UNIVERSIDADE FEDERAL DE VIÇOSA

Sobre a constante consecutiva de Davenport com peso

Pedro Augusto Costa
Magister Scientiae

VIÇOSA - MINAS GERAIS
2025

PEDRO AUGUSTO COSTA

Sobre a constante consecutiva de Davenport com peso

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*.

Orientador: Abilio L. Cardoso Junior

Coorientador: Allan de Oliveira Moura

VIÇOSA - MINAS GERAIS
2025

Ficha catalográfica elaborada pela Biblioteca Central da Universidade Federal de Viçosa - Campus Viçosa

T
C837s
2025

Costa, Pedro Augusto, 2000-
Sobre a constante consecutiva de Davenport com peso / Pedro Augusto Costa. – Viçosa, MG, 2025.
1 dissertação eletrônica (79 f.)

Orientador: Abílio Lemos Cardoso Júnior.
Dissertação (mestrado) - Universidade Federal de Viçosa, Departamento de Matemática, 2025.
Referências bibliográficas: f. 78-79.
DOI: https://doi.org/10.47328/ufvbbt.2025.549
Modo de acesso: World Wide Web.

1. Sequências (Matemática). I. Cardoso Júnior, Abílio Lemos, 1979-. II. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. III. Título.

CDD 22. ed. 515.24

Bibliotecário(a) responsável: Euzébio Luiz Pinto CRB-6/3317

PEDRO AUGUSTO COSTA

Sobre a constante consecutiva de Davenport com peso

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: 5 de agosto de 2025.

Assentimento:

_____

Pedro Augusto Costa
Autor

_____

Abilio Lemos Cardoso Junior
Orientador

AGRADECIMENTOS

Primeiramente agradeço a Deus por ter me proporcionado saúde e força para lutar com as dificuldades que encontrei nesta caminhada.

A minha família, em especial aos meus pais, Denise e José Augusto, e minha noiva, Dyohana, por serem meu alicerce para suportar todos os problemas enfrentados, me ensinando a ter paciência e resiliência.

Aos amigos do mestrado do DMA-UFV que me acompanharam, me ajudaram, aconselharam e compartilharam horas de estudo na sala.

A todos os professores do DMA-UFV.

Ao meu orientador, Abílio, pelas horas que estudamos juntos, pela paciência em me ensinar e pela confiança que depositou em mim.

Aos professores Allan, Anderson e Hemar, por aceitarem meu convite para participar da banca.

Este trabalho foi realizado com o apoio das seguintes agências de pesquisa brasileiras: Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001, Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) e Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

“A Matemática é a rainha das ciências e a teoria dos números é a rainha da Matemática.”

Carl Friedrich Gauss

RESUMO

COSTA, Pedro Augusto, M.Sc., Universidade Federal de Viçosa, agosto de 2025. **Sobre a constante consecutiva de Davenport com peso**. Orientador: Abilio Lemos Cardoso Junior. Coorientador: Allan de Oliveira Moura.

Este trabalho estuda uma variação da constante de Davenport, denominada constante consecutiva de Davenport, além de investigar as sequências extremas associadas, ambos no contexto do anel dos inteiros módulo n considerado como módulo sobre ele próprio. A variação consiste na exigência de que a subsequência ponderada cuja soma resulta em zero seja formada por termos consecutivos. O primeiro objetivo consiste em determinar o valor dessa constante para os inteiros módulo p, onde p é um número primo, considerando diferentes conjuntos de pesos: o grupo das unidades dos inteiros módulo p, seus quadrados e seus cubos. Em seguida, o estudo se estende para o caso geral com n sendo um número natural, com restrições específicas dependendo do conjunto dos pesos. Na sequência, o trabalho caracteriza as sequências extremas associadas à constante consecutiva de Davenport, estabelecendo suas propriedades estruturais. Por fim, o último capítulo apresenta resultados inéditos referentes a uma nova variação da constante de Davenport, agora utilizando pesos, mas sem impor a restrição de consecutividade na subsequência.

Palavras-chave: problemas de soma-zero com peso; constante de Davenport; sequências extremas

ABSTRACT

COSTA, Pedro Augusto, M.Sc., Universidade Federal de Viçosa, August, 2025. **On weighted consecutive Davenport constant**. Adviser: Abilio Lemos Cardoso Junior. Co-adviser: Allan de Oliveira Moura.

This work studies a variation of the Davenport constant, namely the consecutive Davenport constant, and investigates the associated extremal sequences, both in the context of the ring of integers modulo n as a module over itself. This variation requires that the weighted subsequence whose sum results in zero is formed by consecutive terms. The first objective is to determine the value of this constant for the integers modulo p, where p is a prime number, considering different sets of weights: the group of units of the integers modulo p, its squares, and its cubes. Subsequently, the study extends to the general case where n is a natural number, with specific restrictions depending on the set of weights. The work then characterizes the extremal sequences associated with the consecutive Davenport constant, establishing their structural properties. Finally, the last chapter presents original results concerning a new variation of the Davenport constant, which also uses weights but without imposing the consecutivity restriction on the subsequence.

Keywords: weighted zero-sum problems; Davenport constant; extremal sequences

Sumário

1 Introdução

A Teoria Aditiva dos Números, um campo clássico da matemática, estuda as propriedades de subconjuntos de números inteiros com a operação de adição. Dentro desta linha de pesquisa, os problemas de soma zero se destacam como uma área de pesquisa particularmente recente e com uma vasto caminho a ser seguido. Estes problemas, em sua essência, buscam estabelecer condições para garantir que uma sequência de elementos de um grupo abeliano admita uma subsequência cuja soma seja o elemento neutro. A raiz dessa linha de pesquisa começa com o famoso *Teorema de Cauchy-Davenport* [3, 5], um resultado fundamental que fornece um limite inferior para a cardinalidade de um conjunto-soma em $\mathbb{Z}_p$.

A investigação moderna da constante de Davenport começou com o trabalho de **K. Rogers**, em 1963. Em seu artigo *"A combinatorial problem in abelian groups"* [17], Rogers utilizou o *Teorema Fundamental dos Grupos Abelianos Finitos* para escrever um grupo abeliano finito G como $G \cong C_{n_1} \oplus \cdots \oplus C_{n_k}$, com $n_1 \mid n_2 \mid \cdots \mid n_k$, e provou que a constante de Davenport satisfaz $D(G) \geqslant \sum_{i=1}^{k}(n_i - 1) + 1$. Além disso, mostrou que a igualdade ocorre para grupos cíclicos, estabelecendo assim o resultado fundamental de que $D(C_n) = n$. Esse trabalho pode ser considerado o ponto de partida da formulação moderna da constante de Davenport.

Posteriormente, a constante de Davenport ganhou uma maior importância devido à sua conexão com a *Teoria Algébrica dos Números*. Se K é um corpo de números e G é o grupo de classes de ideais do anel de inteiros de K, então $D(G)$ representa o maior número de ideais primos, contados com multiplicidade, que podem aparecer na decomposição de um elemento irredutível. Essa interpretação, desenvolvida na obra de **A. Geroldinger** e **F. Halter-Koch** [6], estabeleceu uma ponte entre problemas de soma zero em grupos finitos e a fatoração em domínios de Dedekind. Isso foi proposto primeiramente por Davenport, por isso a constante leva seu nome.

Formalmente, para um grupo abeliano finito G, a saber aditivo, a *constante de Davenport*, denotada por $D(G)$, é definida como o menor inteiro k tal que toda sequência de k elementos sobre G possui uma subsequência não vazia cuja soma é zero, o elemento neutro de G.

O tema também foi abordado nos trabalhos de **J. E. Olson**, que, em 1969, mostrou que a igualdade $D(G) = D^*(G)$, sendo $D^*(G) = 1 + \sum_{i=1}^{k}(n_i - 1)$, é válida para todos os p-grupos e para grupos abelianos de posto (rank) no máximo dois [15, 16]. A conjectura

que $D(G) = D^*(G)$ para todo grupo abeliano finito prevaleceu por pouco tempo, até que **P. van Emde Boas** e **D. Kruyswijk** identificaram contraexemplos para certos grupos de posto maior ou igual a quatro [18]. Determinar o valor exato de $D(G)$ para grupos arbitrários permanece como um dos grandes problemas em aberto da área.

Ao longo do tempo, surgiram importantes generalizações do conceito clássico. Um dos avanços mais significativos foi feito por **S. D. Adhikari** e **P. Rath** (veja [1]), que introduziram a *constante de Davenport com peso*, denotada por $D_A(G)$. Nesta versão, considera-se um conjunto de pesos $A \subseteq \mathbb{Z}$ e busca-se subsequências (g_i) e coeficientes $a_i \in A$ tais que a soma ponderada $\sum a_i g_i$ resulta em 0.

O presente trabalho se insere em uma outra variação importante, ao propor o estudo de um novo invariante, a *constante consecutiva de Davenport com peso*, denotada por $C_A(G)$ e introduzida por **S. Mondal, K. Paul** e **S. Paul**, em 2023, no trabalho intitulado *On a different weighted zero-sum constant* [12]. Esta constante combina as restrições de peso e consecutividade, buscando o menor inteiro k tal que toda sequência de k elementos de G admita uma subsequência de termos consecutivos cuja a soma ponderada é zero.

Esses mesmos autores publicaram, em 2022, o artigo nomeado por *Extremal sequences for a weighted zero-sum constant* [11], no qual classificaram as sequências extremas com peso em A. A saber, uma sequência é dita sequência extrema com peso em A quando possui tamanho $C_A(G) - 1$ e não admite subsequência de termos consecutivos de soma zero com peso em A.

O objetivo central desta dissertação é descrever os resultados obtidos em [11, 12]. Primeiramente, focamos no cálculo de seu valor para o grupo $G = \mathbb{Z}_p$, onde p é primo, explorando diferentes subconjuntos de pesos A, como $U(p)$, $U(p)^2$ e $U(p)^3$. Em seguida, estendemos a análise para o caso geral $G = \mathbb{Z}_n$, com $n \in \mathbb{N}$. Outro pilar do trabalho é a caracterização das sequências extremas com peso em A.

Finalmente, no último capítulo é abordado um novo invariante e apresentado os resultado obtidos. A modificação feita, a partir da constante $D_A(G)$, é que agora queremos estudar o menor inteiro positivo k tal que qualquer sequência de tamanho k possui subsequência cuja a soma de seus termos ponderada em A pertença a um subconjunto B de G, com a restrição de que $0 \in B$. Denotamos o novo invariante por $D_A(G, B)$. Considerando $G = \mathbb{Z}_p$, foi possível calcular a constante para os subconjuntos de pesos $U(p)$, $U(p)^2$ e $U(p)^3$.

2 Preliminares

Neste capítulo vamos introduzir alguns conceitos que são necessários para o entendimento do estudo a ser realizado. Serão apresentados conceitos introdutórios da teoria aditiva dos números, como adição de subconjuntos e a e-transformada, a fim de apresentar as provas dos teoremas de Cauchy-Davenport e Kneser, utilizando [14] como referência. Em adição, apresentaremos um estudo sobre subgrupo de índice 3 no grupo multiplicativo de um corpo, utilizando o artigo [10] como referência principal.

2.1 Adição de Subconjuntos de um Grupo Abeliano

Sejam $(G,+)$ um grupo abeliano e $A_1,...,A_k$ subconjuntos finitos não vazios de G. Definimos o conjunto-soma sendo

$$A_1+\cdots+A_k=\{a_1+\cdots+a_k : a_i\in A_i, i=1,...,k\}\subset G.$$

De forma similar, definimos o conjunto-diferença entre dois subconjuntos finitos não vazios A e B de G como

$$A-B=\{a-b : a\in A, b\in B\}.$$

Neste momento, devemos tomar cuidado para não confundirmos o conjunto-diferença com a diferença de conjuntos, logo usaremos a notação $A\backslash B$ para a diferença de conjuntos.

Por fim, dados $g\in G$ e $A\subset G$, definimos

$$g+A=\{g+a : a\in A\}.$$

Sejam $A,B\subset G$. Para cada $g\in G$, denotaremos por $r_{A,B}(g)$ o número de representações de g como soma de um elemento de A com um elemento de B. Em outras palavras, $r_{A,B}(g)$ é a quantidade de pares ordenados $(a,b)\in A\times B$ tais que $g=a+b$.

Lema 2.1.1. *Sejam G um grupo abeliano finito e $A,B\subset G$ não vazios. Se existe $t\in\mathbb{N}$ tal que*

$$|A|+|B|\geqslant|G|+t,$$

então $r_{A,B}(g)\geqslant t$, para todo $g\in G$.

Demonstração. Seja $g \in G$ qualquer. Temos

$$|G| \geqslant |A \cup (g - B)| = |A| + |g - B| - |A \cap (g - B)| = |A| + |B| - |A \cap (g - B)|.$$

Logo, $r_{A,B}(g) = |A \cap (g - B)| \geqslant |A| + |B| - |G| \geqslant t$, como queríamos. □

Lema 2.1.2. *Sejam G um grupo abeliano finito e $A, B \subset G$ não vazios tais que*

$$|A| + |B| > |G|.$$

Então $A + B = G$.

Demonstração. Como $A, B \subset G$ são não vazios tais que $|A| + |B| > |G|$, segue que $|A| + |B| \geqslant |G| + 1$, ou seja, estamos sobre as hipóteses do Lema 2.1.1 para $t = 1$. Assim, dado $g \in G$, existe pelo menos uma maneira de escrever $g = a + b$, com $a \in A$ e $b \in G$. Isto é, $G \subset A + B$ e, como $A + B \subset G$ trivialmente, temos $G = A + B$. □

Observação 2.1.1. *Pelo Lema 2.1.2, dado um grupo abeliano G, para estudarmos o conjunto-soma $A + B$ devemos nos ocupar somente com os casos em que os subconjuntos não vazios A, B de G tais que $|A| + |B| \leqslant |G|$.*

2.2 A e-transformada

Considere G um grupo abeliano finito e (A, B) um par ordenado de subconjuntos não vazios de G. Para cada $e \in G$, definimos a e-transformada de (A, B) como sendo o par $(A(e), B(e))$ de subconjuntos de G, dados por:

$$A(e) = A \cup (B + e), B(e) = B \cap (A - e)$$

Em particular, $A \subset A(e)$ e $B(e) \subset B$.

Lema 2.2.1. *Sejam G um grupo abeliano finito e $A, B \subset G$ não vazios. Para cada $e \in G$, a e-transformada de (A, B) satisfaz:*

1. *$A(e) + B(e) \subset A + B$;*
2. *$A(e) \backslash A = e + (B \backslash B(e))$;*
3. *$|A(e)| + |B(e)| = |A| + |B|$;*
4. *Se $e \in A$ e $0 \in B$, então $e \in A(e)$ e $0 \in B(e)$.*

Demonstração. Note que o quarto item segue da definição de e-transformada. Para as demais afirmações, temos:

1. Seja $g \in A(e) + B(e)$ qualquer, ou seja, existem $a' \in A(e)$ e $b' \in B(e)$ tais que $g = a' + b'$. Note que, por $b' \in B(e)$, temos $b' \in B$ e $b' \in A - e$. Assim,

   - Se $a' \in A$, então $g = a' + b'$ é tal que $a' \in A$ e $b' \in B$, ou seja, $g \in A + B$.
   - Se $a' \in B + e$, existe $b \in B$ tal que $a' = b + e$. Além disso, $b' \in A - e$, ou seja, existe $a \in A$ tal que $b' = a - e$. Logo,

   $$g = a' + b' = (b + e) + (a - e) = a + b \in A + B.$$

   Assim, temos a afirmação.

2. De fato,

   $$\begin{aligned} A(e)\backslash A &= (B + e)\backslash A \\ &= \{b + e : b \in B \text{ e } b + e \notin A\} \\ &= e + \{b \in B : b \notin A - e\} \\ &= e + \{b \in B : b \notin (e)\} \\ &= e + (B\backslash B(e)). \end{aligned}$$

3. Pelo item anterior, temos:

   $$|A(e)| - |A| = |A(e)\backslash A| = |e + (B\backslash B(e))| = |B\backslash B(e)| = |B| - |B(e)|.$$

   Como A e B são finitos, pois G o é, então $|A|$ e $|B(e)|$ são números, donde $|A(e)| + |B(e)| = |A| + |B|$.

□

2.3 O Teorema de Cauchy-Davenport

Nesta seção, demonstraremos o famoso Teorema de Cauchy-Davenport, importante ferramenta utilizada posteriormente neste trabalho. Para tanto, faremos a demonstração abaixo.

Teorema 2.3.1 (Teorema de I. Chowla)**.** *Sejam $m \geqslant 2$, A e B dois subconjuntos não vazios de $\mathbb{Z}_m$. Se $0 \in B$ e $\text{mdc}(b, m) = 1$, para todo $b \in B\backslash\{0\}$, então*

$$|A + B| \geqslant \min\{|A| + |B| - 1, m\}.$$

Demonstração. Pela Observação 2.1.1, precisamos nos preocupar apenas com o caso em que $|A| + |B| \leqslant m$. Ou seja,

$$\min\{|A| + |B| - 1, m\} = |A| + |B| - 1 \leqslant m - 1.$$

Note que se $|A| = 1$ ou $|B| = 1$, o teorema é válido. De fato, suponha, sem perda de generalidade, $|A| = 1$. Dessa forma, temos

$$|A + B| = |B| = |B| + 1 - 1 = |A| + |B| - 1 \geqslant \min\{|A| + |B| - 1, m\}.$$

Suponha, por contradição, que existam $A, B \subset \mathbb{Z}_m$ tais que $\min\{|A|, |B|\} \geqslant 2$ e $|A + B| < |A| + |B| - 1$. A última desigualdade nos fornece $A \neq \mathbb{Z}_m$. De fato, se $A = \mathbb{Z}_m$, teríamos $|A| = m$ e $|B| \geqslant 2$, o que contraria o fato de $|A| + |B| \leqslant m$.

Agora, escolha um par (A, B) de tal modo que a cardinalidade de B seja mínima. Como $|B| \geqslant 2$, existe $b' \in B$ diferente de 0. Se $a + b' \in A$, para todo $a \in A$, então $a + jb' \in A$, para todo $j \in \{0, 1, ...\}$ e para todo $a \in A$. Como $\text{mdc}(b', m) = 1$, por hipótese, então b' gera $\mathbb{Z}_m$, donde

$$\{a + jb' : j \in \{0, 1, ..., m - 1\}\} = \mathbb{Z}_m,$$

o que é uma contradição com o fato de $A \neq \mathbb{Z}_m$.

Logo, existe $e \in A$ tal que $e + b' \notin A$. Considere $(A(e), B(e))$ a e-transformada do par (A, B). Pelo Lema 2.2.1, temos

$$|A(e) + B(e)| \leqslant |A + B| < |A| + |B| - 1 = |A(e)| + |B(e)| - 1. \tag{2.1}$$

Usando a desigualdade acima, podemos concluir que $|B(e)| \geqslant 2$. De fato, como $0 \in B$, segue $|B(e)| = 1$ se, e somente se, $B(e) = \{0\}$. Neste caso, teríamos

$$|A(e) + B(e)| = |A(e)| \text{ e } |A(e)| + |B(e)| - 1 = |A(e)| + 1 - 1 = |A(e)|.$$

Isto posto e usando a Desigualdade (2.1), temos o absurdo $|A(e)| < |A(e)|$. Ou seja, $|B(e)| \geqslant 2$.

Por fim, como $e \in A$ e $0 \in B$, segue do Lema 2.2.1 que $0 \in B(e)$. Como $B \subset B(e)$, segue da hipótese deste teorema que $\text{mdc}(b, m) = 1$, para todo $b \in B(e)\backslash\{0\}$. Além disso, $e + b' \notin A$, ou seja, $b' \notin A - e$. Logo, $b' \notin B(e)$. Portanto, $b' \in B$, mas $b' \notin B(e)$, donde temos o absurdo $|B| > |B(e)|$. □

Agora estamos prontos para demonstrar o teorema principal desta seção.

Teorema 2.3.2 (Teorema de Cauchy-Davenport)**.** *Sejam p um número primo e $A, B \subset \mathbb{Z}_p$ não vazios. Então*

$$|A + B| \geqslant \min\{|A| + |B| - 1, p\}.$$

Demonstração. Como B é um subconjunto não vazio de $\mathbb{Z}_p$, tome $b_0 \in B$. Dessa forma, $0 \in B - b_0$ e $\text{mdc}(b, p) = 1$, para todo $0 \neq b \in B - b_0$. Pelo teorema anterior,

$$\begin{aligned} |A + B| &= |A + (B - b_0)| \\ &\geqslant \min\{|A| + |(B - b_0)| - 1, p\} \\ &= \min\{|A| + |B| - 1, p\}. \end{aligned}$$

□

Corolário 2.3.1. *Sejam $n \geqslant 2$, p primo e $A_1, ..., A_n$ subconjuntos não vazios de $\mathbb{Z}_p$. Então,*

$$|A_1 + ... + A_n| \geqslant \min\left\{\sum_{i=1}^{n} |A_i| - n + 1, p\right\}.$$

Demonstração. A demonstração é feita por indução. Para o caso de dois subconjuntos somente, este corolário se torna o Teorema 2.3.2. Suponha que o resultado é válido para n subconjuntos não vazios de $\mathbb{Z}_p$. Novamente pelo Teorema 2.3.2, temos

$$\begin{aligned} |A_1 + ... + A_{n+1}| &\geqslant \min\{|A_1 + ... + A_n| + |A_{n+1}|, p\} \\ &\geqslant \min\left\{\sum_{i=1}^{n} |A_i| - n + 1 + |A_{n+1}| - 1, p\right\} \\ &\geqslant \min\left\{\sum_{i=1}^{n+1} |A_i| - (n+1) + 1, p\right\}. \end{aligned}$$

□

2.4 O Teorema de Kneser para Grupos

Nesta seção, a proposta é provar o Teorema de Kneser para grupos abelianos finitos. Tal teorema será de suma importância para provar alguns resultados dos problemas de soma-zero. Vamos introduzir o conceito de estabilizador.

Definição 2.4.1. *Dado $A \subset G$ não vazio, com G sendo um grupo abeliano, o estabilizador de A, denotado por* $\mathrm{Stab}(A)$ *é definido como:*

$$\mathrm{Stab(A)} = \{x \in G : x + A = A\}.$$

A fim de verificar algumas propriedades do estabilizador de um conjunto não vazio, temos a próxima proposição:

Proposição 2.4.1. *Sejam G um grupo abeliano finito e $A, B \subset G$ não vazios.*

1. *$H = \mathrm{Stab}(A)$ é um subgrupo normal de G;*
2. *$\mathrm{Stab}(A) = G$ se, e somente se, $A = G$;*
3. *Se $H = \mathrm{Stab}(A)$ e $\phi : G \to \dfrac{G}{H}$ é o homomorfismo canônico, ou seja, $\phi(g) = g + H$, então $\mathrm{Stab}(\phi(A))$ é trivial;*
4. *$\mathrm{Stab}(A) \subset \mathrm{Stab}(A + B)$;*

5. Se $H = \mathrm{Stab}(A+B)$, então $|A+H|, |B+H|$ e $|A+B|$ são múltiplos de $|H|$.

Demonstração. 1. Como G é um grupo abeliano, basta verificar que $H = \mathrm{Stab}(A)$ é subgrupo de G. De fato, dado $x \in H$, temos $x + A = A$, donde $-x + A = A$. Logo, $-x \in H$. Agora, se $y \in H$ é outro elemento dado, segue que $x + A = A$ e $y + A = A$. Daí, pelo que vimos anteriormente, $-y + A = A$ e, portanto,

$$(x - y) + A = x + (-y + A) = x + A = A,$$

ou seja, $x - y \in H$. Logo, H é subgrupo de G e, consequentemente, um subgrupo normal de G.

2. Suponha $\mathrm{Stab}(A) = G$. Devemos mostrar que $G \subset A$. Como $x + A = A$, para todo $x \in G$, em particular, temos $a + A = A$, para todo $a \in A$. Logo, $A + A = A$ e, consequentemente, $A - A = A$. Dado $g \in G$, temos que $g + A = A$, ou seja, $g + a = b$, para algum $a, b \in A$. Logo, $g = b - a \in A - A = A$. Como $g \in G$ é qualquer, temos $G \subset A$.

Reciprocamente, se $A = G$, então $\mathrm{Stab}(A) = \{x \in G : x + A = A\} = \{x \in G : x + G = G\} = G$.

3. Seja $\phi(x) \in \mathrm{Stab}(\phi(A))$ qualquer. Vamos mostrar que $x \in H$. De fato, se $a \in A$ é um elemento arbitrário, por $\phi(x) \in \mathrm{Stab}(\phi(A))$, temos

$$\phi(x + a) = \phi(x) + \phi(a) = \phi(),$$

para algum $\in A$. Logo, $(x + a) + H = + H$, ou seja, $(x + a) - \in H$. Como $H = \mathrm{Stab}(A)$ e $\in A$, segue que $x + a = (x + a) - + \in A$. Daí, existe $a' \in A$ tal que $x + a = a'$. Como $a \in A$ foi tomado arbitrariamente, então $x \in H$, donde $\phi(x) = 0$, como queríamos.

4. Seja $g \in \mathrm{Stab}(A)$ qualquer. Assim, $g + A = A$, donde

$$g + (A + B) = (g + A) + B = A + B,$$

ou seja, $g \in \mathrm{Stab}(A + B)$. Logo, temos a validade da afirmação.

5. Vimos que H é subgrupo de G. Como G é finito, A também o é, digamos $A = \{a_1, ..., a_k\}$. Daí, temos

$$A + H = \bigcup_{i=1}^{k} (x_i + H).$$

Logo, existem no máximo k classes laterais geradas por elementos de A, ou seja, existem l índices $1 \leqslant i_1 \leqslant ... \leqslant i_l \leqslant k$, em que $1 \leqslant l \leqslant k$ tais que

$$A + H = \bigcup_{j=1}^{l} \left(x_{i_j} + H\right) \text{ e } l|H| = |A + H|.$$

Usando a mesma ideia, podemos provar a afirmação para $|B + H|$ e $|A + B| = |(A + B) + H|$. □

O próximo resultado é uma das ferramentas utilizadas na demonstração do Teorema de Kneser. Uma outra demonstração desse teorema pode ser encontrada em [13].

Teorema 2.4.1. *Sejam $\{0\} \neq G$ um grupo abeliano e A, B dois subconjuntos finitos e não vazios de G. Se $|A| + |B| \leqslant |G|$, então existe um subgrupo próprio H de G tal que*

$$|A + B| \geqslant |A| + |B| - |H|.$$

Demonstração. A demonstração é feita por indução sobre $|B|$. Se $|B| = 1$, temos

$$|A + B| = |A| = |A| + 1 - 1 = |A| + |B| - 1 \geqslant |A| + |B| - |H|,$$

para todo subgrupo H de G.

Agora, suponha $|B| > 1$ e que o resultado seja válido para todos os pares A', B' de subconjuntos finitos e não vazios de G tais que $|B'| < |B|$. Para o melhor entendimento, vamos separar a demonstração em dois casos:

1. Caso $a + b_2 - b_1 \in A$, para todos $a \in A$ e $b_1, b_2 \in B$: Neste caso, $A + b_2 - b_1 = A$, para todos $b_1, b_2 \in B$. Seja H o subgrupo gerado por todos os elementos do tipo $b_2 - b_1$, com $b_1, b_2 \in B$. Temos então $1 < |B| \leqslant |H|$. Além disso, podemos verificar que $|A| \neq |B|$. Daí, $A + H = A \neq G$ e H é um subgrupo próprio de G tal que

$$|A + B| \geqslant |A| \geqslant |A| + |B| - |H|.$$

2. Caso existam $a \in A$ e $b_1, b_2 \in B$ tais que $a + b_2 - b_1 \notin A$: Neste caso, escolhendo $e = a - b_1$, temos

$$b_2 \notin A - (a - b_1) = A - e.$$

Por outro lado, $b_1 \in A - e$, visto que $0 \in A - a$.

Agora, considere a e-transformada $A(e), B(e)$. Pela definição de e-transformada, verifica-se que $b_2 \notin B(e)$, uma vez que $b_2 \notin A - e$. Além disso, $b_1 \in B(e)$, novamente pela definição de e-transformada, ou seja, $B(e) \subset G$ é não vazio e finito. Mais ainda, $B(e) \subset B$, donde $|B(e)| < |B|$, visto que $b_2 \in B$ e $b_2 \notin B(e)$. Logo, podemos aplicar a hipótese de indução para o par $(A(e), B(e))$, donde $|A(e) + B(e)| \geqslant |A(e)| + |B(e)| - |H|$. Pelo item 1 do Lema 2.2.1, temos $|A + B| \geqslant |A(e) + B(e)|$. Por fim, novamente pelo Lema 2.2.1, agora item 3, temos $|A(e)| + |B(e)| = |A| + |B|$. Juntando essas três informações, concluímos

$$\begin{aligned} |A + B| \geqslant & |A(e) + B(e)| \\ \geqslant & |A(e)| + |B(e)| - |H| \\ = & |A| + |B| - |H|. \end{aligned}$$

Portanto, o resultado é válido. □

O resultado acima é responsável pelo próximo lema e, a partir disso, teremos mais dois resultados anunciados, em que cada um deles é consequência do seu antecessor.

Lema 2.4.1. *Sejam* $\{0\} \neq G$ *um grupo abeliano e* $C = C_1 \cup C_2$*, com* C_1, C_2 *sendo subconjuntos próprios e não vazios de* G*. Então*

$$|C_i| + |\operatorname{Stab}(C_i)| \leqslant |C| + |\operatorname{Stab}(C)|,$$

para $i = 1$ *ou* $i = 2$*.*

Demonstração. Para simplificar a notação, vamos utilizar $H_i = \operatorname{Stab}(C_i)$, para $i = 1, 2$, e $H = \operatorname{Stab}(C)$. Se tivermos $|C_i| + |\operatorname{Stab}(C_i)| \leqslant |C|$, para $i = 1$ ou $i = 2$, o resultado segue. Então, vamos nos ocupar no caso

$$|C_i| + |\operatorname{Stab}(C_i)| > |C|, \tag{2.2}$$

com $i = 1$ e $i = 2$.

Como H_1, H_2 são subgrupos de G, então $H_1 + H_2$ também o é. Agora, considere m_i o índice de H_i em $H_1 + H_2$, para $i = 1, 2$, e $K = H_1 \cap H_2$, com $|K| = k$. Pelo Teorema dos Isomorfismos de Grupos,

$$\frac{H_1 + H_2}{H_1} \cong \frac{H_2}{K}$$

e

$$\frac{H_1 + H_2}{H_2} \cong \frac{H_1}{K}.$$

Por $|(H_1 + H_2)/H_1| = m_1$ e $|(H_1 + H_2)/H_2| = m_2$, temos $|H_1| = m_2 k$, $|H_2| = m_1 k$ e $|H_1 + H_2| = m_1 m_2 k$. Além disso, $K \subset H_i$, logo $C_i = K + C_i$ e, consequentemente, C_i é uma união de classes de K em G. Do mesmo modo, $C_1 \backslash C_2$ e $C_2 \backslash C_1$ são uniões de classes de K em G. Logo,

$$|C_1| \equiv |C_2| \equiv |C_1 \backslash C_2| \equiv |C_2 \backslash C_1| \equiv 0 \pmod{k}.$$

Sabemos que C é a união de subconjuntos próprios C_1 e C_2, donde $C_1 \backslash C_2$ e $C_2 \backslash C_1$ são não vazios. Disso e da equação (2.2), temos

$$0 < |C_1 \backslash C_2| = |C \backslash C_2| = |C| - |C_2| < |C_2| + |H_2| - |C_2| = |H_2| = m_1 k.$$

Logo,

$$k \leqslant |C_1 \backslash C_2| \leqslant (m_1 - 1)k. \tag{2.3}$$

Analogamente,

$$k \leqslant |C_2 \backslash C_1| \leqslant (m_2 - 1)k. \tag{2.4}$$

Agora, sejam $c' \in C_1 \backslash C_2$ e

$$D = c' + H_1 + H_2.$$

Ou seja, D é uma união de classes de H_1 em G da forma

$$D_1 = c' + h_2 + H_1 \tag{2.5}$$

e D também é a união de classes de H_2 em G da forma

$$D_2 = c' + h_1 + H_2, \tag{2.6}$$

em que $h_1 \in H_1$ e $h_2 \in H_2$. Considere D_1 uma classe de H_1 em G da forma (2.5) e D_2 uma classe de H_2 em G da forma (2.6). Como $h_2 + K \subset H_2$ e $h_1 + K \subset H_1$, então

$$c' + h_1 + h_2 + K \subset D_1 \cap D_2.$$

Por outro lado, se $g \in D_1 \cap D_2$, existem $h_1' \in H_1$ e $h_2' \in H_2$ tais que

$$g = c' + h_1 + h_2' = c' + h_1' + h_2.$$

Logo,

$$g - (c' + h_1 + h_2) = h_1' - h_1 \in H_1$$

e

$$g - (c' + h_1 + h_2) = h_2' - h_2 \in H_2,$$

ou seja,

$$g - (c' + h_1 + h_2) \in H_1 \cap H_2 = K.$$

Isto implica que $g \in c' + h_1 + h_2 + K$ e, pelo que vimos anteriormente, concluí-se que $c' + h_1 + h_2 + K = D_1 \cap D_2$. Assim, uma interseção de uma classe de H_1 em D por uma classe de H_2 em D é uma classe de K em D.

Como o índice de H_i em $H_1 + H_2$ é m_i, então $H_1 + H_2$ é a união de m_i classes de H_i em $H_1 + H_2$ disjuntas duas a duas e, consequentemente, $D = c' + H_1 + H_2$ é também a união de classes de H_i disjuntas duas a duas. Como $H_i + C_i = C_i$ é uma união de H_i-classes, segue que $C_i \cap D$ é a união de u_i H_i-classes duas a duas disjuntas e assim $C_i^c \cap D$, em que C_i^c denota o complementar de C_i, é a união de $m_i - u_i$ H_i-classes duas a duas disjuntas. Como a interseção de uma H_1-classe em D com uma H_2-classe em D gera uma K-classe,

$$(C_2 \backslash C_1) \cap D = (C_2 \cap D) \cap (C_1^c \cap D)$$

é a união de $u_2(m_1 - u_1)$ K-classes duas a duas distintas e, consequentemente,

$$|(C_2 \backslash C_1) \cap D| = u_2(m_1 - u_1)k. \tag{2.7}$$

De forma similar,

$$(C_1 \backslash C_2) \cap D = (C_1 \cap D) \cap (C_2^c \cap D)$$

é a união de $u_1(m_2 - u_2)$ K-classes duas a duas disjuntas e assim,

$$|(C_1 \backslash C_2) \cap D| = u_1(m_2 - u_2)k. \tag{2.8}$$

Como $c' \in (C_1 \backslash C_2) \cap D \subset C_1 \backslash C_2$, segue que

$$0 < |(C_1 \backslash C_2) \cap D| = u_1(m_2 - u_2)k \leqslant |(C_1 \backslash C_2)| \leqslant (m_1 - 1)k.$$

Dessa maneira, $1 \leqslant u_1(m_2 - u_2) \leqslant m_1 - 1$. Logo,

$$1 \leqslant u_1 \leqslant m_1 - 1 \text{ e } 1 \leqslant u_2 \leqslant m_2 - 1.$$

Das Equações (2.3), (2.4), (2.7) e (2.8), temos

$$\begin{aligned}
0 \leqslant & (m_1 - u_1 - 1)(u_2 - 1)k + (m_2 - u_2 - 1)(u_1 - 1)k \\
= & u_2(m_1 - u_1)k - (m_2 - 1)k + u_1(m_2 - u_2)k - (m_1 - 1)k \\
= & |C_2 \backslash C_1| - (m_2 - 1)k + |(C_1 \backslash C_2) \cap D| - (m_1 - 1)k \\
= & |(C_2 \backslash C_1) \cap D| - (m_2 - 1)k - |(C_2 - C_1) \cap D^c| + |C_1 \backslash C_2| - (m_1 - 1)k - |(C_1 \backslash C_2) \cap D^c| \\
\leqslant & 0
\end{aligned}$$

e assim, concluímos que $|C_2 \backslash C_1| = (m_2 - 1)k$ e $|C_1 \backslash C_2| = (m_1 - 1)k$. Como $K = H_1 \cap H_2$, temos

$$K + C = K + (C_1 \cup C_2) = (K + C_1) \cup (K + C_2) = C_1 \cup C_2 = C$$

e, consequentemente, $K \subset \operatorname{Stab}(C)$. Logo,

$$\begin{aligned}
|C| - |C_2| = & |C \backslash C_2| \\
= & |C_1 \backslash C_2| \\
= & m_1 k - k \\
= & |H_2| - |H| \\
\geqslant & |H_2| - |\operatorname{Stab}(C)|.
\end{aligned}$$

De forma similar, temos

$$|C| - |C_1| \geqslant |H_1| - |\operatorname{Stab}(C)|.$$

Portanto,

$$|C_i| + |\operatorname{Stab}(C_i)| \leqslant |C| + |\operatorname{Stab}(C)|,$$

para ambos $i = 1$ e $i = 2$, como queríamos demonstrar. □

De forma mais geral, temos o seguinte resultado:

Lema 2.4.2. *Sejam $n \in \mathbb{N}$, $n \geqslant 2$ e $\{0\} \neq G$ um grupo abeliano. Se C é um subconjunto finito de G tal que*

$$C = C_1 \cup C_2 \cup ... \cup C_n,$$

em que cada C_i, $i \in \{1, ..., n\}$, é um subconjunto próprio e não vazio de C, então

$$|C_i| + |\operatorname{Stab}(C_i)| \leqslant |C| + |\operatorname{Stab}(C)|,$$

para algum $i \in \{1, ..., n\}$.

Demonstração. A demonstração é feita por indução sobre n. O caso $n = 2$ é justamente o Lema 2.4.1. Suponha $n \geqslant 3$ e que o resultado seja válido para $n-1$. Se tivermos $|C_i| + |\operatorname{Stab}(C_i)| \leqslant |C|$, para algum $i \in \{1, ..., n\}$, o resultado segue. Então, vamos nos ocupar com o caso $|C_i| + |\operatorname{Stab}(C_i)| > |C|$, para todo $i \in \{1, ..., n\}$. Se C é a união de $n-1$ dos subconjuntos $C_1, ..., C_n$, a hipótese de indução nos garante o resultado. Dessa forma, nos preocupemos com o caso em que C não é a união de $n-1$ dos subconjuntos $C_1, ..., C_n$. Considere $C' = C_1 \cup C_2 \cup ... \cup C_{n-1}$. Então C' é um subconjunto próprio de C e $C_1, .., C_{n-1}$ são subconjuntos próprios de C'. Assim, a hipótese de indução nos garante

$$|C_i| + |\operatorname{Stab}(C_i)| \leqslant |C'| + |\operatorname{Stab}(C')|,$$

para algum $i \in \{1, ..., n-1\}$. Como $C = C' \cup C_n$, o Lema 2.4.1 nos garante:

$$|C_n| + |\operatorname{Stab}(C_n)| \leqslant |C| + |\operatorname{Stab}(C)|$$

ou

$$|C'| + |\operatorname{Stab}(C')| \leqslant |C| + |\operatorname{Stab}(C)|,$$

o que significa que o resultado vale para n. Portanto, este lema está provado por indução sobre n. □

Lema 2.4.3. *Sejam $n \geqslant 2$ e $C_1, ..., C_n$ subconjuntos finitos e não vazios de um grupo abeliano $G \neq \{0\}$. Se $C = C_1 \cup C_2 \cup ... \cup C_n$, então*

$$\min\{|C_i| + |\operatorname{Stab}(C_i)| : i = 1, ..., n\} \leqslant |C| + |\operatorname{Stab}(C)|.$$

Demonstração. Se $C_i = C$ para algum $i \in \{1, ..., n\}$, o resultado segue trivialmente. Por outro lado, se $C_i \neq C$, para todo $i \in \{1, ..., n\}$, estamos nas hipóteses do Lema 2.4.2. Logo, existe $i \in \{1, ..., n\}$ tal que

$$\min\{|C_i| + |\operatorname{Stab}(C_i)| : i = 1, ..., n\} \leqslant |C_i| + |\operatorname{Stab}(C_i)| \leqslant |C| + |\operatorname{Stab}(C)|.$$

□

Agora temos todas as ferramentas para demonstrar o teorema mais importante desta seção.

Teorema 2.4.2 (Teorema de Kneser)**.** *Sejam G um grupo abeliano e A e B subconjuntos não vazios e finitos de G. Se $H = \operatorname{Stab}(A + B)$ e $|A + B| < |A| + |B|$, então*

$$|A + B| = |A + H| + |B + H| - |H|.$$

Demonstração. Considere A e B subconjuntos não vazios e finitos de G satisfazendo as hipóteses. Como são finitos, podemos escrever $A = \{a_1, ..., a_m\}$ e $B = \{b_1, ..., b_n\}$. Para

cada $b_i \in B$, $i \in \{1, ..., n\}$, considere os pares de subconjuntos finitos (A_i, B_i) de G tais que

$$A \subset A_i,$$

$$b_i \in B_i,$$

$$A_i + B_i \subset A + B,$$

$$|A_i| + |B_i| = |A + H| + |B + H|.$$

Note que $(A+H, B+H)$ é um par de subconjuntos não vazios e finitos de G que satisfazem essas propriedades. Logo, a coleção não é vazia. Pela finitude dos conjuntos A_i, existe A_i tal que $|A_i|$ é maximal. Fixe (A_i, B_i) com esta propriedade. Considerando $C_i = A_i + B_i$, temos $|C_i| \leqslant |A_i|$ e

$$A + b_i \subset A_i + B_i = C_i \subset A + B.$$

Sejam $a \in A$ e $e = a - b_i$. Para este $e \in G$, usando a definição de e-transformada, temos

$$A_i(e) = A_i \cup (B_i + e) = A_i \cup (a + B_i - b_i)$$

e

$$B_i(e) = B_i \cap (A_i - e) = B_i \cap (-a + A_i + b_i).$$

Dessa forma, $A_i \subset A_i(e)$ e $b_i \in B_i(e)$. Pelo Lema 2.2.1, temos

$$A_i(e) + B_i(e) \subset A_i + B_i \subset A + B$$

e

$$|A_i(e)| + |B_i(e)| = |A_i| + |B_i| = |A + H| + |B + H|.$$

Como $A_i \subset A_i(e)$, segue que $A_i = A_i(e)$, pela maximalidade de $|A_i|$. Além disso, $a \in a + B_i - b_i \subset A_i$ para cada $a \in A_i$. Logo,

$$A_i \subset A_i + B_i - b_i = C_i - b_i \subset A_i,$$

ou seja, $A_i = C_i - b_i$. Então, $|A_i| = |C_i|$, $\operatorname{Stab}(A_i) = \operatorname{Stab}(C_i - b_i) = \operatorname{Stab}(C_i)$ e $B_i - b_i \subset \operatorname{Satb}(A_i) = \operatorname{Stab}(C_i)$. Com isso, $|B_i| \leqslant |\operatorname{Stab}(C_i)|$. Daí,

$$|A + H| + |B + H| = |A_i| + |B_i| \leqslant |C_i| + |\operatorname{Stab}(C_i)|,$$

para todo $i \in \{1, .., n\}$. Como $\bigcup_{i=1}^{n} C_i = A + B$, temos

$$\begin{aligned} |A + H| + |B + H| &= \min \{|C_i| + \operatorname{Stab}(C_i)\} \\ &\leqslant |A + B| + |\operatorname{Stab}(A + B)| \\ &= |A + B| + |H| \end{aligned}$$

pelo Lema 2.4.3. Pela Proposição 2.4.1, $|A+H|$, $|B+H|$ e $|A+B|$ são múltiplos de $|H|$. Isto posto, se $|A+H|+|B+H| < |A+B|+|H|$, então

$$|A|+|B| \leqslant |A+H|+|B+H| \leqslant |A+B|,$$

o que contradiz a hipótese deste teorema.

Portanto, $|A+H|+|B+H| = |A+B|+|H|$. □

O próximo resultado nos diz o que acontece se retirarmos a hipótese de $|A+B| < |A|+|B|$.

Teorema 2.4.3. *Sejam G um grupo abeliano e $A, B \subset G$ não vazios e finitos. Se $H = \mathrm{Stab}(A+B)$, então*

$$|A+B| \geqslant |A+H|+|B+H|-|H|.$$

Demonstração. Considere os subconjuntos de G como na hipótese deste teorema. Vamos separar em casos:

1. Caso em que $|(A+H)+(B+H)| \geqslant |A+H|+|B+H|$: Neste caso, nada há a fazer, pois
$$\begin{aligned} |A+B| =& |(A+H)+(B+H)| \\ \geqslant& |A+H|+|B+H| \\ \geqslant& |A+H|+|B+H|-|H|. \end{aligned}$$
2. Caso em que $|(A+H)+(B+H)| < |A+H|+|B+H|$: Neste caso, como $H = \mathrm{Stab}(A+B) = \mathrm{Stab}((A+H)+(B+H))$, podemos aplicar o Teorema 2.4.2 para os subconjuntos $A+H$ e $B+H$ de G e obter
$$|A+B| = |(A+H)+(B+H)| = |A+H|+|B+H|-|H|.$$

Portanto, o resultado é válido. □

Por fim, buscamos uma generalização do resultado anterior.

Corolário 2.4.2. *Sejam $n \geqslant 2$, $A_1, ..., A_n$ subconjuntos não vazios e finitos de um grupo abeliano G e $H = \mathrm{Stab}(A_1 + ... + A_n)$. Então*

$$|A_1 + ... + A_n| \geqslant |A_1| + ... + |A_n| - (n-1)|H|.$$

Demonstração. Vamos fazer a demonstração por indução sobre n. O caso $n = 2$ basta recorrer ao teorema anterior. Suponha $n \geqslant 3$ e que o resultado seja válido para $n-1$.

Considere $H' = \mathrm{Stab}(A_1 + ... + A_{n-1})$. Perceba que $H' \subset H$. Pela hipótese de indução, temos

$$\begin{aligned}|A_1 + \cdots + A_n| \geqslant & |A_1 + \cdots + A_{n-1}| + |A_n| - |H| \\ \geqslant & |A_1| + \cdots + |A_{n-1}| - (n-2)|H'| + |A_n| - |H| \\ \geqslant & |A_1| + \cdots + |A_{n-1}| + |A_n| - (n-1)|H|.\end{aligned}$$

ou seja, vale para n, e portanto, está demonstrado este corolário. □

2.5 Subgrupos de Índice Três em um Corpo

Esta seção será destinada a provar um resultado importante utilizado no estudo das sequências sobre $\mathbb{Z}_p$ que admitam soma-zero com peso em $U(p)^3$, em que

$$U(p)^3 = \{x^3 : x \in U(p)\}$$

e $U(p)$ é o grupo multiplicativo das unidades de $\mathbb{Z}_p$. Primeiramente, vamos provar uma série de resultados sobre subgrupos de índice três. Tais resultados podem ser encontrados também em [10].

Seja F um corpo e considere um grupo multiplicativo $G \subset F^*$ de índice n. Então, $x^n \in G$, para todo $x \in F^*$. Para simplificar a notação, vamos considerar $P = \sum G$ como o conjunto-soma $G + ... + G$, com m parcelas. Note que P satisfaz: $P + P \subset P$ e $P \cdot P \subset P$. Além disso, se $0 \neq x \in P$, então $x^{-1} \in P$, visto que $x^{-1} = x^{n-1}\,(x^{-1})^n$.

Lema 2.5.1. *Suponha $-1 \in P = \sum G$. Então P é um subcorpo de F. Além disso,*

1. *Se F é infinito, então $P = F$;*
2. *Se F é finito, com $[F : P] = d$ e $|P| = q$, então*

$$[F^* : P^*] = \frac{q^d - 1}{q - 1}.$$

Demonstração. Como $-1 \in P = \sum G$, então P também é fechado para a subtração, donde se torna um subcorpo de F. Além disso,

1. Suponha, por absurdo, que $P \neq F$. Daí, existe $\alpha \in F$ tal que $\alpha \notin P$. Note que, para cada $a \in P$, as classes laterais $(a + \alpha)P^*$ são todas distintas. De fato, se $(a + \alpha)P^* = (b + \alpha)P^*$, com $a, b \in P$, então existe $c \in P^*$ tais que $a + \alpha = (b + \alpha)c$. Equivalentemente, $a - bc = (c - 1)\alpha$. Caso $c \neq 1$, teríamos

$$\alpha = \frac{a - bc}{c - 1} \in P,$$

o que é uma contradição. Logo, $c = 1$ e $a = b$. Com isso,

$$\left|\frac{F^*}{P^*}\right| \geqslant |P|. \tag{2.9}$$

Além disso, por $G \subset P^*$, temos

$$\left|\frac{F^*}{G}\right| \geqslant \left|\frac{F^*}{P^*}\right| \text{ e } |P| \geqslant |G|. \tag{2.10}$$

Pelas Desigualdades (2.9) e (2.10), segue que

$$n = \left|\frac{F^*}{G}\right| \geqslant \left|\frac{F^*}{P^*}\right| \geqslant |P| \geqslant |G|.$$

Assim, $|G|$ é finito e, consequentemente, $|F^*|$ também o é. Mas, isso contraria a hipótese deste lema. Logo, $P = F$.

2. Sabemos que $|F| = |P|^{[F:P]} = q^d$. Como $|F|$ é finito, temos então

$$[F^* : P^*] = \frac{|F^*|}{|P^*|} = \frac{q^d - 1}{q - 1}.$$

□

A partir de agora vamos assumir que G é um subgrupo de F^* de índice três. Dessa forma, ${F^*}^3 \subset G$, senão extrapolaríamos a quantidade de classes laterais distintas de G em F^*. Em particular, $-1 \in G$. O próximo lema nos fornece uma propriedade importante dos subgrupos próprios de G.

Lema 2.5.2. *Seja G um subgrupo de índice três em F^*. Se $H \subset G$ é um subgrupo próprio de G, então existe $g \in G$ tal que $1 - g \notin G$ e $g \notin H$.*

Demonstração. Primeiramente vamos encontrar $g \in G$, $g \neq 1$, tal que $1 - g \notin G$. Se $G + G \subset G \cup \{0\}$, então $G \cup \{0\}$ é fechado para a adição. Se F é infinito, o Lema 2.5.1 garante que $F^* = G$, o que contraria nossa hipótese. Se F é finito, novamente pelo Lema 2.5.1, temos

$$3 = \frac{q^d - 1}{q - 1} \text{ e } d \in \{1, 2, 3\}, \text{ isto é, } |F| = 4 \text{ e } |G| = 1,$$

o que é um absurdo, pois G não admitiria subgrupo próprio. Assim, existem $a, b \in G$ tais que $a + b \notin G \cup \{0\}$. Defina $g = -a^{-1}b$. Note que $g \neq 1$, senão $a + b = 0$, o que é um absurdo. Além disso, $1 - g \notin G$, senão existiria $g' \in G$ tal que $1 + a^{-1}b = g'$. Neste caso, $a + b = ag' \in G$, o que é um absurdo. Sendo assim, vamos fixar tal $g \in G$.

Suponha que a conclusão deste lema seja falsa, ou seja, para todo $g \in G$, temos $1 - g \in G$ ou $g \in H$. Considere $c \in G \backslash H$. Como $c \notin H$, então $1 - c \in G$. Ainda mais, $g \in H$, pois $1 - g \notin G$. Com isso, concluímos que $cg \notin H$ e, consequentemente, $1 - cg \in G$. Note que $(1 - c) - (1 - cg) = -c(1 - g) \notin G$, senão $1 - g \in G$. Então,

$$x = \frac{1 - cg}{1 - c} \in G$$

e satisfaz $1-x \notin G$, donde $x \in H$. Além disso, $x \neq g$, pois $g \neq 1$. Dessa forma, se $|H| = n$, temos $n-1$ possibilidades para x, já que $g \in H$ e o mesmo acontece com c, uma vez que

$$c = \frac{x-1}{x-g}.$$

Como $c \in G\backslash H$ é qualquer, temos $|G\backslash H| \leqslant n-1$ e, por isso,

$$|G| \leqslant n + n - 1 = 2|H| - 1 < 2|H|.$$

Daí, $G = H$, pois teríamos $\dfrac{|G|}{|H|} = 1$, ou seja $G = H$, o que é um absurdo. Portanto, o resultado é válido. □

Lema 2.5.3. *Sejam F e G como acima. Suponha que as três classes laterais sejam G, aG e a^2G. Se $|F| > 7$, então $aG \cup a^2G \subset G + G$.*

Demonstração. Pelo Lema 2.5.2, existe $g \in G$ tal que $1 - g \notin G$ e $g^2 \neq 1$. Assim, $1-g$ e $1+g$ são diferentes de zero. Escolha $a \in F^*$ de tal forma que seu representante de classe seja $1-g$. Daí, existe $g' \in G$ tal que $a = (1-g)g' = g' + (-gg') \in G + G$ e, consequentemente, $aG \subset G + G$. Suponha que a tese deste resultado seja falsa. Logo, a^2G não está contida em $G+G$. Assim, concluímos que $a^2G \cap (G+G) = \emptyset$ e $(aG+aG) \cap G = \emptyset$. De fato, suponha que exista $x \in (G+G) \cap a^2G$. Então, existem $g_1, g_2, g_3 \in G$ tais que $x = g_1 + g_2 = a^2g_3$. Dado $h \in a^2G$, existe $g_4 \in G$ tal que $h = a^2g_4$. Logo,

$$h = a^2g_4 = a^2g_4\frac{g_3}{g_3} = (a^2g_3)\frac{g_4}{g_3} = (g_1+g_2)\frac{g_4}{g_3} = g_1\frac{g_4}{g_3} + g_2\frac{g_4}{g_3}.$$

Como $g_1\dfrac{g_4}{g_3}, g_2\dfrac{g_4}{g_3} \in G$, segue que $h \in G+G$, o que é um absurdo, pois teríamos $a^2G \subset G+G$. Ou seja, $a^2G \cap G + G = \emptyset$. Note que $a^3 \in G$ e, por $a^2G \cap (G+G) = \emptyset$, segue que $G \cap (aG + aG) = \emptyset$.

Como $1+g \in G+G$, então pelo que discutimos acima $1+g \notin a^2G$. Analogamente, $(1+g)(1-g) = 1-g^2 \notin a^2G$. Pela escolha de a, segue que $1+g \notin aG$, o que implica que $1+g \in G$. Novamente pela escolha de a, temos $1-g^2 \in aG$. Agora, vamos analisar o elemento 2. Como $2 = 1+1 \in G+G$, então $2 \notin a^2G$. Se $2 \in aG$, então $1+g = (1-g)+2g \in G \cap (aG+aG)$, o que já vimos que não acontece. Suponha $2 = 0$. Neste caso, $(1-g)^2 = 1+g^2 \in a^2G \cap (G+G)$, já que $(1-g)^2 \in a^2G$ pela escolha de a e $1, g^2 \in G$. Mas, isso é uma contradição com o que vimos na primeira parte da demonstração. Concluímos que $2 \in G$.

Agora, vamos analisar o elemento $1+g^2$. Como este elemento pertente a $G+G$, então já eliminamos a possibilidade dele pertencer a a^2G. Se $1+g^2 \in aG$, então $1-g^4 = (1+g^2)(1-g^2) \in (G+G) \cap a^2G$, o que é uma contradição. De forma similar, supondo $1+g^2 \in G$, temos $(1-g)^2 = (1+g^2) - 2g \in a^2G \cap (G+G)$, o que também é uma contradição. Por fim, se $1+g^2 = 0$, então $-2g = (1-g)^2 \in a^2G$, pela escolha de a, o que

nos traz outra contradição. Dessa forma, todas as possibilidade de $1+g^2$ estão eliminadas. Portanto, o resultado está demonstrado por redução ao absurdo. □

Lema 2.5.4. *Se $|F| > 16$, então $G \subset G+G$.*

Demonstração. Suponha, por absurdo, que G não esteja contido em $G+G$. Por consequência, $(G+G)\cap G = \emptyset$. De fato, se $(G+G)\cap G \neq \emptyset$, existiria $x \in G$ tal que $x \in G+G$, isto é, $x = g_1 + g_2$, com $g_1, g_2 \in G$. Assim, dado $z \in G$, temos

$$z = z\frac{x}{x} = \frac{z}{x}x = \frac{z}{x}(g_1+g_2) = \frac{z}{x}g_1 + \frac{z}{x}g_2 \in G+G,$$

o que é uma contradição com a nossa suposição de que G não está contido em $G+G$. Pelo Lema 2.5.2, existe $g \in G$ tal que $1-g \notin G$ e $g^4 \neq 1$. Dessa forma, $1-g$, $1+g$, $1-g^2$ e $1+g^2$ são diferentes de zero. Seja $a = 1-g \notin G$. Pela nossa suposição, como $1+g \in G+G$, temos $1+g \notin G$, donde $1-g^2 = (1-g)(1+g) \notin G$ e isso implica que $1+g \notin a^2G$, ou seja, $1+g \in aG$. De forma similar, como $1+g^2 \in G+G$, então $1+g^2 \notin G$. Agora, vejamos que $1-g^2 \in a^2G$. De fato, já vimos que $1-g^2$ é não nulo e não pertence a G. Supondo que $1-g^2 \in aG$, concluímos, pela escolha do elemento a, que $1+g \in G$, pois $a^3 \in G$, o que é um absurdo pelo que já vimos. Concluímos que $1-g^2 \in a^2G$. Como $(1+g^2)(1-g^2) = 1-g^4 \in G+G$, segue que $(1+g^2)(1-g^2) \notin G$. Vamos verificar que $1+g^2 \in a^2G$. De fato, como $1+g^2 \neq 0$ e $1+g^2 \notin G$, se $1+g^2 \notin a^2G$, a única possibilidade é que $1+g^2 \in aG$. Note que, por $1-g^2 \in a^2G$, teríamos $(1+g^2)(1-g^2) \in G$, pois $a^3 \in G$. Porém, já vimos que $(1+g^2)(1-g^2) \notin G$. Logo, temos $1+g^2 \in a^2G$. Agora, vamos analisar o que acontece com o elemento 2. Como $2 = 1+1 \in G+G$, então $2 \notin G$. Também temos $2 = (1+g)+(1-g) \in aG+aG$, pelo que já vimos. Assim, $2 \notin aG$, uma vez que G não intercepta $G+G$. Ainda é verdade que $2 \notin a^2G$, pois $2 = (1-g^2)+(1+g^2) \in a^2G+a^2G$. Logo, se a característica de F for diferente de 2, temos uma contradição, pois o elemento $2 \in F$ não seria 0, excluindo todas as suas possibilidades.

Suponha que a característica de F seja 2. Como $|F| > 16$, o Lema 2.5.2 garante que existe $h \in G$ tal que $1-h \notin G$ e $h^5 \neq 1$. Considere $a = 1+h$. Como $a \in G+G$, então $a \notin G$, já que G e $G+G$ não possuem interseção. Assim, podemos considerar as classes laterais como anteriormente. Como $a^3 = (1+h)^3 \in G$, segue que $(1+h)^4 \in aG$, ou seja, $(1+h)(1+h+h^2+h^3) = 1+h^4 = (1+h)^4 \in aG$, o que fornece $1+h+h^2+h^3 \in G$. Além disso, $1+h^3 \neq 0$, senão $h(1+h) = h+h^2 \in G$, o que é uma contradição pelo fato de G e $G+G$ não terem interseção. Como $(1+h+h^2)(1+h) = 1+h^3 \in G+G$, então $(1+h+h^2)(1+h) = 1+h^3 \notin G$, o que nos fornece $0 \neq 1+h+h^2 \notin a^2G$. Similarmente, $1+h+h^2 = (1+h)^3+h^3 \notin G$, logo $1+h+h^2 \in aG$. Seja $x = 1+h+h^2+h^3+h^4$. Então, $x(1+h) = 1+h^5 \in G+G$, ou seja, $x(1+h) \notin G$. Dessa forma, $x \notin a^2G$. Além disso, $x = (1+h+h^2+h^3)+h^4 \in G+G$, ou seja, $x \notin G$. Mais ainda, $x \neq 0$. De fato, se $x = 0$, então

$$h+h^2+h^3+h^4 = 1 \Rightarrow h^2+h^3+h^4+h^5 = h \Rightarrow h+h^2+h^3+h^4 = h^5.$$

Como $h + h^2 + h^3 + h^4 = 1$, teríamos $h^5 = 1$, o que é um absurdo. Logo, $x \neq 0$. Por fim, note que $x = (1 + h) + h^2(1 + h + h^2) \in aG + aG$, já que $(1 + h) \in aG$ e $1 + h + h^2 \in aG$. Entretanto, por G e $G + G$ não terem interseção, segue que aG não tem interseção com $aG + aG$. Logo, $x \notin aG$. Com isso, excluímos todas as possibilidades para o x, o que é um absurdo. Portanto, temos a veracidade deste resultado. □

Teorema 2.5.1. *Seja F um corpo com $|F| \neq 4, 7, 13, 16$. Suponha G subgrupo de índice 3 em F^*. Então, $G + G = F$.*

Demonstração. Com o Lema 2.5.3 e o Lema 2.5.4, concluímos que $G \subset G+G$ e $aG \cup a^2G \subset G + G$, quando $|F| > 16$. Logo, $F^* = G \cup aG \cup a^2G \subset G + G$. Como $G + G \subset F$, segue que $F = G + G$, quando $|F| > 16$. Note que os casos em que $|F| \leqslant 16$, não precisamos nos preocupar. De fato, como F^* admite um subgrupo G de índice três, então $|F| \equiv 1 \pmod 3$, ou seja, $|F| \in \{4, 7, 13, 16\}$, o que não é possível, pelas hipóteses deste teorema. □

Teorema 2.5.2. *Seja F um corpo finito com $|F| = q$ e $q \neq 4, 7$. Suponha G subgrupo de índice 3 em F^*. Se $a \in G + G$, $a \notin G \bigcup \{0\}$, então $G + aG = F^*$.*

Demonstração. Primeiramente, note que $G + aG \subset F$, dado que F é corpo. Vamos mostrar que $0 \notin G + aG$. De fato, se $0 \in G + aG$, existem $g_1, g_2 \in G$ tais que $0 = g_1 + ag_2$. Mas, isso fornece que $a = -\dfrac{g_1}{g_2} \in G$, o que contradiz a hipótese deste teorema. Logo, $G + aG \subset F^*$. Agora. vamos provar a inclusão contrária. Note que $G \subset G + aG$. De fato, como $a \in G + G$, existem $g, h \in G$ tais que $a = g + h$. Dessa forma, $g = -h + a \in G + aG$, logo $G \subset G + aG$. Se $|F| \neq 4, 7$, o Lema 2.5.3 nos garante que podemos escrever $a^2 = x + y$, em que $x, y \in G$. Daí, $ax = a^3 - ay \in G + aG$, donde $aG \subset G + aG$. Por fim, falta mostrar que $a^2G \subset G + aG$. Seja $W = \{g - 1 : 1 \neq g \in G\}$. Como G é uma classe lateral e tem índice três em F^*, segue que $|G| = \dfrac{q-1}{3}$. Concluímos então que W possui exatamente $\dfrac{q-1}{3} - 1 = \dfrac{q-4}{3}$ elementos. Considere também os conjuntos $W^{-1} = \{w^{-1} : w \in W\}$ e $V = G \cup W \cup W^{-1}$. Note

$$\begin{aligned} |V| =& |G| + |W| + |W^{-1}| - |G \cap W \cap W^{-1}| \\ =& \frac{q-1}{3} + \frac{q-4}{3} + \frac{q-4}{3} - |G \cap W \cap W^{-1}| \\ \leqslant& q - 3. \end{aligned}$$

Assim, existe $\delta \in F^*$ tal que $\delta \notin V$. Daí, δ não está em G. Analogamente, $\delta \notin W$, donde $\delta^{-1} \notin W$. Suponha que $1 + \delta \in G$, ou seja, existe $g \in G$ tal que $1 + \delta = g$. Entretanto, isso nos fornece $\delta \in W$, o que é um absurdo. Logo, $1 + \delta \notin G$. Similarmente, $1 + \delta^{-1} \notin G$. De forma imediata, concluímos que $1 + \delta \notin \delta G$, senão teríamos uma contradição com o fato de que $1 + \delta^{-1} \notin G$. Ou seja, $1 + \delta \notin G \cup \delta G$, forçando $1 + \delta \in \delta^2 G$. Logo, $\delta^2 G \subset G + \delta G$ e, consequentemente, $\delta G \subset G + \delta^2 G$. Por se tratar de classes laterais, segue que aG é igual a δG ou $\delta^2 G$. Se $aG = \delta^2 G$, então $a^2 G = \delta G$ e $a^2 G \subset G + aG$. Se $aG = \delta G$, então

$a^2G = \delta^2 G$ e $a^2G \subset G + aG$. De qualquer forma, $a^2G \subset G + aG$, como queríamos. Com isso, concluímos a inclusão contrária, visto que $F^* = G \cup aG \cup a^2G \subset G + aG$. Portanto, este teorema está devidamente demonstrado. □

3 Constante de Davenport com peso

Neste capítulo, vamos focar no estudo da constante de Davenport com peso, uma generalização da clássica constante de Davenport, que é um conceito fundamental na teoria aditiva de grupos. A constante de Davenport, denotada por $D(G)$, representa o menor inteiro k tal que toda sequência de k elementos em um grupo finito G possua uma subsequência de soma-zero. Ao longo dos anos, diversas variações dessa constante foram exploradas, e uma delas envolve a adição de pesos aos elementos da sequência, focando em subsequências de soma-zero tanto gerais quanto consecutivas. Neste capítulo utilizamos resultados que podem ser encontrados em [12].

3.1 Introdução

Definição 3.1.1. *Seja $(G,+)$ um grupo finito. Uma sequência $S=(x_1,\ldots,x_l)$ é chamada sequência de soma-zero quando $x_1+x_2+\cdots+x_l=0$, em que 0 é o elemento neutro do grupo G.*

Teorema 3.1.1. *Seja $(G,+)$ um grupo finito, com $|G|=n$ e $k\geq n$. Se $S=(x_1,...,x_k)$ é uma sequência sobre G de tamanho k, existem $i,j\in\{1,...,k\}$ tal que $i\leq j$ e $x_i+x_{i+1}+\cdots+x_j=0$.*

Demonstração. Seja $S=(x_1,...,x_k)$ uma sequência sobre G de tamanho k e defina $y_i=x_1+x_2+\cdots+x_i$, para cada $i\in\{1,...,k\}$. Se $y_i=0$ para algum $i\in\{1,...,k\}$, então o resultado é válido. Agora, suponha $y_i\neq 0$, $\forall i\in\{1,...,k\}$. Como $k\geq n$, pelo Princípio da Casa dos Pombos, existem $i,j\in\{1,...,k\}$, com $i<j$, tais que $y_i=y_j$. Dessa forma, $-y_i+y_j=0$, ou seja,

$$0=-y_i+y_j=-x_i-x_{i-1}-\cdots-x_1+x_1+x_2+\cdots+x_j=x_{i+1}+\cdots+x_j.$$

□

A partir daqui, sempre que escrevermos sobre subsequência, subentende-se que seja uma subsequência não vazia da sequência original.

Definição 3.1.2. *Para um grupo abeliano finito G, a constante (consecutiva) de Davenport, denotada por $D(G)$ ($C(G)$), é definida como o menor inteiro k tal que toda sequência em G de k elementos admite uma subsequência (de termos consecutivos) de soma-zero.*

Com o Teorema 3.1.1, temos $C(G) \leqslant |G|$, para todo grupo finito G. Além disso, $D(G) \leqslant C(G)$. Logo, essas constantes existem para qualquer grupo abeliano finito G. Vejamos um exemplo:

Exemplo 3.1.1. *Seja $G = \mathbb{Z}_6$ o grupo aditivo dos inteiros módulo 6. Vamos calcular as constantes de Davenport de G. Considere a sequência $S = (1, 1, 1, 1, 1)$ sobre $\mathbb{Z}_6$ de tamanho 5. Note que tal sequência não admite subsequência de soma-zero, logo $C(G) \geqslant D(G) \geqslant 6$. Dessa forma, $6 \leqslant D(G) \leqslant C(G) \leqslant 6$, pelo Teorema 3.1.1. Portanto, $D(G) = C(G) = 6 = |G|$.*

O exemplo acima ilustra que a constante de Davenport coincide com a ordem do grupo. Veremos mais a frente que o mesmo ocorre para todos os grupos cíclicos.

Para o restante da seção, R será considerado um anel com unidade e A um subconjunto não vazio de R.

Definição 3.1.3. *Dado um R-módulo M e A subconjunto de R não vazio, uma sequência $S = (x_1, ..., x_k)$ sobre M é chamada sequência de soma-zero com peso em A se para cada $i \in \{1, ..., k\}$, existem $a_i \in A$ tais que*

$$a_1x_1 + \cdots + a_kx_k = 0.$$

Quando $A = \{1\}$, uma sequência de soma-zero com peso em A é chamada simplesmente de sequência de soma-zero.

Definição 3.1.4. *Sejam M um R-módulo finito e $A \subset R$ não vazio. A constante de Davenport de M com peso em A, $D_A(M)$, é definida como o menor inteiro positivo k tal que qualquer sequência sobre M de tamanho k admite uma subsequência de soma-zero com peso em A.*

Observação 3.1.1. *Pelo Teorema 3.1.1, notamos que em um grupo abeliano finito $(G, +)$, sempre conseguimos uma subsequência de termos consecutivos de soma-zero.*

Isso motiva a seguinte definição:

Definição 3.1.5. *Sejam M um R-módulo finito e $A \subset R$ não vazio. A constante consecutiva de Davenport de M com peso em A, $C_A(M)$, é definida como o menor inteiro positivo k tal que qualquer sequência sobre M de tamanho k admite uma subsequência de termos consecutivos de soma-zero com peso em A.*

Observação 3.1.2. *Sejam M um R-módulo finito e $A \subset R$ não vazio. As constantes $D_A(M)$ e $C_A(M)$ existem.*

Demonstração. Sejam M um R-módulo finito, com $|M| = n$, e $A \subset R$ não vazio. Dado uma sequência $S = (x_1, ..., x_n)$ sobre M de tamanho $|M|$, de forma similar ao Teorema 3.1.1, conseguimos encontrar uma subsequência de termos consecutivos T de S de soma-zero. Ou seja, existem $i, j \in \{1, ..., n\}$, com $i < j$, tais que $T = (x_i, x_{i+1}, ..., x_j)$ e $x_i + x_{i+1} + \cdots + x_j = 0$. Note que se multiplicarmos a equação anterior por um elemento $a \in A$ qualquer, teremos que T é uma subsequência de termos consecutivos de soma-zero com peso em A. De fato,

$$ax_i + ax_{i+1} + \cdots + ax_j = a(x_i + x_{i+1} + \cdots + x_j) = a \cdot 0 = 0.$$

Dessa forma, para qualquer $A \subset R$ não vazio, temos $C_A(M) \leq |M|$. Além disso, para qualquer $A \subset R$ não vazio, temos $D_A(M) \leq C_A(M)$. Portanto, as constantes $C_A(M)$ e $D_A(M)$ existem. □

Quando $A = \{1\}$, denotamos $C_A(M)$ e $D_A(M)$ por $C(M)$ e $D(M)$, respectivamente. Além disso, vamos considerar o anel $\mathbb{Z}_n$ como um $\mathbb{Z}_n$-módulo e $A \subset \mathbb{Z}_n$. Para simplificar as notações, denotaremos $C_A(\mathbb{Z}_n)$ e $D_A(\mathbb{Z}_n)$ por $C_A(n)$ e $D_A(n)$, respectivamente.

Para o resultado abaixo, vamos considerar o grupo G como um $\mathbb{Z}$-módulo.

Corolário 3.1.2. *Se G é um grupo cíclico finito, então $D(G) = C(G) = |G|$.*

Demonstração. Seja G um grupo cíclico finito, com $|G| = n$. Se $n = 1$, então $G = \{0\}$ e o resultado é válido, pois a única sequência possível é a sequência de tamanho 1 formada pelo elemento neutro do grupo G. Suponha $n \geqslant 2$. Pelo Teorema 3.1.1, temos $C(G) \leqslant |G|$. Dessa forma, $D(G) \leqslant C(G) \leqslant |G|$. Agora, basta mostrar $D(G) \geq n$. Como G é um grupo cíclico, existe $g \in G$ tal que $G = \langle g \rangle$. Considere a sequência constante $S = (g, ..., g)$ de tamanho $n - 1$. Como a ordem do elemento g é $n = |G|$, então S não admite subsequência de soma-zero, donde $D(G) \geq n$. Portanto,

$$|G| \leqslant D(G) \leqslant C(G) \leqslant |G|,$$

ou seja, $D(G) = C(G) = |G|$. □

Teorema 3.1.2. *Para $A = \mathbb{Z}_n \backslash \{0\}$, temos $D_A(n) = C_A(n) = 2$.*

Demonstração. Como $A = \mathbb{Z}_n \backslash \{0\}$, então se considerarmos a sequência unitária formada pelo elemento $1 \in \mathbb{Z}_n$, não existe $a \in \mathbb{Z}_n \backslash \{0\}$ tal que $a \cdot 1 = 0$. Daí, $C_A(n) \geqslant D_A(n) \geqslant 2$. Seja $S = (x_1, x_2)$ uma sequência qualquer sobre $\mathbb{Z}_n$. Se $x_1 = 0$ ou $x_2 = 0$, então temos uma subsequência de S de soma-zero com tamanho 1, ou seja, $C_A(n) \leqslant 2$. Agora, se $x_1 \neq 0$ e $x_2 \neq 0$, então tomando $a_1 = x_2$, $a_2 = -x_1 \in A$, temos $a_1x_1 + a_2x_2 = 0$. Logo, a sequência S possui soma-zero com peso em A, ou seja, $C_A(n) \leqslant 2$. Assim, em todos os casos, temos $2 \geqslant C_A(n) \geqslant D_A(n) \geqslant 2$, o que termina a demonstração. □

Para $j \geqslant 1$, definimos $U(n)^j = \{x^j : x \in U(n)\}$, em que

$$U(n) = \{x \in \mathbb{Z}_n : (x, n) = 1\}.$$

Observação 3.1.3. *Pelo Teorema 3.1.2, se p é um número primo, temos $D_{U(p)}(p) = C_{U(p)}(p) = 2$.*

Se $n = p_1 p_2 \dots p_k$, em que p_i é um número primo para cada $i \in \{1, ..., k\}$, definimos $\Omega(n) = k$. Além disso, para um divisor m de n, definimos o homomorfismo canônico

$$f_{n,m} : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$$

tal que $f(a + n\mathbb{Z}) = a + m\mathbb{Z}$. Ao considerar a soma

$$a_1 x_1 + \cdots + a_s x_s,\ x_1, ..., x_s \in \mathbb{Z}_n \text{ e } a_1, ..., a_s \in \mathbb{Z},$$

a ação do homomorfismo na soma acima resulta em

$$a_1 f_{n,m}(x_1) + \cdots + a_s f_{n,m}(x_s),$$

pois cada $a_i x_i$, $i \in \{1, ..., s\}$, é visto como $x_i + \cdots + x_i$, em que a soma é feita a_i vezes.

Observação 3.1.4. *Seja $A \subseteq \mathbb{Z}_m - \{0\}$ e $m \in \mathbb{N}$ dado. Considere a sequência*

$$(1, \underbrace{0, \dots, 0}_{m-1}, 1, \underbrace{0, \dots, 0}_{m-1}, 1, 0, \dots),$$

em $\mathbb{Z}_n$ de tamanho arbitrário. Essa sequência não possui subsequência consecutiva de soma-zero de tamanho m, ou seja, não podemos prescrever $C_A(G)$.

3.2 Caso $A = U(p)^2$, em que p é um número primo

Sejam p um número primo e $A = U(p)^2$. Note que $A = Im(\phi)$, em que $\phi : U(p) \to U(p)$ é definida por $\phi(x) = x^2$. Além disso, o único elemento de ordem 2 no grupo multiplicativo $U(p) = \mathbb{Z}_p$ é $p - 1$. De fato, se $p - i \in U(p)$, então

$$1 = (p - i)^2 \Leftrightarrow 1 = p^2 - 2pi + i = i,$$

ou seja, a classe i em $\mathbb{Z}_p$ deve ser a mesma classe do 1 em $\mathbb{Z}_p$ para que tenhamos um elemento de ordem 2. Logo, o único elemento de ordem 2 em $U(p)$ é $p - 1$. Ainda temos $1^2 = 1$. Com isso, $ker(\phi) = \{-1, 1\}$. Pelo Primeiro Teorema do Isomorfismo,

$$\frac{U(p)}{\{-1, 1\}} \cong \operatorname{Im} \psi = U(p)^2 \Rightarrow \left|U(p)^2\right| = \frac{p-1}{2}.$$

Teorema 3.2.1. *Para um primo p, temos $D_{U(p)^2}(p) = C_{U(p)^2}(p) = 3$ quando $p \neq 2$ e $D_{U(2)^2}(2) = C_{U(2)^2}(2) = 2$.*

Demonstração. Quando $p = 2$ ou $p = 3$, temos $U(p)^2 = \{1\}$, pois

$$U(2)^2 = \left\{x^2 \mid x \in U(2)\right\} = \left\{1^2\right\} = \{1\} \text{ e } U(3)^2 = \left\{x^2 \mid x \in U(3)\right\} = \left\{1^2, 2^2\right\} = \{1\}.$$

Como $\mathbb{Z}_p$ é cílico, $D_{U(3)^2}(3) = C_{U(3)^2}(3) = 3$ e $D_{U(2)^2}(2) = C_{U(2)^2}(2) = 2$, pelo Corolário 3.1.2. Para $p = 5$, temos

$$U(5)^2 = \left\{x^2 \mid x \in U(5)\right\} = \{1, 4, 9, 16\} = \{1, 4\} = \{-1, 1\}.$$

Suponha $S = (x, y, z)$ uma sequência sobre $\mathbb{Z}_5$ e considere o conjunto $\{x \pm y, -x \pm y, \pm z\}$. Como este conjunto possui seis elementos de $\mathbb{Z}_5$, então pelo menos dois elementos deste conjunto são iguais. Daí, conseguimos uma subsequência de termos consecutivos de soma-zero e peso em Q_5. Sendo assim, $D_{U(5)^2}(5) \leqslant C_{U(5)^2}(5) \leqslant 3$.

Para um primo $p \geqslant 7$, seja $S = (x, y, z)$ uma sequência sobre $\mathbb{Z}_p$. Se algum termo da sequência é zero, temos uma subsequência de soma-zero com peso em Q_p de tamanho 1. Suponha que os elementos de S são não nulos. Para $w \in \mathbb{Z}_p$, considere a classe lateral $U(p)^2 w = \{aw : a \in U(p)^2\}$. Assim,

$$\left|U(p)^2 x\right| = \left|U(p)^2 y\right| = \left|U(p)^2 z\right| = \left|U(p)^2\right| = \frac{p-1}{2}.$$

Note:

$$\left|U(p)^2 x\right| + \left|U(p)^2 y\right| + \left|U(p)^2 z\right| - 2 = \frac{(3p-3)}{2} - 2 = \frac{3p-7}{2} \geqslant p,$$

pois $p \geqslant 7$. Como $|U(p)^2 x + U(p)^2 y + U(p)^2 z| \leqslant p$, pelo Corolário 2.3.1, temos

$$U(p)^2 x + U(p)^2 y + U(p)^2 z = \mathbb{Z}_p.$$

Então, existem $a_1, a_2, a_3 \in U(p)^2$ tais que $a_1 x + a_2 y + a_3 z = 0$. Dessa forma, S é uma sequência sobre $\mathbb{Z}_p$ de soma-zero com peso em $U(p)^2$. Logo, $D_{U(p)^2}(p) \leqslant C_{U(p)^2}(p) \leqslant 3$.

Agora, vamos mostrar que $D_{U(p)^2}(p) \geqslant 3$, para $p \geqslant 5$ primo. Considere $x \in U(p) \backslash U(p)^2$. Vamos verificar que $(-1, x)$ é uma sequência sobre $\mathbb{Z}_p$ que não admite uma subsequência de soma-zero com peso em $U(p)^2$. De fato, $0 \notin U(p)^2$ e $x, -1$ são não nulos, logo não existe uma subsequência de tamanho 1 de soma-zero com peso em $U(p)^2$. Agora, suponha que existam $a, b \in U(p)^2$ tais que $ax + b(-1) = 0$. Daí, $x = a^{-1} \cdot b$. Como $U(p)^2$ é um subgrupo de $U(p)$ e $a \in U(p)^2$, então $a^{-1} \in U(p)^2$. Sendo assim, $a^{-1} \cdot b \in U(p)^2$ o que contradiz o fato de $x \in U(p) \backslash U(p)^2$. Logo, $D_{U(p)^2}(p) \geqslant 3$, para $p \geqslant 5$ primo.

Portanto, reunindo todas as informações, temos

$$3 \leqslant D_{U(p)^2}(p) \leqslant C_{U(p)^2}(p) \leqslant 3,$$

ou seja, $D_{U(p)^2}(p) = C_{U(p)^2}(p) = 3$, para $p \geqslant 5$ primo, o que finaliza a demonstração. □

3.3 Caso $A = U(p)^3$, em que p é um número primo

Quando $p \not\equiv 1 \pmod 3$, não existe elemento de ordem três em $U(p)$. De fato, se existisse elemento de ordem três em $U(p)$, então existiria um subgrupo de $U(p)$ de ordem três, o que contradiz o fato de $p \not\equiv 1 \pmod 3$, pelo Teorema de Lagrange. Daí, o núcleo de ψ é trivial, em que $\psi : U(p) \to U(p)$ é definida por $\psi(x) = x^3$. Pelo Primeiro Teorema do Isomorfismo, $U(p)^3 = U(p)$. Neste caso, pelo Teorema 3.1.2, temos $D_{U(p)^3}(p) = C_{U(p)^3}(p) = 2$.

Quando $p \equiv 1 \pmod 3$, existe um elemento c de ordem três em $U(p)$, pelo Lema de Cauchy. Então, o núcleo de ψ é o subgupo cíclico $\langle c\rangle = \operatorname{Ker}\psi$. Note que $U(p)^3 = \operatorname{Im}(\psi)$. Assim, pelo Teorema de Lagrange, $U(p)^3$ é um subgrupo de índice três em $U(p)$.

Lema 3.3.1. *Seja p um número primo tal que $p \equiv 1 \pmod 3$ e $p \neq 7, 13$. Suponha que S seja uma sequência sobre $\mathbb{Z}_p$ tal que pelo menos três elementos estão em $U(p)$. Então, S é uma sequência de soma-zero com peso em $U(p)^3$.*

Demonstração. Seja S uma sequência sobre $\mathbb{Z}_p$ e x, y, z elementos de S que estão em $U(p)$. Tome w como a soma dos termos restantes de S, caso existam. A equação $zX^3 = w$ possui no máximo três raízes em $\mathbb{Z}_p$. Como existem pelo menos quatro elementos em $U(p)$ quando $p > 5$, podemos encontrar $t \in U(p)$ tal que $zt^3 \neq w$. Assim, se $z' = w - zt^3$, temos $z' \neq 0$. Note que, se existirem $a, b, c \in U(p)^3$ tais que $ax + by + c(-t^3)z + cw = 0$, então S é uma sequência de soma-zero com peso em $U(p)^3$, pois por $-1, t^3 \in U(p)^3$, temos $-t^3 \in U(p)^3$. Dessa forma, é suficiente mostrar que $S' = (x, y, z')$ é uma sequência de soma-zero com peso em $U(p)^3$. Para qualquer $c \in U(p)$, a sequência (cx, cy, cz') é uma sequência de soma-zero com peso em $U(p)^3$ se, e somente se, (x, y, z') também o é. Como $c \in U(p)$ é qualquer, pelo automorfismo $\psi : U(p) \to U(p)$ definido por $\psi(v) = cv$, podemos escolher c de forma que $cx \in U(p)^3$, caso $x \notin U(p)^3$. Logo, podemos assumir $x \in U(p)^3$. Agora, note que $|\mathbb{Z}_p| = p \notin \{7, 13\}$, e além disso, $p \notin \{4, 16\}$, pois p é um número primo. Dessa forma, como $U(p)^3$ tem índice 3 em $U(p) = \mathbb{Z}_p^*$, as hipóteses do Teorema 2.5.1 estão verificadas, logo $U(p)^3 + U(p)^3 = \mathbb{Z}_p$. Temos duas possibilidades:

1. Se $y \in U(p)^3$, então $U(p)^3 y = U(p)^3$ e, por $U(p)^3 + U(p)^3 = \mathbb{Z}p$, temos que $-z' \in U(p)^3 + U(p)^3 = U(p)^3 + U(p)^3 y$, pois $-z' \in \mathbb{Z}_p$.

2. Se $y \notin U(p)^3$, então $y \notin U(p)^3 \cup \{0\}$, pois y é uma unidade de $\mathbb{Z}_p$. Como $y \in \mathbb{Z}_p$ e $U(p)^3 + U(p)^3 = \mathbb{Z}_p$, então $y \in U(p)^3 + U(p)^3$. Pelo Teorema 2.5.2, temos $U(p)^3 + yU(p)^3 = U(p)$. Como $z' \neq 0$, então $-z \in U(p) = U(p)^3 + U(p)^3 y$.

Em ambos os casos, $-z \in U(p) = U(p)^3 + U(p)^3 y$. Como $x \in U(p)^3$, temos $U(p)^3 = U(p)^3 x$. Dessa forma, $-z' \in U(p)^3 x + U(p)^3 y$, ou seja, existem $a, b \in U(p)^3$ tais que $-z' = ax + by$.

Daí,

$$ax + by + w - zt^3 = 0,$$

isto é, S' é uma sequência de soma-zero com peso em $U(p)^3$. Pela discussão feita anteriormente, S é uma sequência de soma-zero com peso em $U(p)^3$. □

Observação 3.3.1. *O Lema 3.3.1 não é válido para $p = 7$ e $p = 13$. Note que $U(7)^3 = \{\pm 1\}$ e $U(13)^3 = \{\pm 1, \pm 5\}$. Considere a sequência $(1, 1, 1)$ sobre $\mathbb{Z}_p$. É claro que pelo menos 3 elementos dessa sequência são unidades, pois $1 \in U(p)$. Agora, basta notar que não existem $a_1, b_1, c_1 \in U(7)^3$ ou $a_2, b_2, c_2 \in U(13)^3$ tais que*

$$a_1 \cdot 1 + b_1 \cdot 1 + c_1 \cdot 1 = 0$$

ou

$$a_2 \cdot 1 + b_2 \cdot 1 + c_2 \cdot 1 = 0.$$

Teorema 3.3.1. *Se p é um número primo tal que $p \equiv 1 \pmod 3$, temos $D_{U(p)^3}(p) \geqslant 3$. Mais ainda, se $p \neq 7$, $D_{U(p)^3}(p) = C_{U(p)^3}(p) = 3$.*

Demonstração. Seja $x \in U(p) \backslash U(p)^3$ com p um número primo tal que $p \equiv 1 \pmod 3$. A sequência $(-1, x)$ não admite uma subsequência de soma-zero com peso em $U(p)^3$. De fato, $\mathbb{Z}_p$ é corpo e, em particular, um domínio. Logo, não existe $a \in U(p)^3$ tal que $a(-1) = 0$ ou $ax = 0$, visto que a, x são não nulos. Agora, se $(-1, x)$ fosse uma sequência de soma-zero com peso em $U(p)^3$, existiriam $a, b \in U(p)^3$ tais que $a(-1) + bx = 0$, ou seja, $bx = a$. Como $U(p)^3$ é subgrupo de $U(p)$ e $b \in U(p)^3$, existe $b^{-1} \in U(p)^3$. Daí, $x = b^{-1}a$. Além disso, $a \in U(p)^3$ e, consequentemente, $x = b^{-1}a \in U(p)^3$ o que é falso, pois $x \in U(p) \backslash U(p)^3$. Logo, $D_{U(p)^3}(p) \geqslant 3$.

Para a segunda parte, seja $S = (x, y, z)$ uma sequência sobre $\mathbb{Z}_p$, com $p \notin \{7, 13\}$. Queremos mostrar que S possui subsequência de termos consecutivos de soma-zero com peso em $U(p)^3$. Podemos assumir $x, y, z \in U(p)$, pois $U(p) = \mathbb{Z}_p^*$ e, se $x, y, z \notin U(p)$, então x, y, z são nulos, o que geraria uma subsequência de soma-zero e tamanho um com peso em $U(p)^3$. Como $p \equiv 1 \pmod 3$ e $p \neq 7$, pelo Lema 3.3.1, S é uma sequência de soma-zero com peso em $U(p)^3$, pois $x, y, z \in U(p)$. Daí, $C_{U(p)^3}(p) \leqslant 3$. Como temos $D_{U(p)^3} \leqslant C_{U(p)^3}(p) \leqslant 3$ e $D_{U(p)^3}(p) \geqslant 3$ como visto anteriormente, então $D_{U(p)^3} = C_{U(p)^3}(p) = 3$.

Como $13 \equiv 1 \pmod 3$, pela primeira parte demonstrada neste Lema, temos $C_{U(p)^3}(p) \geqslant D_{U(p)^3} \geqslant 3$. Falta mostrar que $C_{U(p)^3}(p) \leqslant 3$. Seja $S = (x, y, z)$ uma sequência sobre $\mathbb{Z}_{13}$. Podemos assumir $x, y, z \in U(13)$ e mais ainda, podemos supor $x \in U(13)^3$ por motivos já vistos anteriormente.

1. Suponha $y \in U(13)^3$. Então, (x, y) é uma subsequência de soma-zero com peso em $U(13)^3$, pois $yx - xy = 0$ e $y, x \in U(13)^3$. Então, $C_{U(13)^3}(13) \leqslant 3$.

2. Suponha $y \in B = U(13)\backslash U(13)^3$. Como $U(13)^3 = \{\pm 1, \pm 5\}$, então

$$B = \{\pm 2, \pm 3, \pm 4, \pm 6\}.$$

Note que qualquer elemento de B pode ser escrito como uma soma de um elemento de $U(13)^3$ com outro elemento de $U(13)^3$, isto é, $B \subset U(B)^3 + U(B)^3$. Como $|\mathbb{Z}_{13}| \neq 4, 7$, $U(13)^3$ tem índice 3 em $U(13)$, $y \in B \subset U(13)^3 + U(13)^3$ e $y \notin U(13)^3 \bigcup \{0\}$, temos $U(13)^3 + U(13)^3 y = U(13)$. Como $x \in U(13)^3$, então $U(13)^3 = U(13)^3 x$. Daí, $U(13) = U(13)^3 x + U(13)^3 y$. Como $z \in U(13)$ e $U(13)$ é um grupo multiplicativo, $-z \in U(13)$, pois $-1 \in U(13)$. Daí, existem $a, b \in U(13)^3$ tais que $-z = ax + by$, ou seja, $ax + by + z = 0$. Logo, S é uma sequência de soma-zero com peso em $U(13)^3$. Daí, $C_{U(13)^3}(13) \leqslant 3$.

Assim, $D_{U(13)^3}(13) = C_{U(13)^3} = 3$. □

Perceba que, até este momento, as constantes de Davenport se coincidiram. O próximo resultado nos fornece um caso em que isso não é verdadeiro.

Lema 3.3.2. *Temos* $D_{U(7)^3}(7) = 3$ *e* $C_{U(7)^3}(7) = 4$.

Demonstração. Observe que $U(7)^3 = \{1^3, 2^3, 3^3, 4^3, 5^3, 6^3\} = \{\pm 1\}$. Seja $S = (x, y, z)$ uma sequência sobre $\mathbb{Z}_7$ de tamanho três. Queremos mostrar que S possui uma subsequência de soma-zero com peso em $\{\pm 1\}$. Podemos supor que $x, y, z \in U(7)$, caso contrário, teremos uma subsequência de S de soma-zero com peso em $\{\pm 1\}$ trivialmente. Se quaisquer dois termos da sequência S são iguais a menos de sinal, então conseguimos uma subsequência de S de soma-zero com peso em $\{\pm 1\}$. Por outro lado, como $U(7) = \{\pm 1, \pm 2, \pm 3\}$, a menos de permutação ou troca de sinais, a sequência S é $(1, 2, 3)$, que é uma sequência de soma-zero em $\{\pm 1\}$. Daí, $D_{\{\pm 1\}}(7) \leqslant 3$. Logo, segue do Teorema 3.3.1 que $D_{U(7)^3}(7) = D_{\{\pm 1\}}(7) = 3$.

Como a sequência $(1, 3, 1)$ sobre $\mathbb{Z}_7$ não possui subsequência consecutiva de soma-zero com peso em $\{\pm 1\}$, então $C_{\{\pm 1\}}(7) \geqslant 4$. Considere $S = (x, y, z, w)$ em $\mathbb{Z}_7$. Considere a sequência $(x+y, x-y, -x+y, -x-y, z+w, z-w, -z+w, -z-w)$ de tamanho oito sobre $\mathbb{Z}_7$. Pelo Princípio da Casa dos Pombos, pelo menos dois termos dessa sequência são iguais, donde conseguimos uma subsequência de termos consecutivos de S de soma-zero com peso em $\{\pm 1\}$. Então, $C_{\{\pm 1\}}(7) \leqslant 4$ e, consequentemente, $C_{U(7)^3}(7) = C_{\{\pm 1\}}(7) = 4$. □

3.4 Caso $A = U(n)$

Lema 3.4.1. *Sejam* $n = m_1 m_2$ *e* A, A_1, A_2 *subconjuntos de* $\mathbb{Z}_n, \mathbb{Z}_{m_1}$ *e* $\mathbb{Z}_{m_2}$, *respectivamente. Suponha* $f_{n,m_1}(A) \subset A_1$ *e* $f_{n,m_2}(A) \subset A_2$. *Então,* $C_A(n) \geqslant C_{A_1}(m_1) C_{A_2}(m_2)$.

Demonstração. Sejam $C_{A_1}(m_1) = \kappa$ e $C_{A_2}(m_2) = \ell$. Lembre-se que essas constantes existem, pela Observação 3.1.2. Assuma que essas constantes, κ e ℓ, sejam pelo menos 2. Como $C_{A_1}(m_1) = \kappa$, existe uma sequência $S_1' = (x_1', ..., x_{\kappa-1}')$ sobre $\mathbb{Z}_{m_1}$ de tamanho $\kappa - 1$ que não admite subsequência de termos consecutivos de soma-zero com peso em A_1. Analogamente, como $C_{A_2}(m_2) = \ell$, existe uma sequência $S_2' = (y_1', ..., y_{\ell-1}')$ sobre $\mathbb{Z}_{m_2}$ de tamanho $\ell - 1$ que não admite subsequência de termos consecutivos de soma-zero com peso em A_2.

Para cada $i \in \{1, ..., \kappa - 1\}$, sejam $f_{n,m_1}(x_i) = x_i'$ e $S_1 = (m_2x_1, ..., m_2x_{\kappa-1})$. Para cada $j \in \{1, ..., \ell - 1\}$, sejam $f_{n,m_2}(y_j) = y_j'$ e $S_2 = (y_1, ..., y_{\ell-1})$. Defina a sequência S sobre $\mathbb{Z}_n$ de tamanho $(\kappa - 1)\ell + \ell - 1 = \kappa\ell - 1$ como

$$(m_2x_1, ..., m_2x_{\kappa-1}, y_1, m_2x_1, ..., m_2x_{\kappa-1}, y_2, m_2x_1, ..., m_2x_{\kappa-1}, ..., y_{\ell-1}, m_2x_1, ..., m_2x_{\kappa-1}).$$

Com o intuito de ficar mais claro o argumento, vamos renomear as entradas de S como $z_i, i \in \{1, ..., \kappa\ell - 1\}$. Suponha que S possua uma subsequência T de termos consecutivos de soma-zero com peso em A e que T possua pelo menos um elemento de S_2, ou seja, existem,$i, j \in \{1, ..., \kappa\ell - 1\}, i < j$, tais que

$$a_iz_i + \cdots + a_jz_j = 0, \tag{3.1}$$

com $a_i, ..., a_j \in A$ e pelo menos um z_i sendo um elemento de S_2. Dessa forma, aplicando o epimorfismo f_{n,m_2} na Equação (3.1), as parcelas que possuem termos de S_1 serão iguais a zero, visto que esses elementos são múltiplos de m_2, restando somente as imagens dos termos que possuem elementos da sequência S_2. Daí, temos uma subsequência S_3 de termos consecutivos de S_2 tal que a imagem de S_3 por f_{n,m_2} admite uma subsequência de termos consecutivos de soma-zero com peso em A_2, uma vez que $f_{n,m_2} \subset A_2$. Isso não é possível, pela escolha de S_2'. Então, T não possui termos de S_2, isto é, T é uma subsequência de S_1.

Seja T' uma sequência sobre $\mathbb{Z}_{m_1}$ tal que seus termos são obtidos dividindo os termos de T por m_2 e aplicando o epimorfismo f_{n,m_1}. Pela discussão do parágrafo acima, $T = (m_2x_i, ..., m_2x_j)$, $i, j \in \{1, ..., \kappa - 1\}$. Daí $T' = (f_{n,m_1}(x_i), ..., f_{n,m_1}(x_j))$, $i, j \in \{1, ..., \kappa - 1\}$. Como T é uma subsequência de S de termos consecutivos de soma-zero com peso em A, então existem $a_i', ..., a_j' \in A$, com $i, j \in \{1, ..., \kappa - 1\}$ tais que

$$a_i'(m_2x_i) + \cdots + a_j'(m_2x_j) = 0 \Leftrightarrow m_2(a_i'x_i + \cdots + a_j'x_j) = 0.$$

Como f_{n,m_1} é homomorfismo de anéis, temos

$$f_{n,m_1}(m_2)\left[f_{n,m_1}(a_i')f_{n,m_1}(x_i) + \cdots + f_{n,m_1}(a_j')f_{n,m_1}(x_j)\right] = 0.$$

Daí,

$$f_{n,m_1}(a_i')f_{n,m_1}(x_i) + \cdots + f_{n,m_1}(a_j')f_{n,m_1}(x_j) = 0.$$

Como $f_{n,m_1}(A) \subset A_1$, então T' é uma subsequência de S_1' de termos consecutivos de soma-zero com peso em A_1. Isso não pode ocorrer pela escolha de S_1'. Então S não admite subsequência de termos consecutivos de soma-zero com peso em A. Como o tamanho de S é $\kappa\ell - 1$, temos $C_A(n) \geqslant \kappa\ell$.

Agora, se $\kappa = \ell = 1$, temos a veracidade do resultado, pois $C_A(n) \geqslant 1$. Suponha que exatamente um deles seja igual a 1, digamos $\ell = 1$ e $k > 1$. Como a sequência S_1 definida anteriormente não admite subsequência de termos consecutivos de soma-zero com peso em A, pois S não admite, então $C_A(n) \geqslant \kappa$, o que prova este lema. □

A próxima proposição será utilizada algumas vezes daqui em diante, então será feita sua demonstração, com base no que foi feito no artigo [4]. Em particular, a fim de ficar mais claro a ideia, usaremos a notação $a + n\mathbb{Z}$ para denotar a classe de $a \in \mathbb{Z}$ em $\mathbb{Z}_n$.

Proposição 3.4.1. *Observe que dados $m, n \in \mathbb{N}$ tais que m divide n, então*

$$f_{n,m}(U(n)) = U(m).$$

Mais ainda, $f_{n,m}(U(n)^2) = U(m)^2$ e $f_{n,m}(U(n)^3) = U(m)^3$.

Demonstração. Dado $a + n\mathbb{Z} \in U(n)$, devemos mostrar que $\text{mdc}(a, m)$. De fato, se $\text{mdc}(a, m) \neq 1$, como m divide n, teríamos $\text{mdc}(a, n) \neq 1$. Logo, $\text{mdc}(a, m) = 1$, donde $f_{n,m}(a + n\mathbb{Z}) \in U(m)$. Daí, $f_{n,m}(U(n)) \subset U(m)$.

Por outro lado, dado $a + m\mathbb{Z} \in U(m)$, devemos mostrar que existe $b + n\mathbb{Z} \in \mathbb{Z}_n$ tal que $a + m\mathbb{Z} = f_{n,m}(b + n\mathbb{Z}) = b + m\mathbb{Z}$. Isso é equivalente a mostrar que para todo $a \in \mathbb{Z}$ tal que $\text{mdc}(a, m) = 1$, deve existir $a + mx$, com $x \in \mathbb{Z}$ tal que $\text{mdc}(a + mx, n) = 1$. Se todos os divisores primos de n também dividem m, então $\text{mdc}(a, m) = 1$ implica em $\text{mdc}(a, n) = 1$. Assim, basta tomar $b = a$. Agora, suponha que exista um primo p tal que $p \mid n$, mas $p \nmid m$. Se $a + mx \equiv 0 \pmod{p}$, para todo $x \in \mathbb{Z}$, em particular, $a + m(x+1) \equiv 0 \pmod{p}$. Porém, isso nos garante que $a + mx \equiv a + m(x + 1) \pmod{p}$, o que é uma contradição, pois p seria um divisor de m. Logo, existe $x \in \mathbb{Z}$ tal que $a + mx$ não é divisível por p. Replicando esta ideia para os outros possíveis primos que dividem n mas não m e fazendo as trocas de a por $a + mx$ e m por pm, respectivamente, encontramos o número inteiro que satisfaça o nosso objetivo. Logo, $U(m) \subset f_{n,m}(U(n))$.

Concluímos então que vale $U(m) = f_{n,m}(U(n))$. Por fim, também é verdade que $f_{n,m}(U(n)^2) = U(m)^2$ e $f_{n,m}(U(n)^3) = U(m)^3$. Para verificar as afirmações, basta usar o fato de $f_{n,m}$ ser um homomorfismo de grupos. □

Corolário 3.4.1. *Para $n \in \mathbb{N}$ qualquer, temos $C_{U(n)}(n) \geqslant 2^{\Omega(n)}$.*

Demonstração. Para provar este corolário, usaremos indução sobre $\Omega(n)$.

1. Para $\Omega(n) = 1$, n é um número primo. Logo, $\mathbb{Z}_n \backslash \{0\} = U(n)$ e, pelo Teorema 3.1.2, $C_{U(n)}(n) = 2$. Assim, o resultado é válido para $\Omega(n) = 1$.

2. Suponha, por hipótese de indução, que $\Omega(n) > 1$ e que o resultado seja válido para todo $k \in \mathbb{N}$ tal que $\Omega(k) < \Omega(n)$, isto é, vale $C_{U(k)}(k) \geqslant 2^{\Omega(k)}$, toda vez que $\Omega(k) < \Omega(n)$. Como $\Omega(n) > 1$, existem pelo menos dois números primos na decomposição de n e não necessariamente distintos, então considere p um primo divisor de n. Pela discussão anterior, considerando $n' = \dfrac{n}{p}$, temos $\Omega(n') \geqslant 1$ e, além disso, $\Omega(n') = \Omega(n) - 1 < \Omega(n)$. Pela hipótese de indução, $C_{U(n')}(n') \geqslant 2^{\Omega(n')}$. Também é verdade que $C_{U(p)}(p) = 2$. Como $p \mid n$ e $n' \mid n$, pela Proposição 3.4.1, temos $f_{n,p}(U(n)) \subset U(p)$ e $f_{n,n'}(U(n)) \subset U(n')$. Pelo Lema 3.4.1,

$$C_{U(n)}(n) \geqslant C_{U(n')}(n')C_{U(p)}(p) \geqslant 2^{\Omega(n')}2 = 2^{\Omega(n)-1}2 = 2^{\Omega(n)}.$$

   Dessa forma, concluímos a indução.

Portanto, por indução sobre $\Omega(n)$, $C_{U(n)}(n) \geqslant 2^{\Omega(n)}$. □

Note que o resultado anterior é para $n \in \mathbb{N}$ qualquer e conseguimos encontrar uma cota inferior para a constante consecutiva de Davenport, ou seja, devemos procurar sequências de tamanho entre $2^{\Omega(n)}$ e n. Essa limitação reduz bastante as contas. Agora, se fizermos certa restrição sobre n, conseguimos dizer exatamente qual é o valor da constante. Veja o próximo resultado:

Corolário 3.4.2. *Seja $n = 2^k$ para algum $k \in \mathbb{N}$. Então $C_{U(n)}(n) = C_{\{\pm 1\}}(n) = n$.*

Demonstração. Como $\{1\} \subset \{\pm 1\} \subset U(n)$, temos $C_{U(n)}(n) \leqslant C_{\{\pm 1\}}(n) \leqslant C(n)$. Por $\mathbb{Z}_n$ ser um grupo cíclico, temos $C(n) = n$, pelo Corolário 3.1.2. Por outro lado, como $n = 2^k$, então $\Omega(n) = k$, o que fornece $2^k \leqslant C_{U(n)}(n)$, pelo Corolário 3.4.1. Dessa forma,

$$n = 2^k \leqslant C_{U(n)}(n) \leqslant C_{\{\pm 1\}}(n) \leqslant C(n) = n,$$

ou seja, $C_{U(n)}(n) = C_{\{\pm 1\}}(n) = n$. □

Os dois próximos lemas garantirão que $C_{\{\pm 1\}}(n) \neq D_{\{\pm 1\}}(n)$. Para simplificar a notação, usaremos $\log_2 n = \log n$.

Lema 3.4.2. *Para $n \in \mathbb{N}$ qualquer, temos $D_{\{\pm 1\}}(n) \geqslant \lfloor \log n \rfloor + 1$.*

Demonstração. De fato, dado $n \in \mathbb{N}$, escolha $r \in \mathbb{N}$ de tal forma que $2^{(r+1)} \leqslant n < 2^{(r+2)}$ e considere a sequência $S = (1, 2, 2^2, ..., 2^r)$ sobre $\mathbb{Z}_n$. Note que, pela fórmula das séries geométricas, temos

$$1 + 2 + \cdots + 2^r = 2^{r+1} - 1 < n$$

e, consequentemente,

$$-1-2-\cdots-2^r = -2^{r+1}+1 > -n.$$

Dessa maneira, a soma dos elementos de S com qualquer combinação de sinais forma uma série com valor absoluto menor que n. Esta soma também não pode ser igual a zero, pois se $j_i \in \{0,1,2,...,r\}$ e $\alpha_i \in \{0,1\}$, em que $i = 1,2,...,k$ e $k \leqslant n$ de modo que $j_1 < j_2 < ... < j_k$ e

$$(-1)^{\alpha_1}2^{j_1} + (-1)^{\alpha_2}2^{j_2} + \cdots + (-1)^{\alpha_k}2^{j_k} = 0,$$

então

$$1 + (-1)^{\alpha_2-\alpha_1}2^{j_2-j_1} + \cdots + (-1)^{\alpha_k-\alpha_1}2^{j_k-j_1} = 0,$$

o que é um absurdo, já que do lado esquerdo temos um número ímpar e do lado direito um número par. Assim, a sequência S não possui subsequência tal que a soma de seus termos, ponderada em $A = \{-1,1\}$, seja um múltiplo de n. Mais ainda, S possui um total de $r+1 = \lfloor \log n \rfloor$ elementos. Portanto, $D_{\{\pm 1\}}(n) \geqslant \lfloor \log n \rfloor + 1$. □

Lema 3.4.3. *Sejam $n \in \mathbb{N}$ e $S = (x_1,...,x_k)$ uma sequência sobre $\mathbb{Z}_n$, com $k > \log n$. Então, existe um subconjunto J de $\{1,...,k\}$ e $a_j \in \{-1,1\}$, para cada $j \in J$, tais que*

$$\sum_{j\in J} a_j x_j = 0.$$

Com isso, temos $D_{\{\pm 1\}}(n) \leqslant \lfloor \log n \rfloor + 1$.

Demonstração. Considere todas as sequências da forma

$$\left(\sum_{j\in I} x_j\right),$$

em que I é um subconjunto de $\{1,...,k\}$. Como $\{1,...,k\}$ possui k elementos, segue que existem 2^k subconjuntos deste conjunto. Pela hipótese, $k > \log n$, donde $2^k > n$. Como o número de somas ultrapassa a ordem de $\mathbb{Z}_n$, existem $J_1, J_2 \subset \{1,...,k\}$ não vazios tais que $J_1 \neq J_2$ e

$$\sum_{j\in J_1} x_j = \sum_{j\in J_2} x_j.$$

Logo,

$$\sum_{j\in J_1} x_j - \sum_{j\in J_2} x_j = 0 \Rightarrow \sum_{j\in J_1} x_j + \sum_{j\in J_2} -x_j = 0.$$

Se escolhermos $J = (J_1 \cup J_2)\backslash(J_1 \cap J_2)$, é verdade que $J \neq \emptyset$ é um subconjunto de $\{1,...,k\}$. Além disso, considerando $a_j = 1$, caso $j \in J_1$, e $a_j = -1$, caso $j \in J_2$, temos

$$\sum_{j\in J} a_j x_j = 0.$$

Com isso, concluímos que toda sequência sobre $\mathbb{Z}_n$ com comprimento maior que $\log n$ possui uma subsequência de soma-zero com peso em $A = \{-1, 1\}$. Portanto,

$$D_{\{\pm 1\}}(n) \leqslant \lfloor \log n \rfloor + 1.$$

□

Teorema 3.4.1. *Seja $n \in \mathbb{N}$. Então $D_{\{\pm 1\}}(n) = \lfloor \log n \rfloor + 1$.*

Demonstração. De fato, o Lema 3.4.2 e o Lema 3.4.3 garantem este resultado. □

O teorema anterior e o Corolário 3.4.2 verificam, novamente, que podemos obter uma divergência entre as constantes C_A e D_A, o que nos motiva a estudar sobre a constante consecutiva de Davenport.

Definição 3.4.1. *Seja p um número primo divisor de n. Usamos a notação $v_p(n) = r$ para significar que p^r divide n, mas p^{r+1} não, isto é, a valoração p-ádica de n.*

Seja S uma sequência sobre $\mathbb{Z}_n$. Suponha que p seja um número primo divisor de n, com $v_p(n) = r$. A sequência $S^{(p)}$ sobre $\mathbb{Z}_{p^r}$ é definida como a imagem de S pelo homomorfismo canônico f_{n,p^r}.

Proposição 3.4.2. *A sequência S sobre $\mathbb{Z}_n$ é uma sequência de soma-zero com peso em $U(n)$ se, e somente se, para todo primo p divisor de n, $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_{p^{v_p(n)}}$ de soma-zero com peso em $U(p^{v_p(n)})$.*

Demonstração. Seja $S = (x_1, ..., x_k)$ uma sequência de soma-zero com peso em $U(n)$, isto é, existem $a_1, ..., a_k \in U(n)$ tais que

$$a_1x_1 + \cdots + a_kx_k = 0. \tag{3.2}$$

Considere p um número primo divisor de n. Daí, $S^{(p)} = (f_{n,p^r}(x_1), ..., f_{n,p^r}(x_k))$ é uma sequência sobre $\mathbb{Z}_{p^r}$. Como p^r divide n, já vimos que $f_{n,p^r}(U(n)) \subset U(p^r)$. Pela Equação (3.2), existem $a'_1 = f_{n,p^r}(a_1), ..., a'_k = f_{n,p^r}(a_k) \in U(p^r)$ tais que

$$a'_1 f_{n,p^r}(x_1) + \cdots + a'_k f_{n,p^r}(x_k) = 0,$$

ou seja, $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_{p^r}$ de soma-zero com peso em $U(p^r)$.

Reciprocamente, suponha que $n = p_1^{r_1}p_2^{r_2}...p_l^{r_l}$ seja a decomposição de n em fatores primos. Para cada primo p_i, $i \in \{1, ..., l\}$, divisor de n, considere $v_{p_i}(n) = r_i$. Além disso, temos $S^{(p_i)} = (y_{1_{p_i}}, ..., y_{k_{p_i}})$ sendo uma sequência sobre $\mathbb{Z}_{p^{r_i}}$ de soma-zero com peso sobre $U(p_i^{r_i})$, para todo $i \in \{1, .., l\}$, ou seja, existem $a_{1_{p_i}}, ..., a_{k_{p_i}} \in U(p_i^{r_i})$ tais que

$$a_{1_{p_i}}x_1 + \cdots + a_{k_{p_i}}x_k = 0 \pmod{p_i^{r_i}}, \tag{3.3}$$

para todo $i \in \{1, .., l\}$. Pelo Teorema Chinês do Resto (Cap. 5, Seção 5.8, p. 117–118 de [2]), existe um isomorfismo entre $U(n)$ e $U(p_1^{r_1}) \times \cdots \times U(p_l^{r_l})$, isto é, conseguimos identificar $a_j = (a_{j_{p_1}}, ..., a_{j_{p_l}})$, $j \in \{1, ..., k\}$, com $a_j \in U(n)$. Dessa forma, pelas l equações formadas por (3.3), $a_1x_1 + \cdots + a_kx_k = (0, ..., 0) = 0 \pmod{n}$, uma vez que temos um isomorfismo entre $\mathbb{Z}_n$ e $\mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_l^{r_l}}$. □

Para um primo p divisor de n, seja $A_p^j = \{x^j : x \in U(p^r)\}$. Podemos generalizar a Proposição 3.4.2 e obter o seguinte resultado:

Observação 3.4.1. *A sequência S sobre $\mathbb{Z}_n$ é uma sequência de soma-zero sobre $U(n)^j$ se, e somente se, para todo primo p divisor de n, $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_{p^{v_p(n)}}$ de soma-zero com peso em A_p^j.*

Lema 3.4.4. *Sejam m um divisor de n e $b \in U(m)$. Então, existe $a \in U(n)$ tal que $f_{n,m}(a) = b$. Além disso, se $b \in U(m)^2$, existe $a \in U(n)^2$ tal que $f_{n,m}(a) = b$.*

Demonstração. Seja $\mathbb{Z}^+ = \{i \in \mathbb{Z} : i > 0\}$. Como b é coprimo com m, pelo Teorema de Dirichlet (Cap. 9, p. 146–156 de [2]), existem infinitos números primos na progressão aritmética $\{b + im : i \in \mathbb{Z}^+\}$. Como apenas um número finitos desses primos vão dividir n, existe $i \in \mathbb{Z}^+$ tal que $a = b + im \in U(n)$. Logo, $f_{n,m}(a) = f_{n,m}(b + im) = b$, como queríamos.

Por fim, dado $b \in U(m)^2$, existe $c \in U(m)$ tal que $b = c^2$. Pela primeira parte deste lema, existe $c' \in U(n)$ tal que $f_{n,m}(c') = c$. Assim, existe $a = (c')^2$ tal que

$$f_{n,m}(a) = f_{n,m}((c')^2) = (f_{n,m}(c'))^2 = c^2 = b.$$

□

Corolário 3.4.3. *Seja p um número primo divisor de n e $n' = \dfrac{n}{p}$. Se $c' \in U(n')$, existe $c \in U(n)$ tal que $f_{n,n'}(c) = c'$.*

Demonstração. Se p é um número primo que divide n, então $n' = \dfrac{n}{p}$ divide n. Assim, se $c' \in U(n')$, pelo lema anterior, existe $c \in U(n)$ tal que $f_{n,n'}(c) = c'$. □

Lema 3.4.5. *Seja S uma sequência sobre $\mathbb{Z}_n$ e p um primo divisor de n que divide todos os elementos de S. Suponha $n' = \dfrac{n}{p}$ e S' uma sequência sobre $\mathbb{Z}_{n'}$ obtida dividindo os termos de S por p. Se S' é uma sequência de soma-zero com peso em $U(n')$, então S é uma sequência de soma-zero com peso em $U(n)$. Mais ainda, se S' é uma sequência de soma-zero com peso em $U(n')^2$, então S é uma sequência de soma-zero com peso em $U(n)^2$.*

Demonstração. Seja $S = (x_1, ..., x_k)$ uma sequência sobre $\mathbb{Z}_n$. Então $S' = (x'_1, ..., x'_k)$, em que $x'_i = f_{n,n'}\left(\frac{x_i}{p}\right)$, para cada $i \in \{1, ..., k\}$. Como S' é uma sequência de soma-zero com peso em $U(n')$, para cada $i \in \{1, .., k\}$, existe a'_i tais que $a'_1x'_1 + \cdots + a'_kx'_k = 0$. Pelo corolário anterior, para cada $i \in \{1, ..., k\}$, existe $a_i \in U(n)$ tais que $f_{n,n'}(a_i) = a'_i$. Como $a'_1x'_1 + \cdots + a'_kx'_k = 0$, temos

$$f_{n,n'}\left(\frac{a_1x_1 + \cdots + a_kx_k}{p}\right) = 0,$$

ou seja, n' divide $\frac{a_1x_1 + \cdots + a_kx_k}{p}$. Dessa forma, n divide $a_1x_1 + \cdots + a_kx_k$, o que sigifica que $a_1x_1 + \cdots + a_kx_k = 0$ sobre $\mathbb{Z}_n$. Logo, S é uma sequência de soma-zero em $U(n)$.

Para a segunda parte, veremos que para cada $a'_i \in U(n')^2$, $i \in \{1, ..., k\}$, existe $a'_i \in U(n)^2$ tal que $f_{n,n'}(a_i) = a'_i$. De fato, seja $a'_i \in U(n')^2$ qualquer. Daí, $a'_i = y^2$, com $y \in U(n')$. Novamente pelo lema anterior, existe $x \in U(n)$ tal que $f_{n,n'}(x) = y$. Como $f_{n,n'}$ é um homomorfismo, basta tomar $a_i = x^2 \in U(n)^2$ para obter $f_{n,n'}(a_i) = a'_i$. Com isso, a demonstração da segunda parte do resultado segue de forma similar a primeira parte. □

Observação 3.4.2. *Usando uma ideia similar a utilizada na segunda parte da demonstração do lema acima, podemos concluir que se S' é uma sequência de soma-zero com peso em $U(n')^3$, então S é uma sequência de soma-zero com peso em $U(n)^3$.*

O próximo lema será demonstrado seguindo a ideia da demonstração feita no artigo [8].

Lema 3.4.6. *Seja p^r, com p um número primo ímpar.*

1. *Se $x, y \in \mathbb{Z}_{p^r}$ são coprimos com p, então dado $t \in \mathbb{Z}_{p^r}$, existem unidades α, β em $\mathbb{Z}_{p^r}$ tais que $\alpha x + \beta y = t$.*

2. *Se uma sequência S sobre $\mathbb{Z}_{p^r}$ possui pelo menos dois termos coprimos com p, então S é uma sequência de soma-zero com peso em $U(p^r)$.*

Demonstração. Seja p^r, em que p é um número primo ímpar.

1. Note que $t + y \not\equiv t - y \pmod{p}$. Caso contrário, p dividiria y, já que p é um número primo ímpar. Dessa forma, podemos escolher $\beta \in \{-1, 1\}$ tal que $t - \beta y \not\equiv 0 \pmod{p}$, ou seja, $t - \beta y$ é uma unidade em $\mathbb{Z}_{p^r}$. Como x é uma unidade em $\mathbb{Z}_{p^r}$, x^{-1} também o é, donde $\alpha = x^{-1}(t - \beta y)$ é uma unidade em $\mathbb{Z}_{p^r}$. Daí, existem α, β unidades em $\mathbb{Z}_n$ tais que $\alpha x + \beta y = t$.

2. Suponha $S = (x_1, ..., x_k)$ uma sequência sobre $\mathbb{Z}_{p^r}$ tal que pelo menos dois termos de S sejam unidades em $\mathbb{Z}_{p^r}$, digamos x_1 e x_2. Pelo item anterior, existem $a_1, a_2 \in U(p^r)$ tais que $a_1x_1 + a_2x_2 = -x_3 - \cdots - x_k$. Basta escolher $a_i = 1$, com $i = 3, ..., k$, para obter $a_1x_1 + \cdots + a_kx_k = 0$. Logo, S é uma sequência de soma-zero com peso em $U(p^r)$.

□

Teorema 3.4.2. *Quando n é um número ímpar, temos $C_{U(n)}(n) \leqslant 2^{\Omega(n)}$.*

Demonstração. Considere a sequência $S = (x_1, ..., x_k)$ de forma arbitrária sobre $\mathbb{Z}_n$ com tamanho $k = 2^{\Omega(n)}$. O nosso objetivo é provar que S admite subsequência de soma-zero com peso em $U(n)$. Vamos separar a demonstração em dois casos.

1. Caso: Para um primo p divisor de n, pelo menos dois termos de S são coprimos com p.

   Seja p um número primo divisor de n e $r = v_p(n)$. Seja $S^{(p)}$ definida antes da Proposição 3.4.2. Como n é um número ímpar e p divide n, então p é um número primo ímpar. Pelo lema anterior, $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_{p^r}$ de soma-zero com peso em $U(p^r)$. Como isso é válido para qualquer primo p divisor de n, S é uma sequência de soma-zero com peso em $U(n)$, pela Proposição 3.4.2. Logo, $C_{U(n)}(n) \leqslant 2^{\Omega(n)}$.

2. Caso: Existe um número primo p divisor de n tal que no máximo um termo de S é coprimo com p.

   Este caso vamos demonstrar por indução sobre $\Omega(n)$. Se $\Omega(n) = 1$, então n é um número primo. Dessa forma, $U(n) = \mathbb{Z}_n \backslash \{0\}$. Pelo Teorema 3.1.2, $C_{U(n)}(n) = 2 \leqslant 2^{\Omega(n)}$. Suponha que $\Omega(n) > 1$ e que o resultado seja válido para $\Omega(n) - 1$, por hipótese de indução. Podemos dividir a sequência S em duas partes iguais de tamanho $\frac{k}{2}$. O possível elemento de S que é coprimo com p não estará em uma dessas duas partes da sequência S, ou seja, uma dessas partes possui todos elementos divisíveis por p. Assim, existe uma subsequência T de S de tamanho $\frac{k}{2}$ tal que p divide todos os termos de T.
   Seja $n' = \frac{n}{p}$ e T' a sequência sobre $\mathbb{Z}_{n'}$ obtida dividindo os termos de T por p e aplicando $f_{n,n'}$ em cada termo. Como $n' = \frac{n}{p}$, segue que $\Omega(n') = \Omega(n) - 1$. Além disso, T' é uma sequência que possui tamanho $\frac{2^{\Omega(n)}}{2} = 2^{\Omega(n)-1} = 2^{\Omega(n')}$. Pela hipótese de indução, T' possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n')$. Pelo Lema 3.4.5, T possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n)$. Como T é uma subsequência de S de termos

consecutivos, então S possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n)$. Dessa forma, este caso é válido por indução sobre $\Omega(n)$.

Portanto, este teorema está devidamente provado. □

Corolário 3.4.4. *Quando n é um número ímpar, temos $C_{U(n)}(n) = 2^{\Omega(n)}$.*

Demonstração. O resultado segue diretamente da aplicação do teorema anterior e do Corolário 3.4.1. □

3.5 Caso $A = U(n)^2$

Nesta seção, vamos generalizar os resultados obtidos na Seção 3.2.

Corolário 3.5.1. *Se $n = 2^r m$, com m um número ímpar, então $C_{U(n)^2}(n) \geqslant 2^r 3^{\Omega(m)}$.*

Demonstração. A demonstração é feita usando indução sobre $\Omega(n)$. Suponha $\Omega(n) = 1$, ou seja, n é um número primo. Se n é par, então $r = 1$ e

$$C_{U(n)^2}(n) = 2 = 2^r 3^{\Omega(m)}$$

em que a primeira igualdade ocorre pelo Teorema 3.2.1. Se n é ímpar, então $r = 0$ e $n = m$. Novamente pelo Teorema 3.2.1, temos

$$C_{U(n)^2}(n) = 3 = 2^r 3^{\Omega(m)}.$$

Considere $n' = \dfrac{n}{p}$, em que p é um divisor primo de n. Suponha que $\Omega(n) > 1$ e que o resultado seja válido para $\Omega(n) - 1$. Vamos separar a demonstração em dois casos.

1. Se esse primo é $p = 2$: Neste caso, como 2 e $2^r m$ dividem n, $f_{n,2}(U(n)^2) \subset U(2)^2$ e $f_{n,2^r m}(U(n)^2) \subset U(2^r m)^2$. Pelo Lema 3.4.1, pelo Teorema 3.2.1 e por hipótese de indução, temos

$$C_{U(n)^2}(n) \geqslant C_{U(2)^2}(2) C_{U(2^{r-1}m)^2}(2^{r-1}m) = 2(2^{r-1}3^{\Omega(m)}) = 2^r 3^{\Omega(m)}.$$

2. Se esse primo p divide m: Considere $t = \dfrac{m}{p}$. Como p e $2^r t$ dividem n, $f_{n,p}(U(n)^2) \subset U(p)^2$ e $f_{n,2^r t}(U(n)^2) \subset U(2^r t)^2$. Como p divide m, que é um número ímpar, então p é um número primo ímpar. Pelo Teorema 3.2.1, temos $C_{U(p)^2}(U(p)) = 3$. Por hipótese de indução e pelo Lema 3.4.1, temos

$$C_{U(n)^2}(n) \geqslant C_{U(p)^2}(p) C_{U(2^r t)^2}(2^r t) = 3(2^r 3^{\Omega(m)-1}) = 2^r 3^{\Omega(m)}.$$

Portanto, o resultado está devidamente demonstrado. □

Lema 3.5.1. *Sejam $p \geqslant 7$, $r \in \mathbb{N}$ e $n = p^\alpha$. Então, dados $x_1, x_2, x_3 \in U(n)$, temos*

$$U(n)^2x_1 + U(n)^2x_2 + U(n)^2x_3 = \mathbb{Z}_n.$$

Demonstração. Seja $H = \text{Stab}(U(n)^2x_1+U(n)^2x_2+U(n)^2x_3)$. Como $\mathbb{Z}_n$ é cíclico, então $\dfrac{\mathbb{Z}_n}{H}$ também o é, digamos $\mathbb{Z}_m$, em que $m = p^\beta$, $\beta \leqslant \alpha$. Considere $\phi : \mathbb{Z}_n \to \mathbb{Z}_m$ o homomorfismo canônico. Como m divide n, pela Proposição 3.4.1, segue que $\phi(U(n)^2) = U(m)^2$. Dessa forma,

$$\sum_{i=1}^{3} U(m)^2\phi(x_i) = \phi\left(\sum_{i=1}^{3} U(n)x_i\right).$$

Outra implicação da Proposição 3.4.1 é que $\phi(U(n)) = U(m)$, logo para cada x_i, $i = 1, 2, 3$, $\phi(x_i)$ gera $\mathbb{Z}_m$. Pela Proposição 2.4.1, segue que

$$\text{Stab}\left(\sum_{i=1}^{3} U(m)^2\phi(x_i)\right) = \{\phi(0)\},$$

visto que $H = \text{Stab}\,(U(n)^2x_1 + U(n)^2x_2 + U(n)^2x_3)$. Aplicando o Corolário 2.4.2, como

$$\left|\sum_{i=1}^{3} U(m)^2\phi(x_i)\right| \geqslant 3|U(m)^2| - 2 = 3\left(\frac{p^\beta - p^{\beta-1}}{2}\right) - 2 \geqslant p^\beta,$$

então $\displaystyle\sum_{i=1}^{3} U(m)^2\phi(x_i) = \mathbb{Z}_m$. Assim, concluímos, pela Proposição 2.4.1, que

$$\text{Stab}\left(\sum_{i=1}^{3} U(m)^2\phi(x_i)\right) = \mathbb{Z}_m.$$

Dessa forma, $\mathbb{Z}_m = \{0\}$, ou seja, $H = \mathbb{Z}_n$. Portanto, novamente pela Proposição 2.4.1 temos $\text{Stab}\,(U(n)^2x_1 + U(n)^2x_2 + U(n)^2x_3) = \mathbb{Z}_n$ e, consequentemente,

$$U(n)^2x_1 + U(n)^2x_2 + U(n)^2x_3 = \mathbb{Z}_n.$$

□

Lema 3.5.2. *Seja $n = p^r$, em que $p \geqslant 7$ é um número primo. Suponha que S seja uma sequência sobre $\mathbb{Z}_n$ tal que pelo menos três elementos de S são unidades. Então S é uma sequência de soma-zero com peso em $U(n)^2$.*

Demonstração. Seja $S = (x_1, ..., x_k)$ uma sequência sobre $\mathbb{Z}_n$ tal que pelo menos três de seus termos sejam unidades, digamos x_1, x_2 e x_3. Pelo lema anterior,

$$U(n)^2x_1 + U(n)^2x_2 + U(n)^2x_3 = \mathbb{Z}_n.$$

Logo, existem $a_1, a_2, a_3 \in U(n)^2$ tais que

$$a_1x_1 + a_2x_2 + a_3x_3 = -x_4 - \cdots - x_k,$$

ou seja, tomando $a_i = 1 \in U(n)^2$, $i \in \{4, ..., k\}$, segue que

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + \cdots + a_kx_k = 0.$$

Logo, S é uma sequência de soma-zero com peso em $U(n)^2$. □

Observação 3.5.1. *O lema anterior falha quando $p < 7$. Quando $n = 2$ ou $n = 5$, a sequência $(1, 1, 1)$ sobre $\mathbb{Z}_n$ não é uma sequência de soma-zero com peso em $U(n)^2$, pois $U(2)^2 = \{1\}$ e $U(5)^2 = \{\pm 1\}$. Para $n = 3$, a sequência $(1, 2, 1)$ sobre $\mathbb{Z}_3$ não é uma sequência de soma-zero com peso em $U(3)^2$.*

Teorema 3.5.1. *Se todo primo divisor de n é pelo menos 7, então $C_{U(n)^2}(n) \leqslant 3^{\Omega(n)}$.*

Demonstração. Seja $S = (x_1, ..., x_k)$ uma sequência sobre $\mathbb{Z}_n$ com tamanho $k = 3^{\Omega(n)}$. Queremos mostrar que S possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n)^2$. Vamos separar a demonstração em dois casos.

1. Caso: Para qualquer primo p divisor de n, pelo menos três termos de S é coprimo com p.

   Seja p um número primo divisor de n e $v_p(n) = r$. Então, $S^{(p)}$ possui pelo menos três unidades, em que $S^{(p)}$ é a sequência definida antes da Proposição 3.4.2. Como p é pelo menos 7, pelo lema anterior, $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_{p^r}$ de soma-zero com peso em $U(p^r)^2$. Como isso é válido para todo primo divisor de n, pela Observação 3.4.1, segue que S é uma sequência de soma-zero com peso em $U(n)^2$. Dessa forma, o resultado é válido.

2. Caso: Existe um número primo p divisor de n tal que no máximo dois termos de S são coprimos com p.

   Neste caso, vamos usar indução sobre $\Omega(n)$. Se $\Omega(n) = 1$, então n é um número primo. Como todo primo divisor de n é pelo menos 7, então $C_{U(n)^2}(n) = C_{Q_n}(n) = 3$, pelo Teorema 3.2.1. Suponha $\Omega(n) > 1$ e, por hipótese de indução, que o resultado seja válido para $\Omega(n) - 1$.

   Podemos dividir a sequência S em três partes iguais de tamanho $\frac{k}{3}$. Pelo menos uma dessas partes possuem todos os termos divisíveis por p, ou seja, S admite uma subsequência T de termos consecutivos em que todos os seus termos são divisíveis por p. Sejam $n' = \frac{n}{p}$ e T' a sequência formada pela imagem da sequência obtida dividindo todos os termos de T por p, pelo epimorfismo $f_{n,n'}$. Como p divide n, temos $\Omega(n') = \Omega(n) - 1$. Além disso, a sequência T' tem tamanho $\frac{k}{3} = 3^{\Omega(n')}$, donde T' possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n')^2$, por hipótese de indução. Pelo Lema 3.4.5, T admite uma subsequência de termos consecutivos de soma-zero com peso em $U(n)^2$. Como T é uma subsequência de S,

segue que S possui uma subsequência de soma-zero com peso em $U(n)^2$, o que torna verídico o resultado.

Portanto, o resultado é válido. □

Corolário 3.5.2. *Se todo primo p divisor de n é pelo menos 7, então $C_{U(n)^2}(n) = 3^{\Omega(n)}$.*

Demonstração. Pelo teorema anterior, $C_{U(n)^2}(n) \leqslant 3^{\Omega(n)}$. Agora, como n não é divisível por 2, $r = 0$ no Corolário 3.5.1. Daí, $C_{U(n)^2}(n) \geqslant 3^{\Omega(n)}$. Portanto, $C_{U(n)^2}(n) = 3^{\Omega(n)}$. □

3.6 Caso $A = U(n)^3$

Nesta seção, iremos generalizar os resultados da Seção 3.3.

Seja $n = p_1^{r_1}p_2^{r_2}...p_s^{r_s}$, em que cada $p_i's$, $i \in \{1, ..., s\}$, é um número primo distinto. Suponha que 7 não divida n. Considere o conjunto $I = \{i : p_i \equiv 1 \pmod 3\}$. Sejam $n_1 = \prod_{i \in I} p_i^{r_i}$ e $n_2 = \dfrac{n}{n_1}$. Vamos utilizar a notação $n = n_1n_2$ por toda esta seção.

Corolário 3.6.1. *Seja $m = 7^r n$, em que 7 não divide n e $n = n_1n_2$. Então $C_{U(m)^3}(m) \geqslant 2^{\Omega(n_2)}3^{\Omega(n_1)}4^r$.*

Demonstração. Vamos provar este resultado por indução sobre $\Omega(n)$.

1. Se $\Omega(n) = 1$, então n é um número primo diferente de 7, pois 7 não divide n. Como 7^r e n dividem m, temos $f_{m,7^r}(U(m)^3) \subset U(7^r)^3$ e $f_{m,n}(U(m)^3) \subset U(n)^3$. Pelo Lema 3.4.1, $C_{U(m)^3}(m) \geqslant C_{U(7^r)^3}(7^r)C_{U(n)^3}(n)$. Aplicando recursivamente o Lema 3.4.1 para $C_{U(7^r)^3}(7^r)$, obtemos $C_{U(7^r)^3}(7^r) \geqslant 4^r$, pois pelo Lema 3.3.2, temos $C_{U(7)^3}(7) = 4$. Agora falta estudar $C_{U(n)^3}(n)$. Se $n \equiv 1 \pmod 3$, temos $n = n_1$, $n_2 = 1$ e $C_{U(n)^3}(n) = 3$, pelo Teorema 3.3.1, uma vez que $n \neq 7$. Daí,

$$C_{U(m)^3}(m) \geqslant 4^r 3 \geqslant 2^0 3^1 4^r = 2^{\Omega(n_2)}3^{\Omega(n_1)}4^r.$$

   Se $n \not\equiv 1 \pmod 3$, temos $n = n_2$ e $n_1 = 1$. Além disso, já sabemos que $U(n)^3 = U(n) = \mathbb{Z}_n\backslash\{0\}$, donde $C_{U(n)^3}(n) = 2$, pelo Teorema 3.1.2. Então,

$$C_{U(m)^3}(m) \geqslant 4^r 2 \geqslant 2^1 3^0 4^r = 2^{\Omega(n_2)}3^{\Omega(n_1)}4^r,$$

   ou seja, o resultado é verdadeiro para $\Omega(n) = 1$.

2. Suponha que o resultado seja válido para $\Omega(n) = k - 1$, isto é, se n tem $k - 1$ primos em sua decomposição, então $C_{U(n)^3}(n) \geqslant 2^{\Omega(n_2)}3^{\Omega(n_1)}4^r$. Agora, suponha $\Omega(n) = k$, ou seja, n possui um primo p a mais em sua decomposição. Como p

divide n, considere $t = \dfrac{n}{p}$. Como p e $7^r t$ dividem m, temos $f_{m,p}(U(m)^3) \subset U(p)^3$ e $f_{m,7^r t}(U(m)^3) \subset U(7^r t)^3$. Pelo Lema 3.4.1,temos

$$C_{U(m)^3}(m) \geqslant C_{U(p)^3}(p) C_{U(7^r t)^3}(7^r t). \tag{3.4}$$

a) Caso $p \equiv 1 \pmod 3$: Neste caso, retiramos um número primo de n_1, logo $C_{U(7^r t)^3}(7^r t) \geqslant 2^{\Omega(n_2)} 3^{\Omega(n_1)-1} 4^r$, por hipótese de indução. Como $p \neq 7$, temos $C_{U(p)^3}(p) = 3$, pelo Teorema 3.3.1. Pela Desigualdade (3.4), concluímos

$$C_{U(m)^3}(m) \geqslant 3\left(2^{\Omega(n_2)} 3^{\Omega(n_1)-1} 4^r\right) = 2^{\Omega(n_2)} 3^{\Omega(n_1)} 4^r.$$

b) Caso $p \not\equiv 1 \pmod 3$: Neste caso, retiramos um número primo de n_2, logo $C_{U(7^r t)^3}(7^r t) \geqslant 2^{\Omega(n_2)-1} 3^{\Omega(n_1)} 4^r$, por hipótese de indução. Como $p \not\equiv 1 \pmod 3$, já vimos que $U(p)^3 = U(p) = \mathbb{Z}_p \backslash \{0\}$, donde $C_{U(p)^3}(p) = 2$, pelo Teorema 3.1.2. Novamente pela Desigualdade (3.4), temos

$$C_{U(m)^3}(m) \geqslant 2\left(2^{\Omega(n_2)-1} 3^{\Omega(n_1)} 4^r\right) = 2^{\Omega(n_2)} 3^{\Omega(n_1)} 4^r.$$

Logo, o resultado é válido quando $\Omega(n) = k$.

Portanto, o resultado é válido por indução sobre $\Omega(n)$. □

Teorema 3.6.1. *Seja n livre de quadrados e não divisível por $2, 7$ e 13. Então $C_{U(n)^3}(n) \leqslant 2^{\Omega(n_2)} 3^{\Omega(n_1)}$.*

Demonstração. Seja S uma sequência sobre $\mathbb{Z}_n$ de tamanho $k = 2^{\Omega(n_2)} 3^{\Omega(n_1)}$. Queremos mostrar que S possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n)^3$. Vamos separar em casos.

1. Caso: Dado um primo p divisor de n_1, pelo menos três termos de S são coprimos com p, e dado primo p divisor de n_2, pelo menos dois termos de S são coprimos com p.

   Sejam p um número primo divisor de n e $S^{(p)}$ a sequência definida como antes da Proposição 3.4.2. Se p divide n_1, então $p \equiv 1 (\mathrm{mod}\, 3)$ e $S^{(p)}$ possui pelo menos três unidades, uma vez que pelo menos três termos de S são coprimos com p. Assim, segue do Lema 3.3.1 que $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_p$ de soma-zero com peso em $U(p)^3$, pois $p \neq 7, 13$. Se p divide n_2, então $p \not\equiv 1 \pmod 3$ e $S^{(p)}$ possui pelo menos duas unidades, pois pelo menos dois termos de S são coprimos com p. Como $p \neq 2$, $S^{(p)}$ é uma sequência de soma-zero com peso $U(p)$, pelo Lema 3.4.6. Vimos que no caso em que $p \not\equiv 1 \pmod 3$, temos $U(p) = U(p)^3$. Então, para todo primo p divisor de n, $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_p$ de soma-zero com peso em $U(p)^3$ e, pela Observação 3.4.1, S é uma sequência de soma-zero com peso em $U(n)^3$.

2. Os outros dois casos serão feitos por indução sobre $\Omega(n)$.

   Suponha $\Omega(n) = 1$, ou seja, n é um número primo. Sendo assim, $U(n) = \mathbb{Z}_n \backslash \{0\}$

   a) Se $n \equiv 1 \pmod 3$: Neste caso, $n = n_1$. Como $n \neq 2, 7, 13$, tem-se $|U(n)| \geqslant 3$. Além disso, $\Omega(n_1) = 1$ e $\Omega(n_2) = 0$, donde S tem tamanho 3. Assim, S possui três termos que são unidades e, como $n \neq 7, 13$, temos que S é uma sequência de soma-zero com peso em $U(n)^3$, pelo Lema 3.3.1. Daí, $C_{U(n)^3}(n) \leqslant 3 = 2^{\Omega(n_2)}3^{\Omega(n_1)}$.

   b) Se $n \not\equiv 1 \pmod 3$: Neste caso, $n = n_2$. Além disso, $|U(n)| \geqslant 2$, o que significa que S é uma sequência de tamanho 2 em que seus termos são unidades. Logo, S é uma sequência de soma-zero com peso em $U(n)$, pelo Lema 3.4.6. Como já vimos, por $n \not\equiv 1 \pmod 3$, então $U(n) = U(n)^3$, o que significa que S é uma sequência de soma-zero com peso em $U(n)^3$. Assim, $C_{U(n)^3}(n) \leqslant 2 = 2^{\Omega(n_2)}3^{\Omega(n_1)}$.

   Logo, o caso $\Omega(n) = 1$ está verificado.

   Suponha $\Omega(n) > 1$ e , por hipótese de indução, que seja válido o resultado para $\Omega(n) - 1$.

   a) Caso: Existe um primo p divisor de n_1 tal que no máximo dois termos de S são coprimos com p.
   Seja $n' = \dfrac{n}{p}$. Se escrevermos n' como $n'_1 n'_2$ utilizando a notação introduzida no início desta seção, temos $n'_1 = \dfrac{n_1}{p}$ e $n'_2 = n_2$, uma vez que $p \equiv 1 \pmod 3$. Dividindo a sequência em três partes iguais de tamanho $\dfrac{k}{3}$, existe uma subsequência T de S de termos consecutivos de tamanho $\dfrac{k}{3}$ tal que p divide todos os termos de T. Dividindo os termos de T por p obtemos uma nova sequência cuja imagem por $f_{n,n'}$ é uma sequência sobre $\mathbb{Z}_{n'}$ que chamaremos de T'. Dessa forma, T' é uma sequência de tamanho $\dfrac{k}{3} = 2^{\Omega(n_2)}3^{\Omega(n_1)-1} = 2^{\Omega(n'_2)}3^{\Omega(n'_1)}$. Como n é livre de quadrados n' também o é. Além disso, n' não é divisível por $2, 7$ ou 13. Como $\Omega(n') = \Omega(n) - 1$, pela hipótese de indução, T' admite uma subsequência de termos consecutivos de soma-zero com peso em $U(n')^3$. Pela Observação 3.4.2, temos que T possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n)^3$. Como T é uma subsequência de S de termos consecutivos, isso significa que S admite uma subsequência de termos consecutivos de soma-zero com peso em $U(n)^3$.

   b) Caso: Existe um primo p divisor de n_2 tal que no máximo um dos termos de S é coprimo com p.
   Seja $n' = \dfrac{n}{p}$. Se escrevermos n' como $n'_1 n'_2$ utilizando a notação introduzida no início desta seção, temos $n'_1 = n_1$ e $n'_2 = \dfrac{n_2}{p}$, pois $p \not\equiv 1 \pmod 3$. Dividindo a

sequência em duas partes iguais de tamanho $\frac{k}{2}$, existe uma subsequência T de S de termos consecutivos de tamanho $\frac{k}{2}$ tal que p divide todos os termos de T. Dividindo os termos de T por p obtemos uma nova sequência cuja imagem por $f_{n,n'}$ é uma sequência sobre $\mathbb{Z}_{n'}$ que chamaremos de T'. Daí, T' é uma sequência de tamanho $\frac{k}{2} = 2^{\Omega(n_2)-1}3^{\Omega(n_1)} = 2^{\Omega(n_2')}3^{\Omega(n_1')}$. Por uma argumentação similar ao caso anterior, S admite uma subsequência de termos consecutivos de soma-zero com peso em $U(n)^3$.

Em todos os caso temos a veracidade do resultado.

Portanto, o teorema está devidamente demonstrado. □

Corolário 3.6.2. *Seja n livre de quadrados e não divisível por 2, 7 e 13. Então $C_{U(n)^3}(n) = 2^{\Omega(n_2)}3^{\Omega(n_1)}$.*

Demonstração. Como 7 não divide n, podemos usar $r = 0$ no Corolário 3.6.1. Usando isso e o teorema anterior, segue o resultado. □

Observação 3.6.1. *Pelo Corolário 3.6.1 podemos observar que as conclusões do teorema e corolário anteriores são falsas quando n é divisível por 7. Tome como contraexemplo $n = 7$. Pelo Lema 3.3.2, temos $C_{U(7)^3}(7) = 4 > 3$.*

Lema 3.6.1. *Seja $n = p^r$ em que $p \geqslant 13$ é um número primo tal que $p \equiv 1 \pmod 3$. Seja S uma sequência em $\mathbb{Z}_n$ tal que pelo menos quatro termos são unidades. Então, S é uma sequência de soma-zero com peso em $U(n)^3$.*

Demonstração. Seja $S = (x_1, ..., x_k)$ uma sequência sobre $\mathbb{Z}_n$ tal que pelo menos quatro de seus termos são unidades, digamos x_1, x_2, x_3, x_4. Como $p \equiv 1 \pmod 3$, temos $|U(n)^3| = \frac{p^r - p^{r-1}}{3}$. Considere $H = \text{Stab}\left(x_1U(n)^3 + x_2U(n)^3 + x_3U(n)^3 + x_4U(n)^3\right)$. Como $\mathbb{Z}_n$ é cíclico, segue que $\frac{\mathbb{Z}_n}{H}$ também o é, digamos $\mathbb{Z}_m$, com $m = p^l$, $l \leqslant r$. Agora, considere $\psi : \mathbb{Z}_n \to \mathbb{Z}_m$ o homomorfismo canônico, em que $\ker(\psi) = H$. Pela Observação 3.4.1, segue que $\psi\left(U(n)^3\right) = U(m)^3$ e pela Observação 2.4.1 temos

$$\{\psi(0)\} = \text{Stab}\left(\psi\left(\sum_{i=1}^{4} x_iU(n)^3\right)\right) = \text{Stab}\left(\sum_{i=1}^{4} \psi(x_i)U(m)^3\right).$$

Como x_i é uma unidade em $\mathbb{Z}_n$, para todo $i = 1, 2, 3, 4$, então $\psi(x_i)$ é uma unidade em $\mathbb{Z}_m$, para todo $i = 1, 2, 3, 4$. Pelo Corolário 2.4.2, temos

$$\left|\sum_{i=1}^{4} \psi(x_i)U(m)^3\right| \geqslant 4\left|U(m)^3\right| - 3 = \frac{4\left(p^l - p^{l-1}\right)}{3} - 3.$$

Como $p \geqslant 13$, temos $\dfrac{4(p-1)}{3} - 3 \geqslant p$, donde

$$\left(\frac{4(p^l - p^{l-1})}{3} - 3\right) = \left(\frac{4p^{l-1}(p-1)}{3} - 3\right) \geqslant p^{l-1}(p+3) - 3 = p^l + 3p^{l-1} - 3 \geqslant p^l.$$

Dessa forma, $\sum_{i=1}^{4} \psi(x_i)U(m)^3 = \mathbb{Z}_m$, ou seja, pela Observação 2.4.1, segue que Stab $\left(\sum_{i=1}^{4} \psi(x_i)U(m)^3\right)$ $\mathbb{Z}_m$. Já vimos que Stab $\left(\sum_{i=1}^{4} \psi(x_i)U(m)^3\right) = \{\psi(0)\}$, o que implica $\mathbb{Z}_m = \{\psi(0)\}$ e, consequentemente, $H = \mathbb{Z}_n$.

Por $H = \text{Stab}\,(x_1U(n)^3 + x_2U(n)^3 + x_3U(n)^3 + x_4U(n)^3)$ e novamente pela Observação 2.4.1, temos $x_1U(n)^3 + x_2U(n)^3 + x_3U(n)^3 + x_4U(n)^3 = \mathbb{Z}_n$. Com isso, existem $a_1, a_2, a_3, a_4 \in U(n)^3$ tais que

$$a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 = -x_5 - \cdots - x_k.$$

Logo, colocando $a_i = 1 \in U(n)^3$, $\forall i \in \{5, ..., k\}$, existem $a_i \in \{1, ..., k\}$ tais que $a_1x_1 + \cdots + a_kx_k = 0$. Portanto, S é uma sequência de soma-zero com peso em $U(n)^3$.

□

Observação 3.6.2. *Seja p um número primo e $r \geqslant 2$. Como $|U(p^r)| = p^{r-1}(p-1)$, se $p \equiv 2 \pmod 3$, então 3 não divide $|U(p^r)|$. Então, o homomorfismo $\psi : U(p^r) \to U(p^r)$ dado por $\psi(x) = x^3$ tem núcleo trivial e, portanto, $U(p^r)^3 = U(p^r)$.*

Corolário 3.6.3. *Seja $n = p^r$ em que p é um número primo ímpar tal que $p \neq 3, 7$. Seja S uma sequência sobre $\mathbb{Z}_n$ tal que pelo menos quatro termos de S são unidades. Então S é uma sequência de soma-zero com peso em $U(n)^3$.*

Demonstração. Se $p \equiv 2 \pmod 3$, como p é ímpar, segue do Lema 3.4.6 que S é uma sequência de soma-zero com peso em $U(n)$. Como já vimos, quando $p \not\equiv 1 \pmod 3$, temos $U(n) = U(n)^3$. Logo, S é uma sequência de soma-zero com peso em $U(n)^3$. Se $p \equiv 1 \pmod 3$, como $p \neq 7$, o resultado segue do Lema 3.6.1. □

Observação 3.6.3. *O corolário anterior não é verdadeiro quando $p = 2, 3, 7$.*

Como $U(7)^3 = \{\pm 1\}$, a sequência $(1, 1, 1, 1, 1)$ sobre $\mathbb{Z}_7$ não é uma sequência de soma-zero com peso em $U(7)^3$.

Como $U(9)^3 = \{\pm 1\}$, a sequência $(1, 1, 1, 1, 1)$ sobre $\mathbb{Z}_9$ não é uma sequência de soma-zero com peso em $U(9)^3$.

Teorema 3.6.2. *Se n não é divisível por $2, 3$ e 7, então $C_{U(n)^3}(n) \leqslant 2^{\Omega(n_2)}4^{\Omega(n_1)}$.*

Demonstração. Seja S uma sequência sobre $\mathbb{Z}_n$ de tamanho $k = 2^{\Omega(n_2)}4^{\Omega(n_1)}$. Precisamos mostrar que S possui uma subsequência de termos consecutivos de soma-zero com peso em $U(n)^3$. Novamente, vamos separar em casos.

1. Caso: Para qualquer primo p divisor de n_1 pelo menos quatro termos de S são coprimos com p e para qualquer primo p divisor de n_2 pelo menos dois termos de S são coprimos com p.

   Sejam p um número primo divisor de n, $v_p(n) = r$ e $S^{(p)}$ definida antes da Proposição 3.4.2. Se p divide n_1, então $S^{(p)}$ tem pelo menos quatro termos que são unidades, visto que pelo menos quatro termos de S são coprimos com p. Pelo Lema 3.6.1 segue que $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_{p^r}$ de soma-zero com peso em $U(p^r)^3$, visto que $p \neq 7$. Se p divide n_2, então $S^{(p)}$ possui pelo menos duas unidades, já que neste caso, S possui pelo menos dois termos coprimos com p. Como $p \neq 2$, segue do Lema 3.4.6 que $S^{(p)}$ é uma sequência sobre $\mathbb{Z}_{p^r}$ de soma-zero com peso em $U(p^r)^3$.

2. Caso: Existe um primo p divisor de n_1 tal que no máximo três termos de S são coprimos com p, ou existe um primo p divisor de n_2 tal que no máximo um termo de S é coprimo com p.

   A demonstração desses casos é feita de forma bastante similar aos casos b) e c) do Teorema 3.6.1.

□

4 Sequências extremas com peso

Neste capítulo, investigamos sequências extremas no contexto da constante consecutiva de Davenport com peso em A, seguindo as notações estabelecidas anteriormente e concentrando-nos no grupo $\mathbb{Z}_n$. Nosso objetivo é caracterizar, sempre que possível, as sequências de comprimento $C_A(n)-1$ que não admitem nenhuma subsequência de termos consecutivos cuja soma, ponderada pelos elementos de A, seja nula.

A análise desenvolvida neste capítulo complementa os resultados dos capítulos anteriores, oferecendo uma visão mais refinada da interação entre a estrutura das sequências extremas e constante $C_A(n)$. Os resultados estudados neste capítulo podem ser encontrados em [11].

4.1 Introdução

Definição 4.1.1. *Sejam $A \subset R$ não vazio e $k = C_A(M)$. Suponha $k \geqslant 2$. Então, existe uma sequência S sobre M de tamanho $k-1$ que não admite uma subsequência de termos consecutivos de soma-zero com peso em A. Esta sequência será chamada de sequência extrema com peso A.*

Observação 4.1.1. *Dada S uma sequência extrema com peso em A, permutando os elementos de S produzimos uma nova sequência S' que pode não ser uma sequência extrema com peso em A. Por exemplo, $S = (2,3,2)$ não admite subsequência de termos consecutivos de soma-zero com peso em A, com $A = \{-1,1\}$. Pelo Corolário 3.4.2, $C_A(4) = 4$, e consequentemente S é uma sequência extrema com peso A. A sequência $S' = (3,2,2)$ obtida pela permutação dos elementos de S possui a subsequência $T' = (2,2)$ de termos consecutivos de soma-zero com peso em A, ou seja, S' não é uma sequência extrema com peso A.*

No próximo resultado temos uma caracterização das sequências extremas de $\mathbb{Z}_n$ com peso em $A = \{1\}$.

Teorema 4.1.1. *Sejam $A = \{1\}$ e $S = (x_1, ..., x_{n-1})$ uma sequência sobre $\mathbb{Z}_n$. Para cada $i \in \{1, .., n-1\}$, considere $y_i = x_1 + \cdots + x_i$. Então, S é uma sequência extrema com peso em A se, e somente se,*

$$\{y_i : 1 \leqslant i \leqslant n-1\} = \mathbb{Z}_n \backslash \{0\}.$$

Demonstração. Sejam $A = \{1\}$ e $S = (x_1, ..., x_{n-1})$ uma sequência sobre $\mathbb{Z}_n$. Pelo Corolário 3.1.2, $C_A(n) = n$, logo S é uma sequência extrema com peso em A se, e somente se, S não

admite subsequência de termos consecutivos de soma-zero. Sejam $i, j \in \{1, ..., n-1\}$ tais que $i < j$. Pelo que vimos na demonstração do Teorema 3.1.1, $y_i = y_j$ se, e somente se, $x_{i+1} + ... + x_j = 0$. Como S não pode ter subsequência de soma-zero, segue que $y_i \neq y_j$, para todos $i, j \in \{1, .., n-1\}$. Então, $\{y_i : 1 \leqslant i \leqslant n-1\}$ possui $n-1$ elementos. □

Observação 4.1.2. *Seja $A = \{1\}$. Para construir uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, podemos escolher $x_1 \in \mathbb{Z}_n \backslash \{0\}$ de $n-1$ maneiras. Dado x_1, podemos escolher x_2 de $n-2$ maneiras para que $y_2 \in \mathbb{Z}_n \backslash \{0, y_1\}$, pois não podemos escolher $x_2 = 0$ e nem $x_2 = -x_1$. Seguindo esse raciocínio, para $i \in \{3, .., n-1\}$, dados $x_1, x_2, ..., x_{i-1}$, podemos escolher x_i de $n-i$ maneiras para que $y_i \in \mathbb{Z}_n \backslash \{0, y_1, ..., y_{i-1}\}$. Dessa forma, existem $(n-1)!$ sequências extremas sobre $\mathbb{Z}_n$ com peso em A.*

Teorema 4.1.2. *Para $A = \mathbb{Z}_n \backslash \{0\}$, a sequência (x) de tamanho 1 é uma sequência extrema com peso em A se, e somente se, x é uma unidade.*

Demonstração. Note que (x) é uma sequência de soma-zero se, e somente se, x é um divisor de zero em $\mathbb{Z}_n$, ou seja, se, e somente se, $\text{mdc}(x, n) \neq 1$. Assim, (x) é uma sequência extrema com peso em A se, e somente se, $\text{mdc}(x, n) = 1$, isto é, se, e somente se, x é uma unidade em $\mathbb{Z}_n$. □

Observação 4.1.3. *O Teorema anterior caracteriza as sequências extremas com peso em $U(p)$, quando p é um número primo, pois $U(p) = \mathbb{Z}_p \backslash \{0\}$.*

4.2 Caso $A = U(p)^2$, em que p é um número primo

Como $U(2)^j = U(2)$, para todo $j \geqslant 1$, então o Teorema 4.1.2 caracteriza as sequências extremas com peso em $A = U(2)^j$.

Teorema 4.2.1. *Sejam F um corpo e A um subgrupo de $F^* = F \backslash \{0\}$. Uma sequência (x, y) sobre F^* admite uma subsequência de soma-zero com peso em A se, e somente se, x e $-y$ estão na mesma classe lateral de A.*

Demonstração. Seja $S = (x, y)$ uma sequência sobre F^*. Note que x e $-y$ estão na mesma classe lateral de A se, e somente se, existe $c \in A$ tal que $x = -cy$. Isto é, se, e somente se, existe $c \in A$ tal que $x + cy = 0$, o que prova o resultado. □

Corolário 4.2.1. *Sejam F um corpo e A um subgrupo de $F^* = F \backslash \{0\}$. Uma sequência (x, y) sobre F não admite uma subsequência de soma-zero com peso em A se, e somente se, $x, y \in U(p)$ e x, $-y$ não estão na mesma classe lateral de A.*

Demonstração. Segue imediatamente do teorema anterior. □

No Teorema 3.2.1 foi provado que $C_{U(2)^2}(2) = 2$ e $C_{U(p)^2}(p) = 3$, para p número primo distinto de 2. Isso motiva o próximo resultado.

Corolário 4.2.2. *Sejam $A = U(p)^2$, com p um número primo ímpar e $S = (x, y)$ uma sequência sobre $\mathbb{Z}_p$. Então, S é uma sequência extrema com peso em A se, e somente se, $x, y \in U(p)$ e $x, -y$ não estão na mesma classe lateral de A em $U(p)$.*

Demonstração. Basta considerar o corpo $\mathbb{Z}_p$ e o subgrupo Q_p de $\mathbb{Z}_p\backslash\{0\}$ no corolário anterior. □

4.3 Caso $A = U(p)^3$, em que p é um número primo

Seja p um número primo. Na Seção 3.3 vimos que quando $p \not\equiv 1 \pmod 3$, temos $U(p) = U(p)^3$. Dessa forma, o Teorema 4.1.2 caracteriza as sequências sobre $\mathbb{Z}_p$ que são extremas com peso em A, pois $A = \mathbb{Z}_p\backslash\{0\}$.

No Teorema 3.3.1 e no Lema 3.3.2, foi provado que $C_{U(p)^3}(p) = 3$ se $p \neq 7$ e $C_{U(7)^3}(7) = 4$, com $p \equiv 1 \pmod 3$. Isso motiva o próximo resultado, que caracteriza as sequências sobre $\mathbb{Z}_p$ que são extremas com peso em A quando $p \equiv 1 \pmod 3$.

Corolário 4.3.1. *Seja $A = U(p)^3$ em que $p \neq 7$ é um número primo tal que $p \equiv 1 \pmod 3$. Seja $S = (x, y)$ uma sequência sobre $\mathbb{Z}_p$. Então, S é uma sequência extrema com peso em A se, e somente se, $x, y \in U(p)$ e $x, -y$ não estão na mesma classe lateral de A em $U(p)$.*

Demonstração. Seja $S = (x, y)$ uma sequência sobre $\mathbb{Z}_p$. Como $C_A(p) = 3$, então S é uma sequência extrema com peso em A se, e somente se, S não admite subsequência de soma-zero com peso em A. Olhando $\mathbb{Z}_p$ como corpo, podemos concluir o resultado usando o Corolário 4.2.1. □

Para o caso $p = 7$ precisamos da definição abaixo.

Definição 4.3.1. *Sejam $S = (x_1, ..., x_k)$ e $T = (y_1, ..., y_k)$ duas sequências sobre $\mathbb{Z}_n$ e A um subgrupo de $U(n)$. Dizemos que S é A-equivalente a T se existem $c \in U(n)$ e $a_i \in A$, $1 \leqslant i \leqslant k$, tais que $cy_i = a_i x_i$.*

Com essa definição, percebe-se que se S é uma sequência de soma-zero com peso em A, então qualquer sequência A-equivalente a S também o é. Isso posto, se S é uma sequência extrema com peso em A, qualquer sequência A-equivalente a S também o é.

Proposição 4.3.1. *Seja $A = U(7)^3$. Então, S é uma sequência extrema com peso em A se, e somente se, S é A-equivalente a $(1, 3, 1)$.*

Demonstração. Seja S uma sequência sobre $\mathbb{Z}_7$. Suponha S uma sequência extrema com peso em A. Como visto no início desta seção, $C_A(7) = 4$, donde S tem tamanho 3. Como S não possui subsequência de termos consecutivos de soma-zero com peso em A, todos os termos de S são não nulos. Disso, os termos de S estão em $\{\pm 1, \pm 2, \pm 3\}$. Como $A = \{-1, 1\}$, dois termos consecutivos de S não podem ser iguais a menos de sinal. Note que $(1, 2, 1)$ e qualquer permutação de $(1, 2, 3)$ são sequências de soma-zero com peso em A, o que indica que S não pode ser A-equivalente a essas sequências. Assim, S necessariamente tem que ser A-equivalente a uma sequência em que o segundo termo seja 3 e o último seja 1. Agora, multiplicando por uma unidade, S deve ser A-equivalente a uma sequência com o primeiro termo igual a 1. Logo, S deve ser A-equivalente a uma sequência da forma $(1, 3, 1)$.

Reciprocamente, como $T = (1, 3, 1)$ não possui subsequência de soma-zero com peso em A, então T é uma sequência extrema com peso em A. Pelo raciocínio anterior a esta proposição, qualquer sequência A-equivalente a T é uma sequência extrema com peso em A, donde S o é. □

Observação 4.3.1. *O Teorema 4.1.2, Corolário 4.3.1 e a proposição anterior caracterizam todas as sequências extremas com peso em $U(p)^3$, em que p é um número primo.*

4.4 Caso $A = U(n)$

Pelo Corolário 3.4.4, sabemos que $C_A(n) = 2^{\Omega(n)}$, quando $A = U(n)$, n ímpar. O próximo resultado nos fornece um método de construção de sequências extremas sobre $\mathbb{Z}_n$ com peso em A.

Teorema 4.4.1. *Sejam $A = U(n)$, em que n é ímpar, p um número primo divisor de n, $n' = \dfrac{n}{p}$ e $A' = U(n')$. Então, $S = (pu_1, ..., pu_k, x^*, pv_1, ..., pv_k)$ é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, com $S_1' = (u_1, ..., u_k)$, $S_2' = (v_1, ..., v_k)$ sendo sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A' e $x^* \in \mathbb{Z}_n$ um elemento não divisível por p.*

Demonstração. Como n' é ímpar, $C_{A'}(n') = 2^{\Omega(n')}$. Como S_1' é uma sequência extrema sobre $\mathbb{Z}_{n'}$ com peso em A, então $k = 2^{\Omega(n')} - 1$. Seja S a sequência definida no enunciado deste Teorema. Quemos mostrar que S não admite subsequência de termos consecutivos de soma-zero com peso em A. Suponha, por absurdo, que exista T subsequência de S de termos consecutivos de soma-zero com peso em A e defina as sequências $S_1 = (pu_1, ..., pu_k)$ e $S_2 = (pv_1, ..., pv_k)$ sobre $\mathbb{Z}_n$.

Suponha que x^* não seja um termo de T. Então, T é uma subsequência ou de S_1 ou de S_2. Seja T' a sequência sobre $\mathbb{Z}_{n'}$ tal que seus termos são obtidos dividindo os termos de T por p. Como já vimos anteriormente, $f_{n,n'}(A) \subset A'$, pois n' divide n. Dividindo por

p a soma-zero com peso em A obtida de T, teremos uma soma-zero com peso em A' de termos consecutivos ou de S_1' ou de S_2', o que é um absurdo. Daí, x^* é um termo de T.

Considerando a soma-zero com peso em A obtida de T, vemos que um múltiplo de p é igual a x^* multiplicado por uma unidade de $\mathbb{Z}_n$. Dessa forma, temos uma contradição, pois p não divide x^*. Então, S não possui subsequência de termos consecutivos de soma-zero com peso em A. Como n é ímpar, $C_A(n) = 2^{\Omega(n)}$. Além disso, S é uma sequência de tamanho $2k+1 = 2^{\Omega(n)} - 1$, donde S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. □

Exemplo 4.4.1. *Vamos dar um exemplo de como usar o teorema anterior para construir sequências extremas com peso em A. Pelo Teorema 4.1.2, temos que (2) e (4) são sequências extremas sobre $\mathbb{Z}_5$ com peso em $U(5)$. Pelo teorema anterior, $(10, 4, 20)$ e $(10, 21, 20)$ são sequências extremas sobre $\mathbb{Z}_{25}$ com peso em $U(25)$. Repetindo esse processo, $(30, 12, 60, 38, 30, 63, 60)$ é uma sequência extrema sobre $\mathbb{Z}_{75}$ com peso em $U(75)$.*

Lema 4.4.1. *Sejam $A = U(n)$, em que n é ímpar, $l = 2^{\Omega(n)} - 1$ e p um número primo divisor de n. Então uma sequência S sobre $\mathbb{Z}_n$ possui uma subsequência de termos consecutivos de soma-zero com peso em A se S possui uma subsequência T de termos consecutivos de tamanho pelo menos $\frac{l+1}{2}$ tal que cada termo de T é divisível por p.*

Demonstração. Sejam $n' = \frac{n}{p}$ e $A' = U(n')$. Como $l = 2^{\Omega(n)} - 1$, temos $\frac{l+1}{2} = 2^{\Omega(n)-1}$ e, consequentemente, T tem tamanho pelo menos $2^{\Omega(n')}$. Seja T' a sequência sobre $\mathbb{Z}_{n'}$ obtida dividindo os elementos de T por p. Como n é ímpar, segue que n' é ímpar, donde $C_{A'}(n') = 2^{\Omega(n')}$ pelo Corolário 3.4.4. Como T' é uma sequência sobre $\mathbb{Z}_{n'}$ de tamanho pelo menos $2^{\Omega(n')}$, T' admite uma subsequência de termos consecutivos de soma-zero com peso em A'. Pelo Lema 3.4.5, T possui uma subsequência de termos consecutivos de soma-zero com peso em A. Como T é uma subsequência de S de termos consecutivos, segue que S admite subsequência de termos consecutivos de soma-zero com peso em A. □

Corolário 4.4.2. *Seja $A = U(n)$, com n um número ímpar. Suponha S uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A e p um número primo divisor de n. Então, p é coprimo com pelo menos um termo de S.*

Demonstração. Pelo Corolário 3.4.4, se S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A de tamanho l, então $l = 2^{\Omega(n)} - 1$. Suponha que não exista termo de S que seja coprimo com p. Como l é pelo menos $\frac{l+1}{2}$, pelo lema anterior, S possui subsequência de termos consecutivos de soma-zero com peso em A, o que contradiz a hipótese. Daí, pelo menos um termo de S é coprimo com p. □

O próximo teorema mostra que o método fornecido pelo Teorema 4.4.1 é o único para se obter sequências extremas sobre $\mathbb{Z}_n$ com peso em A, quando n é ímpar.

Teorema 4.4.2. *Seja $A = U(n)$, com n é um número ímpar. Suponha que $S = (x_1, ..., x_l)$ é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Então existe um número primo p divisor de n tal que p divide todos os termos de S exceto o termo do meio x_{k+1}, em que $k+1 = \frac{l+1}{2}$. Mais ainda, se $S_1 = (x_1, .., x_k)$, $S_2 = (x_{k+2}, .., x_l)$, $n' = \frac{n}{p}$ e $A' = U(n')$, então S_1' e S_2' são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A', em que S_1' e S_2' são sequências sobre $\mathbb{Z}_{n'}$ obtidas dividindo os termos das sequências S_1 e S_2 por p, respectivamente.*

Demonstração. Sabemos que $C_A(n) = 2^{\Omega(n)}$, pelo Corolário 3.4.4. Logo, por S ser uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, então $l = 2^{\Omega(n)} - 1$. Suponha que para todo primo q divisor de n, existem pelo menos dois termos de S que não sejam divisíveis por q. Sejam q um número primo divisor de n e $v_q(n) = r$. Como n é ímpar, q é ímpar. Considere a sequência $S^{(q)}$ definida antes da Proposição 3.4.2. Como pelo menos dois termos de S não são divisíveis por q, a sequência $S^{(q)}$ possui pelo menos duas unidades em seus termos. Pelo Lema 3.4.6, $S^{(q)}$ é uma sequência de soma-zero com peso em $U(q^r)$. Como funciona para todo primo q divisor de n, pela Proposição 3.4.2, S é uma sequência de soma-zero com peso em A. Isso contradiz a hipótese deste teorema. Daí, existe um primo p divisor de n tal que no máximo um termo de S não é divisível por p. Pelo Corolário 4.4.2, existe exatamente um termo de S, digamos x^*, que não é divisível por p.

Suponha $x^* \neq x_{k+1}$. Dessa forma, existe uma subsequência T de S de termos consecutivos de tamanho pelo menos $k+1$ tal que p divide todos os termos de T, pois o termo que não é divisível por p não está no meio da sequência. Como T possui tamanho pelo menos $k+1 = \frac{l+1}{2}$, pelo Lema 4.4.1 temos que S possui uma subsequência de termos consecutivos de soma-zero com peso em A, o que contradiz a hipótese deste teorema. Logo, $x^* = x_{k+1}$.

Sejam $n' = \frac{n}{p}$ e, para cada $i = 1, 2$, S_i e S_i' definidas no enunciado deste teorema. Se S_1' possui uma subsequência de termos consecutivos de soma-zero com peso em A', então S_1 possui uma subsequência de termos consecutivos de soma-zero com peso em A, pelo Lema 3.4.5. Como S_1 é um subsequência de S de termos consecutivos, então S possui uma subsequência de termos consecutivos de soma-zero com peso em A. Isso contradiz a hipótese deste teorema. Dessa forma, S_1' não possui subsequência de termos consecutivos de soma-zero com peso em A'. Agora falta mostrar que S_1' tem tamanho $C_{A'}(n') - 1 = 2^{\Omega(n')} - 1$. Como $k + 1 = \frac{l+1}{2} = 2^{\Omega(n)-1} = 2^{\Omega(n')}$, de fato S_1' tem tamanho $2^{\Omega(n')} - 1$. Então, S_1' é uma sequência extrema sobre $\mathbb{Z}_{n'}$ com peso em A'. Por um argumento bastante similar, concluimos que S_2' é uma sequência extrema sobre $\mathbb{Z}_{n'}$ com peso em A'. □

Observação 4.4.1. *Os Teorema 4.4.1 e 4.4.2 caracterizam todas as sequências extremas em $\mathbb{Z}_n$ com peso em $U(n)$, quando n é um número ímpar.*

Proposição 4.4.1. *Sejam $A = U(n)$, com n um número ímpar, e $n = p_1p_2$, em que p_1 e p_2 são números primos não necessariamente distintos. Então, S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A se, e somente se, S é da forma (b_1q_1, a_1, b_2q_1), em que q_1, q_2 é uma permutação de p_1, p_2 e $q_1 \nmid a_1$, $q_2 \nmid b_1b_2$.*

Demonstração. Suponha S uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Como $\Omega(n) = 2$, segue que S tem tamanho $2^{\Omega(n)} - 1 = 3$. Então podemos escrever $S = (x_1, x_2, x_3)$, com $x_1, x_2, x_3 \in \mathbb{Z}_n$. Pelo Teorema 4.4.2, existe um primo $q_1 \in \{p_1, p_2\}$ tal que x_2 é o único termo de S que é coprimo com q_1, donde $q_1 \nmid x_2$. Sejam $n' = \dfrac{n}{q_1}$, $x_1' = \dfrac{x_1}{q_1}, x_3' = \dfrac{x_3}{q_1}$ e $A' = U(n')$. Novamente pelo Teorema 4.4.2, temos que as sequências (x_1') e (x_3') são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A'. Como n' é um número primo, digamos q_2, pelo Teorema 4.1.2 segue que $x_1', x_3' \in U(q_2)$. Então, S é da forma (b_1q_1, a_1, b_2q_1), em que q_1, q_2 é uma permutação de p_1, p_2 e $q_1 \nmid a_1$, $q_2 \nmid b_1b_2$.

Reciprocamente, suponha que S seja uma sequência do tipo (b_1q_1, a_1, b_2q_2) e considere $n' = \dfrac{n}{q_1}$. Como $q_1 \in \{p_1, p_2\}$, segue que $\dfrac{n}{q_1}$ é um número primo, digamos q_2. Note que n é ímpar e $q_1 \in \{p_1, p_2\}$ é um número primo que divide n. Além disso, q_1 não divide a_1. Mais ainda, como $q_2 \nmid b_1$ e $q_2 \nmid b_1$, pois q_2 é um número primo e $q_2 \nmid b_1b_2$, segue que $b_1, b_2 \in U(n') = U(q_2)$. Pelo Teorema 4.1.2 $S_1' = (b_1)$ e $S_2' = (b_2)$ são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em $U(n')$. Pelo Teorema 4.4.1, $S = (b_1q_1, a_1, b_2q_1)$ é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. □

Proposição 4.4.2. *Sejam $A = U(n)$, com n um número ímpar, e $n = p_1p_2p_3$, em que p_1, p_2 e p_3 são números primos não necessariamente distintos. Então, S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A se, e somente se, S é de um dos dois tipos:*

1. *$(a_1q_1q_2, b_1q_1, a_2q_1q_2, c_1, a_3q_1q_2, b_2q_1, a_4q_1q_2)$, com $q_1 \nmid c_1$, $q_2 \nmid b_1b_2$ e $q_3 \nmid a_1a_2a_3a_4$.*
2. *$(a_1q_1q_2, b_1q_1, a_2q_1q_2, c_1, b_2q_1q_3, a_3q_1, b_3q_1q_3)$, com $q_1 \nmid c_1$, $q_2 \nmid b_1b_2b_3$ e $q_3 \nmid a_1a_2a_3$.*

em que q_1, q_2, q_3 é uma permutação de p_1, p_2, p_3 e $a_1, a_2, a_3, a_4, b_1, b_2, b_3, c_1 \in \mathbb{Z}_n$.

Demonstração. Suponha S uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Como $\Omega(n) = 3$, segue que S tem tamanho $2^{\Omega(n)} - 1 = 7$. Então podemos escrever $S = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, com $x_1, x_2, x_3, x_4, x_5, x_6, x_7 \in \mathbb{Z}_n$. Pelo Teorema 4.4.2, existe um primo $q_1 \in \{p_1, p_2, p_3\}$, digamos p_1 tal que x_4 é o único termo de S que não é divisível por q_1. Sejam $n' = \dfrac{n}{q_1}$, $x_1' = \dfrac{x_1}{q_1}, x_2' = \dfrac{x_2}{q_1}, x_3' = \dfrac{x_3}{q_1}, x_5' = \dfrac{x_5}{q_1}, x_6' = \dfrac{x_6}{q_1}, x_7' = \dfrac{x_7}{q_1}$ e $A' = U(n')$. Novamente pelo Teorema 4.4.2, as sequências $S_1' = (x_1', x_2', x_3')$ e $S_2' = (x_5', x_6', x_7')$ são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A'. Note que n' continua sendo um número ímpar, logo podemos aplicar a proposição anterior, com duas possibilidades:

1. ***O primo que divide os termos de*** S_1'***, exceto*** x_2'***, é o mesmo que divide os termos de*** S_2'***, exceto*** x_6'***, digamos*** q_2: Neste caso, S_1' e S_2' são da forma (a_1q_2, b_1, a_2q_2) e (a_3q_2, b_2, a_3q_2), respectivamente, em que q_2 e q_3 são permutações de p_2 e p_3, $q_2 \nmid b_1$ e $q_2 \nmid b_2$, e $q_3 \nmid a_1a_2$ e $q_3 \nmid a_3a_4$. Como q_2 e q_3 são números primos, segue que $q_2 \nmid b_1b_2$ e $q_3 \nmid a_1a_2a_3a_4$. Assim, a sequência S é da forma $(a_1q_1q_2, b_1q_1, a_2q_1q_2, c_1, a_3q_1q_2, b_2q_1, a_4q_1q_2)$, com $q_1 \nmid c_1$, $q_2 \nmid b_1b_2$ e $q_3 \nmid a_1a_2a_3a_4$.

2. ***O primo que divide os termos de*** S_1'***, exceto*** x_2'***, é diferente do que divide os termos de*** S_2'***, exceto*** x_6'***, digamos*** q_2 ***e*** q_3***, respectivamente***: Neste caso, S_1' e S_2' são da forma (a_1q_2, b_1, a_2q_2) e (b_2q_3, a_3, b_3q_3), respectivamente, em que q_2 e q_3 são permutações de p_2 e p_3, $q_2 \nmid b_1$ e $q_3 \nmid a_3$, e $q_3 \nmid a_1a_2$ e $q_2 \nmid b_2b_3$. Como q_2 e q_3 são números primos, segue que $q_2 \nmid b_1b_2b_3$ e $q_3 \nmid a_1a_2a_3$. Assim, a sequência S é da forma $(a_1q_1q_2, b_1q_1, a_2q_1q_2, c_1, b_2q_1q_3, a_3q_1, b_3q_1q_3)$, com $q_1 \nmid c_1$, $q_2 \nmid b_1b_2b_3$ e $q_3 \nmid a_1a_2a_3$.

Para a recíproca, basta usar o resultado anterior. □

4.5 Caso $A = U(n)^2$

Quando todo divisor primo de n é pelo menos 7, foi mostrado no Corolário 3.5.2 que $C_{U(n)^2} = 3^{\Omega(n)}$. O próximo resultado nos fornece um método de construir sequências extremas sobre $\mathbb{Z}_n$ com peso em $A = U(n)^2$.

Teorema 4.5.1. *Sejam $A = U(n)^2$ em que todo divisor primo de n é pelo menos 7 e p um divisor primo de n. Considere $n' = \frac{n}{p}$ e $A' = U(n')^2$. Então, a sequência $S = (pu_1, ..., pu_k, x^*, pv_1, ..., pv_k, x^{**}, pw_1, ..., pw_k)$ é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, em que $S_1' = (u_1, ..., u_k)$, $S_2' = (v_1, ..., v_k)$ e $S_3' = (w_1, ..., w_k)$ são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A' e $x^*, x^{**} \in \mathbb{Z}_n$ são tais que a imagem da sequência (x^*, x^{**}) pelo mapa natural $f_{n,p} : \mathbb{Z}_n \to \mathbb{Z}_p$ não possui subsequência de soma-zero com peso em $U(p)^2$.*

Demonstração. Como S_1' é uma sequência extrema sobre $\mathbb{Z}_{n'}$ com peso em A' de tamanho k, então $k = 3^{\Omega(n')} - 1$. Considere a sequência S do enunciado. Para que S seja uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, devemos mostrar que S não possui subsequência de termos consecutivos de soma-zero com peso em A e que tenha tamanho $3^{\Omega(n)} - 1$. Suponha que isso seja falso, ou seja, existe uma subsequência T de termos consecutivos de S que tem soma-zero com peso em A. Defina as sequências $S_1 = (pu_1, ..., pu_k)$, $S_2 = (pv_1, ..., pv_k)$ e $S_3 = (pw_1, ..., pw_k)$ sobre $\mathbb{Z}_n$.

Já vimos que $f_{n,n'}(A) \subset A'$. Assim, se T é uma subsequência de alguma sequências S_i, $i \in \{1, 2, 3\}$, definida anteriormente, dividindo a soma-zero com peso em A obtida de T, teremos uma contradição com o fato de S_i' não possuir subsequência de soma-zero com

peso em A', para todo $i \in \{1,2,3\}$. Daí, $T \cap \{x^*, x^{**}\} \neq \emptyset$. Novamente considerando a soma-zero com peso em A obtida de T, por T e $\{x^*, x^{**}\}$ possuírem termos em comum, uma combinação linear ponderada em A de uma subsequência de (x^*, x^{**}) é sempre um múltiplo de p.

Como p divide n, novamente podemos dizer que $f_{n,p}(A) \subset U(p)^2$. Assim, obtemos uma contradição com o fato que a imagem da sequência (x^*, x^{**}) pelo mapa natural $f_{n,p}$ não possuir uma subsequência de soma-zero com peso em $U(p)^2$. Dessa forma, S não admite subsequência de termos consecutivos de soma-zero com peso em A. Por fim, S possui tamanho $3k+2 = (3^{\Omega(n')}-1)3+2 = 3^{\Omega(n)}-1$. Com isso, S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. □

Exemplo 4.5.1. *Note que $U(7)^2 = \{1,2,4\}$, donde as classes laterais de $U(7)^2$ são:*

$$U(7)^2 = 2U(7)^2 = 4U(7)^2$$

e

$$3U(7)^2 = 5U(7)^2 = 6U(7)^2.$$

Pelo Corolário 4.2.2, $(4,1),(3,3),(2,1)e\ (1,1)$ são sequências extremas sobre $\mathbb{Z}_7$ com peso em $U(7)^2$. Usando o teorema anterior, $S = (28,7,15,21,21,36,14,7)$ é uma sequência extrema sobre $\mathbb{Z}_{49}$ com peso em $U(49)^2$.

Lema 4.5.1. *Sejam $A = U(n)^2$, em que todo divisor primo de n é pelo menos 7, $l = 3^{\Omega(n)}-1$ e q um divisor primo de n. Então, a sequência S sobre $\mathbb{Z}_n$ admite subsequência de termos consecutivos de soma-zero com peso em A se S admite uma subsequência T de termos consecutivos com tamanho pelo menos $\dfrac{l+1}{3}$ tal que cada termo de T é divisível por q.*

Demonstração. Sejam $n' = \dfrac{n}{q}$ e T' a sequência sobre $\mathbb{Z}_{n'}$ obtida dividindo os termos de T por q. Como T é de tamanho pelo menos $\dfrac{l+1}{3}$, então T' é uma sequência sobre $\mathbb{Z}_{n'}$ de tamanho pelo menos $\dfrac{3^{\Omega(n)}}{3} = 3^{\Omega(n')}$. Além disso, como todo divisor primo de n é pelo menos 7, segue do Corolário 3.5.2 que $C_{A'}(n') = 3^{\Omega(n')}$, em que $A' = U(n')^2$. Dessa forma, T' admite subsequência de termos consecutivos de soma-zero com peso em A'. Pelo Lema 3.4.5, T admite subsequência de termos consecutivos de soma-zero com peso em A. Como T é uma subsequência de termos consecutivos de S, segue que S admite subsequência de termos consecutivos de soma-zero com peso em A. □

Corolário 4.5.2. *Seja $A = U(n)^2$, em que todo divisor primo de n é pelo menos 7. Suponha que S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Então, para todo primo q divisor de n, q é coprimo com pelo menos dois termos de S.*

Demonstração. Como S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, segue que S tem tamanho $l = 3^{\Omega(n)} - 1$, pelo Corolário 3.5.2. Suponha que exista um divisor primo de n, digamos q, tal que no máximo um termo de S é coprimo com q. Então, existe uma subsequência de S, digamos T, de termos consecutivos com tamanho pelo menos $\frac{l+1}{3}$ tal que cada termo de T é divisível por q. Pelo Lema 4.5.1, S admite subsequência de termos consecutivos de soma-zero com peso em A, o que é uma contradição com a hipótese deste teorema. Portanto, pelo menos dois termos de S são coprimos com q. □

Teorema 4.5.2. *Seja $A = U(n)^2$, em que todo divisor primo de n é pelo menos 7. Suponha $S = (x_1, ..., x_l)$ uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Então, existe um número primo p divisor de n tal que p divide todos os termos de S, exceto x_{k+1} e $x_{2(k+1)}$, em que $k+1 = \frac{l+1}{3}$. Mais ainda, se $S_1 = (x_1, .., x_k), S_2 = (x_{k+2}, .., x_{2k+1}), S_3 = (x_{2k+3}, .., x_l)$, $n' = \frac{n}{p}$ e $A' = U(n')^2$, então S_1', S_2' e S_3' são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A', em que S_1', S_2' e S_3' denotam as sequências sobre $\mathbb{Z}_{n'}$ obtidas dividindo os termos de S_1, S_2 e S_3 por p.*

Demonstração. Pelo Corolário 3.5.2, $C_A(n) = 3^{\Omega(n)}$, donde $l = 3^{\Omega(n)} - 1$, visto que S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Suponha que para todo primo q divisor de n pelo menos três termos de S não são divisíveis por q. Seja q um divisor de n, $v_q(n) = r$ e $A_q = U(q^r)$. Sendo $S^{(q)}$ definida como antes da Proposição 3.4.2. Então, $S^{(q)}$ possui pelo menos três termos que são unidades em $\mathbb{Z}_{q^r}$, já que pelo menos três termos de S não são divisíveis por q, que é um número primo. Como q é um número primo maior ou igual a 7, segue do Lema 3.5.2 que $S^{(q)}$ é uma sequência sobre $\mathbb{Z}_{q^r}$ de soma-zero com peso em A_q^2. Como isso vale para todo número primo divisor de n, pela Observação 3.4.1 S é uma sequência de soma-zero com peso em A, o que é uma contradição com a hipótese deste teorema. Logo, existe um número primo p divisor de n tal que no máximo dois termos de S não são divisíveis por p.

Pelo corolário anterior, S possui exatamente dois termos não divisíveis por p, digamos x^* e x^{**}. Vamos assumir que x^* aparece primeiro que x^{**} em S. Além disso, suponhamos que $x^* \neq x_{k+1}$ ou $x^{**} \neq x_{2(k+1)}$, em que $k+1 = \frac{l+1}{3}$. Então, existe uma subsequência T de termos consecutivos de S de tamanho pelo menos $k+1$ tal que p divide todos os termos de T. Como todo divisor primo de n é pelo menos 7 e T possui tamanho pelo menos $\frac{l+1}{3}$, temos que S admite subsequência de termos consecutivos de soma-zero com peso em A, pelo Lema 4.5.1. Isso é uma contradição com a hipótese sobre S. Logo, $x^* = x_{k+1}$ e $x^{**} = x_{2(k+1)}$.

Seja $n' = \frac{n}{p}$ e, para cada $i \in \{1, 2, 3\}$, considere S_i e S_i' definidas nas hipóteses deste teorema. Suponha, sem perda de generalidade, que S_1' admite subsequência termos consecutivos de soma-zero com peso em A'. Então S_1 também admite subsequência de

termos consecutivos de soma-zero com peso em A, pelo Lema 3.4.5. Como S_1 é uma subsequência de termos consecutivos de S, então S admite uma subsequência de termos consecutivos de soma-zero com peso em A. Isso é uma contradição com nossa hipótese sobre S, donde S_1' não possui subsequência de termos consecutivos de soma-zero com peso em A'. Por fim, como $k+1 = \dfrac{l+1}{3}$ e $l+1 = 3^{\Omega(n)}$, temos que $k+1 = 3^{\Omega(n')}$. Daí, S_1' tem tamanho $k = 3^{\Omega(n')} - 1$ e, por definição, S_1' é uma sequência extrema sobre $\mathbb{Z}_{n'}$ com peso em A'. O mesmo acontece com S_2' e S_3'. □

Teorema 4.5.3. *Usando as notações do Teorema 4.5.2, a imagem da sequência (x^*, x^{**}) pelo mapa natural $f_{n,p}$ é uma sequência extrema sobre $\mathbb{Z}_p$ com peso em $U(p)^2$.*

Demonstração. Se $n = p$, então S é uma sequência extrema sobre $\mathbb{Z}_p$ com peso em Q_p. Temos que $T^* = (x^*, x^{**})$ é uma sequência extrema sobre $\mathbb{Z}_p$ com peso em $U(p)^2$, visto que T^* é uma sequência de tamanho $l = 2 = 3^1 - 1 = 3^{\Omega(p)} - 1$ e não possui subsequência de soma-zero com peso em $U(p)^2$, pelo Teorema 4.5.1. Então podemos assumir que n não é um número primo. Suponha que a imagem de T^* pelo mapa natural $f_{n,p}$ seja uma sequência de soma-zero com peso em $U(p)^2$, isto é, existem $c, d \in U(p)^2$ tais que

$$cf_{n,p}(x^*) + df_{n,p}(x^{**}) = 0. \tag{4.1}$$

Pelo Lema 3.4.4, existem $a, b \in U(n)^2$ tais que $c = f_{n,p}(a)$ e $d = f_{n,p}(b)$. Usando a Equação (4.1) e o fato de $f_{n,p}$ ser homomorfismo de módulos, segue que p divide $y = ax^* + by^{**}$ em $\mathbb{Z}_n$. Considere T a sequência obtida retirando os termos x^* e x^{**} de S e adicionando o termo y no final de S. Já que S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, p divide todos os termos de T, pelo Teorema 4.5.2.

Sejam $n' = \dfrac{n}{p}$ e $A' = U(n')^2$. Considere a sequência T' sobre $\mathbb{Z}_{n'}$ obtida dividindo os termos de T por p. Seja q um divisor primo de n'. Como S_1' é uma sequência extrema sobre $\mathbb{Z}_{n'}$ com peso em A' e, como todo divisor primo de n' é pelo menos 7, pois n possui essa propriedade, então pelo menos dois termos de S_1' são coprimos com q, vide Corolário 4.5.2. De forma análoga, pelo menos dois termos de S_2' são coprimos com q. Então, T' possui pelo menos quatro termos coprimos com q. Como isso é verdadeiro para todo primo q divisor de n', por um argumento similar ao utilizado no primeiro parágrafo da demonstração do Teorema 4.5.2, temos que T' é uma sequência de soma-zero sobre $\mathbb{Z}_{n'}$ com peso em A'. Pelo Lema 3.4.5, T é uma sequência de soma-zero sobre $\mathbb{Z}_n$ com peso em A.

Note que T é a concatenação das sequências S_1, S_2, S_3 e (y). Além disso, $a, b \in A$, donde S é uma sequência de soma-zero sobre $\mathbb{Z}_n$. Mas, isso não pode acontecer, visto a hipótese sobre S. Dessa forma, a imagem da sequência T^* pelo homomorfismo canônico $f_{n,p}$ não pode ser uma sequência de soma-zero sobre $\mathbb{Z}_p$ com peso em $U(p)^2$. Como $C_{U(p)^2}(p) = 3$, para $p > 2$, então a imagem da sequência T^* é uma sequência extrema sobre $\mathbb{Z}_p$ com peso em $U(p)^2$. □

Os Teoremas 4.5.1, 4.5.2 e 4.5.3 caracterizam todas as sequências extremas sobre $\mathbb{Z}_n$ com peso sobre $U(n)^2$, quando todo divisor primo de n é pelo menos 7.

Proposição 4.5.1. *Usando as notações do Teorema 4.5.2, p é o único divisor primo de n tal que p é coprimo com exatamente dois termos de S, e qualquer outro primo divisor de n é coprimo com pelo menos três termos de S.*

Demonstração. Pelo Teorema 4.5.2, sabemos que p é coprimo com exatamente dois termos de S. Seja q um número primo divisor diferente de p. Pelo Corolário 4.5.2, q é coprimo com pelo menos dois termos de S. Agora vamos mostrar que q não pode ser coprimo com exatamente dois termos de S. Suponha que isso seja falso, ou seja, q é coprimo com exatamente dois termos da sequência S. Por um argumento similar usado no primeiros dois parágrafos da demonstração do Teorema 4.5.2, esses dois termos devem ser x^* e x^{**}. Daí, q divide todos os termos de S_1. Como $q \neq p$ e q divide todos os termos de S_1, então q divide todos os termos de S_1'. Como q é um divisor de n' e S_1' é uma sequência extrema sobre $\mathbb{Z}_{n'}$ com peso em A', então q tem que ser coprimo com pelo menos dois termos de S_1', vide Corolário 4.5.2. Note que temos uma contradição com a suposição de que q é coprimo com exatamente dois termos de S. Portanto, q é coprimo com pelo menos três termos de S. □

Proposição 4.5.2. *Seja $A = U(n)^2$ em que $n = p_1p_2$ é um produto de dois números primos não necessariamente distintos que são pelo menos 7. Então, uma sequência sobre $\mathbb{Z}_n$ é uma sequência extrema com peso em A se, e somente se, é da forma $(b_1q_1, b_2q_1, a_1, b_3q_1, b_4q_1, a_2, b_5q_1, b_6q_1)$, em que q_1, q_2 é uma permutação de p_1, p_2, a sequência (b_i, b_{i+1}) é uma sequência extrema sobre $\mathbb{Z}_{q_2}$ com peso em $U(q_2)^2$, para $i = 1, 3, 5$, e a imagem da sequência (a_1, a_2) pelo homomorfismo f_{n,q_1} é uma sequência extrema sobre $\mathbb{Z}_{q_1}$ com peso em $U(q_1)^2$.*

Demonstração. Seja S uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Como todo divisor primo de n é pelo menos 7, temos $C_A(n) = 3^{\Omega(n)} = 9$, pelo Corolário 3.5.2. Assim, S possui tamanho 8, digamos $S = (x_1, ..., x_8)$. Novamente, todo primo divisor de n é pelo menos 7, donde existe um primo $q_1 \in \{p_1, p_2\}$, digamos $q_1 = p_1$, tal que os únicos elementos de S que são coprimos com q_1 são x_3 e x_6, vide Teorema 4.5.2. Sejam $n' = \dfrac{n}{q_1}$, $A' = U(n')^2$ e as sequências $S_1' = \left(\dfrac{x_1}{q_1}, \dfrac{x_2}{q_1}\right)$, $S_2' = \left(\dfrac{x_4}{q_1}, \dfrac{x_5}{q_1}\right)$ e $S_3' = \left(\dfrac{x_7}{q_1}, \dfrac{x_8}{q_1}\right)$.

Novamente pelo Teorema 4.5.2, as sequências S_1', S_2' e S_3' são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A', ou seja, são sequências extremas sobre $\mathbb{Z}_{q_2}$ com peso em $U(q_2)^2$, em que q_2 é o número primo n'. Pelo Teorema 4.5.3, a imagem da sequência (x_3, x_6) pelo homomorfismo canônico f_{n,q_1} é uma sequência extrema sobre $\mathbb{Z}_{q_1}$ com peso em $U(q_1)^2$. Assim, S é da forma $(b_1q_1, b_2q_1, a_1, b_3q_1, b_4q_1, a_2, b_5q_1, b_6q_1)$, em que q_1, q_2 é uma permutação de p_1, p_2, a sequência (b_i, b_{i+1}) é uma sequência extrema sobre $\mathbb{Z}_{q_2}$, para $i = 1, 3, 5$, e a

imagem da sequência (a_1, a_2) pelo homomorfismo f_{n,q_1} é uma sequência extrema sobre $\mathbb{Z}_{q_1}$ com peso em $U(q_1)^2$.

Reciprocamente, seja q_1 um divisor primo de n, digamos $q_1 = p_1$. Daí, $q_2 = n' = \dfrac{n}{q_1}$. Note que a sequência (b_i, b_{i+1}), para $i = 1, 3, 5$, é uma sequência extrema sobre $\mathbb{Z}_{q_2}$ com peso em $U(q_2)^2$ e a imagem de (a_1, a_2) pelo homomorfismo f_{n,q_1} é uma sequência extrema sobre $\mathbb{Z}_{q_1}$ com peso $U(q_1)^2$. Assim, segue do Teorema 4.5.1 que $S = (b_1q_1, b_2q_1, a_1, b_3q_1, b_4q_1, a_2, b_5q_1, b_6q_1)$ é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. □

4.6 Caso $A = U(n)^3$

Nesta seção, vamos utilizar a mesma notação introduzida no início da Seção 3.6.

Lema 4.6.1. *Seja $A = U(p)^3$, em que p é um número primo tal que $p \neq 2, 7, 13$. Se pelo menos três elementos de S são unidades de $\mathbb{Z}_p$, então S é uma sequência de soma-zero sobre $\mathbb{Z}_p$ com peso em A.*

Demonstração. Se $p \equiv 1 \pmod 3$, usando o Lema 3.3.1, S é uma sequência de soma-zero sobre $\mathbb{Z}_p$ com peso em A. Se $p \not\equiv 1 \pmod 3$, já vimos que $U(p) = U(p)^3$. Como $p \neq 2$, então p é um número primo ímpar, donde S é uma sequência de soma-zero sobre $\mathbb{Z}_p$ com peso em $U(p) = U(p)^3$, pelo Lema 3.4.6. Dessa forma, o resultado está demonstrado. □

Observação 4.6.1. *O lema anterior falha para os casos $p = 2, 7, 13$. Considere a sequência $S = (1, 1, 1)$, que é formada por três unidades de $\mathbb{Z}_p$. Como $U(2)^3 = \{1\}$, claramente S não é sequência de soma-zero com peso em $U(2)^3$. Agora, para $p = 7$, temos $U(7)^3 = \{-1, 1\}$ e, para $p = 13$, temos $U(13)^3 = \{-5, -1, 1, 5\}$. Fazendo as possibilidades de soma da sequência S com peso em $U(7)^3$ e $U(13)^3$, não teremos S como uma sequência sobre $\mathbb{Z}_p$ de soma-zero com peso em $U(p)^3$, para $p = 7, 13$.*

Pelo Corolário 3.6.2, sabemos que $C_{U(n)^3}(n) = 2^{\Omega(n_2)}3^{\Omega(n_1)}$, em que n é livre de quadrados e não divisível por $2, 7, 13$. O próximo teorema nos fornece uma maneira de se obter sequências extremas sobre $\mathbb{Z}_n$ com peso em $A = U(n)^3$.

Teorema 4.6.1. *Seja $A = U(n)^3$, em que n é livre de quadrados e não divisível por $2, 7, 13$. Se p é um primo divisor de n, $n' = \dfrac{n}{p}$ e $A' = U(n')^3$, então as construções abaixo nos fornecem sequências extremas sobre $\mathbb{Z}_n$ com peso em A.*

1. *Caso em que $p \equiv 1 \pmod 3$: Neste caso,*

$$S = (pu_1, ..., pu_k, x^*, pv_1, ..., pv_k, x^{**}, pw_1, ..., pw_k),$$

em que $x^*, x^{**} \in \mathbb{Z}_n$ são tais que a imagem da sequência (x^*, x^{**}) pelo homomorfismo $f_{n,p}$ não possui subsequência de soma-zero com peso em $U(p)^3$ e $S'_1 = (u_1, ..., u_k)$, $S'_2 = (v_1, ..., v_k)$, $S'_3 = (w_1, ..., w_k)$ são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A'.

2. *Caso em que $p \not\equiv 1 \pmod 3$: Neste caso, $S = (pu_1, ..., pu_k, x^*, pv_1, ..., pv_k)$, em que $x^* \in \mathbb{Z}_n$ não é divisível por p e $S'_1 = (u_1, ..., u_k)$, $S'_2 = (v_1, ..., v_k)$ são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A'.*

Demonstração. Sejam $n = n_1 n_2$ e $n' = \dfrac{n}{p}$, em que p é um número primo divisor de n. Como n é livre de quadrados e não é divisível por $2, 7$ e 13, n' também o é. Com isso, $C_{U(n')^3}(n') = 2^{\Omega(n'_2)}3^{\Omega(n'_1)}$. Vamos separar a demonstração em dois casos:

1. Caso $p \equiv 1 \pmod 3$: Neste caso, podemos escrever $n' = n'_1 n'_2$, em que $n'_1 = \dfrac{n_1}{p}$ e $n'_2 = n_2$. Dessa forma, $C_{U(n')^3}(n') = 2^{\Omega(n_2)}3^{\Omega(n_1)-1}$. Como $S'_1 = (u_1, ..., u_k)$, $S'_2 = (v_1, ..., v_k)$, $S'_3 = (w_1, ..., w_k)$ são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A', temos $k = C_{U(n')^3}(n') - 1 = 2^{\Omega(n'_2)}3^{\Omega(n'_1)} - 1 = 2^{\Omega(n_2)}3^{\Omega(n_1)-1} - 1$.

   Primeiro vamos mostrar que S da forma da hipótese deste teorema, item 1, não admite subsequência de termos consecutivos de soma-zero com peso em A. Suponha, por contradição, que isso não aconteça. Sendo assim, seja T uma subsequência de termos consecutivos de S de soma-zero com peso em A e defina as sequências $S_1 = (pu_1, ..., pu_k)$, $S_2 = (pv_1, ..., pv_k)$, $S_3 = (pw_1, ..., pw_k)$. Já vimos que a imagem de A pelo homomorfismo $f_{n,n'}$ está contida em $A' = U(n')^3$. Por um argumento similar ao utilizado no segundo parágrafo da demonstração do Teorema 4.5.1, se T é uma subsequência ou de S_1, S_2 ou S_3, temos uma contradição. Logo $T \cap \{x^*, x^{**}\} \neq \emptyset$. Dessa forma, se considerarmos a soma-zero com peso em A obtida de T, uma combinação linear ponderada em A de uma subsequência de (x^*, x^{**}) é sempre um múltiplo de p. Sabemos que a imagem de A pelo homomorfismo $f_{n,p}$ está contida em $U(p)^3$. Assim, se considerarmos uma combinação linear ponderada em A de uma subsequência de (x^*, x^{**}), temos uma subsequência de (x^*, x^{**}) de termos consecutivos de soma-zero com peso em $U(p)^3$, o que é uma contradição com a hipótese do teorema. Logo, S da forma da hipótese deste teorema, item 1, não admite subsequência de termos consecutivos de soma-zero com peso em A. Por fim, S possui tamanho

$$3k + 2 = 3(2^{\Omega(n_2)}3^{\Omega(n_1)-1} - 1) + 2 = 2^{\Omega(n_2)}3^{\Omega(n_1)} - 1.$$

   Logo, S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A.

2. Caso $p \not\equiv 1 \pmod 3$: Neste caso, podemos escrever $n' = n'_1 n'_2$, em que $n'_1 = n_1$ e $n'_2 = \dfrac{n_2}{p}$. Dessa forma, $C_{U(n')^3}(n') = 2^{\Omega(n_2)-1}3^{\Omega(n_1)}$. Como $S'_1 = (u_1, ..., u_k)$ e

$S_2' = (v_1, ..., v_k)$ são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A', temos $k = C_{U(n')^3}(n') - 1 = 2^{\Omega(n_2')}3^{\Omega(n_1')} - 1 = 2^{\Omega(n_2)-1}3^{\Omega(n_1)} - 1$.

Para mostrar que S da forma da hipótese deste teorema não admite subsequência de termos consecutivos de soma-zero com peso em A, a demonstração é similar ao caso anterior. Por fim, S possui tamanho

$$2k + 1 = 2(2^{\Omega(n_2)-1}3^{\Omega(n_1)} - 1) + 1 = 2^{\Omega(n_2)}3^{\Omega(n_1)} - 1.$$

Logo, S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A.

□

Vamos utilizar o teorema acima para construir sequências extremas no próximo exemplo

Exemplo 4.6.1. ***a)*** *Como* $5 \not\equiv 1 \pmod 3$*, segue que* $U(5)^3 = U(5)$*. Por* $2, 3, 4 \in U(5)$*, segue do Teorema 4.1.2 que* $(2), (3)$ *e* (4) *são sequências extremas sobre* $\mathbb{Z}_5$ *com peso em* $U(5)^3$*. Considere a sequência* $(37, 78)$ *sobre* $\mathbb{Z}_{95}$*. A imagem dessa sequência pelo homomorfismo* $f_{95,19}$ *é a sequência* $(-1, 2)$ *sobre* $\mathbb{Z}_{19}$*. Como* $2U(19)^3 = \{2, 3, 5, 14, 16, 17\}$*,* -1 *e* -2 *não estão na mesma classe lateral de* $U(19)^3$ *em* $U(19)$*. Pelo Corolário 4.3.1,* $(-1, 2)$ *é uma sequência extrema sobre* $\mathbb{Z}_{19}$ *com peso em* $U(19)^3$*. Assim, segue do Teorema 4.6.1 que a sequência* $(38, 37, 57, 78, 76)$ *é uma sequência extrema sobre* $\mathbb{Z}_{95}$ *com peso em* $U(95)^3$*.*

b) *Vimos que* $2U(19)^3 = \{2, 3, 5, 14, 16, 17\}$*, logo* 2 *e* -7 *não estão na mesma classe lateral de* $U(19)^3$ *em* $U(19)$*, assim como* 5 *e* -11*. Dai, segue do Corolário 4.3.1 que* $(2, 7)$ *e* $(5, 11)$ *são sequências extremas sobre* $\mathbb{Z}_{19}$ *com peso em* $U(19)^3$*. Note que a sequência* (44) *sobre* $\mathbb{Z}_{95}$ *é tal que sua imagem pelo homomorfismo* $f_{95,5}$*, a sequência* (4)*, é uma sequência extrema sobre* $\mathbb{Z}_5$ *com peso em* $U(5)^3$*. Assim, segue do Teorema 4.6.1 que a sequência* $(10, 35, 44, 25, 55)$ *é uma sequência extrema sobre* $\mathbb{Z}_{95}$ *com peso em* $U(95)^3$*.*

Lema 4.6.2. *Sejam* $A = U(n)^3$*,em que* n *é livre de quadrados e não é divisível por* 2*,* 7 *ou* 13*,* $l = 2^{\Omega(n_2)}3^{\Omega(n_1)} - 1$*,* S *uma sequência sobre* $\mathbb{Z}_n$ *e* q *um divisor primo de* n*. Suponha que, quando* q *divide* n_1*, exista uma subsequência* T *de termos consecutivos de* S *de tamanho pelo menos* $\dfrac{l+1}{3}$ *tal que cada termo de* T *seja divisível por* q *e, quando* q *divide* n_2*, exista uma subsequência* T *de termos consecutivos de* S *de tamanho pelo menos* $\dfrac{l+1}{2}$ *tal que cada termo de* T *é divisível por* q*. Então,* S *possui uma subsequência de termos consecutivos de soma-zero com peso em* A*.*

Demonstração. Sejam $n = n_1n_2$ e q um divisor primo de n. Considere $n' = \dfrac{n}{q}$. Vamos dividir a demonstração em casos.

1. Caso em que q divide n_1: Neste caso, $n_1' = \frac{n_1}{q}$ e $n_2' = n_2$. Seja T' a sequência sobre $\mathbb{Z}_{n'}$ obtida dividindo os termos de T por q. Como T possui tamanho pelo menos $\frac{l+1}{3} = 2^{\Omega(n_2)}3^{\Omega(n_1)-1} = 2^{\Omega(n_2')}3^{\Omega(n_1')}$. Sabemos, pelo Corolário 3.6.2, que $C_{A'}(n') = 2^{\Omega(n_2')}3^{\Omega(n_1')}$, em que $A' = U(n')^3$. Assim, T' possui uma subsequência de termos consecutivos de soma-zero com peso em A'. Pela Observação 3.4.2, T possui uma subsequência de termos consecutivos de soma-zero com peso em A. Como T é uma subsequência de termos consecutivos de S, então S possui subsequência de termos consecutivos de soma-zero com peso em A.

2. Caso em que q divide n_2: Neste caso, $n_1' = n_1$ e $n_2' = \frac{n_2}{q}$. Seja T' a sequência sobre $\mathbb{Z}_{n'}$ obtida dividindo os termos de T por q. Como T possui tamanho pelo menos $\frac{l+1}{2} = 2^{\Omega(n_2)-1}3^{\Omega(n_1)} = 2^{\Omega(n_2')}3^{\Omega(n_1')}$. O restante da demonstração segue de forma análoga ao caso anterior.

Portanto, S possui uma subsequência de termos consecutivos de soma-zero com peso em A. □

Corolário 4.6.2. *Sejam $A = U(n)^3$, em que n é livre de quadrados e não é divisível por 2, 7 ou 13, e S uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Então, para um primo q divisor de n_1 (respectivamente n_2), q é coprimo com pelo menos dois termos (respectivamente pelo menos um termo) de S.*

Demonstração. Sejam q um número primo divisor de n, $n' = \frac{n}{q}$ e S uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Dessa forma, se S possui tamanho l, temos $l = 2^{\Omega(n_2)}3^{\Omega(n_1)} - 1$. Novamente, vamos separar a demonstração em casos.

1. Caso q divida n_1: Suponha que no máximo um termo de S seja coprimo com q. Assim, conseguimos uma subsequência, digamos T, de termos consecutivos de S de tamanho pelo menos $\frac{l+1}{3}$ tal que cada termo de T é divisível por q. Pelo Lema 4.6.2, S possui subsequência de termos consecutivos de soma-zero com peso em A, o que contradiz nossa hipótese sobre S. Logo, pelo menos dois termos de S são coprimos com q.

2. Caso q divida n_2: Suponha que nenhum termo de S seja coprimo com q. Assim, conseguimos uma subsequência, digamos T, de termos consecutivos de S de tamanho pelo menos $\frac{l+1}{2}$ tal que cada termo de T é divisível por q. Pelo Lema 4.6.2, S possui subsequência de termos consecutivos de soma-zero com peso em A, o que contradiz nossa hipótese sobre S. Logo, pelo menos um termo de S é coprimo com q.

Portanto, o resultado está devidamente demonstrado. □

Teorema 4.6.2. *Sejam $A = U(n)^3$, em que n é livre de quadrados e não divisível por 2, 7 ou 13, e $S = (x_1, ..., x_l)$ uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A. Então, S deve ser de uma das duas formas abaixo.*

1. *Existe um número primo p divisor de n_1 tal que p divide todos os termos de S, exceto os termos x_{k+1} e $x_{2(k+1)}$, em que $k+1 = \frac{l+1}{3}$. Além disso, a imagem da sequência (x_{k+1}, x_{2k+2}) pelo homomorfismo $f_{n,p}$ é uma sequência extrema sobre $\mathbb{Z}_p$ com peso em $U(p)^3$. Mais ainda, se $S_1 = (x_1, ..., x_k)$, $S_2 = (x_{k+2}, ..., x_{2k+1})$, $S_3 = (x_{2k+3}, ..., x_l)$, $n' = \frac{n}{p}$ e $A' = U(n')^3$, então S_1', S_2' e S_3' são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A', em que S_1', S_2' e S_3' são sequências sobre $\mathbb{Z}_{n'}$ obtidas os termos de S_1, S_2 e S_1 por p.*

2. *Existe um número primo p divisor de n_2 tal que p divide todos os termos de S, exceto o termo x_{k+1}, em que $k+1 = \frac{l+1}{2}$. Mais ainda, se $S_1 = (x_1, ..., x_k)$, $S_2 = (x_{k+2}, ..., x_l)$, $n' = \frac{n}{p}$ e $A' = U(n')^3$, então S_1' e S_2' são sequências extremas sobre $\mathbb{Z}_{n'}$ com peso em A', em que S_1' e S_2' são sequências sobre $\mathbb{Z}_{n'}$ obtidas os termos de S_1 e S_2 por p.*

Demonstração. Como S é uma sequência extrema sobre $\mathbb{Z}_n$ com peso em A, pelo Corolário 3.6.2, $l = 2^{\Omega(n_2)}3^{\Omega(n_1)} - 1$. Vamos separar a demonstração em casos:

a) Para todo primo q divisor de n_1, pelo menos três termos de S são coprimos com q, e para todo primo q divisor de n_2 , pelo menos dois termos de S são coprimos com q.

Neste caso, como $q \neq 2, 7, 13$, se q divide n_1, então $S^{(q)}$ é uma sequência de soma-zero com peso em $U(q)^3$, pelo Lema 4.6.1, visto que existem pelo menos três termos de S que são coprimos com q. Além disso, como q é um primo ímpar, se q divide n_2, então $S^{(q)}$ é uma sequência de soma-zero sobre $\mathbb{Z}_q$ com peso em $U(q)$, pelo Lema 3.4.6, já que pelo menos dois termos de S são coprimos com q. Dessa forma, para todo q divisor primo de n, $S^{(q)}$ é uma sequência de soma-zero sobre $\mathbb{Z}_n$ com peso em $U(q)^3$. Pela Proposição 3.4.2, temos que S é uma sequência de soma-zero com peso em A, o que contradiz a nossa hipótese de S ser uma sequência extrema com peso em A.

b) Existe um primo p divisor de n_1 tal que no máximo dois termos de S são coprimos com p.

Neste caso, a prova é similar com as provas dos Teoremas 4.5.2 e 4.5.3, utilizando o Lema 4.6.1, Lema 4.6.2 e Corolário 4.6.2 nos lugares do Lema 3.5.2, Lema 4.5.1 e Corolário 4.5.2. Também usamos a consequência do Lema 3.4.4.

c) Existe um primo p divisor de n_2 tal que no máximo um termo de S é coprimo com p.

Neste caso, a prova é similar a do Teorema 4.4.2, utilizando o Lema 4.6.2 e o Corolário 4.6.2 nos lugares do Lema 4.4.1 e do Corolário 4.4.2.

□

Observação 4.6.2. *O Teorema 4.6.1 e Teorema 4.6.2 juntos caracterizam as sequências extremas sobre* $\mathbb{Z}_n$ *com peso em* $U(n)^3$ *quando* n *não é divisível por* $2, 7$ *ou* 13.

5 Generalização da Constante de Davenport com peso

5.1 Introdução

Neste capítulo, será abordada uma generalização da constante de Davenport. No artigo [7], os autores introduziram a constante $D(G, B)$, em que G é um grupo abeliano finito aditivo e B um subconjunto de G que contém o 0, ou seja, o elemento neutro do grupo G. Agora, vamos introduzir um conjunto de pesos para a soma e apresentar resultados a partir desse novo invariante.

Seja G um grupo abeliano finito e B um subconjunto de G de tal forma que $0 \in B$. Para inserirmos o conjuntos dos pesos, digamos A, faremos uma breve discussão. Pelo *Teorema Fundamental dos Grupos Abelianos Finitos* (uma demonstração detalhada do Teorema Fundamental dos Grupos Abelianos Finitos pode ser encontrada em [9]), temos $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, com $n_1 \mid n_2 \mid \cdots \mid n_r$. Sendo assim, vamos considerar G como $\mathbb{Z}_{n_r}$-módulo e $A \subset \{1, ..., n_r - 1\}$, já que n_r é o expoente do grupo G. Como anteriormente, vamos denotar uma sequência sobre G de tamanho l da forma $S = (x_1, ..., x_l)$. Definimos $D_A(G, B)$ como o menor inteiro positivo k tal que qualquer sequência S sobre G de tamanho pelo menos k admite uma subsequência não vazia T tal que $\sigma_A(T) \cap B \neq \emptyset$, em que $\sigma_A(T)$ representa o conjunto de todas as somas da subsequência T com os pesos em A.

Se $B = \{0\}$, então $D_A(G, B) = D_A(G)$, em que $D_A(G)$ denota a constante de Davenport com peso estudada no Capítulo 3. Sendo assim, como estamos assumindo que $0 \in B$ sempre, concluímos que $D_A(G, B) \leqslant D_A(G)$. Então, a constante $D_A(G, B)$ existe para qualquer subconjunto de pesos A sob as condições estabelecidas anteriormente e qualquer $\emptyset \neq B \subset G$ tal que $0 \in B$, visto que $D_A(G)$ sempre existe, segundo a Observação 3.1.2.

O presente capítulo visa calcular os valores de $D_A(G, B)$ para o caso em que $G = \mathbb{Z}_p$, com p um número primo e para esses pesos específicos. Pela discussão feita anteriormente, vamos considerar $\mathbb{Z}_p$ como $\mathbb{Z}_p$-módulo e, consequentemente, o conjunto de pesos A deve ser um subconjunto de $\mathbb{Z}_p$, isto é, $A \subset \{1, ..., p - 1\}$. Em particular, vamos trabalhar com os casos em que $A = U(p)$, $A = U(p)^2$ e $A = U(p)^3$. Com a finalidade de facilitar a notação, denotaremos $D_A(\mathbb{Z}_p, B)$ por $D_A(p, B)$.

Pela Observação 3.1.3, Teorema 3.2.1 e, o Teorema 3.3.1 juntamente com o Lema 3.3.2 e a discussão feita no início da Seção 3.3 do Capítulo 3, sabemos que $D_A(p, B) \leqslant 2$, $D_A(p, B) \leqslant 3$ e $D_A(p, B) \leqslant 3$, para A sendo $U(p)$, $U(p)^2$ e $U(p)^3$ respectivamente. Ou

seja, o trabalho feito no Capítulo 3 explicita, de forma imediata, um limitante superior para a constante nesses casos. O que será provado abaixo é que as constantes atingem a cota superior se, e somente se, $B = \{0\}$, para os casos citados acima.

Além disso, foi possível calcular o valor da constante em cada um dos casos. Para o caso $A = U(p)^2$, conseguimos mostrar que $D_A(p, B) = 2$ se, e somente se, existe uma única classe lateral de $U(p)^2$ em $U(p)$ que não intercepta B. E, para o caso $A = U(p)^3$, com $p \equiv 1 \pmod 3$, foi mostrado que $D_A(p, B) = 2$ se,e somente se, existe pelo menos uma e no máximo duas classes laterais de $U(p)^2$ em $U(p)$ que não intercepta B. Quando $p \not\equiv 1 \pmod 3$, temos $U(p) = U(p)^3$ e este caso também foi abordado, utilizando o resultado obtido para $A = U(p)$.

5.2 Valores de $D_A(\mathbb{Z}_p, B)$ para os casos em que $A = U(p)$, $A = U(p)^2$ e $A = U(p)^3$

Proposição 5.2.1. *Sejam p um número primo, $A = U(p)$ e $B \subset \mathbb{Z}_p$ tal que $0 \in B$. Então, $D_A(p, B) = 2$ se, e somente se, $B = \{0\}$.*

Demonstração. Suponha $D_A(p, B) = 2$. Assim, existe $x \in U(p)$ tal que $\sigma_A(x) \cap B = \emptyset$. Agora, como $x \in U(p)$, temos $\sigma_A(x) = \{xa : a \in U(p)\} = U(p)$, ou seja, $U(p) \cap B = \emptyset$. Logo, $B = \{0\}$.

Reciprocamente, se $B = \{0\}$, basta usar a Observação 3.1.3. □

Pelo que foi discutido, se $A = U(p)$, temos $D_A(p, B) \leqslant D_A(p) = 2$. Sendo assim, se $|B| \geqslant 2$, então $D_A(p, B) = 1$.

Lema 5.2.1. *Sejam p um número primo, $A = U(p)^2$ e $B \subset \mathbb{Z}_p$ tal que $0 \in B$ e $|B| \geqslant 2$. Então, $D_A(p, B) \leqslant 2$.*

Demonstração. Se $p = 2$, então $D_A(2, B) \leqslant D_A(2) = 2$, em que a última igualdade acontece pelo Teorema 3.2.1. Suponha $p \geqslant 3$. Dada uma sequência $S = (x, y)$ sobre $\mathbb{Z}_p$, se $x = 0$ ou $y = 0$, o resultado é válido. Vamos tratar o caso em que $x, y \in U(p)$. Para $p = 3$, como $|B| \geqslant 2$, então $1 \in B$ ou $2 \in B$. De qualquer forma, $U(3)^2 \cap B \neq \emptyset$, ou seja, $\sigma_A(x) \cap B \neq \emptyset$ ou $\sigma_A(y) \cap B \neq \emptyset$. Daí, $D_A(3, B) \leqslant 2$. Suponha $p \geqslant 5$. Como

$$\left|xU(p)^2\right| + \left|yU(p)^2\right| - 1 = \frac{p-1}{2} + \frac{p-1}{2} - 1 = p - 2,$$

pelo Teorema 2.3.2, temos $|xU(p)^2 + yU(p)^2| \geqslant p - 2$. Caso $|B| \geqslant 3$, o resultado é válido, já que existem pelo menos $p - 2$ elementos de $\mathbb{Z}_p$ no conjunto-soma $xU(p)^2 + yU(p)^2$. Suponha que $B = \{0, r\}$, com $r \in U(p)$. Se 0 ou r pertence a $xU(p)^2 + yU(p)^2$, então

$\sigma_A(x,y) \cap B \neq \emptyset$ e o resultado segue imediatamente. Caso $0, r \notin xU(p)^2 + yU(p)^2$, mostraremos que $r \in xU(p)^2 \cup yU(p)^2$. Se $xU(p)^2 \neq yU(p)^2$, como $U(p)^2$ tem índice dois em $U(p)$, ou $r \in xU(p)^2$ ou $r \in yU(p)^2$. Neste caso, $r \in xU(p)^2 \cup yU(p)^2$. Suponha $xU(p)^2 = yU(p)^2$ e $r \notin xU(p)^2$. Assim, existe $c \in U(p)$ tal que $c \neq r$ e $r \in cU(p)^2$. Agora, como $|xU(p)^2 + yU(p)^2| \geqslant p-2$ e $0, r \notin xU(p)^2 + yU(p)^2$, temos $c \in xU(p)^2 + yU(p)^2$. Assim, existem $q_1, q_2, q \in U(p)^2$ tais que

$$c = xq_1 + yq_2 \text{ e } r = cq.$$

Daí,

$$r = cq = (xq_1 + yq_2)q = x(q_1q) + y(q_2q) \in xU(p)^2 + yU(p)^2,$$

o que é uma contradição. Logo, $r \in xU(p)^2 = yU(p)^2$. Com isso, concluímos que $r \in xU(p)^2 \cup yU(p)^2$ também neste caso. Logo, se $0, r \notin xU(p)^2 + yU(p)^2$, temos $\sigma_A(x) \cap B \neq \emptyset$ ou $\sigma_A(y) \cap B \neq \emptyset$. Portanto, $D_A(p,B) \leqslant 2$. □

Podemos perceber que, dado B subconjunto não vazio de $\mathbb{Z}_2$ tal que $0 \in B$, temos $D_A(2,B) = 2$ se, e somente se, $B = \{0\}$. O próximo resultado fornece a única ocasião em que a cota superior de $D_A(p,B)$ é atingida, com $p \geqslant 3$.

Lema 5.2.2. *Sejam $p \geqslant 3$ um número primo, $A = U(p)^2$ e $B \subset \mathbb{Z}_p$ tal que $0 \in B$. Então, $D_A(p,B) = 3$ se, e somente se, $B = \{0\}$.*

Demonstração. Suponha $D_A(p,B) = 3$. Usando a contrapositiva do Lema 5.2.1, temos $|B| = 1$, ou seja, $B = \{0\}$.

Reciprocamente, se $B = \{0\}$, basta usar o Teorema 3.2.1. □

Teorema 5.2.1. *Sejam $p \geqslant 3$ um número primo, $A = U(p)^2$ e $B \subset \mathbb{Z}_p$ tal que $0 \in B$ e $|B| \geqslant 2$. Então, $D_A(p,B) = 2$ se, e somente se, existe uma única classe lateral $xU(p)^2$ em $U(p)$ que não intersecta B.*

Demonstração. Se $D_A(p,B) = 2$, existe $x \in U(p)$ tal que $\sigma_A(x) \cap B = \emptyset$, ou seja, $xa \notin B$, para todo $a \in U(p)^2$. Logo, $xU(p)^2 \cap B = \emptyset$. Agora, vamos provar que tal classe lateral é única. De fato, suponha que exista outra classe lateral que não intersecta B. Como $[U(p) : U(p)^2] = 2$, segue que $B = \{0\}$, o que é uma contradição com a hipótese. Logo, não pode existir duas classes laterais distintas de $U(p)^2$ em $U(p)$ em que ambas não tem interseção com B.

Reciprocamente, suponha que exista uma única classe lateral $xU(p)^2$ em $U(p)$ que não intersecta B. Considere $S = (x)$ a sequência unitária formada por tal x. Pela hipótese, S é sequência sobre $\mathbb{Z}_p$ tal que $\sigma_A(S) \cap B = \emptyset$. Logo, $D_A(p,B) \geqslant 2$. Pelo Lema 5.2.1, temos $D_A(p,B) \leqslant 2$. Logo, $D_A(p,B) = 2$. □

Com isso, se $|B| \geqslant 2$ e $xU(p)^2 \cap B \neq \emptyset$, para todo $x \in U(p)$, podemos concluir $D_A(p, B) = 1$.

Agora, vamos estudar o caso em que $A = U(p)^3$. Como visto anteriormente, se $p \not\equiv 1 \pmod 3$, então $U(p)^3 = U(p)$ e a Proposição 5.2.1 caracteriza este caso.

Lema 5.2.3. *Seja p um número primo tal que $p \equiv 1 \pmod 3$. Se $A = U(p)^3$ e $0 \in B \subset \mathbb{Z}_p$ é tal que $|B| \geqslant 2$, então $D_A(p, B) \leqslant 2$.*

Demonstração. Considere $S = (x, y)$ uma sequência qualquer sobre $\mathbb{Z}_p$. Se $x = 0$ ou $y = 0$, o resultado é válido trivialmente. Agora, suponha $x, y \in U(p)$ e $p \neq 7, 13$. Como $|B| \geqslant 2$, existe $r \in B$ tal que $r \in U(p)$. Assim, $S' = (-x, -y, r)$ é uma sequência em que os três termos são unidades em $\mathbb{Z}_p$. Pelo Lema 3.3.1, S' é uma sequência de soma-zero com peso em $U(p)^3$. Daí, existem $t_1, t_2, t_3 \in U(p)^3$ tais que $rt_1 - xt_2 - yt_3 = 0$, ou seja,

$$r = x(t_2t_1^{-1}) + y(t_3t_1^{-1}) \in xU(p)^3 + yU(p)^3.$$

Logo, $\sigma_A(x, y) \cap B \neq \emptyset$ e $D_A(p, B) \leqslant 2$ para $p \neq 7, 13$.

Se $p = 7$, então $U(7)^3 = \{\pm 1\}$ e as outras duas classes laterais de $U(7)^3$ em $U(7)$ são $2U(7)^3 = \{\pm 2\}$ e $3U(7)^3 = \{\pm 3\}$. Se $x, y \in U(7)^3$, temos $xy - yx = 0 \in B$, ou seja $\sigma_A(x, y) \cap B \neq \emptyset$. Mais ainda, se $xU(7)^3 = yU(7)^3$, então existem $t_1, t_2 \in U(7)^3$ tais que $t_1x = -t_2y$, já que $-1 \in U(7)^3$. Assim sendo, $t_1x + t_2y = 0 \in B$, isto é, $\sigma_A(x, y) \cap B \neq \emptyset$. Assim, suponha sem perda de generalidade que $x \in U(7)^3$. Além disso, suponha $xU(7)^3 \neq yU(7)^3$, ou seja, ou $yU(7)^3 = 2U(7)^3$ ou $yU(7)^3 = 3U(7)^3$. Se $xU(7)^3 \cap B \neq \emptyset$ ou $yU(7)^3 \cap B \neq \emptyset$, teremos $\sigma_A(x) \cap B \neq \emptyset$ ou $\sigma_A(y) \cap B \neq \emptyset$. Logo, suponha que as classes laterais $xU(7)^3$ e $yU(7)^3$ não possuem interseção com B. Se $yU(7)^3 = 2U(7)^3$, temos

$$3 = 1 + 2 \in xU(7)^3 + yU(7)^3 \text{ e } -3 = -1 - 2 \in xU(7)^3 + yU(7)^3.$$

Se $yU(7)^3 = 3U(7)^3$, temos

$$2 = 3 - 1 \in yU(7)^3 + xU(7)^3 \text{ e } -2 = -3 + 1 \in yU(7)^3 + xU(7)^3.$$

Em qualquer um dos casos, temos $\sigma_A(x, y) \cap B \neq \emptyset$. Por fim, suponha $x, y \notin U(7)^3$. Como $|B| \geqslant 2$, existe pelo menos um elemento de $U(7)^3$ que pertence a B. Por

$$1 = 3 - 2 \in xU(7)^3 + yU(7)^3 \text{ e } -1 = -3 + 2 \in xU(7)^3 + yU(7)^3,$$

então $\sigma_A(x, y) \cap B \neq \emptyset$, como desejado. Logo, $D_A(7, B) \leqslant 2$.

Se $p = 13$, então $U(13)^3 = \{\pm 1, \pm 5\}$ e as outras duas classes laterais de $U(13)^3$ em $U(13)$ são $2U(13)^3 = \{\pm 2, \pm 3\}$ e $4U(13)^3 = \{\pm 4, \pm 7\}$. Se $x, y \in U(13)^3$, temos $xy - yx = 0 \in B$. Mais ainda, se $xU(13)^3 = yU(13)^3$, então existem $t_1, t_2 \in U(13)^3$

tais que $t_1x = -t_2y$, já que $-1 \in U(13)^3$. Assim sendo, $t_1x + t_2y = 0 \in B$, isto é, $\sigma_A(x,y) \cap B \neq \emptyset$. Suponha sem perda de generalidade que $x \in U(13)^3$. Além disso, suponha $xU(13)^3 \neq yU(13)^3$ Se $xU(13)^3 \cap B \neq \emptyset$ ou $yU(13)^3 \cap B \neq \emptyset$, então $\sigma_A(x) \cap B \neq \emptyset$ ou $\sigma_A(y) \cap B \neq \emptyset$. Logo, suponha que as classes laterais $xU(13)^3$ e $yU(13)^3$ não possuem interseção com B. Se $yU(13)^3 = 2U(13)^3$, temos

$$4 = 1 + 3 \in xU(7)^3 + yU(7)^3, \ -4 = -1 - 3 \in xU(7)^3 + yU(7)^3,$$

$$7 = 5 + 2 \in xU(7)^3 + yU(7)^3 \text{ e } -7 = -5 - 2 \in xU(7)^3 + yU(7)^3.$$

Se $yU(13)^3 = 4U(13)^3$, temos

$$2 = -5 + 7 \in xU(7)^3 + yU(7)^3, \ -2 = 5 - 7 \in xU(7)^3 + yU(7)^3,$$

$$3 = -1 + 4 \in xU(7)^3 + yU(7)^3 \text{ e } -3 = 1 - 4 \in xU(7)^3 + yU(7)^3.$$

Em qualquer um dos casos, temos $\sigma_A(x,y) \cap B \neq \emptyset$. Por fim, suponha $x, y \notin U(13)^3$. Como $|B| \geqslant 2$, existe pelo menos um elemento de $U(13)^3$ que pertence a B. Por

$$1 = 10 - 9 \in xU(13)^3 + yU(13)^3, \ -1 = -10 + 9 \in xU(13)^3 + yU(13)^3,$$

$$5 = 11 - 6 \in xU(13)^3 + yU(13)^3 \text{ e } -5 = -11 + 6 \in xU(13)^3 + yU(13)^3,$$

temos $(xU(13)^3 + yU(13)^3) \cap B \neq \emptyset$, como desejado. Logo, $D_A(13, B) \leqslant 2$.

Portanto, qualquer que seja o número primo p tal que $p \equiv 1 \pmod 3$, temos $D_A(p, B) \leqslant 2$. □

Lema 5.2.4. *Sejam p um número primo tal que $p \equiv 1 \pmod 3$, $A = U(p)^3$ e $B \subset \mathbb{Z}_p$ tal que $0 \in B$. Então, $D_A(p, B) = 3$ se, e somente se, $B = \{0\}$.*

Demonstração. Suponha $D_A(p, B) = 3$. Pelo Lema 5.2.3, $|B| = 1$ e, consequentemente, $B = \{0\}$.

Reciprocamente, se $B = \{0\}$, basta usar o Teorema 3.3.1 e Lema 3.3.2. □

Teorema 5.2.2. *Sejam p um número primo tal que $p \equiv 1 \pmod 3$, $A = U(p)^3$ e $B \subset \mathbb{Z}_p$ tal que $0 \in B$ e $|B| \geqslant 2$. Então, $D_A(p, B) = 2$ se, e somente se, existe pelo menos uma e no máximo duas classes laterais de $U(p)^3$ em $U(p)$ que não possuem interseção com B.*

Demonstração. Suponha que $D_A(p, B) = 2$. Daí, existe $x \in U(p)$ tal que $xt \notin B$, para todo $t \in U(p)^3$, ou seja, $xU(p)^3 \cap B = \emptyset$ e existe pelo menos um classe lateral de $U(p)^3$ em $U(p)$ que não tem interseção com B. Agora, como $[U(p) : U(p)^3] = 3$, se as três classes laterais de $U(p)^3$ em $U(p)$ não possuem interseção com B, então $B = \{0\}$, o que é uma contradição com a hipótese. Logo, no máximo duas classes laterais de $U(p)^3$ em $U(p)$ não possui interseção com B.

Reciprocamente, suponha que exista pelo menos uma e no máximo duas classes laterais de $U(p)^3$ em $U(p)$ que não possuem interseção com B. Considere $S = (x)$. Como $x \in U(p)$ e $xt \notin B$, para todo $t \in U(p)^3$, então $\sigma_A(x) \cap B = \emptyset$. Logo, $D_A(p, B) \geqslant 2$. Pelo Lema 5.2.3, temos $D_A(p, B) \leqslant 2$, o que termina a demonstração. □

Podemos perceber que, se $p \equiv 1 \pmod 3$, $B \subset \mathbb{Z}_p$ é tal que $0 \in B$ e $|B| \geqslant 2$, $xU(p)^3 \cap B \neq \emptyset$, para todo $x \in U(p)$, então $D_A(p, B) = 1$.

Considerações finais

Neste capítulo, foram apresentados resultados inéditos sobre uma generalização da constante de Davenport com peso. Os teoremas desenvolvidos ampliam o conhecimento atual sobre o invariante, fornecendo estimativas exatas e construções explícitas em contextos até então não explorados.

A abordagem adotada combina técnicas clássicas da teoria aditiva, como o uso do *Teorema de Cauchy-Davenport* com adaptações específicas ao contexto dos pesos, respeitando a estrutura envolvida. Em particular, as análises aqui apresentadas constituem um avanço em relação aos resultados já consolidados para a constante de Davenport usual e suas variantes não ponderadas.

Estes resultados são, até onde sabemos, inéditos, e reforçam a relevância de se estudar versões ponderadas de constantes aditivas clássicas. A ideia é consolidar as contribuições aqui desenvolvidas e submetê-las para publicação em forma de artigo científico em periódico especializado da área.

Referências

[1] S. D. Adhikari and P. Rath. Davenport constant with weights and some related questions. *Integers*, 6:A30, 2006. Citado na página 9.

[2] T. M. Apostol. Introduction to Analytic Number Theory. *Springer – Undergraduate Texts in Mathematics*, 1976. Citado na página 42.

[3] A. L. Cauchy. Recherches sur les nombres. *Journal de l'École Polytechnique*, 9:99–116, 1813. Citado na página 8.

[4] M. N. Chintamani and B. K. Moriya. Generalizations of some zero sum theorems. *Proceedings of the Indian Academy of Sciences – Mathematical Sciences*, 122(1):15–21, 2012. Citado na página 38.

[5] H. Davenport. On the addition of residue classes. *J. London Math. Soc.*, 10(1):30–32, 1935. Citado na página 8.

[6] A. Geroldinger and F. Halter-Koch. Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory. *Chapman and Hall/CRC*, 2006. Citado na página 8.

[7] H. Godinho, A. Lemos and V. G. L. Neumann. A generalization of the Davenport constant over abelian groups. *Preprint*. Citado na página 72.

[8] S. Griffiths. The Erdős–Ginzburg–Ziv theorem with units. *Discrete Mathematics*, 308(23):5473–5484, 2008. Citado na página 43.

[9] I. N. Herstein. Tópicos de Álgebra. *Bookman*, 2ª edição, 2006. Citado na página 72.

[10] D. B. Leep and D. B. Shapiro. Multiplicative subgroups of index three in a field. *Proceedings of the American Mathematical Society*, 105(4):802–807, 1989. Citado 2 vezes nas páginas 10 e 23.

[11] S. Mondal, K. Paul and S. Paul. Extremal sequences for a weighted zero-sum constant. *Integers*, 22:A93, 2022. Citado 2 vezes nas páginas 9 e 54.

[12] S. Mondal, K. Paul and S. Paul. On a different weighted zero-sum constant. *Discrete Math.*, 346(6):113350, 2023. Citado 2 vezes nas páginas 9 e 29.

[13] M. B. Nathanson. Additive Number Theory. Inverse Problems and the Geometry of Sumsets. *Graduate Texts in Mathematics*, 165, Springer-Verlag, New York, 1996. Citado na página 16.

[14] F. A. A. de Oliveira. Teorema de Erdős-Ginzburg-Ziv com peso. Dissertação de Mestrado, Universidade Federal de Viçosa, 2014. Orientador: Abílio Lemos Cardoso Júnior. Citado na página 10.

[15] J. E. Olson. A combinatorial problem on finite abelian groups I. *J. Number Theory*, 1(1):8–10, 1969. Citado na página 8.

[16] J. E. Olson. A combinatorial problem on finite abelian groups II. *J. Number Theory*, 1(2):195–199, 1969. Citado na página 8.

[17] K. Rogers. A combinatorial problem in abelian groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 59:559–562, 1963. Citado na página 8.

[18] P. van Emde Boas and D. Kruyswijk. A combinatorial problem on finite abelian groups III. *Report ZW-1969-008*, Mathematisch Centrum, Amsterdam, 1969. Citado na página 9.