Universidade Federal de Uberlândia
Instituto de Matemática e Estatística
Curso de Graduação em Matemática

O PROBLEMA DE SOMA ZERO PARA GRUPOS ABELIANOS FINITOS.

João Victor Alvino

Uberlândia-MG
2023

João Victor Alvino

O PROBLEMA DE SOMA ZERO PARA GRUPOS ABELIANOS FINITOS.

Monografia apresentada ao Curso de Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **BACHARELADO EM MATEMÁTICA**.

Área de concentração: Matemática
Linha de pesquisa: Teoria de grupos

Orientador(a): Victor Gonzalo Lopez Neumann

Uberlândia-MG
2023

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

B295 2024

Baruselli, Joao Victor Alvino Sampaio, 2002-
O problema da soma zero para grupos abelianos finitos [recurso eletrônico] / Joao Victor Alvino Sampaio Baruselli. - 2024.

Orientador: Victor Gonzalo Lopez Neumann.
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Uberlândia, Graduação em Matemática.
Modo de acesso: Internet.
Inclui bibliografia.

1. Matemática. I. Neumann, Victor Gonzalo Lopez ,1974-, (Orient.). II. Universidade Federal de Uberlândia. Graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:

Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Instituto de Matemática e Estatística
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.famat.ufu.br - famat@ufu.br

ATA DE DEFESA - GRADUAÇÃO

Curso de Graduação em:	Bacharelado em Matemática				
Defesa de:	Trabalho de Conclusão de Curso 2 (FAMAT 31804)				
Data:	24/04/2024	Hora de início:	15:00	Hora de encerramento:	16:45
Matrícula do Discente:	12011MAT018				
Nome do Discente:	João Victor Alvino Sampaio Baruselli				
Título do Trabalho:	O Problema de Soma Zero para Grupos Abelianos Finitos				
A carga horária curricular foi cumprida integralmente?	(X) Sim ( ) Não				

Reuniu-se na Sala 1F129, Campus Santa Mônica, da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Curso de Graduação em Matemática, assim composta: Professores:Josimar Joao Ramirez Aguirre-IME/UFU; Alonso Sepúlveda Castellanos-IME/UFU; Victor Gonzalo Lopez Neumann-IME/UFU, orientador do candidato.

Iniciando os trabalhos, o presidente da mesa, Dr Victor Gonzalo Lopez Neumann, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra, para a exposição do seu trabalho. A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do curso.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato:

(X) Aprovado Nota [95] (noventa e cinco)

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 24/04/2024, às 17:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alonso Sepulveda Castellanos**, **Professor(a) do Magistério Superior**, em 25/04/2024, às 08:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Josimar João Ramirez Aguirre**, **Professor(a) do Magistério Superior**, em 25/04/2024, às 14:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5365947** e o código CRC **B5084867**.

Referência: Processo nº 23117.028936/2024-79 SEI nº 5365947

Agradecimentos

Agradeço a minha família pelo apoio e a motivação para procurar ensino superior, em especial agradeço aos meus pais pelo apoio financeiro e emocional me permitindo prosseguir com a educação superior.

Agradeço aos meus amigos por me ajudarem nas matérias que eu tinha dificuldade e pelo companheirismo na jornada.

Agradeço aos meus colegas de sala pela companhia durante as aulas.

Agradeço ao corpo docente do IME pelas aulas.

Resumo

O foco desse trabalho é o estudo da constante de Davenport e problemas de soma zero. Para poder introduzir e definir os problemas a serem estudados, será feita uma revisão de alguns conceitos sobre teoria de grupos e também alguns resultados específicos sobre grupos abelianos finitos que não costumam ser estudados durante a graduação. A constante de Davenport está relacionada à resolução de problemas de soma zero em grupos abelianos finitos. Com o objetivo de calcular a constante de Davenport serão também utilizadas propriedades de contagem e de anéis.

Palavras-chave: Grupos Abelianos Finitos; Constante de Davenport; Sequências de Soma Zero; Sequências de Produto Um.

Abstract

The focus of this work is to study the Davenport's constant and zero-sum problems. In order to introduce and define the problems to be studied, a review of some concepts in group theory will be done, along with some specific results on finite abelian groups that are not commonly covered in undergraduate studies. The Davenport's constant is associated with the resolution of zero-sum problems in finite abelian groups. To calculate the Davenport's constant of abelian groups, properties of counting and ring properties will also be utilized.

Keywords: Finite Abelian Groups; Davenport's Constant, Zero Sum Sequencies; Product One Sequencies.

Sumário

Introdução

Em 1966, durante uma conferência sobre teoria dos grupos e teoria dos números (ver [9, 4]), Thomas H. Davenport apontou que a constante de Davenport de um grupo de classes G de um corpo de números F é igual ao máximo número de ideais primos (contando multiplicidade) que aparecem na decomposição de um inteiro irredutível de F. Em geral, a constante de Davenport de um grupo G é o menor inteiro positivo k tal que toda sequência com comprimento maior ou igual que k possui uma subsequência de soma zero. Essa constante tem papéis importantes na teoria de fatoração não única e possui uma conexão com a teoria de grafos.

Porém, logo após a introdução da constante de Davenport, surgiu o problema de como determiná-la, o qual ficou conhecido como o problema de soma zero em grupos abelianos finitos. O interesse por esse problema levou ao descobrimento de diversos teoremas que permitem encontrar a constante de Davenport em certos grupos abelianos finitos. Estes teoremas serão o foco deste trabalho.

O descobrimento destes teoremas começou em 1968 com as publicações de John E. Olson (ver [9, 10]), em que Olson conseguiu provar teoremas que permitem o cálculo da constante de Davenport com grande facilidade. Como um breve exemplo, ele consegui provar que se um dado grupo G é isomorfo a $C_{p^{e_1}} \oplus C_{p^{e_2}} \oplus \cdots \oplus C_{p^{e_r}}$, em que p é um número primo, $e_1 \leq \cdots \leq e_r$ e $e_i \in \mathbb{N}$, para todo $1 \leq i \leq r$, então a constante de Davenport de G será dada por $1 + \sum_{i=1}^{r}(p^{e_i} - 1)$. Caso este resultado não existisse, o cálculo da constante teria que ser feito a mão, isto é, teria que se verificar que toda sequência de tamanho maior ou igual que $1 + \sum_{i=1}^{r}(p^{e_i} - 1)$ possui uma subsequência de soma zero, e que existem sequências de tamanho n que não possuem subsequência de soma zero, para todo $1 \leq n \leq 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$.

Este estudo continuou por muitos anos, com diversos artigos (ver [4, 1, 2]) sendo publicados nos anos e décadas subsequentes apresentando diversos resultados e auxiliando com o cálculo da constante de Davenport para diversos grupos. Porém, estes resultados normalmente dependem da classe de isomorfismo à qual o grupo pertence, sejam estes como o que foi apresentado anteriormente, ou com algum outro grupo distinto.

Então, para tentar aplicar estes resultados a um número maior de grupos abelianos finitos, também serão enunciados e demonstrados uma série de teoremas sobre grupos abelianos finitos. Estes terão o intuito de provar o teorema fundamental de grupos abelianos finitos. Este teorema estabelece que para todo grupo abeliano finito G existem inteiros positivos $n(1),\ldots,n(k)$, tais que $G \cong \mathbb{Z}_{n(1)} \oplus \cdots \oplus \mathbb{Z}_{n(k)}$.

Este trabalho está organizado da seguinte maneira: no primeiro capítulo será feita uma revisão de conceitos básicos sobre teoria de grupos e grupos abelianos finitos. No segundo, teoremas sobre grupos abelianos finitos serão enunciados e demonstrados, alguns dos quais não são vistos na graduação. E no terceiro, será realizado um estudo sobre a constante de Davenport e teoremas que permitem encontrá-la mais facilmente.

CAPÍTULO 1

Grupos Abelianos.

Antes de começar o estudo de grupos abelianos, comecemos relembrando a noção de relação de equivalência.

Definição 1.1 *Seja A um conjunto não vazio, uma relação $\sim$ sobre A será chamada de relação de equivalência de A, se para quaisquer $a, b, c \in A$ as seguintes propriedades forem cumpridas.*

1. $a \sim a$;
2. *Se* $a \sim b$, *então* $b \sim a$;
3. *Se* $a \sim b$ *e* $b \sim c$, *então* $a \sim c$.

Definição 1.2 *Seja A um conjunto e $\sim$ uma relação de equivalência de A, define-se classe de equivalência de a, como o conjunto $\overline{a} = \{x \in A \mid x \sim a\}$.*

Lembremos agora algumas definições e teoremas que foram apresentados na graduação para que possamos introduzir novos resultados.

Usaremos a notação usual de $\mathbb{Z}$ para denotar os números inteiros e $\mathbb{N}$ para denotar os números naturais.

Definição 1.3 *Um conjunto não vazio G com uma operação binária $\cdot$ forma um grupo se cumpre as seguintes propriedades:*

1. $a, b \in G$ *implica* $a \cdot b \in G$ *(operação interna).*

2. *$a,b,c \in G$ implica $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (associatividade).*

3. *Existe um elemento $e \in G$ tal que $a\cdot e = e\cdot a = a$ para todo $a \in G$ (elemento neutro).*

4. *Para todo $a \in G$ existe um elemento $a^{-1} \in G$ tal que $a\cdot a^{-1} = a^{-1}\cdot a = e$ (elemento inverso).*

Se além das propriedades acima também tem-se que $a,b \in G$ implica $a\cdot b = b\cdot a$, para todo $a,b \in G$, então o grupo G é dito abeliano, essa propriedade é chamada de comutatividade.

Denotaremos um grupo G com uma operação binária $\cdot$ por $(G,\cdot)$ ou simplesmente por G, deixando subtendido que $\cdot$ é a operação.

Para um grupo G, um $g \in G$ e $i \in \mathbb{Z}$, define-se g na potencia i como:

$$g^i = \begin{cases} \underbrace{g\cdot g\cdots g}_{i \text{ vezes.}} & \text{, se } i > 0; \\ e & \text{, se } i = 0; \\ (g^{-1})^{-i} & \text{, se } i < 0. \end{cases}$$

As propriedades de potenciação usuais são válidas em um grupo, ou seja, se $a,b \in G$ e $i,j \in \mathbb{Z}$, então

$$a^i \cdot a^j = a^{i+j},$$

$$(a^i)^j = a^{ij},$$

$$(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}.$$

Se G é grupo abeliano, então também vale $(a\cdot b)^i = a^i \cdot b^i$.

A ordem de um grupo G é o número de elementos no grupo, e será denotada por $o(G)$. Caso a ordem de G seja finita, então diremos que G é um grupo finito. Se $a \in G$, então a ordem de a é o menor inteiro positivo m tal que $a^m = e$, caso m não exista então a tem ordem infinita. A ordem de a será denotada por $o(a)$.

A partir deste ponto, dado um grupo G e $a,b \in G$, denotaremos $a\cdot b$ simplesmente por ab, deixando subtendido que a operação entre os elementos a e b é a operação de G.

Definição 1.4 *Seja p um primo e G um grupo. Se todo elemento de G tem ordem igual a uma potencia de p, então G é chamado de p-grupo.*

Definição 1.5 *Um subconjunto H de um grupo G é chamado de subgrupo se, H forma um grupo com a operação de G. Caso H seja subgrupo de G, denotaremos $H \leq G$.*

Definição 1.6 *Para um grupo G e um elemento $g \in G$, definimos o conjunto de elementos gerados por g como $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$. O conjunto $\langle g \rangle$ é subgrupo de G.*

A demonstração que $\langle g \rangle$ é um subgrupo de G pode ser encontrada em [3, Proposição V.2.4]. Um grupo G é dito cíclico quando ele pode ser gerado por um elemento, isto é, $G = \langle g \rangle$, para algum $g \in G$. Denotaremos um grupo cíclico com n elementos por C_n, para que seja possível diferenciá-lo dos demais grupos com facilidade.

1.1 Propriedades dos Inteiros.

A relação de equivalência mais usada neste trabalho será a congruência módulo n definida em $\mathbb{Z}$, esta relação de equivalência é definida da seguinte forma: dados $x, y \in \mathbb{Z}$ diz-se que x é congruente a y módulo n se, e somente se, $x - y$ é um múltiplo de n. Caso x seja congruente a y módulo n, escreve-se $x \equiv y \pmod{n}$.

Definição 1.7 *Dado um $n \in \mathbb{N}$, o conjunto $\mathbb{Z}_n$ é o conjunto das classes de equivalência módulo n*

Proposição 1.8 *O conjunto $\mathbb{Z}_n$ com a operação de adição quociente dada por $\overline{a} + \overline{b} = \overline{a+b}$, para todos $a, b \in \mathbb{Z}$, é um grupo de ordem n.*

Demonstração: Ver [5, Teorema 6]. ■

Definição 1.9 *A função $|\cdot| : \mathbb{Z} \to \mathbb{Z}$, chamada de módulo, é definida da seguinte maneira: dado $x \in \mathbb{Z}$,*

$$|x| = \begin{cases} x & , \text{se } x \geq 0; \\ -x & , \text{se } x < 0. \end{cases}$$

Deve-se ter cuidado para não confundir a congruência módulo n com a função módulo, já que ambas tem nome similares mas são coisas diferentes.

Definição 1.10 *Para $a, b \in \mathbb{Z}$, dizemos que b divide a se, $a = bc$, para algum $c \in \mathbb{Z}$. Caso b divida a, denotaremos $b|a$.*

Teorema 1.11 (Divisão de Euclides) *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existem $n, r \in \mathbb{Z}$ tais que $a = nb + r$ e $0 \leq r < |b|$. Neste resultado, n e r são únicos.*

Demonstração: Ver [8, Theorem 1.1] ■

Definição 1.12 *O máximo divisor comum de dois números $a, b \in \mathbb{Z}$ é um número $c \in \mathbb{Z}$ tal que,*

1. *c é divisor comum de a e b;*
2. *Qualquer divisor de a e b é divisor de c.*

Denotaremos o máximo divisor comum de a e b por (a, b).

Definição 1.13 *O mínimo múltiplo comum de dois números $x, y \in \mathbb{Z}$ é um número $d \in \mathbb{Z}$ tal que,*

1. *$x|d$ e $y|d$;*
2. *Sempre que $x|z$ e $y|z$, então $d|z$.*

Denotaremos o mínimo múltiplo comum x e y por $[x, y]$.

1.2 Grupos Normais e Quocientes.

Seja G um grupo, $H \leq G$ e $g \in G$. Chamaremos o conjunto $Hg = \{hg \mid h \in H\}$ de classe lateral a direita de H em G que contém g. De forma análoga definiremos as classes laterais à esquerda de H.

Definição 1.14 *Seja G um grupo, se $H \leq G$, o índice de H em G é o número de classes laterais à direita de H em G. Denotaremos o índice de H em G por $[G : H]$.*

Definição 1.15 *Seja G um grupo e $H \leq G$, dizemos que H é um subgrupo normal de G, se para todo $g \in G$ e $h \in H$ tem-se $ghg^{-1} \in H$. Caso H seja subgrupo normal de G, denotaremos $H \lhd G$.*

Proposição 1.16 *Se $H \lhd G$, então o conjunto $G/H = \{Hg \mid g \in G\}$, com a operação herdada do grupo G, forma um grupo e é chamado de grupo quociente.*

Demonstração: A prova que G/H é grupo pode ser encontrada em [5, VI, Proposição 6]. ■

Definição 1.17 *Se G é um grupo, $H \lhd G$ e $H \neq G$, chamaremos H de subgrupo normal maximal se para todo $H \leq N \lhd G$, então $H = N$ ou $N = G$.*

Definição 1.18 *Se G é um grupo e $S \neq \emptyset$ um subconjunto de G, o centralizador de S em G é $C_G(S) = \{g \in G \mid g \cdot s = s \cdot g, \text{ para todo } s \in S\}$. Quando $S = G$, esse conjunto é chamado de centro de G e é denotado por $Z(G)$.*

Definição 1.19 *Se G é um grupo e H, N são subconjuntos não vazios de G, então o produto de H e N é o conjunto $HN = \{hn \in G \mid h \in H \text{ e } n \in N\}$.*

Definição 1.20 *Dados dois conjuntos não vazios A, B, definimos o produto cartesiano deles como o conjunto de todos os pares (a,b) em que $a \in A$ e $b \in B$. O produto cartesiano de A e B é denotado por $A \times B$. Além disso, para todos $(a,b),(c,d) \in A \times B$, tem-se $(a,b) = (c,d)$ se, e somente se $a = c$ e $b = d$.*

De forma geral, define-se o produto cartesiano $A_1 \times A_2 \times \cdots \times A_n$ de conjuntos não vazios $A_1, A_2, \ldots, A_n$, como sendo o conjunto de n-uplas ordenadas $(a_1, a_2, \ldots, a_n)$, em que $a_i \in A_i$, para todo $1 \leq i \leq n$.

Quando estivermos lidando com dois ou mais grupos, o elemento neutro do grupo G será denotado por e_G, para evitar confusão com os demais elementos neutros. Caso haja apenas um grupo, continuaremos denotando o elemento neutro por e.

Definição 1.21 *A soma direta de dois grupos A, B é o grupo $A \oplus B = (A \times B, *)$, em que $*$ é definida como $(x_1, x_2) * (y_1, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2)$, e $x_1, x_2 \in A$ e $y_1, y_2 \in B$.*

De forma geral, a soma direta de n grupos $A_1, A_2, \ldots, A_n$ será o grupo $A_1 \oplus A_2 \oplus \cdots \oplus A_n = (A_1 \times A_2 \times \cdots \times A_n, *)$, em que $*$ é definida como $(x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n) = (x_1 \cdot y_1, x_2 \cdot y_2, \ldots, x_n \cdot y_n)$, e $x_i, y_i \in A_i$, para todo $1 \leq i \leq n$.

Note que para todo $1 \leq i \leq n$ a operação $x_i \cdot y_i$ é a operação do grupo A_i. A prova de que $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ é grupo pode ser encontrada em [8, Theorem 3.19].

1.3 Funções e Isomorfismos.

Definição 1.22 *Uma função ϕ de G em H é dita sobrejetora se para todo $h \in H$, existe $g \in G$ tal que $\phi(g) = h$.*

Definição 1.23 *Uma função ϕ de G em H é dita injetora se quando $g_1 \neq g_2$, então $\phi(g_1) \neq \phi(g_2)$, para todo $g_1, g_2 \in G$.*

Se uma função é sobrejetora e injetora ao mesmo tempo, dizemos que ela é bijetora.

Definição 1.24 *Uma função ϕ de um grupo G para um grupo H é dita um homomorfismo se para todos $a, b \in G$ tem-se $\phi(ab) = \phi(a)\phi(b)$.*

Note que a operação ab está contida em G, enquanto a operação $\phi(a)\phi(b)$ está contida em H.

Definição 1.25 *Dois grupos G, H são ditos isomorfos se existe um homomorfismo bijetor (ou isomorfismo) entre eles. Neste caso escrevemos $G \cong H$.*

Definição 1.26 *Se ϕ é homomorfismo de G em H, o núcleo (ou kernel) de ϕ é definido por* $\ker(\phi) = \{x \in G \mid \phi(x) = e_H\}$.

As demonstrações dos próximos 4 resultados podem ser encontrados no Capítulo 2 de [6].

Teorema 1.27 *Seja ϕ um homomorfismo sobrejetor de G em H com* $\ker(\phi) = K$. *Então $G/K \cong H$.*

Teorema 1.28 (Teorema de Lagrange) *Se G é um grupo finito e $H \leq G$, então $o(H)$ divide $o(G)$.*

Corolário 1.29 *Se G é um grupo finito e $a \in G$, então $o(a)$ divide $o(G)$.*

Corolário 1.30 *Seja G um grupo e p um número primo. Se G tem p elementos, então G é cíclico de ordem p, ou seja $G \cong C_p$.*

Proposição 1.31 *Sejam H, K, H_1, K_1 grupos tais que H_1 é subgrupo normal de H e K_1 é subgrupo normal de K. Então*

$$(H \oplus K)/(H_1 \oplus K_1) \cong H/H_1 \oplus K/K_1.$$

Demonstração: Definimos $f : H \oplus K \longrightarrow H/H_1 \oplus K/K_1$, com $f(h,k) = (H_1 h, K_1 k)$. Veja que f é um homomorfismo de grupos sobrejetor tal que $\ker(f) = H_1 \oplus K_1$, de fato:

Sejam $(h,k), (\tilde{h}, \tilde{k}) \in H \oplus K$. Tem-se

$$f((h,k) * (\tilde{h}, \tilde{k})) = f(h \cdot \tilde{h}, k \cdot \tilde{k}) = (H_1(h \cdot \tilde{h}), K_1(k \cdot \tilde{k})) =$$

$$(H_1h \cdot H_1\tilde{h}, K_1k \cdot K_1\tilde{k}) = (H_1h, K_1k) * (H_1\tilde{h}, K_1\tilde{k}) =$$

$$f((h,k)) * f((\tilde{h},\tilde{k})).$$

Se $(H_1h, K_1k) \in H/H_1 \oplus K/K_1$ então $f(h,k) = (H_1h, K_1k)$. Ou seja f é sobrejetora e para $(h,k) \in H \oplus K$ tem-se

$$\begin{aligned}(h,k) \in \ker(f) &\Longleftrightarrow f(h,k) = (H_1, K_1)\\ &\Longleftrightarrow (H_1h, K_1k) = (H_1, K_1)\\ &\Longleftrightarrow h \in H_1 \text{ e } k \in K_1\\ &\Longleftrightarrow (h,k) \in H_1 \times K_1.\end{aligned}$$

Ou seja $\ker(f) = H_1 \oplus K_1$. Pelo Teorema 1.27 tem-se $(H \oplus K)/(H_1 \oplus K_1) \cong H/H_1 \oplus K/K_1$. ■

De modo geral esta proposição pode ser generalizada, resultando no teorema abaixo.

Teorema 1.32 *Seja $G_1, \ldots, G_k$ grupos com $N_j \lhd G_j$ para cada $1 \leq j \leq k$. Então $(G_1 \oplus \cdots \oplus G_k)/(N_1 \oplus \cdots \oplus N_k) \cong (G_1/N_1) \oplus \cdots \oplus (G_k/N_k)$.*

Demonstração: Ver [8, Theorem 6.9]. ■

Corolário 1.33 *Seja $G \cong H \oplus K$ e $Q \cong H_1 \oplus K_1$, em que H, K, H_1, K_1 grupos tal que H_1 é subgrupo de H, K_1 é subgrupo de K e $[H : H_1] = [K : K_1] = p$, então $G/Q \cong C_p \oplus C_p$.*

Demonstração: Como $[H : H_1] = [K : K_1] = p$, então $H/H_1 \cong C_p$ e $K/K_1 \cong C_p$. Pela proposição anterior, tem-se

$$G/Q \cong (H \oplus K)/(H_1 \oplus K_1) \cong H/H_1 \oplus K/K_1 \cong C_p \oplus C_p.$$

■

CAPÍTULO 2

Teorema Fundamental de Grupos Abelianos Finitos.

A determinação da estrutura de grupos finitos é um tema que fascina os matemáticos. Em geral, dada a ordem de um grupo finito, não é uma tarefa fácil determinar a estrutura desse grupo. Se o grupo for abeliano, o Teorema Fundamental de Grupos Abelianos Finitos responde a essa questão. No presente capítulo abordaremos a demonstração desse resultado.

Teorema 2.1 *Se G é um grupo, $g \in G$, e $o(g) = n \in \mathbb{N}$, então para $k \in \mathbb{Z} - \{0\}$, $o(g^k) = \frac{n}{(k,n)}$. Em particular, $o(g^k) = n$ se, e somente se $(k,n) = 1$.*

Demonstração: Ver [8, Theorem 2.8]. ■

Teorema 2.2 *Seja G um grupo e $x_1, x_2, \ldots, x_k \in G$ com todos $x_i x_j = x_j x_i$. Se $o(x_i)$ e $o(x_j)$ são coprimos, para todo $1 \leq i, j \leq k$, com $i \neq j$, então $o(x_1 x_2 \ldots x_k) = o(x_1)o(x_2)\ldots o(x_k)$.*

Demonstração: Ver [8, Theorem 4.16]. ■

Teorema 2.3 *Seja G um grupo e $g \in G$ com $o(g) = m$. Então $S = \{k \in \mathbb{Z} \mid g^k = e_G\} = m\mathbb{Z}$. Em particular, $g^k = e_G$ se, e somente se $m|k$.*

Demonstração: Ver [8, Theorem 2.7]. ■

Teorema 2.4 *Seja G um grupo abeliano finito, e seja $x \in G$ com $o(g) \leq o(x)$, para todo $g \in G$. Se $y \in G$, então $o(y)|o(x)$. Em outras palavras, $y^{o(x)} = e$, para todo $y \in G$.*

Demonstração: Suponha que existe $y \in G$ tal que $o(y)$ não divide $o(x)$. Pela fatoração única nos naturais, existe um primo q que aparece na fatoração de $o(y)$ e não aparece (ou aparece com potência menor) na fatoração de $o(x)$. Isto é, existem números naturais m,k e inteiros não negativos s,t tais que $o(x) = q^s k$, $o(y) = q^t m$, $(km,q) = 1$ e $t > s \geq 0$. Usando o Teorema 2.1, $o(x^{q^s}) = k$ e $o(y^m) = q^t$. Observe que $(o(x^{q^s}), o(y^m)) = 1$. Como G é um grupo abeliano, então $o(x^{q^s} y^m) = q^t k$, pelo Teorema 2.2. Isso contradiz a maximalidade de $o(x)$, então devemos concluir que $o(y)|o(x)$ e pelo Teorema 2.3 segue que $y^{o(x)} = e$. ■

Teorema 2.5 *Seja G um grupo, então:*

- *Se $H \leq Z(G)$ e $K \leq G$, então $HK \leq G$;*
- *Se G é abeliano e $H_1, \ldots, H_m \leq G$, então $H_1 \cdots H_m \leq G$.*

Demonstração: Ver [8, Theorem 4.11]. ■

Teorema 2.6 *Se $H,K \lhd G, HK = G$ e $H \cap K = \langle e \rangle$, então $G \cong H \oplus K$.*

Demonstração: Ver [8, Theorem 7.9]. ■

Teorema 2.7 *Se $C = \langle g \rangle$ é infinito, então $C \cong (\mathbb{Z}, +)$, e se $o(C) = n$, então $C = C_n \cong \mathbb{Z}_n$.*

Demonstração: Ver [8, Theorem 6.8]. ■

Teorema 2.8 *Para A, B, C, D, E grupos, com $A \cong C$ e $B \cong D$, temos $A \oplus B \cong B \oplus A, A \oplus B \cong C \oplus D$, e $A \oplus B \oplus E \cong (A \oplus B) \oplus E \cong A \oplus (B \oplus E)$.*

Demonstração: Ver [8, Theorem 7.10]. ■

Teorema 2.9 *Se $G = N_1 \cdots N_k$, $N_i \lhd G$, para todo $1 \leq i \leq k$, e se $N_1 N_2 \ldots N_{j-1} \cap N_j = \{e\}$ quando $k \geq j \geq 2$, então $G \cong N_1 \oplus \cdots \oplus N_k$. Por outro lado, se $G \cong G_1 \oplus \cdots \oplus G_k$ existem $N_1, \ldots, N_k \lhd G, N_i \cong G_i, G = N_1 \cdots N_k$ e $N_1 N_2 \cdots N_{j-1} \cap N_j = \{e\}$ para cada $k \geq j \geq 2$.*

Demonstração: Ver [8, Theorem 7.8]. ■

Teorema 2.10 (Fundamental dos Grupos Abelianos Finitos) *Se G é um grupo abeliano finito, então existem inteiros positivos $n(1), \ldots, n(k)$, tais que $G \cong \mathbb{Z}_{n(1)} \oplus \cdots \oplus \mathbb{Z}_{n(k)}$, e $n(j)|n(j-1)$ para todo $2 \leq j \leq k$.*

Demonstração: Como G é um grupo abeliano, podemos dizer que qualquer $H \leq G$ é normal e G/H é um grupo. Temos também que o Teorema 2.5 é válido e que $(xy)^m = x^m y^m$ para quaisquer $x, y \in G$.

Algum $x_1 \in G$ tem ordem máxima $n(1)$. Se $G = \langle x_1 \rangle$, então $o(G) = n(1)$ e $G \cong \mathbb{Z}_{n(1)}$ pelo Teorema 2.7. Caso contrário, defina $H_1 = \langle x_1 \rangle$. Para algum y $\in G$, $o(H_1 y) = m$ é máximo em G/H_1. Já que $G \neq H_1$, então $m > 1$, $y \notin H_1$, e $y^m \in H_1$ com m sendo a miníma potência de y satisfazendo essa propriedade. Observe que $(H_1 y)^{o(y)} = H_1 y^{o(y)} = H_1$, logo $m | o(y)$ pelo Teorema 2.3, e $o(y) | n(1)$ pelo Teorema 2.4. Assim, por transitividade $m | n(1)$ e podemos escrever $n(1) = ms$.

Como $y^m \in H_1$ então $y^m = x_1^k$, usando o Teorema da divisão de Euclides é possível escrever $k = qm + j$ com $0 \leq j < m$, o que resulta em $y^m = x_1^{mq} x_1^j$. Portanto, se $x_2 = x_1^{-q} y$, então $H_1 y = H_1 x_2$, e assim $o(H_1 x_2) = m$ em G/H_1, mas usando o Teorema 2.4 de novo, $e = x_2^{n(1)} = x_2^{ms} = ((x_1^{-q} y)^m)^s = x_1^{js}$. Pelo Teorema 2.3 tem-se que $n(1) | js$, mas $0 \leq j < m$ implica que $0 \leq js < n(1)$. Desta forma $j = 0$ e $x_2^m = (x_1^{-q} y)^m = x_1^{-qm} y^m = e$.

Já que $m = o(H_1 x_2)$ então $\langle x_1 \rangle \cap \langle x_2 \rangle = \langle x_2^m \rangle = \{e\}$, como mencionado acima. Além disso, $o(x_2) | m$, o que permite usar o Teorema 2.3, e $m \leq o(x_2)$ já que $m = o(H_1 x_2)$, então $o(x_2) = m$.

Defina $H_2 = \langle x_2 \rangle$ e $n(2) = m$ então $n(2) | n(1)$ e $H_1 \cap H_2 = \langle e \rangle$. Se $G = H_1 \oplus H_2$ então pelo Teorema 2.6, Teorema 2.7 e Teorema 2.8, teremos $G \cong \langle x_1 \rangle \oplus \langle x_2 \rangle \cong \mathbb{Z}_{n(1)} \oplus \mathbb{Z}_{n(2)}$, acabando a demonstração.

Quando $G \neq H_1 \oplus H_2$ continuamos com o mesmo processo. O passo geral é como a demonstração acima mas as condições iniciais são um pouco mais complicadas. Suponha que existe um conjunto maximal $\{x_1, x_2, ..., x_k\} \subseteq G$ tal que $o(x_i) = n(i)$; $n(i) | n(i-1)$ para todo $2 \leq i \leq k$ e, denotando $H_0 = \langle e \rangle$ e $H_j = \langle x_1 \rangle \cdots \langle x_j \rangle$, para $j \leq k$, temos $o(H_{j-1} x_j) = n(j)$, em que $n(j)$ é a ordem máxima entre as ordens de todos elementos de G/H_{j-1}. Observe que quando G não é cíclico temos $k \geq 2$. É claro que k tem que ser finito pois G é finito. Já que $o(x_j) = n(j) = o(H_{j-1} x_j)$ e $H_{j-1} \cap \langle x_j \rangle = \langle x_j^{n(j)} \rangle = \langle e \rangle$, então $H_k \cong \langle x_1 \rangle \oplus \cdots \oplus \langle x_k \rangle$ pelo Teorema 2.9. Consequentemente se $G = H_k$, então $\langle x_i \rangle \cong \mathbb{Z}_{n(i)}$, para todo $1 \leq i \leq k$, e pelo Teorema 2.8 o teorema está provado.

Quando $G \neq H_k$, contradizemos a maximalidade de k encontrando x_{k+1}, em que x_{k+1} satisfaz $o(x_{k+1}) | n(k)$ e $o(H_k x_{k+1}) = o(x_{k+1})$ é ordem máxima entre as ordens de G/H_k. Podemos afirmar que para algum $y \in G$, $o(H_k y) = m$, sendo m a máxima ordem possivel dos elementos em G/H_k. Agora pela definição de $n(k)$ e o teorema da divisão de Euclides tem-se que $y^{n(k)} \in H_{k-1} \leq H_k$, então $(H_k y)^{n(k)} = H_k$ e pelo Teorema 2.3 conclui-se que $m | n(k)$. Embora $y^m \in H_k$, pode ser que $y^m \in H_j \leq H_k$ para $j < k$. Entre todos os elementos $x \in G$ que satisfazem $o(H_k x) = m$ em G/H_k, existe $x \in G$ tal que $x^m \in H_j$ para o qual j é mínimo. Isto é, se $g \in G$ com $o(H_k g) = m$ então $g^m \notin H_{j-1}$ (se $j > 0$). Sem perda de generalidade podemos assumir que a escolha inicial de $y \in G$ satisfaz essa condição. Se

$j=0$, então $y^m=e$. Já que $(H_k y)^t \neq H_k$ para $1 \leq t < m$ segue que $o(y)=m$. Daí, $H_k \cap \langle y \rangle = \langle y^m \rangle = \langle e \rangle$. De $m|n(k)$ e usando $x_{k+1}=y$, contradizemos a maximalidade de k, logo $j \geq 1$.

Pelas escolhas de y e j, tem-se que $y^m = x_1^{a(1)} x_2^{a(2)} \cdots x_j^{a(j)} = h x_j^{a(j)}$ com $h \in H_{j-1}$ e $a(j)>0$. Como foi visto acima $m|n(k)$ e por suposição $n(k)|n(j)$, logo $n(j)=ms$ e o teorema da divisão mostra que $a(j)=mq+v$, com $0 \leq v < m$. Agora $y^m = h x_j^{mq} x_j^v$, logo, se $w = x_j^{-q} y$ então $w^m = h x_j^v$. Observe que $H_k w = H_k y$ então $o(H_k w)=m$ e já que a ordem de qualquer elemento em G/H_{j-1} divide $n(j)$, teremos $w^{n(j)} \in H_{j-1}$. Mas $w^{n(j)} = w^{ms} = (h x_j^v)^s = h^s x_j^{vs} \in H_{j-1}$, fazendo com que $x_j^{-vs} \in H_{j-1}$. Logo $(H_{j-1} x_j)^{vs} = H_{j-1}$, e $n(j)|vs$ pelo Teorema 2.3, mas $0 \leq v < m$ força $vs < ms = n(j)$, então $v=0$. Consequentemente $w^m = h \in H_{j-1}$, o que contradiz a minimalidade de j. Isso mostra que $G \neq H_k$ não é possível, provando o teorema. ■

Ilustramos esse teorema com $o(G)=72$. Se $G = \oplus_{i=1}^k \mathbb{Z}_i$. Então $o(G)=n(1)...n(k)$ então precisamos apenas listar os fatores de 72.

Existem 6 possibilidades: 72; 36,2; 24,3; 18,2,2; 12,6; 6,6,2. Que correspondem as somas diretas: $\mathbb{Z}_{72}$; $\mathbb{Z}_{36} \oplus \mathbb{Z}_2$; $\mathbb{Z}_{24} \oplus \mathbb{Z}_3$; $\mathbb{Z}_{18} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$; $\mathbb{Z}_{12} \oplus \mathbb{Z}_6$; $e \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

Teorema 2.11 *Se G é um grupo e $H \neq \emptyset$ um subconjunto de G, então os seguintes itens são equivalentes:*

1. $H \leq G$.
2. $x,y \in H \Rightarrow xy, x^{-1} \in H$.
3. $x,y \in H \Rightarrow xy^{-1} \in H$.
4. $x,y \in H \Rightarrow x^{-1}y \in H$.

E se H é finito, então $H \leq G$ se, e somente se, $x,y \in H$ implicar $xy \in H$.

Demonstração: Ver [8, Theorem 2.12]. ■

Teorema 2.12 *Para $G_1,\ldots,G_k$ grupos, com $G = G_1 \oplus \cdots \oplus G_k$, então:*

1. $Z(G_1 \oplus \cdots \oplus G_k) = Z(G_1) \oplus \cdots \oplus Z(G_k)$.
2. *Se G_j, $1 \leq j \leq k$, é finito, então* $o(G) = o(G_1) \cdot o(G_2) \cdots o(G_k)$.
3. *Se* $g=(g_1,\ldots,g_k) \in G$, *então* $o(g)=n \in \mathbb{N} \iff o(g_i) \in \mathbb{N}$, *para* $1 \leq i \leq k$, *e* $n = \text{mmc}\{o(g_1),\ldots,o(g_k)\}$.

Demonstração: Ver [8, Theorem 3.20]. ■

Teorema 2.13 *Seja $G = \langle g \rangle$ um grupo com $o(G) = n$. Se $k \in \mathbb{N}$ e $k|n$ então $H_k = \langle g^{n/k} \rangle$ é o único subgrupo de G de ordem k, e*

$$\{H \mid H \text{ é subgrupo de } G\} = \{H_k \mid k \text{ é um divisor positivo de } n\}.$$

Logo, qualquer $H \leq G$ é cíclico, $o(H)|o(G)$, e existe um único subgrupo de G para cada $k|n$.

Demonstração: Ver [8, Theorem 3.1]. ■

Teorema 2.14 *Se G é um grupo e $g \in G$ então $o(g) = m \in \mathbb{N}$ se, e somente se $o(\langle g \rangle) = m$ e $\langle g \rangle = \{e_G, g, g^2, \ldots, g^{m-1}\}$. Logo se $o(g) = m$ então $\langle g^k \rangle = \langle g \rangle$ se, e somente se $(k, m) = 1$.*

Demonstração: Ver [8, Theorem 2.16]. ■

Teorema 2.15 *Se G é grupo e $N \lhd G$ então,*

1. *Se $o(G) = p^t$, com p primo e $t \in \mathbb{N}$, então $o(G/N) = p^k$, em que $k \in \mathbb{N}$ e $k < t$, a não ser que $N = \langle e \rangle$.*
2. *Se $y \in Z(G)$, então $Ny \in Z(G/N)$.*
3. *Se G é abeliano então G/N é abeliano.*
4. *Se $g \in G$ e $k \in \mathbb{Z}$, então $Ng^k = (Ng)^k$.*
5. *Se $G = \langle x \rangle$ é cíclico, então $G/N = \langle Nx \rangle$ é cíclico.*

Demonstração: Ver [8, Theorem 5.7]. ■

Para o próximo teorema temos que definir $\text{sub}(G, N)$ e $\text{sub}(G)$.

Definição 2.16 *Se G é um grupo e N é um subconjunto de G, $\text{sub}(G, N)$ é o conjunto de subgrupos de G que contém N e $\text{sub}(G)$ é o conjunto de subgrupos de G.*

Teorema 2.17 *Seja $\phi : G \to B$ um homomorfismo sobrejetor de grupos com $\ker\phi = N$. Então $\alpha : Sub(G, N) \to Sub(B)$ dado por $\alpha(H) = \phi(H)$ e $\beta : Sub(B) \to Sub(G, N)$ dado por $\beta(K) = \phi^{-1}(K)$ são inversos e bijetores que preservam inclusão, então:*

1. *α e β enviam subgrupos normais em subgrupos normais.*
2. *Se $N \leq H \leq L \leq G$, então $[L:H] = [\phi(L):\phi(H)]$.*
3. *Se $K \leq V \leq B$, então $[V:K] = [\phi^{-1}(V):\phi^{-1}(K)]$.*
4. *Se $H,L \in Sub(G,N), H \lhd L \iff \phi(H) \lhd \phi(L)$, então $L/H \cong \phi(L)/\phi(H)$.*
5. *Se $N \lhd L \leq G$, então $\phi(L) \cong L/N$.*
6. *Se $N \leq H \lhd G$, então $G/H \cong B/\phi(H)$.*
7. *Se N é finito e $K \leq B$ é finito, então $o(\phi^{-1}(K)) = o(N) \cdot o(K)$.*

Demonstração: Ver [8, Theorem 7.2]. ■

Teorema 2.18 *Seja G um grupo abeliano, com $o(G) = p^n$ e p primo. Se $G \cong \mathbb{Z}_{p^{n(1)}} \oplus \cdots \oplus \mathbb{Z}_{p^{n(k)}}$, em que $n(1) \geq \cdots \geq n(k) \geq 1$, e se $G \cong \mathbb{Z}_{p^{m(1)}} \oplus \cdots \oplus \mathbb{Z}_{p^{m(s)}}$, em que $m(1) \geq \cdots \geq m(s) \geq 1$, então $k = s$ e $n(j) = m(j)$, para todo $1 \leq j \leq s$.*

Demonstração: Seja $A = \mathbb{Z}_{p^{n(1)}} \oplus \cdots \oplus \mathbb{Z}_{p^{n(k)}}$ e $B = \mathbb{Z}_{p^{m(1)}} \oplus \cdots \oplus \mathbb{Z}_{p^{m(s)}}$. Argumentaremos por indução em n. Quando $n = 1$ certamente $k = s = 1$ e $n(1) = m(1) = 1$.

Assumimos que quando $o(G) = p^t$ para $t < n$ existe apenas uma representação para G, como no Teorema 2.10.

Seja $G(p) = \{g \in G | g^p = e\}$ e sejam $x, y \in G(p)$. Já que G é abeliano, $(xy)^p = x^p y^p = e$, G é finito e pelo Teorema 2.11 tem-se que $G(p) \leq G$, e $G(p)$ é unicamente determinado por G. Se $G(p) = G$, então $A(p) = A$ e $B(p) = B$, então $k = s = n$ e $n(i) = 1 = m(j)$, para todo $1 \leq i, j \leq n$. Quando $G(p) \neq G$ definimos $k \geq a \geq 1$ máximo com $n(a) > 1$ e $s \geq b \geq 1$ máximo com $m(b) > 1$. Pelo Teorema 2.12, $g \in A(p)$ exatamente quando cada uma de suas coordenadas g_j, tem-se $g_j^p = \overline{0}$. Em $\mathbb{Z}_{p^{n(i)}}$ existe um único $\langle \overline{x_i} \rangle \leq \mathbb{Z}_{p^{n(i)}}$ de ordem p pelo Teorema 2.13, $\langle \overline{x_i} \rangle = \mathbb{Z}_{p^{n(i)}}(p)$ pelo Teorema 2.14, e $\mathbb{Z}_{p^{n(i)}}/\langle \overline{x_i} \rangle$ é cíclico de ordem $p^{n(i)-1}$ pelo Teorema 2.15. Logo, pelo isomorfismo entre G e A tem-se, $G(p) \cong A(p) = \langle \overline{x_1} \rangle \oplus \cdots \oplus \langle \overline{x_k} \rangle$, então pela equivalência no Teorema 2.17 produz $G/G(p) \cong A/\oplus_{i=1}^{k} \langle \overline{x_i} \rangle$. Teorema 1.32, Teorema 2.7, Teorema 2.8 mostram que $G/G(p) \cong \mathbb{Z}_{p^{n(1)-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{n(a)-1}}$ e $o(G(p)) = o(A(p)) = p^k$. Analogamente, $G/G(p) \cong B/B(p) \cong \mathbb{Z}_{p^{m(1)-1}} \oplus \cdots \oplus \mathbb{Z}_{p^{m(b)-1}}$ e $p^s = o(B(p)) = o(G(p)) = p^k$, portanto $k = s$. Mas $o(G/G(p)) = p^t$ para $t < n$, então pela nossa suposição da indução, $a = b$ e $n(j) = m(j)$ para $1 \leq j \leq a$. Já que $n(i) = m(i) = 1$ para $a < i \leq k$, e assim o teorema é provado por indução. ■

Teorema 2.19 *Seja $n = p_1^{a_1} \cdots p_k^{a_k}$ para $p_1 < \cdots < p_k$ primos, e $a_i \in \mathbb{N}$, para $1 \leq i \leq k$.*

1. *Se $d \in \mathbb{N}$ então $d|n \Leftrightarrow d = p_1^{b_1} \cdots p_k^{b_k}$ com todo $0 \leq b_i \leq a_i$ para todo $1 \leq i \leq k$.*
2. *n tem exatamente $(a_1+1)(a_2+1)\cdots(a_k+1)$ divisores distintos em $\mathbb{N}$.*

Demonstração: Ver [8, Theorem 1.18]. ■

Teorema 2.20 *Se $n = n_1 \cdots n_k \in \mathbb{N}$, com $n_1, n_2, \ldots, n_k$ coprimos dois a dois, então $\rho : \mathbb{Z}_n \to \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ definido por $\rho(\overline{a}) = (\overline{a}, \ldots, \overline{a})$ é um isomorfismo.*

Demonstração: Ver [8, Theorem 7.11]. ■

Observe que no teorema acima, as classes de equivalência dependem do grupo em que se encontram, ou seja, $\overline{a}$ em $\mathbb{Z}_{n_i}$ é o conjunto de elementos congruentes a a modulo n_i, para todo $1 \leq i \leq k$.

Teorema 2.21 *Seja G um grupo abeliano finito, em que $G \cong \mathbb{Z}_{n(1)} \oplus \cdots \oplus \mathbb{Z}_{n(k)}$, com $n(j)|n(j-1)$ para todos $2 \leq j < k$, e a sequência $(n(1), \ldots, n(k))$ é unicamente determinada por G. Se $o(G) = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ para $p_1 < \cdots < p_t$ primos, então $G \cong \mathbb{Z}_{p_1^{\alpha(1,1)}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{\alpha(1,s(1))}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha(t,1)}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha(t,s(t))}}$, em que, $\alpha(i,1) \geq \cdots \geq \alpha(i,s(i))$ e a sequência $(\alpha(i,1), \alpha(i,2), \ldots, \alpha(i,s(i)))$ é unicamente determinada por G, para todo $1 \leq i \leq t$.*

Demonstração: Pelo Teorema 2.10, $G \cong \mathbb{Z}_{n(1)} \oplus \cdots \oplus \mathbb{Z}_{n(k)}$, com $n(j)|n(j-1)$ para $j \geq 2$. Pela fatoração de $o(G)$, existem inteiros $\alpha(i,j) \geq 0$, para todos $1 \leq i \leq t$ e $1 \leq j \leq k$, tais que $n(j) = p_1^{\alpha(1,j)} p_2^{\alpha(2,j)} \ldots p_t^{\alpha(t,j)}$.

Já que $n(j)|n(j-1)$, para $j \geq 2$, pelo Teorema 2.19, $\alpha(i,1) \geq \alpha(i,2) \geq \cdots \geq \alpha(i,k) \geq 0$, para todo $1 \leq i \leq t$. Logo, pelo Teorema 2.20, $\mathbb{Z}_{n(j)} \cong \mathbb{Z}_{p_1{}^{\alpha(1,j)}} \oplus \cdots \oplus \mathbb{Z}_{p_t{}^{\alpha(t,j)}}$, omitindo qualquer somando em que $\alpha(i,j) = 0$. Usando o Teorema 2.8, é possível rearranjar a soma:

$$G \cong \mathbb{Z}_{p_1^{\alpha(1,1)}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{\alpha(1,s(1))}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha(t,1)}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{\alpha(t,s(t))}},$$

em que $s(i)$ é o máximo inteiro, satisfazendo $\alpha(i,s(i)) > 0$. Seja A a soma direta acima (a direita). Para cada $1 \leq j \leq t$, defina $A_j = \{g \in A \mid o(g) = p_j^d$, para algum $d \geq 0\}$. Pelo Teorema 2.12(3.), tem-se que $x \in A_j$ se, e somente se, as coordenadas de x são zero, exceto, talvez, nas coordenadas das componentes $\mathbb{Z}_{p_j{}^{\alpha(j,v)}}$, para $1 \leq v \leq s(j)$. Dessa forma,

$$\mathbb{Z}_{p_j}^{\alpha(j,1)} \oplus \cdots \oplus \mathbb{Z}_{p_j}^{\alpha(j,s(j))} \cong A_j \cong G_j = \{g \in G | o(g) = p_j^d, \text{ para algum } d \geq 0\}.$$

Logo, pelo Teorema 2.18, $(p_j^{\alpha(j,1)},\ldots,p_j^{\alpha(j,s(j))})$ é unicamente determinado por G.

Isso prova a segunda afirmação do teorema. Se $G \cong \mathbb{Z}_{m(1)} \oplus \cdots \oplus \mathbb{Z}_{m(v)}$ com $m(j)|m(j-1)$ para $2 \leq j \leq v$, em que $m(j) = p_1^{b(1,j)} \ldots p_t^{b(t,j)}$, temos uma representação correspondente para G como uma soma direta de grupos cíclicos de ordens $p_i^{b(i,j)}$, para $1 \leq i \leq t$ e $1 \leq j \leq v$. Mas, como vimos acima, existe apenas uma única representação de cada G_j. Então, $\alpha(i,j) = b(i,j)$ para todos i e j, o que significa que $n(j) = m(j)$ para todo j, provando o teorema. ■

Definição 2.22 *Se G é um grupo abeliano finito, os inteiros $n(1),...,n(k)$ no teorema anterior são os* ***fatores invariantes*** *de G e seus divisores primos $p_j^{\alpha(j,i)}$, listados em ordem decrescente para cada primo, são os* ***divisores elementares*** *de G.*

Definição 2.23 *O expoente de um grupo finito G é definido como*

$$\exp(G) = \min\{m \in \mathbb{N} \mid g^m = e, \forall g \in G\}.$$

Teorema 2.24 *Um grupo abeliano finito G é cíclico se, e somente se, $o(G) = \exp(G)$.*

Demonstração: Se $G = \langle x \rangle$, então $o(x) = o(G)$ pelo Teorema 2.14, e certamente $\exp(G) \geq o(G)$. Mas $\exp(G) \leq o(G)$, pois todo elemento elevado a ordem do grupo é sempre a identidade. Assim, $\exp(G) = o(G)$.

Agora, definimos G como grupo abeliano com $n(1),\ldots,n(k)$ fatores invariantes. Pelo Teorema 2.21 e Teorema 2.12 nas ordens de soma direta, $g^{n(1)} = e$ para todo $g \in G$, então $\exp(G) \leq n(1)$. Portanto, $o(G) = \exp(G)$ implica $o(G) = n(1)$. Logo, $n(1)$ é o único fator invariante e $G \cong \mathbb{Z}_{o(G)}$ ■

Teorema 2.25 *Um grupo abeliano finito é cíclico se, e somente se, para cada primo p divisor de sua ordem, existem exatamente p elementos satisfazendo $x^p = e$.*

Demonstração: Se $G = \langle x \rangle$ e $p|o(G)$ com p primo, então G contém um único subgrupo H de ordem p (Teorema 2.13), e se $g \in G$ com $g^p = e$ então $g \in H$ pelo Teorema 2.14. Logo os p elementos de H são precisamente os elementos em G satisfazendo $x^p = e$. Agora, assuma que para qualquer p primo em que $p|o(G)$, o conjunto $\{x \in G | x^p = e\}$ tem exatamente p elementos. Se G tem mais de um fator invariante, então usando o Teorema 2.21, se o primo $q|n(2)$ temos que $q|n(1)$. Já que $G \cong \mathbb{Z}_{n(1)} \oplus \mathbb{Z}_{n(2)} \ldots$, e já que existem $\langle x \rangle \leq \mathbb{Z}_{n(1)}$ e $\langle y \rangle \leq \mathbb{Z}_{n(2)}$ com $o(\langle x \rangle) = o(\langle y \rangle) = q$, então existem q^2 elementos g em G que correspondem ao conjunto $\{(ix, jy, \overline{0}, \ldots, \overline{0}) \mid 0 \leq i, j \leq q-1\}$ e satisfazem $g^q = e$, contradizendo a nossa suposição. Logo, G tem apenas um único fator invariante, então $G \cong \mathbb{Z}_{n(1)}$ é cíclico. ■

CAPÍTULO 3

Constante de Davenport

3.1 Anéis e Monoides.

Definição 3.1 *Seja A um conjunto não vazio onde estejam definidas duas operações fechadas, denotas por $+$ e $\cdot$, as quais serão respectivamente chamadas de soma e produto em A. O conjunto A é um anel se as seguintes propriedades forem cumpridas para todos $a, b, c \in A$.*

1. $(a+b)+c = a+(b+c)$ *(associatividade da soma);*
2. *Existe* $0 \in A$ *tal que* $0+a = a+0 = a$ *(elemento neutro da soma);*
3. *Para todo* $a \in A$*, existe um único* $x = -a$ *tal que* $x+a = a+x = 0$ *(elemento inverso da soma);*
4. $a+b = b+a$ *(comutatividade da soma);*
5. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(associatividade do produto);*
6. $a \cdot (b+c) = a \cdot b + a \cdot c$ *e* $(a+b) \cdot c = a \cdot c + b \cdot c$ *(distributividade a direita e a esquerda);*

Além disso,

7. *se existe* $1 \in A$ *tal que* $1 \cdot a = a \cdot 1 = a$*, então A é chamado de anel com unidade;*
8. *Se* $a \cdot b = b \cdot a$*, para todos* $a, b \in A$*, então A é chamado de anel comutativo;*
9. *Se* $x, y \in A$ *tal que* $x \cdot y = 0$*, então* $x = 0$ *ou* $y = 0$*, caso isso ocorra dizemos que A é um anel sem divisores de zero.*

Caso A seja um anel comutativo, com unidade e sem divisores de zero, então dizemos que A é um domínio de integridade.

Definição 3.2 *Um monoide é um trio composto por:*

1. *Um conjunto G;*
2. *Uma operação binária fechada e associativa $\cdot$;*
3. *Um elemento neutro $e \in G$ tal que para todo $a \in G$ tem-se $a \cdot e = a = e \cdot a$.*

Dizemos que um monoide é abeliano se $a \cdot b = b \cdot a$, para todos $a, b \in G$.

3.2 Sequências e a Constante de Davenport.

Uma sequência em um grupo abeliano finito G é definida como:

$$S = \prod_{g \in G} g^{v_g(S)} = g_1 \cdot g_2 \cdots g_m \in \mathscr{F}(G),$$

em que $v_g(S) \in \mathbb{N}$ é o grau do elemento g na sequência S, ou seja a quantidade de vezes que g aparece na sequência, dizemos que g é um elemento de S se $v_g(S) > 0$. Observe que não importa a posição do elemento na sequência, mas sim o número de vezes que cada elemento aparece na sequência. Dessa forma, $\mathscr{F}(G)$ é um monoide abeliano formado pelo conjunto das sequências de G com a operação de concatenação de sequências, denotada por $\cdot$ e definida como

$$T \cdot S = t_1 \cdots t_n \cdot s_1 \cdots s_m = s_1 \cdots s_m \cdot t_1 \cdots t_n = S \cdot T,$$

para quaisquer sequências $T = t_1 \cdots t_n$ e $S = s_1 \cdots s_m$ de G. Por definição, a operação é interna e comutativa. Além disso, o elemento neutro de $\mathscr{F}(G)$ é a sequência vazia. Provemos que a operação é associativa. Sejam $T = t_1 \cdots t_n$, $S = s_1 \cdots s_m$ e $R = r_1 \cdots r_k$ sequências de G, então

$$(T \cdot R) \cdot S = t_1 \cdots t_n \cdot r_1 \cdots r_k \cdot S = t_1 \cdots t_n \cdot r_1 \cdots r_k \cdot s_1 \cdots s_m = T \cdot r_1 \cdots r_k \cdot s_1 \cdots s_m = T \cdot (R \cdot S).$$

Se a notação do grupo G é aditiva, define-se a soma dos elementos da sequencia S, como

$$\sigma(S) = \sum_{i=1}^{m} g_i.$$

Se a notação do grupo G é multiplicativa, define-se a produto dos elementos da sequencia S, como

$$\pi(S) = \prod_{i=1}^{m} g_i.$$

Diremos que a sequência S tem soma zero se $\sigma(S) = 0$, e diremos que tem produto um se $\pi(S) = 1$. O comprimento da sequência S é dada por:

$$|S| = \sum_{g \in G} v_g(S) \quad \text{ou} \quad |S| = m.$$

Uma sequência T é dita subsequência de S se $v_g(T) \leq v_g(S)$, para todo $g \in G$.

Definição 3.3 *A constante de Davenport de um grupo abeliano finito G, denotada por $D(G)$, é o menor inteiro positivo tal que toda sequência S de G em que $|S| \geq D(G)$ possui uma subsequência de soma zero (ou subsequência de produto um, caso a operação do grupo seja multiplicativa).*

Teorema 3.4 *Seja G um grupo abeliano finito. Então $D(G) \leq o(G)$.*

Demonstração: Consideremos $o(G) = n$ e $g_1 \cdot g_2 \cdots g_n$ uma sequência em G. Agora considere $i = 1, \ldots, n$ com $S_i = \sum_{k=1}^{i} g_k$. Se existe $1 \leq i \leq n$ tal que $S_i = 0$, então a prova está completa. Caso não exista, então existe $1 \leq i < j \leq n$ com $S_i = S_j$, ou seja:

$$g_1 + \cdots + g_i = g_1 + \cdots + g_i + g_{i+1} + \cdots + g_j \Rightarrow 0 = g_{i+1} + \cdots + g_j,$$

logo existe a subsequência $g_{i+1} \cdots g_j$ de soma zero para todo S_k com $j \leq k \leq n$, fazendo com que $j = D(G) \leq n$. ■

Para ilustrarmos a definição de constante de Davenport e o teorema acima, consideremos o seguinte exemplo: Dado o grupo $\mathbb{Z}_5$ (o grupo de inteiros módulo 5), podemos observar que $o(\mathbb{Z}_5) = 5$, pelo teorema 3.4, temos $D(\mathbb{Z}_5) \leq 5 = o(\mathbb{Z}_5)$, agora podemos observar que $1 \cdot 1 \cdot 1 \cdot 1 \cdot 1$ é uma sequência com soma zero em $\mathbb{Z}_5$, como a constante de Davenport tem que ser menor ou igual a 5 e a subsequência $1 \cdot 1 \cdot 1 \cdot 1$ não tem soma zero, então $|1 \cdot 1 \cdot 1 \cdot 1| = 4 < D(\mathbb{Z}_5) \leq 5 = o(\mathbb{Z}_5)$, como a constante de Davenport é inteira, teremos que $D(\mathbb{Z}_5) = 5$.

Teorema 3.5 *Dado um grupo $\mathbb{Z}_n$, teremos que $D(\mathbb{Z}_n) = n$.*

Demonstração: Pelo Teorema 3.4, sabemos que $D(\mathbb{Z}_n) \leq n = o(\mathbb{Z}_n)$. Agora consideremos a seguinte sequência de $\mathbb{Z}_n$:

$$S = 1 \cdot 1 \cdot 1 \cdots 1,$$

em que $|S| = n$. Como S tem n elementos, S tem uma subsequência T com x elementos, tal que $1 \leq x \leq n-1$, estes são todos 1, portanto teremos que $1 \leq \sigma(T) \leq n-1$, ou seja $\sigma(T) \neq 0$. Logo $n-1 < D(\mathbb{Z}_n) \leq n$, como a constante de Davenport tem que ser inteira, teremos que $D(\mathbb{Z}_n) = n$. ■

3.3 O anel de grupo $R[M]$.

Agora definiremos o anel de grupo $R[M]$, em que M é um monoide abeliano e R é um anel comutativo com unidade, em seguida provaremos que $R[M]$ se trata de um anel comutativo com unidade.

Definição 3.6 *Seja M um monoide abeliano com a notação multiplicativa e R um anel comutativo com unidade. Consideraremos $R[M]$ o conjunto de todas as funções $f : M \to R$ tal que $m \mapsto f(m)$, em que $f(m) \neq 0$ para um número finito de elementos $m \in M$.*

Definimos operações de soma e multiplicação em $R[M]$ da seguinte forma:

(a) $(f+g)(m) = f(m) + g(m)$;

(b) $(fg)(m) = \sum_{pq=m} f(p)g(q)$.

Uma observação é que no item (b), a soma percorre todos os pares (p,q) de elementos de M tais que $pq = m$.

Definimos 0 e 1 em $R[M]$ como as funções $0(m)$ e $1(m)$, respectivamente, em que $0(m) = 0$, para todo $m \in M$, e $1(m) = 1$, para $m = 1 \in M$, $1(m) = 0$, para $m \neq 1 \in M$.

Proposição 3.7 *Com as operações definidas acima, $R[M]$ é um anel comutativo com unidade.*

Demonstração: Consideremos $f, g, h \in R[M]$ e $m \in M$, então:

1. Como R é um anel comutativo e $f(m), g(m) \in R$, então $f(m) + g(m) = g(m) + f(m)$, logo:

$$(f+g)(m) = f(m) + g(m) = g(m) + f(m) = (g+f)(m).$$

2. Sabemos que $0(m) = 0 \in R$ é o elemento neutro de R, logo:

$$(f+0)(m) = (0+f)(m) = (0)(m) + f(m) = 0 + f(m) = f(m).$$

Portanto, o elemento neutro da soma existe em $R[M]$.

3. Como $f(m), g(m), h(m) \in R$, então $(f(m)+g(m))+h(m) = f(m)+(g(m)+h(m))$, logo

$$((f+g)(m))+h(m) = (f(m)+g(m))+h(m) = f(m)+(g(m)+h(m)) =$$

$$f(m)+((g+h)(m)).$$

portanto a associatividade é valida.

4. Como $f(m) \in R$ e R é anel, então $-f(m) \in R$, logo

$$(f+(-f))(m) = f(m)+(-f(m)) = 0 = 0(m).$$

5. Agora provaremos a associatividade da multiplicação.

$$((fg)h)(m) = \sum_{pq=m} (fg)(p)h(q) = \sum_{pq=m} \sum_{xy=p} (f(x)g(y))h(q) =$$

essa soma varia em x, y, q de tal forma que $xyq = m$, logo

$$\sum_{pq=m} \sum_{xy=p} (f(x)g(y))h(q) = \sum_{xyq=m} f(x)g(y)h(q)$$

Denotando $yq = p'$, podemos reescrever

$$\sum_{xyq=m} f(x)g(y)h(q) = \sum_{xp'=m} f(x)(\sum_{qy=p'} g(q)h(y)) =$$

$$\sum_{xp'=m} (f(x)(gh)(p')) = (f(gh))(m)$$

6. Primeiramente verificaremos a comutatividade da multiplicação, para facilitar a prova da distributividade. Como R é anel comutativo, temos

$$(fg)(m) = \sum_{pq=m} f(p)g(q) = \sum_{qp=m} g(q)f(p) = (gf)(m).$$

7. Agora podemos verificar que a multiplicação é distributiva. Veja que

$$[f(g+h)](m) = \sum_{pq=m} f(p)(g+h)(q) = \sum_{pq=m} f(p)(g(q)+h(q)).$$

Como a distributividade é valida em R, tem-se

$$\begin{aligned}[f(g+h)](m) &= \sum_{pq=m} f(p)g(q)+f(p)h(q) = \sum_{pq=m} f(p)g(q) + \sum_{pq=m} f(p)h(q) \\ &= (fg)(m)+(fh)(m) = [fg+fh](m).\end{aligned}$$

Ou seja, a distributividade é valida. A distributividade $(g+h)f = gf+hf$ segue diretamente da comutatividade e da prova acima.

8. O elemento neutro da multiplicação é $1(m)$,

$$(f1)(m) = \sum_{pq=m} f(p)1(q).$$

Como para $q \neq 1$, $1(q) = 0$, então

$$\sum_{pq=m} f(p)1(q) = f(m)1(1) = f(m)1 = f(m).$$

Assim, $(f1)(m) = (1f)(m) = f(m)$. Em outras palavras, $1(m)$ é a unidade de $R[M]$.

Portanto, $R[M]$ é um anel comutativo com unidade.

■

A partir de agora consideraremos $R = \mathbb{Z}$ e $M = G$, em que G é um grupo abeliano, e denotaremos as funções f de G em $\mathbb{Z}$, por

$$\sum_{g\in G} f(g)\cdot g.$$

Assim, por exemplo se $g_1, g_2, g_3 \in G$, o elemento $2g_1+3g_2-4g_3$ denota a função $f : G \longrightarrow \mathbb{Z}$ definida por $f(g_1) = 2$, $f(g_2) = 3$, $f(g_3) = -4$ e $f(g) = 0$, para todo $g \in G\backslash\{g_1, g_2, g_3\}$.

Observemos que $\mathbb{Z}[G]$ não é necessariamente um anel de integridade. Por exemplo, tomemos $G = C_2 = \{e, a\}$, com $a^2 = e$. Isso faz com que o elemento $f \in \mathbb{Z}[C_2]$ seja da forma

$$f(e)\cdot e + f(a)\cdot a.$$

Veja que

$$(1\cdot e+1\cdot a)\cdot(1\cdot e-1\cdot a)=(1\cdot 1+1\cdot(-1))\cdot e+(1\cdot(-1)+1\cdot 1)\cdot a=0\cdot e+0\cdot a=0,$$

sendo que $1\cdot e+1\cdot a\neq 0$ e $1\cdot e-1\cdot a\neq a$. Logo, existem divisores de 0 em grupos da forma $\mathbb{Z}[G]$.

3.4 Teoremas sobre a Constante de Davenport.

Agora provaremos alguns resultados que serão usados para demonstrar o próximo teorema.

Lema 3.8 *Sejam $n,j\in\mathbb{N}$ tais que $j\leq n-1$. Então*

$$\binom{n-1}{j}+\binom{n-1}{j-1}=\binom{n}{j}.$$

Demonstração: Por definição, temos

$$\binom{n-1}{j}+\binom{n-1}{j-1}=\frac{(n-1)!}{j!(n-1-j)!}+\frac{(n-1)!}{(j-1)!(n-1-(j-1))!}=$$

$$\frac{(n-1)!}{j!(n-j-1)!}+\frac{(n-1)!}{(j-1)!(n-j)!}=\frac{(n-1)!}{(j-1)!(n-j-1)!}\left(\frac{1}{j}+\frac{1}{(n-j)}\right)=$$

$$\frac{(n-1)!}{(j-1)!(n-j-1)!}\left(\frac{n-j+j}{j(n-j)}\right)=\frac{(n-1)!}{(j-1)!(n-j-1)!}\frac{n}{j(n-j)}=$$

$$\frac{n!}{j!(n-j)!}=\binom{n}{j}.$$

■

Proposição 3.9 *Seja A um anel comutativo com unidade, então para todos $a,b\in A$ e $n\in\mathbb{N}$ tem-se que*

$$(a+b)^n=\sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j}.$$

Demonstração: Claramente a proposição é valida para $n=0$ e $n=1$, já que

$$(a+b)^0=1 \text{ e } (a+b)^1=a+b,$$

logo consideremos $n\geq 2$ e suponha que a proposição vale para $n-1$. Assim, temos

$$(a+b)^n = (a+b)^{n-1}(a+b) = \left(\sum_{j=0}^{n-1}\binom{n-1}{j}a^j b^{n-1-j}\right)(a+b) =$$

$$\sum_{j=0}^{n-1}\binom{n-1}{j}a^{j+1}b^{n-1-j} + \sum_{j=0}^{n-1}\binom{n-1}{j}a^j b^{n-j} =$$

$$a^n + \sum_{j=0}^{n-2}\binom{n-1}{j}a^{j+1}b^{n-1-j} + b^n + \sum_{j=1}^{n-1}\binom{n-1}{j}a^j b^{n-j},$$

considerando $i = j+1$ e realizando uma mudança de variáveis na primeira soma, podemos escrever

$$\sum_{j=0}^{n-2}\binom{n-1}{j}a^{j+1}b^{n-1-j} = \sum_{i=1}^{n-1}\binom{n-1}{i-1}a^i b^{n-i}.$$

Dessa maneira, tem-se

$$(a+b)^n = a^n + \sum_{i=1}^{n-1}\binom{n-1}{i-1}a^i b^{n-i} + \sum_{j=1}^{n-1}\binom{n-1}{j}a^j b^{n-j} + b^n =$$

$$a^n + \sum_{j=1}^{n-1}\left(\binom{n-1}{j-1} + \binom{n-1}{j}\right)a^j b^{n-j} + b^n$$

e pelo Lema 3.8, temos

$$(a+b)^n = a^n + \sum_{j=1}^{n-1}\left(\binom{n-1}{j-1} + \binom{n-1}{j}\right)a^j b^{n-j} + b^n = \sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j}.$$

■

Antes de enunciarmos o próximo teorema lembremos que $\lfloor x \rfloor$ é definido como o maior inteiro menor que x. Ou seja,

$$\lfloor x \rfloor = n, \text{ onde } n \in \mathbb{Z} \text{ e para todo } m \in \mathbb{Z}, \text{ se } m \leq x, \text{ então } m \leq n.$$

Lema 3.10 *Sejam n um inteiro positivo, p um número primo e s um inteiro positivo tais que $p^s \leq n < p^{s+1}$. Então p aparece na fatoração de $n!$*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^s} \right\rfloor \text{ vezes.}$$

Demonstração: Veja que os múltiplos de p entre 1 e n são da forma jp, com $1 \leq j \leq \left\lfloor \frac{n}{p} \right\rfloor$, já que $\left\lfloor \frac{n}{p} \right\rfloor p$ é o maior múltiplo de p menor ou igual a n. Dessa forma, o fator p aparece $\left\lfloor \frac{n}{p} \right\rfloor$ vezes no

produto $n!$. Podemos observar que se um desses fatores múltiplo de p é também múltiplo de p^2, então ele deve ser contado duas vezes na fatoração de $n!$. Há $\left\lfloor \frac{n}{p^2} \right\rfloor$ múltiplos de p^2 entre 1 e n. Assim, contando os múltiplos de p e p^2 simultaneamente, o fator p aparece

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor$$

vezes entre 1 e n, na fatoração de $n!$.

Não podemos esquecer que os múltiplos de p^3, entre 1 e n, devem ser contados três vezes na fatoração de $n!$, e assim sucessivamente. Como p^s é a maior potência de p que é menor ou igual a n, temos que a potência de p que aparece na fatoração de $n!$ é

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^s} \right\rfloor.$$

■

Lema 3.11 *Sejam p um número primo e n, m inteiros positivos tais que $1 \leq m < p^n$. Então, $\binom{p^n}{m}$ é múltiplo de p.*

Demonstração: Como

$$\binom{p^n}{m} = \frac{(p^n)!}{(p^n - m)!m!},$$

devemos contar o número de vezes que o fator p aparece na fatoração de $(p^n)!$, $(p^n - m)!$ e $m!$. Pelo lema anterior, p aparece em $(p^n)!$

$$A = \left\lfloor \frac{p^n}{p} \right\rfloor + \cdots + \left\lfloor \frac{p^n}{p^n} \right\rfloor = p^{n-1} + \cdots + 1$$

vezes. Também pelo lema anterior, p aparece na fatoração de $m!$

$$B = \left\lfloor \frac{m}{p} \right\rfloor + \cdots + \left\lfloor \frac{m}{p^{n-1}} \right\rfloor$$

vezes. Finalmente, p aparece na fatoração de $(p^n - m)!$

$$C = \left\lfloor \frac{p^n - m}{p} \right\rfloor + \cdots + \left\lfloor \frac{p^n - m}{p^{n-1}} \right\rfloor$$

vezes. Dessa forma, $p^{A-(B+C)}$ é a máxima potência de p que aparece na fatoração de $\binom{p^n}{m}$.

Observe que para todo $1 \leq i \leq n-1$, temos

$$\frac{p^n - m}{p^i} + \frac{m}{p^i} = \frac{p^n}{p^i}.$$

Como, $\left\lfloor \frac{p^n-m}{p^i} \right\rfloor \leq \frac{p^n-m}{p^i}$ e $\left\lfloor \frac{m}{p^i} \right\rfloor \leq \frac{m}{p^i}$, então

$$\left\lfloor \frac{p^n - m}{p^i} \right\rfloor + \left\lfloor \frac{m}{p^i} \right\rfloor \leq \frac{p^n}{p^i} = p^{n-i}.$$

Assim,

$$B + C \leq \sum_{i=1}^{n-1} p^{n-i} = p^{n-1} + \cdots + p < p^{n-1} + \cdots + p + 1 = A.$$

Em outras palavras, $A - (B + C)$ é positivo, ou seja, $\binom{p^n}{m}$ é múltiplo de p. ■

Teorema 3.12 *Seja G um grupo isomorfo a $C_{p^{e_1}} \oplus C_{p^{e_2}} \oplus \cdots \oplus C_{p^{e_r}}$ com $1 \leq e_1 \leq \cdots \leq e_r$. Sejam também $g_1, \ldots, g_k \in G$, onde $k \geq 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$. Então,*

$$\prod_{i=1}^{k}(1 - g_i) = (1 - g_1)\cdots(1 - g_k) \equiv 0 \ (mod\ p).$$

Demonstração: Seja $\{x_1, \ldots, x_r\}$ uma base de G, onde x_i tem ordem p^{e_i}. Se para algum $1 \leq i \leq k$, $g_i = uv$, podemos "reduzir" o produto

$$J = (1 - g_1)\cdots(1 - g_i)\cdots(1 - g_k)$$

para a forma

$$\begin{aligned} J &= (1 - g_1)\cdots(1 - u + u(1 - v))\cdots(1 - g_k) \\ &= (1 - g_1)\cdots(1 - u)\cdots(1 - g_k) + u(1 - g_1)\cdots(1 - v)\cdots(1 - g_k), \end{aligned}$$

já que $1 - g_i = 1 - uv = 1 - u + u - uv = 1 - u + u(1 - v)$.

Agora considerando $g_i = x_1^{n_1} \cdots x_r^{n_r}$, podemos reescrever J da seguinte forma

$$\begin{aligned} J &= \alpha_1(1 - g_1)\cdots(1 - x_1)\ldots(1 - g_k) \\ &\quad + \alpha_2(1 - g_1)\cdots(1 - x_2)\ldots(1 - g_k) \\ &\quad + \cdots + \alpha_r(1 - g_1)\cdots(1 - x_r)\ldots(1 - g_k), \end{aligned}$$

onde $\alpha_1,\ldots,\alpha_r$ são elementos de $\mathbb{Z}[G]$. Repetindo esse processo para $g_1,\ldots,g_k$, podemos reescrever J como uma soma de elementos da forma

$$\alpha(1-x_{i_1})(1-x_{i_2})\cdots(1-x_{i_k}), \tag{3.1}$$

com $\alpha \in \mathbb{Z}[G]$. Agrupando essa expressão, temos

$$\alpha(1-x_{i_1})(1-x_{i_2})\cdots(1-x_{i_k}) = \alpha(1-x_1)^{f_1}\cdots(1-x_r)^{f_r},$$

onde f_i é o número de vezes que $(1-x_i)$ aparece na expressão (3.1). Em particular, pela construção segue que $f_1+\cdots+f_r = k \geq 1+\sum_{i=1}^{r}(p^{e_i}-1)$. Agora consideremos por absurdo que para todo $1 \leq i \leq r$ temos $f_i \leq p^{e_i}-1$. Então,

$$1+\sum_{i=1}^{r}(p^{e_i}-1) \leq k = \sum_{i=1}^{r} f_i \leq \sum_{i=1}^{r}(p^{e_i}-1).$$

Como isso é falso, existe $1 \leq i \leq r$ tal que $f_i \geq p^{e_i}$. Ou seja, J é uma soma de elementos da forma

$$\alpha(1-x_1)^{f_1}\cdots(1-x_r)^{f_r} = \alpha(1-x_i)^{p^{e_i}}(1-x_1)^{f_1}\cdots(1-x_i)^{f_i-p^{e_i}}\cdots(1-x_r)^{f_r}.$$

Para provar que $J \equiv 0 \pmod{p}$, basta provar que $(1-x_i)^{p^{e_i}} \equiv 0 \pmod{p}$, para todo $1 \leq i \leq r$.

Pela Proposição 3.9 e usando que $x_i^{p^{e_i}} = 1$, temos

$$(1-x_i)^{p^{e_i}} = \sum_{j=0}^{p^{e_i}} \binom{p^{e_i}}{j}(-x_i)^j = 1+\sum_{j=1}^{p^{e_i}-1}\binom{p^{e_i}}{j}(-x_i)^j + (-1)^{p^{e_i}}.$$

Pelo Lema 3.11, $\binom{p^{e_i}}{j}$ é múltiplo de p, para $1 \leq j < p^{e_i}$. Logo,

$$(1-x_i)^{p^{e_i}} \equiv 1+(-1)^{p^{e_i}} \pmod{p}.$$

Se p é ímpar, então $1+(-1)^{p^{e_i}} = 0$ e se p é par, então $p=2$ e $1+(-1)^{p^{e_i}} = 2 \equiv 0 \pmod{p}$. Em todos os casos, temos

$$(1-x_i)^{p^{e_i}} \equiv 0 \pmod{p}.$$

■

A partir deste ponto consideraremos os grupos estudados com notação multiplicativa, ou seja a constante de Davenport será o menor valor tal que toda sequência de tamanho maior que a constante tenha uma subsequência de produto 1.

Proposição 3.13 *Seja G um grupo isomorfo a $C_{p^{e_1}} \oplus C_{p^{e_2}} \oplus \cdots \oplus C_{p^{e_r}}$ com $1 \leq e_1 \leq \cdots \leq e_r$. Então*

$$D(G) \geq 1 + \sum_{i=1}^{r} (p^{e_i} - 1)$$

Demonstração: Precisamos mostrar uma sequência de tamanho $\sum_{i=1}^{r} (p^{e_i} - 1)$ que não possua subsequência com produto 1. Desta maneira, sejam $x_i \in G$, $C_{p^{e_i}} \cong \langle x_i \rangle$ para todo $1 \leq i \leq r$ e consideremos a sequência

$$S = x_1^{p^{e_1}-1} \cdots x_r^{p^{e_r}-1} \in \mathscr{F}(G).$$

Como $x_i^{\alpha_i} \neq 1$ para todo $1 \leq \alpha_i < p^{e_i}$, com $1 \leq i \leq r$, e $\langle x_i \rangle \cap \langle x_j \rangle = 1 \in G$ para $i \neq j$, então S não possui subsequência com produto 1. ■

Agora para o próximo teorema, será necessário lembrar a definição do β-ésimo polinômio simétrico no anel de polinômios $\mathbb{Z}[x_1, \ldots, x_k]$. Para $1 \leq \beta \leq k$, definimos:

$$\begin{aligned}
p_1(x_1, \ldots, x_k) &= x_1 + \cdots + x_k, \\
p_2(x_1, \ldots, x_k) &= x_1x_2 + \cdots + x_{k-1}x_k, \\
&\vdots \\
p_\beta(x_1, \ldots, x_k) &= \sum_{1 \leq i_1 < \cdots < i_\beta \leq k} \prod_{j=1}^{\beta} x_{i_j}, \\
&\vdots \\
p_k(x_1, \ldots, x_k) &= \prod_{j=1}^{k} x_j.
\end{aligned}$$

Agora definiremos $A(\beta)$, para cada $1 \leq \beta \leq k$, como sendo a soma formal dos produtos de todas as subsequências de $S = \prod_{i=1}^{k} g_i \in \mathscr{F}(G)$ com tamanho igual a β. Dessa forma $A(\beta) = p_\beta(g_1, \ldots, g_k) \in \mathbb{Z}[G]$.

Teorema 3.14 *Seja G um p-grupo abeliano finito, ou seja, um grupo isomorfo a $C_{p^{e_1}} \oplus C_{p^{e_2}} \oplus \cdots \oplus C_{p^{e_r}}$, com $e_1 \leq e_2 \leq \cdots \leq e_r$, em que $e_i \in \mathbb{N}$ para todo $1 \leq i \leq r$. Então,*

$$D(G) = 1 + \sum_{i=1}^{r} (p^{e_i} - 1).$$

Demonstração: Pela Proposição 3.13, temos $D(G) \geq 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$. Logo, resta provar que $D(G) \leq 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$, ou seja, é necessário provar que se uma sequência $S \in \mathscr{F}(G)$ tem comprimento maior que $\sum_{i=1}^{r}(p^{e_i} - 1)$, então S tem uma subsequência T com produto 1.

Para $g \in G$ e $S = \prod_{i=1}^{k} g_i \in \mathscr{F}(G)$, definiremos $E(g)$ como o número de subsequências não vazias de S com comprimento par e produto g e $O(g)$ como o número de subsequências de S com comprimento ímpar e produto g. Observe que se considerarmos $A(0) = 1 \in \mathbb{Z}[G]$ e $A(\beta) = p_\beta(g_1, \ldots, g_k) \in \mathbb{Z}[G]$, para $1 \leq \beta \leq k$, temos

$$\prod_{i=1}^{k}(1 - g_i) = \sum_{\beta=0}^{k}(-1)^\beta A(\beta) = A(0) + \sum_{\beta=1}^{k}(-1)^\beta A(\beta).$$

Para cada $g \in G$, reagrupamos os produtos (na soma $A(\beta)$, para cada β) cujo resultado é g. Se o número de termos usados para obter g é par, esse produto é contado em $E(g)$ e se o número de termos usados para obter g é ímpar, esse produto é contado em $O(g)$. Dessa forma, o coeficiente de g na soma acima é $E(g) - O(g)$. Assim,

$$\begin{aligned}
\prod_{i=1}^{k}(1 - g_i) &= A(0) + \sum_{g \in G}(E(g) - O(g))g \\
&= A(0) + (E(1) - O(1))1 + \sum_{\substack{g \in G \\ g \neq 1}}(E(g) - O(g))g \\
&= 1 + E(1) - O(1) + \sum_{\substack{g \in G \\ g \neq 1}}(E(g) - O(g))g.
\end{aligned}$$

Logo, pelo Teorema 3.12, temos

$$E(g) - O(g) = \begin{cases} 0 \pmod{p}, & \text{se } g \neq 1; \\ -1 \pmod{p}, & \text{se } g = 1, \end{cases}$$

Desse modo, temos que se o produto de uma subsequência de comprimento par for igual a $g \neq 1$, deve existir uma subsequência de comprimento ímpar cujo produto também é $g \neq 1$ fazendo com que as duas se cancelem, e vice-versa, pois o produto das subsequências de comprimento ímpar aparecem negativas no produtório $\prod_{i=1}^{k}(1 - g_i)$ e as de comprimento par aparecem positivas. $E(g)$ pode ser diferente de $O(g)$ apenas se a diferença for um múltiplo de p, devido a congruência módulo p. Agora, para $g = 1$ deve existir uma subsequência de comprimento ímpar cujo produto é 1, para anular o termo 1 que aparece no produtório $\prod_{i=1}^{k}(1 - g_i)$. Dessa forma, segue que S tem uma subsequência com produto 1. Caso contrário, teríamos que S não possui subsequência com tamanho par ou ímpar e produto 1, ou seja, $E(1) = O(1) = 0$, $0 = E(1) - O(1) \equiv -1 \pmod{p}$, uma contradição. Portanto, está

provado o teorema. ■

Agora vamos determinar $D(G)$ para o caso em que G é a soma direta de 2 grupos cíclicos.

Lema 3.15 *Seja $E = C_p \oplus C_p$, com p primo. Se $S = \prod_{i=1}^{k} g_i \in \mathscr{F}(E)$ e $k \geq 3p-2$, então S tem uma subsequência de tamanho t, $1 \leq t \leq p$, tal que $g_{i_1} \cdot g_{i_2} \cdots g_{i_t} = 1$.*

Demonstração: Sejam $F = C_p \oplus C_p \oplus C_p$, $1 = (1,1,1)$ a identidade de F, x um gerador de C_p e $E' = C_p \oplus C_p \oplus \{1\}$ sendo um subgrupo de F. Em particular, isso implica que $E' = E \oplus \{1\} \cong E$. Por abuso de notação, se $g \in E$, então (g,x) denotará um elemento de F. As primeiras duas coordenadas de (g,x) são as duas coordenadas de g e a terceira coordenada de (g,x) é x.

Pelo Teorema 3.14, $D(F) = 3p-2$, e como $k \geq 3p-2$, então alguma subsequência com tamanho $t \leq 3p-2$ de $T = \prod_{i=1}^{k}(g_i,x) \in \mathscr{F}(F)$, em que $g_i \in E$, tem produto 1. Digamos que $T_1 = \prod_{i=1}^{t}(g_i,x)$ é uma subsequência de T com produto 1 e tamanho t.

Como T_1 tem produto 1, temos que $(g_1 \cdot g_2 \cdots g_t, x^t) = 1$, ou seja, $x^t = 1$. Assim, $p|t$, e como $t \leq 3p-2$, tem-se que $|T_1| \in \{p, 2p\}$.

Se $|T_1| = t = p$, então $U = \prod_{i=1}^{t} g_i$ é a subsequência procurada.

Agora, se $|T_1| = 2p$, como $D(E) = 1+2(p-1) = 2p-1$, segue que $U = \prod_{i=1}^{t} g_i$ tem uma subsequência com tamanho $u \leq 2p-1$ e produto igual a 1, digamos que essa sequência seja $U_1 = \prod_{i=1}^{u} g_i$. Se $u \leq p$, o lema está provado. Caso contrário, temos $2p-u < p$ e a subsequência $U_2 = \prod_{i=u+1}^{2p} g_i$ satisfaz o resultado do lema.

■

Teorema 3.16 *Seja $G = H \oplus K$ a soma direta dos grupos abelianos H e K de ordens $o(H) = h$ e $o(K) = k$, onde $h|k$, então $D(G) \leq h+k-1$.*

Demonstração: Seja S uma sequência no grupo abeliano finito G, em que $|S| = s \geq h+k-1$. Iremos proceder por indução sobre h.

Seja $h = 1$. Nesse caso, $G \cong K$. Pelo princípio das gavetas de Dirichlet, se os produtos $\prod_{l=1}^{j} g_l$, para todo $1 \leq j \leq k$, são distintos, segue que $\prod_{l=1}^{j} g_l = 1$ para algum $1 \leq j \leq k$, e o resultado segue. Caso

contrário, temos $\prod_{l=1}^{i} g_l = \prod_{l=1}^{j} g_l$, para alguns $1 \leq i < j \leq k$. Então, usando a lei do cancelamento, a subsequência $T = \prod_{l=i+1}^{j} g_l$ tem produto igual a 1.

Assuma $h > 1$, e suponha $D(Q) \leq o(H_1) + o(K_1) - 1$ para todo grupo $Q = H_1 \oplus K_1$, com $o(H_1) < h$ e $o(H_1) | o(K_1)$.

Seja p um divisor primo de h e sejam H_1 um subgrupo de H e K_1 um subgrupo de K, com índices $[H : H_1] = [K : K_1] = p$. Defina $h_1 = o(H_1)$ e $k_1 = o(K_1)$.

Considere o grupo $Q = H_1 \oplus K_1$. Como $h|k$, então $h_1 = \frac{h}{p}$ divide $k_1 = \frac{k}{p}$. Claramente $h_1 < h$, o que quer dizer que podemos aplicar a hipótese de indução. Isto é $D(Q) \leq h_1 + k_1 - 1$. Observe que

$$G/Q = (H \oplus K)/(H_1 \oplus K_1) \cong H/H_1 \oplus K/K_1 \cong C_p \oplus C_p$$

e $s \geq h + k - 1 = p(h_1 + k_1 - 2) + 2p - 1$. Se $h_1 = k_1 = 1$, então $D(G) = D(C_p \oplus C_p) = 2p - 1$ e, pelo Teorema 3.14, o resultado está provado.

Agora, suponhamos que $h_1 + k_1 \geq 3$. Consideremos a seguinte sequência em $\mathscr{F}(G/Q)$, $T = \prod_{i=1}^{s}(g_i Q)$. Como $s \geq p(h_1 + k_1 - 2) + 2p - 1 \geq 3p - 1$, pelo lema anterior, a sequência T tem uma subsequência T_1 com tamanho t_1, $1 \leq t_1 \leq p$, e produto $Q \in G/Q$. Se $h_1 + k_1 \geq 4$, consideremos a sequência TT_1^{-1}, de tamanho $s - t_1$. Como $s - t_1 \geq p(h_1 + k_1 - 2) + 2p - 1 - t_1 \geq 2p + 2p - 1 - p \geq 3p - 1$, então podemos aplicar o lema anterior à sequência TT_1^{-1}. Dessa forma, TT_1^{-1} possui uma subsequência T_2 de tamanho $1 \leq t_2 \leq p$ e produto Q. Se $h_1 + k_1 \geq 5$, consideremos a sequência $TT_1^{-1}T_2^{-1}$ e novamente pelo lema anterior obtemos uma subsequência T_3, de tamanho $1 \leq t_3 \leq p$, e produto Q. Continuando dessa forma, tem-se $u - 1 = h_1 + k_1 - 2$ subsequências de T, denotadas $T_1, \ldots, T_{u-1}$, de produto Q e tamanho $1 \leq t_1, t_2, \ldots, t_{u-1} \leq p$, tais que $T_1 \cdots T_{u-1}$ é uma subsequência de T. Para cada $1 \leq j \leq u - 1$, a sequência T_j é da forma $T_j = \prod_{i=1}^{t_j}(g_{l_i} Q)$. A partir da sequência T_j, definimos a sequência $S_j = \prod_{i=1}^{t_j} g_{l_i}$. Como a sequência T_j é de produto Q, então a sequência S_j é de produto $q_j \in Q$. Observe que $TT_1^{-1} \cdots T_{u-1}^{-1}$ é uma sequência de tamanho $s - (t_1 + \cdots + t_{u-1}) \geq p(h_1 + k_1 - 2) + 2p - 1 - (t_1 + \cdots + t_{u-1}) \geq p(u-1) + 2p - 1 - (u-1)p = 2p - 1$. Pelo Teorema 3.14, $TT_1^{-1} \cdots T_{u-1}^{-1}$ possui uma subsequência T_u com produto Q. De novo, denotamos S_u a sequência formada pelos elementos g_i que aparecem na forma $(g_i Q)$ na sequência T_u. Como nos casos anteriores, tem-se $\pi(S_u) = q_u \in Q$.

Como $D(Q) \leq h_1 + k_1 - 1$, então a sequência $\prod_{j=1}^{u} q_j \in \mathscr{F}(Q)$, de tamanho $u = h_1 + k_1 - 1$, tem uma

subsequência $\prod_{1\le i\le u} q_i$, com produto igual a $1 \in Q$. Logo, S tem a subsequência $\prod_{1\le i\le u}\prod_{g\in S_i} g \in \mathscr{F}(G)$, com produto igual a 1. Isso prova o teorema. ■

Corolário 3.17 *Seja G a soma direta dos grupos cíclicos C_m e C_n em que $m|n$. Então, $D(G) = m+n-1$.*

Demonstração: Pelo Teorema 3.16 sabemos que $D(G) \le m+n-1$, logo temos apenas que provar que $D(G) \ge m+n-1$. Para isto, iremos construir uma sequência de tamanho $m+n-2$ que não possua subsequência de com produto 1.

Sejam $(x,1),(1,y) \in G$ tal que $C_m \cong \langle(x,1)\rangle$, $C_n \cong \langle(1,y)\rangle$. Seja a sequência $S = \prod_{i=1}^{m-1}(x,1)\cdot\prod_{i=1}^{n-1}(1,y)$. Suponha que exista uma subsequência de S com produto 1. Então ela seria da forma

$$U = \prod_{j=1}^{r}(x,1)\cdot\prod_{j=1}^{s}(1,y), \text{ com } r \le m-1, s \le n-1, \pi(U) = 1,$$

Então $1 = (x^r, y^s)$, logo, $r = 0$ e $s = 0$, uma contradição. Portanto, $D(G) = m+n-1$. ■

Conclusão

Concluindo, neste trabalho relembramos conceitos básicos da graduação sobre grupos abelianos e diversos teoremas sobre grupos abelianos finitos, além disso vimos a definição básica da constante de Davenport e como calculá-la para certas classes de grupos abelianos finitos.

Entre os principais resultados temos o teorema fundamental dos grupos abelianos finitos, e diversos resultados sobre a constante de Davenport.

Espera-se que o trabalho tenha fornecido ideias claras sobre a constante de Davenport e que os resultados aqui apresentados auxiliem para encontrar novos resultados sobre a constante de Davenport para outras classes de grupos abelianos finitos.

Referências Bibliográficas

[1] CHANG, G. J. et al. "**On the number of subsequences with a given sum in a finite abelian group**". Em: ***The Rocky Mountain Journal of Mathematics*** 37.5 (2007). https://doi.org/10.48550/arXiv.1101.4492, pp. 1541–1550.

[2] DEVOS, M. J. ***Subsequence Sums I: the Davenport Constant***. Disponível em: https://www.sfu.ca/~mdevos/notes/comb_numb/notes3.pdf. Acesso em: 08, Mar. 2024.

[3] GARCIA, A. e LEQUAIN, Y. ***Elementos de álgebra***. Brasil, Rio de Janeiro: Projeto Euclides, 2001.

[4] GEROLDINGER, A. e SCHNEIDER, R. "**On Davenport's constant**". Em: ***Journal of Combinatorial Theory, Series A*** 61.1 (1992). https://doi.org/10.1016/0097-3165(92)90061-X, pp. 147–152.

[5] GONÇALVES, A. ***Introdução à álgebra***. Brasil: Projeto Euclides, 1979.

[6] HERSTEIN, I. N. ***Tópicos de álgebra***. Tradução de Adalberto P. Bergamasco, L. H. Jacy Monteiro. Brasil, São Paulo: Editora Polígono S.A, 1970.

[7] JACOBSON, N. ***Basic Algebra I***. Estados Unidos: W. H. Freeman e Company, 1985.

[8] LANSKI, C. ***Concepts In Abstract Algebra***. Los Angeles: Brooks/Cole, 2005.

[9] OLSON, J. E. "**A combinatorial problem on finite Abelian groups, I**". Em: ***Journal of Number Theory*** 1.1 (1969). https://doi.org/10.1016/0022-314X(69)90021-3, pp. 8–10.

[10] OLSON, J. E. "**A combinatorial problem on finite Abelian groups, II**". Em: ***Journal of Number Theory*** 1.2 (1969). https://doi.org/10.1016/0022-314X(69)90037-7, pp. 195–199.