CARLOS HENRIQUE ALVES COSTA

AUTOMORFISMOS DE GRUPOS ABELIANOS FINITOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

VIÇOSA
MINAS GERAIS - BRASIL
2014

Ficha catalográfica preparada pela Biblioteca Central da Universidade Federal de Viçosa - Câmpus Viçosa

T
C837a
2014

Costa, Carlos Henrique Alves, 1987-
Automorfismos de Grupos Abelianos Finitos / Carlos Henrique Alves Costa. – Viçosa, MG, 2014.
vi, 64f. : il. ; 29 cm.

Orientador: Marinês Guerreiro.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 64.

1. Automorfismos. 2. Grupos abelianos. 3. Teoria dos grupos. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. II. Título.

CDD 22. ed. 512.2

CARLOS HENRIQUE ALVES COSTA

AUTOMORFISMOS DE GRUPOS ABELIANOS FINITOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós Graduação em Matemática, para obtenção do título de *Magister Scientiae*.

APROVADA: 18 de Fevereiro de 2014.

Jhone Caldeira Silva

Rogério Carvalho Picanço

Marinês Guerreiro
(Orientadora)

"Não vemos as coisas como elas são, mas como nós somos."
Anaïs Nin

Sumário

RESUMO **v**

ABSTRACT **vi**

INTRODUÇÃO **1**

1 Conceitos Preliminares **4**

1.1 Homomorfismos e Automorfismos de grupos 4

1.2 Ações de Grupos Sobre um Conjunto 9

1.3 p-Grupos 14

1.4 Os Teoremas de Sylow 17

1.5 Produto Direto 22

2 Grupos Abelianos Finitos **31**

2.1 Teorema Fundamental dos Grupos Abelianos Finitos 31

2.2 O Número de Grupos Abelianos não Isomorfos de uma Dada Ordem 38

3 Automorfismos de Grupos Abelianos Finitos **40**

3.1 Automorfismos de Produtos Diretos 40

3.2 Endomorfismos dos Grupos H_p 43

3.3 Contando os Automorfismos de H_p 52

3.4 Automorfismos de p-grupos abelianos finitos 56

3.4.1 Número de Elementos de uma Dada Ordem 58

Considerações Finais **63**

Referências Bibliográficas **64**

RESUMO

COSTA, Carlos Henrique Alves, M.Sc., Universidade Federal de Viçosa, fevereiro de 2014. **Automorfismos de Grupos Abelianos Finitos**. Orientadora: Marinês Guerreiro.

O conjunto de todos os automorfismos de um grupo G forma um grupo denotado por $Aut(G)$. Neste trabalho estudamos automorfismos de grupos abelianos finitos, seguindo principalmente a abordagem feita por Christopher J. Hillar e Darren L. Rhea no artigo "*Automorphisms of finite abelian Groups*"(American Mathematical Monthly 114 n. 10 (2007) 917-923). O objetivo principal é fazer uma caracterização do grupo de automorfismos $Aut(G)$, onde G é um grupo abeliano finito e apresentar uma fórmula para o número de elementos de $Aut(G)$. A determinação desta fórmula é feita de duas maneiras distintas: uma a partir do cálculo do número de elementos do grupo $Aut(G)$ visto como grupo das unidades do anel de endomorfismos $End(G)$ e a outra utilizando certos subgrupos característicos do grupo G. Esse último método segue o desenvolvimento feito por Heinrich Kuhn, em sua tese de doutorado.

ABSTRACT

COSTA, Carlos Henrique Alves, M.Sc., Universidade Federal de Viçosa, february, 2014. **Automorphisms of Finite Abelian Groups**. Adiviser: Marinês Guerreiro.

The set of all automorphisms of a group G form a group denoted by $Aut(G)$. In this work we study automorphisms of finite abelian groups, mainly following the approach by Christopher J. Hillar and Darren L. Rhea according to the paper "*Automorphisms of finite abelian Groups*" (American Mathematical Monthly 114 n. 10 (2007) 917-923). The main objective is to characterize the automorphism group $Aut(G)$, where G is a finite abelian group and present a formula for the number of elements of $Aut(G)$. The determination of this formula is done in two distinct ways: one from the calculation of the number of elements of the group $Aut(G)$ viewed as the group of units of the endomorphisms ring $End(G)$ and the other using certain characteristic subgroups of the group G. This latter method follows the development made by Heinrich Kuhn in his doctoral thesis.

INTRODUÇÃO

Dado um grupo G, um automorfismo φ de G é um homomorfismo $\varphi : G \to G$ bijetor. O conjunto de todos os automorfismos de G é um grupo com a operação de composição de funções, que é denotado por

$$Aut(G) = \{\varphi : G \to G \mid \varphi \text{ é isomorfismo}\}.$$

De modo geral, não é simples determinar o grupo de automorfismos de um grupo finito, mas no caso de grupos abelianos é possível obter teoremas de estrutura transparentes para estes grupos de automorfismos.

A primeira caracterização do grupo de automorfismos $Aut(G)$ de um grupo abeliano finito G foi tratada por Arthur Ranum [9], em 1907, no artigo *The group of classes of congruents matrices with application to the group of isomorphisms of any abelian group* e, além desta, existem poucas exposições. Podemos destacar também a tese de doutorado de Heinrich Kuhn [5], de 1975, sobre endomorfismos de p-grupos abelianos que contém resultados sobre automorfismos de p-grupos abelianos. O principal objetivo do nosso trabalho é fazer uma caracterização do grupo de automorfismos $Aut(G)$ de um grupo abeliano finito G segundo [2] e apresentar duas fórmulas diferentes para o número de elementos de $Aut(G)$. Uma deve-se a Otto Schreier e se encontra no artigo *Über die Erweiterung von Gruppen II* [10], através da qual, o número de elementos de $Aut(G)$ pode ser calculado conhecendo apenas as estruturas de certos subgrupos característicos de G. A outra, deve-se a Christopher J. Hillar e Darren L. Rhea [2] e utiliza um tratamento bastante moderno. Para isso, dividimos este trabalho em três capítulos que passamos a descrever.

No Capítulo 1, o objetivo principal é definir e apresentar alguns conceitos da Teoria de Grupos que serão utilizados ao longo deste trabalho, além de reunir resultados que serão indispensáveis para a demonstração do Teorema Fundamental dos Grupos Abelianos Finitos, que se encontra no Capítulo 2. Seguindo as linhas [1] e [7], iniciamos com as definições de homomorfismos e automorfismos de grupos e mostramos que o conjunto de todos os automorfismos de um grupo forma um grupo com a composição de funções. Em seguida, utilizando as referências [3] e [8], definimos ação de grupos sobre um conjunto, com destaque para a ação por conjugação e definimos os p-grupos, que são grupos nos quais todos os seus elementos têm ordem uma potência de um número primo p fixo. Tais grupos são de fundamental importância para o desenvolvimento do nosso trabalho,

especificamente, para a compreensão dos teoremas de Sylow. Estes teoremas garantem a existência de p-subgrupos em grupos finitos, além de estimar o número destes subgrupos e fornecer informações detalhadas sobre os mesmos. Finalizamos este capítulo apresentando um procedimento que permite construir um grupo a partir de outros grupos dados, o produto direto, que nos diz que, se H e K são dois grupos, então o conjunto

$$H \times K = \{(h, k) \mid h \in H, k \in K\}$$

também é um grupo, com uma operação conveniente. Definimos ainda o produto direto interno e mostramos que se um grupo G é um produto direto interno de uma família finita de subgrupos, então G é isomorfo ao produto direto (externo) desta família de subgrupos. Estes resultados são fundamentais para o desenvolvimento do Capítulo 2.

No Capítulo 2, o principal objetivo é apresentar o Teorema Fundamental dos Grupos Abelianos Finitos, que nos diz que todo grupo abeliano finito G é o produto direto de uma família $\{G_i\}_{1 \leq i \leq r}$ de subgrupos cíclicos. Além disso, o número destes subgrupos cíclicos e suas ordens são determinadas de modo único pelo grupo G. Iniciamos mostrando que se G é um grupo abeliano finito, então G é isomorfo ao produto direto de seus p-subgrupos de Sylow. Em seguida, mostramos que todo p-grupo abeliano finito é o produto direto de uma família finita de subgrupos cíclicos e, além disso, o número de parcelas desta decomposição, assim como suas ordens, são determinadas de modo único, a menos da ordem das parcelas, pelo grupo G. Finalizamos apresentando um modo para determinar, a menos de isomorfismos, todos os grupos abelianos de uma dada ordem.

O Capítulo 3 inicia com a determinação do grupo de automorfismos do produto direto de grupos abelianos, o que nos permite particularizar o problema para a determinação do grupo de automorfismos de um p-grupo abeliano. Em seguida, é feito o estudo do anel de endomorfismos de um p-grupo abeliano e, a partir deste, determina-se o grupo de automorfismos que é o grupo das unidades deste anel.

Finalmente, para G um grupo abeliano finito, utilizando a caracterização do grupo de automorfismos dada pelo Teorema 3.2.11, apresentamos uma fórmula para o número de elementos de $Aut(G)$, que decorre da contagem do número de determinadas matrizes de $GL_n(\mathbb{F}_p)$ descritas na Seção 3.2.

O Capítulo 3 termina com a apresentação de outra fórmula para o número de elementos de $Aut(G)$. Diferente da proposta por Christopher J. Hillar e Darren L. Rhea em [2], é possível conhecer o número de elementos de $Aut(G)$ conhecendo apenas a estrutura de alguns subgrupos característicos de G.

Mostramos inicialmente que se

$$G \cong \underbrace{\mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_1}}}_{\lambda_1 \text{ vezes}} \times \cdots \times \underbrace{\mathbb{Z}_{p^{m_t}} \times \cdots \times \mathbb{Z}_{p^{m_t}}}_{\lambda_t \text{ vezes}}$$

é um p-grupo abeliano finito, com $m_1 > \cdots > m_t$ e $1 \leq \gamma \leq m_1$. Então o subgrupo

$$\Omega_\gamma(G) = \langle a \in G \mid a^{p^\gamma} = 1_G \rangle$$

é um **subgrupo característico** de G. Em seguida, mostramos que $|\Omega_\gamma(G)| = p^{n_\gamma}$, onde $n_\gamma = (\lambda_1 + \lambda_2 + \cdots + \lambda_h)\gamma + \sum_{i<j} \lambda_j m_j$. Com este resultado, é possível determinar o número de elementos de uma dada ordem em um p-grupo abeliano finito e podemos enunciar o seguinte resultado:

Teorema 3.4.7 *Se*

$$G \cong \underbrace{\mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_1}}}_{\lambda_1 \ vezes} \times \cdots \times \underbrace{\mathbb{Z}_{p^{m_t}} \times \cdots \times \mathbb{Z}_{p^{m_t}}}_{\lambda_t \ vezes}$$

é um p-grupo abeliano finito, com $m_1 > \cdots > m_t$ *e* $|\Omega_{m_i}(G)| = p^{n_i}$*, para* $1 \leq i \leq t$*, então a ordem do grupo de automorfismos de* G *é dada por*

$$\prod_{i=1}^{t} \prod_{j=1}^{\lambda_i} \left(p^{n_i} - p^{n_i - j}\right).$$

Apresentamos também o cálculo explícito da ordem de $Aut(G)$, a partir das duas técnicas demonstradas, para um caso particular.

Capítulo 1

Conceitos Preliminares

Neste capítulo apresentaremos alguns conceitos e definições da Teoria de Grupos que serão necessários para a compreensão deste trabalho. Dentre eles, as definições e propriedades de automorfismos de grupos, produtos diretos, os Teoremas de Sylow e o Teorema Fundamental dos Grupos Abelianos Finitos, bem como as conexões entre eles. Consideramos conhecidos os conceitos básicos da Teoria de Grupos e, para maiores detalhes, sugerimos uma consulta a [1] e [7].

1.1 Homomorfismos e Automorfismos de grupos

Nesta seção apresentaremos as definições de homomorfismos e automorfismos de grupos e mostraremos que o conjunto $Aut(G)$, de todos os automorfismos de um grupo G, é um grupo com a operação de composição de funções.

Definição 1.1.1 *Sejam $(G, \star)$ e $(H, \triangle)$ dois grupos. Um **homomorfismo** (de grupos) é uma função $\varphi : G \longrightarrow H$ tal que, para todos $a, b \in G$, satisfaz*

$$\varphi(a \star b) = \varphi(a) \triangle \varphi(b).$$

*(i) Se φ é injetiva, então φ é um **monomorfismo**.*

*(ii) Se φ é sobrejetiva, então φ é um **epimormorfismo**.*

*(iii) Se φ é bijetiva, então φ é um **isomorfismo**.*

Observação 1.1.2 *Quando existe um isomorfismo φ entre dois grupos G e H, dizemos que G e H são **isomorfos** e denotamos $G \cong H$.*

Exemplo 1.1.3 *Seja $(G, \cdot)$ um grupo com $a \in G$. A função*

$$\begin{array}{rccl} \varphi: & \mathbb{Z} & \longrightarrow & G \\ & n & \longmapsto & \varphi(n) = a^n \end{array}$$

é um homomorfismo de $(\mathbb{Z}, +)$ em $(G, \cdot)$ e se G é um grupo cíclico infinito, digamos $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$, então φ é um isomorfismo de grupos. De fato, para todos m, $n \in \mathbb{Z}$, temos,

$$\varphi(m+n) = a^{m+n} = a^m \cdot a^n = \varphi(m)\,\varphi(n).$$

Agora, se $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$, então

$$a^m = a^n \Rightarrow a^m \cdot a^{-n} = 1_G \Rightarrow a^{m-n} = 1_G \Rightarrow m - n = 0 \Rightarrow m = n.$$

Logo a função φ é injetora. Além disso, a função φ é sobrejetora, pois, dado $y \in G$, $y = a^k$, para algum $k \in \mathbb{Z}$. Daí, tome $x = k$ e $\varphi(x) = y$. Portanto, φ é um isomorfismo.

Exemplo 1.1.4 *Seja N um subgrupo normal de um grupo G e consideremos o grupo quociente G/N. A função*

$$\begin{array}{rccl} \varphi: & G & \longrightarrow & G/N \\ & x & \longmapsto & \varphi(x) = xN \end{array}$$

é um epimorfismo de grupos denominado ***homomorfismo canônico*** *de G em G/N. De fato, a função φ é homomorfismo pois, para todos $x, y \in G$, temos*

$$\varphi(xy) = (xy)N = xN\,yN = \varphi(x)\,\varphi(y).$$

Além disso, φ é sobrejetora, pois, dado $y \in G/N$, então, $y = aN$, para algum $a \in G$. Daí tome $x = a$ e $\varphi(x) = y$.

Exemplo 1.1.5 *Seja G um grupo cíclico finito de ordem n, digamos $G = \langle g \rangle$, ou seja, $G = \{1_G, g, g^2, \ldots, g^{n-1}\}$. A função*

$$\begin{array}{rccl} \varphi: & G & \longrightarrow & \mathbb{Z}_n \\ & g^m & \longmapsto & \varphi(g^m) = \bar{m} \end{array}$$

é um isomorfismo de grupos. De fato, a função φ é um homomorfismo, pois, para todos $g^\alpha, g^\beta \in G$, temos

$$\varphi(g^\alpha\, g^\beta) = \varphi(g^{\alpha+\beta}) = \overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta} = \varphi(g^\alpha) + \varphi(g^\beta).$$

A função φ é injetora, pois, se $\bar{\alpha} = \bar{\beta}$, então $\overline{\alpha - \beta} = \bar{0}$ e daí, $g^\alpha = g^\beta$. Além disso, a função φ é sobrejetora, pois, dado $\bar{y} \in \mathbb{Z}_n$ existe um representante de classe $y \in \mathbb{Z}$, com $0 \leq y \leq n-1$. Daí, tome $x = g^y \in G$ e $\varphi(x) = y$.

Teorema 1.1.6 [6, Teorema 8.12] *Seja $\varphi : G \longrightarrow H$ um homomorfismo de grupos. Então valem as seguintes propriedades:*

(1) $\varphi(1_G) = 1_H$.

(2) Dado $a \in G$, $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(3) Se G' *é um subgrupo de* G, *então* $\varphi(G')$ *é um subgrupo de* H.

(4) Se H' *é um subgrupo de* H, *então* $K = \varphi^{-1}(H')$ *é um subgrupo de* G *e, além disso, se* H' *é normal em* H, *então* K *é normal em* G.

Definição 1.1.7 *Seja* $\varphi : G \longrightarrow H$ *um homomorfismo de grupos.*

(i) O conjunto $\mathrm{Im}(\varphi) = \{h \in H \mid h = \varphi(g)$ *para algum* $g \in G\}$ *é um subgrupo de* H *chamado* ***imagem*** *do homomorfismo* φ.

(ii) O conjunto $\ker(\varphi) = \{g \in G \mid \varphi(g) = 1_H\}$ *é um subgrupo normal de* G, *chamado* ***núcleo*** *do homomorfismo* φ.

Proposição 1.1.8 *Se* $\varphi : G \longrightarrow H$ *é um homomorfismo de grupos, então:*

(i) A função φ *é um monomorfismo se, e somente se,* $\ker(\varphi) = \{1_G\}$.

(ii) A função φ *é um isomorfismo se, e somente se, existe um homomorfismo* $\psi : H \longrightarrow G$ *tal que* $\varphi \circ \psi = I_H$ *e* $\psi \circ \varphi = I_G$.

Demonstração:

(i) Sejam $\varphi : G \longrightarrow H$ um homomorfismo e $x \in \ker(\varphi)$. Daí, $\varphi(x) = 1_H = \varphi(1_G)$ e, como φ é monomorfismo, temos $x = 1_G$. Reciprocamente, se $\ker(\varphi) = \{1_G\}$ e $x, y \in G$, então

$$\varphi(x) = \varphi(y) \Rightarrow \varphi(x)\,\varphi(y^{-1}) = 1_H \Rightarrow \varphi(xy^{-1}) = 1_H \Rightarrow xy^{-1} \in \ker(\varphi) = \{1_G\}.$$

Logo $x = y$ e, portanto, φ é um monomorfismo.

(ii) Se $\varphi : G \longrightarrow H$ é um isomorfismo, então $\varphi^{-1} : H \longrightarrow G$ também o é, pois φ^{-1} é uma bijeção e dados $a', b' \in H$, existem $a, b \in G$ tais que $\varphi(a) = a'$ e $\varphi(b) = b'$. Então $a'b' = \varphi(a)\varphi(b) = \varphi(ab)$, de onde vem que $\varphi^{-1}(a'b') = ab = \varphi^{-1}(a')\varphi^{-1}(b')$. Logo φ^{-1} é um homomorfismo. Reciprocamente, suponha que exista um homomorfismo $\psi : H \longrightarrow G$ tal que

$$\varphi \circ \psi = I_H \quad \text{e} \quad \psi \circ \varphi = I_G.$$

Assim $\psi = \varphi^{-1}$ e, assim, φ é bijetora. Portanto, φ é um isomorfismo. ∎

Teorema 1.1.9 (1º Teorema do Isomorfismo)

Seja $f : G \longrightarrow H$ *um homomorfismo de grupos. Então* $\dfrac{G}{\ker(f)} \cong \mathrm{Im}(f)$.

Demonstração: Sejam $N = \ker(f)$ e $\bar{G} = \dfrac{G}{N}$. Defina

$$\begin{array}{rccc} \bar{f}: & \bar{G} & \longrightarrow & \mathrm{Im}(f) \\ & \bar{g} & \longmapsto & f(g). \end{array}$$

A função $\bar{f}$ está bem definida, pois

$$\bar{g} = \bar{h} \Rightarrow gN = hN \Rightarrow gh^{-1}N = N \Rightarrow gh^{-1} \in N \Rightarrow f(gh^{-1}) = f(g)\, f(h)^{-1} = 1_H.$$

Logo $f(g) = f(h)$. Ainda, a função $\bar{f}$ é um homomorfismo, pois, dados $\bar{x}$, $\bar{y} \in \bar{G}$,

$$\bar{f}(\bar{x} \cdot \bar{y}) = \bar{f}(\overline{x \cdot y}) = f(x \cdot y) = f(x)f(y) = \bar{f}(\bar{x})\, \bar{f}(\bar{y}).$$

Além disso, a função $\bar{f}$ é injetora, pois

$$\begin{aligned} \ker(\bar{f}) &= \{\bar{g} \in \bar{G} \mid \bar{f}(\bar{g}) = 1_H\} = \{\bar{g} \in \bar{G} \mid f(g) = 1_H\} \\ &= \{\bar{g} \in \bar{G} \mid g \in \ker(f)\} = \{gN \mid g \in N\} = \{1_{\bar{G}}\}. \end{aligned}$$

Como $\mathrm{Im}(\bar{f}) = \mathrm{Im}(f)$, a função $\bar{f}$ é sobrejetora e, consequentemente, um isomorfismo de grupos. ∎

Definição 1.1.10 *Seja G um grupo.*

*i) Um homomorfismo $\psi : G \longrightarrow G$ é dito um **endomorfismo** de G.*

*ii) Um isomorfismo $\varphi : G \longrightarrow G$ é dito um **automorfismo** de G.*

iii) O conjunto $End(G) = \{\psi : G \to G \mid \psi$ é homomorfismo$\}$ é o conjunto de todos os endomorfismos do grupo G.

iv) O conjunto $Aut(G) = \{\varphi : G \to G \mid \varphi$ é isomorfismo$\}$ é o conjunto de todos os automorfismos do grupo G.

Observação 1.1.11 *O conjunto $End(G)$ não é necessariamente um grupo com a composição de funções, pois nem todos seus elementos possuem inverso. No entanto, se G é um grupo abeliano, então $End(G)$ é um anel com as seguintes operações:*

$$\begin{aligned} (f+g)(a) &= f(a) + g(a) \\ (f \cdot g)(a) &= f \circ g(a), \end{aligned}$$

para todos f, $g \in End(G)$, $a \in G$.

Proposição 1.1.12 *O conjunto $Aut(G)$ é um grupo com a operação de composição de funções.*

Demonstração: Inicialmente provemos que $Aut(G)$ é fechado em relação à composição de funções. Sejam f, $g \in Aut(G)$ e $x, y \in G$. Daí

$$(f \circ g)(xy) = f(g(xy)) = f(g(x)\, g(y)) = f(g(x))\, f(g(y)) = (f \circ g)(x)\, (f \circ g)(y).$$

Como a composição, $f \circ g$, de funções bijetivas é também bijetiva, decorre que $f \circ g \in Aut(G)$.

Agora, a função identidade

$$\begin{array}{rccc} I_d: & G & \longrightarrow & G \\ & x & \longmapsto & x \end{array}$$

é um automorfismo de G e será o elemento neutro de $Aut(G)$, já que, para todos $f \in Aut(G)$ e $x \in G$,

$$(f \circ I_d)(x) = f(I_d(x)) = f(x) \quad \text{e} \quad (I_d \circ f)(x) = I_d(f(x)) = f(x).$$

Além disso, para cada $f \in Aut(G)$, existe $f^{-1} \in Aut(G)$ tal que, para todo $x \in G$,

$$(f \circ f^{-1})(x) = I_d(x) \quad \text{e} \quad (f^{-1} \circ f)(x) = I_d(x).$$

Logo todo elemento de $Aut(G)$ possui inverso. Finalmente, a composição de funções satisfaz a associatividade, pois

$$(f \circ (g \circ h))(x) = (f(g \circ h))(x) = f(g(h(x))) = f \circ g(h(x)) = ((f \circ g) \circ h)(x).$$

Portanto, $Aut(G)$ é um grupo com a composição de funções.

■

Observação 1.1.13 *Um automorfismo φ de um grupo G preserva a ordem dos elementos de G. De fato, sejam G um grupo, $\varphi \in Aut(G)$ e $g \in G$ tal que $O(g) = n$. Daí temos*

$$1_G = \varphi(1_G) = \varphi(g^n) = \varphi(\underbrace{g \cdot g \cdot \cdots \cdot g}_{n\ vezes}) = \underbrace{\varphi(g) \cdot \varphi(g) \cdot \cdots \cdot \varphi(g)}_{n\ vezes} = \varphi(g)^n.$$

Agora suponha que exista um inteiro $m < n$ tal que $\varphi(g)^m = 1_G$. Daí

$$1_G = \varphi(g)^m = \underbrace{\varphi(g) \cdot \varphi(g) \cdot \cdots \cdot \varphi(g)}_{m\ vezes} = \varphi(\underbrace{g \cdot g \cdot \cdots \cdot g}_{m\ vezes}) = \varphi(g^m).$$

Logo $g^m \in \ker(\varphi) = \{1_G\}$ e daí $g^m = 1_G$. Isto contradiz o fato de $O(g) = n$. Portanto, $O(\varphi(g)) = n$.

1.2 Ações de Grupos Sobre um Conjunto

Nesta seção introduzimos o conceito de ação de grupos que é de essencial importância para o desenvolvimento deste trabalho, especificamente, para as demonstrações dos teoremas de Sylow.

Definição 1.2.1 *Uma* ***ação*** *de um grupo finito G sobre um conjunto finito S é uma função*

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

tal que, para todos $x \in S$, $g_1, g_2 \in G$, satisfaz:

(i) $1_G \cdot x = x$, *ou seja, o elemento neutro do grupo age em S como identidade.*

(ii) $(g_1 g_2) \cdot x = g_1(g_2 \cdot x)$, *ou seja, o produto de dois elementos do grupo G age como composição de funções.*

Quando tal ação existe, dizemos que o grupo G **age sobre o conjunto** S, ou que S é um G-**conjunto**.

Exemplo 1.2.2 (Ação por translação à esquerda)

Sejam G um grupo e H um subgrupo de G. Então H age sobre o conjunto G da seguinte maneira

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, x) & \longmapsto & h \cdot x. \end{array}$$

De fato,

(i) $1_G \cdot x = x$, *para todo $x \in G$.*

(ii) $(h_1 h_2) \cdot x \overset{Assoc.}{=} h_1(h_2 x)$, *para todos $h_1, h_2 \in H$, $x \in G$.*

Exemplo 1.2.3 (Ação por translação nas classes laterais)

Sejam H um subgrupo de um grupo G e $S = \dfrac{G}{H} = \{xH \mid x \in G\}$. Então G age sobre S por:

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (g, xH) & \longmapsto & (gx)H. \end{array}$$

De fato,

(i) $1_G \cdot xH = xH$, *para todo $xH \in S$.*

(ii) $(g_1g_2)\cdot xH = (g_1g_2x)H \overset{Assoc.}{=} g_1(g_2xH) = g_1(g_2\cdot xH)$, *para todos* $g_1, g_2 \in G,\ xH \in S$.

Exemplo 1.2.4 (Ação por conjugação)

Sejam G *um grupo e* H *um subgrupo de* G. *A função*

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h,x) & \longmapsto & h\cdot x \ = hxh^{-1} \end{array}$$

define uma ação de H *em* G. *De fato,*

(i) $1_G \cdot x = 1_G x 1_G^{-1} = x$, *para todo* $x \in G$.

(ii) $(h_1h_2)\cdot x = (h_1h_2)x(h_1h_2)^{-1} = h_1(h_2xh_2^{-1})h_1^{-1} = h_1\cdot(h_2xh_2^{-1}) = h_1(h_2\cdot x)$, *para todos* $h_1, h_2 \in H,\ x \in G$.

Proposição 1.2.5 *Seja* G *um grupo que age sobre um conjunto não vazio* S. *A relação* $x \sim y$ *se, e somente se,* $gx = y$, *para algum* $g \in G$, *para* $x, y \in S$, *é uma relação de equivalência.*

Demonstração:

(i) Seja $x \in S$. Como G age sobre S, $1_G \cdot x = x$, para todo $x \in S$. Logo $x \sim x$ e a relação $\sim$ é reflexiva.

(ii) Sejam $x, y \in S$ tais que $x \sim y$. Assim, existe $g \in G$ tal que $g \cdot x = y$. Como G é grupo, existe $g^{-1} \in G$ tal que $x = g^{-1} \cdot y$. Logo $y \sim x$ e a relação $\sim$ é simétrica.

(iii) Sejam $x, y, z \in S$ tais que $x \sim y$ e $y \sim z$. Assim, existem $g_1, g_2 \in G$ tais que $g_1 \cdot x = y$ e $g_2 \cdot y = z$. Daí

$$g_2 \cdot y = z \Leftrightarrow g_2(g_1x) = z \Leftrightarrow (g_2g_1)x = z.$$

Logo $x \sim z$ e a relação $\sim$ é transitiva.

De $(i), (ii)$ e (iii) segue que $\sim$ é uma relação de equivalência. ∎

Definição 1.2.6 *Seja* G *um grupo que age sobre um conjunto não vazio* S. *Dado* $a \in S$, *chamamos de* ***órbita*** *de* a *ou de* G-***órbita*** *de* a *à classe de equivalência de* a *pela relação de equivalência* $\sim$ *definida pela Proposição 1.2.5, ou seja,*

$$Orb(a) = G \cdot a = \{x \cdot a \mid x \in G\}.$$

Observação 1.2.7 *A união disjunta das* G*-órbitas é o conjunto* S.

Definição 1.2.8 *Seja G um grupo que age sobre um conjunto não vazio S e seja $x \in S$. O conjunto*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

é chamado ***subgrupo que fixa*** *x ou* ***estabilizador*** *de x em G* ***ou grupo de isotropia*** *de x.*

Proposição 1.2.9 *O conjunto G_x é um subgrupo de G.*

Demonstração: De fato, $G_x \neq \varnothing$, pois, como G age sobre S, $1_G \cdot y = y$, para todo $y \in S$. Em particular, $1_G \cdot x = x$. Logo $1_G \in G_x$. Além disso, para todos $g_1, g_2 \in G_x$, temos $g_1 \cdot x = x$ e $g_2 \cdot x = x$. De $g_2 \cdot x = x$, temos

$$g_2 \cdot x = x \Leftrightarrow g_2^{-1}(g_2 \cdot x) = g_2^{-1} \cdot x \Leftrightarrow x = g_2^{-1} \cdot x \Rightarrow g_2^{-1} \in G_x.$$

Agora

$$(g_1 g_2^{-1}) \cdot x = g_1(g_2^{-1} \cdot x) = g_1 \cdot x = x.$$

Logo $(g_1 g_2^{-1}) \in G_x$ e, portanto, G_x é subgrupo de G. ∎

Definição 1.2.10 *Seja G um grupo que age sobre um conjunto não vazio S. O conjunto*

$$S_0 = \{x \in S \mid gx = x, \text{ para todo } g \in G\}$$

é chamado ***conjunto dos pontos fixos*** *de S.*

Exemplo 1.2.11 *Seja G um grupo que age sobre si mesmo por conjugação, isto é,*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & ghg^{-1} = h^g. \end{array}$$

A órbita

$$x^G = \{y \in S \mid \exists g \in G : y = gxg^{-1}\} = \{gxg^{-1} \mid g \in G\}$$

é dita ***classe de conjugação de x em G****.*

Exemplo 1.2.12 *Se um subgrupo H de um grupo G age sobre G por conjugação, isto é,*

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h,x) & \longmapsto & hxh^{-1} \end{array}$$

então a órbita de x é

$$x^H = \{hxh^{-1} \mid h \in H\}$$

e o grupo de isotropia de x, também chamado ***centralizador*** *de x em H, é*

$$H_x = \{h \in H \mid hx = x\} = \{h \in H \mid hxh^{-1} = x\} = \{h \in H \mid hx = xh\} = C_H(x).$$

Exemplo 1.2.13 *Seja $S = S(G)$ o conjunto de todos os subgrupos de um grupo finito G. Seja H um subgrupo de G e considere a ação de H sobre S por conjugação, ou seja,*

$$\begin{array}{rcl} H \times S & \longrightarrow & S \\ (h, K) & \longmapsto & hKh^{-1} = K^h. \end{array}$$

Então a órbita de um subgrupo K é

$$K^H = \{hKh^{-1} \mid h \in H\}$$

e o grupo de isotropia de K, também chamado ***normalizador*** *de K em H, é*

$$H_K = \{h \in H \mid hKh^{-1} = K\} = N_H(K).$$

Proposição 1.2.14 *Sejam G um grupo e K um subgrupo de G. Então:*

(i) K é um subgrupo normal de $N_G(K)$.

(ii) K é um subgrupo normal de G se, e somente se, $N_G(K) = G$.

Demonstração:

(i) É claro que, para todo $k \in K$, temos $kKk^{-1} = K$. Logo $K \subseteq N_G(K)$. Além disso, para todo $h \in N_G(K)$, temos $hKh^{-1} = K$. Portanto, K é um subgrupo normal de $N_G(K)$.

(ii) Seja K um subgrupo normal de G. Então, para todo $g \in G$, temos

$$gKg^{-1} = K \Rightarrow g \in N_G(K) \Rightarrow G \subseteq N_G(K).$$

A outra inclusão segue diretamente da Proposição 1.2.9. A recíproca é imediata por (i).

■

Proposição 1.2.15 *Se um grupo G age sobre um conjunto não vazio S, então o tamanho da órbita de x em S é o índice $[G : G_x]$.*

Demonstração: Defina a seguinte função

$$\begin{array}{rcl} \varphi : \ G/G_x & \longrightarrow & x^G \\ gG_x & \longmapsto & gx. \end{array}$$

A função φ está bem definida e é injetora, pois, dados gG_x e $hG_x \in G/G_x$ tais que $gG_x = hG_x$, temos

$$gG_x = hG_x \Leftrightarrow g^{-1}hG_x = G_x \Leftrightarrow g^{-1}h \in G_x \Leftrightarrow g^{-1}hx = x \Leftrightarrow gx = hx.$$

Além disso, a função φ é sobrejetora, pois, dado $y \in x^G$, então y é da forma gx, com $g \in G$. Daí, tome $z = gG_x$ e $\varphi(z) = y$. Portanto φ é uma bijeção. ■

Corolário 1.2.16 *Sejam G um grupo finito e K um subgrupo de G.*

(i) O número de elementos nas classes de conjugação de x em G é $[G : C_G(x)]$ que divide $|G|$.

(ii) Se $x_1^G, x_2^G, \ldots, x_n^G$ $(x_i \in G)$ são as classes de conjugação (distintas 2 a 2) de G, então $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$, que é chamada ***equação das classes*** *de um grupo finito G.*

(iii) O número de subgrupos de G conjugados a K é $[G : N_G(K)]$, que divide $|G|$.

Demonstração:

(i) Considere a ação conjugação de G sobre G. Daí $G_x = C_G(x)$ e, pela Proposição 1.2.15, o número de elementos na classe de conjugação de x é $[G : C_G(x)]$ que, pelo Teorema de Lagrange, divide $|G|$.

(ii) Considere a ação conjugação de G sobre G. Pela Proposição 1.2.15, o tamanho da órbita de x em G é o índice $[G : C_G(x)]$. Pela Observação 1.2.7, $G = x_1^G \dot\cup x_2^G \dot\cup \cdots \dot\cup x_n^G$. Logo

$$|G| = |x_1^G| + |x_2^G| + \cdots + |x_n^G| = \sum_{i=1}^{n} [G : C_G(x_i)].$$

(iii) Seja K um subgrupo de um grupo G e considere a ação conjugação de G sobre $S(G)$, ou seja,

$$\begin{array}{ccc} G \times S(G) & \longrightarrow & S(G) \\ (g, K) & \longmapsto & gKg^{-1}. \end{array}$$

Daí a órbita de K é $K^G = \{gKg^{-1} \mid g \in G\}$ e o grupo de isotropia $G_K = N_G(K)$. Pela Proposição 1.2.15, o tamanho da órbita de K, que é o numero de subgrupos de G conjugados a K, é $K^G = [G : N_G(K)]$ que, pelo Teorema de Lagrange, divide $|G|$.

■

Definição 1.2.17 *Definimos o* ***centro*** *$Z(G)$ de um grupo G como o conjunto dos elementos de G que comutam com todos os elementos de G, ou seja,*

$$Z(G) = \{x \in G \mid gxg^{-1} = x, \text{ para todo } g \in G\}.$$

Assim, $Z(G)$ é o ***conjunto dos pontos fixos*** *da ação de G em G por conjugação.*

Observação 1.2.18 *Da Definição 1.2.17 um elemento $x \in G$ está no centro $Z(G)$ se, e somente se, a classe de conjugação de x em G consiste apenas do elemento x. De fato, se $x \in Z(G)$, então*

$$x^G = \{yxy^{-1} \mid y \in G\} = \{xyy^{-1} \mid y \in G\} = \{x\}.$$

Reciprocamente, se $x^G = \{x\}$, então $x \in Z(G)$. Dessa forma, se G é finito e $x \in Z(G)$, então

$$[G : C_G(x)] = |x^G| = 1.$$

Logo a equação das classes fica:

$$\begin{aligned} |G| &= \sum_{i=1}^{n} [G : C_G(x)] \quad (n = n^o \text{ de classes de conjugação em } G) \\ &= \sum_{x_i \in Z(G)} [G : C_G(x)] + \sum_{x_i \notin Z(G)} [G : C_G(x)] \\ &= |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x)], \end{aligned}$$

onde

$$[G : C_G(x)] > 1 \text{ se, e somente se, } x_i \in G - Z(G).$$

1.3 p-Grupos

Nesta seção estudaremos os grupos cuja ordem é uma potência de um número primo p qualquer, os chamados p-grupos. Tais grupos nos oferecem resultados bem interessantes, como veremos a seguir.

Lema 1.3.1 *Sejam H um grupo de ordem p^n, com p primo e $n \geq 1$, que age sobre um conjunto finito e não vazio S e $S_0 = \{x \in S \mid hx = x, \text{ para todo } h \in H\}$. Então $|S| \equiv |S_0| \pmod{p}$.*

Demonstração: Pela Observação 1.2.18, uma órbita $\bar{x}$ contém exatamente um elemento se, e somente se, $x \in S_0$. Dessa forma, $S = S_0 \dot{\cup} \bar{x}_1 \dot{\cup} \cdots \dot{\cup} \bar{x}_n$, onde $|\bar{x}_i| > 1$ e $x_i \notin S_0$, para todo $i = 1, \cdots, n$. Assim,

$$|S| = |s_0| + \sum_{i=1}^{n} |\bar{x}_i|.$$

Pela Proposição 1.2.15, $|\bar{x}_i| = [H : H_{x_i}] > 1$ e, como $|H| = p^n$, então pelo Teorema de Lagrange, $[H : H_{x_i}]$ divide p^n. Logo $\sum_{i=1}^{n} |\bar{x}_i|$ é um múltiplo positivo de p. Portanto, $|S| \equiv |S_0| \pmod{p}$. ∎

Teorema 1.3.2 (Teorema de Cauchy)

Seja G um grupo finito tal que p divide $|G|$, para algum primo p. Então G contém um elemento de ordem p.

Demonstração: (J. K. Mckay)

Considere o conjunto $S = \{(a_1, a_2, \ldots, a_p) \mid a_i \in G \text{ e } a_1a_2\cdots a_p = 1_G\}$. O conjunto S é não vazio, pois o elemento $(1_G, 1_G, \ldots, 1_G) \in S$. Além disso, o elemento a_p de cada p-upla de S é determinado de modo único como $a_p = (a_1a_2\cdots a_{p-1})^{-1}$. Assim, se $|G| = n$, então $|S| = n^{p-1}$. Como $p \mid n$, então $|S| \equiv 0 \pmod p$.

Considere a ação do grupo aditivo $\mathbb{Z}_p$ sobre S por permutação ádica, isto é, para $k \in \mathbb{Z}_p$, com $0 \leq k \leq p-1$,

$$k \cdot (a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k).$$

Note que $(a_{k+1}, a_{k+2}, \ldots, a_p, a_1, a_2, \ldots, a_k) \in S$, pois num grupo, se $ab = e$, então

$$ba = a^{-1}(ab)a = a^{-1}ea = e.$$

Assim, se $(a_1, a_2, \ldots, a_k, a_{k+1}, \ldots a_p) \in S$, então $\underbrace{a_1a_2\cdots a_k}_{a}\underbrace{a_{k+1}\cdots a_p}_{b} = 1_G$. Logo

$$\underbrace{a_{k+1}a_{k+2}\cdots a_p}_{b}\underbrace{a_1a_2\cdots a_k}_{a} = 1_G.$$

Tal ação está bem definida, pois:

(i) $0 \cdot (a_1, a_2, \ldots, a_p) = (a_1, a_2, \ldots, a_p)$, para todo $(a_1, a_2, \ldots, a_p) \in S$.

(ii) Para todos $k, k' \in \mathbb{Z}_p$, temos

$$\begin{aligned}(k+k') \cdot (a_1, a_2, \ldots, a_p) &= (a_{(k+k')+1}, a_{(k+k')+2}, \ldots, a_p, a_1, a_2, \ldots, a_{(k+k')} \\ &= k \cdot (a_{k'+1}, a_{k'+2}, \ldots, a_p, a_1, a_2, \ldots, a_{k'}) \\ &= k(k' \cdot (a_1, a_2, \ldots, a_p)).\end{aligned}$$

Agora, como

$$S_0 = \{(a_1, a_2, \ldots, a_p) \in S \mid k \cdot (a_1, a_2, \ldots, a_p) = (a_1, a_2, \ldots, a_p), \text{ para todo } k \in \mathbb{Z}_p\},$$

um elemento $(x_1, x_2, \ldots, x_p) \in S_0$ se, e somente se, $x_1 = x_2 = \cdots = x_p$. De fato, se $(x_1, x_2, \ldots, x_p) \in S_0$, então, para todo $k \in \mathbb{Z}$,

$$k \cdot (x_1, x_2, \ldots, x_p) = (x_{k+1}, x_{k+2}, \ldots, x_p, x_1, x_2, \ldots, x_k) = (x_1, x_2, \ldots, x_p).$$

Em particular, para $k = 1$, temos

$$\begin{aligned}1 \cdot (x_1, x_2, \ldots, x_p) = (x_1, x_2, \ldots, x_p) &\Leftrightarrow (x_2, x_3, \ldots, x_p, x_1) = (x_1, x_2, \ldots, x_p) \\ &\Leftrightarrow \begin{cases} x_1 = x_2 \\ x_2 = x_3 \\ x_3 = x_4 \\ \vdots \\ x_{p-1} = x_p \end{cases} \\ &\Leftrightarrow x_1 = x_2 = \cdots = x_p.\end{aligned}$$

A recíproca é imediata.

Observe agora que $S_0 \neq \emptyset$, pois o elemento $(1_G, 1_G, \ldots, 1_G) \in S_0$ e, assim, $|S_0| \neq 0$. Além disso, pelo Lema 1.3.1,

$$0 \equiv |S| \equiv |S_0| \,(\mathrm{mod}\, p),$$

logo existem pelo menos p elementos em S_0. Portanto, existe $1_G \neq a \in G$ tal que $(\underbrace{a, a, \ldots, a}_{p \text{ vezes}}) \in S_0$, ou seja, $a^p = 1_G$. ∎

Definição 1.3.3 *Um grupo no qual todo elemento tem ordem uma potência de algum número primo fixo p é dito um p-**grupo**. Se H é um subgrupo de G e H é um p-grupo, então H é dito um p-**subgrupo** de G.*

Corolário 1.3.4 *Um grupo finito G é um p-grupo, se e somente se, $|G| = p^m$, para algum $m \in \mathbb{Z}_+$.*

Demonstração: Se G é um p-grupo e q é um número primo que divide $|G|$, então, pelo Teorema de Cauchy, G contém um elemento de ordem q. Como todo elemento de G tem ordem uma potência de p, então $p = q$. Logo $|G|$ é uma potência de p. A recíproca segue imediatamente do Teorema de Lagrange. ∎

Corolário 1.3.5 *Se Gé um p-grupo finito, então $|Z(G)| > 1$.*

Demonstração: Seja G um p-grupo de ordem p^n e considere a equação das classes

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x)].$$

Na equação anterior, cada $[G : C_G(x)] > 1$ e divide $|G| = p^n$. Logo cada $[G : C_G(x)]$ é um múltiplo de p e consequentemente $\sum [G : C_G(x)]$ também é um múltiplo de p. Por outro lado, já que o elemento neutro de G pertence ao centro de G, então $Z(G) \neq \emptyset$. Portanto $Z(G)$ tem pelo menos p elementos. ∎

Lema 1.3.6 *Se H é um p-subgrupo de um grupo finito G, então*

$$[N_G(H) : H] \equiv [G : H] \,(\mathrm{mod}\, p).$$

Demonstração: Seja $S = \{xH \mid x \in G\}$ o conjunto das classes laterais de H em G. Então $|S| = [G : H]$. Considere a ação de H em S por translação à esquerda, isto é,

$$\begin{array}{ccc} H \times S & \longrightarrow & S \\ (h, xH) & \longmapsto & hxH. \end{array}$$

Daí

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}hxH = H, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}hxH \in H, \text{ para todo } h \in H \\ &\Leftrightarrow h \in x^{-1}Hx, \text{ para todo } h \in H \\ &\Leftrightarrow H = xHx^{-1} \\ &\Leftrightarrow x \in N_G(H). \end{aligned}$$

Logo $S_0 = \{xH \in S \mid x \in N_G(H)\}$ e, daí, $|S_0| = [N_G(H) : H]$. Portanto, pelo Lema 1.3.1,

$$[G : H] = |S| \equiv |S_0| = [N_G(H) : H] \,(\mathrm{mod}\, p).$$

■

Corolário 1.3.7 *Se H é um p-subgrupo de um grupo finito G tal que p divide $[G : H]$, então $N_G(H) \neq H$.*

Demonstração: Se $p \mid [G : H]$, então, pelo Lema 1.3.6,

$$0 \equiv [G : H] \equiv [N_G(H) : H] \,(\mathrm{mod}\, p).$$

Como $[N_G(H) : H] \geq 1$ em qualquer caso, então devemos ter $[N_G(H) : H] > 1$. Logo, $H \neq N_G(H)$. ■

1.4 Os Teoremas de Sylow

Estes teoremas foram demonstrados pelo matemático norueguês Ludwig Sylow em 1876 e garantem a existência de p-subgrupos em grupos finitos, além de fornecer informações detalhadas sobre estes subgrupos. Tais teoremas ainda são uma importante ferramenta para encontrar p-subgrupos normais não triviais em um grupo finito.

Teorema 1.4.1 (1º Teorema de Sylow)

Seja G um grupo finito de ordem $p^n m$, com $n \geq 1$, p primo e $mdc\{p, m\} = 1$. Então G contém um subgrupo de ordem p^i, para cada $1 \leq i \leq n$, e cada subgrupo de G de ordem p^i, $i < n$, é normal em algum subgrupo de ordem p^{i+1}.

Demonstração: Como p divide $|G|$, pelo Teorema de Cauchy, G possui um subgrupo de ordem p gerado por $a \in G$, ou seja, $|\langle a \rangle| = p$.

Por indução sobre n, suponha H um subgrupo de G de ordem p^i, com $1 \leq i < n$. Daí $p \mid [G : H]$ e, pelo Corolário 1.3.7, $H \neq N_G(H)$. Pela Proposição 1.2.14, $H \trianglelefteq N_G(H)$ e, com isso, $N_G(H)/H$ é grupo. Além disso, pelo Lema 1.3.6, $p \mid [N_G(H) : H]$, daí, pelo Teorema de Cauchy, existe um elemento em $N_G(H)/H$ de ordem p. Assim, pelo Teorema da Correspondência, existe um subgrupo $H_1 \leq N_G(H)$ tal que H_1/H tem ordem p e $H_1 \supsetneq H$. Como $H \trianglelefteq N_G(H)$, então $H \trianglelefteq H_1$ e, pelo Teorema de Lagrange,

$$|H_1| = |H|[H_1 : H] = p^i p = p^{i+1}.$$

■

Definição 1.4.2 *Um subgrupo H de um grupo G é dito um p-**subgrupo de Sylow** de G, para algum primo p, se H é um p-subgrupo maximal de G, isto é, se $H \leq K \leq G$ com K p-subgrupo de G, então $H = K$.*

Corolário 1.4.3 *Seja G um grupo finito tal que $|G| = p^n m$, onde p é um número primo, $n \geq 1$ e $\text{mdc}\{p, m\} = 1$, e seja H um p-subgrupo de G. Então*

(i) H é um p-subgrupo de Sylow de G se, e somente se, $|H| = p^n$.

(ii) Todo conjugado de um p-subgrupo de Sylow de G é um p-subgrupo de Sylow de G.

(iii) Se existe um único p-subgrupo de Sylow de G, digamos H, então H é um subgrupo normal de G.

Demonstração:

i) Seja G um grupo de ordem $p^n m$. Pelo 1º Teorema de Sylow, G contém um subgrupo de ordem p^i, para cada $1 \leq i \leq n$. Como H é um p-subgrupo de Sylow de G, então H é um p-subgrupo maximal de G. Logo $|H| = p^n$. Reciprocamente, se $|H| = p^n$, então H é um p-subgrupo de G. Suponha $H \leq K \leq G$ com K um p-subgrupo de G. Como $|G| = p^n m$ e $|H| = p^n$, então $H = K$ e, assim, H é um p-subgrupo maximal de G. Consequentemente, H é um p-subgrupo de Sylow de G.

ii) Seja G um grupo e H um p-subgrupo de Sylow de G. Defina

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & G \\ & x & \longmapsto & gxg^{-1}. \end{array}$$

A função φ está bem definida, pois dado $x \in G$ e $g \in G$, gxg^{-1} é único. Além disso, a função φ é homomorfismo, pois, para todos $x, y, \in G$,

$$\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y), \text{ para todo } g \in G.$$

Ainda, φ é monomorfismo, pois

$$\ker(\varphi) = \{x \in G \mid \varphi(x) = 1_G\} = \{x \in G \mid gxg^{-1} = 1_G\} = \{1_G\}.$$

Logo φ é um automorfismo de G. Como H é um subgrupo de G, então $\varphi(H) = gHg^{-1}$ também é subgrupo de G. Consideremos a restrição

$$\begin{array}{rccl} \varphi|_H : & H & \longrightarrow & \varphi(H) \\ & h & \longmapsto & \varphi(h) \quad = ghg^{-1}. \end{array}$$

A restrição da função φ a H, restringindo também a imagem a $\varphi(H)$, é um isomorfismo e, portanto, $H \cong gHg^{-1}$, para todo $g \in G$. Como H é um p-subgrupo de Sylow de G arbitrário, então todo conjugado de um p-subgrupo de Sylow de G também é um p-subgrupo de Sylow de G.

iii) Seja G um grupo e H um p-subgrupo de Sylow de G. Por *ii*), gHg^{-1} é um p-subgrupo de Sylow de G, para todo $g \in G$. Como existe um único p-subgrupo de Sylow de G, então devemos ter $H = gHg^{-1}$, para todo $g \in G$. Portanto, $H \lhd G$. ∎

Teorema 1.4.4 (2º Teorema de Sylow)

Se H é um p-subgrupo de um grupo finito G e K é um p-subgrupo de Sylow qualquer de G, então existe $x \in G$ tal que $H < xKx^{-1}$. Em particular, dois quaisquer p-subgrupos de Sylow de G são conjugados.

Demonstração: Seja $S = \{xK \mid x \in G\}$ e faça H agir sobre S por translação à esquerda. Pelo Lema 1.3.1,

$$|S_0| \equiv |S| = [G : K] \,(\mathrm{mod}\, p).$$

Como $p \nmid [G : K]$, pois K é p-subgrupo de Sylow de G, $|S_0| \neq 0$. Assim, existe $xK \in S_0$ e daí temos

$$\begin{aligned} xK \in S_0 &\Leftrightarrow hxK = xK, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}hxK = K, \text{ para todo } h \in H \\ &\Leftrightarrow x^{-1}hx \in K, \text{ para todo } h \in H \\ &\Leftrightarrow h \in xKx^{-1}, \text{ para todo } h \in H \\ &\Leftrightarrow H \subseteq xKx^{-1}. \end{aligned}$$

Em particular, se H é um p-subgrupo de Sylow de G, então $|H| = |K| = |xKx^{-1}|$ e daí $H = xKx^{-1}$. ∎

Teorema 1.4.5 (3º Teorema de Sylow)

Se G é um grupo finito e p é um número primo, então o número de p-subgrupos de Sylow de G divide $|G|$ e é da forma $kp + 1$, para algum $k \geq 1$.

Demonstração: Pelo Teorema 1.4.4, o número de p-subgrupos de Sylow é o número de conjugados de qualquer um deles, digamos H. Pelo Corolário 1.2.16, o número de classes de conjugação, que é o número de conjugados de H em G, é $[G : N_G(H)]$, que pelo Teorema de Lagrange, divide $|G|$. Seja

$$S = \{Q \leq G \mid Q \text{ é um } p\text{-subgrupo de Sylow de } G\}$$

e faça H agir sobre S por conjugação, isto é,

$$\begin{array}{ccc} H \times S & \longrightarrow & S \\ (a, Q) & \longmapsto & aQa^{-1}. \end{array}$$

Assim,

$$Q \in S_0 \Leftrightarrow xQx^{-1} = Q, \text{ para todo } x \in H \Leftrightarrow H \subset N_G(G).$$

Como H e Q são ambos p-subgrupos de Sylow de G e também de $N_G(Q)$, então H e Q são conjugados em $N_G(Q)$, ou seja, existe $y \in N_G(Q)$ tal que $H = yQy^{-1}$. Como $Q \lhd N_G(Q)$, temos $H = Q$. Logo, $S_0 = \{H\}$ e, pelo Lema 1.3.1,

$$|S| \equiv |S_0| \,(\mathrm{mod}\, p) \Rightarrow |S| \equiv 1 (\mathrm{mod}\, p).$$

Portanto, $|S| = kp + 1$, para algum $k \in \mathbb{Z}_+$. ∎

Corolário 1.4.6 *Se H é um p-subgrupo de Sylow de um grupo finito G, então*

$$N_G(N_G(H)) = N_G(H).$$

Demonstração: Todo conjugado de H é um p-subgrupo de Sylow de G e de qualquer subgrupo de G que o contenha. Já que $H \lhd N_G(H)$, então H é o único p-subgrupo de Sylow de $N_G(H) = N$. Além disso, como

$$x \in N_G(N) \Leftrightarrow xNx^{-1} = N,\ xHx^{-1} \leq xNx^{-1} = N \text{ e } |xHx^{-1}| = |H|,$$

então $xHx^{-1} = H$ e daí $x \in N$. Logo $N_G(N_G(H)) \subseteq N_G(H)$.

A outra inclusão é óbvia. ∎

Observação 1.4.7 *Sejam m um inteiro, p um número primo, G um grupo de ordem m e n_p o número de p-subgrupos de Sylow de G. Se não tivermos nenhuma outra informação sobre G, então, em geral, o 3º Teorema de Sylow não permite determinar precisamente o valor de n_p. Vejamos os exemplos a seguir.*

Exemplo 1.4.8 *Seja G um grupo tal que $|G| = 6 = 2 \cdot 3$. Pelo 3º Teorema de Sylow,*

$$\begin{cases} n_2 \equiv 1 (\mathrm{mod}\, 2) \\ n_2 \mid 3 \end{cases} \Rightarrow n_2 = 1 \quad ou \quad n_2 = 3,$$

e ambos os casos podem acontecer: $n_2 = 1$, se $G \cong \mathbb{Z}_6$ e $n_2 = 3$, se $G \cong S_3$.

Exemplo 1.4.9 *Seja G um grupo de ordem $380 = 2^2 \cdot 5 \cdot 19$. Pelo 3º Teorema de Sylow,*

$$\begin{cases} n_5 \equiv 1 (\mathrm{mod}\, 5) \\ n_5 \mid 2^2 \cdot 19 \end{cases} \Rightarrow n_5 = 1 \quad ou \quad n_5 = 76.$$

Analogamente, o 3º Teorema de Sylow nos dá

$$\begin{cases} n_{19} \equiv 1 (\mathrm{mod}\, 19) \\ n_{19} \mid 2^2 \cdot 5 \end{cases} \Rightarrow n_{19} = 1 \quad ou \quad n_{19} = 20.$$

Sejam H um grupo de ordem 5 e K um grupo de ordem 19. Afirmamos que n_5 ou n_{19} é igual a 1. De fato, caso contrário, G possuiria $76 \cdot 4 = 304$ elementos de ordem 5, pois a interseção de dois grupos distintos de ordem 5 é $\{1_G\}$ e também possuiria $20 \cdot 18 = 360$ elementos de ordem 19, o que seria absurdo, pois $|G| = 380$. Portanto, um dos subgrupos H ou K é normal em G e, em todo caso, o conjunto HK é um subgrupo de G de ordem $5 \cdot 19 = 95$, (pois $H \cap K = \{1_G\}$). Agora, pelo 3º Teorema de Sylow, aplicado a HK, vemos que HK possui um único subgrupo de ordem 5, que necessariamente deve ser H e um único subgrupo de ordem 19, que necessariamente deve ser K. Assim, $H \lhd HK$ e daí $HK \subseteq N_G(H)$. Logo

$$n_5 = [G : N_G(H)] \leq [G : HK] = 2^2 \text{ e, portanto, } n_5 = 1.$$

Analogamente, $H \lhd HK$, e temos $HK \subseteq N_G(K)$. Assim,

$$n_{19} = [G : N_G(K)] \leq [G : HK] = 2^2 \text{ e, portanto, } n_{19} = 1.$$

Exemplo 1.4.10 *Seja G um grupo de ordem $321 = 3 \cdot 107$. Aplicando o 3º Teorema de Sylow, resulta em*

$$\begin{cases} n_3 \equiv 1 (\mathrm{mod}\, 3) \\ n_3 \mid 107 \end{cases} \Rightarrow n_3 = 1$$

e também

$$\begin{cases} n_{107} \equiv 1 (\mathrm{mod}\, 107) \\ n_{107} \mid 3 \end{cases} \Rightarrow n_{107} = 1.$$

Logo G possui um único subgrupo H de ordem 3 e um único subgrupo K de ordem 107, assim $H \lhd G$ e também $K \lhd G$. Além disso, H e K são cíclicos, pois ambos são de ordem prima e $H \cap K = \{1_G\}$. Portanto, $G = H \times K$ e G é abeliano. Além disso, como $\mathrm{mdc}\{3, 107\} = 1$, então G é um grupo cíclico, pois

$$G \cong H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_{107} \cong \mathbb{Z}_{321}.$$

1.5 Produto Direto

Nesta seção descreveremos um procedimento importante que permite construir um grupo a partir de outros grupos dados, o produto direto.

Definição 1.5.1 *Sejam $(H, \star)$ e $(K, \triangle)$ dois grupos. Considere o conjunto*

$$H \times K = \{(h, k) \mid h \in H, k \in K\}$$

e defina, para todos $(h_1, k_1), (h_2, k_2) \in H \times K$,

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \star h_2, k_1 \triangle k_2).$$

Dessa forma $(H \times K, \cdot)$ é um grupo chamado ***produto direto externo*** *de H por K ou simplesmente* ***produto direto*** *de H por K.*

De fato, para todos $(h_1, k_1), (h_2, k_2), (h_3, k_3) \in H \times K$, temos

$$\begin{aligned}
[(h_1, k_1) \cdot (h_2, k_2)] \cdot (h_3, k_3) &= (h_1 \star h_2, k_1 \triangle k_2) \cdot (h_3, k_3) \\
&= ((h_1 \star h_2) \star h_3, (k_1 \triangle k_2) \triangle k_3) \\
&= (h_1 \star (h_2 \star h_3), k_1 \triangle (k_2 \triangle k_3)) \\
&= (h_1, k_1)(h_2 \star h_3, k_2 \triangle k_3) \\
&= (h_1, k_1) \cdot [(h_2, k_2) \cdot (h_3, k_3)],
\end{aligned}$$

e a operação definida em $H \times K$ é associativa.

Seja $(1_H, 1_K) \in H \times K$, ($1_H, 1_K$ elemento neutro de H e K, respectivamente). Para todo $(h, k) \in H \times K$, temos

$$(1_H, 1_K) \cdot (h, k) = (1_H \star h, 1_K \triangle k) = (h, k) \quad \text{e} \quad (h, k) \cdot (1_H, 1_K) = (h \star 1_H, k \triangle 1_K) = (h, k).$$

Logo $(1_H, 1_K)$ é o elemento neutro de $(H \times K, \cdot)$

Para cada $(h, k) \in H \times K$, existe $(h^{-1}, k^{-1}) \in H \times K$ tal que

$$(h, k) \cdot (h^{-1}, k^{-1}) = (h \star h^{-1}, k \triangle k^{-1}) = (1_H, 1_K)$$
$$(h^{-1}, k^{-1}) \cdot (h, k) = (h^{-1} \star h, k^{-1} \triangle k) = (1_H, 1_K).$$

Logo $(h, k)^{-1} = (h^{-1}, k^{-1})$ em $H \times K$.

Observação 1.5.2 *Nem H, nem K é um subgrupo de $H \times K$. Mas $H \times K$ contém cópias isomorfas de cada um deles, a saber:*

$$H \times 1_K = \{(h, 1_K) \mid h \in H\} \quad e \quad 1_H \times K = \{(1_H, k) \mid k \in K\}.$$

Proposição 1.5.3 *O grupo $H \times K$ é abeliano se, e somente se, H e K são abelianos.*

Demonstração: Para todos $(h_1, k_1), (h_2, k_2) \in H \times K$,

$$\begin{aligned} H \times K \quad \text{é abeliano} &\Leftrightarrow (h_1, k_1) \cdot (h_2, k_2) = (h_2, k_2) \cdot (h_1, k_1) \\ &\Leftrightarrow (h_1 \star h_2, k_1 \vartriangle k_2) = (h_2 \star h_1, k_2 \vartriangle k_1) \\ &\Leftrightarrow \begin{cases} h_1 \star h_2 = h_2 \star h_1 \\ k_1 \vartriangle k_2 = k_2 \vartriangle k_1 \end{cases} \\ &\Leftrightarrow H, K \text{ são abelianos.} \end{aligned}$$

■

Definição 1.5.4 *Sejam G um grupo , H e K subgrupos normais de G. Se $G = HK$ e $H \cap K = \{1_G\}$, então G é chamado* ***produto direto interno*** *de H por K.*

Teorema 1.5.5 *Se G é o produto direto interno de H por K, então G é isomorfo ao produto direto externo de H por K.*

Demonstração: Seja $G = HK = \{hk \mid h \in H, k \in K\}$, com $H \lhd G$, $K \lhd G$ e $H \cap K = \{1_G\}$. Defina a seguinte função,

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & H \times K \\ & hk & \longmapsto & (h, k). \end{array}$$

A função φ está bem definida, pois, dados $h, h_1 \in H$ e $k, k_1 \in K$ tais que $hk = h_1k_1$, então

$$hk = h_1k_1 \Leftrightarrow h^{-1}h_1 = kk_1^{-1} \in H \cap K = \{1_G\}.$$

Daí $h^{-1}h_1 = 1_G$ e $kk_1^{-1} = 1_G$, ou seja, $h_1 = h$ e $k_1 = k$ e, portanto $\varphi(h_1k_1) = \varphi(hk)$. A função φ é um homomorfismo de grupos, pois, para todos $h \in H, k \in K$, temos

$$khk^{-1} \in H, \text{ pois } H \lhd G \quad \text{e} \quad hk^{-1}h^{-1} \in K, \text{ pois } K \lhd G.$$

Assim, $khk^{-1}h^{-1} \in H \cap K = \{1_G\}$, logo $kh = hk$, ou seja, h e k comutam. Assim,

$$\varphi(hkh_1k_1) = \varphi(h(kh_1)k_1) = \varphi(\underbrace{hh_1}_{\in H}\ \underbrace{kk_1}_{\in K}) = (hh_1, kk_1) = (h, k)(h_1, k_1) = \varphi(hk)\varphi(h_1k_1).$$

Além disso, φ é injetora, pois

$$\ker(\varphi) = \{hk \mid \varphi(hk) = 1_{H\times K}\} = \{kh \mid (h,k) = (1_H, 1_K)\} = \{1_G\}.$$

Ainda, φ é sobretora, pois para todo $y \in H \times K$, y é da forma (h,k), onde $h \in H$, $k \in K$, assim, existe $x = hk \in G$ tal que $\varphi(x) = y$. Portanto φ é um isormorfismo de grupos e $G \cong H \times K$. ∎

O exemplo a seguir mostra que todas as hipóteses do Teorema 1.5.5 são necessárias.

Exemplo 1.5.6 *Sejam $G = S_3$, $H = \langle(123)\rangle$, $K = \langle(12)\rangle$. Daí temos*

$$H = \{1_{S_3}, (123), (132)\} \quad e \quad K = \{1_{S_3}, (12)\}$$

e, assim, $H \cap K = \{1_{S_3}\}$. Além disso,

$$HK = \{1_{S_3}, (123), (132), (12), (23), (13)\} = S_3.$$

Agora, $H \lhd S_3$, mas $K \not\lhd S_3$, pois,

$$(123)K = \{(123), (23)\} \quad e \quad K(123) = \{(123), (13)\},$$

ou seja, $(123)K \neq K(123)$.

Considere agora $f_0 = 1_{S_3}$, $f_1 = (123)$, $f_2 = (13)$, $f_3 = (132)$, $f_4 = (23)$, $f_5 = (12)$. Assim,

$$H \times K = \{(f_0, f_0), (f_0, f_5), (f_1, f_0), (f_1, f_5), (f_3, f_0), (f_3, f_5)\}.$$

Note que $H \times K$ é um grupo cíclico de ordem 6, a saber, $H \times K = \langle(f_1, f_5)\rangle$, ou seja, $H \times K \cong \mathbb{Z}_6$, que é um grupo abeliano. Logo $G = S_3$ não é isomorfo a $H \times K$, visto que S_3 não é abeliano.

Proposição 1.5.7 *Se $A \lhd H$ e $B \lhd K$, então $A \times B \lhd H \times K$ e, além disso,*

$$\frac{H \times K}{A \times B} \cong \frac{H}{A} \times \frac{K}{B}.$$

Demonstração: Para todos $a \in A, b \in B$, temos

$$hah^{-1} \in H, \text{ pois } A \lhd H \quad \text{e} \quad kbk^{-1} \in K, \text{ pois } B \lhd K.$$

Daí, para todos $(a,b) \in A \times B$, $(h,k) \in H \times K$,

$$(h,k) \cdot (a,b) \cdot (h,k)^{-1} = (h,k) \cdot (a,b) \cdot (h^{-1}, k^{-1}) = (hah^{-1}, kbk^{-1}) \in A \times B.$$

Logo $A \times B \lhd H \times K$.

Agora defina

$$\begin{array}{rccc} \psi: & H\times K & \longrightarrow & \frac{H}{A}\times\frac{K}{B} \\ & (h,k) & \longmapsto & (hA,kB). \end{array}$$

A função ψ está bem definida e é homomorfismo de grupos, pois, para todos (h,k), $(h_1,k_1)\in H\times K$,

$$\begin{aligned} \psi((h,k)\cdot(h_1,k_1)) &= \psi((hh_1,kk_1)) = (hh_1A,kk_1B) = (hA,kB)\cdot(h_1A,k_1B) \\ &= \psi(h,k)\cdot\psi(h_1,k_1). \end{aligned}$$

Ainda, a função ψ é sobrejetora, pois, para todo $y\in\dfrac{H}{A}\times\dfrac{K}{B}$, y é da forma (hA,kB), onde $h\in H, k\in K$. Daí, existe $x=(h,k)\in H\times K$ tal que $\psi(x)=y$.

Agora,

$$\begin{aligned} \ker(\psi) &= \{(k,h)\in H\times K \mid \psi(h,k)=1_{\frac{H}{A}\times\frac{K}{B}}\} \\ &= \{(h,k)\in H\times K \mid (hA,kB)=(A,B)\} \\ &= \{(h,k)\in H\times K \mid hA=A,\ kB=B\} \\ &= \{(h,k)\in H\times K \mid h\in A,\ k\in B\} \\ &= A\times B. \end{aligned}$$

Assim, pelo 1º Teorema do Isomorfismo,

$$\frac{H\times K}{\ker(\psi)}\cong \mathrm{Im}(\psi),\ \text{ou seja, }\frac{H\times K}{A\times B}\cong\frac{H}{A}\times\frac{K}{B}.$$

■

Observação 1.5.8 *Em particular, na Proposição 1.5.7, temos*

$$A\times\{1_K\}\lhd H\times K.$$

Corolário 1.5.9 *Se $G=H\times K$, então* $\dfrac{G}{H\times\{1_K\}}\cong K$.

Demonstração: Pela Observação 1.5.8, $H\times\{1_K\}\lhd H\times K$, assim, $\dfrac{G}{H\times\{1_K\}}$ é um grupo. Defina a seguinte função,

$$\begin{array}{rccc} \varphi: & H\times K & \longrightarrow & K \\ & (h,k) & \longmapsto & \varphi(h,k) = k. \end{array}$$

É fácil ver que tal função é um epimorfismo de grupos e que $\ker(\varphi) = H \times \{1_K\}$. Daí, pelo 1º Teorema do Isomorfismo,

$$\frac{G}{H \times \{1_K\}} \cong K.$$

■

A definição de produto direto $G \times H$ de grupos G e H pode ser estendida a uma família (possivelmente infinita) de grupos $\{G_i \mid i \in I\}$. No que segue, generalizaremos para o caso de uma família finita.

Definição 1.5.10 *Sejam $G_1, G_2, \ldots G_n$ grupos. Considere o conjunto*

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$$

e defina, para todos $(g_1, g_2, \ldots, g_n)$, $(h_1, h_2, \ldots, h_n) \in \prod_{i=1}^{n} G_i$, uma operação $(*)$ como segue,

$$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n).$$

Dessa forma $\prod_{i=1}^{n} G_i$ é um grupo.

Uma demontração análoga ao que foi feito após a Definição 1.5.1, nos mostra que a operação $*$ em $\prod_{i=1}^{n} G_i$ é associativa e tem como elemento neutro o elemento $(1_{G_1}, 1_{G_2}, \ldots, 1_{G_n})$. Além disso, $(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$ em $\prod_{i=1}^{n} G_i$.

Proposição 1.5.11 *O grupo $\prod_{i=1}^{n} G_i$ é abeliano se, e somente se, cada G_i é abeliano, para $i = 1, ..., n$.*

Demonstração: O grupo $\prod_{i=1}^{n} G_i$ é abeliano se, e somente se, para todos $(g_1, g_2, \ldots, g_n)$, $(h_1, h_2, \ldots, h_n) \in \prod_{i=1}^{n} G_i$

$$\begin{aligned}
(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) &= (h_1, h_2, \ldots, h_n) * (g_1, g_2, \ldots, g_n), \\
\Leftrightarrow (g_1 h_1, g_2 h_2, \ldots, g_n h_n) &= (h_1 g_1, h_2 g_2, \ldots, h_n g_n) \\
\Leftrightarrow g_1 h_1 = h_1 g_1, g_2 h_2 &= h_2 g_2, \ldots, g_n h_n = h_n g_n.
\end{aligned}$$

Logo cada G_i é abeliano, para $(i = 1, ..., n)$.

■

Proposição 1.5.12 *Sejam $G_1, G_2, \ldots G_n$ grupos.*

(i) A função

$$\begin{array}{rccl} \iota_i : & G_i & \hookrightarrow & \prod_{i=1}^n G_i \\ & g_i & \longmapsto & \iota_i(g_i) \quad = (1_{G_1}, 1_{G_2}, \ldots, g_i, \ldots, 1_{G_n}) \end{array}$$

é um monomorfismo de grupos.

(ii) O conjunto $\iota_i(G_i)$ é um subgrupo normal de $\prod_{i=1}^n G_i$.

(iii) A função

$$\begin{array}{rccl} \pi_k : & \prod_{i=1}^n G_i & \longrightarrow & G_k \\ & (g_1, g_2, \ldots, g_k, \ldots, g_n) & \longmapsto & g_k \end{array}$$

é um epimorfismo de grupos.

Demonstração:

(*i*) Sejam $g_i, h_i \in G_i$, com $1 \leq i \leq n$.

$$\begin{aligned} \iota_i(g_i h_i) &= (1g_1, 1g_2, \ldots, g_i h_i, \ldots, 1g_n) \\ &= (1g_1, 1g_2, \ldots, g_i, \ldots, 1g_n) * (1g_1, 1g_2, \ldots, h_i, \ldots, 1g_n) \\ &= \iota_i(g_i)\iota_i(h_i) \end{aligned}$$

Logo a função ι_i é um homomorfismo de grupos. Além disso,

$$\begin{aligned} \ker(\iota_i) &= \{g_i \in G_i \mid \iota_i(g_i) = 1_{\prod_{i=1}^n G_i}\} \\ &= \{g_i \in G_i \mid (1_{G_1}, 1_{G_2}, \ldots, g_i, \ldots, 1_{G_n}) = (1_{G_1}, 1_{G_2}, \ldots, 1_{G_i}, \ldots, 1_{G_n})\} \\ &= \{g_i \in G_i \mid g_i = 1_{G_i}\} \\ &= \{1_{G_i}\}. \end{aligned}$$

Logo ι_i é um monomorfismo de grupos.

(*ii*) Para todos $(g_1, g_2, \ldots, g_n) \in \prod_{i=1}^n G_i$, $(1_{G_1}, 1_{G_2}, \ldots, h_i, \cdots, 1_{G_n}) \in \iota_i(G_i)$,

$$\begin{aligned} &(g_1, g_2, \ldots, g_n) * (1_{G_1}, 1_{G_2}, \ldots, h_i, \ldots, 1_{G_n}) * (g_1, g_2, \ldots, g_n)^{-1} \\ &\quad = (g_1, g_2, \ldots, g_n) * (1_{G_1}, 1_{G_2}, \ldots, h_i, \ldots, 1_{G_n}) * (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}) \\ &\quad = (g_1 g_1^{-1}, g_2 g_2^{-1}, \ldots, g_i h_i g_i^{-1}, \ldots, g_n g_n^{-1}) \\ &\quad = (1_{G_1}, 1_{G_2}, \ldots, g_i h_i g_i^{-1}, \ldots, 1_{G_n}) \ \in \iota_i(G_i). \end{aligned}$$

Logo $\iota_i(G_i)$ é um subgrupo normal de $\prod_{i=1}^n G_i$.

(*iii*) Sejam $(g_1, g_2, \ldots, g_n)$, $(h_1, h_2, \ldots, h_n) \in \prod_{i=1}^n G_i$. Daí

$$\begin{aligned} \pi_k((g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n)) &= \Pi_k(g_1 h_1, g_2 h_2, \ldots, g_k h_k, \ldots, g_n h_n) \\ &= g_k h_k \\ &= \pi_k(g_1, g_2, \ldots, g_n)\, \pi_k(h_1, h_2, \ldots, h_n). \end{aligned}$$

Logo π_k é um homomorfismo de grupos.

Agora, para todo $g_k \in G_k$, existe um elemento $(1_{G_1}, 1_{G_2}, \ldots, g_k, \ldots, 1_{G_n}) \in \prod_{i=1}^{n} G_i$ tal que $\pi_k(1_{G_1}, 1_{G_2}, \ldots, g_k, \ldots, 1_{G_n}) = g_k$. Logo π_k é um epimorfismo de grupos.

■

Definição 1.5.13 *Sejam G um grupo e $H_1, H_2, \ldots, H_n$ subgrupos de G. Dizemos que G é o* ***produto direto interno*** *de $H_1, H_2, \ldots, H_n$ se, e somente se, as seguintes condições são satisfeitas:*

(1) $h_i h_j = h_j h_i$, *para todos* $h_i \in H_i,\ h_j \in H_j,$ *com* $i \neq j$.

(2) Todo elemento $g \in G$ *se escreve de modo único na forma* $g = h_1 h_2 \cdots h_n$, *onde* $h_i \in H_i,\ i \in \{1, ..., n\}$.

Proposição 1.5.14 *Sejam G um grupo e $H_1, H_2, \ldots, H_n$ subgrupos de G. Então G é o produto direto interno de $H_1, H_2, \ldots, H_n$ se, e somente se, as seguintes condições são satisfeitas:*

(i) $H_i \lhd G$, *para todo* $i = 1, ..., n$.

(ii) $G = H_1 H_2 \cdots H_n$.

(iii) $H_i \cap H_1 \cdots H_{i-1} H_{i+1} \cdots H_n = \{1_G\}$, *para todo* $i \in \{1, ..., n\}$.

Demonstração: Suponha satisfeitas as condições (i), (ii), (iii) e sejam $x \in H_i$ e $y \in H_j$, com $i \neq j$. Considere o elemento comutador de x e y, $xyx^{-1}y^{-1}$. Temos

$$xyx^{-1}y^{-1} \in H_j, \text{ pois } H_j \lhd G, \text{ por } (i) \quad \text{e} \quad xyx^{-1}y^{-1} \in H_i, \text{ pois } H_i \lhd G, \text{ por } (i).$$

Logo

$$xyx^{-1}y^{-1} \in H_i \cap H_j \subseteq H_i \cap H_1 \cdots H_{i-1} H_{i+1} \cdots H_n = \{1_G\}, \text{ por } (iii).$$

Portanto, $xy = yx$ e a condição *(1)* é satisfeita.

Para mostrar a condição *(2)*, considere $g \in G$. Por (ii), existem $h_i \in H_i$, $i = 1, ..., n$, tais que $g = h_1 h_2 \cdots h_n$. Queremos mostrar que tais h_i são únicos. Suponha

$$h_1 h_2 \cdots h_n = k_1 k_2 \cdots k_n, \text{ com } k_i \in H_i, \quad i = 1, ..., n. \tag{1.1}$$

Multiplicando ambos os membros por k_1^{-1} à esquerda e por $h_n^{-1} \cdots h_2^{-1}$ à direita, temos

$$k_1^{-1} h_1 = k_2 \cdots k_n h_n^{-1} h_2^{-1}.$$

Como a condição *(1)* é satisfeita, podemos aplicá-la várias vezes, obtendo assim,

$$k_1^{-1}h_1 = k_2h_2^{-1}k_3h_3^{-1}\cdots k_nh_n^{-1}.$$

Logo, $k_1^{-1}h_1 \in H_1 \cap H_2\cdots H_n = \{1\}$ e, portanto, $h_1 = k_1$.

Procedendo de forma análoga, ou seja, multiplicando ambos os membros da equação (1.1) por $k_2^{-1}k_1^{-1}$ à esquerda e por $h_n^{-1}\cdots h_3^{-1}$ à direita, obtemos

$$k_2^{-1}h_2 = k_3\cdots k_nh_n^{-1}h_3^{-1}.$$

Aplicando a condição *(1)* repetidas vezes, temos

$$k_2^{-1}h_2 = k_3h_3^{-1}k_4h_4^{-1}\cdots k_nh_n^{-1}.$$

Logo, $k_2^{-1}h_2 \in H_2 \cap H_3\cdots H_n = \{1_G\}$ e, portanto, $h_2 = k_2$.

Continuando o processo de forma análoga, resulta que $h_i = k_i$, para todo $i = 1, \cdots, n$. Portanto a condição *(2)* é satisfeita.

Reciprocamente, suponha satisfeitas as condições *(1)* e *(2)*. Queremos mostrar que cada $H_i \lhd G$, ou seja, $gk_ig^{-1} \in H_i$, para todos $k_i \in H_i$, $g \in G$ e $i = 1, ..., n$. Por *(2)*, todo elemento $g \in G$ se escreve na forma $g = h_1h_2\cdots h_n$, com $h_j \in H_j$. Assim,

$$gk_ig^{-1} = h_1\cdots h_i\cdots h_nk_ih_1^{-1}\cdots h_i^{-1}\cdots h_n^{-1}.$$

Aplicando a condição *(1)* repetidas vezes resulta em

$$gk_ig^{-1} = h_1\cdots h_ik_ih_i^{-1}\cdots h_1^{-1}.$$

Como $h_ik_ih_i^{-1} \in H_i$, podemos novamente aplicar a condição *(1)* repetidas vezes, e obter

$$gk_ig^{-1} = h_ik_ih_i^{-1} \in H_i.$$

Logo H_i é normal em G, para todo $i = 1, \ldots, n$ e a condição (i) é satisfeita.

A condição (ii) é imediata por *(2)*.

Para mostrar a condição (iii), seja $x \in H_i \cap H_1\cdots H_{i-1}H_{i+1}\cdots H_n$. Por um lado $x \in H_1\cdots H_{i-1}H_{i+1}\cdots H_n$, daí

$$x = h_1h_2\cdots h_{i-1}h_{i+1}\cdots h_n, \text{ com } h_j \in H_j,\ j = 1, ..., i-1, i+1, ..., n.$$

Por outro, $x \in H_i$, logo, $x = h_i \in H_i$. Assim, $h_i = h_1h_2\cdots h_{i-1}h_{i+1}h_n$. multiplicando por h_i^{-1} ambos os membros e aplicando a condição *(2)*, obtemos

$$1_G = h_1h_2\cdots h_{i-1}h_i^{-1}h_{i+1}\cdots h_n.$$

Mas $1_G = 1_{G_1}1_{G_2}\cdots 1_{G_n}$, logo, pela unicidade *(2)*, $h_i = 1_{G_i}$, para todo $i = 1, \cdots, n$.

■

Proposição 1.5.15 *Sejam G um grupo e $H_1, H_2, \ldots, H_n$ subgrupos de G. Se G é o produto direto interno de $H_1, H_2, \ldots, H_n$, então $G \cong H_1 \times H_2 \times \cdots \times H_n$.*

Demonstração: Como $G = H_1H_2 \cdots H_n$, então $g = h_1h_2 \cdots h_n$ para todos $g \in G$, $h_i \in H_i$ e $i = 1, \ldots, n$. Defina uma função ψ como segue,

$$\begin{array}{rccl} \psi: & G & \longrightarrow & H_1 \times H_2 \times \cdots \times H_n \\ & g & \longmapsto & (h_1, h_2, \ldots, h_n). \end{array} .$$

Como todo elemento $g \in G$ se escreve de maneira única na forma $g = h_1h_2 \cdots h_n$, então a função ψ está bem definida.

A função ψ é um homomorfismo de grupos, pois, pela condição *(1)*, para todos $g, g' \in G$, com $g = h_1h_2 \cdots h_n$ e $g' = h'_1h'_2 \cdots h'_n$, onde $h_i \in H_i$, $h'_i \in H_i$, para todo $i = 1, ..., n$,

$$gg' = h_1h_2 \cdots h_nh'_1h'_2 \cdots h'_n = h_1h'_1h_2h'_2 \cdots h_nh'_n.$$

Daí,

$$\psi(gg') = (h_1h'_1, h_2h'_2, \ldots, h_nh'_n) = (h_1, h_2, \ldots, h_n)(h'_1, h'_2, \ldots, h'_n) = \psi(g)\psi(g').$$

Além disso, ψ é monomorfismo, pois

$$\begin{array}{rcl} \ker(\psi) & = & \{g \in G \mid \psi(g) = 1_{H_1 \times \cdots \times H_n}\} \\ & = & \{g \in G \mid (h_1, h_2, \ldots, h_n) = (1_{G_1}, 1_{G_2}, \ldots, 1_{G_n})\} \\ & = & \{1_G\} \end{array}$$

e ψ é epimorfismo, pois, para todo $y \in H_1 \times H_2 \times \cdots \times H_n$, y se escreve na forma $y = (h_1, h_2, \ldots, h_n)$, com $h_i \in H_i$ e $i = 1, \ldots, n$. Daí, tome $x = h_1h_2 \cdots h_n \in G$ e $\psi(x) = y$. Portanto ψ é um isomorfismo de grupos. ∎

Capítulo 2

Grupos Abelianos Finitos

Como uma aplicação dos resultados do Capítulo 1, provamos que todo grupo abeliano finito é um produto direto de seus p-subgrupos de Sylow. Além disso, mostramos também vários resultados a respeito de p-grupos abelianos finitos que são utilizados para a demonstração do Teorema Fundamental dos Grupos Abelianos Finitos, nosso principal objetivo neste capítulo. Além disso, determinamos, a menos de isomorfismos, todos os grupos abelianos de uma dada ordem. A principal referência para este capítulo é [6].

2.1 Teorema Fundamental dos Grupos Abelianos Finitos

O Teorema Fundamental dos Grupos Abelianos Finitos é de grande importância para o desenvolvimento deste trabalho, pois estabelece que todo grupo abeliano finito pode ser escrito como produto direto de subgrupos cíclicos de ordem prima.

Proposição 2.1.1 *Se G é um grupo abeliano finito, então G é um produto direto interno de seus p-subgrupos de Sylow e, portanto, G é isomorfo ao produto direto de seus p-subgrupos de Sylow.*

Demonstração: Seja G um grupo abeliano finito, digamos de ordem $n \geq 1$. Pelo Teorema Fundamental da Aritmética, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, onde $p_1, p_2, \ldots, p_k$ são números primos distintos e essa decomposição é única, a menos da ordem dos fatores. Seja H_i o p_i-subgrupo de Sylow de G, com $|H_i| = p_i^{\alpha_i}$, $i = i, \ldots, n$. Tais subgrupos existem pelo 1º Teorema de Sylow. Queremos mostrar que G é produto direto interno de $H_1, H_2, \ldots, H_k$, ou seja, que todas as condições da Proposição 1.5.14 são satisfeitas. Como G é abeliano, a condição (i) é satisfeita para cada H_i.

Agora, queremos mostrar que $G = H_1H_2\cdots H_k$. Pelas propriedades de produtos de grupos, H_1H_2 é subgrupo de G, pois $H_2 \lhd G$. Além disso,

$$|H_1H_2| = |H_1||H_2| = p_1^{\alpha_1}p_2^{\alpha_2}, \quad \text{pois} \quad H_1 \cap H_2 = \{1_G\}.$$

Novamente, $(H_1H_2)H_3$ é subgrupo de G, pois $H_3 \lhd G$. Temos também

$$|(H_1H_2)H_3| = |H_1||H_2||H_3| = p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}, \quad \text{pois } H_1H_2 \cap H_3 = \{1_G\}.$$

Continuando de forma análoga, $H_1H_2\cdots H_k$ é subgrupo de G e

$$|H_1H_2\cdots H_k| = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}.$$

Logo $G = H_1H_2\cdots H_k$ e a condição (ii) é satisfeita.

Para mostrar a condição (iii), seja $x \in H_i \cap H_1\cdots H_{i-1}H_{i+1}\cdots H_n$. Assim,

$$o(x) \mid p_i^{\alpha_i} \quad \text{e} \quad o(x) \mid p_1^{\alpha_1}\cdots p_{i-1}^{\alpha_{i-1}}, p_{i+1}^{\alpha_{i+1}}\cdots p_k^{\alpha_k} = Y.$$

Logo $o(x) = mdc\{p_i^{\alpha_i}, Y\}$. Como os p_i, com $i = 1, \ldots, n$, são primos distintos, então $o(x) = 1$ e, assim,

$$H_i \cap H_1\cdots H_{i-1}H_{i+1}\cdots H_n = \{1_G\}.$$

Portanto, pela Proposição 1.5.15, G é isomorfo ao produto direto de seus p-subgrupos de Sylow. ∎

Lema 2.1.2 *Seja G um p-grupo abeliano finito e $g \in G$ um elemento de ordem máxima em G. Então $\langle g\rangle$ é um fator direto de G, isto é, existe $M \lhd G$ tal que $G = M \times \langle g\rangle$.*

Demonstração: Sejam $|G| = p^\alpha$ e $g \in G$ um elemento de ordem máxima em G. Se $o(g) = p^\alpha$, então $M = \{1_G\}$ e o resultado segue.

Se $o(g) < |G|$, escolha M maximal de modo que $M \cap \langle g\rangle = \{1_G\}$. Se $M \cdot \langle g\rangle = G$, então $G = M \times \langle g\rangle$ e temos o resultado.

Suponha $M \cdot \langle g\rangle \neq G$. Como $M \lhd G$, então $M \cdot \langle g\rangle \neq G$ é um subgrupo normal de G, assim $\dfrac{G}{M \cdot \langle g\rangle}$ é um p-grupo não trivial. Pelo Teorema de Cauchy, existe $\bar{x} \in \dfrac{G}{M \cdot \langle g\rangle}$ tal que $o(\bar{x}) = p$ e $x \in G - M \cdot \langle g\rangle$. Daí, $\bar{x}^p = \bar{1}$, ou seja, $x^p \in M \cdot \langle g\rangle$. Assim, existem $y \in M$ e $\beta \in \mathbb{Z}$ tais que $x^p = yg^\beta$. Como p^α é a ordem máxima dos elementos de G, temos

$$1_g = x^{p^\alpha} = (x^p)^{p^{\alpha-1}} = (y)^{p^{\alpha-1}} \cdot (g^\beta)^{p^{\alpha-1}}$$

e, com isso, $g^{\beta p^{\alpha-1}} \in M \cap \langle g\rangle = \{1_G\}$. Logo $g^{\beta p^{\alpha-1}} = 1_G$ e, assim, $p \mid \beta$, isto é $\beta = p \cdot \gamma$, para algum $\gamma \in \mathbb{Z}$. Dessa forma, $x^p = yg^{p\gamma}$ e $y = (xg^{-\gamma})^p \in M$, mas $xg^{-\gamma} \notin M$. Assim, $\langle xg^{-\gamma}, M\rangle \cap \langle g\rangle \neq \{1_G\}$, senão contradiz a maximalidade de M. Logo existem $\delta, \varepsilon \in \mathbb{Z}$ e $y' \in M$ tais que $g^\varepsilon = (xg^{-\gamma})^\delta y'$, ou seja, $x^\delta = (y')^{-1}g^{\varepsilon+\gamma\delta} \in M \cdot \langle g\rangle$. Além disso $p \mid \delta$,

pois, se $p \nmid \delta$, então $\text{mdc}\{p, \delta\} = 1$ e pelo Teorema de Bézout, existiriam $a, b \in \mathbb{Z}$ tais que $ap + b\delta = 1$ e assim

$$x = x^{ap+b\delta} = (x^p)^a (x^\delta)^b \in M \cdot \langle g \rangle.$$

Mas isso contradiz o fato de $x \in G - M \cdot \langle g \rangle$. Então $(xg^{-\gamma})^\delta = ((xg^{-\gamma})^p)^s \in M$, para algum $s \in \mathbb{Z}$, e como $y' \in M$, temos $g^\varepsilon \in M$.

Logo existe um elemento, não trivial, $g^\varepsilon \in M \cdot \langle g \rangle$, mas isto contradiz a escolha de M. Portanto, $G = M \cdot \langle g \rangle$ e, consequentemente, $G = M \times \langle g \rangle$.

■

Teorema 2.1.3 *Todo p-grupo abeliano finito G é o produto direto de uma família finita de subgrupos cíclicos.*

Demonstração: Seja G um grupo de ordem p^α, $\alpha \geq 1$ e $\alpha \in \mathbb{Z}$. Vamos fazer a demonstração por indução sobre α.

Se $\alpha = 1$, então $|G| = p$. Daí, G é cíclico e nada temos a fazer. Suponha $\alpha > 1$ e o teorema válido para todo p-grupo abeliano finito de ordem p^t, com $1 \leq t < \alpha$ e seja $g \in G$ um elemento de ordem máxima p^k. Se $k = \alpha$, então G é cíclico e, neste caso, nada temos a demonstrar. Se $k < \alpha$, o Lema 2.1.2 nos mostra que $G = M \times \langle g \rangle$, com $M \neq \{1_G\}$ e $M \neq G$. Logo, pelo Teorema de Lagrange, $|M| = p^t$, com $1 \leq t < \alpha$. Por hipótese de indução, segue-se que M é produto direto de uma família finita de subgrupos cíclicos. Portanto, G é produto direto de uma família finita de subgrupos cíclicos.

■

O Teorema 2.1.3 nos diz que se H_p é um p-grupo abeliano finito de ordem p^α, então existem inteiros $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_r > 0$, tais que

$$H_p = C_{p^{\beta_1}} \times C_{p^{\beta_2}} \times \cdots \times C_{p^{\beta_r}},$$

onde $C_{p^{\beta_i}}$ é um grupo cíclico de ordem p^{β_i}. Além disso, os números $\beta_1, \beta_2, \ldots, \beta_r$ são ditos invariantes do p-grupo H_p e são tais que $\beta_1 + \beta_2 + \cdots + \beta_r = \alpha$.

Exemplo 2.1.4 *Seja*

$$G = \mathbb{Z}_4 \times \mathbb{Z}_4 = \left\{ \begin{array}{cccc} (\bar{0},\bar{0}) & (\bar{0},\bar{1}) & (\bar{0},\bar{2}) & (\bar{0},\bar{3}) \\ (\bar{1},\bar{0}) & (\bar{1},\bar{1}) & (\bar{1},\bar{2}) & (\bar{1},\bar{3}) \\ (\bar{2},\bar{0}) & (\bar{2},\bar{1}) & (\bar{2},\bar{2}) & (\bar{2},\bar{3}) \\ (\bar{3},\bar{0}) & (\bar{3},\bar{1}) & (\bar{3},\bar{2}) & (\bar{3},\bar{3}) \end{array} \right\}$$

Considere

$$H_1 = \langle (\bar{0},\bar{1}) \rangle = \{(\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{0},\bar{2}), (\bar{0},\bar{3})\} \quad e \quad H_2 = \langle (\bar{1},\bar{0}) \rangle = \{(\bar{0},\bar{0}), (\bar{1},\bar{0}), (\bar{2},\bar{0}), (\bar{3},\bar{0})\}.$$

Note que H_1 e H_2 são subgrupos cíclicos de G e $G = H_1 \times H_2$. Considere agora

$$H_1' = \langle(\bar{1}, \bar{2})\rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{2}), (\bar{2}, \bar{0}), (\bar{3}, \bar{2})\} \quad e \quad H_2' = \langle(\bar{1}, \bar{1})\rangle = \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1}), (\bar{2}, \bar{2}), (\bar{3}, \bar{3})\}.$$

Observe que H_1' e H_2' também são subgrupos cíclicos de G e $G = H_1' \times H_2'$.

Como H_1, H_2, H_1', H_2' são dois a dois distintos, obtivemos uma decomposição de G como produto direto de subgrupos cíclicos de duas maneiras diferentes.

Este exemplo ilustra que não temos unicidade na decomposição do Teorema 2.1.3. Observe, no entanto, que o número de parcelas destas decomposições são iguais. Além disso, $o(H_i) = o(H_i')$, para $i = 1, 2$.

Tendo em vista generalizar este resultado, apresentamos inicialmente os seguintes lemas:

Lema 2.1.5 *Se $H = \langle a\rangle$ é um grupo cíclico de ordem p^α, então o conjunto*

$$H_1 = \{x \in H \mid x^p = 1_H\}$$

é um subgrupo de H de ordem p.

Demonstração: É claro que H_1 é não vazio, pois $1_H \in H_1$. Sejam $x, y \in H_1$. Assim $x^p = 1_H$ e $y^p = 1_H$, daí

$$y^{-p}y^p = y^{-p} \Rightarrow y^{-p} = 1_H \Rightarrow (y^{-1})^p = 1_H \Rightarrow y^{-1} \in H_1.$$

Logo, $(xy^{-1})^p = x^p y^{-p} = 1_H$ e, assim, $xy^{-1} \in H_1$. Portanto, H_1 é um subgrupo de H.

Agora, os elementos $(a^i)^{p^{\alpha-1}}$, com $i = 1, \ldots, p$, pertencem a H_1, pois

$$((a^i)^{p^{\alpha-1}})^p = ((a^i)^{p^\alpha}) = (a^{p^\alpha})^i = 1_H^i = 1_H.$$

Além disso, os elementos $(a^i)^{p^{\alpha-1}}$, com $i = 1, \ldots, p$, são dois a dois distintos.

Por outro lado, seja $x = a^j$, para $1 \leq j \leq p^{\alpha-1}$, um elemento qualquer de H e suponhamos $x \in H_1$. Assim $(a^j)^p = 1_H$ e daí $p^\alpha \mid (pj)$, ou seja, $p^{\alpha-1} \mid j$. Logo $j = ip^{\alpha-1}$, com $1 \leq i \leq p-1$. Portanto, $|H_1| = p$. ∎

Lema 2.1.6 *Se um p-grupo abeliano G é o produto direto de uma família $(H_i)_{1\leq i\leq r}$ de subgrupos cíclicos de G, então:*

(i) O conjunto $G_p = \{x \in G \mid x^p = 1_G\}$ é um subgrupo de G de ordem p^r.

(ii) O conjunto $G^{(p)} = \{y^p \mid y \in G\}$ é um subgrupo de G.

(iii) O conjunto $(H_i)^{(p)} = \{z^p \mid z \in H_i\}$ *é um subgrupo cíclico de* $G^{(p)}$*, para todo* $i = 1, \ldots, r$.

Demonstração:

(i) O conjunto G_p é não vazio, pois $1_G \in G$. Se $x_1,\ x_2 \in G_p$, então $x_1^p = 1_G$ e $x_2^p = 1_G$ e daí $x_2^{-1} \in G_p$. Além disso,

$$(x_1 x_2^{-1})^p = x_1^p x_2^{-p} = 1_G, \text{ ou seja, } x_1 x_2^{-1} \in G_p.$$

Portanto, G_p é um subgrupo de G.

Agora, um elemento $x \in G$ pode ser representado de modo único sob a forma

$$x = x_1\, x_2 \cdots x_r, \text{ onde } x_i \in H_i,\ i = 1, \ldots, r.$$

Agora,

$$x \in G_p \Leftrightarrow x^p = 1_G \Leftrightarrow (x_1\, x_2 \cdots x_r)^p = 1_G \Leftrightarrow x_1^p\, x_2^p \cdots x_r^p = 1_G.$$

Como $x_i^p \in H_i$ e $G = H_1 \times H_2 \times \cdots \times H_r$, então $x_1^p\, x_2^p \cdots x_r^p = 1_G$ se, e somente se, $x_i^p = 1_G$, para todo $i = 1, ..., r$. Assim, $x \in G_p$ se, e somente se, $x_i \in H_i$, para todo $i = 1, \ldots, r$. Pelo Lema 2.1.5, $|H_i| = p$ e, portanto, $|G_p| = p^r$.

(ii) É claro que $G^{(p)}$ é não vazio, pois $1_G \in G^{(p)}$. Sejam então $x^p, y^p \in G^{(p)}$, com $x, y \in G$. Como $y^{-1} \in G$, então $(y^{-p}) \in G^{(p)}$. Daí $x^p \cdot y^{-p} = (x \cdot y^{-1})^p \in G^{(p)}$. Logo $G^{(p)}$ é um subgrupo de G.

(iii) De modo análogo ao que foi feito em (ii) prova-se que $(H_i)^{(p)}$ é um subgrupo de $G^{(p)}$.

Para mostrar que $(H_i)^{(p)}$ é cíclico, vamos mostrar que $(H_i)^{(p)} = \langle a_i^p \rangle$, onde $H_i = \langle a_i \rangle$. Seja $t^p \in (H_i)^{(p)}$ com $t = a_i^\gamma$. Então $t^p = (a_i^\gamma)^p = (a_i^p)^\gamma \in \langle a_i^p \rangle$ e, assim, $(H_i)^{(p)} \subseteq \langle a_i^p \rangle$. A outra inclusão é óbvia e isto prova a igualdade. ∎

Lema 2.1.7 *Sejam* $m, n, k \in \mathbb{Z}$ *com* $mk = n$*. Então*

$$m\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \overline{m}, \overline{2m}, \ldots, \overline{(k-1)m}\} \cong \mathbb{Z}_k.$$

Demonstração: Sejam

$$G = \mathbb{Z}_n \cong \frac{\mathbb{Z}}{n\mathbb{Z}} \quad \text{e} \quad H \cong m\mathbb{Z}_n = \frac{m\mathbb{Z}}{n\mathbb{Z}}.$$

Assim, $n\mathbb{Z}$ é um subgrupo de $m\mathbb{Z}$ se, e somente se, existe $k \in \mathbb{Z}$ tal que $mk = n$. Com essa condição, pelo 3º Teorema do Isomorfismo, temos

$$\frac{G}{H} \cong \frac{\dfrac{\mathbb{Z}}{n\mathbb{Z}}}{\dfrac{m\mathbb{Z}}{n\mathbb{Z}}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} = \mathbb{Z}_m.$$

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

Teorema 2.1.8 *Se um p-grupo abeliano G é o produto direto de duas famílias distintas $\{H_i\}_{1\leq i\leq r}$ e $\{H'_j\}_{1\leq j\leq s}$ de subgrupos cíclicos de G e se $H_i \neq \{1_{H_i}\}$ para $i = 1, 2, \ldots, r$ e $H'_j \neq \{1_{H'_j}\}$, para $j = 1, 2, \ldots, s$, então $r = s$ e, reordenando os índices, se necessário, temos $|H_i| = |H'_i|$, para $i = 1, 2, \ldots, r$.*

Demonstração:

Seja G um grupo de ordem $|G| = p^\alpha$. Vamos fazer a prova por indução finita sobre o número natural α.

Se $\alpha = 1$, então G é cíclico e neste caso, $r = s = 1$ e $H_1 = H'_1 = G$.

Suponha $\alpha > 1$ e o teorema verdadeiro para todo p-grupo abeliano de ordem $p^{\alpha'}$, onde $1 \leq \alpha' < \alpha$. Reordenando os conjuntos $\{H_i\}_{1\leq i\leq r}$ e $\{H'_j\}_{1\leq j\leq s}$, se necessário, coloquemos

$$H_i = \langle a_i\rangle \text{ e } |H_i| = p^{e_i}, \text{ com } e_1 \geq e_2 \geq \cdots \geq e_r \geq 1.$$

$$H'_j = \langle b_j\rangle \text{ e } |H_i| = p^{f_i}, \text{ com } f_1 \geq f_2 \geq \cdots \geq f_r \geq 1.$$

O Lema 2.1.6 (i), aplicado à família $\{H_i\}_{1\leq i\leq r}$, nos diz que $|G_p| = p^r$ e trocando a família $\{H_i\}_{1\leq i\leq r}$ pela família $\{H'_j\}_{1\leq j\leq s}$, obtemos $|G| = p^s$. Logo $r = s$.

Agora, se $e_1 = 1$, então $|H_i| = p$, para todo $i = 1, \ldots, r$. Como $G = H_1 \times H_2 \times \cdots \times H_r$, segue-se que todo elemento diferente do neutro de G tem ordem p e daí $G = G_p$. Por outro lado, suponha $f_1 > 1$, pelo 1º Teorema de Sylow, existe um elemento em $H'_j \subseteq G$ de ordem maior que do que p e isso é absurdo. Logo, $e_i = f_j$, para todo $i = 1, \ldots, r$ e, neste caso, o teorema está provado.

Suponha que exista $e_i > 1$ e indiquemos por m, com $1 \leq m \leq r$, o maior índice i tal que $e_i > 1$, ou seja , $e_\gamma = 1$, para todo inteiro $m < \gamma \leq r$. Neste caso, devemos ter $f_1 > 1$, pois, caso $f_1 = 1$, teríamos $f_j = 1$, para todo $j = 1, \ldots, s$ e assim, teríamos $e_i = 1$, para todo $i = 1, \ldots, r$, contradizendo o fato de $e_i > 1$. Logo $f_1 > 1$ e existe um índice maior n, com $1 < n \leq r = s$ tal que $f_\delta = 1$, para todo inteiro $n < \delta \leq s = r$.

Afirmação 2.1.9 *Para o grupo G considerado acima, temos*

$$G^{(p)} = (H_1)^{(p)} \times (H_2)^{(p)} \times \cdots \times (H_m)^{(p)} \quad e \quad G^{(p)} = (H'_1)^{(p)} \times (H'_2)^{(p)} \times \cdots \times (H'_n)^{(p)}.$$

De fato, pelo Lema 2.1.6 (iii), para cada $i = 1, \ldots, m$, $(H_i)^{(p)}$ é um subgrupo de $G^{(p)}$. Assim, $(H_1)^{(p)}\,(H_2)^{(p)} \cdots (H_m)^{(p)} \leq G^{(p)}$.

Agora, se $x \in G^{(p)}$, então $x = y^p$, para algum $y \in G$. Além disso, y pode ser escrito, de modo único, sob a forma $y = y_1\, y_2 \cdots y_r$, com $y_i \in H_i$. Como $|H_\gamma| = p^{e_\gamma} = p$, pois $e_\gamma = 1$, para $m < \gamma \leq r$, então $y_\gamma^p = 1_{H_\gamma}$, para $m < \gamma \leq r$. Assim,

$$x = y_1^p\, y_2^p \cdots y_m^p \in (H_1)^{(p)}\,(H_2)^{(p)} \cdots (H_m)^{(p)}.$$

Logo, $G^{(p)} = (H_1)^{(p)}\,(H_2)^{(p)} \cdots (H_m)^{(p)}$ *e como* $(H_i)^{(p)} \subseteq H_i$*, tal produto é direto. Portanto,*

$$G^{(p)} = (H_1)^{(p)} \times (H_2)^{(p)} \times \cdots \times (H_m)^{(p)}.$$

A outra parte da afirmação pode ser provada de forma análoga.

Conclui-se daí que

$$|G^{(p)}| = |(H_1)^{(p)}|\,|(H_2)^{(p)}| \cdots |(H_m)^{(p)}| \;=\; |(H_1')^{(p)}|\,|(H_2')^{(p)}| \cdots |(H_n')^{(p)}|.$$

Como H_i é um subgrupo de ordem p^{e_i}, então $H_i \cong \mathbb{Z}_{p^{e_i}}$. A restrição desse isomorfismo ao subgrupo cíclico $(H_i)^{(p)}$ de H_i nos diz que $(H_i)^{(p)} \cong p\mathbb{Z}_{p^{e_i}} \cong \mathbb{Z}_{p^{e_i-1}}$ e, pelo Lema 2.1.7, $|(H_i)^{(p)}| = p^{e_i-1}$, para todo $i = 1, \ldots, r$.

Analogamente temos $|(H_j')^{(p)}| = p^{f_j-1}$, para todo $j = 1, \ldots, r$. Daí

$$|G^{(p)}| = (e_1 - 1) + (e_2 - 1) + \cdots + (e_m - 1) \;=\; (f_1 - 1) + (f_2 - 1) + \cdots + (f_n - 1) < \alpha.$$

Aplicando a hipótese de indução em

$$G^{(p)} = (H_1)^{(p)} \times (H_2)^{(p)} \times \cdots \times (H_m)^{(p)} \;=\; (H_1')^{(p)} \times (H_2')^{(p)} \times \cdots \times (H_n')^{(p)},$$

resulta em $m = n$ e $|H_i| = |H_i'|$, para $i = 1, \ldots, m$. Agora, como $e_\gamma = 1$, para $m < \gamma \leq r$ e $f_\delta = 1$, para $m = n < \delta \leq r = s$, então

$$|H_\gamma| = p^{e_\gamma} = 1 = p^{f_\delta} = |H_\delta'|.$$

Portanto $|H_i| = |H_1'|$, para todo $i = 1, \ldots, r$. ∎

Pela Proposição 2.1.1, todo grupo abeliano finito G é o produto direto de seus p-subgrupos de Sylow. Pelo Teorema 2.1.3, todo p-grupo abeliano é o produto direto de uma família finita de seus subgrupos cíclicos. Além disso, pelo Teorema 2.1.8, o número de parcelas desta decomposição, assim como suas ordens, são determinadas de modo único, a menos da ordem das parcelas, pelo grupo G. Isto prova o seguinte resultado.

Teorema 2.1.10 (Teorema Fundamental dos Grupos Abelianos Finitos)

Todo grupo abeliano finito G *é o produto direto de uma família* $\{G_i\}_{1 \leq i \leq r}$ *de subgrupos cíclicos. Além disso, o número destes subgrupos cíclicos e suas ordens são determinadas de modo único pelo grupo* G*.*

Queremos agora determinar todos os grupos abelianos de uma dada ordem, para isto, enunciamos o seguinte

Lema 2.1.11 *Sejam* G *e* G' *dois grupos abelianos finitos tais que* G *é o produto direto de uma família* $\{G_i\}_{1 \leq i \leq r}$ *de subgrupos cíclicos e* G' *é o produto direto de uma família* $\{G_i'\}_{1 \leq i \leq r}$*) de subgrupos cíclicos. Nestas condições, se* $|G_i| = |G_i'|$*, para* $i = 1, \ldots, r$*, então* $G \cong G'$*.*

Demonstração: Por hipótese, G_i e G_i' são grupos cíclicos de mesma ordem, logo existe um isomorfismo

$$\begin{array}{rccc} h_i: & G_i & \longrightarrow & G_i' \\ & x_i & \longmapsto & h_i(x_i) \end{array}$$

para cada $i = 1, \ldots, r$.

Agora, como $G = G_1 \times G_2 \times \cdots \times G_r$, um elemento $x \in G$ se escreve de modo único na forma $x = (x_1, x_2, \ldots, x_n)$ com $x_i \in G_i$. Considere, assim, a aplicação $h : G \longrightarrow G'$ definida por

$$h(x) = (h_1(x_1),\, h_2(x_2), \ldots, h_r(x_r)),$$

onde $x = (x_1, x_2, \ldots, x_n)$, com $x_i \in G_i$. Tal função está bem definida, pois, para cada $i = 1, \ldots, r$, a função $h_i : G_i \longrightarrow G_i'$ está bem definida.

Sejam $x = (x_1,\, x_2,\, \ldots,\, x_r)$ e $y = (y_1,\, y_2,\, \ldots,\, y_r) \in G$. Então

$$\begin{aligned} h(xy) &= (h_1(x_1y_1),\, h_2(x_2y_2),\, \ldots,\, h_r(x_ry_r)) \\ &= (h_1(x_1)\, h_1(y_1),\, h_2(x_2)\, h_2(y_2),\, \ldots,\, h_r(x_r)\, h_r(y_r)) \\ &= (h_1(x_1),\, h_2(x_2),\, \ldots,\, h_r(x_r))\, (h_1(y_1),\, h_2(y_2),\, \ldots,\, h_r(y_r)) \\ &= h(x)\, h(y). \end{aligned}$$

Logo, h é um homomorfismo de grupos. Além disso, h é injetora, pois

$$\begin{aligned} \ker(h) &= \{x \in G \mid h(x) = 1_{G'}\} \\ &= \{x \in G \mid (h_1(x_1,)\, h_2(x_2),\, \ldots,\, h_r(x_r)) = (1_{G_1'},\, 1_{G_2'},\, \ldots,\, 1_{G_r'})\} \\ &= \{x \in G \mid x_i = 1_{G_i},\ \text{para todo } i = 1, \ldots, r\} \\ &= \{1_G\}. \end{aligned}$$

Ainda, h é sobrejetora, pois G e G' tem a mesma ordem. Logo h é um isomorfismo de grupos e, portanto, $G \cong G'$. ∎

2.2 O Número de Grupos Abelianos não Isomorfos de uma Dada Ordem

Nosso objetivo aqui é determinar, a menos de isomorfismos, todos os grupos abelianos finitos de uma dada ordem. Para isto, introduziremos o conceito de partição do número $k \geq 1$.

Definição 2.2.1 *Chama se* ***partição*** *de k a toda n-upla $(k_1, k_2, \ldots, k_n)$ de números naturais não nulos tal que $k_1 \geq k_2 \geq \cdots \geq k_n$ e $k = \sum_{i=1}^{n} k_i$. Indicamos por $P(k)$ o* ***número de partições*** *de k.*

Seja $n > 1$ um número inteiro. Considerando a decomposição de n em fatores primos distintos, temos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Daí, temos o seguinte

Corolário 2.2.2 *Existem exatamente* $P(\alpha_1) P(\alpha_2) \cdots P(\alpha_r)$ *grupos abelianos não isomorfos de ordem* n*, onde* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

Demonstração: O Lema 2.1.11 nos mostra que se dois grupos abelianos de mesma ordem têm o mesmo tipo de decomposição, então eles são isomorfos. Assim, o número de grupos abelianos (não isomorfos) de ordem n é o número de decomposições diferentes, como produto direto de seus subgrupos cíclicos que tal grupo pode admitir, isto é, o número de grupos abelianos (não isomorfos) de ordem n é $P(\alpha_1) P(\alpha_2) \cdots P(\alpha_r)$, onde $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. ■

Exemplo 2.2.3 *Vamos determinar todos os grupos abelianos não isomorfos de ordem* 1200.

Decompondo a ordem de G *em fatores primos, obtemos,* $|G| = 1200 = 2^4 \cdot 3^1 \cdot 5^2$. *Vamos então determinar as partições dos expoentes* 4, 1 *e* 2. *Note que,*

$$4 = \begin{cases} 1111 \\ 211 \\ 22 \\ 31 \\ 4 \end{cases}, \quad 1 = \{1 \quad , \quad 2 = \begin{cases} 11 \\ 2 \end{cases} .$$

Logo, existem exatamente $5 \cdot 1 \cdot 2 = 10$ *grupos abelianos, não isomorfos, de ordem* 1200. *A saber:*

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$

$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$

$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

$\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$

$\mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

$\mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$

$\mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$

$\mathbb{Z}_{2^4} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2}$.

Capítulo 3

Automorfismos de Grupos Abelianos Finitos

Neste capítulo fazemos uma caracterização do grupo de automorfismos $Aut(G)$ de um grupo abeliano finito G e apresentamos duas fórmulas para o número de elementos de $Aut(G)$. As principais referências para este capítulo são, o artigo *Automorphisms of finite abelian Groups* de Christopher J. Hillar e Darren L. Rhea [2], que caracteriza o grupo de automorfismos $Aut(G)$ de uma forma mais acessível e moderna e a tese de doutorado de Heinrich Kuhn [5], intitulada *Endomorphismem Abelscher p-Gruppen*, que trata também de automorfismos de p-grupos abelianos.

Com o propósito de fazer tal caracterização, descrevemos o anel de endomorfismos de H_p, onde H_p é um p-grupo abeliano finito e identificamos as unidades $Aut(H_p) \subset End(H_p)$. Através desta descrição o anel de endomorfismos $End(H_p)$ pode ser visto como um quociente de um subanel das matrizes $M_n(\mathbb{Z})$. Como consequência desta investigação, apresentamos prontamente uma fómula para o número de elementos de $Aut(G)$, para qualquer grupo abeliano finito G. A outra fórmula segue o desenvolvimento feito por Heinrich Kuhn em sua tese de doutorado [5] e utiliza apenas certos subgrupos característicos do grupo G.

3.1 Automorfismos de Produtos Diretos

Seja G um grupo abeliano finito. Pelo Teorema 2.1.10, G é isomorfo ao produto direto de grupos da forma

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

onde p é um número primo e $1 \leq e_1 \leq \cdots \leq e_n$ são inteiros positivos.

O seguinte lema nos diz que é suficiente trabalhar com os grupos do tipo H_p.

Lema 3.1.1 *Sejam H e K dois grupos abelianos com ordens relativamente primas. Então*

$$Aut(H) \times Aut(K) \cong Aut(H \times K).$$

Demonstração: Sejam $\alpha \in Aut(H),\ \beta \in Aut(K),\ h \in H,\ k \in K$. É fácil verificar que a função

$$\begin{array}{rccc} \phi_{\alpha,\beta}: & H \times K & \longrightarrow & H \times K \\ & (h,k) & \longmapsto & (\alpha(h), \beta(k)) \end{array}$$

é um automorfismo de $H \times K$. Afirmamos que a seguinte função

$$\begin{array}{rccc} \phi: & Aut(H) \times Aut(K) & \longrightarrow & Aut(H \times K) \\ & (\alpha, \beta) & \longmapsto & \phi_{\alpha,\beta} \end{array}$$

é um isomorfismo de grupos. De fato, para todos $\alpha_1, \alpha_2 \in Aut(H),\ \beta_1, \beta_2 \in Aut(K)$, $h \in H$, $k \in K$, temos

$$\begin{aligned} \phi((\alpha_1,\beta_1)(\alpha_2,\beta_2))(h,k) &= \phi(\alpha_1\alpha_2, \beta_1\beta_2)(h,k) \\ &= \phi_{\alpha_1\alpha_2,\beta_1\beta_2}(h,k) \\ &= (\alpha_1\alpha_2(h), \beta_1\beta_2(k)) \\ &= \phi_{\alpha_1,\beta_1}(\alpha_2(h), \beta_2(k)) \\ &= (\phi_{\alpha_1,\beta_1} \circ \phi_{\alpha_2,\beta_2})(h,k) \\ &= (\phi(\alpha_1,\beta_1) \circ \phi(\alpha_2,\beta_2))(h,k). \end{aligned}$$

Logo ϕ é um homomorfismo de grupos.

Para mostrar que ϕ é injetora, suponha $(\alpha, \beta) \in \ker(\phi)$. Então $\phi(\alpha, \beta) = Id_{H\times K}$, ou seja,

$$\begin{aligned} & \phi_{\alpha,\beta}(h,k) = (h,k), \text{ para todo } (h,k) \in H \times K \\ \Rightarrow\ & (\alpha(h), \beta(k)) = (h,k), \text{ para todo } (h,k) \in H \times K \\ \Rightarrow\ & \begin{cases} \alpha(h) = h, \text{ para todo } h \in H \\ \beta(k) = k, \text{ para todo } k \in K \end{cases} \\ \Rightarrow\ & \begin{cases} \alpha = Id_H \\ \beta = Id_K \end{cases} \\ \Rightarrow\ & \ker(\phi) = \{(Id_H, Id_K)\} \end{aligned}$$

e assim ϕ é injetiva.

Para provar a sobrejetividade, sejam $|H| = m$ e $|K| = n$, com $\text{mdc}(m,n) = 1$. Dado $\omega \in Aut(H \times K)$, queremos construir automorfismos $\omega_H \in Aut(H)$ e $\omega_K \in Aut(K)$ tais que

$$\phi(\omega_H, \omega_K) = \omega. \tag{3.1}$$

Fixe $\omega \in Aut(H \times K)$ e considere as projeções canônicas

$$\begin{array}{rccc} \pi_H: & H \times K & \longrightarrow & H \\ & (h,k) & \longmapsto & h \end{array} \quad \text{e} \quad \begin{array}{rccc} \pi_K: & H \times K & \longrightarrow & K \\ & (h,k) & \longmapsto & k \end{array}.$$

Assim, temos um homomorfismo $\gamma : K \to H$ dado pela composição dos seguintes homomorfismos:

$$\begin{array}{ccccccc} K & \overset{i}{\hookrightarrow} & H \times K & \overset{\omega}{\longrightarrow} & H \times K & \overset{\pi_H}{\longrightarrow} & H \\ k & \longmapsto & (1_H, k) & \longmapsto & \omega(1_H, k) & \longmapsto & \pi_H(\omega(1_H, k)), \end{array}$$

ou seja, $\gamma(k) = \pi_H(\omega(1_H, K))$. Pelo 1º Teorema do Isomorfismo,

$$\frac{K}{\ker(\gamma)} \cong \mathrm{Im}(\gamma)$$

e assim $[K : \ker(\gamma)]$ divide $|H| = m$. Por outro lado, como $\ker(\gamma) \leq K$, pelo Teorema de Lagrange, $[K : \ker(\gamma)]$ também divide $|K| = n$. Como $\mathrm{mdc}(m, n) = 1$, então $[K : \ker(\gamma)] = 1$, o que implica $K = \ker(\gamma)$. Logo, $\gamma(k) = 1_H$ para todo $k \in K$. Portanto, γ é o homomorfismo trivial.

Analogamente, definindo o homomorfismo $\delta : H \to K$ por

$$\begin{array}{ccccccc} H & \overset{i}{\hookrightarrow} & H \times K & \overset{\omega}{\longrightarrow} & H \times K & \overset{\pi_K}{\longrightarrow} & K \\ h & \longmapsto & (h, 1_K) & \longmapsto & \omega(h, 1_K) & \longmapsto & \pi_K(\omega(h, 1_K)), \end{array}$$

isto é, $\delta(h) = \pi_K(\omega(h, 1_K))$ tem-se também que δ é o homomorfismo trivial.

Finalmente, defina os endomorfismos ω_H e ω_K de H e K respectivamente por:

$$\begin{array}{rccc} \omega_H: & H & \longrightarrow & H \\ & h & \longmapsto & \pi_H(\omega(h, 1_K)) \end{array} \quad \text{e} \quad \begin{array}{rccc} \omega_K: & K & \longrightarrow & K \\ & k & \longmapsto & \pi_K(\omega(1_H, k)). \end{array}$$

Observe que se $\omega(h, k) = (h', k')$, então $\pi_H(\omega(h, k)) = h'$ e $\pi_H(\omega(h, k)) = k'$. Logo

$$\begin{aligned} \omega(h,k) &= (\pi_H(\omega(h,k)), \pi_K(\omega(h,k))) \\ &= (\pi_H(\omega((h,1_K)(1_H,k))), \pi_K(\omega((1_H,k)(h,1_K)))) \\ &= (\pi_H(\omega(h,1_K)\omega(1_H,k)), \pi_K(\omega(1_H,k)\omega(h,1_K))) \\ &= (\pi_H(\omega(h,1_K))\pi_H(\omega(1_H,k)), \pi_K(\omega(1_H,k))\pi_K(\omega(h,1_K))) \\ &= (\pi_H(\omega(h,1_K))\gamma(k), \pi_K(\omega(1_H,k))\delta(h)) \\ &= (\omega_H(h), \omega_K(k)) \\ &= \phi_{\omega_H\omega_K}(h,k) \\ &= \phi(\omega_H, \omega_K)(h,k). \end{aligned}$$

Portanto, existem $\omega_H \in End(H)$ e $\omega_K \in End(K)$ que satisfazem a condição (3.1). Falta provar que $\omega_H \in Aut(H)$ e $\omega_K \in Aut(K)$. Para isto, basta que ω_H e ω_K sejam injetoras (já que H e K são grupos finitos).

Suponha $\omega_H(h) = 1_H$, para algum $h \in H$. Daí

$$\begin{aligned}\omega(h, 1_K) &= (\pi_H(w(h, 1_K)), \pi_K(w(h, 1_K))) \\ &= (\omega_H(h), \delta(h)) \\ &= (1_H, 1_K).\end{aligned}$$

Pela injetividade de ω, temos $h = 1_H$, portanto, $\omega_H \in Aut(H)$. Um argumento análogo nos mostra que $\omega_K \in Aut(K)$ e isto completa a prova.

■

Pelo Lema 3.1.1, para um grupo abeliano finito de ordem $|G| = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, temos

$$G \cong H_{p_1} \times H_{p_2} \times \cdots \times H_{p_n} \quad \text{e} \quad Aut(G) \cong Aut(H_{p_1}) \times Aut(H_{p_2}) \times \cdots \times Aut(H_{p_n}).$$

3.2 Endomorfismos dos Grupos H_p

A fim de realizar a caracterização proposta, será necessário dar uma descrição de $End(H_p)$, o anel dos endomorfismos de H_p. Os elementos de $End(H_p)$ são homomorfismos de H_p nele próprio, com as operações do anel dadas por:

$$\begin{aligned}(f + g)(a) &= f(a) + g(a) \\ (f \cdot g)(a) &= f \circ g(a),\end{aligned}$$

onde f, $g \in End(H_p)$ e $a \in H_p$. Estes anéis se comportam como anéis de matrizes com algumas características importantes que discutiremos abaixo.

Sejam p um número primo e $H_p = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$, com $1 \leq e_1 \leq \cdots \leq e_n$. Então $|H_p| = p^{e_1 + \cdots + e_n}$ e, além disso, $p^{e_1} \mid p^{e_2} \mid \cdots \mid p^{e_n}$.

Para cada $h \in \mathbb{Z}$, sempre existe $0 \leq h' \leq p^{e_i} - 1$ tal que $\bar{h} \equiv \bar{h}' \pmod{p^{e_i}}$ e, com esta representação, um elemento de H_p é um vetor coluna $(\bar{h}_1, \ldots, \bar{h}_n)^T$ em que cada $\bar{h}_i \in \mathbb{Z}_{p^{e_i}}$ e $h_i \in \mathbb{Z}$ é um representante de classe tal que $0 \leq h_i' \leq p^{e_i} - 1$. Com estas noções bem estabelecidas, definimos o seguinte conjunto de matrizes.

Definição 3.2.1 *$R_p = \{(a_{ij}) \in M_n(\mathbb{Z}) : p^{e_i - e_j} \mid a_{ij}$ para todos i, j tais que $1 \leq j \leq i \leq n\}$.*

Exemplo 3.2.2 *Seja $H_p = \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^5}$, ou seja, $e_1 = 1, e_2 = 2, e_3 = 5$. Então*

$$R_p = \left\{ \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21}p & a_{22} & a_{23} \\ a_{31}p^4 & a_{32}p^3 & a_{33} \end{bmatrix}, \text{ com } a_{ij} \in \mathbb{Z} \right\}.$$

Exemplo 3.2.3 *Seja* $H_p = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$, *ou seja,* $e_1 = 2, e_2 = 2, e_3 = 3, e_4 = 3$. *Então*

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

Lema 3.2.4 *O conjunto* R_p *forma um anel com a multiplicação usual de matrizes.*

Demonstração: Seja $A = (a_{ij}) \in R_p$. Afirmamos que a condição $p^{e_i - e_j} \mid a_{ij}$, para todos $1 \leq j \leq i \leq n$, é equivalente à existência de uma decomposição

$$A = PA'P^{-1}$$

em que $A' \in \mathbb{Z}^{n \times n}$ e $P = diag(p^{e_1}, \ldots, p^{e_n})$. De fato, como $p^{e_i - e_j} \mid a_{ij}$, para todos $1 \leq j \leq i \leq n$, existe $a'_{ij} \in \mathbb{Z}$ tal que $a_{ij} = p^{e_i - e_j} a'_{ij} \in \mathbb{Z}$, para todos $1 \leq j \leq i \leq n$. Observe, no entanto, que para cada par (i, j), com $i < j$, temos $e_i \leq e_j$ e podemos considerar $a'_{ij} = p^{e_j - e_i} a_{ij}$ e daí $a_{ij} = p^{e_i - e_j} a'_{ij} \in \mathbb{Z}$. Assim,

$$\begin{aligned} A &= \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \\ &= \begin{bmatrix} p^{e_1 - e_1} a'_{11} & p^{e_1 - e_2} a'_{12} & \cdots & p^{e_1 - e_n} a'_{1n} \\ p^{e_2 - e_1} a'_{21} & p^{e_2 - e_2} a'_{22} & \cdots & p^{e_2 - e_n} a'_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p^{e_n - e_1} a'_{n1} & p^{e_n - e_2} a'_{n2} & \cdots & p^{e_n - e_n} a'_{nn} \end{bmatrix} \\ &= \begin{bmatrix} p^{e_1} a'_{11} p^{-e_1} & p^{e_1} a'_{12} p^{-e_2} & \cdots & p^{e_1} a'_{1n} p^{-e_n} \\ p^{e_2} a'_{21} p^{-e_1} & p^{e_2} a'_{22} p^{-e_2} & \cdots & p^{e_2} a'_{2n} p^{-e_n} \\ \vdots & \vdots & \ddots & \vdots \\ p^{e_n} a'_{n1} p^{-e_1} & p^{e_n} a'_{n2} p^{-e_2} & \cdots & p^{e_n} a'_{nn} p^{-e_n} \end{bmatrix} \\ &= PA'P^{-1}. \end{aligned}$$

Agora, dadas as matrizes $A, B \in R_p$,

$$\begin{aligned} A + B &= PA'P^{-1} + PB'P^{-1} = P(A' + B')P^{-1} \in R_p \qquad \text{e} \\ AB &= PA'P^{-1}PB'P^{-1} = PA'B'P^{-1} \in R_p. \end{aligned}$$

Logo o conjunto R_p é fechado em relação à adição e à multiplicação usual de matrizes. Além disso, $(R_p, +)$ é um grupo abeliano e a multiplicação é associativa com a matriz identidade como o elemento neutro de R_p. Portanto, $(R_p, +, \cdot)$ é um anel.

■

Observação 3.2.5 *Seja*

$$\begin{array}{rccl} \pi_i: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_{p^{e_i}} \\ & h & \longmapsto & \pi_i(h) = \bar{h} \end{array}$$

a projeção canônica em $\mathbb{Z}_{p^{e_i}}$ e seja $\Pi : \mathbb{Z}^n \to H_p$ o homomorfismo dado por

$$\Pi(h_1, \ldots, h_n)^T = (\pi_1(h_1), \ldots, \pi_n(h_n))^T = (\bar{h}_1, \ldots, \bar{h}_n)^T.$$

Então Π é um endomorfismo de grupos, uma vez que cada π_i, para $1 \leq i \leq n$, é um endomorfismo de grupos.

Podemos agora dar uma descrição de $End(H_p)$ como quociente do anel de matrizes R_p.

Teorema 3.2.6 *A aplicação $\psi : R_p \to End(H_p)$ dada por*

$$\psi(A)(\bar{h}_1, \ldots, \bar{h}_n)^T = \Pi(A(h_1, \ldots, h_n)^T)$$

é um homomorfismo de anéis sobrejetor.

Demonstração: Primeiramente vamos verificar que a aplicação

$$\begin{array}{rccl} \psi(A): & H_p & \longrightarrow & H_p \\ & (\bar{h}_1, \ldots, \bar{h}_n)^T & \longmapsto & \Pi(A(h_1, \ldots, h_n)^T) \end{array}$$

está bem definida.

Seja $A = (a_{ij}) \in R_p$ e suponha $(\bar{r}_1, \ldots, \bar{r}_n)^T$, $(\bar{s}_1, \ldots, \bar{s}_n)^T \in H_p$ tais que

$$(\bar{r}_1, \ldots, \bar{r}_n)^T = (\bar{s}_1, \ldots, \bar{s}_n)^T,$$

para r_i, s_i inteiros, com $1 \leq i \leq n$. Daí

$$\bar{r}_i = \bar{s}_i \Rightarrow r_i \equiv s_i \,(\mathrm{mod}\, p^{e_i}) \Rightarrow p^{e_i} \mid r_i - s_i, \text{ para todo } i = 1, \ldots, n. \tag{3.2}$$

A k-ésima entrada do vetor $\Pi(A(\bar{r}_1, \ldots, \bar{r}_n)^T) - \Pi(A(\bar{s}_1, \ldots, \bar{s}_n)^T)$ é

$$\begin{aligned}\pi_k\left(\sum_{i=1}^{n} a_{ki}r_i\right) - \pi_k\left(\sum_{i=1}^{n} a_{ki}s_i\right) &= \pi_k\left(\sum_{i=1}^{n} a_{ki}r_i - \sum_{i=1}^{n} a_{ki}s_i\right)\\ &= \pi_k\left(\sum_{i=1}^{n} a_{ki}(r_i - s_i)\right) = \bar{0} \text{ em } \mathbb{Z}_{p^{e_k}},\end{aligned}$$

pois, por (3.2), $p^{e_i} \mid (r_i - s_i)$, ou seja, $(r_i - s_i) = p^{e_i}t_i$, para algum $t_i \in \mathbb{Z}$. Daí, para $k < i$, temos

$$a_{ki}(r_i - s_i) = a_{ki}p^{e_i}t_i = a_{ki}p^{e_k}p^{e_i-e_k}t_i \equiv 0 \pmod{p^{e_k}}.$$

Agora, como $A = (a_{ij}) \in R_p$, então, para $i \leq k$, $p^{e_k-e_i} \mid a_{ki}$, ou seja, $a_{ki} = p^{e_k-e_i}x_i$, para algum $x_i \in \mathbb{Z}$. Além disso, por (3.2), $(r_i - s_i) = p^{e_i}t_i$, para algum $t_i \in \mathbb{Z}$. Logo

$$a_{ki}(r_i - s_i) = p^{e_k-e_i}x_ip^{e_i}x_i = p^{e_k}x_it_i \equiv 0 \pmod{p^{e_k}}, \text{ com } x_it_i \in \mathbb{Z}.$$

Portanto, a função $\psi(A)$ está bem definida.

Agora dados $(\bar{r}_1, \ldots, \bar{r}_n)^T, (\bar{s}_1, \ldots, \bar{s}_n)^T \in H_p$

$$\begin{aligned}\psi(A)((\bar{r}_1, \ldots, \bar{r}_n)^T + (\bar{s}_1, \ldots, \bar{s}_n)^T) &= \psi(A)((\bar{r}_1 + \bar{s}_1, \ldots, \bar{r}_n + \bar{s}_n)^T)\\ &= \psi(A)((\overline{r_1 + s_1}, \ldots, \overline{r_n + s_n})^T)\\ &= \Pi(A(r_1 + s_1, \ldots, r_n + s_n)^T\\ &= \Pi(A(r_1, \ldots, r_n)^T + (s_1, \cdots, s_n)^T)\\ &= \Pi(A(r_1, \ldots, r_n)^T + \Pi(A(s_1, \cdots, s_n)^T)\\ &= \psi(A)(\bar{r}_1, \ldots, \bar{r}_n)^T + \psi(A)(\bar{s}_1, \ldots, \bar{s}_n)^T.\end{aligned}$$

Logo, a função $\psi(A)$ é um homomorfismo de grupos e, portanto, $\psi(A) \in End(H_p)$ para todo $A \in R_p$.

Para provar a sobrejetividade da função ψ, seja $w_j = (\bar{0}, \ldots, \bar{g}_j, \ldots, \bar{0})^T \in H_p$ o vetor com $\bar{g}_j$ na j-ésima coordenada e zero nas demais e considere $M \in End(H_p)$, um endomorfismo. Suponha $M(w_j) = (\bar{h}_{1j}, \ldots, \bar{h}_{nj})^T = \Pi(h_{1j}, \ldots, h_{1j})^T$, com $h_{ij} \in \mathbb{Z}$. Para $1 \leq i \leq n$, temos

$$\begin{aligned}(\bar{0}, \ldots, \bar{0}) &= M(\bar{0}, \ldots, \bar{0}) = M(p^{e_j}w_j) = p^{e_j}M(w_j)\\ &= p^{e_j}\Pi(h_{1j}, \ldots, h_{nj})^T\\ &= \Pi(p^{e_j}h_{1j}, \ldots, p^{e_j}h_{nj})^T\\ &= (\overline{p^{e_j}h_{1j}}, \ldots, \overline{p^{e_j}h_{nj}}).\end{aligned}$$

Consequentemente, $p^{e_i} \mid p^{e_j} h_{ij}$, para todo $1 \leq i \leq n$. Além disso, quando $i \geq j$, temos $p^{e_i - e_j} \mid h_{ij}$, formando assim uma matriz $H = (h_{ij}) \in R_p$. Portanto, dado $M \in End(H_p)$, existe $H = (h_{ij}) \in R_p$ tal que $\psi(H) = M$. Isto prova que a função ψ é sobrejetora.

Finalmente, precisamos mostrar que ψ é um homomorfismo de anéis. Sejam $A = (a_{ij})$, $B = (b_{ij}) \in R_p$ e $(\bar{h}_1, \ldots, \bar{h}_n)^T \in H_p$.

$$\begin{aligned}
\psi(A+B)(\bar{h}_1, \ldots, \bar{h}_n)^T &= \Pi((A+B)(h_1, \ldots, h_n)^T) \\
&= \Pi((A)(h_1, \ldots, h_n)^T + (B)(h_1, \ldots, h_n)^T) \\
&= \Pi((A)(h_1, \ldots, h_n)^T) + \Pi((B)(h_1, \ldots, h_n)^T) \\
&= \psi(A)(\bar{h}_1, \ldots, \bar{h}_n)^T + \psi(B)(\bar{h}_1, \ldots, \bar{h}_n)^T.
\end{aligned}$$

Ainda,

$$\begin{aligned}
\psi(A) \circ \psi(B)(\bar{h}_1, \ldots, \bar{h}_n)^T &= \psi(A)(\Pi((B)(h_1, \ldots, h_n)^T)) \\
&= \psi(A) \left(\Pi \left(\sum_{k=1}^{n} b_{1k} h_k, \ldots, \sum_{k=1}^{n} b_{nk} h_k \right)^T \right) \\
&= \psi(A) \left(\sum_{k=1}^{n} \Pi \left(b_{1k} h_k, \ldots, b_{nk} h_k \right)^T \right) \\
&= \sum_{k=1}^{n} \psi(A) \left(\overline{b_{1k} h_k}, \ldots, \overline{b_{nk} h_k} \right)^T \\
&= \sum_{k=1}^{n} \Pi \left(A \left(b_{1k} h_k, \ldots, b_{nk} h_k \right)^T \right) \\
&= \Pi \left(\sum_{k=1}^{n} \left(\sum_{t=1}^{n} a_{1t} b_{tk} h_k, \ldots, \sum_{t=1}^{n} a_{nt} b_{tk} h_k \right)^T \right) \\
&= \Pi \left(\sum_{k=1}^{n} \left(\sum_{t=1}^{n} a_{1t} b_{tk} \right) h_k, \ldots, \sum_{k=1}^{n} \left(\sum_{t=1}^{n} a_{nt} b_{tk} \right) h_k \right)^T \\
&= \pi(AB(h_1, \ldots, h_n)^T) \\
&= \psi(AB)(\bar{h}_1, \ldots, \bar{h}_n)^T.
\end{aligned}$$

Portanto $\psi(AB) = \psi(A) \circ \psi(B)$ e isto completa a prova. ∎

Lema 3.2.7 *Para a função ψ definida no Teorema 3.2.6, temos*

$$\ker(\psi) = \{(a_{ij}) \in R_p : p^{e_i} \mid a_{ij}, \text{ para todos } i, j \in \{1, \ldots, n\}\}.$$

Demonstração: Se $A = (a_{ij}) \in R_p$ tem a propriedade que cada a_{ij} é divisível por p^{e_i}, então, para todo $(\bar{h}_1, \ldots, \bar{h}_n)^T \in H_p$, temos

$$\begin{aligned}
\psi(A)(\bar{h}_1, \ldots, \bar{h}_n)^T &= \Pi(A(h_1, \ldots, h_n)^T) \\
&= \Pi\left(\sum_{j=1}^{n} a_{1j}h_j, \ldots, \sum_{j=1}^{n} a_{nj}h_j\right)^T \\
&= \Pi\left(\sum_{j=1}^{n} (a_{1j}h_j, \ldots, a_{nj}h_j)^T\right) \\
&= \sum_{j=1}^{n} \Pi\left(a_{1j}h_j, \ldots, a_{nj}h_j,\right)^T \\
&= \sum_{j=1}^{n} (\pi_1(a_{1j}h_j), \ldots, \pi_n(a_{nj}h_j))^T \\
&= (\bar{0}, \ldots, \bar{0})^T.
\end{aligned}$$

Portanto, $A \in \ker(\psi)$.

Reciprocamente, seja $A = (a_{ij}) \in \ker(\psi)$, ou seja, $\psi(A)(\bar{h}_1, \ldots, \bar{h}_n)^T = (\bar{0}, \ldots, \bar{0})^T$, para todo $(\bar{h}_1, \ldots, \bar{h}_n)^T \in H_p$. Daí

$$\begin{aligned}
(\bar{0}, \ldots, \bar{0})^T &= \psi(A)(\bar{h}_1, \ldots, \bar{h}_n)^T \\
&= \Pi(A(h_1, \ldots, h_n)^T) \\
&= \Pi\left(\sum_{j=1}^{n} a_{1j}h_j, \ldots, \sum_{j=1}^{n} a_{nj}h_j\right)^T \\
&= \left(\pi_1\left(\sum_{j=1}^{n} a_{1j}h_j\right), \ldots, \pi_n\left(\sum_{j=1}^{n} a_{nj}h_j\right)\right)^T \\
&= \left(\sum_{j=1}^{n} \bar{a}_{1j}\bar{h}_j, \ldots, \sum_{j=1}^{n} \bar{a}_{nj}\bar{h}_j\right)^T.
\end{aligned}$$

Com isso,

$$\begin{aligned}
&\bar{a}_{11}\bar{h}_1 + \bar{a}_{12}\bar{h}_2 + \cdots + \bar{a}_{1n}\bar{h}_n \equiv 0 \,(\mathrm{mod}\, p^{e_1}) \\
&\bar{a}_{21}\bar{h}_1 + \bar{a}_{22}\bar{h}_2 + \cdots + \bar{a}_{2n}\bar{h}_n \equiv 0 \,(\mathrm{mod}\, p^{e_2}) \\
&\vdots \\
&\bar{a}_{n1}\bar{h}_1 + \bar{a}_{n2}\bar{h}_2 + \cdots + \bar{a}_{nn}\bar{h}_n \equiv 0 \,(\mathrm{mod}\, p^{e_n}).
\end{aligned}$$

Considerando $w_j = (\bar{0}, \ldots, \bar{h}_j, \ldots, \bar{0})^T \in H_p$ o vetor com $\bar{h}_j$ na j-ésima cordenada e zero nas demais, onde $\bar{h_j}$ é um gerador de $\mathbb{Z}_{p^{e_j}}$, temos $\bar{a}_{ij}\bar{h}_j \equiv 0 \,(\mathrm{mod}\, p^{e_i})$, para todos $i, j = 1, \ldots, n$, ou seja, $p^{e_i} \mid a_{ij}h_j$ para todos $i, j = 1, \ldots, n$. Como $\bar{h}_j$ é um gerador de $\mathbb{Z}_{p^{e_j}}$, então $p^{e_i} \nmid h_j$, para todos $i, j = 1, \ldots, n$. Logo a_{ij} é divisível por p^{e_i}, para todos $i, j = 1, \ldots, n$. ∎

Juntos, o Teorema 3.2.6 e o Lema 3.2.7, dão uma caracterização explícita do anel de endomorfismos $End(H_p)$, pois, pelo 1º Teorema do Isomorfismo

$$\frac{R_p}{\ker(\psi)} \cong End(H_p).$$

Seguindo essa discussão, vamos encontrar agora as unidades de $End(H_p)$, visto que

$$U(End(H_p)) = Aut(H_p).$$

Antes de calcular as unidades de $End(H_p)$, enunciamos o seguinte resultado da teoria elementar de matrizes:

Definição 3.2.8 *Dada uma matriz $A \in M_n(\mathbb{K})$ e fixada uma linha i ou uma coluna j qualquer de A , o* ***desenvolvimento de Laplace*** *para o cálculo do determinante de A é dado, respectivamente, por*

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}) \quad ou \quad \det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}),$$

onde $A_{ij} \in \mathbb{M}_{n-1}(\mathbb{K})$ é a matriz formada a partir de A, retirando-se sua linha i e sua coluna j. Além disso, os elementos $c_{ij} = (-1)^{i+j} \det(A_{ij})$ são chamados ***cofatores*** *(em i, j) de A. Assim, definimos a* ***matriz adjunta*** *de A, denotada por $adj(A)$, como a* ***matriz transposta dos cofatores*** *de A, ou seja,*

$$adj(A) = B = (b_{ij}), \ onde\, b_{ij} = (-1)^{i+j} det(A_{ji}).$$

Lema 3.2.9 *Seja $A \in M_n(\mathbb{K})$ com $\det(A) \neq 0$. Então existe uma única matriz $B \in M_n(\mathbb{K})$ (chamada adjunta de A) tal que $AB = BA = \det(A) I_n$.*

Demonstração: Pela definição da matriz adjunta, dada uma matriz $A = (a_{ij}) \in M_n(\mathbb{K})$, existe uma matriz $B = adj(A) \in M_n(\mathbb{K})$ tal que $B = (b_{ij})$, com $b_{ij} = (-1)^{i+j} \det(A_{ji})$. Assim, $AB = (d_{ij})$, onde

$$d_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = \sum_{k=1}^{n} a_{ik} (-1)^{i+j} \det(A_{jk}).$$

Para $i = j$, temos $d_{ii} = \sum_{k=1}^{n} a_{ik} (-1)^{i+j} \det(A_{ik}) = \det(A)$, pois é o desenvolvimento de Laplace de $\det(A)$ pela i-ésima linha.

Para $i \neq j$, afirmamos que $d_{ij} = \sum_{k=1}^{n} a_{ik}(-1)^{i+j} \det(A_{jk})$ é o desenvolvimento de Laplace de $\det(A')$ pela j-ésima linha, onde $A' = (a'_{ij})$ é a matriz obtida a partir de A, substituindo-se a j-ésima linha pela i-ésima linha. De fato, supondo $i < j$, se $A_1, \ldots, A_i, \ldots, A_j, \ldots, A_n$ são as linhas de A, então $A_1, \ldots, A_i, \ldots, A_i, \ldots, A_n$ são as linhas de A'. Assim $a_{ik} = a'_{jk}$ e $\det(A_{jk}) = \det(A'_{jk})$. Logo,

$$d_{ij} = \sum_{k=1}^{n} a'_{jk}(-1)^{i+j} \det(A'_{jk}) = \det(A') = 0,$$

pois A' possui duas linhas iguais. Portanto,

$$AB = \begin{bmatrix} \det(A) & & 0 \\ & \ddots & \\ 0 & & \det(A) \end{bmatrix}$$

$$= \det(A) \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} = \det(A) I_n.$$

Considerando o desenvolvimento de Laplace do $\det(A)$ por meio de uma de suas colunas, um cálculo análogo nos mostra que $BA = \det(A) I_n$. Portanto,

$$AB = BA = \det(A) I_n, \text{ onde } B = adj(A).$$

Para provar a unicidade, suponha A_1 e $A_2 \in M_n(\mathbb{K})$ tais que $A_1 = adj(A)$ e $A_2 = adj(A)$, ou seja,

$$AA_1 = A_1 A = \det(A) I_n \quad \text{e} \quad AA_2 = A_2 A = \det(A) I_n.$$

Assim,

$$AA_1 = AA_2 \Rightarrow AA_1 - AA_2 = 0 \Rightarrow A(A_1 - A_2) = 0.$$

Por hipótese, $det(A) \neq 0$, então, multiplicando ambos os membros da equação por A^{-1}, temos $A_1 = A_2$. ∎

Lema 3.2.10 *Seja uma matriz $A \in R_p$, com $\det(A) \neq 0$. Então existe uma única matriz $B = Adj(A) \in R_p$, tal que $AB = BA = \det(A) I_n$.*

Demonstração: Dada uma matriz $A \in R_p$, com $\det(A) \neq 0$, o Lema 3.2.9 nos diz que existe uma única matriz $B \in M_n(\mathbb{K})$ tal que $AB = BA = \det(A) I_n$. Falta provar que $B \in R_p$. Como $A \in R_p$, então existe $A' \in M_n(\mathbb{Z})$ tal que $A = PA'P^{-1}$. Como

$$0 \neq \det(A) = \det(PA'P^{-1}) = \det(A'),$$

então, pelo Lema 3.2.9, existe uma única matriz $B' \in M_n(\mathbb{K})$ tal que

$$A'B' = B'A' = \det(A')I_n.$$

Seja $C = PB'P^{-1}$. Assim

$$AC = PA'P^{-1}PB'P^{-1} = PA'B'P^{-1} = P\det(A')I_nP^{-1} = \det(A)I_n \qquad \text{e}$$

$$AC = PA'P^{-1}PB'P^{-1} = PA'B'P^{-1} = PB'A'P^{-1} = PB'P^{-1}PA'P^{-1} = CA.$$

Pela unicidade de B (Lema 3.2.9), temos $B = C = PB'P^{-1}$ e assim $B \in R_p$ como desejado. ∎

Escrevendo $\mathbb{F}_p$ para o corpo $\mathbb{Z}_p$, apresentamos a seguir uma descrição completa de $Aut(H_p)$.

Teorema 3.2.11 *Dada uma matriz $A \in R_p$, um endomorfismo $M = \psi(A)$ é um automorfismo se, e somente se, $A \pmod p \in GL_n(\mathbb{F}_p)$.*

Demonstração: Seja $\psi(A) = M$ um automorfismo de H_p. Pelo fato de ψ ser sobrejetora, existe uma matriz $C \in R_p$ tal que $\psi(C) = M^{-1} \in End(H_p)$. Daí

$$\psi(AC - I_n) = \psi(AC) - \psi(I_n) = \psi(A)\psi(C) - Id_{H_p} = MM^{-1} - Id_{End(H_p)} = 0.$$

Logo $AC - I_n \in Ker(\psi)$ e, pelo Lema 3.2.7, p divide cada entrada da matriz $AC - I_n$, ou seja, $AC \equiv I_n \pmod p$. Além disso,

$$1 \equiv \det(AC) \equiv \det(A)\det(C) (\mathrm{mod}\, p).$$

Em particular, $p \nmid det(A)$ e o resultado segue.

Reciprocamente, seja $A \in R_p$ tal que $p \nmid \det(A)$, ou seja, $A \pmod p \in GL_n(\mathbb{F}_p)$. Assim, $\mathrm{mdc}(\det(A), p) = 1$. Além disso, $\mathrm{mdc}(\det(A), p^{e_j}) = 1$, para todo $1 \leq j \leq n$. Daí, pelo Teorema de Bézout, existem inteiros r e s tais que

$$\det(A) \cdot s + p^{e_j} \cdot r = 1, \text{ ou seja, } \det(A) \cdot s \equiv 1 \pmod{p^{e_j}}, \text{ sempre que } 1 \leq j \leq n.$$

Dessa forma, s é o inverso de $\det(A) \pmod{p^{e_j}}$. Agora, como $A \in R_p$, pelo Lema 3.2.10, existe uma única matriz $B \in R_p$, tal que $AB = BA = \det(A)I_n$. Assim, podemos definir um elemento de R_p por

$$A^{(*)} := s \cdot B$$

e, portanto,

$$\psi(A) \circ \psi(A^{(*)}) = \psi(AA^{(*)}) = \psi(As \cdot B) = \psi(s \cdot \det(A)I_n) \equiv \psi(I_n) = Id_{End(H_p)} \pmod{p^{e_j}} \quad \text{e}$$

$$\psi(A^{(*)}) \circ \psi(A) = \psi(A^{(*)}A) = \psi(s \cdot BA) = \psi(s \cdot \det(A)I_n) \equiv \psi(I_n) = Id_{End(H_p)} \pmod{p^{e_j}}.$$

Isto prova que $\psi(A)$ é um automorfismo de H_p. ∎

Exemplo 3.2.12 *Considere o caso quando $e_i = 1$, para $i = 1, \ldots, n$, ou seja,*

$$H_p \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p.$$

Então H_p é um p-grupo abeliano elementar que pode ser visto como o espaço vetorial $\mathbb{F}_p^n$ sobre $\mathbb{F}_p$ e assim, $End(H_p)$ é isomorfo ao anel $M_n(\mathbb{F}_p)$ das matrizes $n \times n$ com coeficientes no corpo $\mathbb{F}_p$. Neste caso, o Teorema 3.2.11 é simplesmente uma afirmação que $Aut(H_p)$ corresponde ao conjunto das matrizes invertíveis $GL_n(\mathbb{F}_p)$.

3.3 Contando os Automorfismos de H_p

Nesta seção, apresentamos um modo para calcular o número de elementos de $Aut(H_p)$ usando a caracterização feita na Seção 3.2. O cálculo procede em dois estágios:

1) Encontrar todos os elementos de $GL_n(\mathbb{F}_p)$ que podem ser estendidos a uma matriz $A \in R_p$.

2) Calcular todas as maneiras distintas de estender tal elemento a um endomorfismo de H_p.

Pelo Teorema 3.2.11, dada uma matriz $A \in R_p$, um endomorfismo $M = \psi(A)$ é um automorfismo se, e somente se, $A \pmod p \in GL_n(\mathbb{F}_p)$. Agora, pela definição de R_p, uma matriz $A \in R_p$ se, e somente se, $p^{e_i - e_j} \mid a_{ij}$, para todos $1 \leq j \leq i \leq n$. Assim, dada uma entrada $\bar{a}_{ij}$ de $A \pmod p$, $\bar{a}_{ij} = \bar{0}$, sempre que $e_j < e_i$, com $1 \leq j \leq i \leq n$. Como ilustração, considere o seguinte:

Exemplo 3.3.1 *Seja $H_p = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^3}$, ou seja, $e_1 = e_2 = 2, e_3 = e_4 = 3$ e considere $A \in R_p$. Então*

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

Logo,

$$A \pmod p = \begin{bmatrix} \bar{a}_{11} & \bar{a}_{12} & \bar{a}_{13} & \bar{a}_{14} \\ \bar{a}_{21} & \bar{a}_{22} & \bar{a}_{23} & \bar{a}_{24} \\ \bar{0} & \bar{0} & \bar{a}_{33} & \bar{a}_{34} \\ \bar{0} & \bar{0} & \bar{a}_{43} & \bar{a}_{44} \end{bmatrix}, \quad com\ \bar{a}_{ij} \in \mathbb{Z}_p.$$

Para o caso geral, definimos os seguintes $2n$ números:

$$d_k = \max\{l : e_l = e_k\} \quad \text{e} \quad c_k = \min\{l : e_l = e_k\}.$$

já que $e_k = e_k$, temos $d_k \geq k$ e $c_k \leq k$. Assim, precisamos encontrar todas as matrizes $M \in GL_n(\mathbb{F}_p)$ que são da forma:

$$M = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1n} \\ \vdots & \vdots & \cdots & \vdots \\ m_{d_1 1} & m_{d_1 2} & \cdots & m_{d_1 n} \\ 0 & m_{d_2 2} & \cdots & m_{d_2 n} \\ 0 & 0 & \cdots & m_{d_3 n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & m_{d_n n} \end{bmatrix} = \begin{bmatrix} m_{1c_1} & m_{1c_2} & \cdots & m_{1c_n} & \cdots & m_{1n} \\ \vdots & m_{2c_2} & \cdots & m_{2c_n} & \cdots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & m_{nc_n} & \cdots & m_{nn} \end{bmatrix}.$$

Para isto, calcularemos o número de escolhas possíveis para cada coluna de M.

Para que uma matriz M pertença a $GL_n(\mathbb{F}_p)$, as colunas de M devem ser linearmente independentes. Assim, existem $p^{d_1} - 1$ escolhas possíveis para a 1ªcoluna de M, já que a coluna nula não é permitida. Escolhida a 1ª coluna, existem $p^{d_2} - p$ escolhas possíveis para a segunda coluna de M, uma vez que os múltiplos da 1ª coluna não são permitidos. Escolhidas a 1ª e a 2ª colunas, existem $p^{d_3} - p^2$ possíveis escolhas para a 3ª coluna de M, pois as combinações lineares das duas primeiras colunas não são permitidas. Continuando esse processo, escolhidas as $k-1$ primeiras colunas de M, existem $p^{d_k} - p^{k-1}$ possíveis escolhas para a k-ésima coluna, visto que as combinações lineares das $k-1$ primeiras colunas não são permitidas. Portanto, existem

$$\prod_{k=1}^{n} (p^{d_k} - p^{k-1})$$

matrizes em $GL_n(\mathbb{F}_p)$ que podem ser estendidas a R_p.

Finalmente, basta calcular o número de maneiras de estender cada elemento $M \in GL_n(\mathbb{F}_p)$ a um endomorfismo de H_p. Pela caracterização feita na Seção 3.2, temos

$$End(H_p) \cong \frac{R_p}{\ker(\psi)}.$$

Note que uma matriz $A' \in \ker(\psi)$ é da forma

$$A' = \begin{bmatrix} p^{e_1} a'_{11} & p^{e_1} a'_{12} & \cdots & p^{e_1} a'_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ p^{e_n} a'_{n1} & p^{e_n} a'_{n2} & \cdots & p^{e_n} a'_{nn} \end{bmatrix} \text{ com } a'_{ij} \in \mathbb{Z}.$$

Assim, um elemento de $R_p/\ker(\psi)$ terá como representante uma matriz $B = (b_{ij})$ tal que $p^{e_i} \nmid b_{ij}$, para pelo menos um par (i,j). Como $B \in R_p$, para $1 \leq j \leq i \leq n$, devemos ter $p^{e_i - e_j} \mid b_{ij}$. Assim, para a extensão destes elementos, devemos escolhê-los em $\mathbb{Z}/p^{e_i}\mathbb{Z}$ de tal modo que $p^{e_i - e_j} \mid b_{ij}$, ou seja, do conjunto $p^{e_i - e_j}\mathbb{Z}/p^{e_i}\mathbb{Z}$. Os outros podem ser quaisquer elementos não nulos de $\mathbb{Z}/p^{e_i}\mathbb{Z}$. No entanto, observe que, para $e_i = e_j$, temos

$p^{e_i-e_j}\mathbb{Z}/p^{e_i}\mathbb{Z} = \mathbb{Z}/p^{e_i}\mathbb{Z}$. Portanto, para $e_i > e_j$, vamos calcular todas as maneiras de estender cada elemento m_{ij} (com $\bar{m}_{ij} \in \mathbb{Z}_p$) a um elemento $\bar{a}_{ij} \in p^{e_i-e_j}\mathbb{Z}/p^{e_i}\mathbb{Z}$ tal que

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

Para $e_i \leq e_j$, vamos calcular todas as maneiras de estender cada elemento m_{ij} (com $\bar{m}_{ij} \in \mathbb{Z}_p$) a um elemento $\bar{a}_{ij} \in \mathbb{Z}/p^{e_i}\mathbb{Z}$ tal que

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

Pelo Lema 2.1.7, temos

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

Agora, quando $e_i > e_j$, $m_{ij} = \bar{0}$ em $\mathbb{Z}_p$. Assim, $\bar{a}_{ij}$ pode assumir qualquer valor em $p^{e_i-e_j}\mathbb{Z}_{p^{e_i}}$, pois, dado $\bar{a}_{ij} \in p^{e_i-e_j}\mathbb{Z}_{p^{e_i}}$, $\bar{a}_{ij} = \overline{p^{e_i-e_j}l} \,(\mathrm{mod}\, p^{e_i})$, com $0 \leq \bar{l} \leq p^{e_j}-1$. Logo

$$\begin{aligned} a_{ij} &= p^{e_i-e_j}l + p^{e_i}t \quad \text{com} \quad l,t \in \mathbb{Z} \\ &= p(p^{e_i-e_j-1}l + p^{e_i-1}t) \equiv 0 \,(\mathrm{mod}\, p). \end{aligned}$$

Portanto, existem p^{e_j} maneiras de estender cada um dos $n-d_j$ elementos nulos de cada coluna da matriz M.

Quando $e_i \leq e_j$, $m_{ij} \neq \bar{0}$ em $\mathbb{Z}_p$. Além disso,

$$a_{ij} \equiv m_{ij} \,(\mathrm{mod}\, p) \;\Leftrightarrow\; a_{ij} = m_{ij} + ps \quad (\text{para algum } s \in \mathbb{Z}).$$

Logo $\overline{a}_{ij} = \overline{m_{ij} + ps} = \overline{m}_{ij} + \overline{ps} \,(\mathrm{mod}\, p^{e_i})$.

Agora

$$\overline{ps} \in \mathbb{Z}/p^{e_i}\mathbb{Z} \;\Leftrightarrow\; \overline{ps} \in p\mathbb{Z}/p^{e_i}\mathbb{Z} = \{\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{(p^{e_i-1}-1)p}\} \cong \mathbb{Z}_{p^{e_i-1}}.$$

Portanto, existem p^{e_i-1} maneiras de estender cada um dos $n-c_i+1$ elementos não nulos em cada linha da matriz M, pois podemos adicionar elementos de $p\mathbb{Z}/p^{e_i}\mathbb{Z}$. Isto prova o seguinte resultado:

Teorema 3.3.2 *Seja $H_p = \mathbb{Z}_{p^{e_1}} \times \cdots \times \mathbb{Z}_{p^{e_n}}$ um grupo abeliano. Então*

$$|Aut(H_p)| = \prod_{k=1}^{n}(p^{d_k} - p^{k-1}) \prod_{j=1}^{n}(p^{e_j})^{n-d_j} \prod_{i=1}^{n}(p^{e_i-1})^{n-c_i+1}.$$

Exemplo 3.3.3 *Seja $H_2 = \mathbb{Z}_2 \times \mathbb{Z}_{2^3}$. Vamos encontrar o número de elementos de $Aut(H_2)$ usando a caracterização feita.*

Considere $H_2 = \mathbb{Z}_2 \times \mathbb{Z}_{2^3}$. *Dessa forma,* $e_1 = 1$ *e* $e_2 = 3$, *além disso, como* $d_k = \max\{l : e_l = e_k\}$ *e* $c_k = \min\{l : e_l = e_k\}$, *então* $d_1 = 1$, $d_2 = 2$, $c_1 = 1$ *e* $c_2 = 2$. *Assim, vamos encontrar todas as matrizes* $M \in GL_n(\mathbb{F}_2)$ *que são da forma*

$$M = \begin{bmatrix} m_{11} & m_{12} \\ 0 & m_{22} \end{bmatrix} \text{ com } \bar{m}_{ij} \in \mathbb{Z}_2.$$

Observe que existem 2 matrizes $M \in GL_n(\mathbb{F}_2)$ *que podem ser estendidas a* R_p, *a saber,*

$$\begin{bmatrix} \bar{1} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix} \quad e \quad \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}.$$

Basta agora calcular todas a maneiras de estender cada uma destas matrizes a um endomorfismo de H_2. *Faremos isto calculando as maneiras de estender cada um dos elementos* $m_{ij} \in M$. *Primeiramente, vamos estender o elemento* m_{21} *a um elemento* $\bar{a}_{21} \in 2^{e_2-e_1}\mathbb{Z}/2^{e_2}\mathbb{Z}$ *de forma que*

$$a_{21} \equiv m_{21} \pmod{p}.$$

Neste caso, $m_{21} = 0$ *em* $\mathbb{Z}_2$ *e* $2^{e_2-e_1}\mathbb{Z}/2^{e_2}\mathbb{Z} = 2^2\mathbb{Z}/2^3\mathbb{Z} = \{\bar{0}, \bar{4}\}$. *Daí, para qualquer* $\bar{a}_{21} \in 2^2\mathbb{Z}/2^3\mathbb{Z}$, *temos* $a_{21} \equiv m_{21} \pmod{p}$. *Logo existem 2 maneiras de estender o elemento* $m_{21} \in M$.

Vamos agora estender o elemento m_{11} *a um elemento* $\bar{a}_{11} \in \mathbb{Z}/2^{e_1}\mathbb{Z}$ *de forma que*

$$a_{11} \equiv m_{11} \pmod{p}$$

Neste caso, $m_{11} \equiv 1 \pmod{p}$ *e* $\mathbb{Z}/2^{e_1}\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$. *Daí,* $\bar{1}$ *é o único valor de* $\bar{a}_{11}$ *que satisfaz a congruência* $a_{11} \equiv m_{11} \pmod{p}$. *Logo existe apenas uma maneira de estender o elemento* $m_{11} \in M$.

Para o elemento m_{12}, *vamos estendê-lo a um elemento* $\bar{a}_{12} \in \mathbb{Z}/2^{e_1}\mathbb{Z}$ *de forma que*

$$a_{12} \equiv m_{12} \pmod{p}.$$

Neste caso, ou $m_{12} \equiv 1 \pmod{p}$ *ou* $m_{12} \equiv 0 \pmod{p}$ *e* $\mathbb{Z}/2^{e_1}\mathbb{Z} = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$. *Se* $m_{12} \equiv 1 \pmod{p}$, *então já vimos que existe apenas uma maneira de estendê-lo. Se* $m_{12} \equiv 0 \pmod{p}$, *também existe uma única maneira de estendê-lo, uma vez que* $\bar{0}$ *é o único valor de* $\bar{a}_{12}$ *que satisfaz a congruência* $a_{12} \equiv m_{12} \pmod{p}$. *Logo existe uma única maneira de estender o elemento* $m_{12} \in M$.

Para o elemento m_{22}, *vamos estendê-lo a um elemento* $\bar{a}_{22} \in \mathbb{Z}/2^{e_2}\mathbb{Z}$ *de forma que*

$$a_{22} \equiv m_{22} \pmod{p}.$$

Neste caso, $m_{22} \equiv 1 \pmod{p}$ *e* $\mathbb{Z}/2^{e_2}\mathbb{Z} = \mathbb{Z}/2^3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$. *Daí, para qualquer* $\bar{a}_{22} \in \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$, *temos satisfeita a congruência* $a_{22} \equiv m_{22} \pmod{p}$, *ou seja, podemos adicionar o elemento* $\bar{m}_{22}$ *a elementos do conjunto* $2\mathbb{Z}/2^3\mathbb{Z} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$. *Logo existem 4 maneiras de estender o elemento* $m_{22} \in M$ *e, portanto,*

$$|Aut(H_2)| = 2\,(2 \cdot 1 \cdot 1 \cdot 4) = 16.$$

3.4 Automorfismos de p-grupos abelianos finitos

Nesta seção apresentamos uma nova fórmula para a ordem do grupo de automorfismos $Aut(A)$, onde A é um p-grupo abeliano finito. Esta abordagem envolve a estrutura dos subgrupos do grupo abeliano e segue o trabalho desenvolvido por Heinrich Kuhn em [5].

Definição 3.4.1 *Um* ***p-grupo abeliano finito***

$$A \cong \underbrace{\mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_1}}}_{\lambda_1 \text{ vezes}} \times \cdots \times \underbrace{\mathbb{Z}_{p^{m_t}} \times \cdots \times \mathbb{Z}_{p^{m_t}}}_{\lambda_t \text{ vezes}}$$

é dito um grupo do tipo $(\underbrace{m_1, \ldots, m_1}_{\lambda_1 \text{ vezes}}; \ldots; \underbrace{m_t, \ldots, m_t}_{\lambda_t \text{ vezes}})$ *que, para simplificar a notação, escrevemos* $(\lambda_1 \times m_1; \ldots; \lambda_t \times m_t)$.

Exemplo 3.4.2 *Seja A um grupo abeliano de ordem p^{28} e do tipo $(2 \times 9;\ 6;\ 4)$. Então $A \cong C_{p^9} \times C_{p^9} \times C_{p^6} \times C_{p^4}$.*

Definição 3.4.3 *Seja A um p-grupo abeliano finito do tipo $(\lambda_1 \times m_1; \ldots; \lambda_t \times m_t)$ com $m_1 > \cdots > m_t$ e $1 \leq \gamma \leq m_1$. O conjunto*

$$\Omega_\gamma(A) = \langle a \in A \mid a^{p^\gamma} = 1_A \rangle$$

é o conjunto de todos os elementos de A cuja ordem divide p^γ.

Proposição 3.4.4 *Seja A um p-grupo abeliano finito do tipo $(\lambda_1 \times m_1; \ldots; \lambda_t \times m_t)$ com $m_1 > \cdots > m_t$ e $1 \leq \gamma \leq m_1$. O subgrupo*

$$\Omega_\gamma(A) = \langle a \in A \mid a^{p^\gamma} = 1_A \rangle$$

é um ***subgrupo característico*** *de A.*

Demonstração: O conjunto $\Omega_\gamma(A) = \langle a \in A \mid a^{p^\gamma} = 1_A \rangle$ é não vazio, pois $1_A \in \Omega_\gamma(A)$. Sejam $a,\ b \in \Omega_\gamma(A)$. Assim, $a^{p^\gamma} = 1_A$, $b^{p^\gamma} = 1_A$ e daí $b^{-1} \in \Omega_\gamma(A)$. Então

$$(a\, b^{-1})^{p^\gamma} = a^{p^\gamma} (b^{-1})^{p^\gamma} = 1_A.$$

Logo, $a\, b^{-1} \in \Omega_\gamma(A)$ e, portanto, $\Omega_\gamma(A)$ é um subgrupo de A. Agora sejam x um elemento arbitrário de $\Omega_\gamma(A)$ e φ um automorfismo de A. Então,

$$1_A = \varphi\left(x^{p^\gamma}\right) = \varphi(\underbrace{x \cdot x \cdots x}_{p^\gamma \text{ vezes}}) = \underbrace{\varphi(x) \cdot \varphi(x) \cdots \varphi(x)}_{p^\gamma \text{ vezes}} = \varphi(x)^{p^\gamma}.$$

Logo $\varphi(x) \in \Omega_\gamma(A)$, para todo $x \in \Omega_\gamma(A)$. Portanto, $\varphi\left(\Omega_\gamma\right) \subseteq \Omega_\gamma$.

■

Proposição 3.4.5 *Seja A um p-grupo abeliano finito do tipo $(\lambda_1 \times m_1; \cdots ; \lambda_t \times m_t)$ com $m_1 > \cdots > m_t$ e considere $1 \leq \gamma \leq m_1$ e $m_h \geq \gamma > m_{h+1}$. Se $|\Omega_\gamma(A)| = p^{n_\gamma}$, então*

$$n_\gamma = (\lambda_1 + \lambda_2 + \cdots + \lambda_h)\gamma + \sum_{i<j} \lambda_j m_j.$$

Demonstração: Seja

$$A = C_{p^{m_1}} \times \cdots \times C_{p^{m_1}} \times \cdots \times C_{p^{m_t}} \times \cdots \times C_{p^{m_t}},$$

onde cada subgrupo cíclico $C_{p^{m_i}} = \langle A_{i,k} \rangle$, com $i = 1, \ldots, t$ e $k = 1, \ldots, \lambda_i$ e considere $m_h \geq \gamma > m_{h+1}$. Os elementos de $\Omega_\gamma(A)$ são tais que $\left(A_{i,k}^{x_{i,k}}\right)^{p^\gamma} = 1_A$, para todos $i = 1, \ldots, t$, $k = 1, \ldots, \lambda_i$ e $x_{i,k} = 1, 2, \ldots, p^{m_i}$, isto é, os elementos de $\Omega_\gamma(A)$ são tais que

$$p^\gamma \, x_{i,k} \equiv 0 \, (\mathrm{mod}\, p^{m_i}).$$

Observe que, para $i \geq h$, temos $m_i \leq m_h$, assim a congruência $p^\gamma \, x_{i,k} \equiv 0 \, (\mathrm{mod}\, p^{m_i})$ admite p^{m_i} soluções, para $i \geq h$.

Agora, para $i < h$, temos $m_i > m_h$ e queremos saber quantas soluções a congruência $p^\gamma \, x_{i,k} \equiv 0 \, (\mathrm{mod}\, p^{m_i})$ possui, para $x_{i,k} = 1, 2, \cdots, p^{m_i}$. Ora,

$$p^\gamma \, x_{i,k} \equiv 0 \, (\mathrm{mod}\, p^{m_i}) \Leftrightarrow x_{i,k} = p^{m_i - \gamma} \cdot c, \tag{3.3}$$

onde $c \in \mathbb{Z}$ e $x_{i,k} \in \{1, 2, \ldots, p^{m_i}\}$. Assim, escrevendo os elementos do conjunto $\{1, 2, \ldots, p^{m_i}\}$ de forma adequada, obtemos

$$\begin{array}{cccc}
1, & 2, & \cdots, & p^{m_i-\gamma} \\
p^{m_i-\gamma}+1, & p^{m_i-\beta}+2, & \cdots, & 2p^{m_i-\gamma} \\
\vdots & \vdots & \cdots & \vdots \\
(p-1)p^{m_i-\gamma}+1, & (p-1)p^{m_i-\gamma}+2, & \cdots, & p^{m_i-\gamma+1} \\
\vdots & \vdots & \cdots & \vdots \\
(p^\gamma-1)p^{m_i-\gamma}+1, & (p^\gamma-1)p^{m_i-\gamma}+2, & \cdots, & p^{m_i}.
\end{array}$$

Note que todos os elementos da última coluna, e apenas estes, satisfazem a condição (3.3). Além disso, existem $p^{m_i-\gamma}$ elementos em cada linha e, como existem p^{m_i} elementos ao todo, então a quantidade de elementos em cada coluna é p^γ, pois $p^{m_i-\gamma}p^\gamma = p^{m_i}$. Logo, a congruêcia $p^\gamma \, x_{i,k} \equiv 0 \, (\mathrm{mod}\, p^{m_i})$ possui p^γ soluções para $i < h$. Portanto,

$$|\Omega_\gamma(A)| = p^{(\lambda_1+\lambda_2+\cdots+\lambda_h)\gamma+\lambda_{h+1}m_{h+1}+\cdots+\lambda_t m_t}.$$

■

3.4.1 Número de Elementos de uma Dada Ordem

Proposição 3.4.6 *Seja A um p-grupo abeliano finito do tipo $(\lambda_1 \times m_1; \cdots ; \lambda_t \times m_t)$ com $m_1 > \cdots > m_t$ e considere $1 \leq \gamma \leq m_1$ e $m_h \geq \gamma > m_{h+1}$. O número de elementos de A cuja ordem é p^γ é*

$$p^{n_\gamma}\left(1 - p^{-(\lambda_1+\cdots+\lambda_h)}\right).$$

Demonstração: Seja A um p-grupo abeliano finito do tipo $(\lambda_1 \times m_1; \cdots ; \lambda_t \times m_t)$ com $m_1 > \cdots > m_t$ e $1 \leq \gamma \leq m_1$. Para determinar o número de elementos de A cuja ordem é p^γ, é necessário apenas encontrar a ordem do grupo gerado por todos os elementos cuja ordem divide p^γ e subtrair deste número a ordem do grupo gerado por todos os elementos cuja ordem divide $p^{\gamma-1}$. Observe que, como $m_h \geq \gamma > m_{h+1}$, então, ou $m_h \geq \gamma - 1 > m_{h+1}$ ou $m_{h+1} \geq \gamma - 1 > m_{h+2}$. Agora, quando $m_h \geq \gamma - 1 > m_{h+1}$, um cálculo análogo ao que é feito a seguir nos dá o resultado desejado. Considere então o caso em que $m_{h+1} \geq \gamma - 1 > m_{h+2}$. Assim, o número de elementos de A cuja ordem é p^γ é

$$\begin{aligned}
|\Omega_\gamma(A)| &- |\Omega_{\gamma-1}(A)| \\
&= p^{(\lambda_1+\cdots+\lambda_h)\gamma+\lambda_{h+1}m_{h+1}+\cdots+\lambda_t m_t} - p^{(\lambda_1+\cdots+\lambda_h+\lambda_{h+1})(\gamma-1)+\lambda_{h+2}m_{h+2}+\cdots+\lambda_t m_t} \\
&= p^{(\lambda_1+\cdots+\lambda_h)\gamma+\lambda_{h+1}m_{h+1}+\cdots+\lambda_t m_t} - p^{(\lambda_1+\cdots+\lambda_h)(\gamma-1)+\lambda_{h+1}m_{h+1}+\lambda_{h+2}m_{h+2}+\cdots+\lambda_t m_t} \\
&= p^{(\lambda_1+\cdots+\lambda_h)\gamma+\lambda_{h+1}m_{h+1}+\cdots+\lambda_t m_t}\left(1 - p^{-(\lambda_1+\cdots+\lambda_h)}\right) \\
&= p^{n_\gamma}\left(1 - p^{-(\lambda_1+\cdots+\lambda_h)}\right).
\end{aligned}$$

■

Teorema 3.4.7 *Se A é um p-grupo abeliano finito do tipo $(\lambda_1 \times m_1; \cdots ; \lambda_t \times m_t)$, com $m_1 > \cdots > m_t$ e $|\Omega_{m_i}(A)| = p^{n_i}$, para $1 \leq i \leq t$, então a ordem do grupo de automorfismos de A é dada por*

$$\prod_{i=1}^{t}\prod_{j=1}^{\lambda_i}\left(p^{n_i} - p^{n_i-j}\right).$$

Demonstração:

Seja

$$A = C_{p^{m_1}} \times \cdots \times C_{p^{m_1}} \times \cdots \times C_{p^{m_t}} \times \cdots \times C_{p^{m_t}},$$

onde cada subgrupo cíclico $C_{p^{m_i}} = \langle A_{i,k} \rangle$, com $i = 1, \ldots, t$ e $k = 1, \ldots, \lambda_i$. Então o grupo de automorfismos $Aut(A)$ fica completamente determinado pela imagens $\varphi(A_{i,k})$, onde

$i = 1, \ldots, t$, $k = 1, \ldots, \lambda_i$ e φ é um automorfismo de A. Consequentemente a ordem do grupo de automorfismos de A é completamente determinada conhecendo-se o número de possibilidades de escolhas para as imagens de cada um dos geradores $A_{i,k}$, com $i = 1, \ldots, t$ e $k = 1, \ldots, \lambda_i$. Encontrar o número de possibilidades de escolhas para as imagens de cada um dos geradores $A_{i,k}$ é equivalente a responder a seguinte questão:

Escolhidas as imagens $\varphi(A_{\alpha,\beta})$, para $\alpha = 1, \ldots, i-1$, $\beta = 1, \ldots, \lambda_\alpha$ e $\alpha = i$, $\beta = 1, \ldots, k-1$, quantas possibilidades existem para $\varphi(A_{i,k})$, de tal forma que a função φ seja um automorfismos de A?

Seja $M_{i,k}$ o número de elementos que podem ser escolhidos para $\varphi(A_{i,k})$. Estes elementos devem satisfazer o seguinte:

(i) Sua ordem é $\leq p^{m_i}$.

(ii) Sua p^{m_i-1}-ésima potência não pertence ao subgrupo $\langle A_{\alpha,\beta}\rangle$, para $\alpha = 1, \ldots, i-1$, $\beta = 1, \ldots, \lambda_\alpha$ e $\alpha = i$, $\beta = 1, \ldots, k-1$.

De fato, como um automorfismo preserva a ordem dos elementos e $o(A_{i,k}) = p^{m_i}$, devemos ter $o(\varphi(A_{i,k})) = p^{m_i}$.

Agora seja $x \in A$ tal que $o(x) \leq p^{m_i}$ e $x^{p^{m_i-1}} \in \langle A_{\alpha,\beta}\rangle$. Assuma que $\varphi(A_w)$ já esteja definida, para todo $A_w \in \langle A_{\alpha,\beta}\rangle$ e suponha $\varphi(A_{i,k}) = x$. Daí

$$\varphi\left(A_{i,k}^{p^{m_i-1}}\right) = x^{p^{m_i-1}} \in \langle A_{\alpha,\beta}\rangle$$

e, assim, $x^{p^{m_i-1}} = (A_1^s)^{p^{m_i-1}}$, para algum $A_1 \in \langle A_{\alpha,\beta}\rangle$ e $s \in \mathbb{Z}$. Como $\varphi(A_w)$, para todo $A_w \in \langle A_{\alpha,\beta}\rangle$, já está definida, considere $\varphi(A_1) = y$. Assim,

$$\varphi(A_1^s) = y^s \quad \text{e} \quad \varphi\left((A_1^s)^{p^{m_i-1}}\right) = (y^s)^{p^{m_i-1}},$$

donde,

$$\varphi\left(A_1^s \cdot A_{i,k}^{p^{m_i-1}}\right) = y^s (y^s)^{p^{m_i-1}} = (y^s)^{p^{m_i-1}+1}.$$

Note que o elemento $A_1^s \cdot A_{i,k}^{p^{m_i-1}} \notin \langle A_{\alpha,\beta}\rangle$, pois $\langle A_{i,k}\rangle \not\subseteq \langle A_{\alpha,\beta}\rangle$.

Por outro lado,

$$\varphi\left((A_1^s)^{p^{m_i-1}+1}\right) = \varphi\left(A_1^s \cdot (A_1^s)^{p^{m_i-1}}\right) = y^s (y^s)^{p^{m_i-1}} = (y^s)^{p^{m_i-1}+1}.$$

Observe, no entanto, que $(A_1^s)^{p^{m_i-1}+1} \in \langle A_{\alpha,\beta}\rangle$. Logo, temos dois elementos distintos com mesma imagem, o que contraria o fato de φ ser automorfismo.

Vamos agora encontrar o número de elementos de A, cuja ordem é $\leq p^{m_i}$ e cuja p^{m_i-1}-ésima potência pertence a $\langle A_{\alpha,\beta}\rangle$.

Observe que, dado um elemento $x \in A$ tal que $o(x) \leq p^{m_i}$, então, $o\left(x^{p^{m_i-1}}\right) \leq p$. Além disso, o subgrupo $\langle A_{\alpha,\beta}\rangle$ possui exatamente $p^{\lambda_1+\cdots+\lambda_{i-1}+k-1}$ elementos cuja ordem é $\leq p$ e todos estes elementos são representados como p^{m_i-1}-ésimas potências.

De fato, para cada um dos geradores $A_{\alpha,\beta}$, com $\alpha = 1,\ldots,i-1$, $\beta = 1,\ldots,\lambda_\alpha$ e $\alpha = i$, $\beta = 1,\ldots,k-1$, temos $o(A_{\alpha,\beta}) = p^{m_\alpha}$. Além disso, para todo inteiro s tal que $\mathrm{mdc}(s,\, p^{m_\alpha}) = 1$, temos $o\left((A_{\alpha,\beta})^s\right) = p^{m_\alpha}$. Assim,

$$o\left(A_{\alpha,\beta}^{p^{m_\alpha-1}}\right) = p \quad \text{e} \quad o\left(\left(A_{\alpha,\beta}^{s}\right)^{p^{m_\alpha-1}}\right) = p,$$

desde que $\mathrm{mdc}(s,\, p^{m_\alpha}) = 1$. Além disso, todos o elementos de A de ordem $\leq p$ são escritos dessa forma ou como produto de elementos dessa forma. Agora, como $m_\alpha \geq m_i$, podemos escrever

$$A_{\alpha,\beta}^{p^{m_\alpha-1}} = \left(A_{\alpha,\beta}^{p^{m_\alpha-m_i}}\right)^{p^{m_i-1}} \quad \text{e} \quad \left(A_{\alpha,\beta}^{s}\right)^{p^{m_\alpha-1}} = \left(\left(A_{\alpha,\beta}^{s}\right)^{p^{m_\alpha-m_i}}\right)^{p^{m_i-1}}.$$

Observe ainda que $o\left(\left(A_{\alpha,\beta}^{s}\right)^{p^{m_\alpha-m_i}}\right) \leq p^{m_i}$, pois, como $o\left(\left(\left(A_{\alpha,\beta}^{s}\right)^{p^{m_\alpha-m_i}}\right)^{p^{m_i-1}}\right) = p$, então $\left(\left(\left(A_{\alpha,\beta}^{s}\right)^{p^{m_\alpha-m_i}}\right)^{p^{m_i-1}}\right)^{p} = 1_A$, ou seja, $\left(\left(A_{\alpha,\beta}^{s}\right)^{p^{m_\alpha-m_i}}\right)^{p^{m_i}} = 1_A$. Agora, fazendo o produto destes elementos por todos os elementos de A cuja ordem $\leq p^{m_i-1}$, obtemos todos os elementos de A cuja ordem $\leq p^{m_i}$ e cuja p^{m_i-1}-ésima potência pertence a $\langle A_{\alpha,\beta}\rangle$.

Logo

$$M_{i,k} = |\Omega_{m_i}(A)| - p^{\lambda_1+\cdots+\lambda_{i-1}+k-1}|\Omega_{m_i-1}(A)|.$$

Ademais, como $m_{i-1} > m_i > m_{i+1}$, então ou $m_{i-1} > m_i - 1 > m_{i+1}$ ou $m_{i+1} \leq m_i - 1 > m_{i+2}$ e ambos os casos nos dão o mesmo resultado. Considere assim o caso em que $m_{i+1} \leq m_i - 1 > m_{i+2}$. Logo

$$\begin{aligned}
M_{i,k} &= |\Omega_{m_i}(A)| - p^{\lambda_1+\cdots+\lambda_{i-1}+k-1}|\Omega_{m_i-1}(A)| \\
&= p^{(\lambda_1+\cdots+\lambda_i)m_i+\lambda_{i+1}m_{i+1}+\cdots+\lambda_t m_t} - p^{\lambda_1+\cdots+\lambda_{i-1}+k-1}p^{(\lambda_1+\cdots+\lambda_{i+1})(m_i-1)+\lambda_{i+2}m_{i+2}+\cdots+\lambda_t m_t} \\
&= p^{(\lambda_1+\cdots+\lambda_i)m_i+\lambda_{i+1}m_{i+1}+\cdots+\lambda_t m_t} - p^{\lambda_1+\cdots+\lambda_{i-1}+k-1}p^{(\lambda_1+\cdots+\lambda_i)(m_i-1)+\lambda_{i+1}m_{i+1}+\cdots+\lambda_t m_t} \\
&= p^{(\lambda_1+\cdots+\lambda_i)m_i+\lambda_{i+1}m_{i+1}+\cdots+\lambda_t m_t} - p^{(\lambda_1+\cdots+\lambda_i)(m_i)+\lambda_{i+1}m_{i+1}+\cdots+\lambda_t m_t-\lambda_i+k-1} \\
&= p^{n_i} - p^{n_i-\lambda_i+k-1}.
\end{aligned}$$

Portanto,

$$\begin{aligned}
|Aut(A)| &= \prod_{i=1}^{t}\prod_{k=1}^{\lambda_i}\left(p^{n_i} - p^{n_i-\lambda_i+k-1}\right) \\
&= \prod_{i=1}^{t}\prod_{j=1}^{\lambda_i}\left(p^{n_i} - p^{n_i-j}\right).
\end{aligned}$$

■

Exemplo 3.4.8 *Seja $H_2 = \mathbb{Z}_{2^3} \times \mathbb{Z}_2$. Vamos agora encontrar o número de elementos de $Aut(H_2)$ usando o Teorema 3.4.7.*

Considere $H_2 = \mathbb{Z}_{2^3} \times \mathbb{Z}_2$ com $H_2 = \langle a, b \mid a^7 = b^2 = 1_{H_2} \rangle$, ou seja, $\mathbb{Z}_{2^3} = \langle a \rangle$ e $\mathbb{Z}_2 = \langle b \rangle$. Nestas condições

$$H_2 = \{1_{H_2}, a, a^2, a^3, a^4, a^5, a^6, a^7, b, ab, a^2b, a^3b, a^4b, a^5b, a^6b, a^7b\}.$$

Observe que H_2 possui:

- 8 *elementos de ordem* 8, *a saber,*

$$a, a^3, a^5, a^7, ab, a^3b, a^5b, a^7b.$$

- 4 *elementos de ordem* 4, *a saber,*

$$a^2, a^6, a, a^2b, a^6.$$

- 3 *elementos de ordem* 2, *a saber,*

$$a^4, b, a^4b$$

  e o elemento neutro.

O grupo de automorfismos $Aut(H_2)$ fica completamente determinado pelas imagens $\varphi(a)$ e $\varphi(b)$, onde φ é um automorfismo de H_2. Assim, para encontrarmos a ordem de $Aut(H_2)$, precisamos encontrar o número de possibilidades para $\varphi(a)$ e $\varphi(b)$. Ora, para $\varphi(a)$ temos 8 *possibilidades, uma vez que a única exigência que temos é que $\varphi(a)$ e a tenham a mesma ordem. Agora escolhida uma imagem $\varphi(a)$, quantas possibidades existem para $\varphi(b)$? Tais elementos devem ter a mesma ordem que b, ou seja, ordem* 2 *e não podem pertencer ao subgrupo $\langle a \rangle$. Logo existem* 2 *possibilidades para $\varphi(b)$, a saber, b, a^4b. Portanto,*

$$|Aut(H_2)| = 8 \cdot 2 = 16.$$

A seguir, descrevemos todos os automorfismos de $H_2 = \mathbb{Z}_{2^3} \times \mathbb{Z}_2$.

$$I_d: \begin{array}{rcl} a & \mapsto & a \\ b & \mapsto & b \end{array} \qquad \varphi_1: \begin{array}{rcl} a & \mapsto & a^3 \\ b & \mapsto & b \end{array} \qquad \varphi_2: \begin{array}{rcl} a & \mapsto & a^5 \\ b & \mapsto & b \end{array} \qquad \varphi_3: \begin{array}{rcl} a & \mapsto & a^7 \\ b & \mapsto & b \end{array}$$

$$\varphi_4: \begin{array}{rcl} a & \mapsto & ab \\ b & \mapsto & b \end{array} \qquad \varphi_5: \begin{array}{rcl} a & \mapsto & a^3b \\ b & \mapsto & b \end{array} \qquad \varphi_6: \begin{array}{rcl} a & \mapsto & a^5b \\ b & \mapsto & b \end{array} \qquad \varphi_7: \begin{array}{rcl} a & \mapsto & a^7b \\ b & \mapsto & b \end{array}$$

$$\varphi_8 : \begin{array}{rcl} a & \mapsto & a \\ b & \mapsto & a^4b \end{array} \qquad \varphi_9 : \begin{array}{rcl} a & \mapsto & a^3 \\ b & \mapsto & a^4b \end{array} \qquad \varphi_{10} : \begin{array}{rcl} a & \mapsto & a^5 \\ b & \mapsto & a^4b \end{array} \qquad \varphi_{11} : \begin{array}{rcl} a & \mapsto & a^7 \\ b & \mapsto & a^4b \end{array}$$

$$\varphi_{12} : \begin{array}{rcl} a & \mapsto & ab \\ b & \mapsto & a^4b \end{array} \qquad \varphi_{13} : \begin{array}{rcl} a & \mapsto & a^3b \\ b & \mapsto & a^4b \end{array} \qquad \varphi_{14} : \begin{array}{rcl} a & \mapsto & a^5b \\ b & \mapsto & a^4b \end{array} \qquad \varphi_{15} : \begin{array}{rcl} a & \mapsto & a^7b \\ b & \mapsto & a^4b. \end{array}$$

Considerações Finais

Neste trabalho, seguindo o artigo [2], descrevemos o anel $End(H_p)$ de endomorfismos do p-grupo abeliano finito H_p como um quociente de um subanel de matrizes $n \times n$ com entradas em $\mathbb{Z}$ e identificamos as unidades $Aut(H_p) \subseteq End(H_p)$. Como consequência dessa investigação, obtivemos prontamente uma fórmula para o número de elementos de $Aut(G)$ para qualquer grupo abeliano finito G (Teorema 3.3.2). Apresentamos também uma outra fórmula para o número de elementos de $Aut(G)$ que foi apresentada por Otto Schreier em 1926, no artigo *Über die Erweiterung von Gruppen II* [10]. Em ambos os casos, os invariantes do p-grupo são fundamentais para determinar a ordem do grupo de automorfismos de G. No entanto, em [10], para se conhecer sobre o número de elementos de $Aut(G)$ é suficiente conhecer a estrutura de certos subgrupos característicos de G.

Conhecendo a ordem do grupo de automorfismos de um grupo abeliano finito G, podemos obter informações sobre $Aut(G)$, como por exemplo, resultados sobre os seus p-subgrupos de Sylow e algumas estimativas sobre os subgrupos de Frattini do grupo G, dentre outras informações.

A importancia de estudar o grupo de automorfismos $Aut(G)$ é que este tem aplicações em várias áreas da Matemática, tais como Teoria dos Grupos Finitos, Teoria de Representação de Grupos e Álgebras, K-Teoria, Combinatória, Geometria e Códigos Corretores de Erros. Isto, por si só, já é uma boa motivação para prosseguir os estudos na direção desta dissertação.

Referências Bibliográficas

[1] GARCIA, A. and LEQUAIN, Y. *Elementos de Álgebra*. 6ª edição, IMPA, Rio de Janeiro, 2012.

[2] HILLAR, C. J., RHEA, D. L. *Automorphisms of finite abelian groups*. American Mathematical Monthly 114 n. 10 (2007) 917-923.

[3] HUNGERFORD, T. W., *Algebra, Graduate Texts in Mathematics 73.* Springer-Verlag, New York, 1974.

[4] HUPPERT, B., *Endliche Gruppen I.* Springer-Verlag, New York, 1967.

[5] KUHN, H., *Endomorphismem abelscher p-Gruppen.* Dissertation zur Erlangung des Grades eines Doktors der naturwissenschaften, dem fachbereich mathematik der Eberhard-Karls-Universität zu Tübingen , Tübingen, 1975.

[6] MONTEIRO, L.H. J., *Elementos de Álgebra.* 2ªedição, Livros Técnicos e Científicos, Rio de Janeiro, 1978.

[7] ROTMAN, J. J., *An Introduction to the Theory of Groups, Graduate Texts in Mathematics 148.* Springer-Verlag, New York, 1994.

[8] MARTIN, P. A. *Grupos, Corpos e Teoria de Galois*. Editora Livraria da Física, São Paulo, 1971.

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

[10] SCHREIER, O., *Über die Erweiterung von Gruppen II.* Abh. Math. Sem. Univ. Hamburg 6 (1926) 321-346.