grupo cíclico** gerado pelo elemento $g \in G$.

Proposição 2.1 *Seja* $G =< a >= \{..., a^{-1}, e, a, a^2, ...\}$ *um grupo cíclico de ordem infinita. então:*

i) A função $f : (\mathbb{Z}, +) \to (G, *)$ *onde* $f(z) = a^z$ *é um isomorfismo.*

ii) O elemento a^z *gera* G *se, e só se* $z = 1$ *ou* $z = -1$.

Demonstração:

i) De fato a função f é um isomorfismo, note que:

$f(z_1 + z_2) = a^{z_1+z_2} = a^{z_1} * a^{z_2} = f(z_1) * f(z_2),\ \forall\ z_1, z_2 \in \mathbb{Z}$.

Observe que claramente a função f é bijetiva e com isso temos que f é um isomorfismo.

ii) A função $f(z) =^z$ sendo um isomorfismo, temos que a^z gera G se, e só se z gera $\mathbb{Z}$ e os únicos elementos que geram $\mathbb{Z}$ são $z = 1$ ou $z = -1$.

■

Proposição 2.2 *Seja* $G =< a >= \{e, a, ..., a^{n-1}\}$ *um grupo cíclico finito de ordem* n.

i) Se H *é um subgrupo de* G *então* H *é cíclico. De maneira precisa,* $H =< a^m >$ *onde* m *é o menor inteiro positivo tal que* $a^m \in H$*; o subgrupo* H *tem ordem igual a* n/m.

ii) Se d *é divisor de* n *então existe um único subgrupo* H *de* G *com ordem igual a* d. *Este subgrupo* H *é igual a* $< a^{n/d} >$.

Demonstração:

i) Considerando m o menor inteiro positivo onde $a^m \in H$, daí temos que $< a^m > \subseteq H$. Por outro lado, se $a^u \in H$, mostraremos que $m|u$ (o que implicará que $a^u \in < a^m >$). Note que,

$$u = qm + r; 0 \leq r < m.$$

Segue que $a^u = (a^m)^q \cdot a^r$. Como $a^u \in H$ e $a^m \in H$ segue que $a^r \in H$ e como m é mínimo, teremos $r = 0$ e com isso $m|u$, e segue de imediato que a ordem de a^m(que é a ordem de H) é igual a n/m.

ii) Seja d um divisor de n. O subgrupo $< a^{n/d} >$ tem ordem d. Provaremos que é único. Considerando H um subgrupo qualquer de ordem d, pelo item anterior tem-se que $H =< a^m >$, onde m é um inteiro tal que que $\frac{n}{m}$ seja a ordem de H, ou seja, $d = \frac{n}{m}$, logo $m = n/d$, isto é, $< a^{n/d} >= H$.

■

2.2 Grupos finitos gerados por dois elementos

A priori, temos que os grupos gerados por um elemento, como exemplo os grupos cíclicos, são facilmente classificados. Entretanto os grupos gerados por dois elementos podem ser extremamente complicados e por isso iremos restringir o estudo aos grupos finitos gerados por dois elementos bastante específicos, que são os grupos finitos $G =< a, b >$, onde a, b satisfazem a relação $ba = a^s b$.

Considerando o conjunto das permutações de ordem 3, pois o mesmo está nas condições do que queremos trabalhar na seção, basta observar que:

$$G_3 = \left\{ id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \beta, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

Temos que o grupo G_3 possui a ordem (cardinalidade) 6, e que temos a seguinte apresentação para este grupo:

$$\left\{ G_3 =< \alpha, \beta >, \alpha^3 = id, \beta^2 = id, \beta\alpha = \alpha^2\beta \right\}$$

Por outro lado, mostraremos que se F é um grupo que possui ordem 6, onde existem elementos X, Y tal que F tenha a seguinte apresentação:

$$\left\{ F =< X, Y >, X^3 = e, Y^2 = e, XY = X^2Y \right\}$$

então, existe um isomorfismo entre G_3 e F. Logo temos que, a menos de isomorfismo, o grupo G_3 é o único grupo de ordem 6 e que é gerado por dois elementos α, β satisfazendo a relação

$$\left\{ \alpha^3 = e, \beta^2 = e, \beta\alpha = \alpha^2\beta \right\}.$$

Vamos agora determinar as características dos homomorfismos definidos sobre um grupo gerado por dois elementos que satisfazem a relação $ba = a^s b$

Teorema 2.1 *Seja $s \geq 1$ inteiro. Sejam G um grupo finito e $a, b \in G$ satisfazendo $ba = a^s b$ (equivalentemente, $I_b(a) = a^s$). Sejam G' um grupo e $\alpha, \beta \in G$. Sejam $n, m \geq 1$ tais que*

$$a^n = e, \quad b^m \in < a > \qquad (*)$$

então:

i) a) $b^t.a^r = a^{rs^t}.b^t; \forall r, t \in \mathbb{N}$ $e < a, b >= \{a^i b^j \quad | \quad 0 \leq i \leq n-1; 0 \leq j \leq m-1\}$

b) Se os inteiros m, n são escolhidos minimamente satisfazendo (*), então o grupo $< a, b >$ tem ordem igual a nm.

ii) Se os inteiros n, m são escolhidos minimamente, e se u é um inteiro tal que $b^m = a^u$, então existe um homomorfismo $f :< a, b >\to G'$ com $f(a) = \alpha$ e $f(b) = \beta$ se e somente se

$$\beta\alpha = \alpha^n\beta, \quad \alpha^n = e, \quad \beta^m = \alpha^u.$$

Antes das demonstrações vamos enunciar alguns resultados importantes, que são:

1) $I_g : G \to G$, $I_g(x) = gxg^{-1}$ é denominado **automorfismo interno associado ao elemento** $g \in G$. O conjunto dos automorfismos internos de G será denotado por $I(G)$, logo
$$I(G) := \{I_g : g \in G\} \subseteq Aut(G).$$

2) $I(G)$ é um subgrupo de Aut$G$. Segue das igualdades que
$$(I_g)^{-1} = I_{g_1^{-1}} \text{ e } I_{g_1} \circ I_{g_2} = I_{g_1 g_2}.$$

Demonstração:

i) a) Queremos mostrar que $b^t \cdot a^r = a^{rs^t} \cdot b^t$, o que é equivalente a mostrar que $I_b(a) = a^s$. Realizando indução sobre t, para $t = 1$ temos:

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

Supondo $t \geq 2$ e tendo como hipótese de indução o caso anterior, temos que

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

Através disso mostramos que todo elemento de $< a, b >$ pode ser escrito na forma $a^u b^w$, onde $u, w \in \mathbb{N}$. Segue que a condição $b^m \in < a >$ nos permite descrever um elemento $a^u b^w$ da forma $a^t b^j; t \in \mathbb{N}$ e $0 \geq j \geq m - 1$; a condição $a^n = e$ nos permite descrever $a^t b^j$ na forma $a^i b^j$ tal que $0 \geq j \geq m - 1$ e $0 \geq i \geq n - 1$ e com isso

$$G = \{a^i b^j \quad | \quad 0 \geq j \geq m - 1; 0 \geq i \geq n - 1\}.$$

b) Suponhamos que n, m são minimais satisfazendo (*), queremos mostrar que $< a, b >$ possui ordem nm, ou seja, é suficiente observar que se $0 \geq i, k \geq n-1; 0 \geq j, l \geq m-1$ e $a^i b^j = a^k b^l$ então $i = k$ e $j = l$.

Considerando $l \geq j$ e operando ambos os lados da igualdade $a^i b^j = a^k b^l$ pelos termos a^{-i} pela esquerda e b^{-l} pela direita tem-se

$$b^{j-l} = a^{k-i} \in < a >,$$

onde $0 \geq j - l \geq j \geq m - 1$ e pela minimalidade de m segue que $j - l = 0$ e sequencialmente $a^{k-i} = e$ e pela minimalidade de n temos que $i = k$.

ii) Suponha que exista um homomorfismo $f :< a, b >\to G^{'}$ com $f(a) = \alpha$ e $f(b) = \beta$. Temos que $ba = a^s b$, dai

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

De forma análoga como $a^n = e$ logo $\alpha^n = e$, tem-se também que $b^m = a^u$ logo $\beta^m = \alpha^u$.

Por outro lado suponhamos $\beta\alpha = \alpha^s\beta$, $\alpha^n = e$, $\beta^m = \alpha$, pelo item i) aplicado em $G^{'}, \alpha, \beta$, tem-se que $\beta^t\alpha^r = \alpha^{rs^t}, \forall r, t \in \mathbb{N}$. Mostraremos que a aplicação $f :< a, b >\to G^{'}$ definida por

$$f(a^i b^j) = \alpha^i\beta^j,$$

para $0 \geq j \geq m-1$ e $0 \geq i \geq n-1$, é um homomorfismo. Temos que f está bem definida graças as escolhas minimais dos elementos $n \cdot m$, daí para $i, j, k, l \in \mathbb{N}$ determinamos $j + l = pm + v$ com $0 \geq v \geq m-1$ e também $i + ks^j + pu = qn + w$ com $0 \geq w \geq n-1$. Segue que

$$\begin{gathered} f(a^i b^j . akb^l) = f(a^i . b^j a^k . b^l) = f(a^i . a^{ks^j} b^j . b^l) = f(a^{i+ks^j} b^{j+l}) = f(a^{i+ks^j} b^{pm} b^v) = \\ f(a^{i+ks^j} a^{pu} b^v) = f(a^w b^u) = \alpha^w\beta^u = \alpha^{i+ks^j}\alpha^{pu}\beta^u = \alpha^{i+ks^j}\beta^{pm}\beta^v = \alpha^{i+ks^j}\beta^{j+l} = \\ \alpha^i . \alpha^{ks^j}\beta^j . \beta^l = \alpha^i\beta^j . \alpha^k\beta^l = f(a^i b^j) . f(a^k b^l) \end{gathered}$$

■

2.3 Grupos de permutações

Nesta seção observaremos que todo grupo finito é isomorfo a um subgrupo de um grupo de permutações.

Teorema 2.2 (Teorema de Cayley) *Seja G um grupo finito de ordem n e seja $G^{'}$ o conjunto subjacente (o conjunto G sem estrutura de grupo). Então*

$$\begin{gathered} T : G \to P(G^{'}) \backsimeq G_n \\ g \mapsto T_g : G^{'} \to G^{'} \\ x \to gx \end{gathered}$$

é um homomorfismo injetivo.

Demonstração: Considere r e $s \in G$, para todo elemento y de $G^{'}$ temos que

$$T_{rs}(y) = (rs)y = r(sy) = T_r(T_s(y)) = T_r \circ T_s(y);$$

Logo

$$T_{rs} = T_r \circ T_s$$

e com isso observamos que T é um homomorfismo entre o grupo G e o grupo $P(G')$. Note que T é injetivo pois se $g \in N(T)$, temos $id_{G'} = T_g$, ou seja, $x = T_g(x) = gx$, $\forall x \in G$ e portanto $g = e$.

■

Definição 2.1 *Uma permutação $\beta \in G_n$ é chamada de **r-ciclo** se existem elementos distintos $b_1, b_2, ..., b_r \in \{1, ..., n\}$ tais que $\beta(b_1) = b_2$; $\beta(b_2) = b_3$,..., $\beta(b_{r-1}) = b_r$, $\beta(b_r) = b_1$ e tais que $\beta(j) = j$, $\forall j \in \{1, ..., n\} - \{b_1, ..., b_r\}$; tal r-ciclo será denotado por $(b_1...b_n)$. O número r é chamado **comprimento do ciclo**. E os 2-ciclos são denominados de **transposições**.*

Exemplo 2.1 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ *é um 5-ciclo, denotado por* (12345)*, o mesmo poderia ser denotado por* (23451) *ou* (34512) *ou* (45123) *ou* (51234)*.*

Exemplo 2.2 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}$ *é um* $3-ciclo$*, denotado por* (143)*, podendo ser denotado por* (431) *e* (314)*.*

Exemplo 2.3 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$ *é uma tranposição, denotado por* (13) *ou* (31)*.*

Definição 2.2 *Seja $\beta \in G_n$ um r-ciclo e seja $\gamma \in G_n$ um s-ciclo. As permutações β e γ são disjuntas se nenhum elemento de $\{1, 2, ..., n\}$ é movido por ambas, isto é, para todo $d \in \{1, 2, ..., n\}$ temos $\beta(d) = d$ ou $\gamma(d) = d$.*

Exemplo 2.4 *Considerando G_5. Os ciclos* (123) *e* (45) *são disjuntos e os ciclos* (14) *e* (25) *também, no entanto, os ciclos* (135) *e* (25) *não são disjuntos, pois o elemento 5 é movido por ambos.*

Proposição 2.3 *Seja $\beta \in G_n, \beta \neq id$. Então a permutação β é igual a um produto de ciclos disjuntos de comprimentos ≥ 2 onde tal fatoração é única a menos da ordem de fatores.*

Demonstração: Como $\beta \neq id$, existe j_i tal que $\beta(j_1) \neq j_1$. Considere a sequência

$$j_i, \beta(j_i), \beta^2(j_i), \ldots$$

Existe $r_i, 2 \leq r_1 \leq n$, tal que $j_1, \beta(j_1), \ldots, \beta^{r_1-1}(j_1)$ são todos distintos e

$$\beta^{r_1}(j_i) \in \{j_1, \beta(j_1), \ldots, \beta^{r_1-1}(j_1)\}.$$

É fácil ver que $\beta^{r_1}(j_1) = j_1$. Portanto, a restrição ao conjunto $\{j_1, \beta(j_1), ..., \beta^{r_1-1}(j_1)\}$ é

$$\beta|_{\{j_1, \beta(j_1, ..., \beta^{r_1-1}(j_1)\}} = (j_1 \beta(j_1) ... \beta^{r_1-1}(j_1)).$$

Denotaremos tal r_1-ciclo $(j_1\beta(j_1)...\beta^{r_1-1}(j_1))$ por δ_1. Se a restrição de δ ao complementar de $\{j_1, \beta(j_1), ..., \beta^{r_1-1}(j_1)\}$ é a identidade, então $\delta = \delta_1$. Caso contrário, tomemos um elemento $j_2 \in \{1, 2, ..., n\} - \{j_1, \beta(j_1), ..., \beta^{r_1-1}(j_1)\}$ tal que $\beta(j_2) = j_2$; de forma análoga ao processo anterior, existirá um inteiro $r_2 \geq 2$ tal que

$$\beta|_{\{j_2,\beta(j_2,...,\beta^{r_2-1}(j_2)\}} = (j_2\beta(j_2)...\beta^{r_2-1}(j_2)).$$

Denotaremos tal r_2-ciclo $(j_2\beta(j_2)...\beta^{r_2-1}(j_2))$ por δ_2. Note que δ_1 e δ_2 são disjuntos. Se a restrição de β ao complementar do conjunto $\{j_1, \beta(j_1), ..., \beta^{r_1-1}(j_1), j_2, \beta(j_2), ..., \beta^{r_2-1}(j_2)\}$ é a identidade, então $\delta = \delta_1\delta_2 = \delta_2\delta_1$, observe que caso contrário tomamos um

$$j_3 \in \{1, 2, ...\} - \{j_1, \beta(j_1), ..., \beta^{r_1-1}(j_1), j_2, \beta(j_2), ..., \beta^{r_2-1}(j_2)\}$$

e continuamos o processo, onde o mesmo terá um número finito de etapas e através disso obteremos que $\delta = \delta_1\delta_2...\delta t$, de modo que $\delta_1\delta_2...\delta t$ são ciclos disjuntos de comprimento ≥ 2.

Por fim, para provar a unicidade, suponhamos que tem-se

$$\delta = \alpha_1\alpha_2...\alpha_k,$$

onde α_1,α_2,...,α_n são ciclos disjuntos, onde cada um deles possui comprimento ≥ 2. Como $\alpha_1...\alpha_k(j_1) = \beta(j_1) \neq j_1$ e como os $\alpha_j^{'s}$ são ciclos disjuntos, existe um único α_l tal que

$$\alpha_l(j_1) = \beta(j_1).$$

Como os $\alpha_j^{'s}$ comutam entre si, suponhamos que $l = 1$ e daí $\alpha(j_1) = \beta(j_1)$. Mostraremos então que $\alpha_1 = \delta_1$. O ciclo α_1 não pode deixar $\beta(j_1)$ fixo, ou seja, $\beta(j_1)$ sobre $\beta(j_1)$, pois, α_1 já manda j_1 sobre $\beta(j_1)$ e como os $\alpha_j^{'s}$ são ciclos disjuntos, então, para todo $l \geq 2, \alpha_l$ deixa $\beta(j_1)$ fixo e portanto

$$\beta(\beta(j_1)) = \alpha(\alpha(j_1)),$$

assim

$$\alpha_1(\beta(j_1)) = \beta^2(j_1).$$

Analogamente, obtemos que

$$\alpha_1(\beta^{t-1}(j_1) = \beta^t(j_1),$$

para todo $t \geq 0$, e portanto temos que $\alpha_1 = \delta_1$. Ao continuarmos o processo tomando j_2 no lugar de j_1, obtemos que $\alpha_2 = \delta_2$, ao continuarmos com o processo obtemos que $k = s$ e que a menos da ordem $\delta_k = \alpha_k$, para cada $k = 1, ..., s$. ■

2.4 Classificação de Grupos de Ordem Pequena

Para realizar a classificação de um grupo abeliano G precisamos efetuar a decomposição do mesmo em soma direta de *p-subgrupos* de Sylow G e sequencialmente decompor cada *p-grupo* como uma soma direta de subgrupos cíclicos de G. O processo das duas decomposições descreve o **Teorema Fundamental dos Grupos Abelianos Finitos**.

Vamos descrever esses principais resultados:

Teorema 2.3 (Primeiro Teorema de Sylow) *Sejam p um número primo e G um grupo de ordem $p^m b$ com $mdc(p, b) = 1$. Então, para cada $n, 0 \leq n \leq m$, existe um subgrupo H de G tal que $|H| = p^n$.*

Demonstração: Presente em [3]. ∎

Definição 2.3 *Seja p um primo. Um grupo G, não necessariamente finito, no qual todo elemento tem sua ordem igual a uma potência de p é denominado um* ***p-grupo***

Definição 2.4 (p-subgrupos de Sylow) *Seja G um grupo finito, p um primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que tem ordem p^m são denominados* ***p-subgrupos de Sylow de G****.*

Definição 2.5 *Sejam G um grupo e $G_1, G_2, ..., G_n$ subgrupos de G. Dizemos que G é o* ***Soma Direta Interna*** *de $G_1, G_2, ..., G_n$ e denotaremos por $G_1 \oplus G_2 \oplus ... \oplus G_n$, se as condições seguintes são satisfeitas:*

i) Para todo $g \in G$ temos que existem únicos $x_1 \in G_1, ..., x_n \in G_n$ tais que $g = x_1 + ... + x_n$;

ii) Para $i \neq j, x \in G_i, y \in G_j$ temos $x + y = y + x$.

2.4.1 Grupos de ordem 4

Proposição 2.4 *Seja γ um homomorfismo de grupos. Se $|a| < \infty$, então $|\gamma(a)|$ divide $|a|$.*

Considerando os Grupos aditivos que possuem 4 elementos, sendo eles

$$\mathbb{Z}_4 = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} \qquad \text{e} \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{1})\}$$

Observe que $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$ não são isomorfos. Caso contrário existiria um isomorfismo $f : \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_2$. Sendo assim, $f(\overline{1}) = (\overline{a}, \overline{b})$, para alguns $\overline{a}, \overline{b} \in \mathbb{Z}_2 \times \mathbb{Z}_2$. Em particular, teríamos

$$f(\overline{2}) = f(\overline{1}) + f(\overline{1}) = (\overline{a}, \overline{b}) + (\overline{a}, \overline{b}) = (\overline{0}, \overline{0}) = f(\overline{0}).$$

Como f é bijetora, teríamos que $\overline{2} = \overline{0}$, o que é uma contradição, pois $\overline{2} \neq \overline{0}$ em $\mathbb{Z}_4$.

Agora mostraremos que qualquer outro grupo G com 4 elementos é isomorfo a $\mathbb{Z}_4$ ou a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Considere os casos:

1. Seja G um grupo de quatro elementos, se um de seus elementos possui ordem 4, então G é cíclico.

   Exemplo 2.5 *Considere* $G =< a >= \{e, a, a^2, a^3\}$*, e seja*

   $$\theta : \mathbb{Z}_4 \to G$$

   $$\bar{i} \mapsto a^i$$

   Note que θ *é um isomorfismo, logo* $\mathbb{Z} \simeq G$*.*

2. Se G não possuir nenhum elemento de ordem 4, pelo Teorema de Lagrange, seus elementos, com exceção do elemento neutro, possuem ordem 2, então, G é abeliano.

   Demonstração: Sejam $a, b \in G$, como G é um grupo temos que $ab, ba \in G$ e sabemos que

   $$|a| = |b| = |ab| = |ba| = 2.$$

   Assim,

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

   Como a e b são arbitrários, temos que G é abeliano. Seja $G = \{e, a, b, c\}$, onde a, b, c são distintos. Vamos determinar o resultado da multiplicação ab.

   i) $ab \neq a$, pois caso contrário, $b = e$, que é um absurdo.

   ii) $ab \neq b$, pois caso contrário, $a = e$, que é um absurdo.

   iii) $ab \neq c$, pois caso contrário, $b = a$, pois b tem ordem 2, o que é uma contradição.

   Logo $ab = c$ e $ba = c$, pois G é abeliano. Assim:

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

   Determinando a relação: $(\overline{0}, \overline{0}) \mapsto e$, $(\overline{1}, \overline{0}) \mapsto a$, $(\overline{0}, \overline{1}) \mapsto b$, $(\overline{1}, \overline{1}) \mapsto c$.

   Temos que G é isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. ■

CAPÍTULO 3

APLICAÇÕES

Neste capítulo nosso objetivo está centrado em trazer uma abordagem aplicada a parte da teoria de grupos estudada anteriormente. Aqui mostramos que o software GAP surge como uma ferramenta de grande importância para auxiliar no estudo de assuntos voltados para teorias algébricas de maneira geral, em especial na teoria de grupos. Destacamos no escopo de nosso trabalho tópicos clássicos da Teoria de grupos, como representação de grupo de permutação e também uma aplicação do Teorema de Lagrange, além do mais, a referência [1], que norteou a escrita do capítulo, traz inúmeros códigos que contribuem para diversos assuntos citados ou não no escopo do presente trabalho, reafirmando a grande valia da utilização do software para o estudo de tópicos de álgebra abstrata.

3.1 GAP: Groups, Algorithms and Programming

O software GAP é um recuso computacional voltado para o estudo de álgebra cujo intuito é o de facilitar a pesquisa e o ensino de teorias relacionadas com contextos mais abstratos, de modo que os algoritmos do programa efetuem cálculos que por muitas vezes são trabalhosos e possibilitem a visualização de diversas estruturas, tais como: Espaços vetoriais, Anéis, Grupos, Corpos finitos. Caso o leitor busque conhecer o GAP, indicamos [2].

3.1.1 Preceitos básicos da linguagem GAP

O primeiro elemento a ser destacado é o operador (#), pois qualquer informação que venha após ele é entendida pelo programa como comentário, isto é, não é compilado como parte do código descrito.

O segundo ponto importante é relacionado a atribuição para uma variável utilizando o operador (**:=**). Outro fator acerca do GAP é que todo comando informado deve ser finalizado com (**;**), pois caso tal operador não esteja presente ao final do comando o mesmo não é reconhecido pelo programa, ou seja, não há prosseguimento na compilação do código até que o operador esteja presente.
Após cada comando compilado o GAP descreve informações acerca do que foi interpretado, caso isso não seja necessário para o programador, basta finalizar o código utilizando o operador (**;;**).

Para maiores detalhes indicamos [1].

Agora, traremos um exemplo acerca dos grupos das permutações, que faz parte dos assuntos clássicos relacionados ao estudo de teoria de grupos para entendermos como o GAP descreve as informações sobre tal estrutura.

Exemplo 3.1 *Grupo das permutações de ordem 24*
gap> G1:= SmallGroup(24,12);
<pc group of size 24 with 4 generators>
gap> StructureDescription(G1);
"S4"
gap> List(G1); # Listando os elementos de G1
*<identity> of ..., f4, f3, f3*f4, f2, f2*f4, f2*f3, f2*f3*f4,* $f2^2$, $f2^2 * f4$, $f2^2 * f3$, $f2^2 * f3 * f4$, *f1, f1*f4, f1*f3, f1*f3*f4, f1*f2, f1*f2*f4, f1*f2*f3, f1*f2*f3*f4,* $f1 * f2^2$, $f1 * f2^2 * f4$, $f1 * f2^2 * f3$, $f1 * f2^2 * f3 * f4$
gap> AllSubgroups(G1); # Determinando os subgrupos de G1
*Group([ ]), Group([f3]), Group([f4]), Group([f3*f4]), Group([f1]), Group([f1*f2]),* *Group([* $f1 * f2^2$ *]), Group([f1*f2*f4]), Group([f1*f3*f4]), Group([* $f1 * f2^2 * f3$ *]), Group([f2]), Group([f2*f3]), Group([f2*f4]), Group([f2*f3*f4]), Group([f3, f4]),*
Group([$f1 * f2^2, f3$ *]),*
*Group([f1*f2, f4]), Group([f1, f3*f4]), Group([* $f1 * f2^2 * f3 * f4, f3$ *]),*
*Group([f1*f2*f3, f4]), Group([f1*f4, f3*f4]), Group([f1, f2]), Group([f1*f3*f4, f2*f3]),*
*Group([f1, f2*f4]), Group([f1*f3*f4, f2*f3*f4]),*
*Group([f3, f4, f1]), Group([f1*f2, f3*f4, f4]), Group([*$f1 * f2^2, f3 * f4, f4$ *]), Group([f3, f4, f2]), Group([f3, f4, f2, f1])*

O próximo exemplo tratará acerca do Teorema de Lagrange, onde através de um algoritmo mostraremos que a recíproca do mesmo não é sempre válida. Nesse exemplo serão construídas duas funções auxiliares, descritas por **Ordens** e **ContemSubgrupoTodaordem**. Utilizaremos para exemplificação o grupo alternado A_n, definido como:

$$A_n = \{\alpha \in G_n\} \text{ onde } \alpha \text{ é permutação par.}$$

Sendo esse subgrupo denominado como **grupo alternado** ou como **grupo das permutações pares**.

Exemplo 3.2 *Teorema de Lagrange*

```
gap> #Ordens
gap> Ordens:= function(g)
> local subgruposdeg, classesdeconj,
> listadosrepresentantes, listadasordens;
> subgruposdeg:= LatticeSubgroups(g);
> classesdeconj:= ConjugacyClassesSubgroups(subgruposdeg);
> listadosrepresentantes:= List(classesdeconj, x-> Representative (x));
>listadasordens:= List(listadosrepresentantes, y-> Order(y));
> return listadasordens;
> end;
gap> #ContemSubgrupoTodaOrdem
gap> ContemSubgrupoTodaOrdem:= function(G)
> local ordemg, listadivisores, listadeordenssubgrupos, listaordenada, tamanho, x, cont
> cont:= 0;
> ordemg:= Order(G);
> listadivisores:= DivisorsInt(ordemg);
> listadeordenssubgrupos:= Ordens(G);
> listaordenada:= Set(listadeordenssubgrupos);
> for x in listadivisores do
> if x in listaordenada then
> cont:= cont+1;
> fi;
> od;
> tamanho:= Length(listadivisores);
> if tamanho=cont then
> return true;
> fi;
> return false;
> end;
gap> G:= AlternatingGroup(4);
Alt( [ 1 .. 4 ] )
gap> Order(G); #Mostra a ordem de G
12
gap> divisores:= DivisorsInt(Order(G)); #Calcula os divisores inteiros da ordem de G [ 1,
2, 3, 4, 6, 12 ]
gap> ContemSubgupoTodaOrdem(G); False
gap> Ordens(G); [ 1, 2, 3, 4, 12 ]
```

Ou seja, existe um divisor d, onde G não possui um subgrupo com tal ordem, e nesse exemplo vemos que isso ocorre quando $d = 6$, isto é, 6 divide $|G|$ mas não existe subgrupos de G com ordem 6.

CONSIDERAÇÕES FINAIS

No presente trabalho trouxemos os principais conceitos acerca da Teoria Básica de Grupos, desde definições, exemplos e teoremas da área de pesquisa até aplicações de tal assunto no software GAP, que serviram como um alicerce facilitador para o processo de aprendizagem e pesquisa sobre a estrutura algébrica de Grupo, pois através de toda essa organização pode-se compreender alguns dos principais resultados dessa teoria algébrica, de modo que o GAP contribuiu para melhor interpretação de alguns resultados, visto que a estrutura de Grupo é um tópico que possui elementos matemáticos bastante abstratos.

É importante ressaltar também o estudo do software GAP. Uma vez que não se trata de um tópico comum nos cursos de graduação em Matemática. Então a apresentação e manipulação, ainda que em pequenas etapas do software nos dá uma bagagem significativa e abre um caminho de pesquisa interessante para futuros trabalhos. Aliando assim a teoria algébrica a uma importante ferramenta computacional.

Outro ponto relevante acerca do trabalho aqui descrito é que o mesmo servirá como alicerce para a pesquisa de nossa próxima iniciação científica, que tratará sobre **Códigos de Grupo: construções, exemplos e análise via GAP**, de modo que os assuntos aqui abordados são pré-requisitos chave para desenvolver o trabalho acerca da temática proposta.

Portanto, o projeto atendeu a proposta de ser uma introdução a teoria de grupos, contendo uma projeção organizacional voltada para apresentação dos principais elementos que fundamentam determinada estrutura algébrica e cumpre também o papel de ser um alicerce para avanços em pesquisas, de modo que contribua para construção de novos teoremas, proposições e também seja uma base sólida para desenvolvimento de áreas que possuam aplicação matemática fundamentadas em tal teoria.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ALTOÉ, T. J. *Grupos e corpos com aplicações em GAP*. 2017. Trabalho de Conclusão de Curso (Graduação em Bacharelado em Matemática) – Instituto de Ciências Exatas, Universidade Federal Fluminense, Volta Redonda, 2017.

[2] GAP: Groups, Algorithms, Programming - a System for Computational Discrete Algebra. Disponível em: https://www.gap-system.org/

[3] GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. Projeto Euclides. 5. ed. Rio de Janeiro: IMPA, 2008.

[4] GONÇALVES, A. *Introdução à Álgebra*. Projeto Euclides, IMPA, Rio de Janeiro, (2006).