Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Classificação de Automorfismos de Grupos Finitos

por

Flávio Alves de Albuquerque

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2011

João Pessoa - PB

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Classificação de Automorfismos de grupos Finitos

por

Flávio Alves de Albuquerque

Dissertação apresentada ao Departamento de Matemática da Universidade Federal da Paraíba, como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva - UFPB (Orientador)

Prof. Dr. João Montenegro de Miranda - UECE

Prof. Dra. Jacqueline Fabiola Rojas Arancibia - UFPB

A345c Albuquerque, Flávio Alves de.
Classificação de automorfismos de grupo finitos / Flávio Alves de Albuquerque.-- João Pessoa, 2011.
56f.
Orientador: Antônio de Andrade e Silva
Dissertação (Mestrado) – UFPB/CCEN
1. Matemática. 2. Grupos abelianos. 3. Endomorfismos. 4. Classificação de automorfismos. 5. Álgebra.

UFPB/BC

CDU: 51(043)

Agradecimentos

A Deus, que concedeu ao filho de uma feirante e de um guarda municipal a possibilidade de vencer mais uma etapa da vida.

Aos meus pais, Felipe de Albuquerque Melo Filho e Maria do Socorro Alves de Albuquerque por tudo que sou.

Aos professores do Departamento De Matemática da UFPB, em especial aos professores, Dr. Fernando Antônio Xavier de Sousa e Dr. Daniel Marinho Pellegrino.

Ao meu orientador e amigo Professor Dr. Antônio de Andrade e Silva pela paciência, dedicação e por ter sido meu maior incentivador, ainda na graduação, a seguir na vida acadêmica.

A todos os colegas de curso que de alguma forma contribuiram com esse trabalho.

A todos os colegas professores de Matemática do IFPB - Campus João Pessoa.

Por fim, a minha esposa Andréa Santos de Albuquerque, a meus filhos Flávio Henrique Santos de Albuquerque e Ana Beatriz Santos de Albuquerque pela compreensão de tê-los pivado da minha presença, por varios momentos importantes de suas vidas.

Dedicatória

A minha família

Resumo

Neste trabalho estudamos Grupos Abelianos finitos, onde enunciamos e provamos o Teorema fundamental dos grupos abelianos finitamente gerados, bem como determinamos uma caracterização dos automorfismos de um p-grupo, além disso, exibimos um algoritmo que determina a contagem do número de automorfismos desses p-grupos. Por fim, mostramos os automorfismos do grupo não-Abeliano Diedral .

Palavras chave- Grupos Abelianos finitos, Endomorfismos, Classificação de Automorfismos e Grupo Diedral.

Abstract

In this paper we study finite Abelian groups, where state and prove the fundamental theorem of finitely generated abelian groups, as well as determine a characterization of automorphisms of a p-group, moreover, we exhibit an algorithm that determines the count of the number of automorphisms of p-groups. Finally, we show the automorphisms of the non-Abelian dihedral group.

Key words- Finite Abelian groups, endomorphisms, automorphisms and classification of dihedral group.

Notação

- $\mathbb{F}_p$ - Corpo finito com p elementos onde p é um número primo;
- G - Grupo;
- 1, 1_G - Elemento identidade do grupo G;
- $\mathrm{End}\,(G)$ - Conjunto dos endomorfismos do grupo G;
- $\mathrm{Aut}\,(G)$ - Conjunto dos automorfismos do grupo G;
- $\mathrm{Inn}\,(G)$ - Conjunto dos automorfismos internos do gupo G;
- $\mathcal{Z}_n$ - Anél dos inteiros módulo n;
- [] - Indica referência;
- $\langle S \rangle$ - Subgrupo gerado por S;
- $|G|$ - Ordem do grupo G;
- $\simeq$ - Isomorfismo;
- $\frac{\mathbb{Z}}{n\mathbb{Z}}$ - Conjunto das classes de equivalência de $\mathbb{Z}$ módulo n;
- $H \times K$ - Produto direto de H por K;
- $H \rtimes K$ - Produto semidireto de H por K;
- $H \leq G$ - H é Subgrupo de G;
- $H \trianglelefteq G$ - H é Subgrupo Normal de G;
- $\frac{G}{H}$ - Grupo quociente de G por um subgrupo normal H;
- $\det(A)$ - Determinante da matriz A;
- $Gl_t\,(A)$ - Grupo das matrizes invertíveis;
- D_n - Grupo diedral de ordem $2n$.

Sumário

Introdução

Histórico

Em entrevista a Revista Matemática Universitária [4], o matemático Walter Feit, afirma que o início da Teoria dos Grupos se deu com a descoberta da irressolubilidade das equações de quinto grau por radicais feita por Galois. Nessa teoria um dos problemas mais difíceis que se apresenta é sem dúvida o da classificação dos grupos finitos. Apenas para dar uma ideia da extrema dificuldade, podemos informar que existem 14 tipos distintos de grupos de ordem 16 sendo 5 abelianos (apenas 1 cíclico) e 9 não abelianos.

Um dos teoremas que levou a classificação dos grupos simples finitos foi o teorema da ordem ímpar que afirma "Qualquer grupo de ordem ímpar é solúvel," trata-se de um enunciado breve e simples cuja prova, obtida em 1962 por Walter Feit e John Thompson, ocupou 255 páginas do *Pacific Journal of Mathematic*. As técnicas introduzidas ao longo da prova foram a base de muitos dos desenvolvimentos posteriores na teoria dos grupos finitos. O teorema da ordem ímpar é um elemento crucial em todas as demonstrações dos teoremas da classificação dos grupos simples.

Em 1981, depois de muitos anos de trabalho, foi completada, pelo matemático Gorenstein, a classificação dos grupos simples que são "as partículas elementares" da teoria dos grupos finitos.

A primeira caracterização dos automorfismos de um grupo G foi tratada no artigo "The group of classes of congruent matrices with application to the group isomorphisms of any abelian group" de Ranum em 1907. Além deste, há poucas exposições. Nosso objetivo com este trabalho é contribuir com um tratamento acessível e moderno a essa caracterização no caso de grupos finitos.

Descrição do trabalho

Esta dissertação é constituída de três capítulos.

No Capítulo 1, apresentamos os conceitos básicos relativos a Teoria dos Grupos, pois esses conceitos permeiam a maioria dos resultudaos abordados bem como enunciamos e provamos o teorema fundamental dos grupos abelianos finitamente gerados e exibimos um exemplo.

No Capítulo 2, fazemos uma caracterização dos endomorfismos do grupo H_p mostrando o isomorfismo entre $\mathrm{End}\,(H_p)$ e o conjunto de matrizes R_p, mostramos um algoritmo e uma fórmula explicita para a determinação do número de automorfismos de H_p e exibimos um exemplo.

Finalmente, no Capítulo 3, fazemos a classificação dos automorfismos do grupo não abeliano Diedral como forma de comparar com a classificação dos automorfismos dos grupos abelianos.

Capítulo 1

Preliminares

Neste capítulo o leitor encontrará alguns resultados básicos necessários para a compreenssão da abordagem que será feita. Apresentaremos as definições de Grupos, Subgrupos, Homomorfismos, Endomorfismos e Automorfismos de grupos e algumas propriedades relevantes destes e as conexões existentes entre eles, bem como a definição de produto direto e o Teorema fundamental para grupos abelianos finitos. O leitor interessado em mais detalhes pode consultar [5].

1.1 Grupos

Um conjunto G munido de uma operação binária

$$\begin{aligned} * : \ G \times G &\rightarrow G \\ (a,b) &\mapsto a * b \end{aligned}$$

é um grupo se os axiomas seguintes são satisfeitos:

1. Associatividade,
$$a * (b * c) = (a * b) * c, \ \forall \ a, b, c \in G.$$

2. Existe $1 \in G$ tal que
$$a * 1 = 1 * a = a, \ \forall \ a \in G.$$

3. Para cada $a \in G$, existe $b \in G$ tal que
$$a * b = b * a = 1,$$

em que b será denotado por a^{-1} ou $-a$, dependendo da operação binária $*$ ser comutativa ou não.

Assim, um grupo é um par $(G, *)$, onde G é um conjunto e $*$ é uma operação binária sobre G. Na maioria das vezes, diremos simplesmente "o grupo G," sem mencionar qual é a operação binária que está sendo considerada.

4. Se em um grupo G o axioma

$$a * b = b * a, \ \forall \ a, b \in G,$$

é verificado, diremos que G é um *grupo abeliano* ou um *grupo comutativo.*

Sejam G um grupo e H um subconjunto não vazio de G. Diremos que H é um *subgrupo* de G, em símbolos $H \leq G$, quando H munido com a operação binária induzida por G for um grupo.

Sejam A e B subconjuntos de G. Definimos

$$AB = \{ab : a \in A \text{ e } b \in B\} \text{ e } A^{-1} = \{a^{-1} : a \in A\}.$$

Então é fácil verificar que

$$A(BC) = (AB)C, \ \forall \ A, B, C \subseteq G.$$

Proposição 1.1 (Critério de Subgrupo) *Sejam G um grupo e H um subconjunto não vazio de G. Então H é um subgrupo de G se, e somente se, as seguintes condições são satisfeitas*:

1. $1_G \in H$, *com* 1_G *o elemento identidade de* G.

2. *Se* $a, b \in H$, *então* $ab \in H$ (*isto é,* $HH \subseteq H$). (*fechamento*)

3. *Se* $a \in H$, *então* $a^{-1} \in H$ (*isto é,* $H^{-1} \subseteq H$). (*existência de inverso*)

Sejam G um grupo, S um subconjunto de G e $\mathcal{F}$ a família de todos os subgrupos de G contendo S, isto é,

$$\mathcal{F} = \{K \leq G : S \subseteq K\}.$$

Como $G \in \mathcal{F}$ temos que $\mathcal{F} \neq \emptyset$. Seja

$$H = \bigcap_{K \in \mathcal{F}} K.$$

Então H é um subgrupo de G e $S \subseteq H$. Note que se L é qualquer subgrupo de G tal que $S \subseteq L$, então $L \in \mathcal{F}$ e $H \subseteq L$. Portanto, H é o menor subgrupo de G contendo S. O subgrupo H é chamado o *subgrupo de G gerado por S* e será denotado por

$$H = \langle S \rangle .$$

Proposição 1.2 *Sejam G um grupo e S um subconjunto não vazio qualquer de G. Então o subgrupo gerado por S é*:

$$\langle S \rangle = \{a_1 a_2 \cdots a_n : n \in \mathbb{N},\ \ a_i \in S \cup S^{-1}\}.$$

Em particular, se $S = \{a\}$, então $\langle S \rangle = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. De fato,

$$\begin{aligned}
\langle a \rangle &= \{a_1^{t_1} \cdots a_n^{t_n} : n \in \mathbb{N},\ \ a_i \in \{a\} \text{ e } t_i \in \{-1, 1\}\} \\
&= \{a^{t_1} \cdots a^{t_n} : n \in \mathbb{N} \text{ e } t_i \in \{-1, 1\}\} \\
&= \{a^{\sum_{i=1}^{n} t_i} : n \in \mathbb{N} \text{ e } t_i \in \{-1, 1\}\} \\
&= \{a^m : m \in \mathbb{Z}\}.
\end{aligned}$$

Seja G um grupo. Diremos que G é *grupo cíclico* se existir $a \in G$ tal que $G = \langle a \rangle$

1.2 Homomorfismos de Grupos

Sejam G e H grupos. Uma função $\sigma : G \to H$ é um *homomorfismo de grupos* se

$$\sigma(ab) = \sigma(a)\sigma(b),\ \ \forall\ a, b \in G.$$

Intuitivamente, um homomorfismo de grupos σ de G em H é uma função que preserva as operações dos grupos. O conjunto de todos os homomorfismos de G em H será denotado por

$$\mathrm{Hom}\,(G, H) = \{\sigma : G \longrightarrow H : \sigma \text{ é um homomorfismo de grupos}\}.$$

Note que o conjunto $\mathrm{Hom}\,(G, H)$ é sempre não vazio, pois ele contém o homomorfismo $\sigma : G \longrightarrow H$ definido por $\sigma(a) = 1_H$, para todo $a \in G$, chamado de *homomorfismo trivial*.

Seja $\sigma : G \longrightarrow H$ um homomorfismo de grupos. Diremos que σ é um *monomorfismo* (uma *imersão*) se σ é injetora e que σ é um *epimorfismo* (uma *submersão*) se σ é sobrejetora. Diremos

que σ é um *isomorfismo* se σ é bijetora. Quando existir um isomorfismo entre G e H, diremos que G e H são *isomorfos* e será denotado por $G \simeq H$. Intuitivamente, um isomorfismo σ de G sobre H é uma regra que consiste em renomear os elementos de G, isto é, o nome do elemento sendo $\sigma(a)$ ao invés de $a \in G$.

Um *endomorfismo* de um grupo G é um homomorfismo de grupos $\sigma : G \longrightarrow G$. O conjunto de todos os endomorfismos de G será denotado por

$$\mathrm{End}\,(G) = \{\sigma : G \longrightarrow G : \sigma \text{ é um homomorfismo de grupos}\}.$$

Note que o conjunto $\mathrm{End}\,(G)$ contém o homomorfismo $I : G \longrightarrow G$ definido por $I(a) = a$, para todo $a \in G$, chamado de *endomorfismo identidade*.

Um *automorfismo* de um grupo G é um isomorfismo $\sigma : G \longrightarrow G$. O conjunto de todos os automorfismo de G será denotado por

$$\mathrm{Aut}\,(G) = \{\sigma : G \longrightarrow G : \sigma \text{ é um isomorfismo de grupos}\}.$$

Proposição 1.3 *Sejam G e H grupos. Então*:

1. *O conjunto* $\mathrm{Aut}\,(G)$ *munido com a operação usual de composição de funções é um subgrupo do grupo de permutações $P(G)$. Em particular,* $\mathrm{Aut}\,(G) = \mathrm{End}\,(G) \cap P(G)$.

2. *Se $\sigma \in \mathrm{Hom}\,(G, H)$, então $\sigma(1_G) = 1_H$ e $\sigma(a^{-1}) = \sigma(a)^{-1}$, para todo $a \in G$.*

Observação 1.4 *Seja $G = \langle S \rangle$, com*

$$S = \{a_i : a_i \in G \text{ e } i \in I\}.$$

Então para cada $\sigma \in \mathrm{End}\,(G)$ o valor de $\sigma(a)$ para qualquer $a \in G$ é completamente determinado por $\sigma(a_i)$, para todo $i \in I$. Em particular, $G = \langle \sigma(S) \rangle$, para todo $\sigma \in \mathrm{Aut}\,(G)$.

Proposição 1.5 *Sejam G um grupo qualquer, $a \in G$ fixado e $\kappa_a : G \longrightarrow G$ a função definida como $\kappa_a(x) = axa^{-1}$, para todo $x \in G$. Então*:

1. *$\kappa_a \in \mathrm{Aut}\,(G)$ e chama-se* automorfismo interno *de G e os automorfismos σ de $\mathrm{Aut}\,(G)$, com $\sigma \neq \kappa_a$, são chamados de* automorfismos externos *de G.*

2. *Se*

$$\mathrm{Inn}\,(G) = \{\kappa_a \in \mathrm{Aut}\,(G) : a \in G\},$$

então $\mathrm{Inn}\,(G)$ *é um subgrupo de* $\mathrm{Aut}\,(G)$*. Em particular,*

$$\sigma \circ \kappa_a \circ \sigma^{-1} \in \mathrm{Inn}\,(G)\,,\ \ \forall\ \sigma \in \mathrm{Aut}\,(G)\,.$$

Portanto, $\mathrm{Inn}\,(G)$ *é um subgrupo normal de* $\mathrm{Aut}\,(G)$*.*

Seja $\sigma : G \longrightarrow H$ um homomorfismo de grupos. A *imagem* de σ é o conjunto

$$\begin{aligned} \mathrm{Im}\,\sigma &= \{h \in H : h = \sigma(a),\ \text{para algum}\ a \in G\} \\ &= \{\sigma(a) : a \in G\} = \sigma(G). \end{aligned}$$

O *núcleo* de σ é o conjunto

$$\ker \sigma = \{a \in G : \sigma(a) = 1_H\} = \sigma^{-1}(1_H).$$

Se L é um subconjunto de H, então a *imagem inversa* (ou *pullback*) de L é o conjunto

$$\sigma^{-1}(L) = \{a \in G : \sigma(a) \in L\}.$$

Proposição 1.6 *Sejam* G*,* H *grupos e* $\sigma \in \mathrm{Hom}\,(G, H)$*. Então*:

1. $\mathrm{Im}\,\sigma$ *é um subgrupo de* H*.*
2. $\ker \sigma$ *é um subgrupo de* G*. Além disso,* $aNa^{-1} \subseteq N$*, para todo* $a \in G$*, com* $N = \ker \sigma$*. Portanto* $\ker \sigma$ *é um subgrupo normal de* G*.*
3. *Para quaisquer* $a, b \in G$*,* $\sigma(a) = \sigma(b)$ *se, e somente se,* $a^{-1}b \in \ker \sigma$*.*
4. σ *é um monomorfismo se, e somente se,* $\ker \sigma = \{1_G\}$*.*
5. σ *é um epimorfismo se, e somente se,* $\mathrm{Im}\,\sigma = H$*. Neste caso, diremos que* H *é a* imagem homomórfica *de* G*.*
6. σ *é um isomorfismo se, e somente se, existir* $\sigma^{-1} \in \mathrm{Hom}\,(H, G)$ *tal que* $\sigma^{-1} \circ \sigma = I_G$ *e* $\sigma \circ \sigma^{-1} = I_H$ *se, e somente se,* $\ker \sigma = \{1_G\}$ *e* $\mathrm{Im}\,\sigma = H$*.*

Proposição 1.7 *Seja* $G = \langle a \rangle$ *um grupo cíclico de ordem* n*. Para um* $k \in \mathbb{Z}$ *fixado, consideremos o endomorfismo* $\sigma_k : G \to G$ *definido por* $\sigma_k(a) = a^k$*.*

1. $\sigma_k = \sigma_m$ *se, e somente se,* $m \equiv k\ \pmod{n}$*.*

2. *Se* $\sigma \in \mathrm{End}\,(G)$, *então existe um único* $k \in \{0, 1, \ldots, n-1\}$ *tal que* $\sigma = \sigma_k$.

3. *Se* $d = \mathrm{mdc}(m, n)$, *então* $\ker \sigma_m = \ker \sigma_d$ *e* $\mathrm{Im}\,\sigma_m = \mathrm{Im}\,\sigma_d$.

4. $\sigma_k \in \mathrm{Aut}\,(G)$ *se, e somente se,* $\mathrm{mdc}(n, k) = 1$.

5. *Se* $\sigma \in \mathrm{Aut}(G)$, *então* $\sigma = \sigma_k$, *para algum* $k \in \{0, 1, \ldots, n-1\}$ *tal que com* $\mathrm{mdc}(n, k) = 1$.

6. *A função* $\varphi : \mathcal{U}(\mathbb{Z}_n) \to \mathrm{Aut}(G)$ *definida como* $\varphi(\overline{k}) = \sigma_k$ *é um isomorfismo, em que*

$$\mathcal{U}(\mathbb{Z}_n) = \{\overline{k} \in \mathbb{Z}_n : \mathrm{mdc}(n, k) = 1\}.$$

Neste caso, $\mathrm{Aut}(G)$ *é um grupo cíclico de ordem* $\phi(n)$.

Prova. Vamos provar apenas o item (4). Suponhamos que $\sigma_k \in \mathrm{Aut}\,(G)$. Então

$$n = |a| = |\sigma_k(a)| = \left|a^k\right|.$$

Seja $d = \mathrm{mdc}(n, k)$. Então

$$\left(a^k\right)^{\frac{n}{d}} = (a^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e \Rightarrow n \text{ divide } \frac{n}{d} \Rightarrow d = 1.$$

Logo, $\mathrm{mdc}(n, k) = 1$.

Reciprocamente, suponhamos que $\mathrm{mdc}(n, k) = 1$, então existem $r, s \in \mathbb{Z}$ tais que

$$rn + sk = 1.$$

Assim,

$$b = b^1 = b^{rn+sk} = (b^k)^s, \ \forall \ b \in G.$$

Logo,

$$b \in \ker \sigma_k \Rightarrow \sigma_k(b) = e \Rightarrow b^k = e \Rightarrow b = (b^k)^s = e^s = e,$$

isto é, σ_k é injetora. Dado $b \in G$, existe $c = b^s \in G$ tal que $\sigma_k(c) = b$, isto é, σ_k é sobrejetora. É claro que σ_k é um homomorfismo de grupos. ■

Sejam G um grupo e N um subgrupo de G. Diremos que N é um *subgrupo normal* (ou *subgrupo invariante*) em G, em símbolos $N \trianglelefteq G$, se

$$aha^{-1} \in N, \ \forall \ a \in G \text{ e } h \in N,$$

ou, equivalentemente,

$$\kappa_a(N) \subseteq N, \ \forall \ \kappa_a \in \mathrm{Inn}(G).$$

Proposição 1.8 *Seja G um grupo. Então*:

1. *N é um subgrupo normal em G se, e somente se $aN = Na$, para todo $a \in G$.*
2. *N é um subgrupo normal em G se, e somente se $aNa^{-1} = N$, para todo $a \in G$.*
3. *Se N e K são subgrupos normais em G, então $N \cap K$ é um subgrupo normal em G.*
4. *Se N é um subgrupo normal em G e K é um subgrupo de G, então $N \cap K$ é um subgrupo normal em K.*
5. *Se N e K são subgrupos normais em G, então NK é um subgrupo normal em G.*
6. *Se N e K são subgrupos normais em G, com $N \cap K = \{e\}$, então $hk = kh$, para todo $h \in N$ e $k \in K$.*

Sejam G um grupo e N um subgrupo normal em G. Então $\frac{G}{N}$ munido com a operação binária

$$(aN) * (bN) = abN, \ \forall \ a, b \in G,$$

é um grupo, chamado de *grupo quociente* ou *grupo fator* de G por N.

Observação 1.9 *Qualquer subgrupo normal é núcleo de um homomorfismo.*

Teorema 1.10 (Primeiro Teorema de Isomorfismo) *Seja $\varphi : G \to K$ um homomorfismo de grupos. Então*

$$\frac{G}{\ker \varphi} \simeq \operatorname{Im} \varphi.$$

Em particular, se G é grupo finito, então $|G| = |\ker \varphi| \, |\operatorname{Im} \varphi|$. Neste caso, $|\ker \varphi|$ divide $|G|$ e $|\operatorname{Im} \varphi|$ divide $|G|$.

Proposição 1.11 *Sejam G e H grupos isomorfos. Então* $\operatorname{Aut}(G)$ *e* $\operatorname{Aut}(H)$ *são grupos isomorfos.*

Prova. Seja $\theta : G \longrightarrow H$ qualquer isomorfismo de grupos. Então a função $f : \operatorname{Aut}(G) \to \operatorname{Aut}(H)$ definida como $f(\sigma) = \theta \circ \sigma \circ \theta^{-1}$ é claramente um isomorfismo, confira diagrama:

$$\begin{array}{ccc} G & \underrightarrow{\sigma} & G \\ \theta^{-1} \uparrow & & \downarrow \theta \\ H & \overrightarrow{\theta \circ \sigma \circ \theta^{-1}} & H \end{array}$$

Portanto, $\operatorname{Aut}(G)$ e $\operatorname{Aut}(H)$ são grupos isomorfos. ■

1.3 Produto Direto

Sejam G_1, G_2,..., G_n grupos. O *produto direto* (externo) dos grupos G_1, G_2,..., G_n é o conjunto

$$G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) : g_i \in G_i\}$$

munido da operação binária

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 *_1 h_1, g_2 *_2 h_2, \ldots, g_n *_n h_n),$$

com $(1_{G_1}, \ldots, 1_{G_n})$ o elemento identidade e $\left(g_1^{-1}, \ldots, g_n^{-1}\right)$ é o inverso do elemento $(g_1, \ldots, g_n)$.

Proposição 1.12 *Sejam $G_1, G_2, \ldots, G_n$ grupos e*

$$G = \prod_{i=1}^{n} G_i.$$

1. *A função $\lambda_i : G_i \hookrightarrow G$ definida como*

$$\lambda_i(g_i) = (1_{G_1}, \ldots, g_i, \ldots, 1_{G_n})$$

é um homomorfismo de grupos injetor. Neste caso,

$$G_i \simeq \widehat{G}_i = \lambda_i(G_i) = \{1_{G_1}\} \times \cdots \times \{1_{G_{i-1}}\} \times G_i \times \{1_{G_{i+1}}\} \times \cdots \times \{1_{G_n}\}.$$

Em particular, se identificamos G_i com $\widehat{G}_i$, então G_i é um subgrupo normal em G e

$$\frac{G}{G_i} \simeq G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. *A função $\pi_i : G \twoheadrightarrow G_i$ definida como*

$$\pi_i (g_1, \ldots, g_n) = g_i$$

é um homomorfismo de grupos sobrejetor. Neste caso,

$$\begin{aligned} \ker \pi_i &= \pi_i^{-1}(1_{G_i}) = G_1 \times \cdots \times G_{i-1} \times \{1_{G_i}\} \times G_{i+1} \times \cdots \times G_n \\ &\simeq G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n. \end{aligned}$$

3. *Sob a identificação do item* (1), *$ab = ba$, para todo $a \in G_i$ e $b \in G_j$, com $i \neq j$.*

Sejam G um grupo e H_i subgrupos de G, $i = 1, \ldots, n$. Diremos que G é o *produto direto* (*interno*) dos H_i se as seguintes condições são satisfeitas:

1. $h_i h_j = h_j h_i$, para todo $h_i \in H_i$ e $h_j \in H_j$ com $i \neq j$.

2. Qualquer $a \in G$ pode ser escrito de modo único sob a forma

$$a = h_1 \cdots h_n, \;\; h_i \in H_i, \;\; i = 1, \ldots, n.$$

Observe que, ao contrário do produto direto externo, o produto direto interno nem sempre existe, por exemplo, se $G = S_3$, $H = \langle \sigma \rangle$ e $K = \langle \tau \rangle$, com

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

então H e K são subgrupos de G, mas $\sigma\tau \neq \tau\sigma$. Portanto, G não é um produto direto interno de H e K. Note que o produto direto interno pode ser generalizado para uma família qualquer de grupos.

Proposição 1.13 *Sejam G um grupo e H_i subgrupos de G, $i = 1, \ldots, n$. Então G é um produto direto interno dos H_i se, e somente se,*

1. $G = H_1 \cdots H_n$.

2. H_i *é um subgrupo normal em* G, *para cada* $i = 1, \ldots, n$.

3. $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{1\}$, *para cada* $i = 1, \ldots, n$.

4. $H_i \cap (H_1 \cdots H_{i-1}) = \{1\}$, *para cada* $i = 2, \ldots, n$.

Corolário 1.14 *Sejam G um grupo e H_i subgrupos de G, $i = 1, \ldots, n$. Se G é um produto direto interno dos H_i, então*

$$G \simeq H_1 \times \cdots \times H_n.$$

Como um abuso de notação vamos escrever $G = H_1 \times \cdots \times H_n$, ou seja, qualquer elemento $g \in H_1 \times \cdots \times H_n$ pode ser escrito de modo único sob a forma

$$g = h_1 \cdots h_n, \;\; h_i \in H_i, \;\; i = 1, \ldots, n.$$

Prova. Como $G = H_1 \cdots H_n$ temos que a função $\varphi : G \to H_1 \times \cdots \times H_n$ definida por $\varphi(a) = (h_1, \ldots, h_n)$, com $a = h_1 \cdots h_n$, está bem definida. Agora, é fácil verificar que φ é um isomorfismo. ■

Lema 1.15 *Sejam G um grupo e $a \in G$, com ordem mn e* $\mathrm{mdc}(m,n) = 1$. *Então existem únicos $b, c \in G$ tais que*

$$a = bc = cb, \ \ com \ \ |b| = m \ \ e \ \ |c| = n.$$

Prova. (Existência) Como $\mathrm{mdc}(m,n) = 1$ temos que existem $r, s \in \mathbb{Z}$ tais que $rm + sn = 1$. Logo,

$$a = a^1 = a^{rm+sn} = a^{rm}a^{sn} = a^{sn}a^{rm}.$$

Pondo $b = a^{sn}$ e $c = a^{rm}$, obtemos $a = cb = bc$. Sejam $|b| = k$ e $|c| = l$. Então $b^k = e$ e $c^l = e$. Como

$$b^m = (a^{sn})^m = (a^{mn})^s = e^s = e \ \text{ e } \ c^n = (a^{rm})^n = (a^{mn})^r = e^r = e$$

temos que existem $u, v \in \mathbb{Z}$ tais que $m = uk$ e $n = vl$. Assim, kl divide $\mathrm{mmc}(m,n) = mn$, pois

$$mn = (uk)(vl) = (uv)kl.$$

Por outro lado,

$$a^{kl} = (bc)^{kl} = (b^k)^l(c^l)^k = e^l e^k = e \Rightarrow mn \mid kl.$$

Logo,

$$mn = kl \Rightarrow ukn = kl \Rightarrow un = l \Rightarrow n \mid l.$$

Portanto, $n = l$. De modo inteiramente análogo prova-se que $m = k$, ou seja, $|b| = m$ e $|c| = n$.

(Unicidade) Suponhamos que $a = xy = yx$, com $|x| = m$ e $|y| = n$. Então

$$bc = xy \Leftrightarrow x^{-1}b = yc^{-1}.$$

Logo,

$$ax = (xy)x = x(yx) = xa \ \text{ e } \ ay = (yx)y = y(xy) = ya.$$

É fácil verificar que

$$bx = xb, \ \ by = yb, \ \ cx = xc \ \text{ e } \ cy = yc.$$

Assim,

$$(x^{-1}b)^m = x^{-m}b^m = e \ \text{ e } \ (x^{-1}b)^n = (yc^{-1})^n = y^n c^{-n} = e.$$

Portanto, $x^{-1}b = e$, pois $\mathrm{mdc}(m,n) = 1$. Donde concluímos que $b = x$ e $c = y$. ■

Corolário 1.16 *Sejam $m, n \in \mathbb{N}$, com* $\mathrm{mdc}(m,n) = 1$. *Então*:

1. $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$.

2. Se $n = p_1^{\alpha_1}.p_2^{\alpha_2}.\cdots.p_k^{\alpha_k}$, *então* $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$.

Prova. Como $\mathbb{Z}_{mn} = \langle a \rangle$ temos, pelo Lema 1.15, que existem únicos $b, c \in \mathbb{Z}_{mn}$ tais que

$$a = bc = cb, \text{ com } |b| = m \text{ e } |c| = n.$$

Logo, a função $\sigma : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ definida como $\sigma(a) = (b, c)$ é bijetora e é um homomorfismo. ■

1.4 Grupos Abelianos Finitos

Nesta seção apresentaremos um método sistemático de determinar todos os grupos abelianos finitos de uma determinada ordem. Mas antes vamos apresentar alguns conceitos e resultados.

Lema 1.17 *Sejam* G *um* p*-grupo abeliano finito e* $g^{p^k} \neq 1$, *para algum* $k \in \mathbb{Z}_+$. *Se a ordem de* g^{p^k} *é igual a* p^m, *então a ordem de* g *é igual a* p^{k+m}.

Prova. Seja p^n a ordem de g. Então $n > k$. Como

$$g^{p^{k+m}} = \left(g^{p^k}\right)^{p^m} = 1$$

temos que p^n divide p^{k+m}, isto é, $n \leq m + k$ Por outro lado, como

$$\left(g^{p^k}\right)^{p^{n-k}} = g^{p^n} = 1$$

temos que p^m divide p^{n-k}, isto é, $m \leq n - k$ Portanto, $p^n = p^{k+m}$. ■

Lema 1.18 *Sejam* G *um grupo abeliano e* $n \in \mathbb{N}$, *com* $n \geq 2$. *Então a função* $\varphi : G \to G$ *definida como* $\varphi(x) = x^n$ *é um homomorfismo de grupos. Além disso,*

$$\frac{G}{\ker \varphi} \simeq \operatorname{Im} \varphi, \ \ker \varphi = \{a \in G : a^n = 1\} \ e \ \operatorname{Im} \varphi = \{a^n : a \in G\}.$$

Proposição 1.19 *Sejam* G *um grupo abeliano de ordem* $n > 1$ *e*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

a fatoração de n *em fatores primos distintos. Então*

$$G = H_{p_1} \times H_{p_2} \times \cdots \times H_{p_k},$$

com $H_{p_i} = \{a \in G : a^{p_i^{\alpha_i}} = 1\}$ *de ordem* $p_i^{\alpha_i}$ *para* $i \in \{1, \ldots, k\}$. *Além disso dita decomposição é única.*

Prova. Vamos usar indução sobre l, com $1 \leq l \leq k$. Como

$$H_{p_i} = \{a \in G : a^{p_i^{\alpha_i}} = 1\}$$

é um subgrupo normal em G temos que $H_{p_1} \cdots H_{p_l}$ é um subgrupo de G. Sejam $H = H_{p_1} \cdots H_{p_{l-1}}$ e $K = H_{p_l}$. Então, pelo Corolário 1.14,

$$H = H_{p_1} \times \cdots \times H_{p_{l-1}} \text{ e } |H| = |H_{p_1}| \cdots \left|H_{p_{l-1}}\right|.$$

Por outro lado, como o $\text{mdc}(|H|, |K|) = 1$ temos, pelo Teorema de Lagrange, que $H \cap K = \{1\}$. Logo,

$$H \times K = \left(H_{p_1} \times \cdots \times H_{p_{l-1}}\right) \times H_{p_l} \simeq H_{p_1} \times \cdots \times H_{p_{l-1}} \times H_{p_l}.$$

Em particular,

$$G = H_{p_1} \times H_{p_2} \times \cdots \times H_{p_k},$$

que é o resultado desejado. ■

Sejam p um número primo e E um p-grupo. Diremos que E é um *p-grupo abeliano elementar* se qualquer elemento de $E - \{1\}$ possui ordem p.

Lema 1.20 *Seja E um p-grupo abeliano elementar. Então para qualquer $x \in E$ existe um subgrupo M de E tal que $E = M \times \langle x \rangle$.*

Prova. Se $x = 1$, então $E = M$. Se $x \neq 1$, então existe um subgrupo M de E de ordem maximal tal que $x \notin M$. Se $[E : M] \neq p$, então o conjunto

$$\overline{E} = \frac{E}{M}$$

é um p-grupo abeliano elementar e existe $\overline{y} \in \overline{E} - \langle \overline{x} \rangle$. Como $\overline{y}^p = \overline{1}$ temos que $\overline{x} \notin \langle \overline{y} \rangle$. Assim, pelo Teorema da correspodência, $\langle \overline{y} \rangle = \langle yM \rangle$ é da forma $\frac{L}{M}$, onde L é um subgrupo de E contendo M e $x \notin L$, o que cotradiz a maximalidade M. Logo,

$$[E : M] = p, \;\; E = M \langle x \rangle \;\; \text{e} \;\; M \cap \langle x \rangle = \{1\}.$$

Portanto, pelo Corolário 1.14, $E = M \times \langle x \rangle$. ■

Teorema 1.21 *Sejam G um grupo abeliano de ordem $n > 1$ e*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

a fatoração de n em fatores primos distintos. Então:

1. *$G = H_{p_1} \times H_{p_2} \times \cdots \times H_{p_k}$, com $|H_{p_i}| = p_i^{\alpha_i}$.*

2. *Para cada $H_{p_i} \in \{H_{p_1}, \ldots, H_{p_k}\}$, com $|H_{p_i}| = p_i^{\alpha_i}$, obtemos*

$$H_{p_i} = \mathbb{Z}_{p_i^{e_1}} \times \mathbb{Z}_{p_i^{e_2}} \times \cdots \times \mathbb{Z}_{p_i^{e_t}},$$

com $1 \leq e_1 \leq e_2 \leq \cdots \leq e_t$ e $e_1 + e_2 + \cdots + e_t = \alpha_i$ (em que t e $e_1, \ldots, e_t$ dependem de i). Neste caso, diremos que H_{p_i} é um grupo do tipo

$$(p_i^{e_1}, p_i^{e_2}, \ldots, p_i^{e_t})$$

3. *As decomposições em* (1) *e* (2) *são únicas.*

Prova. (Existência) Pelo Corolário 1.14, basta provar que H_p, com p um número primo, é um produto de grupos cíclicos. Vamos usar indução sobre $|H_p|$. Consideremos a função $\varphi : H_p \to H_p$ definida como $\varphi(x) = x^p$. Então, pelo Lema 1.18, φ é um homomorfismo de grupos. Sejam $E = \ker \varphi$ e $K = \operatorname{Im} \varphi$. Então, pelo Primeiro Teorema de Isomorfismo,

$$\frac{H_p}{E} \simeq K \text{ implica que } E, \ \frac{H_p}{K}$$

são p-grupos abelianos elementares e

$$|H_p| = |E|\,|K| \ \text{ e } \ [H_p : K] = |E|\,,$$

ou seja, desde que $|E| > 1$, $|K| < |H_p|$. Assim, pela hipótese de indução,

$$K = \langle k_1 \rangle \times \langle k_2 \rangle \times \cdots \times \langle k_t \rangle = \mathbb{Z}_{p_i^{e_1}} \times \mathbb{Z}_{p_i^{e_2}} \times \cdots \times \mathbb{Z}_{p_i^{e_t}}, \ \ e_i \geq 1, \ \ i = 1, \ldots, t.$$

Como $k_i \in K = \operatorname{Im} \varphi$ temos que existe $h_i \in H_p$ tal que

$$k_i = \varphi(h_i) = h_i^p, \ \ i = 1, \ldots, t.$$

Seja $H_0 = \langle h_1, h_2, \ldots, h_t \rangle$ o subgrupo finitamente gerado de H_p. Então:

(a) $H_0 = \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \times \langle h_t \rangle$.

(b) O grupo quociente

$$\frac{H_0}{K} = \langle h_1 K \rangle \times \langle h_2 K \rangle \times \cdots \times \langle h_t K \rangle$$

é um p-grupo abeliano elementar de ordem p^t.

(c) O subgrupo

$$E \cap K = \left\langle h_1^{p_i^{e_1-1}} \right\rangle \times \left\langle h_2^{p_i^{e_2-1}} \right\rangle \times \cdots \times \left\langle h_t^{p_i^{e_t-1}} \right\rangle$$

é um grupo abeliano elementar de ordem p^t.

De fato, como

$$H_0 = \langle h_1, h_2, \ldots, h_t \rangle = \langle h_1 \rangle \langle h_2 \rangle \cdots \langle h_t \rangle, \text{ com } \langle h_i \rangle \cap \langle h_2 \rangle \cdots \langle h_{i-1} \rangle = \{1\},$$

temos, pelo Corolário 1.14, que $H_0 = \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \times \langle h_t \rangle$. Os outros itens, provam-se de modo análogo. Agora, se $E \subseteq K$ então

$$[H_p : K] = |E| = |E \cap K| = p^t = [H_0 : K].$$

Logo, $H_p = H_0$ e o teorema está provado. Se E não é subgrupo de K, então existe $x \in E$ tal que $x \notin K$, de modo que

$$|\langle \overline{x} \rangle| = |\langle xK \rangle| = |\langle x \rangle| = p.$$

Assim, pelo Lema 1.20, existe um subgrupo $\overline{M}$ de

$$\overline{H}_p = \frac{H_p}{K}$$

tal que

$$\overline{H}_p = \overline{M} \times \langle \overline{x} \rangle.$$

Pelo Teorema da correspodência, $\overline{M} = yK$ é da forma $\frac{M}{K}$, onde M é um subgrupo de H_p contendo K, ou seja, $M \cap \langle x \rangle = \{1\}$, pois a ordem de x é igual a p e $x \notin M$. Portanto,

$$H_p = M \times \langle x \rangle.$$

Pela hipótese de indução, M é um produto de grupos cíclicos e, consequentemente, H_p é um produto de grupos cíclicos.

(Unicidade) Vamos usar indução sobre $|H_p|$. Suponhamos que H_p tenha duas decomposições do tipo

$$(p^{e_1}, p^{e_2}, \ldots, p^{e_s}) \text{ e } (p^{f_1}, p^{f_2}, \ldots, p^{f_t}),$$

com $1 \leq e_1 \leq e_2 \leq \cdots \leq e_s$ e $1 \leq f_1 \leq f_2 \leq \cdots \leq f_t$. Já vimos que a função $\varphi : H_p \to H_p$ definida como $\varphi(x) = x^p$ é um homomorfismo de grupos. Sejam $E = \ker \varphi$ e $K = \operatorname{Im} \varphi$. Então

$$E \text{ e } \frac{H_p}{K}$$

são p-grupos abelianos elementares e, pelo Primeiro Teorema de Isomorfismo,

$$|H_p| = |E|\,|K| \;\text{ e }\; [H_p : K] = |E|\,,$$

ou seja, $|K| < |H_p|$ e K é do tipo

$$(p^{e_1-1}, p^{e_2-1}, \ldots, p^{e_s-1}) \;\text{ e }\; (p^{f_1-1}, p^{f_2-1}, \ldots, p^{f_t-1}),$$

Note que se $e_i - 1 = 0$ ou $f_j - 1 = 0$, então o grupo fator de K correspondendo a p^{e_i-1} ou p^{f_j-1} é simplesmente o grupo $\{1\}$. Assim, pela hipótese de indução, obtemos $e_i - 1 = f_i - 1$, para todo i, com $e_i - 1 > 0$ ou $f_i - 1 > 0$, ou seja, $e_i = f_i$. Portanto, as duas sequências

$$(p^{e_1}, p^{e_2}, \ldots, p^{e_s}) \;\text{ e }\; (p^{f_1}, p^{f_2}, \ldots, p^{f_t}),$$

podem diferir apenas nas primeira coordenadas, as quais são iguais a p. Neste caso,

$$(p, \ldots, p, p^{e_1}, p^{e_2}, \ldots, p^{e_u}) \;\text{ e }\; (p, \ldots, p, p^{e_1}, p^{e_2}, \ldots, p^{e_u}),$$

Assim, a ordem de H_p é igual

$$p^{\beta} p^{e_1+e_2+\cdots+e_u} = p^{\gamma} p^{e_1+e_2+\cdots+e_u},$$

Logo, $\beta = \gamma$ e unicidade está provado. ■

Os números inteiros $p_j^{\alpha_j}$ descritos no Teorema chamam-se *divisores elementares* de G e

$$G = H_{p_1} \times H_{p_2} \times \cdots \times H_{p_k}$$

chama-se *decomposição em divisores elementares* de G. Os subgrupos H_{p_i} são p_i-subgrupos de Sylow de G. Assim, eles são únicos.

Note que para um número primo p fixado, p^e divide p^f se, e somente se, $e \leq f$. Além disso,

$$p^{e_1} p^{e_2} \cdots p^{e_t} = p^{\alpha}$$

se, e somente se,

$$e_1 + e_2 + \cdots + e_t = \alpha.$$

Portanto, a decomposição em divisores elementares de G, com a condição "divisibilidade" dos inteiros p^e vista como a condição "aditiva" de seus expoentes implica que os divisores elementares de G podem ser vistos como os fatores invariantes dos p-subgrupos de Sylow, para qualquer número primo p dividindo a ordem de G. Observe que os divisores elementares de G não são fatores invariantes de G, mas são fatores invariantes do subgrupo H_p.

Observação 1.22 *As condições* (1), (2) *e* (3) *para os fatores invariantes descritas no Teorema podem ser escolhidas como*:

1. $e_j \geq 1$ *para todo* $i = 1, \ldots, t$.

2. $e_i \leq e_{i+1}$ *para todo* $i = 1, \ldots, t-1$.

3. $e_1 + e_2 + \cdots + e_t = \alpha$.

Portanto, cada lista de fatores invariantes é simplesmente uma partição de α. (ordenados em ordem crescente). Em particular, o número de grupos abelianos não isomorfos de ordem p^α (igual ao número de listas distintas) é igual ao número de partições de α. Note que ssse número não dependente de p. Por exemplo, o número de grupos abelianos de ordem p^4 é obtida a partir da lista de partições de 4:

Fatores Invariantes	Grupos abelianos
4	$\mathbb{Z}_{p^4}$
$1, 3$	$\mathbb{Z}_p \times \mathbb{Z}_{p^3}$
$2, 2$	$\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$
$1, 1, 2$	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$
$1, 1, 1, 1$	$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Assim, existem exatamente 5 grupos de ordem p^4 não isomorfos. Neste caso, se

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

e q_i é o número de partições de α_i, então o número de grupos abelianos de ordem n é igual a

$$q_1 q_2 \cdots q_k.$$

Finalizaremos esta seção classificando todos os grupos abelianos de ordem

$$n = 1800 = 2^3 3^2 5^2,$$

listamos os grupos abelianos desta ordem como segue:

Ordem p^α	Partições de α	Grupos abelianos
2^3	$3; 1, 2; 1, 1, 1$	$\mathbb{Z}_{2^3}; \mathbb{Z}_2 \times \mathbb{Z}_{2^2}; \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
3^2	$2, 1, 1$	$\mathbb{Z}_{3^2}; \mathbb{Z}_3 \times \mathbb{Z}_3$
5^2	$2; 1, 1$	$\mathbb{Z}_{5^2}; \mathbb{Z}_5 \times \mathbb{Z}_5$

Portanto, existem 12 grupos abelianos distintos de ordem 1800:

$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$
$\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_{25}$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

Capítulo 2

Automorfismos de Grupos Abelianos Finitos

Neste capítulo, descreveremos o endomorfismo de anéis H_p como um quociente de um subanel das matrizes de $\mathbb{Z}^{t\times t}$ e em seguida vamos classificar todos os automorfismos de um grupo abeliano finito G e enumeramo-los.

2.1 Endomorfismos de p-Grupos Abelianos

Nesta seção vamos determinar os endomorfismos de p-grupos abelianos finitos. Seja

$$G = \langle a \rangle \simeq \mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$$

um grupo cíclico isomorfo ao grupo aditivo dos números inteiros de módulo n. Então já vimos que $n\mathbb{Z}$ é um subgrupo de $m\mathbb{Z}$ se, e somente se, existe único $k \in \mathbb{Z}$ tal que $n = km$. Com essa condição,

$$H \simeq \frac{m\mathbb{Z}}{n\mathbb{Z}}$$

é um subgrupo de G. Assim, pelo Terceiro Teorema de Isomorfismo,

$$\frac{G}{H} \simeq \frac{\frac{\mathbb{Z}}{n\mathbb{Z}}}{\frac{m\mathbb{Z}}{n\mathbb{Z}}} \simeq \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Portanto, $[G : H] = m$ e, pelo Teorema de Lagrange, $|H| = k$. Logo, concluímos que

$$H \simeq \frac{\mathbb{Z}}{k\mathbb{Z}} \text{ e } H = \{1, a^m, a^{2m}, \ldots, a^{(k-1)m}\} = G^m \trianglelefteq G.$$

Note que

$$H \simeq \{\overline{0}, \overline{m}, \overline{2m}, \ldots, \overline{(k-1)m}\} = m\mathbb{Z}_n.$$

Por exemplo, podemos identificar $\mathbb{Z}_4$ com o subgrupo $K = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$ de $\mathbb{Z}_{12}$.

Proposição 2.1 *Seja G um grupo abeliano finito. Então o conjunto* $\mathrm{End}(G)$ *munido com as operações binárias $\sigma + \tau$ e $\sigma \circ \tau$ definidas como*

$$(\sigma + \tau)(x) = \sigma(x) + \tau(x) \ \text{ e } \ (\sigma \circ \tau)(x) = \sigma(\tau(x)), \ \forall \ x \in G,$$

é um anel com identidade. Em particular, $\mathrm{End}(\mathbb{Z}_n)$ *é isomorfo a $\mathcal{Z}_n$, com $\mathcal{Z}_n$ o anel dos números inteiros de módulo n.*

Prova. Pelo item (2) da Proposição 1.7, qualquer $\sigma \in \mathrm{End}(\mathbb{Z}_n)$ é da forma $\sigma = \sigma_k$, onde $k \in \{0, 1, \ldots, n-1\}$ e $\sigma_k : \mathbb{Z}_n \to \mathbb{Z}_n$ é a função definida como $\sigma_k(\overline{1}) = \overline{k}$. Então é fácil verificar que a função $f : \mathrm{End}(\mathbb{Z}_n) \to \mathcal{Z}_n$ definida como $f(\sigma_k) = \overline{k}$ é um isomorfismo de aneis. ■

Lema 2.2 *Sejam H, K grupos, $\pi_1 : H \times K \to H$, $\pi_2 : H \times K \to K$ as projeções canônicas e $\lambda_1 : H \to H \times K$, $\lambda_2 : K \to H \times K$ as imerções canônicas. Então*:

1. $\lambda_1(h) \cdot \lambda_2(k) = \lambda_2(k) \cdot \lambda_1(h)$, *para todo $h \in H$ e $k \in K$.*
2. $\pi_1 \circ \lambda_1 = I_H$ *e* $\pi_2 \circ \lambda_2 = I_K$.
3. *Se $i \neq j$, então $\pi_i \circ \lambda_j$ é o homomorfismo trivial.*
4. $(\lambda_1 \circ \pi_1) \cdot (\lambda_2 \circ \pi_2) = I_{H \times K}$.
5. $\pi_1 \circ \sigma \circ \lambda_1 \in \mathrm{End}(H)$ *e* $\pi_2 \circ \sigma \circ \lambda_2 \in \mathrm{End}(K)$, *para todo* $\sigma \in \mathrm{End}(H \times K)$.

Seja

$$H_p = \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_t}},$$

com $1 \leq e_1 \leq e_2 \leq \cdots \leq e_t$, $e_1 + e_2 + \cdots + e_t = \alpha$ e $|H_p| = p^\alpha$. Note que

$$p^{e_1} \mid p^{e_2} \mid \cdots \mid p^{e_t}.$$

Seja g_i o gerador de $\mathbb{Z}_{p^{e_i}}$. Então cada $g \in H_p$ pode ser escrito sob a forma

$$g = g_1^{k_1} \cdots g_t^{k_t},$$

com $0 \leq k_i \leq (p^{e_i} - 1)$. Assim, uma "base" de H_p é o conjunto

$$\{g_1, \ldots, g_t\}.$$

É útil, às vezes, considerar os k_i como elementos do anel $\mathcal{Z}_{p^{e_i}}$, de modo que a exponenciação define um isomorfismo entre o grupo cíclico $\mathbb{Z}_{p^{e_i}}$ e o grupo cíclico aditivo dos inteiros módulo p^{e_i}, a saber,

$$g_i \leftrightarrow \overline{1} = \{x \in \mathbb{Z} : x \equiv 1 (\mathrm{mod}\, p^{e_i})\} \text{ e } (\mathbb{Z}_{p^{e_i}}, +) = \langle \overline{1} \rangle = \{\overline{0}, \overline{1}, \ldots, \overline{p^{e_i} - 1}\}.$$

Portanto, em tudo que segue, cada elemento de H_p vai ser identificado com um vetor coluna

$$(\overline{h}_1, \ldots, \overline{h}_t)^T,$$

onde $\overline{h}_i \in \mathbb{Z}_{p^{e_i}}$ e $h_i \in \mathbb{Z}$ é o representante de classe. Assim, vamos considerar o conjunto das matrizes quadradas de ordem t:

$$R_p = \left\{(a_{ij}) \in \mathbb{Z}^{t \times t} : p^{e_i - e_j} \text{ divide } a_{ij}, \text{ se } 1 \leq j \leq i \leq t\right\}.$$

Exemplo 2.3 *Seja* $H_p = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^5}$. *Então*

$$R_p = \left\{ \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ p^2 a_{31} & p^2 a_{32} & a_{33} & a_{34} \\ p^4 a_{41} & p^4 a_{42} & p^2 a_{43} & a_{44} \end{bmatrix} : a_{ij} \in \mathbb{Z} \right\}.$$

Observação 2.4 *Seja* $A = (a_{ij}) \in R_p$ *fixada. Então a condição que* $p^{e_i - e_j}$ *divide* a_{ij} *é equivalente a existência de uma decomposição*

$$A = PBP^{-1},$$

em que $B \in \mathbb{Z}^{t \times t}$ *e* $P = \mathrm{diag}(p^{e_1}, p^{e_2}, \ldots, p^{e_t})$. *De fato, como* $p^{e_i - e_j}$ *divide* a_{ij} *temos que existe* $b_{ij} \in \mathbb{Z}$ *tal que* $a_{ij} = p^{e_i - e_j} b_{ij}$. *Assim,*

$$\begin{aligned} A &= \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1t} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t1} & a_{m2} & \ldots & a_{mm} \end{bmatrix} \\ &= \begin{bmatrix} p^{e_1} b_{11} p^{-e_1} & p^{e_1} b_{12} p^{-e_2} & \ldots & p^{e_1} b_{1t} p^{-e_t} \\ p^{e_2} b_{21} p^{-e_1} & p^{e_2} b_{22} p^{-e_2} & \ldots & p^{e_2} b_{2t} p^{-e_t} \\ \vdots & \vdots & \ddots & \vdots \\ p^{e_t} b_{t1} p^{-e_1} & p^{e_t} b_{t2} p^{-e_2} & \ldots & p^{e_t} b_{tt} p^{-e_t} \end{bmatrix} \\ &= PBP^{-1}. \end{aligned}$$

Lema 2.5 *R_p é um anel com unidade não comutativo.*

Prova. Dados $A_1, A_2 \in R_p$, obtemos

$$A_1 + A_2 = PB_1P^{-1} + PB_2P^{-1} = P(B_1 + B_2)P^{-1} \in R_p,$$

pois $B_1 + B_2 \in \mathbb{Z}^{t\times t}$. Logo, $A_1 + A_2 \in R_p$, isto é, a soma usual de matrizes é uma operação binária sobre R_p. É claro que essa operação é associativa, comutativa, a matriz nula O_t é o elemento identidade de R_p e $-A$ é o elemento inverso de A em R_p. Agora,

$$A_1 \cdot A_2 = (PB_1P^{-1}) \cdot (PB_2P^{-1}) = P(B_1 \cdot B_2)P^{-1} \in R_p,$$

pois $B_1 \cdot B_2 \in \mathbb{Z}^{t\times t}$. Logo, $A_1 \cdot A_2 \in R_p$, isto é, o produto usual de matrizes é uma operação binária sobre R_p. É claro que essa operação é associativa e a matriz identidade I_t é o elemento identidade de R_p. Portanto, $(R_p, +, \cdot)$ é um anel com unidade não comutativo. ■

Seja $\pi : \mathbb{Z}^t \longmapsto H_p$ a função definida como

$$\pi\left(h_1, \ldots, h_t\right)^T = \left(\pi_1\left(h_1\right), \ldots, \pi_t\left(h_t\right)\right)^T = \left(\overline{h}_1, \ldots, \overline{h}_t\right)^T,$$

em que $\pi_i : \mathbb{Z} \to \mathbb{Z}_{p^{e_i}}$ são as projeções canônicas. Então π é claramente um homomorfismo de grupos sobrejetor.

Teorema 2.6 *Seja $E_p = \mathrm{End}(H_p)$. Então a função $\sigma : R_p \longmapsto E_p$ definida como $\sigma(A) = \sigma_A$ é um homomorfismo de aneis sobrejetor, em que $\sigma_A : H_p \to H_p$ é definida como*

$$\sigma_A(\overline{h}_1, \ldots, \overline{h}_t)^T = \pi(A(h_1, \ldots, h_t)^T).$$

Prova. Seja $A = (a_{ij}) \in R_p$ fixada. A função $\sigma_A : H_p \to H_p$ definida como

$$\sigma_A(\overline{h}_1, \ldots, \overline{h}_t)^T = \pi(A(h_1, \ldots, h_t)^T)$$

é um homomorfismo de grupos. Dados $(\overline{g}_1, \ldots, \overline{g}_t)^T, (\overline{h}_1, \ldots, \overline{h}_t)^T \in \mathbb{Z}^{t\times 1}_{p^{e_i}}$, se

$$(\overline{g}_1, \ldots, \overline{g}_t)^T = (\overline{h}_1, \ldots, \overline{h}_t)^T,$$

então

$$g_i \equiv h_i \pmod{p^{e_i}} \Rightarrow p^{e_i} \mid (g_i - h_i), \ \forall\ i = 1, \ldots, t.$$

Assim, a k-ésima entrada do vetor coluna

$$\pi(A(g_1, \ldots, g_t)^T) - \pi(A(h_1, \ldots, h_t)^T)$$

é igual a:

$$\begin{aligned}
\pi_k\left(\sum_{i=1}^{t} a_{ki}g_i\right) - \pi_k\left(\sum_{i=1}^{t} a_{ki}h_i\right) &= \pi_k\left(\sum_{i=1}^{t} a_{ki}g_i - \sum_{i=1}^{t} a_{ki}h_i\right) \\
&= \pi_k\left(\sum_{i=1}^{t} a_{ki}\left(g_i - h_i\right)\right) \\
&= \sum_{i=1}^{t} \pi_k\left(\frac{a_{ki}}{p^{e_k-e_i}}(p^{e_k-e_i}\left(g_i - h_i\right)\right) \\
&= \overline{0},
\end{aligned}$$

pois p^{e_k} divide $p^{e_k-e_i}\left(g_i - h_i\right)$, se $k \geq i$ e p^{e_k} divide $\left(g_i - h_i\right)$, se $k < i$. Portanto, σ_A está bem definida.

$$\begin{aligned}
\sigma_A((\overline{g}_1, \ldots, \overline{g}_t)^T + (\overline{h}_1, \ldots, \overline{h}_t)^T) &= \sigma_A((\overline{g}_1 + \overline{h}_1, \ldots, \overline{g}_t + \overline{h}_t)^T) \\
&= \sigma_A((\overline{g_1 + h_1}, \ldots, \overline{g_t + h_t})^T) \\
&= \pi(A(g_1 + h_1, \ldots, g_t + h_t)^T) \\
&= \pi(A(g_1, \ldots, g_t)^T + A(h_1, \ldots, h_t)^T) \\
&= \pi(A(g_1, \ldots, g_t)^T) + \pi(A(h_1, \ldots, h_t)^T) \\
&= \sigma_A(\overline{g}_1, \ldots, \overline{g}_t)^T + \sigma_A(\overline{h}_1, \ldots, \overline{h}_t)^T.
\end{aligned}$$

Assim, σ_A é um homomorfismo de grupos, ou seja, $\sigma_A \in E_p$, para todo $A \in R_p$. Portanto, a função $\sigma : R_p \longmapsto E_p$ definida como $\sigma(A) = \sigma_A$ está bem definida e é um homomorfismo de grupos. Mostraremos agora que $(\sigma_A \circ \sigma_B)(\overline{g}_1, \ldots, \overline{g}_t)^T = (\sigma_{AB})(\overline{g}_1, \ldots, \overline{g}_t)^T$, então dados

$A = (a_{ij}), B = (b_{ij}) \in R_p$, obtemos

$$\begin{aligned}
(\sigma_A \circ \sigma_B)(\overline{g}_1, \ldots, \overline{g}_t)^T &= \sigma_A(\pi(B(g_1, \ldots, g_t)^T)) = \sigma_A\left(\pi\left(\sum_{k=1}^{t} b_{1k}g_k, \ldots, \sum_{k=1}^{t} b_{tk}g_k\right)^T\right) \\
&= \sigma_A\left(\sum_{k=1}^{t} \pi(b_{1k}g_k, \ldots, b_{tk}g_k)^T\right) = \sum_{k=1}^{t} \sigma_A\left(\overline{b_{1k}g_k}, \ldots, \overline{b_{tk}g_k}\right) \\
&= \sum_{k=1}^{t} \pi\left(A(b_{1k}g_k, \ldots, b_{tk}g_k)^T\right) = \pi\left(\sum_{k=1}^{t} A(b_{1k}g_k, \ldots, b_{tk}g_k)^T\right) \\
&= \pi\left(\sum_{k=1}^{t}\left(\sum_{m=1}^{t} a_{1m}b_{mk}g_k, \ldots, \sum_{m=1}^{t} a_{tm}b_{mk}g_k\right)^T\right) \\
&= \pi\left(\sum_{k=1}^{t}\left(\sum_{m=1}^{t} a_{1m}b_{mk}\right)g_k, \ldots, \sum_{k=1}^{t}\left(\sum_{m=1}^{t} a_{tm}b_{mk}\right)g_k\right)^T \\
&= \pi(AB(g_1, \ldots, g_t)^T) \\
&= (\sigma_{AB})(\overline{g}_1, \ldots, \overline{g}_t)^T.
\end{aligned}$$

Logo,

$$\sigma(AB) = \sigma_{AB} = \sigma_A \circ \sigma_B = \sigma(A) \circ \sigma(B)$$

Portanto, σ é um homomorfismo de aneis.

Agora, dados $\varphi \in E_p$ e

$$w_j = (0, \ldots, 0, g_j, 0, \ldots, 0)^T \in H_p.$$

Então φ é completamente determinado por $\varphi(w_j)$, pois se

$$\varphi(w_j) = (\overline{h}_{1j}, \ldots, \overline{h}_{tj})^T = \pi(h_{1j}, \ldots, h_{tj})^T,$$

então

$$\begin{aligned}
(0, \ldots, 0) &= \varphi(0, \ldots, 0) = \varphi(p^{e_j}w_j) \\
&= \varphi(w_j + \cdots + w_j) \ \ p^{e_j}\text{-parcelas} \\
&= \varphi(w_j) + \cdots + \varphi(w_j) \\
&= (\overline{p^{e_j}h}_{1j}, \ldots, \overline{p^{e_j}h}_{tj})^T.
\end{aligned}$$

Logo, p^{e_i} divide $p^{e_j}h_{ij}$, para todos i e j. Neste caso, $p^{e_i - e_j}$ divide h_{ij} se $j \leq i$. Consequentemente, dado $\varphi \in E_p$, existe $H = (h_{ij}) \in R_p$ tal que $\sigma(H) = \varphi$, ou seja, σ é sobrejetor. ■

Observe, pelo Primeiro Teorema de Isomorfismos, que

$$\frac{R_p}{\ker \sigma} \simeq E_p.$$

Vamos agora provar que o núcleo de σ é o conjunto

$$N_p = \{(a_{ij}) \in R_p : p^{e_i} \text{ divide } a_{ij}, \ \forall \ i,j \in \{1,\ldots,t\}\}$$

De fato, se $A = (a_{ij}) \in N_p$, então

$$\begin{aligned}
\sigma_A(\overline{h}_1,\ldots,\overline{h}_t)^T &= \pi(A(h_1,\ldots,h_t)^T) \\
&= \pi\left(A\left(\sum_{j=1}^{t}(0,\ldots,0,h_j,0,\ldots,0)^T\right)\right) \\
&= \sum_{j=1}^{t}\pi(A(0,\ldots,0,h_j,0,\ldots,0)^T) \\
&= \sum_{j=1}^{t}(\pi_1(a_{1j}),\ldots,\pi_t(a_{tj}))^T \\
&= (\overline{0},\ldots,\overline{0})^T
\end{aligned}$$

Portanto, $A \in \ker\sigma$. Reciprocamente, se $A = (a_{ij}) \in \ker\sigma$, então, pelos cálculos acima, obtemos

$$\sigma(A) = \sigma_A = (0,\ldots,0) \Rightarrow \pi_i(a_{ij}) = 0.$$

Assim, p^{e_i} divide a_{ij}, para todo $i,j \in \{1,\ldots,t\}$. Assim, $A \in N_p$. Portanto, obtemos uma caracterização do anel E_p como o anel quociente das matrizes

$$\frac{R_p}{\ker \sigma}.$$

Dado $A = (c_{ij}) \in \mathbb{Z}^{t\times t}$, é bem conhecida da Teoria das Matrizes, a expansão de Laplace do determinante de A:

$$\det(A) = \sum_{j=1}^{t}(-1)^{i+j}a_{ij}\det(A_{ij}), \ \ i = 1,\ldots,t.$$

com A_{ij} a matriz obtida de A eliminando-se a i-ésima linha e j-ésima coluna da matriz A. O escalar $c_{ij} = (-1)^{i+j}\det(A_{ij})$ é chamado o *cofator* do termo a_{ij} no $\det A$ e a matriz $C = (c_{ij}) \in \mathbb{Z}^{t\times t}$ é chamada a *matriz dos cofatores* da matriz A.

Lema 2.7 *Seja $A \in \mathbb{Z}^{t\times t}$. Então*

$$A \cdot \mathrm{adj}(A) = \mathrm{adj}(A) \cdot A = (\det(A))I_t,$$

onde $\mathrm{adj}(A) \in \mathbb{Z}^{t\times t}$ *é a transposta da matriz dos cofatores de A, a qual é chamada de* adjunta clássica *de A.*

Prova. Seja $B = \text{adj}(A) = (b_{ij})$, de modo que

$$b_{ij} = c_{ji} = (-1)^{i+j} \det(A_{ji}), \ \ \forall \ i, j \in \{1, \ldots, t\}.$$

Então

$$A \cdot \text{adj}(A) = AB = (d_{ij}), \ \ \text{com} \ \ d_{ij} = \sum_{k=1}^{t} a_{ik} b_{kj} = \sum_{k=1}^{t} a_{ik} (-1)^{j+k} \det(A_{jk}).$$

Se $i = j$, então $d_{ii} = \det(A)$. Agora, se $i \neq j$, digamos $i < j$, e seja $\widehat{A} = (\widehat{a}_{ij})$ a matriz obtida de A substituindo-se a j-ésima linha pela i-ésima linha, isto é, se $L_1, \ldots, L_t$ são as linhas de A, então

$$L_1, \ldots L_i, \ldots, L_{j-1}, L_i, L_{j+1}, \ldots, L_t$$

são as linhas de $\widehat{A}$. Logo, $\widehat{a}_{ik} = a_{ik} = \widehat{a}_{jk}$ e $\det(\widehat{A}_{jk}) = \det(A_{jk})$, para todo k. Em particular, $\det(\widehat{A}) = 0$, pois $\widehat{A}$ possui duas linhas iguais. Assim,

$$d_{ij} = \sum_{k=1}^{t} \widehat{a}_{jk} (-1)^{k+j} \det(\widehat{A}_{jk}) = \det(\widehat{A}) = \begin{cases} \det(A) & \text{se } i = j \\ 0 & \text{se } i \neq j, \end{cases}$$

isto é, $A \cdot \text{adj}\, A = (\det(A)) I_t$. Como $(\text{adj}(A))^t = \text{adj}(A^t)$ temos que

$$(\det(A)) I_t = (\det(A^t)) I_t = A^t \cdot \text{adj}(A^t) = (\text{adj}(A) \cdot A)^t.$$

Logo,

$$\text{adj}(A) \cdot A = ((\det(A)) I_t)^t = (\det(A)) I_t.$$

Portanto,

$$A \cdot \text{adj}(A) = \text{adj}(A) \cdot A = (\det(A)) I_t,$$

que é o resultado desejado. ■

Lema 2.8 *Seja $A \in R_p$, com $\det(A) \neq 0$. Então existe uma única matriz $B \in R_p$ tal que*

$$AB = BA = \det(A)\, I.$$

Prova. Seja $A \in R_p$ fixada, com $\det A \neq 0$. Então, pelo Lema 2.7, existe uma única matriz $B \in \mathbb{Z}^{t \times t}$ tal que

$$AB = BA = \det(A)\, I_t.$$

Afirmação. $B \in R_p$.

De fato, já vimos que existe $C \in \mathbb{Z}^{t\times t}$ tal que $A = PCP^{-1}$. Novamente, pelo Lema 2.7, existe uma única matriz $D \in \mathbb{Z}^{t\times t}$ tal que

$$CD = DC = \det(C)\, I_t.$$

Note que

$$\det(A) = \det\left(PCP^{-1}\right) = \det(P)\det(C)\det\left(P^{-1}\right) = \det(C).$$

Pondo $M = PDP^{-1}$, obtemos

$$\begin{aligned} AM &= (PCP^{-1})(PDP^{-1}) = PCDP^{-1} = \det(A)\, I_t \\ &= PDCP^{-1} = (PDP^{-1})(PCP^{-1}) \\ &= MA. \end{aligned}$$

Portanto, pela unicidade de B, $B = M = PDP^{-1}$, ou seja, $B \in R_p$. ■

Teorema 2.9 *Seja $A = (a_{ij}) \in R_p$ fixada. A função $\sigma_A \in E_p = \mathrm{End}(H_p)$ é um automorfismo se, e somente se, $A = (\overline{a}_{ij})$ é um elemento do grupo linear geral $\mathrm{GL}_t(\mathbb{F}_p)$, com*

$$\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$$

um corpo finito.

Prova. Suponhamos que $\sigma_A \in E_p$ seja um automorfismo. Então

$$\sigma_A \circ \sigma_A^{-1} = I.$$

Pondo $\sigma(B) = \sigma_A^{-1}$, obtemos

$$\sigma(AB) = \sigma(A) \circ \sigma(B) = \sigma_A \circ \sigma_A^{-1} = I = \sigma(I_t) \Rightarrow \sigma(AB - I_t) = 0.$$

Logo, $AB - I_t \in \ker\sigma = N_p$. Assim, $A = (\overline{a}_{ij}) \in \mathrm{GL}_t(\mathbb{F}_p)$, pois

$$\det(AB) \equiv 1 \pmod{p}.$$

Reciprocamente, suponhamos que $\mathrm{mdc}(\det(A), p) = 1$. Então existe $s \in \mathbb{Z}$ tal que

$$\det(A) \cdot s \equiv 1 \pmod{p^{e_i}}, \;\; i = 1, \ldots, t.$$

Pelo Lema 2.8, existe uma única matriz $B \in R_p$ tal que

$$AB = BA = \det(A)\, I_t.$$

Assim, $A^{-1} = s \cdot B \in R_p$ e

$$\sigma(A) \circ \sigma(A^{-1}) = \sigma(AA^{-1}) = \sigma(As \cdot B) = \sigma(s \det(A)\, I_t) = \sigma(I_t) = I.$$

Portanto, $\sigma_A \in E_p$ é um automorfismo, com inverso $\sigma_{A^{-1}}$. ■

Exemplo 2.10 *Seja H_p um p-grupo abeliano elementar. Então H_p é isomorfo ao espaço vetorial $\mathbb{F}_p^t$, para algum t, pois $pg = 0$, para todo $g \in H_p$ e a função $\cdot : \mathbb{F}_p \times H_p \longrightarrow H_p$ definida como $\cdot(\overline{x}, g) = xg$ é claramente uma ação de $\mathbb{F}_p$ sobre H_p, ou seja, H_p com esta operação é um espaço vetorial sobre $\mathbb{F}_p$ de dimensão t, para algum $t \geq 1$. Portanto, H_p é isomorfo a $\mathbb{F}_p^t$. Neste caso, $E_p = \mathrm{End}(H_p)$ é isomorfo ao conjunto das matrizes $M_t(\mathbb{F}_p)$. Assim, o Teorema 2.9, simplesmente afirma que $\mathrm{Aut}(H_p)$ corresponde ao grupo das matrizes invertíveis $\mathrm{GL}_t(\mathbb{F}_p)$.*

2.2 Algoritmo

Nesta seção apresentaremos um algoritmo para determinar uma fórmula explícita para determinar o número de automorfismos de grupo abeliano finito qualquer.

1.º **Passo**. Determinar todas as matrizes M em $\mathrm{GL}_t(\mathbb{F}_p)$ que podem ser estendida para uma matriz A em R_p.

2.º **Passo**. Calcular o número de maneira distinta de estender M a um endomorfismo em E_p.

Para isso vamos definir os seguinte $2t$ números:

$$d_k = \max\{l : e_l = e_k\} \in \{1, \ldots, t\} \text{ e } c_k = \min\{l : e_l = e_k\} \in \{1, \ldots, t\}$$

Como $e_k = e_k$ temos que $d_k \geq k$ e $c_k \leq k$. Além disso,

$$1 \leq d_1 \leq d_2 \leq \cdots \leq d_t \text{ e } 1 = c_1 \leq c_2 \leq \cdots \leq c_t.$$

Portanto, basta determinar os elementos $M \in GL_t(\mathbb{F}_p)$ que são da forma:

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1t} \\ \vdots & \vdots & \cdots & \vdots \\ m_{d_1 1} & m_{d_1 2} & \cdots & m_{d_1 t} \\ 0 & m_{d_2 2} & \cdots & m_{d_2 t} \\ 0 & 0 & \cdots & m_{d_3 t} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & m_{d_t t} \end{bmatrix} = \begin{bmatrix} m_{1c_1} & m_{1c_2} & \cdots & m_{1c_t} & \cdots & m_{1t} \\ 0 & m_{2c_2} & \cdots & m_{2c_t} & \cdots & m_{2t} \\ \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & m_{tc_t} & \cdots & m_{tt} \end{bmatrix}.$$

Teorema 2.11 *Seja*

$$H_p = \mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times \cdots \times \mathbb{Z}_{p^{e_t}},$$

com $1 \leq e_1 \leq e_2 \leq \cdots \leq e_t$, $e_1 + e_2 + \cdots + e_t = \alpha$ *e* $|H_p| = p^\alpha$. *Então*

$$|\mathrm{Aut}\,(H_p)| = \prod_{k=1}^{t} \left(p^{d_k} - p^{k-1}\right) \prod_{j=1}^{t} \left(p^{e_j}\right)^{t-d_j} \prod_{i=1}^{t} \left(p^{e_i-1}\right)^{t-(c_i-1)}.$$

Prova. Como as colunas da matriz M em $\mathrm{GL}_t(\mathbb{F}_p)$ são linearmente independentes temos que existem $p^{d_1} - 1$ possíveis escolhas para a primeira coluna de M, pois a coluna

$$C = (0, \ldots, 0)^T$$

não é permitida. Assim, escolhida a primeira coluna, existem $p^{d_2} - p$ possíveis escolhas para a segunda coluna de M, pois precisamos substituir as colunas

$$C_2 = xC_1, \ \forall \ x \in \mathbb{F}_p,$$

ou seja,

$$C_2 \notin \{xC_1 : x \in \mathbb{F}_p\} \simeq \mathbb{F}_p.$$

Logo, escolhidas a primeira e a segunda coluna, existem $p^{d_3} - p^2$ possíveis escolhas para a terceira coluna de M, pois precisamos substituir as colunas

$$C_3 = xC_1 + yC_2, \ \forall \ x, y \in \mathbb{F}_p,$$

ou seja,

$$C_3 \notin \{xC_1 + yC_2 : x, y \in \mathbb{F}_p\} \simeq \mathbb{F}_p^2.$$

Continuando com esse processo, obtemos

$$\prod_{k=1}^{t} \left(p^{d_k} - p^{k-1}\right).$$

matrizes distintas M em $\mathrm{GL}_t(\mathbb{F}_p)$ que podem ser estendidas. Agora, vamos estender cada elemento m_{ij} para $a_{ij} \in \mathbb{Z}$ com

$$\overline{a}_{ij} \in \frac{p^{e_i-e_j}\mathbb{Z}}{p^{e_i}\mathbb{Z}} = \left\{\overline{0}, \overline{p^{e_i-e_j}}, \overline{2p^{e_i-e_j}}, \ldots, \overline{(p^{e_j}-1)p^{e_i-e_j}}\right\} = p^{e_i-e_j}\mathbb{Z}_{p^{e_i}}$$

tal que

$$a_{ij} \equiv m_{ij} \,(\mathrm{mod}\, p).$$

Se $e_i > e_j$, então existem p^{e_j} maneiras de zerar cada um dos $(t - d_j)$ elementos m_{ij} em cada coluna C_j da matriz M, pois qualquer elemento de

$$\frac{p^{e_i - e_j}\mathbb{Z}}{p^{e_i}\mathbb{Z}}$$

será zerado. Por outro lado, se $e_i \leq e_j$, então existem $p^{e_i - 1}$ maneiras de cada um dos $(t - (c_i - 1))$ elementos m_{ij} ser diferente de zero em cada linha C_i da matriz M, pois podemos adicionar elementos de

$$\frac{p\mathbb{Z}}{p^{e_i}\mathbb{Z}} = \left\{\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{(p^{e_i - 1} - 1)p}\right\} = p^{e_i - e_j}\mathbb{Z}_{p^{e_i}}.$$

Portanto,

$$|\mathrm{Aut}\,(H_p)| = \prod_{k=1}^{t}\left(p^{d_k} - p^{k-1}\right)\prod_{j=1}^{t}\left(p^{e_j}\right)^{t-d_j}\prod_{i=1}^{t}\left(p^{e_i - 1}\right)^{t-(c_i-1)}.$$

que é o resultado desejado. ■

Exemplo 2.12 *Seja $H_3 = \mathbb{Z}_3 \times \mathbb{Z}_{3^2}$, com $e_1 = 1$ e $e_2 = 2$. Então*

$$d_k = \max\{l : e_l = e_k\} \in \{1, 2\} \;\; e \;\; c_k = \min\{l : e_l = e_k\} \in \{1, 2\}.$$

Logo,

$$M = \begin{bmatrix} m_{11} & m_{12} \\ 0 & m_{22} \end{bmatrix},$$

onde $\overline{m}_{11}, \overline{m}_{12}, \overline{m}_{22} \in \mathbb{F}_3$, com $\overline{m}_{11} \cdot \overline{m}_{22} \neq \overline{0}$. Assim, existem

$$(3^{d_1} - 1)(3^{d_2} - 3) = 2 \cdot 6 = 12$$

matrizes que podem ser estendidas. Agora, vamos estender cada elemento m_{ij} de $\overline{m}_{ij} \in \mathbb{F}_3$ para

$$\overline{a}_{ij} \in \frac{3^{e_i - e_j}\mathbb{Z}}{3^{e_i}\mathbb{Z}} = \left\{\overline{0}, \overline{3^{e_i - e_j}}, \overline{2 \cdot 3^{e_i - e_j}}, \ldots, \overline{(3^{e_j} - 1)3^{e_i - e_j}}\right\} = 3^{e_i - e_j}\mathbb{Z}_{3^{e_i}}$$

tal que

$$a_{ij} \equiv m_{ij} \,(\mathrm{mod}\, 3)\,.$$

O elemento $\overline{m}_{21} = \overline{0} \in \mathbb{F}_3$, $(e_2 > e_1)$, pode ser estendido de $3^{e_1} = 3$ maneiras para

$$\overline{a}_{21} \in \frac{3\mathbb{Z}}{9\mathbb{Z}} = \{\overline{0}, \overline{3}, \overline{6}\} = 3\mathbb{Z}_9.$$

Finalmente, cada um dos elementos $\overline{m}_{11}, \overline{m}_{12}, \overline{m}_{22} \in \mathbb{F}_3$, $(e_i \leq e_j)$, *pode ser estendido de* 3^{e_i-1} *maneiras para*

$$\begin{aligned} \overline{a}_{11} &\in \frac{3\mathbb{Z}}{3\mathbb{Z}} = \{\overline{0}\} = 3\mathbb{Z}_3 \\ \overline{a}_{12} &\in \frac{3\mathbb{Z}}{3\mathbb{Z}} = \{\overline{0}\} = 3\mathbb{Z}_3 \\ \overline{a}_{22} &\in \frac{3\mathbb{Z}}{3^2\mathbb{Z}} = \{\overline{0}, \overline{3}, \overline{6}\} = 3\mathbb{Z}_9. \end{aligned}$$

Portanto,

$$\begin{aligned} |\mathrm{Aut}\,(H_3)| &= \prod_{k=1}^{2} \left(3^{d_k} - 3^{k-1}\right) \prod_{j=1}^{2} \left(3^{e_j}\right)^{t-d_j} \prod_{i=1}^{2} \left(p^{e_i-1}\right)^{t-(c_i-1)} \\ &= (3^{d_1}-1)(3^{d_2}-3)(3^{e_1})^{2-d_1}(3^{e_1})^{2-d_2}(3^{e_1-1})^{2-(c_1-1)}(3^{e_2-1})^{2-(c_2-1)} \\ &= 2 \cdot 6 \cdot 3 \cdot 3 \\ &= 108. \end{aligned}$$

Capítulo 3

Automorfismos dos Grupos Diedrais

Neste capítulo vamos classificar os automorfismos dos grupos diedrais com o objetivo de comparar com a classificação dos grupos abelianos, visto no capítulo anterior, e com isto mostrar a extrema dificuldade na teoria dos grupos da classificação dos grupos finitos.

3.1 Grupos Diedrais

Nesta seção apresentaremos as principais propriedades dos grupos diedrais. Mas antes vamos apresentar os conceitos básicos de ação de grupo e produto semidireto.

Sejam G um grupo qualquer e S um conjunto não vazio qualquer. Uma *ação* (*à esquerda*) de G sobre S é uma função $* : G \times S \longrightarrow S$, com $*(a, x) = a * x$, tal que as seguintes condições são satisfeitas:

1. $a * (b * x) = (ab) * x$, para todos $a, b \in G$ e $x \in S$.

2. $1_G * x = x$, para todo $x \in S$ e 1_G é o elemento identidade de G.

Neste caso, diremos que G *age* sobre S e que S é um *G-conjunto*. Se $|S| = n$, então n é chamado o *grau* do G-conjunto S. Com o objetivo de simplificar a notação usaremos ax ao invés de $a * x$.

Exemplo 3.1 *Sejam H, G dois grupos, $\sigma : H \to G$ um homomorfismo de grupos e $S = G$. A função $* : H \times S \longrightarrow S$ definida por $a * x = \sigma(a)x$, para todo $a \in H$ e $x \in S$, é uma ação de H sobre S. Em particular, se H é um subgrupo de G, então a ação é chamada de* translação à esquerda.

Observação 3.2 *Seja S um G-conjunto não vazio. Então, para um $a \in G$ fixado, a função $\varphi_a : S \to S$ definida por $\varphi_a(x) = ax$ é um elemento do grupo de permutações de S, $P(S)$, pois*

$$(\varphi_{a^{-1}} \circ \varphi_a)(x) = \varphi_{a^{-1}}(\varphi_a(x)) = \varphi_{a^{-1}}(ax) = \left(a^{-1}a\right) x = 1_G x = x, \ \forall \ x \in S.$$

Logo, $\varphi_{a^{-1}} \circ \varphi_a = 1_S$. De modo inteiramente análogo, prova-se que $\varphi_a \circ \varphi_{a^{-1}} = 1_S$.

Teorema 3.3 *Sejam G um grupo e S um conjunto não vazio.*

1. *Qualquer ação de G sobre S induz um homomorfismo de grupos $\varphi : G \longrightarrow P(S)$.*
2. *Qualquer homomorfismo de grupos $\varphi : G \longrightarrow P(S)$ induz uma ação de G sobre S. Neste caso, dizemos que φ é uma* representação por permutação *de G em $P(S)$.*

Seja S um G-conjunto não vazio. Dados $x, y \in S$, definimos

$$x \sim y \Leftrightarrow \ \text{existe } a \in G \text{ tal que } y = ax.$$

Então $\sim$ é uma relação de equivalência sobre S. De fato, $x \sim x$, para todo $x \in S$, pois $1_G x = x$. Dados $x, y \in S$, se $x \sim y$, então existe $a \in G$ tal que $y = ax$. Logo,

$$x = 1_G x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}y.$$

Assim, $y \sim x$, pois $a^{-1} \in G$. Finalmente, dados $x, y, z \in S$, se $x \sim y$ e $y \sim z$, então existem $a, b \in G$ tais que $y = ax$ e $z = by$. Logo,

$$z = by = b(ax) = (ba)x.$$

Assim, $x \sim z$, pois $ba \in G$.

A classe de equivalência

$$\overline{x} = \{y \in S : x \sim y\} = \{ax : a \in G\}$$

chama-se de *órbita* (ou *trajetória*) de x e será denotada por $\mathcal{O}(x)$.

Sejam G um grupo qualquer e $S = G$. Então a função $* : G \times S \longrightarrow S$ definida como $a * x = axa^{-1}$, para todo $a \in G$ e $x \in S$, é uma ação de G sobre S, chamada de *ação por conjugação*. Dado $x \in S$, a órbita de x:

$$\mathcal{O}(x) = \{a * x : a \in G\} = \{axa^{-1} : a \in G\}$$

é chamada a *classe de conjugação* de x e será denotada por $\mathcal{C}_x$. O estabilizador de x

$$G_x = \{a \in G : axa^{-1} = x\} = \{a \in G : ax = xa\} = \mathcal{C}_G(x).$$

Portanto,

$$|\mathcal{C}_x| = [G : \mathcal{C}_G(x)], \ \forall \ x \in S.$$

e G não age transitivamente sobre G.

Sejam $G = S_3$ o grupo de permutações $N = A_3 = \langle \sigma \rangle$ e $H = \langle \tau \rangle$, com

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

É fácil verificar que G possui as seguintes propriedades:

a. $G = NH$.

b. N é subgrupo normal em G.

c. $N \cap H = \{1_G\}$.

Neste caso, G não é um produto direto interno de N e H, pois H não é subgrupo normal em G. Mas isto motiva a seguinte definição.

Sejam G um grupo e H, N subgrupos de G. Diremos que G é o *produto semidireto* (*interno*) de N por H, em símbolos $G = N \rtimes H$, se as seguintes condições são satisfeitas:

1. $G = NH$.

2. N é subgrupo normal em G.

3. $N \cap H = \{1_G\}$.

Observação 3.4 *Seja $G = N \rtimes H$ o produto semidireto de N por H.*

1. *Pelo Segundo Teorema de Isomorfismo, temos que*

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

e H chama-se um complementar *de N. Consequentemente, se G é grupo finito, então*

$$|G| = |N| \, [G : N] = |N| \, |H| \, .$$

2. *Como* $G = NH$ *e* $N \cap H = \{1\}$ *temos que cada* $x \in G$ *pode ser escrito de modo único sob a forma* $x = nh$, $n \in N$ *e* $h \in H$.

3. *Para um* $h \in H$ *fixado, a função* $\varphi_h : N \to N$ *definida como* $\varphi_h(n) = hnh^{-1}$ *é um automorfismo de* N, *pois* N *é um subgrupo normal em* G *Além disso,* $\varphi_{hk} = \varphi_h \circ \varphi_k$, *para todos* $h, k \in H$. *Portanto, a função* $\varphi : H \to \mathrm{Aut}(N)$ *definida por* $\varphi(h) = \varphi_h$ *é um homomorfismo de grupos. Neste caso, dizemos que* H *age sobre* N *como um grupo de automorfismo e* φ *é chamado o homomorfismo por conjugação de* N. *Como*

$$(n_1h_1)(n_2h_2) = [n_1(\varphi(h_1)(n_2))]h_1h_2, \text{ para alguns } n_1, n_2 \in N \text{ e } h_1, h_2 \in H,$$

temos que a operação do grupo G *pode ser expressa em termos das operações de* N, H *e o homomorfismo* φ.

4. *Se* $\varphi(h) = I_N$, *para todo* $h \in H$, *então* $\varphi_h(n) = n$, *para todo* $n \in N$. *Logo,*

$$hnh^{-1} = n \Rightarrow n^{-1}hn = h \in H,$$

isto é, H *é um subgrupo normal em* G. *Portanto,*

$$G = N \times H.$$

Reciprocamente, se $G = N \times H$, *então os elementos de* H *comutam com os elementos de* N *e, assim, o homomorfismo* φ *é trivial.*

5. *Se* $\varphi(h) \neq I_N$, *para algum* $h \in H$, *então* $\varphi_h(n) \neq n$, *para algum* $n \in N$. *Logo,*

$$hnh^{-1} \neq n \Rightarrow hn \neq nh.$$

Portanto, G *é um grupo não abeliano.*

Reciprocamente, sejam N, H grupos e φ um homomorfismo grupos de H em $\mathrm{Aut}(N)$. Definimos uma operação binária sobre $N \times H$ do seguinte modo:

$$(n_1, h_1)(n_2, h_2) = (n_1\varphi(h_1)(n_2), h_1h_2).$$

Então é fácil verificar que $N \times H$ com essa operação é um grupo com elemento identidade $(1, 1)$ e $(\varphi(h^{-1})(n^{-1}), h^{-1})$ o elemento inverso de (n, h). O grupo $N \times H$ é chamado o *produto semidireto* (*externo*) de N por H via φ e será denotado por

$$G = N \rtimes_\varphi H.$$

Note que

$$\widehat{N} = \{(n,1) : n \in N\} \text{ e } \widehat{H} = \{(1,h) : h \in H\}$$

são subgrupos de G tais que $N \simeq \widehat{N}$ e $H \simeq \widehat{H}$. A função $\sigma : G \to G$ definida por $\sigma(n,h) = (1,h)$ é um homomorfismo de grupos, onde $\operatorname{Im}\sigma = \widehat{H}$, $\ker\sigma = \widehat{N}$ e $\sigma^2 = \sigma$. Consequentemente, $\widehat{N}$ é um subgrupo normal em G e pelo Primeiro Teorema de isomorfismo

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

Como

$$(n,1)(1,h) = (n\varphi(1)(1),h) = (n1_N(1),h) = (n,h)$$

temos que $G = \widehat{N}\widehat{H}$. Além disso, $\widehat{N} \cap \widehat{H} = \{(1,1)\}$. Portanto, G é o produto semidireto (interno) de $\widehat{N}$ por $\widehat{H}$. Finalmente,

$$(1,h)(n,1)(1,h)^{-1} = (\varphi(h)(n),1)$$

implica que a função $\psi : \widehat{H} \to \operatorname{Aut}(\widehat{N})$ definida por $\psi(1,h) = \psi_{(1,h)}$, com

$$\psi_{(1,h)}(n,1) = (\varphi(h)(n),1),$$

é o homomorfismo por conjugação de $\widehat{N}$. Portanto, identificando $\widehat{N}$ com N e $\widehat{H}$ com H, temos que φ é o homomorfismo por conjugação de N e G é o produto semidireto (interno) de N por H. Neste caso,

$$N \rtimes_\varphi H = \{nh : n \in N,\ h \in H\},$$

com

$$(n_1h_1)\cdot(n_2h_2) = n_1\varphi(h_1)(n_2)\cdot h_1h_2 \text{ e } \varphi(h_1)(n_2) = \varphi_{h_1}(n_2) = h_1n_2h_1^{-1}.$$

Exemplo 3.5 *Sejam N um grupo abeliano qualquer e $H = \langle b\rangle \simeq \mathbb{Z}_2$. Se definirmos $\varphi : H \to \operatorname{Aut}(N)$ como $\varphi(b) = \varphi_b$, com $\varphi_b(a) = a^{-1}$, para todo $a \in N$, então $G = N \rtimes_\varphi H$ é um grupo não abeliano, em que*

$$\varphi_b(a) = bab^{-1} = a^{-1},\ \forall\ a \in N,$$

isto é, $b \in \mathcal{Z}(G)$. Em particular, se $N = \langle a\rangle \simeq \mathbb{Z}_n$ é cíclico, então $G \simeq D_n$. Explicitamente,

$$D_n = \left\langle a, b : a^n = b^2 = 1 \text{ e } ab = ba^{-1}\right\rangle,$$

em que a é identificado com $(a,1)$ e b é identificado com $(1,b)$. Note que o grupo D_n é isomorfo ao grupo $L = \langle R,T\rangle$, gerado pelas matrizes

$$R = \begin{bmatrix} \cos(\frac{2\pi}{n}) & -\operatorname{sen}(\frac{2\pi}{n}) \\ \operatorname{sen}(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{bmatrix} \text{ e } T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Sejam G grupo e H um subgrupo de G. Diremos que H é um *subgrupo característico* em G se

$$\sigma(H) \subseteq H, \ \forall \ \sigma \in \mathrm{Aut}\,(G)\,.$$

Note que qualquer subgrupo característico em G é um subgrupo normal.

Proposição 3.6 *Seja*

$$D_n = \left\langle a, b : a^n = b^2 = 1 \ \textit{e} \ ab = ba^{-1} \right\rangle, \ \textit{com} \ n > 2.$$

Então as classes de conjugação de D_n são:

1. *Se n é um número ímpar, então*

$$\mathcal{C}_1 = \{1\}, \mathcal{C}_b = \{b, ab, \ldots, a^{n-1}b\} \ \textit{e} \ \mathcal{C}_{a^i} = \{a^i, a^{-i}\}, \ \ , i = 1, \ldots, \frac{1}{2}(n-1).$$

2. *Se n é um número par, então*

$$\begin{aligned} \mathcal{C}_1 &= \{1\}, \\ \mathcal{C}_b &= \{a^{2i}b : i \in \mathbb{Z}_n\} = \{b, a^2b, \ldots, a^{n-2}b\}, \\ \mathcal{C}_{ab} &= \{a^{2i+1}b : i \in \mathbb{Z}_n\} = \{ab, a^3b, \ldots, a^{n-1}b\} \\ C_{a^{\frac{n}{2}}} &= \{a^{\frac{n}{2}}\} \ \textit{e} \ \mathcal{C}_{a^i} = \{a^i, a^{-i}\}, \ \ , i = 1, \ldots, \frac{1}{2}(n-2). \end{aligned}$$

Consequentemente,

$$\mathcal{Z}\,(D_n) = \begin{cases} \{1\}, & \textit{se } n \textit{ é um número ímpar} \\ \langle a^{\frac{n}{2}} \rangle, & \textit{se } n \textit{ é um número par.} \end{cases}$$

Além disso, $C_n = \langle a \rangle$ é um subgrupo característico de D_n.

Prova. Como $D_n = \langle a, b \rangle$ temos que cada elemento de D_n pode ser escrito sob a forma

$$a^{t_1}b^{t_2}\cdots a^{t_{m-1}}b^{t_m}, \ \text{onde} \ m \in \mathbb{N} \ \text{e} \ t_i \in \mathbb{Z}.$$

Assim, usando sucessivamente as relações

$$a^n = b^2 = 1 \ \text{e} \ bab^{-1} = bab = a^{-1},$$

cada elemento de D_n pode ser escrito de maneira única sob a forma

$$a^ib^j, \ \text{onde} \ i \in \mathbb{Z}_n \ \text{e} \ j \in \mathbb{Z}_2.$$

Por exemplo,

$$a^i b^j = a^k b^l \Rightarrow a^{i-k} = b^{l-j}.$$

Como $\langle a \rangle \cap \langle b \rangle = \{1\}$ temos que $i - k \equiv 0 \pmod{n}$ e $l - j \equiv 0 \pmod{2}$. Portanto,

$$D_n = \{a^i b^j : i \in \mathbb{Z}_n \text{ e } j \in \mathbb{Z}_2\}$$

A classe de conjugação

$$\begin{aligned} \mathcal{C}_{a^i} &= \{x a^i x^{-1} : x \in D_n\} \\ &= \{(a^k b^j) a^i (a^k b^j)^{-1} : k \in \mathbb{Z}_n \text{ e } j \in \mathbb{Z}_2\} \\ &= \{b^j a^i b^{-j} : j \in \mathbb{Z}_2\} = \{a^i, a^{-i}\}. \end{aligned}$$

Agora,

$$a^j (a^i b) a^{-j} = a^{j+i} b a^{-j} = a^{j+i} a^j b = a^{2j+i} b, \ \forall \ i \in \mathbb{Z}.$$

Logo, se n é um número ímpar, então $\text{mdc}(2, n) = 1$, ou seja, 2 é um elemento invertível em $\mathbb{Z}_n$. Pondo

$$j = \frac{1}{2}(k - i), \ \forall \ k \in \mathbb{Z},$$

temos que cada $a^i b$ é conjugado a qualquer $a^k b$. Portanto,

$$\mathcal{C}_b = \{a^i b : i \in \mathbb{Z}_n\} = \{b, ab, \ldots, a^{n-1} b\}.$$

Observe que

$$(a^j b)(a^i b)(a^j b)^{-1} = a^j b a^{i-j} = a^j a^{j-i} b = a^{2j-i} b, \ \forall \ i \in \mathbb{Z}.$$

Assim, se n é um número par, então existem duas classes de conjugação, quando i é um número par ou ímpar, a saber,

$$\mathcal{C}_b = \{a^{2k} b : k \in \mathbb{Z}_n\} = \{b, a^2 b, \ldots, a^{n-2} b\}$$

e

$$\mathcal{C}_{ab} = \{a^{2k+1} b : k \in \mathbb{Z}_n\} = \{ab, a^3 b, \ldots, a^{n-1} b\}.$$

Note que

$$x \in \mathcal{Z}(D_n) \Leftrightarrow \mathcal{C}_x = \{x\}.$$

Portanto,

$$\mathcal{Z}(D_n) = \begin{cases} \{1\}, & \text{se } n \text{ é um número ímpar} \\ \langle a^{\frac{n}{2}} \rangle, & \text{se } n \text{ é um número par.} \end{cases}$$

Finalmente, como

$$(a^ib)^2 = a^iba^ib = a^{i-i}b^2 = 1, \ \forall \ i \in \mathbb{Z},$$

temos que a^ib possui ordem 2. Logo, o único subgrupo cíclico de D_n de ordem n, $n > 2$, é $C_n = \langle a \rangle$. Portanto, C_n é característico. ■

Exemplo 3.7 *Sejam $D_n = \langle a, b \rangle$ o grupo diedral e k um inteiro positivo dividindo n. Então $\langle a^k \rangle$ é um subgrupo normal em D_n e*

$$\frac{D_n}{\langle a^k \rangle}$$

é um grupo diedral.

Solução. Sabemos que

$$xa^kx^{-1} = \begin{cases} a^k \\ ou \\ a^{-k} \end{cases}$$

logo $\langle a^k \rangle \trianglelefteq D_n$. Além disso pode-se verificar que $\frac{D_n}{\langle a^k \rangle}$ é um grupo diedral, Confira Proposição 3.10 a seguir. ■

Proposição 3.8 *Os subgrupos maximais de D_n são diedrais ou cíclico. Em particular, $C_n = \langle a \rangle$ é o único subgrupo cíclico maximal e*

$$D_p = \langle a^{\frac{n}{p}}, a^ib \rangle$$

são os subgrupos diedrais maximais, para algum número primo p dividindo n.

Prova. Seja M um subgrupo maximal de D_n. Se M é um subgrupo cíclico de D_n, então $M = C_n$. Se M não é um subgrupo cíclico de D_n, então $M = \langle c, a^ib \rangle$, com $c \in \langle a \rangle$, pois $\langle a^ib, a^jb \rangle = D_n$, $i \neq j$; $i, j = 0, 1, \ldots, n-1$, e $M \neq D_n$. Como M é um subgrupo maximal temos que c é o único elemento de $\langle a \rangle$, com ordem p, para algum número primo p dividindo n, a saber, $c = a^{\frac{n}{p}}$. Portanto,

$$D_p = \langle a^{\frac{n}{p}}, a^ib \rangle$$

é um grupo diedral. ■

Corolário 3.9 *Seja H um subgrupo próprio de D_n. Então H é um subgrupo normal em D_n se, e somente se, H é um subgrupo de $\langle a \rangle$ ou n é um número par. No último caso, H é um dos subgrupos maximais de índice 2,*

$$M_1 = \langle a^2, b \rangle \simeq \mathbb{Z}_{\frac{n}{2}} \rtimes \mathbb{Z}_2 \ \ ou \ \ M_2 = \langle a^2, ab \rangle \simeq \mathbb{Z}_{\frac{n}{2}} \rtimes \mathbb{Z}_2.$$

Além disso, os subgrupos característicos próprios de D_n são todos subgrupos de $\langle a \rangle$.

Prova. Seja H um subgrupo normal em D_n. Se $a^i \in H$, então

$$\mathcal{C}_{a^i} = \{a^i, a^{-i}\} \subseteq H,$$

ou seja, H é um subgrupo de $\langle a \rangle$. Se $a^i b \in H$, então

$$x(a^i b)x^{-1} \in H, \ \forall \ x \in D_n.$$

Assim, se n é um número ímpar, então

$$\mathcal{C}_b = \{a^i b : i \in \mathbb{Z}_n\} = \{b, ab, \ldots, a^{n-1}b\} \subseteq H.$$

Portanto, $H = D_n$, pois $D_n = \langle b, a^i b \rangle$, $i = 1, \ldots, n-1$. Se n é um número par, então

$$\mathcal{C}_b = \{a^{2i} b : i \in \mathbb{Z}_n\} = \{b, a^2 b, \ldots, a^{n-2}b\} \subseteq H$$

ou

$$\mathcal{C}_{ab} = \{a^{2i+1} b : i \in \mathbb{Z}_n\} = \{ab, a^3 b, \ldots, a^{n-1}b\} \subseteq H.$$

Logo, se $\mathcal{C}_b \subseteq H$, então $a^2 = (ab)a \in H$, isto é, $\langle a^2 \rangle \subseteq H$. Se $\mathcal{C}_{ab} \subseteq H$, então $a^2 = (ba)(ba^3) \in H$, isto é, $\langle a^2 \rangle \subseteq H$. Portanto,

$$M_1 = \langle a^2, b \rangle \ \text{ ou } \ M_2 = \langle a^2, ab \rangle.$$

Finalmente, se n é um número par, então é claro que a função $\varphi : D_n \to D_n$ definida como $\varphi(a) = a^{-1}$ e $\varphi(b) = ab$ é um automorfismo externo de D_n tal que $\varphi(M_1) = M_2$. Portanto, os subgrupos característicos próprios de D_n são todos subgrupos de $\langle a \rangle$. ■

Proposição 3.10 *Seja $D_n = \langle a, b \rangle$ um grupo diedral.*

1. *Qualquer grupo quociente de D_n por um subgrupo próprio é um grupo diedral.*

2. *Qualquer subgrupo de D_n é um grupo diedral ou um grupo cíclico.*

Prova. (1) Basta provar que se $\varphi : D_n \to H$ é um homomorfismo de grupos sobrejetor, então H é um grupo diedral. Como $D_n = \langle a, b \rangle$ temos que

$$H = \langle \varphi(a), \varphi(b) \rangle,$$

pois φ é sobrejetora e

$$\varphi(a^i b^j) = \varphi(a)^i \varphi(b)^j.$$

Sendo

$$\varphi(a)^n = \varphi(b)^2 = 1 \text{ e } \varphi(b)\varphi(a)\varphi(b)^{-1} = \varphi(a)^{-1},$$

temos que H é um grupo diedral.

(2) Vamos usar indução sobre n para provar que qualquer subgrupo de D_n é um grupo diedral ou um grupo cíclico. Se $n = 1$, nada há para ser provado. Suponhamos que o resultado seja válido para todo m, com $1 \leq m < n$. Agora, se existisse um subgrupo próprio H de D_n que não seja diedral e nem cíclico, então H está contido em um subgrupo maximal de D_n, digamos M. Assim, pela Proposição 3.8, M é um grupo diedral ou é um grupo cíclico. Logo, pela hipótese de indução aplicada a M, H é um grupo diedral ou um grupo cíclico, o que é uma contradição. Portanto, qualquer subgrupo de D_n é um grupo diedral ou um grupo cíclico. ■

Sejam G um grupo e H, K subconjuntos de G. O *subgrupo comutador* de H e K é definido como

$$[H, K] = \langle [h, k] : h \in H \text{ e } k \in K \rangle,$$

com $[h, k] = hkh^{-1}k^{-1}$. Em particular, o grupo derivado $G' = [G, G]$.

Lema 3.11 *Sejam G um grupo e H, K subgrupos de G.*

1. *K normaliza H ($K \subseteq \mathcal{N}_G(H)$) se, e somente se, $[H, K]$ é um subgrupo de H.*
2. *Se K é um subgrupo normal em G e $K \subseteq H$, então $[H, G]$ é um subgrupo de K se, e somente se,*
$$\frac{H}{K} \leq \mathcal{Z}\left(\frac{G}{K}\right).$$
3. *Se $\varphi : G \longrightarrow L$ é um homomorfismo de grupos, então*
$$\varphi([H, K]) = [\varphi(H), \varphi(K)].$$
Em particular, $\varphi(G') = \varphi([G, G]) = [\varphi(G), \varphi(G)] = \varphi(G)' = (\operatorname{Im}\varphi)' \subseteq L'$.

Sejam G um grupo e $G^{(1)} = G'$ o subgrupo comutador de G. Para cada $n \in \mathbb{N}$ definimos, indutivamente, o n-ésimo subgrupo comutador de G como

$$G^{(n)} = (G^{(n-1)})' \text{ com } G^{(0)} = G.$$

É fácil verificar, pelo item (3) do Lema 3.11, que cada $G^{(n+1)}$ é um subgrupo característico em $G^{(n)}$, para todo $n \in \mathbb{N}$. Mais geralmente, $\varphi(G^{(n)}) \subseteq G^{(n)}$, para todo $\varphi \in \operatorname{End}(G)$. Note que

$$\cdots \leq G^{(n)} \leq \cdots \leq G^{(1)} \leq G^{(0)} = G$$

é uma cadeia de subgrupos de G chamada de *série derivada* de G e será denotada por

$$\left(G^{(n)}\right)_{n\in\mathbb{Z}_+}.$$

Seja G um grupo. Diremos que G é um *grupo solúvel* se existir $n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$. O menor $n \in \mathbb{N}$ tal que $G^{(n)} = \{1\}$ é chamado o *índice de solubilidade*.

Teorema 3.12 *O grupo diedral D_n é um grupo solúvel, para todo $n \in \mathbb{N}$.*

Prova. Pelo Exemplo 3.5,

$$D_n = \{a^i b^j : i = 0, \ldots, n-1 \text{ e } j = 0, 1\},$$

$a^n = b^2 = 1$ e $ab = ba^{-1} = ba^{n-1}$. Assim, indutivamente, obtemos

$$a^m b = ba^{-m} = ba^{n-m}, \ \forall \ m \in \mathbb{Z}.$$

Logo,

$$[x, y] = xyx^{-1}y^{-1} = \begin{cases} 1, & \text{se } x = a^r \text{ e } y = a^s \\ a^{2r}, & \text{se } x = a^r \text{ e } y = a^s b \\ a^{-2s}, & \text{se } x = a^r b \text{ e } y = a^s \\ a^{2r}, & \text{se } x = a^r b \text{ e } y = a^s b. \end{cases}$$

Portanto,

$$D_n^{(1)} = [D_n, D_n] = \left\langle a^2 \right\rangle = \begin{cases} \mathbb{Z}_n, & \text{se } n \text{ é um número ímpar} \\ \mathbb{Z}_{\frac{n}{2}}, & \text{se } n \text{ é um número par.} \end{cases}$$

Assim,

$$D_n^{(2)} = \left[D_n^{(1)}, D_n^{(1)}\right] = \{1\}.$$

Portanto, D_n é um grupo solúvel de índice de solubilidade igual a 2. ■

Seja G um grupo. Uma *série subnormal* em G é uma cadeia finita de subgrupos de G

$$\{1\} = G_n \leq G_{n-1} \leq \cdots \leq G_1 \leq G_0 = G$$

tais que

$$G_{i+1} \trianglelefteq G_i, \ 0 \leq i \leq n-1,$$

e será denotada por

$$S = (G_i)_{i=0}^{n-1}.$$

Os grupos

$$\frac{G_i}{G_{i+1}},\ 0 \leq i \leq n-1,$$

são chamados de *grupos fatores*. O *comprimento* de uma série subnormal é o número de grupos fatores não triviais.

Uma *série normal* em G é uma cadeia finita de subgrupos de G

$$\{1\} = G_n \leq G_{n-1} \leq \cdots \leq G_0 = G$$

tais que

$$G_{i+1} \trianglelefteq G,\ 0 \leq i \leq n-1.$$

Uma série normal $S = (G_i)_{i=0}^{n-1}$ em G é chamada de *série central superior* em G se

$$\frac{G_i}{G_{i+1}} \leq \mathcal{Z}\left(\frac{G}{G_{i+1}}\right),\ 1 \leq i \leq n-1.$$

Seja G um grupo. Diremos que G é um *grupo nilpotente* se G possui uma série central. O menor comprimento da série central é chamado o *índice de nilpotência* de G.

Proposição 3.13 *Qualquer p-grupo é um grupo nilpotente.*

Prova. Seja G um p-grupo, com $|G| = p^n$ e $n \in \mathbb{Z}_+$. Vamos usar indução sobre n para provar que G é um grupo nilpotente. Se $n = 0$ ou 1, então G é um grupo abeliano e, portanto, nilpotente. Suponhamos que o resultado seja válido para todo m, com $1 \leq m < n$. Pelo Teorema de Burnside, $\mathcal{Z}(G) \neq \{1\}$. Se $G = \mathcal{Z}(G)$, então G é um grupo abeliano e, portanto, nilpotente. Se $G \neq \mathcal{Z}(G)$, então $\mathcal{Z}(G)$ é um p-grupo, com

$$\left|\frac{G}{\mathcal{Z}(G)}\right| = p^s < p^n = |G|.$$

Pela hipótese de indução,

$$\frac{G}{\mathcal{Z}(G)}$$

é um grupo nilpotente. Logo, ele possui uma série central

$$\{\mathcal{Z}(G)\} = \overline{G}_m \leq \overline{G}_{m-1} \leq \cdots \leq \overline{G}_0 = \frac{G}{\mathcal{Z}(G)}.$$

Assim, pelo Teorema da Correspondência, existe um único subgrupo normal G_i em G tal que

$$\overline{G}_i = \frac{G_i}{\mathcal{Z}(G)},\ 0 \leq i \leq m-1.$$

Portanto,

$$\{1\} \leq G_0 = \mathcal{Z}(G) \leq \cdots \leq G_m = G$$

é uma série subnormal em G, com

$$G_{i+1} \trianglelefteq G \text{ e } \frac{G_i}{G_{i+1}} \simeq \frac{\overline{G}_i}{\overline{G}_{i+1}} \leq \mathcal{Z}\left(\frac{\overline{G}_0}{\overline{G}_{i+1}}\right) \simeq \mathcal{Z}\left(\frac{G}{G_{i+1}}\right), \ 0 \leq i \leq m-1,$$

isto é, G é um grupo nilpotente. ■

Seja G um grupo qualquer. A cadeia de subgrupos de G

$$G = \mathcal{Z}^0(G) \geq \mathcal{Z}^1(G) \geq \cdots \geq \mathcal{Z}^n(G) \geq \cdots$$

é chamada de *série central descendente* de G. Note que se G é grupo finito, então existe $n \in \mathbb{N}$ tal que

$$\mathcal{Z}^n(G) = \mathcal{Z}^{n+1}(G) = \cdots .$$

Proposição 3.14 *Seja G um grupo. Então G é um grupo nilpotente de índice de nilpotência n se, e somente se, $\mathcal{Z}^n(G) = \{1\}$, mas $\mathcal{Z}^{n-1}(G) \neq \{1\}$.*

Prova. Suponhamos que G seja nilpotente. Então G tem uma série central

$$\{1\} = G_n \leq G_{n-1} \leq \cdots \leq G_0 = G.$$

com $G_{n-1} \neq \{1\}$.

Afirmação. $\mathcal{Z}^i(G)$ é um subgrupo de G_i, para todo $i \in \mathbb{Z}_+$.
De fato, se $i = 0$, nada há para ser provado. Suponhamos que o resultado seja válido para $i > 0$, isto é, $\mathcal{Z}^i(G)$ é um subgrupo de G_i. Como

$$\frac{G_i}{G_{i+1}} \leq \mathcal{Z}\left(\frac{G}{G_{i+1}}\right)$$

temos que $[G_i, G]$ é um subgrupo de G_{i+1}. Logo, pela hipótese de indução, obtemos

$$\mathcal{Z}^{i+1}(G) = [\mathcal{Z}^i(G), G] \leq [G_i, G] \leq G_{i+1}.$$

Assim, $\mathcal{Z}^{i+1}(G)$ é um subgrupo de G_{i+1}. Em particular, $\mathcal{Z}^n(G) \subseteq G_n = \{1\}$. Portanto, $\mathcal{Z}^n(G) = \{1\}$, mas $\mathcal{Z}^{n-1}(G) \neq \{1\}$.

A recíproca segue da definição. ■

Proposição 3.15 *O grupo diedral D_n é um grupo nilpotente se, e somente se, $n = 2^k$, para algum $k \in \mathbb{N}$.*

Prova. Pelo Teorema 3.12, obtemos

$$\mathcal{Z}^1(D_n) = [\mathcal{Z}^0(D_n), D_n] = \left\langle a^2 \right\rangle = \begin{cases} \mathbb{Z}_n, & \text{se } n \text{ é um número ímpar} \\ \mathbb{Z}_{\frac{n}{2}}, & \text{se } n \text{ é um número par.} \end{cases}$$

De modo inteiramente análogo, obtemos

$$\mathcal{Z}^2(D_n) = [\mathcal{Z}^1(D_n), D_n] = \left\langle a^4 \right\rangle.$$

Assim, indutivamente, obtemos

$$\mathcal{Z}^m(D_n) = [\mathcal{Z}^{m-1}(D_n), D_n] = \left\langle a^{2^m} \right\rangle, \ \forall \ m \in \mathbb{N}.$$

Portanto, se D_n é um grupo nilpotente, então existe um menor $k \in \mathbb{N}$ tal que $\mathcal{Z}^k(D_n) = \{1\}$, isto é, $a^{2^k} = 1$ e $n = 2^k$. ■

3.2 Automorfismo dos Grupos Diedrais

Nesta seção vamos classificar o grupo de automorfismo dos grupos diedrais D_n, com $n > 2$. Já vimos que

$$H = \mathcal{U}(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n : \text{mdc}(n, a) = 1\}$$

é um grupo cíclico tal que H é isomorfo ao grupo de automorfismo $\text{Aut}(\mathbb{Z}_n)$, por isto, vamos identificar H com $\text{Aut}(\mathbb{Z}_n)$.

Teorema 3.16 *Seja $D_n = \langle a, b \rangle$ um grupo diedral, com $n > 2$. Então o grupo de automorfismo $\text{Aut}(D_n)$ é isomorfo ao grupo $\mathbb{Z}_n \rtimes_\varphi H$, com a ação $\varphi : H \to \text{Aut}(\mathbb{Z}_n) = H$ definida como $\varphi(s) = s$. Explicitamente,*

$$\text{Aut}(D_n) = \{\sigma_{r,s} : r \in \mathbb{Z}_n \ \ e \ \ s \in H\},$$

em que

$$\sigma_{r,s}(a^i) = a^{is} \ \ e \ \ \sigma_{r,s}(a^i b) = a^{is+r} b.$$

Prova. Note que

$$\begin{aligned}
\sigma_{r,s}(a^i a^j) &= a^{(i+j)s} = a^{is} a^{js} = \sigma_{r,s}(a^i)\sigma_{r,s}(a^j) \\
\sigma_{r,s}(a^i a^j b) &= a^{(i+j)s+r} b = a^{is}(a^{js+r} b) = \sigma_{r,s}(a^i)\sigma_{r,s}(a^i b) \\
\sigma_{r,s}(a^i b a^j) &= \sigma_{r,s}(a^{i-j} b) = a^{(i-j)s+r} b = a^{is+r} b a^{js} = \sigma_{r,s}(a^i b)\sigma_{r,s}(a^j) \\
\sigma_{r,s}(a^i b a^j b) &= \sigma_{r,s}(a^{i-j}) = a^{is+r-r-js} = (a^{is+r} b)(b a^{-r-js}) \\
&= (a^{is+r} b)(a^{js+r} b) = \sigma_{r,s}(a^i b)\sigma_{r,s}(a^j b),
\end{aligned}$$

isto é, $\sigma_{r,s}$ é um homomorfismo de grupos. Por construção $\sigma_{r,s}$ é sobrejetor. Agora, se $a^i \in \ker \sigma_{r,s}$, então $a^{is} = 1$, com $i \in \mathbb{Z}_n$ e $s \in H$. Assim, $is = 0$, pois $0 \leq ir < n$. Se $a^i b \in \ker \sigma_{r,s}$, então $a^{is+r}b = 1$, com $i, r \in \mathbb{Z}_n$ e $s \in H$. Logo, $a^{is+r} = b$, de modo que

$$a^{is+r+1} = a^{is+r}a = ba = a^{-1}b = a^{-1}a^{is+r} = a^{is+r-1} \Rightarrow a^2 = 1,$$

o que é impossível, pois $n > 2$. Portanto $\ker \sigma_{r,s} = \{1\}$ e $\sigma_{r,s}$ é um homomorfismo de grupos injetor. Consequentemente, $\sigma_{r,s} \in \mathrm{Aut}(D_n)$, para todo $r \in \mathbb{Z}_n$ e $s \in H$.

Reciprocamente, seja σ um elemento qualquer de $\mathrm{Aut}(D_n)$. Então $\sigma(a) = a^s$, para algum $s \in \mathbb{Z}_n$, pois $C_n = \langle a \rangle$ é um subgrupo característico de D_n. Como σ é bijetor temos que $\mathrm{mdc}(n, s) = 1$, de modo que $s \in H$. Note que $\sigma(b) = a^r b$, pois $b^2 = 1$.

Afirmação. $\sigma = \sigma_{r,s}$.

De fato, como

$$\sigma(a^i) = a^{is} = \sigma_{r,s}(a^i) \text{ e } \sigma(a^i b) = a^{is+r}b = \sigma_{r,s}(a^i b)$$

temos que $\sigma = \sigma_{r,s}$.

Finalmente, dados $\sigma_{r,s}, \sigma_{t,u} \in \mathrm{Aut}(D_n)$, obtemos

$$(\sigma_{r,s} \circ \sigma_{t,u})(a^i b) = \sigma_{r,s}(a^{iu+t}b) = a^{(iu+t)s+r}b = a^{isu+st+r}b = \sigma_{st+r,su}(a^i b)$$

e

$$(\sigma_{r,s} \circ \sigma_{t,u})(a^i) = \sigma_{r,s}(a^{iu}) = a^{isu} = \sigma_{st+r,su}(a^i),$$

ou seja, $\sigma_{r,s} \circ \sigma_{t,u} = \sigma_{st+r,su}$. Então a função $f : \mathrm{Aut}(D_n) \to \mathbb{Z}_n \rtimes_\varphi H$ definida como $f(\sigma_{r,s}) = (r, s)$ é um isomorfismo de grupos, pois

$$(r, s) \cdot (t, u) = (r + \varphi(s)(t), su) = (r + st, su)$$

e $f^{-1}(r, s) = \sigma_{-rs^{-1},s^{-1}}$. ■

Observação 3.17 $|\mathrm{Aut}(D_n)| = n\phi(n)$, *com* ϕ *a função de Euler.*

Referências Bibliográficas

[1] Bhattacharya, P. B.; Jain, S. K.; Nagpaul, S. R.; **Basic Abstract Álgebra**. 2 ed.Cambridge: Cambridge Univ. Press, 1994.

[2] Christopher J. H; Darren L. R.; "Automorphisms of Finite Abelian Groups," **Amer. Math. Monthly**, 2007,

[3] Dummit D.; Foote R. **Abstract Algebra**. 3 ed. Danvers: John Wiley and Sons, 2004.

[4] Feit, W.;"O teorema da ordem ímpar e a classificação dos grupos simples," **Revista Matemática Universitária, SBM 7** (1988) 11-20.

[5] Garcia, A. e Lequain, Y.;**Álgebra: Elementos de Álgebra**. 3 ed. Projeto Euclides-IMPA. Rio de Janeiro, 2005.

[6] Gorenstein, D.; The Classification of the finite simple groups, Number 2, **Mathematical Surveys and Monographs**, 1995.

[7] Lang, S.;**Algebra**. 3 ed. New York: Springer, 2002.

[8] Pan,J.M.;"The order of the automorphism group of finite abelian group," **J. Yunnan Univ. Nat. Sci**. **26** (2004) 370-372.

[9] Ranum, A.;"The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group," **Trans. Amer. Math. Soc. 8** (1907) 71-91.