FILIPE AUGUSTO ALVES DE OLIVEIRA

TEOREMA DE ERDÖS-GINZBURG-ZIV 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*.

VIÇOSA
MINAS GERAIS - BRASIL
2014

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

T
O48t
2014

Oliveira, Filipe Augusto Alves de, 1986-
Teorema de Erdös-Ginzburg-Ziv com peso / Filipe Augusto Alves de Oliveira. – Viçosa, MG, 2014.
vii, 77 f. ; 29 cm.

Orientador: Abílio Lemos Cardoso Júnior.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Inclui bibliografia.

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

CDD 22 ed. 515.25

"De que me irei ocupar no céu, durante toda a Eternidade,
se não me derem uma infinidade de problemas de Matemática para resolver?"
Augustin Louis Cauchy.

Agradecimentos

Em primeiro lugar, agradeço a Deus por ter me dado toda força e paciência necessária para vencer todos os obstáculos desta caminhada e, principalmente, por ter colocado ao meu lado todos aqueles que agradecerei aqui, além daqueles que direta ou indiretamente contribuíram para esta conquista.

A minha família, em especial as minhas duas mães, Efigênia e Maria, por serem as minhas maiores incentivadoras e por terem me ensinado, com toda a simplicidade e carinho, as lições mais valiosas de minha vida.

A todos os meus amigos, que não me deixaram fraquejar em nenhum momento.

Aos amigos do mestrado do DMA-UFV que, além de me acompanharem em muitas horas de estudo, foram muito importantes em tantos outros momentos.

A todos os professores e funcionários do DMA pela dedicação.

Ao meu orientador, Abílio, pela confiança a mim depositada e por toda a atenção, suporte e compreensão durante os nossos estudos.

Aos professores Anderson, Marinês e Allan, por aceitarem o convite de participar da banca.

A minha esposa, Bárbara, por estar sempre ao meu lado, suportando todos os momentos de dificuldades e por ser sempre um porto seguro para meus sentimentos.

E finalmente, a CAPES, pelo suporte financeiro.

Sumário

Resumo **vi**

Abstract **vii**

Introdução **1**

1 Conceitos Preliminares **7**

1.1 Uma Demonstração do Teorema de Erdös-Ginz-burg-Ziv 7

1.2 Adição de Subconjuntos de um Grupo Abeliano 12

1.3 A e-transformada 13

1.4 O Teorema de Cauchy-Davenport 14

1.5 O Teorema de Kneser para Grupos 17

2 Teorema de Erdös-Ginzburg-Ziv com Peso {1,-1} **30**

2.1 Limite Inferior para $E_A(n)$, quando $A = \{1, -1\}$ 31

2.2 Limite Superior para $E_A(n)$, quando $A = \{1, -1\}$ 32

2.2.1 O Caso em que n é Par 32

2.2.2 Um Resultado Condicional 35

2.2.3 Sequências Completas de Inteiros 40

2.2.4 O Caso em que n é Ímpar 45

3 Teorema de Erdös-Ginzburg-Ziv com Peso Qualquer **49**

3.1 Teorema de EGZ com Peso 56

3.1.1 Demonstração do Teorema de EGZ com Peso 70
3.2 Considerações Finais 71

Referências Bibliográficas **74**

Resumo

OLIVEIRA, Filipe Augusto Alves de. Universidade Federal de Viçosa, M.Sc., fevereiro de 2014. **Teorema de Erdös-Ginzburg-Ziv com Peso**. Orientador: Abílio Lemos Cardoso Júnior. Coorientador: Allan de Oliveira Moura.

Neste trabalho apresentaremos generalizações para um famoso resultado da Teoria Aditiva dos Números que é o Teorema de Erdös-Ginzburg-Ziv. Nosso primeiro objetivo é encontrar o menor valor para o comprimento de uma sequência de inteiros em que sempre podemos encontrar uma subsequência de n termos que, somados com pesos em $\{1, -1\}$, assumam um valor igual a um múltiplo de n. Posteriormente, consideraremos uma generalização para o Teorema de Erdös-Ginzburg-Ziv em que as sequências são formadas de elementos em um grupo abeliano finito qualquer e que podemos, sob algumas condições, colocar pesos quaisquer sobre as somas dos elementos da sequência.

Abstract

OLIVEIRA, Filipe Augusto Alves de, M.Sc., Universidade Federal de Viçosa, February, 2014. **Teorema de Erdös-Ginzburg-Ziv com Peso**. Adiviser: Abílio Lemos Cardoso Júnior. Co-adviser: Allan de Oliveira Moura.

In this work we present generalizations to a famous result of the Additive Number Theory which is the Erdös-Ginzburg-Ziv theorem. Our first goal is to find the lowest value for the length of a sequence of integers for which we can always find a subsequence of n terms which, together with weight in $\{1, -1\}$, assume a value equal to a multiple of n. We also consider one generalizations to Erdös-Ginzburg-Ziv theorem where the sequences are formed by elements in a finite abelian group and for which we can, under some conditions, atribute any weight on the sums of elements of the sequence.

Introdução

Um dos temas importantes de estudo na Teoria Aditiva dos Números é a soma de conjuntos de números inteiros. Considerando $h \geq 2$ um número natural e que A_1, A_2, ..., A_h são conjuntos de números inteiros, definimos o *conjunto soma*

$$A_1 + A_2 + \ldots + A_h$$

como sendo o conjunto de todos os inteiros da forma $a_1 + a_2 + \ldots + a_h$, onde $a_i \in A_i$, para $i = 1, 2, \ldots, h$. Se A é um conjunto de números inteiros e $A_i = A$, para todo $i = 1, 2, \ldots, h$, então vamos denotar o *conjunto soma* $A_1 + A_2 + \ldots + A_h$ por hA. Assim, o *conjunto soma* hA é o conjunto de todas as somas de h elementos de A, com repetições permitidas.

O princípio da Teoria Aditiva dos Números remonta à Grécia Antiga, quando Pitágoras ilustrou a representação de quadrados como soma de dois quadrados. Pitágoras procurava a partir dos conjuntos $A = \{x^2 \ ; \ x \in \mathbb{Z}\}$ e $B = \{y^2 \ ; \ x \in \mathbb{Z}\}$ encontrar em

$$A + B = \{x^2 + y^2 \ ; \ x^2 \in A, y^2 \in B\}$$

os números quadrados, gerando os chamados *números pitagóricos*, ou seja, os números naturais que satisfazem a equação $z^2 = x^2 + y^2$.

Os conjuntos soma também podem ser definidos em qualquer grupo abeliano e, na verdade, em qualquer conjunto em que exista uma operação binária. Por exemplo, podemos considerar conjuntos soma no grupo $\mathbb{Z}/m\mathbb{Z}$ das classes de congruência módulo m. A formulação desta representação baseada em soma de conjuntos deu origem a esta teoria, cujo objtetivo atualmente consiste no estudo de soma de conjuntos em certas estruturas algébricas.

Os clássicos problemas da Teoria Aditiva dos Números foram classificados em duas classes:

(i) Os *problemas diretos* são problemas em que tentamos determinar a estrutura e as propriedades do conjunto soma $A_1 + A_2 + \ldots + A_h$ quando os conjuntos A_i são todos conhecidos. Um dos primeiros modelos de problemas diretos a aparecer na Teoria Aditiva dos Números foi o Teorema de Lagrange que afirma que cada inteiro

não negativo pode ser escrito como a soma de quatro quadrados. Assim, se A é o conjunto de todos os quadrados não negativos, então o conjunto soma $4A$ é o conjunto de todos os inteiros não negativos.

(ii) Os *problemas inversos* são problemas nos quais tentamos deduzir propriedades dos conjuntos A_1, A_2, ..., A_h a partir de propriedades do conjunto soma $A_1 + A_2 + \ldots + A_h$. Por exemplo, se A é um conjunto finito de números inteiros e se a cardinalidade do conjunto soma hA é pequena, o que podemos concluir sobre a estrutura do conjunto A?

Os primeiros estudos realmente significativos desta teoria só apareceram no século XVIII com o teorema dos quatro quadrados de Lagrange, já citado, e os teoremas de Gauss e Cauchy que são exemplos dos primeiros trabalhos em Teoria Aditiva dos Números, embora todos eles ainda abordassem os números poligonais. Em 1770, Edward Waring enuncia, sem provar, que todo número natural é a soma de, no máximo, quatro quadrados, nove cubos e dezenove quartas potências. Este é um dos problemas mais famosos de toda a Teoria dos Números e ficou conhecido como o "Problema de Waring".

Outro importante resultado foi o Teorema de Cauchy-Davenport, demonstrado por Augustin Louis Cauchy em 1813, no qual, dados A e B conjuntos de classes de congruência módulo p, onde p é um número primo, apresenta-se um limite inferior para a cardinalidade do conjunto soma $A + B$. Este teorema viria a ser demonstrado por Harold Davenport, sem o conhecimento da demonstração de Cauchy, em 1935 [12], o que explica a curiosa "parceria"dada no título deste teorema. No Capítulo 1, faremos uma demonstração do Teorema de Cauchy-Davenport, usando o Teorema de I. Chowla. Em 1956, A. G. Vosper classifica todos os pares de conjuntos de resíduos módulo p tais que a cardinalidade do conjunto soma é menor que a soma de suas cardinalidades.

Em 1961, Paul Erdös, Abraham Ginzburg e Abraham Ziv, demonstram em [17] um importante teorema que afirma que qualquer sequência de comprimento $2n-1$ de números inteiros, onde n é um número natural, possui uma subsequência de comprimento n cuja soma dos seus termos é um múltiplo de n. Este teorema é conhecido como o Teorema de Erdös-Ginzburg-Ziv. A demonstração deste importante resultado foi desenvolvida utilizando o *Princípio da Casa dos Pombos* e, no primeiro capítulo, faremos duas diferentes demonstrações deste teorema. Uma série de outras demonstrações do Teorema de Erdös-Ginzburg-Ziv são apresentados no livro [2].

Além disso, a sequência

$$(\overbrace{0,\ldots,0}^{n-1},\overbrace{1,\ldots,1}^{n-1})$$

possui comprimento $2n-2$ e não possui nenhuma subsequência cuja soma seja um múltiplo de n. Portanto, esta sequência nos garante que o número $2n-1$ encontrado por Erdös, Ginzburg e Ziv é o menor possível. Sendo assim, podemos definir o invariante $E(n)$ como sendo o menor inteiro t tal que qualquer sequência de t números inteiros contém n inteiros que somados geram um múltiplo de n. Desta forma, concluimos que $E(n) = 2n - 1$.

A partir deste teorema, teve início o estudo dos *problemas de soma-zero* que tratam de sequências de elementos em um grupo aditivo, abeliano e finito, em que soma de todos os elementos da sequência tem como resultado o elemento neutro (zero) do grupo em questão e passamos a denominar estas sequências como *sequências de soma-zero*. Os problemas de soma-zero, para um inteiro n positivo pré-determinado, consistem na busca pelo menor comprimento que uma sequência de elementos do grupo deve ter para que possamos garantir que exista uma subsequência, de um comprimento pré-determinado ou não, que é de soma-zero. Quando falamos de comprimento de uma sequência de elementos de um grupo, estamos considerando o número de elementos (incluindo o índice de cada um) desta sequência.

Anos depois, observando que se pode enxergar no teorema de Erdös-Ginzburg-Ziv que as sequências de inteiros podem ser associadas a sequências de elementos no conjunto das classes de resíduos módulo n, Paul Erdös passou a buscar a determinação do menor comprimento de uma sequência em $C_p^2 = C_p \oplus C_p$, onde C_p é o grupo cíclico de ordem p, tal que esta sequência possua uma subsequência de comprimento p cuja soma de seus elementos é zero módulo p.

Neste mesmo ambiente, Erdös e Davenport formularam a seguinte pergunta: "Podemos determinar o menor inteiro positivo t tal que toda sequência S de elementos em um grupo G, abeliano e finito, de comprimento $|S| \geq t$ possua uma subsequência cuja soma de seus elementos represente o elemento neutro de G?"

A partir desta pergunta, definiu-se este inteiro como a *constante de Davenport* do grupo G. Denota-se, atualmente, esta constante por $D(G)$. Mesmo sendo muito estudada, ainda existem muitas questões em aberto relativas a esta constante, pois não são muitos os grupos para os quais se conseguiu calcular o seu valor exato.

Em 1968, J. Olson demonstrou em [43] que, para o grupo $G = C_{p^{e_1}} \oplus C_{p^{e_2}} \oplus \ldots \oplus C_{p^{e_n}}$, onde p é um número primo e e_i é um número natural, para $i = 1, 2, \ldots, n$, temos

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

Além disso, neste mesmo ano, Olson mostrou em [44] que, para o grupo $G = C_m \oplus C_n$, onde m divide n, temos $D(G) = m + n - 1$.

Para G um grupo aditivo e abeliano de ordem n, definimos o invariante $E(G)$ como sendo o menor inteiro t tal que qualquer sequência de t elementos de G contém n elementos que somados resultam no *zero* de G. Como um caso particular, $E(C_n) = E(n) = 2n - 1$.

Em 1973, H. Harborth em [26] definiu mais dois invariantes. Dado o grupo

$$C_n^r = \overbrace{C_n \oplus C_n \oplus \ldots \oplus C_n}^{r \text{ vezes}},$$

com $n, r \in \mathbb{N}$, ele definiu o invariante $s(C_n^r)$ (ou $f(n, r)$ na notação de Harborth) como

o menor inteiro t tal que toda sequência S de elementos de C_n^r, com comprimento maior ou igual a t, possui uma subsequência T tal que seu comprimento é n e a soma de seus elementos é o zero de C_n^r. Ele definiu, também, o invariante $g(C_n^r)$ (ou $g(n,r)$ na notação de Harborth) como o menor inteiro t tal que toda sequência S de elementos distintos de C_n^r, com comprimento maior ou igual a t, possui uma subsequência T tal que seu comprimento é n e a soma de seus elementos é o zero de C_n^r. Além de definir estes invariantes, Harborth calculou os valores exatos destes invariantes para grupos específicos, como também definiu algumas propriedades e relações entre eles. Pela definição de Harborth e pelo Teorema de Erdös-Ginzburg-Ziv, temos $s(C_n) = E(C_n) = E(n) = 2n - 1$.

Já em 1996, no artigo [11], Y. Caro conjecturou que, dados os inteiros n e m, com $n \geq 2$ e $S = \{b_i\}_{i=1}^{m+n-1}$ uma sequência qualquer de números inteiros, se $W = \{w_i\}_{i=1}^{n}$ é uma sequência de números inteiros tais que $\sum_{i=1}^{n} w_i \equiv 0(mod\ m)$, então existe uma subsequência rearranjada $\{b_{j_i}\}_{i=1}^{n}$ de S tal que

$$\sum_{i=1}^{n} w_i b_{j_i} \equiv 0(mod\ m).$$

Claramente, tomando $m = n$ e $w_i = 1$, para todo $i \in \{1, 2, \ldots, n\}$, na conjectura acima, obtemos Teorema de Erdös-Ginzburg-Ziv.

Ao longo do tempo, alguns casos particulares desta conjectura foram sendo demonstrados e, em 2006 no artigo [23], o austríaco D. J. Grynkiewicz a demonstrou completamente.

Faremos, agora, algumas considerações. Dado um grupo G abeliano, com ordem n e expoente $exp(G)$, e considerando G como um $\mathbb{Z}$-módulo, primeiro identificaremos $\mathbb{Z}/n\mathbb{Z}$ com o conjunto de números $\{0, 1, \ldots, n-1\}$. Para um conjunto $A \subseteq \mathbb{Z} \setminus \{0\}$, a sequência $T = \{g_1, g_2, \ldots, g_t\}$ de elementos não necessariamente distintos de G e o conjunto $J = \{1, 2, \ldots, t\}$ dos índices, definimos

$$\Sigma_A(T) = \left\{ \sum_{i \in J'} a_i g_i \ ;\ a_i \in A \text{ e } J' \subseteq J \right\}.$$

Se $0 \in \Sigma_A(T)$, diremos que a sequência T é uma *sequência de A-soma-zero* e o conjunto A é denominado o conjunto dos pesos. Com isso, definimos os invariantes com peso:

- $D_A(G)$ é o menor inteiro t tal que qualquer sequência S de elementos de G, com comprimento $|S| \geq t$, contém uma subsequência A-soma-zero não vazia.
- $E_A(G)$ é o menor inteiro t tal que qualquer sequência S de elementos de G, com comprimento $|S| \geq t$, contém uma subsequência A-soma-zero com comprimento igual a $|G| = n$.

- $s_A(G)$ é o menor inteiro t tal que qualquer sequência S de elementos de G, com comprimento $|S| \geq t$, contém uma subsequência A-soma-zero com comprimento igual a $exp(G)$, onde $exp(G)$ é o menor inteiro k tal que $kg = 0$, para todo $g \in G$.

- $g_A(G)$ é o menor inteiro t tal que qualquer sequência S de elementos distintos de G, com comprimento $|S| \geq t$, contém uma subsequência A-soma-zero com comprimento igual a $exp(G)$.

- $\eta_A(G)$ é o menor inteiro t tal que qualquer sequência S de elementos em G, com comprimento $|S| \geq t$, contém uma subsequência A-soma-zero não vazia com comprimento menor ou igual a $exp(G)$.

Ainda em 2006, S. D. Adhikari *et al* demonstram em [1] que, para $A = \{1, -1\}$, temos $E_A(C_n) = s_A(C_n) = n + \lfloor \log_2 n \rfloor$, onde C_n é o grupo cíclico de ordem n e, para um número real x, $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a x. Este resultado é equivalente ao Teorema de Erdös-Ginzburg-Ziv para o peso $A = \{1, -1\}$.

Thangadurai aborda, em 2007, a constante de Davenport com peso para um p-grupo abeliano finito aditivo G em [47].

Seguindo a mesma linha de seu artigo anterior, S. D. Adhikari *et al* provaram, em [3] de 2008, que $s_A(C_n) = 2n - 1$ para o caso em que n é um natural ímpar e $A = \{1, -1\}$ e também demonstraram alguns resultados para a constante de Davenport com peso $D_A(C_p)$, onde p é um número natural primo. Neste mesmo trabalho, alguns resultados aparecem como citação. São eles (considerando sempre que p é um número natural primo):

- Para $a \in F_p^*$ temos, pelo Princípio da Casa dos Pombos, $D_{\{a\}}(C_p) = p$.

- Para $A = \{a, p - a\}$, onde $a \in F_p^*$, temos que $D_A(C_p) = 1 + \lfloor \log_2 p \rfloor$.

- Se $A = \{1, 2, \ldots, p - 1\}$, então $D_A(C_p) = 2$.

- Se $A = \{1, 2, \ldots, t\}$, onde t é um inteiro tal que $1 < t < p$, então $D_A(C_p) = \lceil \frac{p}{t} \rceil$, onde para o número real x, $\lceil x \rceil$ denota o menor inteiro maior ou igual a x.

- Se A é o conjunto dos resíduos quadráticos (ou resíduos não quadráticos) (*mod* p), então $D_A(C_p) = 3$.

Em sua tese de doutorado [36], A. Lemos, apresentou vários resultados para os invariantes $\eta_A(G)$, $g_A(G)$ e $s_A(G)$, quando G é um grupo abeliano finito específico e $A = \{1, -1\}$.

Para $A \subseteq \mathbb{Z}$ e G um grupo abeliano finito aditivo qualquer, D. J. Grynkiewicz, L. E. Marchan e O. Ordaz em [24], no ano de 2012, provaram que $E_A(G) = D_A(G) + |G| - 1$. Este resultado foi provado um pouco antes por Yuan e Zeng para $G = C_n$ em [50] em 2010.

No início do ano de 2013, A. Lemos, H. Godinho e D. Marques realizaram um estudo, [37], onde, dentre outras coisas, deram estimativas para $s_A(C_3^r)$ e provaram que $s_A(C_3^3) = 9$, $s_A(C_3^4) = 21$ e $41 \leq s_A(C_3^5) \leq 45$, onde $A = \{1, -1\}$.

Em nosso estudo, apresentaremos, no primeiro capítulo, duas demonstrações do Teorema de Erdös-Ginzburg-Ziv. Na primeira, usaremos o Teorema de Chevalley-Warning e na segunda, o Teorema de Cauchy-Davenport. Apresentaremos ainda o Teorema de Kneser que, junto com o Teorema de Cauchy-Davenport e as suas respectivas generalizações, formam um conjunto de ferramentas que serão imprescindíveis para o desdobramento dos capítulos subsequentes.

No segundo capítulo abordaremos uma generalização do Teorema de Erdös-Ginzburg-Ziv com peso para o caso em que $G = \mathbb{Z}$ e o conjuntos dos pesos é dado por $A = \{1, n-1\} = \{1, -1\}$ que foi desenvolvida por S.D. Adhikari *et al* no artigo [1].

No último capítulo, enunciaremos e demonstraremos um teorema desenvolvido por D. J. Grynkiewicz em 2006 no artigo [23] que prova completamente uma conjectura de Y. Caro e, sob algumas condições, uma conjectura de Y. Hamidoune. Como um caso particular, o teorema de D. J. Grynkiewicz demostra o Teorema de Erdös-Ginzburg-Ziv com peso qualquer.

Capítulo 1

Conceitos Preliminares

Existem três objetivos neste capítulo e dois deles são demonstrações do Teorema de Erdös-Ginzburg-Ziv. Em primeiro lugar, provaremos que o Teorema de Erdös-Ginzburg-Ziv pode ser visto como uma consequência do Teorema de Chevalley-Warning e, posteriormente, daremos uma nova demonstração usando o Teorema de Cauchy-Davenport. O nosso terceiro objetivo será demonstrar o Teorema de Kneser, o qual será uma ferramenta crucial no capítulo 3, onde provaremos o Teorema de Erdös-Ginzburg-Ziv com peso. Além disso, algumas ferramentas apresentadas neste capítulo serão novamente usadas no Capítulo 2.

1.1 Uma Demonstração do Teorema de Erdös-Ginzburg-Ziv

Como o tema central de nosso trabalho é o Teorema Erdös-Ginzburg-Ziv, vamos demonstrá-lo utilizando um outro forte resultado que é o Teorema de Chevalley-Warning. No livro [2], podemos encontrar outros interessantes métodos para chegarmos a este mesmo resultado.

Vamos começar apresentando um lema que será utilizado na demonstração do Teorema de Chevalley-Warning.

Lema 1.1. *Sejam $\mathbb{F}_q$ um corpo com q elementos e $0 \leq r < q-1$. Convencionando que $0^0 = 1$, temos*

$$\sum_{x \in \mathbb{F}_q} x^r = 0.$$

Demonstração. Para $r = 0$, o resultado óbvio. Suponha $0 < r < q-1$ e considere α um gerador do grupo multiplicativo $\mathbb{F}_q^*$. Assim $\mathbb{F}_q^* = \{\alpha, \alpha^2, \ldots, \alpha^{(q-1)}\}$. Tomando

$\sum_{x\in\mathbb{F}_q} x^r = S$, temos

$$\begin{aligned} S &= 0^r + \sum_{x\in\mathbb{F}_q^*} x^r \Rightarrow \\ S &= \alpha^r + \alpha^{2r} + \ldots + \alpha^{(q-1)r} \Rightarrow \\ \alpha^r S &= \alpha^{2r} + \alpha^{3r} + \ldots + \alpha^{(q-1)r} + \alpha^{qr} \Rightarrow \\ \alpha^r S &= S - \alpha^r + \alpha^{qr} \Rightarrow \\ S(\alpha^r - 1) &= \alpha^{qr} - \alpha^r \Rightarrow \\ S(\alpha^r - 1) &= \alpha^r(\alpha^{(q-1)r} - 1). \end{aligned}$$

Note que $x^{(q-1)} = 1$, para todo $x \in \mathbb{F}_q^*$ e $\alpha^r - 1 \neq 0$ (caso contrário α não seria um gerador $\mathbb{F}_q^*$, pois $0 < r < q-1$), além disso sabemos que em um corpo vale a *Lei do Anulamento do Produto*. Assim, temos

$$\begin{aligned} S(\alpha^r - 1) &= \alpha^r(\alpha^{(q-1)r} - 1) \Rightarrow \\ S(\alpha^r - 1) &= \alpha^r(1-1) \Rightarrow \\ S(\alpha^r - 1) &= 0 \Rightarrow \\ S &= 0. \end{aligned}$$

Assim, concluímos que $\sum_{x\in\mathbb{F}_q} x^r = S = 0$, para todo $0 \leq r < (q-1)$.

□

A partir deste resultado, provaremos, agora, o Teorema de Chevalley-Warning.

Teorema 1.2 (Chevalley-Warning)**.** *Seja p um número primo e $\mathbb{F}_q$ o corpo finito com $q = p^t$ elementos, onde $t \in \mathbb{N}$. Para $i = 1, 2, \ldots, m$, seja $f_i(x_1, x_2, \ldots, x_n)$ um polinômio de grau d_i em n variáveis com coeficientes em $\mathbb{F}_q$. Denotemos por N o número de n-uplas $(x_1, x_2, \ldots, x_n)$ de elementos de $\mathbb{F}_q^n$ tais que $f_i(x_1, x_2, \ldots, x_n) = 0$, para todo $i = 1, 2, \ldots, m$. Se*

$$\sum_{i=1}^{m} d_i < n,$$

então

$$N \equiv 0 (mod\ p).$$

Demonstração. Como o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico, para qualquer $x \in \mathbb{F}_q$

$$x^{q-1} = \begin{cases} 1, & se \quad x \neq 0 \\ 0, & se \quad x = 0 \end{cases}. \tag{1.1}$$

Além disso, como convencionamos que $0^0 = 1$ e considerando $0 \leq r < q-1$, temos, pelo Lema 1.1,

$$\sum_{x \in \mathbb{F}_q} x^r = 0. \tag{1.2}$$

Sejam $x_1, x_2, \ldots, x_n \in \mathbb{F}_q$ e note que

$$\prod_{i=1}^{m}(1 - f_i(x_1, x_2, \ldots, x_n)^{q-1}) = \begin{cases} 1, & se \quad f_i(x_1, x_2, \ldots, x_n) = 0 \text{ para todo } i \\ 0, & se \quad f_i(x_1, x_2, \ldots, x_n) \neq 0 \text{ para algum } i \end{cases}$$

e assim

$$N = \sum_{x_1, \ldots, x_n \in \mathbb{F}_q} \left(\prod_{i=1}^{m}(1 - f_i(x_1, x_2, \ldots, x_n)^{q-1}) \right).$$

Como o grau de $f_i(x_1, x_2, \ldots, x_n)$ é d_i, temos que

$$\prod_{i=1}^{m}(1 - f_i(x_1, x_2, \ldots, x_n)^{q-1}) = \sum_{r_1, \ldots, r_n} a_{r_1 \cdot \ldots \cdot r_n} x_1^{r_1} \ldots x_n^{r_n}$$

é um polinômio de grau no máximo $(q-1) \cdot \sum_{i=1}^{m} d_i$, com coeficientes $a_{r_1 \cdot \ldots \cdot r_n} \in \mathbb{F}_q$. Então

$$\begin{aligned} N &\equiv \sum_{x_1, \ldots, x_n \in \mathbb{F}_q} \left(\prod_{i=1}^{m}(1 - f_i(x_1, x_2, \ldots, x_n)^{q-1}) \right) (mod\ p) \\ &\equiv \sum_{x_1, \ldots, x_n \in \mathbb{F}_q} \sum_{r_1, \ldots, r_n} a_{r_1 \cdot \ldots \cdot r_n} x_1^{r_1} \ldots x_n^{r_n} \ (mod\ p) \\ &\equiv \sum_{r_1, \ldots, r_n} a_{r_1 \cdot \ldots \cdot r_n} \sum_{x_1, \ldots, x_n \in \mathbb{F}_q} x_1^{r_1} \ldots x_n^{r_n} \ (mod\ p) \\ &\equiv \sum_{r_1, \ldots, r_n} a_{r_1 \cdot \ldots \cdot r_n} \prod_{j=1}^{n} \left(\sum_{x_j \in \mathbb{F}_q} x_j^{r_j} \right) (mod\ p), \end{aligned}$$

onde o somatório percorre todas as n-uplas $r_1, r_2, \ldots, r_n$ de inteiros não negativos tais que

$$\sum_{j=1}^{n} r_j \leq (q-1) \cdot \sum_{j=1}^{n} d_j < n \cdot (q-1).$$

Isso implica que, para algum $j \in \{1, \ldots, n\}$, temos $\sum_{x_j \in \mathbb{F}_q} x_j^{r_j} = 0$, pela equação (1.2), já que $0 \leq r_j < (q-1)$ e portanto,

$$\prod_{j=1}^{n} \left(\sum_{x_j \in \mathbb{F}_q} x_j^{r_j} \right) \equiv 0 \, (mod\ p).$$

Assim, concluimos que $N \equiv 0\,(mod\ p)$. □

Agora, veremos que o Teorema de Erdös-Ginzburg-Ziv para o caso em que $n = p$, onde p é um número primo, segue como um corolário do Teorema de Chevalley-Warning (1.2).

Teorema 1.3 (Erdös-Ginzburg-Ziv, para $n = p$ primo)**.** *Dada uma sequência de números inteiros com $2p-1$ elementos, onde p é um número natural primo, então existe uma subsequência de comprimento p cuja soma de seus elementos é um múltiplo de p.*

Demonstração. Dada a sequência $(a_1, a_2, \ldots, a_{2p-1})$ de números inteiros, tomemos a sequência $(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{2p-1}})$ no corpo finito $\mathbb{F}_p = \mathbb{Z}_p$ sendo a redução módulo p da sequência inicial. Considere os polinômios $f_1, f_2 \in \mathbb{F}_p[x_1, x_2, \ldots, x_{2p-1}]$ definidos por

$$f_1(x_1, \ldots, x_{2p-1}) = \sum_{j=1}^{2p-1} x_j^{p-1}$$

e

$$f_2(x_1, \ldots, x_{2p-1}) = \sum_{j=1}^{2p-1} \overline{a_j} x_j^{p-1}$$

Seja d_i o grau do polinômio f_i. Então $d_1 = d_2 = p-1$. Denotemos por N o número das soluções simultâneas desses polinômios. Como $d_1 + d_2 = 2p-2 < 2p-1$, segue do Teorema de Chevalley-Warning (Teorema 1.2) que $N \equiv 0(mod\ p)$. Desde que $f_1(0, \ldots, 0) = f_2(0, \ldots, 0) = 0$, decorre que $N > 1$ e assim $N \geq p \geq 2$. Portanto, os polinômios f_1 e f_2 têm uma solução não trivial, isto é, existem $t_1, t_2, \ldots, t_{2p-1} \in \mathbb{Z}_p$ não todos nulos tais que

$$f_1(t_1, \ldots, t_{2p-1}) = \sum_{j=1}^{2p-1} t_j^{p-1} = \overline{0} \tag{1.3}$$

e

$$f_2(t_1, \ldots, t_{2p-1}) = \sum_{j=1}^{2p-1} \overline{a_j} t_j^{p-1} = \overline{0}. \tag{1.4}$$

Como $t^{p-1} = 1$ se, e somente se, $t \neq \overline{0}$ em $\mathbb{Z}_p$, segue da equação (1.3) que $t_j \neq \overline{0}$ para exatamente p elementos $t_{j_1}, t_{j_2}, \ldots, t_{j_p} \in \mathbb{Z}_p$. Assim a equação (1.4) implica

$$a_{j_1} + a_{j_2} + \ldots + a_{j_p} \equiv 0(mod\ p),$$

donde segue que a sequência de inteiros $(a_1, a_2, \ldots, a_{2p-1})$, possui uma subsequência $(a_{j_1}, a_{j_2}, \ldots, a_{j_p})$ cuja soma de todos os seus elementos tem valor igual a um múltiplo de p. □

Para finalizar, vamos demonstrar que o Teorema de Erdös-Ginzburg-Ziv pode ser estendido para n arbitrário.

Teorema 1.4 (Erdös-Ginzburg-Ziv)**.** *Dada uma sequência com $2n-1$ números inteiros, onde n é um número natural, então existe uma subsequência de comprimento n cuja soma de seus elementos é um múltiplo de n.*

Demonstração. Vimos no teorema anterior que, para $n = p$, onde p é um número primo, o teorema já está demonstrado. Agora, vamos mostrar que, se o resultado vale para m e para n, onde m e n são naturais quaisquer, então vale para mn.

De fato, sejam $x_1, x_2, \ldots, x_{2mn-1} \in \mathbb{Z}$. Por hipótese temos que, para cada subconjunto A de $\{1, 2, \ldots, 2mn-1\}$ com $2n-1$ elementos, existe um subconjunto $B \subset A$ com n elementos tal que $\sum_{i\in B} x_i$ é divisível por n. Assim, construímos B_j indutivamente para todo $1 \leq j \leq 2m-1$, seguindo os seguintes passos

- Escolhemos um subconjunto A_j de $\{1, 2, \ldots, 2mn-1\} \setminus \bigcup_{1\leq k<j} B_k$ com $2n-1$ elementos.
- De A_j escolhemos um subconjunto B_j com n elementos tal que $\sum_{i\in B_j} x_i$ é divisível por n.

Observemos que, se $j \leq 2m-1$, então

$$\begin{aligned}\left|\{1, 2, \ldots, 2mn-1\} \setminus \bigcup_{1\leq k<j} B_j\right| &= 2mn-1-(j-1)n \\ &\geq 2mn-1-(2m-2)n \\ &= 2n-1.\end{aligned}$$

o que garante a construção até $j = 2m-1$. Definamos agora os inteiros $y_j = \frac{1}{n}\sum_{i\in B_j} x_i$ para $1 \leq j \leq 2m-1$. De novo, por hipótese, existe um subconjunto de índices $C \subset \{1, 2, \ldots, 2m-1\}$ com m elementos tal que $\sum_{j\in C} y_j$ é divisível por m e, assim,

$$\sum_{j\in C}\sum_{i\in B_j} x_i = n\sum_{j\in C} y_j$$

é uma soma de $|C||B_j| = mn$ inteiros, que é divisível por mn.

Isto demonstra o Teorema de Erdös-Ginzburg-Ziv para qualquer inteiro.

□

1.2 Adição de Subconjuntos de um Grupo Abeliano

Sejam $G = (G, +)$ um grupo abeliano e A_1, A_2, ..., A_n subconjuntos finitos e não vazios de G. Definimos o *conjunto-soma*

$$A_1 + A_2 + \ldots + A_n = \{a_1 + a_2 + \ldots + a_n / a_i \in A_i, i = 1, 2, \ldots, n\} \subseteq G.$$

Se A e B são subconjuntos finitos e não vazios de G, definimos o *conjunto-diferença*

$$A - B = \{a - b / a \in A, b \in B\} \subseteq G.$$

Não devemos confundir conjunto-diferença com diferença de conjuntos. Dados dois conjuntos A e B sua diferença é o conjunto

$$A \setminus B = \{a \in A / a \notin B\}.$$

Se $c \in G$ e $A \subset G$, definimos

$$c + A = \{c\} + A.$$

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 e outro de B. Dito de outro modo: $r_{A,B}(g)$ é o número de pares ordenados $(a, b) \in A \times B$ tais que $g = a + b$.

Lema 1.5. *Sejam G um grupo abeliano finito e A e B subconjuntos não vazios de G. Se existe $t \in \mathbb{N}$ tal que*

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

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

Demonstração. Dado $g \in G$, temos

$$\begin{aligned} |G| &\geq |A \cup (g - B)| \\ &= |A| + |g - B| - |A \cap (g - B)| \\ &= |A| + |B| - |A \cap (g - B)|. \end{aligned}$$

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

□

Lema 1.6. *Sejam G um grupo abeliano finito e A e B subconjuntos não vazios de G tais que*

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

Então $A + B = G$.

Demonstração. Ponha $t = 1$ no Lema 1.5 e o resultado segue da definição de $r_{A,B}(g)$. □

O Lema 1.6 acima nos diz que para estudar o conjunto $A + B$ devemos nos ocupar apenas com os subconjuntos não vazios A e B de G tais que $|A| + |B| \leq |G|$.

1.3 A e-transformada

Seja (A, B) um par ordenado de subconjuntos não-vazios de um grupo abeliano G finito. 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

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

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

O próximo lema estabelece algumas propriedades da e-transformada.

Lema 1.7. *Sejam A e B subconjuntos não-vazios de um grupo abeliano G finito. Para cada $e \in G$, a e-transformada de (A, B) satisfaz as seguintes condições:*

(i) $A(e) + B(e) \subset A + B$;

(ii) $A(e) \setminus A = e + (B \setminus B(e))$;

(iii) $|A(e)| + |B(e)| = |A| + |B|$, *se A e B são finitos;*

(iv) *Se $e \in A$ e $0 \in B$, então $e \in A(e)$ e $0 \in B(e)$.*

Demonstração. **(i)** Sejam $a' \in A(e)$ e $b' \in B(e)$. Como $a' \in A(e)$ então $a' \in A$ ou $a' \in (B + e)$.

- Se $a' \in A$, temos $b' \in B(e) \subseteq B$ e assim $a' + b' \in A + B$
- Se $a' \in (B + e)$, temos $b' \in B(e) \subseteq (A - e)$, ou seja, existem $b \in B$ e $a \in A$ tais que $a' = b + e$ e $b' = a - e$. Assim,

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

(ii)

$$\begin{aligned} A(e) \setminus A &= (B + e) \setminus A \\ &= \{b + e \,/\, b \in B \text{ e } b + e \notin A\} \\ &= e + \{b \in B \,/\, b \notin A - e\} \\ &= e + \{b \in B \,/\, b \notin B(e)\} \\ &= e + (B \setminus B(e)) \end{aligned}$$

(iii) Como A e B são finitos, usando **(ii)**, temos

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

(iv) Segue diretamente da definição da e-transformada.

□

1.4 O Teorema de Cauchy-Davenport

Nesta seção, demonstraremos o famoso Teorema de Cauchy-Davenport, que dá um limite inferior exato para a cardinalidade do conjunto-soma de dois subconjuntos não vazios de $\mathbb{Z}_p$, o grupo aditivo dos resíduos módulo um primo p. Iremos obtê-lo como consequência do Teorema de I. Chowla.

Teorema 1.8 (I. Chowla)**.** *Sejam $m \geq 2$, A e B subconjuntos não-vazios de $\mathbb{Z}_m$. Se $0 \in B$ e $(b, m) = 1$, para todo $b \in B \setminus \{0\}$, então*

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

Demonstração. Pelo Lema 1.6, precisamos provar o teorema apenas para o caso em que $|A| + |B| \leq m$, ou seja,

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

Se $|A| = 1$ ou $|B| = 1$, o teorema está demonstrado, pois, sem perda de generalidade, podemos considerar $|B| = 1$ e, assim, temos

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

Suponhamos, por contradição, que existam $A, B \subset \mathbb{Z}_m$ tais que $\min\{|A|, |B|\} \geq 2$ e $|A + B| < |A| + |B| - 1$. Esta última desigualdade nos diz que $A \neq \mathbb{Z}_m$, pois, caso contrário, teríamos $|A| = m$ e $|B| \geq 2$, que é um absurdo, considerando a hipótese de $|A| + |B| \leq m$.

Agora, vamos escolher um par (A, B) de modo que a cardinalidade de B seja mínima. Como $|B| \geq 2$, existe um elemento b^* não-nulo em B. Se $a + b^* \in A$, para todo $a \in A$, então $a + jb^* \in A$, para todo $j \in \{0, 1, 2, \ldots\}$. Como, por hipótese, $(b^*, m) = 1$, então

$$\{a + jb^* \ / \ j = 0, 1, \ldots, m - 1\} = \mathbb{Z}_m,$$

o que dá $A = \mathbb{Z}_m$, uma contradição.

Portanto, existe $e \in A$ tal que $e + b^* \notin A$. Aplicando a e-transformada no par (A, B) e usando o Lema 1.7, obtemos um novo par $(A(e), B(e))$ de subconjuntos não vazios de $\mathbb{Z}_m$ tais que

$$|A(e) + B(e)| \leq |A + B| < |A| + |B| - 1 = |A(e)| + |B(e)| - 1.$$

Usando esta desigualdade, concluimos que $B(e) \neq \{0\}$, pois, caso contrário, teríamos

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

Assim, pela desigualdade anterior, $|A(e)| < |A(e)|$, que é um absurdo. Logo, $B(e) \geq 2$.

Além disso, como $e \in A$ e $0 \in B$, pelo ítem **(iv)** do Lema 1.7 temos $0 \in B(e)$. Além disso, $(b, m) = 1$, para todo $b \in B(e) \setminus \{0\}$, pois $B(e) \subset B$. Como $b^* \notin (A - e)$, então $b^* \notin B(e)$. Logo $|B| > |B(e)|$, contradizendo a minimalidade de $|B|$. □

Com esta ferramenta em mãos, vamos agora demonstrar o principal teorema desta seção.

Teorema 1.9 (Cauchy-Davenport)**.** *Sejam p um primo, A e B subconjuntos não-vazios de $\mathbb{Z}_p$. Então*

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

Demonstração. Seja $b_0 \in B$. Temos $0 \in B - b_0$ e $(b, p) = 1$, para todo $b \neq 0$ em $B - b_0$. Usando o teorema anterior, obtemos

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

□

Como consequência do Teorema de Cauchy-Davenport, obtemos o seguinte resultado.

Corolário 1.10. *Sejam $n \geq 2$, p um primo, A_1, A_2, ... e A_n subconjuntos não-vazios de $\mathbb{Z}_p$. Então*

$$|A_1 + A_2 + \ldots + A_n| \geq \min\left\{p, \sum_{i=1}^{n} |A_i| - n + 1\right\}.$$

Demonstração. A prova é por indução. O caso $h = 2$ é o Teorema de Cauchy-Davenport. Suponhamos o teorema válido para n subconjuntos de $\mathbb{Z}_p$. Novamente, Cauchy-Davenport

nos dá

$$\begin{aligned} |A_1 + A_2 + \ldots + A_n + A_{n+1}| &\geq \min\{p, |A_1 + A_2 + \ldots + A_n| + |A_{n+1}| - 1\} \\ &\geq \min\left\{p, \sum_{i=1}^{n} |A_i| - n + 1 + |A_{n+1}| - 1\right\} \\ &\geq \min\left\{p, \sum_{i=1}^{n+1} |A_i| - (n+1) + 1\right\}. \end{aligned}$$

□

Sejam $n \geq 2$, $k_1, \ldots,$ e k_n inteiros positivos tais que $k_1 + \ldots + k_n \leq p + n - 1$. Para cada $i = 1, \ldots, n$, defina $A_i = \{0, 1, \ldots, k_i - 1\} \subset \mathbb{Z}_p$. Com isto,

$$A_1 + \ldots + A_n = \{0, 1, \ldots, k_1 + \ldots + k_n - n\}.$$

Daí

$$|A_1 + \ldots + A_n| = k_1 + \ldots + k_n - n + 1 = \sum_{i=1}^{n} |A_i| - n + 1,$$

e, além disso, é claro que $\emptyset \neq A_i \subseteq \mathbb{Z}_p$, para todo $i = 1, 2, \ldots, n$, pois $k_1 + k_2 + \ldots + k_n \leq p + n - 1$.

Isso mostra que o resultado do Corolário 1.10 (e, consequentemente, o Teorema de Cauchy-Davenport) é o melhor possível.

Para encerrarmos esta seção daremos uma outra demonstração para o Teorema de Erdös-Ginzburg-Ziv usando o Teorema de Cauchy-Davenport.

Teorema 1.11 (Erdös-Ginzburg-Ziv, para p primo)**.** *Dada uma sequência de números inteiros com $2p - 1$ elementos, onde p é um número natural primo, então existe uma subsequência de comprimento p cuja soma de seus elementos é um múltiplo de p.*

Demonstração. Vamos mostrar que, dados o número primo $p \geq 1$ e $(a_0, a_1, \ldots, a_{2p-2})$ uma sequênciade $2p - 1$ inteiros não necessariamente distintos, então existe uma subsequência $(a_{i_1}, a_{i_2}, \ldots, a_{i_p})$ tal que

$$a_{i_1} + a_{i_2} + \ldots + a_{i_p} \equiv 0 (mod\ p).$$

Escolha $a'_i \in \mathbb{Z}$ tal que $a'_i \equiv a_i (mod\ p)$ e $0 \leq a'_i < p$. Reenumere os inteiros a'_i tais que

$$0 \leq a'_0 \leq a'_1 \leq \ldots \leq a'_{2p-2} \leq p - 1 \tag{1.5}$$

Analisemos dois casos:

1^o caso: Existe i, $1 \leq i \leq p-1$ tal que $a'_i = a'_{i+p-1}$. Assim da desigualdade (1.5) segue $a'_i = \ldots = a'_{i+p-1}$ e, como $a'_i \equiv a_i (mod\ p)$, decorre $a_i \equiv a_{i+1} \equiv \ldots \equiv a_{i+p-1} (mod\ p)$ e

$$a_i + a_{i+1} + \ldots + a_{i+p-1} \equiv pa_i \equiv 0 (mod\ p).$$

2^o caso: Considere que, para todo $i = 1, \ldots, p-1$, temos $a'_i \neq a'_{i+p-1}$. Com isso, definimos em $\mathbb{Z}_p$ os seguintes subconjuntos de dois elementos

$$A_i = \{a_i + p\mathbb{Z}, a_{i+p-1} + p\mathbb{Z}\}.$$

Aplicando o Corolário 1.10, que é uma generalização do Teorema de Cauchy-Davenport,

$$|A_1 + A_2 + \ldots + A_{p-1}| \geq \min\{p, 2(p-1) - (p-1) + 1\} = p,$$

assim $A_1 + A_2 + \ldots + A_{p-1} = \mathbb{Z}_p$. Logo, existem classes de congruência $a_{j_i} + p\mathbb{Z} \in A_i$ para todo $i = 1, \ldots, p-1$, tal que $j_i \in \{i, i+p-1\}$ e

$$-a_0 \equiv a_{j_1} + a_{j_2} + \ldots + a_{j_{p-1}} (mod\ p),$$

isto é,

$$a_0 + a_{j_1} + a_{j_2} + \ldots + a_{j_{p-1}} \equiv 0 (mod\ p).$$

Logo $(a_0, a_{j_1}, a_{j_2}, \ldots, a_{j_{p-1}})$ é uma subsequência na forma desejada. □

Na primeira demonstração (Teoremas 1.3 e 1.4), já fizemos a generalização do caso de $n = p$ primo para n assumindo um valor inteiro positivo arbitrário.

1.5 O Teorema de Kneser para Grupos

O principal objetivo desta seção é provar um belo resultado sobre somas de subconjuntos finitos de um grupo abeliano G que é o Teorema de Kneser. Antes de enunciarmos este resultado, vamos fazer algumas definições que serão muito importantes para o restante de nossos estudos.

Definição 1.12. *Seja S um subconjunto não vazio do grupo abeliano G. O* ***estabilizador de S*** *é o conjunto*

$$H(S) = \{g \in G / g + S = S\}.$$

Facilmente verificamos que $H(S)$ é um subgrupo de G, pois

(i) $0 \in H(S)$;

(ii) Dados $a, b \in H(S)$, temos

$$(a-b)+S = (a-b)+(b+S) = a+S = S.$$

Além disso, $H(S)$ é o maior subgrupo de G tal que

$$H(S)+S = S.$$

Um elemento $g \in H(S)$ é chamado de *período* de S e S é chamado de *conjunto periódico*, se $H(S) \neq \{0\}$.

Por exemplo, se S é uma progresão aritmética infinita em $\mathbb{Z}$ com diferença d, então $H(S) = d\mathbb{Z}$. Note que G, neste caso, possui ordem infinita.

Vamos listar algumas propriedades do estabilizador de um subconjunto de um grupo.

Proposição 1.13. *Seja G um grupo abeliano finito. Dados A e B subconjuntos não vazios de G temos:*

(i) *$H(A) \subseteq H(A+B)$;*

(ii) *Se $H = H(A+B)$, então $|A+H|$, $|B+H|$ e $|A+B|$ são múltiplos de $|H|$;*

(iii) *$H(A) = G$ se, e somente se, $A = G$.*

Demonstração. **(i)** Seja $g \in H(A)$, então $g + A = A$. Sendo assim, temos

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

Portanto, $g \in H(A+B)$ e assim temos $H(A) \subseteq H(A+B)$.

(ii) Sendo $H = H(A+B)$, vemos que H é um subgrupo do grupo abeliano G. Consideremos $A = \{x_1, x_2, \ldots, x_l\}$. Assim, temos

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

Logo, existem no máximo l classes geradas por elementos de A, ou seja, existem k índices, $1 \leq i_1 < i_2 < \ldots < i_k \leq l$, onde $1 \leq k \leq l$, tais que

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

De modo análogo, segue o resultado para $|B+H|$ e $|A+B| = |(A+B)+H|$.

(iii) ($\Rightarrow$) Sejam $g \in G$ e $a \in A$. Como $g \in G = H(A)$, então $g + a \in A$. Além disso, $(-a) \in G = H(A)$, ou seja,

$$g = (g + a) + (-a) \in A.$$

Portanto, $A = G$.

($\Leftarrow$) Se $A = G$, então, para qualquer que seja $g \in G$, temos

$$g + A = g + G = G = A,$$

logo $g \in H(A)$ e $H(A) = G$.

□

Em 1953, o matemático alemão Martin Kneser demonstrou em um de seus estudos [34] que dados A e B dois subconjuntos finitos e não-vazios de um grupo abeliano G, então ou

$$|A + B| \geq |A| + |B|$$

ou

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

onde $H = H(A + B)$ é o estabilizador de $A + B$.

O Teorema de Kneser tem muitas aplicações na Teoria Aditiva dos Números. Em nossos estudos vamos usá-lo para demonstrar uma generalização do Teorema de Erdös-Ginzburg-Ziv. Esta generalização será formalmente apresentada no Capítulo 3.

Uma das ferramentas para se provar o Teorema de Kneser é o seguinte teorema:

Teorema 1.14. *Seja G um grupo abeliano, $G \neq \{0\}$, e sejam A e B subconjuntos finitos e não-vazios de G. Se $|A| + |B| \leq |G|$, então existe um subgrupo próprio H de G tal que*

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

Demonstração. Por indução sobre $|B|$. Se $|B| = 1$, então

$$|A + B| = |A| = |A| + |B| - 1 \geq |A| + |B| - |H|$$

para todo subgrupo H de G.

Seja $|B| > 1$. Agora, suponha que o teorema vale para todos os pares A', B' de subconjuntos finitos e não-vazios de G tais que $|B'| < |B|$. Separamos a prova em dois casos.

Caso 1. Supondo

$$a + b_2 - b_1 \in A$$

para todos $a \in A$ e $b_1, b_2 \in B$. Então

$$A + b_2 - b_1 = A,$$

para todos $b_1, b_2 \in B$. Seja H o subgrupo de G gerado por todos os elementos da forma $b_2 - b_1$, onde $b_1, b_2 \in B$. Então

$$1 < |B| \leq |H|$$

e, como $|A| \neq |B|$ (pois, caso contrário, teríamos $|A| + |B| > |G|$), temos

$$A + H = A \neq G.$$

Portanto, H é um subgrupo próprio de G e

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

Caso 2. Supondo que existam $a \in A$ e $b_1, b_2 \in B$ tais que

$$a + b_2 - b_1 \notin A.$$

Tomando

$$e = a - b_1 \in G,$$

temos

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

mas

$$b_1 \in A - (a - b_1) = A - e,$$

pois $0 \in (A - a)$. Aplicando a e-transformada ao par (A, B), obtemos um novo par $(A(e), B(e))$ de subconjuntos de G definidos por

$$A(e) = A \cup (B + e)$$

$$B(e) = B \cap (A - e).$$

Claramente, $b_2 \notin B(e)$ e assim $B(e)$ é um subconjunto próprio de B. Além disso, $b_1 \in B(e)$, ou seja, $B(e)$ é um subconjunto não-vazio de B. Portanto, a hipótese de indução se aplica ao par $(A(e), B(e))$. Usando as propriedades da e-transformada, concluímos que existe um subgrupo próprio H de G tal que

$$\begin{aligned} |A + B| &\overset{(a)}{\geq} |A(e) + B(e)| \\ &\overset{(b)}{\geq} |A(e)| + |B(e)| - |H| \\ &\overset{(c)}{=} |A| + |B| - |H|, \end{aligned}$$

onde usamos o Lema 1.7(i) em (a), a hipótese de indução em (b) e o Lema 1.7(iii) em (c) e com isso completamos a demonstração. □

Este simples resultado é muito importante em nossos estudos, pois é o ponto de partida de uma cadeia de resultados que são essenciais para a demonstração do Teorema de Kneser.

Agora, iremos listar três importantes lemas. A demonstração do primeiro depende do Teorema 1.14 e cada um dos outros dois lemas é consequência de seu antecessor.

Lema 1.15. *Sejam $G \neq \{0\}$ um grupo abeliano e $C = C_1 \cup C_2$ um subconjunto finito de G, onde C_1 e C_2 são subconjuntos próprios e não-vazios de C. Então*

$$|C_i| + |H(C_i)| \leq |C| + |H(C)|,$$

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

Demonstração. Se $|C_i| + |H(C_i)| \leq |C|$, para $i = 1$ ou $i = 2$, então nada há a fazer. Portanto, podemos assumir

$$|C| < |C_i| + |H(C_i)|, \tag{1.6}$$

para $i = 1$ e $i = 2$. Tomemos $H(C_i) = H_i$. Como H_1 e H_2 são subgrupos de G, vamos mostrar que $H_1 + H_2$ também é um subgrupo de G. De fato,

(i) $0 = 0 + 0 \in H_1 + H_2$;

(ii) dados $x, y \in H_1 + H_2$, temos $x = x_1 + x_2$ e $y = y_1 + y_2$ tais que $x_1, y_1 \in H_1$ e $x_2, y_2 \in H_2$. Logo,

$$x - y = (x_1 + x_2) - (y_1 + y_2) = (x_1 - y_1) + (x_2 - y_2) \in H_1 + H_2.$$

Assim, $H_1 + H_2$ é um subgrupo de G. Agora, denotemos por m_i o índice do subgrupo H_i em $H_1 + H_2$. Tomemos $H = H_1 \cap H_2$ com $|H| = h$. Pelo *Teorema do Isomorfismo* da *Teoria de Grupos*, temos

$$(H_1 + H_2)/H_1 \cong H_2/H$$

e

$$(H_1 + H_2)/H_2 \cong H_1/H.$$

Portanto, $|H_1| = m_2 h$, $|H_2| = m_1 h$ e $|H_1 + H_2| = m_1 m_2 h$. Como $H \subseteq H_i$, temos $H + C_i = C_i$ e C_i é uma união de classes de H em G. Portanto $C_1 \setminus C_2$ e $C_2 \setminus C_1$ são uniões de H-classes e assim

$$|C_1| \equiv |C_2| \equiv |C_1 \setminus C_2| \equiv |C_2 \setminus C_1| \equiv 0 (mod\ h).$$

Como C é a união de subconjuntos próprios C_1 e C_2, segue que $C_1 \setminus C_2$ e $C_2 \setminus C_1$ são não-vazios. Pela equação (1.6), temos

$$0 < |C_1 \setminus C_2| = |C \setminus C_2| = |C| - |C_2| < |C_2| + |H(C_2)| - |C_2| = |H_2| = m_1 h$$

e assim

$$h \leq |C_1 \setminus C_2| \leq (m_1 - 1)h. \tag{1.7}$$

Analogamente,

$$h \leq |C_2 \setminus C_1| \leq (m_2 - 1)h. \tag{1.8}$$

Escolha $c^* \in C_1 \setminus C_2$ e seja

$$D = c^* + H_1 + H_2.$$

Então D é a união de H_1-classes da forma

$$D_1 = c^* + h_2 + H_1, \tag{1.9}$$

onde $h_2 \in H_2$, e D é também a união de H_2-classes da forma

$$D_2 = c^* + h_1 + H_2, \tag{1.10}$$

onde $h_1 \in H_1$. Seja D_1 uma H_1-classe da forma (1.9) e seja D_2 uma H_2-classe da forma (1.10). Como $h_2 + H \subseteq H_2$ e $h_1 + H \subseteq H_1$, temos

$$c^* + h_1 + h_2 + H \subseteq D_1 \cap D_2.$$

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

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

Isto implica

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

e

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

e assim

$$g - (c^* + h_1 + h_2) \in H_1 \cap H_2 = H.$$

Logo, temos

$$g \in c^* + h_1 + h_2 + H$$

e assim

$$D_1 \cap D_2 \subseteq c^* + h_1 + h_2 + H.$$

Deste modo,

$$D_1 \cap D_2 = c^* + h_1 + h_2 + H$$

e a interseção de uma H_1-classe em D com uma H_2-classe em D é uma H-classe.

Como o índice de H_i em $H_1 + H_2$ é m_i, então o subgrupo $H_1 + H_2$ é a união de m_i H_i-classes disjuntas duas a duas e assim $D = c^* + H_1 + H_2$ é também a união de m_i H_i-classes 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, digamos, u_i H_i-classes duas a duas disjuntas e assim $\overline{C_i} \cap D$ (onde $\overline{C_i}$ denota o conjunto complementar de C_i) é 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 é uma H-classe, segue que

$$(C_2 \setminus C_1) \cap D = (C_2 \cap D) \cap (\overline{C_1} \cap D)$$

é a união de $u_2(m_1 - u_1)$ H-classes duas a duas disjuntas e assim,

$$|(C_2 \setminus C_1) \cap D| = u_2(m_1 - u_1)h. \tag{1.11}$$

Analogamente,

$$(C_1 \setminus C_2) \cap D = (C_1 \cap D) \cap (\overline{C_2} \cap D)$$

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

$$|(C_1 \setminus C_2) \cap D| = u_1(m_2 - u_2)h. \tag{1.12}$$

Como

$$c^* \in (C_1 \setminus C_2) \cap D \subseteq C_1 \setminus C_2,$$

segue

$$0 < |(C_1 \setminus C_2) \cap D| = u_1(m_2 - u_2)h \leq |C_1 \setminus C_2| \leq (m_1 - 1)h.$$

Portanto, $1 \leq u_1(m_2 - u_2) \leq m_1 - 1$ e assim

$$1 \leq u_1 \leq m_1 - 1$$

e

$$1 \leq u_2 \leq m_2 - 1.$$

Das equações *(1.7)*, *(1.8)*, *(1.11)* e *(1.12)*, temos

$$\begin{aligned}
0 &\leq (m_1 - u_1 - 1)(u_2 - 1)h + (m_2 - u_2 - 1)(u_1 - 1)h \\
&= u_2(m_1 - u_1)h - (m_2 - 1)h + u_1(m_2 - u_2)h - (m_1 - 1)h \\
&= |(C_2 \setminus C_1)| - (m_2 - 1)h + |(C_1 \setminus C_2) \cap D| - (m_1 - 1)h \\
&= {\scriptstyle |(C_2 \setminus C_1) \cap D| - (m_2 - 1)h - |(C_2 \setminus C_1) \cap \overline{D}| + |(C_1 \setminus C_2)| - (m_1 - 1)h - |(C_1 \setminus C_2) \cap \overline{D}|} \\
&\leq 0,
\end{aligned}$$

e assim $|C_2 \setminus C_1| = (m_2 - 1)h$ e $|C_1 \setminus C_2| = (m_1 - 1)h$. Como $H = H_1 \cap H_2$, segue

$$H + C = H + (C_1 \cup C_2) = (H + C_1) \cup (H + C_2) = C_1 \cup C_2 = C,$$

e assim $H \subseteq H(C)$. Portanto,

$$\begin{aligned} |C| - |C_2| &= |C \setminus C_2| \\ &= |C_1 \setminus C_2| \\ &= m_1 h - h \\ &= |H_2| - |H| \\ &\geq |H_2| - |H(C)|. \end{aligned}$$

Analogamente,

$$|C| - |C_1| \geq |H_1| - |H(C)|$$

e assim

$$|C_i| + |H(C_i)| \leq |C| + |H(C)|,$$

para ambos $i = 1$ e $i = 2$. Isto completa a demonstração deste lema. □

Como uma generalização do Lema 1.15, obtemos o seguinte lema.

Lema 1.16. *Sejam $n \in \mathbb{N}$, com $n \geq 2$, e $\{0\} \neq G$ um grupo abeliano. Sendo C um subconjunto finito de G tal que*

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

onde $C_1, C_2, \ldots, C_n$ são subconjuntos próprios e não-vazios de C, então

$$|C_i| + |H(C_i)| \leq |C| + |H(C)|$$

para algum $i = 1, 2, \ldots, n$.

Demonstração. Faremos a prova por indução sobre n. O lema anterior é o caso $n = 2$. Seja $n \geq 3$ e suponhamos que o resultado valha para $n - 1$. Se $|C_i| + |H(C_i)| \leq |C|$, para algum i, então $|C_i| + |H(C_i)| \leq |C| < |C| + |H(C)|$ e a demonstração termina. Caso contrário, temos

$$|C| < |C_i| + |H(C_i)|,$$

para todos $i = 1, 2, \ldots, n$. Se C é a união de $n - 1$ dos subconjuntos $C_1, C_2, \ldots, C_n$, pela hipótese de indução temos o resultado para o caso $n - 1$. Assim, podemos assumir que C não é a união de $n - 1$ dos conjuntos $C_1, C_2, \ldots, C_n$. Seja

$$C' = C_1 \cup C_2 \cup \ldots \cup C_{n-1}.$$

Então os conjuntos $C_1, C_2, \ldots, C_{n-1}$ são subconjuntos próprios de C' e C' é um subconjunto próprio de C. Da hipótese de indução, temos

$$|C_i| + |H(C_i)| \leq |C'| + |H(C')|,$$

para algum $i = 1, 2, \ldots, n-1$. Como

$$C = C' \cup C_n,$$

o Lema 1.15 implica ou

$$|C_n| + |H(C_n)| \leq |C| + |H(C)|$$

ou

$$|C'| + |H(C')| \leq |C| + |H(C)|,$$

e o resultado segue. □

Retirando a hipótese de que $C_i \neq C$, para todo $i = 1, 2, \ldots, n$, obtemos o próximo resultado.

Lema 1.17. *Sejam $C_1, C_2, \ldots, C_n$ subconjuntos finitos e não-vazios de um grupo abeliano G. Se*

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

então

$$\min\{|C_i| + |H(C_i)|/i = 1, 2, \ldots, n\} \leq |C| + |H(C)|.$$

Demonstração. Se $C_i = C$, para algum i, nada há a fazer. Caso contrário, cada conjunto C_i é um subconjunto próprio não-vazio de C e o lema anterior implica

$$|C_i| + |H(C_i)| \leq |C| + |H(C)|,$$

para algum $i = 1, 2, \ldots, n$. □

Teorema 1.18 (Kneser)**.** *Seja G um grupo abeliano e sejam A e B subconjuntos finitos e não-vazios de G. Seja*

$$H = H(A + B) = \{g \in G/g + A + B = A + B\}$$

o estabilizador de $A + B$. Se

$$|A + B| < |A| + |B|,$$

então

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

Demonstração. Seja $C = A + B$ satisfazendo a desigualdade. Seja $B = \{b_1, b_2, \ldots, b_n\}$. para cada $b_i \in B$, consideremos a coleção de todos os pares de subconjuntos finitos (A_i, B_i) de G tais que

$$A \subseteq A_i,$$

$$b_i \in B_i,$$

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

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

Esta coleção não é vazia, pois os conjuntos $A_i = A + H$ e $B_i = B + H$ satisfazem estas condições. Fixando um par (A_i, B_i) para o qual $|A_i|$ é maximal e tomando $C_i = A_i + B_i$, temos $|A_i| \leq |C_i|$ e

$$A + b_i \subseteq A_i + B_i = C_i \subseteq C.$$

Sejam $a \in A_i$ e $e = a - b_i$. Aplicando a e-transformada aos conjuntos A_i e B_i, obtemos os conjuntos

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

e

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

Então $A_i \subseteq A_i(e)$ e $b_i \in B_i(e)$. Usando as propriedades da e-transformada,

$$A_i(e) + B_i(e) \subseteq A_i + B_i \subseteq C = A + B$$

e

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

Da maximalidade de $|A_i|$, temos $A_i(e) = A_i$ e

$$a \in a + B_i - b_i \subseteq A_i,$$

para cada $a \in A_i$. Portanto,

$$A_i \subseteq A_i + B_i - b_i = C_i - b_i \subseteq A_i$$

e assim $A_i = C_i - b_i$. Então $|A_i| = |C_i|$, $H(A_i) = H(C_i - b_i) = H(C_i)$ e

$$B_i - b_i \subseteq H(A_i) = H(C_i).$$

Assim $|B_i| \leq |H(C_i)|$. Obtemos

$$|A + H| + |B + H| = |A_i| + |B_i| \leq |C_i| + |H(C_i)|$$

para todo $i = 1, 2, \ldots, n$. Como

$$\bigcup_{i=1}^{n} C_i = C = A + B,$$

pelo Lema 1.17, temos

$$\begin{aligned} |A+H| + |B+H| &\leq \min\{|C_i| + |H(C_i)|\} \\ &\leq |C| + |H(C)| \\ &= |A+B| + |H|. \end{aligned}$$

Pela Proposição 1.13(ii), cada um dos inteiros $|A+H|$, $|B+H|$ e $|A+B|$ é um múltiplo de $|H|$ e, assim, se

$$|A+H| + |B+H| < |A+B| + |H|,$$

então

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

que contradiz a hipótese inicial do teorema.

Portanto, $|A+H| + |B+H| = |A+B| + |H|$ e isto completa a demonstração deste teorema. □

Uma consequência imediata é que mesmo sem a hipótese $|A+B| < |A| + |B|$, temos

Teorema 1.19. *Seja G um grupo abeliano e sejam A e B subconjuntos finitos e não-vazios de G. Seja $H = H(A+B)$. Então*

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

Demonstração. Considerando os conjuntos $A+H$ e $B+H$, então $H((A+H)+(B+H)) = H(A+B) = H$. Portanto, ou

$$\begin{aligned} |A+B| &= |(A+H)+(B+H)| \\ &\geq |A+H| + |B+H| \\ &\geq |A+H| + |B+H| - |H|, \end{aligned}$$

ou

$$|(A+H)+(B+H)| < |A+H| + |B+H|,$$

e assim, aplicando o Teorema de Kneser (1.18) aos conjuntos $A+H$ e $B+H$, temos

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

□

Generalizando o Teorema 1.19, obtemos o próximo corolário.

Corolário 1.20. *Sejam $h \geq 2$, $A_1, A_2, \ldots, A_h$ subconjuntos finitos e não-vazios de um grupo abeliano G e $H = H(A_1 + A_2 + \ldots + A_h)$. Então*

$$|A_1 + A_2 + \ldots + A_h| \geq |A_1| + |A_2| + \ldots + |A_h| - (h-1)|H|.$$

Demonstração. Por indução sobre h. O caso $h = 2$ vem do teorema anterior. Seja $h \geq 3$ e suponhamos que o teorema valha para $h - 1$. Seja $H' = H(A_1 + A_2 + \ldots + A_{h-1})$. Verificamos facilmente que $H' \subset H$ e também que

$$\begin{aligned} |A_1 + A_2 + \ldots + A_h| &\geq |A_1 + A_2 + \ldots + A_{h-1}| + |A_h| - |H| \\ &\geq |A_1| + |A_2| + \ldots + |A_{h-1}| - (h-2)|H'| + |A_h| - |H| \\ &\geq |A_1| + |A_2| + \ldots + |A_{h-1}| + |A_h| - (h-1)|H|. \end{aligned}$$

□

Como um caso particular do Corolário 1.20, concluimos o seguinte resultado.

Corolário 1.21. *Seja G um grupo abeliano e seja A um subconjunto finito e não-vazio de G. Seja hA uma h-soma do subconjunto A, ou seja,*

$$hA = \underbrace{A + A + \ldots + A}_{h \text{ vezes}},$$

e seja

$$H_h = H(hA) = \{g \in G / g + hA = hA\}$$

o estabilizador de hA. Então

$$|hA| \geq h|A + H_h| - (h-1)|H_h|$$

para todo $h \geq 1$.

Demonstração. Pelo corolário anterior, para qualquer subconjunto finito e não-vazio de G, temos

$$|hB| \geq h|B| - (h-1)|H(hB)|$$

para todo $h \geq 2$. Seja

$$B = A + H_h.$$

Então

$$hB = h(A + H_h) = hA$$

e assim $H(hB) = H(hA) = H_h$. Portanto,

$$|hA| = |hB| \geq h|A + H_h| - (h-1)|H_h|.$$

□

No caso especial, em que G é um grupo cíclico finito cuja ordem é um número primo, o Teorema de Kneser implica facilmente o Teorema de Cauchy-Davenport, como podemos ver no corolário a seguir.

Corolário 1.22 (Cauchy-Davenport)**.** *Seja p um primo e A, B subconjuntos não-vazios de $\mathbb{Z}_p$. Então*

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

Demonstração. Como A e B são subconjuntos não vazios de $\mathbb{Z}_p$, temos que $H = H(A+B)$ é um subgrupo de $\mathbb{Z}_p$, ou seja, $H = \{\overline{0}\}$ ou $H = \mathbb{Z}_p$. Assim, se $H = \mathbb{Z}_p$, então $A+B = \mathbb{Z}_p$, ou seja, $|A + B| = p$. Por outro lado, se $H = \{\overline{0}\}$, o Teorema 1.19 (que é consequência direta do Teorema de Kneser) implica

$$|A + B| \geq |A + H| + |B + H| - |H| = |A| + |B| - 1.$$

□

Capítulo 2

Teorema de Erdös-Ginzburg-Ziv com Peso {1,-1}

O teorema de Erdös-Ginzburg-Ziv nos diz que qualquer sequência de comprimento $2n-1$ de números inteiros possui uma subsequência de comprimento n cuja soma dos seus termos é congruente a zero módulo n.

Como complemento deste teorema, observamos que a sequência

$$(\overbrace{0,\ldots,0}^{n-1},\overbrace{1,\ldots,1}^{n-1})$$

possui comprimento $2n-2$ e não possui nenhuma subsequência cuja soma seja um múltiplo de n.

Desta forma, podemos definir o invariante $E(n)$ como sendo o menor inteiro t tal que qualquer sequência de t números inteiros contém n inteiros que somados geram um múltiplo de n. Assim, podemos concluir que

$$E(n) = 2n - 1.$$

Neste capítulo, consideramos uma generalização para o teorema de Erdös-Ginzburg-Ziv no seguinte sentido:

Seja n um inteiro positivo. Identificaremos $\mathbb{Z}/n\mathbb{Z}$ com o conjunto dos números inteiros $\{0, 1, \ldots, n-1\}$. Considerando o conjunto $\emptyset \neq A \subseteq \mathbb{Z}/n\mathbb{Z}$, podemos definir o invariante $E_A(n)$ como sendo o menor $t \in \mathbb{N}$ tal que para todas as sequências $(x_1, \ldots, x_t) \in \mathbb{Z}^t$ existem n índices $j_1, \ldots, j_n \in \mathbb{N}$, com $1 \leq j_1 < \ldots < j_n \leq t$ e existem $\xi_1, \ldots, \xi_n \in A$ tais que

$$\sum_{i=1}^{n} \xi_i x_{j_i} \equiv 0 \, (mod\ n).$$

Chamaremos os elementos do conjunto A de *pesos* das somas, pois eles serão usados para fazer as *somas ponderadas* (do mesmo conceito de *média ponderada*) dos elementos das sequências. Para evitar casos triviais, sempre vamos assumir que A não contém o 0 e é não vazio.

É fácil ver que $E_{\{1\}}(n) = E(n)$ e, assim,

$$E_A(n) \leq E(n) = 2n - 1,$$

pois se uma sequência tem ao menos $2n-1$ elementos, então existem n deles que somados geram o *zero*, logo, como $A \neq \emptyset$, basta tomar todos os pesos iguais a um elemento de A. Colocando estes pesos em evidência, chegamos novamente ao *zero*.

Além disso, se considerarmos a sequência $(\overbrace{0, \ldots, 0}^{n-1}, 1)$ que tem comprimento igual a n e claramente não possui soma ponderada, com pesos em A, igual a um múltiplo de n, deduzimos

$$E_A(n) \geq n + 1.$$

2.1 Limite Inferior para $E_A(n)$, quando $A = \{1, -1\}$

Aqui, consideraremos o caso em que $A = \{1, n-1\} = \{1, -1\} \subseteq \mathbb{Z}_n$ e denotaremos o invariante E_A por $E_\pm$ neste caso.

Afirmamos que

$$E_\pm(n) \geq n + \lfloor \log n \rfloor,$$

onde aqui e em todo o nosso estudo *log* vai significar a logaritmo na base 2 e $\lfloor \cdot \rfloor$ vai significar o "maior inteiro menor que".

De fato, sendo $r \in \mathbb{N}$, tal que $2^{(r+1)} \leq n < 2^{(r+2)}$ consideremos a sequência de números inteiros

$$(\overbrace{0, 0, \ldots, 0}^{n-1 \text{ vezes}}, 1, 2, \ldots, 2^r).$$

Podemos observar claramente a desigualdade

$$1 + 2 + \ldots + 2^r = 2^{(r+1)} - 1 < n$$

e, por consequência,

$$-1 - 2 - \ldots - 2^r = -2^{(r+1)} + 1 > -n.$$

Assim, obtemos que a soma com qualquer combinação de sinais de n inteiros desta sequência dá origem a uma série cujo valor absoluto é menor que n.

Esta soma também não tem como resultado o *zero*. De fato, considere $j_i \in \{0, 1, \ldots, r\}$, $\alpha_i \in \{0, 1\}$, onde $i = 1, 2, \ldots, k$ e $k \leq n$, de modo que $j_1 < j_2 < \ldots < j_k$ e

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

Logo, dividindo os dois lados por $(-1)^{\alpha_1} 2^{j_1}$, temos

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

Isto é um absurdo, pois de um lado da igualdade temos um número ímpar e do outro, um número par.

Além disso, a sequência dada como exemplo possui um total de $n + r = n + \lfloor \log n \rfloor - 1$ elementos e não possui uma subsequência com n elementos cuja soma, com peso em $\{1, -1\}$, seja igual a um múltiplo de n. Portanto, o número $n + \lfloor \log n \rfloor - 1$ é um limitante inferior para os valores de $E_{\pm}(n)$.

2.2 Limite Superior para $E_A(n)$, quando $A = \{1, -1\}$

O objetivo deste capítulo é demonstrar o Teorema 2.1, enunciado abaixo, notando que, pela seção anterior, $n + \lfloor log\ n \rfloor$ é um limite inferior para $E_{\pm}(n)$.

Teorema 2.1. *Para qualquer inteiro positivo n, temos*

$$E_{\pm}(n) = n + \lfloor log\ n \rfloor.$$

Vamos provar este teorema. Na Subseção 2.2.1, provaremos o caso em que n é par e nas Subseções 2.2.3 e 2.2.4, o caso em que n é ímpar. Na Subseção 2.2.2 apresentamos alguns resultados que implicam o Teorema 2.1 para o caso primo ímpar, que, embora não sejam realmente necessários devido aos outros resultados apresentados, são interessantes por si só, uma vez que este argumento usa a *Desigualdade de Cauchy-Davenport* definida no primeiro capítulo.

2.2.1 O Caso em que n é Par

Antes de enunciarmos o principal resultado desta seção, vamos mostrar o seguinte lema:

Lema 2.2. *Seja $n \in \mathbb{N}$ e $(x_1, x_2, \ldots, x_s)$ uma sequência de inteiros com $s > (\log n) + 1$. Então existem um suconjunto $J \subseteq [s]$ não-vazio com $|J|$ par e coeficientes $\xi_j \in \{1, -1\}$, para cada $j \in J$, tais que*

$$\sum_{j \in J} \xi_j x_j \equiv 0\, (mod\ n).$$

Observação: Aqui e em todo o nosso estudo, se n é um número natural não nulo, definimos $[n] = \{1, 2, \ldots, n\}$.

Demonstração. Considere todas as somas de subsequências da forma

$$\left(\sum_{j\in I} x_j\right)_{I\subseteq[s]},$$

onde $|I|$ é par.

Sabemos que existem 2^{s-1} subconjuntos I de $[s]$, tais que $|I|$ é par. Assim, podemos escolher $J_1, J_2 \subseteq [s]$ não-vazios tais que $|J_1|$ e $|J_2|$ são pares e $J_1 \neq J_2$ e

$$\sum_{j\in J_1} x_j \equiv \sum_{j\in J_2} x_j \,(mod\ n).$$

Estes conjuntos existem pois, por hipótese, $s > (\log n) + 1$ e daí temos $2^{s-1} > n$, ou seja, o número de somas ultrapassa o valor de n.

Daí obtemos

$$\sum_{j\in J_1} x_j \equiv \sum_{j\in J_2} x_j \,(mod\ n) \Rightarrow$$

$$\sum_{j\in J_1} x_j - \sum_{j\in J_2} x_j \equiv 0 \,(mod\ n) \Rightarrow$$

$$\sum_{j\in J_1} x_j + \sum_{j\in J_2} -x_j \equiv 0 \,(mod\ n)$$

Tomando $J = (J_1 \cup J_2) \setminus (J_1 \cap J_2)$, temos $J \neq \emptyset$ (pois $J_1 \neq J_2$) e, considerando

$$\begin{cases} \xi_j = \quad 1 & \text{, se } \ j \in J_1 \\ \xi_j = -1 & \text{, se } \ j \in J_2 \end{cases},$$

temos

$$\sum_{j\in J} \xi_j x_j \equiv 0 \,(mod\ n).$$

Além disso, é fácil ver que $|J| = |J_1| + |J_2| - 2.|J_1 \cap J_2|$ e como $|J_1|$ e $|J_2|$ são pares, então $|J|$ é par.

□

Este lema nem sempre é válido para o caso em que $|J|$ é ímpar. Como exemplo podemos considerar $n = 5$, $s = 4 > (\log 5) + 1$ e a sequência $(1, 1, 1, 1)$ que facilmente verificamos

não possuir subsequência de tamanho ímpar que possua soma, com peso $\{1, -1\}$, igual a um múltiplo de 5. Portanto, para este caso, precisamos proceder de forma diferente.

Agora, vamos enunciar o resultado que demonstra o Teorema 2.1 para o caso em que n é par.

Teorema 2.3. *Seja $n \in \mathbb{N}$ um número par. Considere o número inteiro $N = n + \lfloor \log n \rfloor$. Dada qualquer sequência $(x_1, x_2, \ldots, x_N) \in \mathbb{Z}^N$ existem n índices $\{j_1, j_2, \ldots, j_n\} \subseteq [N]$ e sinais $\xi_1, \xi_2, \ldots, \xi_n \in \{1, -1\}$ tais que*

$$\xi_1 x_{j_1} + \xi_2 x_{j_2} + \ldots + \xi_n x_{j_n} \equiv 0 \, (mod \ n).$$

Demonstração. Vamos reordenar a sequência de tal maneira que:

$$x_1 \equiv x_2 \, (mod \ n), \quad x_3 \equiv x_4 \, (mod \ n), \quad x_5 \equiv x_6 \, (mod \ n), \quad \ldots \quad , \quad x_{2t-1} \equiv x_{2t} \, (mod \ n)$$

e $x_{2t+1}, \ldots, x_N$ sejam todos distintos módulo n.

Com isso, temos $N - 2t \leq n$, pois, caso contrário, existiriam ao menos dois elementos no conjunto $\{x_{2t+1}, \ldots, x_N\}$ que seriam iguais módulo n. Além disso, como $N = n + \lfloor \log n \rfloor$, por hipótese, temos também $2t \geq N - n = \lfloor \log n \rfloor$.

Seja $B = \{r_1, \ldots, r_l\} \subseteq \{2t + 1, 2t + 2, \ldots, N\}$, com $l = |B|$ par, o conjunto maximal que satisfaz à propriedade de que existem $\xi_1, \xi_2, \ldots, \xi_l \in \{1, -1\}$ com

$$\sum_{j=1}^{l} \xi_j x_{r_j} \equiv 0 \, (mod \ n).$$

Observe que mesmo se $B = \emptyset$, a demonstração ainda segue o mesmo raciocínio. Agora, afirmamos que $l + 2t \geq n$. Para mostrar esta afirmação, vamos supor, por contradição, que ela seja falsa, ou seja, $l + 2t < n$.

Como l e n são pares então

$$l + 2t < n \quad \Rightarrow \quad l + 2t \leq n - 2.$$

Consideremos o conjunto

$$C = \{2t + 1, \ldots, N\} \setminus \{r_1, \ldots, r_l\}.$$

Observamos facilmente o seguinte:

$$\begin{aligned} |C| &= N - 2t - l \\ &= N - (2t + l) \\ &= (n + \lfloor \log n \rfloor) - (2t + l) \\ &\geq (n + \lfloor \log n \rfloor) - (n - 2) \\ &= \lfloor \log n \rfloor + 2 \end{aligned}$$

Assim, pelo Lema 2.2, existem um conjunto não-vazio $B' \subseteq C$, com $|B'|$ par, e $\xi_j \in \{1, -1\}$, para cada $j \in B'$, de tal forma que

$$\sum_{j \in B'} \xi_j x_j \equiv 0 \, (mod \ n).$$

Portando, o conjunto $B \cup B'$ verifica a propriedade acima, pois $|B|$,$|B'|$ e $|B \cup B'| = |B| + |B'|$ são pares. Além disso, $B \subsetneq B \cup B'$ contrariando a maximalidade de B.

Assim, mostramos que $l + 2t \geq n$.

Agora, podemos escrever $l + 2t = n + d$, para algum $d \in \mathbb{N}$. Claramente d é par, pois l e n também o são. Se $d = 2d'$ então escolhemos a sequência

$$(x_{2d'+1}, x_{2d'+2}, \ldots, x_{2t-1}, x_{2t}, x_{r_1}, \ldots, x_{r_l})$$

que tem $l + 2t - 2d' = l + 2t - d = n$ elementos e

$$\sum_{j=d'+1}^{t} (x_{2j} - x_{2j-1}) + \sum_{j=1}^{l} \xi_j x_j \equiv 0 \, (mod \ n).$$

□

2.2.2 Um Resultado Condicional

Apresentaremos agora alguns resultados interessantes que estabelecem o Teorema 2.1 sob algumas condições.

O próximo lema é semelhante ao Lema 2.2 e será usado nesta subseção e também na Subseção 2.2.4.

Lema 2.4. *Sejam $n \in \mathbb{N}$ e $(x_1, x_2, \ldots, x_s)$ uma sequência de números inteiros com $s > \log n$. Então existe um conjunto $J \subseteq [s]$ não-vazio e $\xi_j \in \{1, -1\}$, para cada $j \in J$, tais*

que

$$\sum_{j\in J} \xi_j x_j \equiv 0\,(mod\ n).$$

Demonstração. Considere todas as sequências da forma

$$\left(\sum_{j\in I} x_j\right)_{I\subseteq[s]}.$$

Sabemos que existem 2^s subconjuntos I de $[s]$.

Por hipótese, $s > \log n$. Assim, temos $2^s > n$, ou seja, o número de somas ultrapassa o valor de n. Assim, podemos escolher $J_1, J_2 \subseteq [s]$ não-vazios tais que $J_1 \neq J_2$ e

$$\sum_{j\in J_1} x_j \equiv \sum_{j\in J_2} x_j\,(mod\ n).$$

Daí obtemos,

$$\sum_{j\in J_1} x_j \equiv \sum_{j\in J_2} x_j\,(mod\ n) \Rightarrow$$

$$\sum_{j\in J_1} x_j - \sum_{j\in J_2} x_j \equiv 0\,(mod\ n) \Rightarrow$$

$$\sum_{j\in J_1} x_j + \sum_{j\in J_2} -x_j \equiv 0\,(mod\ n)$$

Tomando $J = (J_1 \cup J_2) \setminus (J_1 \cap J_2)$, temos $J \neq \emptyset$, pois $J_1 \neq J_2$ e considerando

$$\begin{cases} \xi_j = \quad 1 & \text{, se } \ j \in J_1 \\ \xi_j = -1 & \text{, se } \ j \in J_2 \end{cases},$$

temos

$$\sum_{j\in J} \xi_j x_j \equiv 0\,(mod\ n).$$

□

Observação: Definimos por $D_A(n)$ o menor inteiro t tal que, dada uma sequência S de t inteiros, S possui uma subsequência de soma-zero com pesos no conjunto A. O Lema 2.4 nos mostra que toda sequência com comprimento maior que $\log n$ possui uma subsequência de soma-zero com pesos em $A = \{1, -1\}$, ou seja,

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

Agora vamos exibir uma sequência que fornece um limitante inferior para $D_{\pm}(n)$.

De fato, sendo r definido por $2^{(r+1)} \leq n < 2^{(r+2)}$, consideremos a sequência de números inteiros

$$(1, 2, 2^2, \ldots, 2^r).$$

Podemos observar claramente a desigualdade

$$1 + 2 + \ldots + 2^r = 2^{(r+1)} - 1 < n$$

e, por consequência,

$$-1 - 2 - \ldots - 2^r = -2^{(r+1)} + 1 > -n.$$

Assim, obtemos que a soma com qualquer combinação com sinais de n inteiros desta sequência dá origem a uma série cujo valor absoluto é menor que n.

Esta soma também não tem como resultado o *zero*, pois considerando $j_i \in \{0, 1, 2, \ldots, r\}$ e $\alpha_i \in \{0, 1\}$, onde $i = 1, 2, \ldots, k$ e $k \leq n$ de modo que $j_1 < j_2 < \ldots < j_k$ e

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

então, dividindo os dois lados por $(-1)^{\alpha_1} 2^{j_1}$, temos

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

Isto é um absurdo, pois de um lado da igualdade temos um número ímpar e do outro, um número par. Além disso, a sequência dada como exemplo possui um total de $r+1 = \lfloor \log n \rfloor$ elementos e não possui uma subsequência cuja soma, com peso em $A = \{1, -1\}$, seja igual a um múltiplo de n. Portanto, o número $\lfloor \log n \rfloor + 1$ é um limitante inferior para os valores de $D_{\pm}(n)$, ou seja, $D_{\pm}(n) \geq \lfloor \log n \rfloor + 1$. Por tudo isso, concluímos a igualdade $D_{\pm}(n) = \lfloor \log n \rfloor + 1$.

Um dos principais resultados do artigo *"A Weighted Generalization of Two Theorems of Gao"* [24] é:

$$E_A(G) = |G| + D_A(G) - 1,$$

para qualquer grupo G finito e abeliano. Vamos usar este resultado para provar o Teorema 2.1. Consideremos C_n um grupo cíclico de ordem n. Como procuramos sequências de inteiros cujas somas sejam múltiplos de um número natural n, podemos trabalhar em C_n ao invés de $\mathbb{Z}$, sem nenhum prejuízo. Portanto, $E_A(C_n) = E_A(n)$ e $D_A(C_n) = D_A(n)$ e, considerando $A = \{1, -1\}$, temos ainda

$$E_{\pm}(n) = E_{\pm}(C_n) = |C_n| + D_{\pm}(C_n) - 1 = n + (\lfloor \log n \rfloor + 1) - 1 = n + \lfloor \log n \rfloor,$$

demonstrando o Teorema 2.1.

É claro que a dificuldade, aqui, está em provar a identidade $E_A(G) = |G| + D_A(G) - 1$.

Vamos, agora, lidar com as sequências em que um ou mais elementos estão na classe *zero*. O próximo resultado analisa este problema e sua demonstração segue o mesmo raciocínio do Teorema 2.3.

Teorema 2.5. *Sejam $n \in \mathbb{N}$ e o número inteiro $N \geq n + \lfloor \log n \rfloor$. Dada qualquer sequência $(x_1, x_2, \ldots, x_N) \in \mathbb{Z}^N$ com pelo menos um múltiplo de n, então existem $m = N - \lfloor \log n \rfloor$ índices $j_1, j_2, \ldots, j_m \in [N]$ e sinais $\xi_1, \xi_2, \ldots, \xi_m \in \{1, -1\}$ tais que*

$$\sum_{i=1}^{m} \xi_i x_{j_i} \equiv 0 \, (mod \ n).$$

Demonstração. Vamos reordenar a sequência de tal maneira que:

$$x_1 \equiv 0 \, (mod \ n), \quad x_2 \equiv x_3 \, (mod \ n), \quad x_4 \equiv x_5 \, (mod \ n), \quad \ldots \quad , \quad x_{2t} \equiv x_{(2t+1)} \, (mod \ n)$$

e $x_{(2t+2)}, \ldots, x_N$ são todos distintos módulo n. Com isso, temos $N - 2t - 1 \leq n$, pois, caso contrário, existiriam ao menos dois elementos no conjunto $\{x_{(2t+2)}, \ldots, x_N\}$ que seriam iguais módulo n. Além disso, como $N \geq n + \lfloor \log n \rfloor$, por hipótese, temos também $2t + 1 \geq N - n \geq \lfloor \log n \rfloor$.

Seja $B = \{r_1, r_2, \ldots, r_l\} \subseteq \{2t + 2, 2t + 3, \ldots, N\}$ o conjunto maximal que satisfaz à propriedade de que existem $\xi_1, \xi_2, \ldots, \xi_l \in \{1, -1\}$ com

$$\sum_{j=1}^{l} \xi_j x_{r_j} \equiv 0 \, (mod \ n).$$

Observe que, mesmo se $B = \emptyset$, a demonstração ainda segue o mesmo raciocínio. Agora, afirmamos que $l + 2t + 1 \geq m$. Para mostrar esta afirmação, vamos supor, por contradição, que ela seja falsa, ou seja, $l + 2t + 1 < m$.

Consideremos o conjunto

$$C = \{2t + 2, \ldots, N\} \setminus \{r_1, r_2, \ldots, r_l\}.$$

Observamos facilmente o seguinte:

$$\begin{aligned} |C| &= N - 2t - 1 - l \\ &= N - (2t + 1 + l) \\ &> N - m \\ &= N - (N - \lfloor \log n \rfloor) \\ &= \lfloor \log n \rfloor. \end{aligned}$$

Assim, pelo Lema 2.4, existe um conjunto não-vazio $B' \subseteq C$ e $\xi_j \in \{1, -1\}$, para cada

$j \in B'$, de tal forma que

$$\sum_{j \in B'} \xi_j x_j \equiv 0 \, (mod \ n).$$

Portando, o conjunto $B \cup B'$ verifica a propriedade acima e, além disso, $B \subsetneqq B \cup B'$ contrariando a maximalidade de B. Assim, mostramos a desigualdade $l + 2t + 1 \geq m$.

Agora, podemos escrever $l + 2t + 1 = m + d$, para algum $d \in \mathbb{N}$, e separamos em dois casos:

Se $d = 2d'$ então escolhemos a sequência

$$(x_1, x_{2d'+2}, x_{2d'+3}, \ldots, x_{2t}, x_{2t+1}, x_{r_1}, \ldots, x_{r_l})$$

que tem $l + (2t + 1) - (2d' + 1) + 1 = l + 2t + 1 - d = m$ elementos e

$$x_1 + \sum_{j=d'+1}^{t} (x_{2j} - x_{2j+1}) + \sum_{j=1}^{l} \xi_j x_j \equiv 0 \, (mod \ n).$$

Se $d = 2d' + 1$ é ímpar, então retiramos x_1 e consideramos a sequência

$$(x_{2d'+1)}, x_{2d'+3}, \ldots, x_{2t}, x_{2t+1}, x_{r_1}, \ldots, x_{r_l})$$

que tem m elementos e também verifica a tese. □

Agora, vamos enunciar e demonstrar alguns resultados que, junto com o Teorema 2.5, prova o Teorema 2.1 para o caso em que n é primo e ímpar.

A Desigualdade de Cauchy-Davenport (Teorema 1.9) citada no Capítulo 1 no diz que dados A e B dois subconjuntos não vazios de $\mathbb{Z}/p\mathbb{Z}$. Então

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

onde $A + B = \{x \in \mathbb{Z}/p\mathbb{Z} \ ; \ x \equiv a + b (mod \ p), a \in A, b \in B\}$ e $|K|$ denota a cardinalidade do subconjunto K de $\mathbb{Z}/p\mathbb{Z}$.

Esta desigualdade foi provada primeiramente por Cauchy em 1813 (não publicado) e depois redescoberta por Davenport [12] em 1947.

Por iteração da Desigualdade de Cauchy-Davenport, obtemos o Corolário 1.10 demonstrado no Capítulo 1, que afirma que, dados $n \geq 2$, p um primo e A_1, A_2, ... , A_n subconjuntos não-vazios de $\mathbb{Z}_p$. Então

$$|A_1 + A_2 + \ldots + A_n| \geq \min\{p, \sum_{i=1}^{n} |A_i| - n + 1\}.$$

Como consequência direta desta desigualdade, obtemos o próximo resultado.

Lema 2.6. *Seja p um primo ímpar. Se $N \geq p-1$ é um inteiro e $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ é uma sequência qualquer de interos não divisíveis por p, então, para cada $b \in \mathbb{Z}$, existem sinais $\xi_1, \ldots, \xi_N \in \{1, -1\}$ tais que*

$$\xi_1 x_1 + \ldots + \xi_N x_N \equiv b (mod\ p).$$

Demonstração. Escolhendo $A_i = \{x_i, -x_i\} \subseteq \mathbb{Z}_p$ (lembrando que estamos identificando o inteiro x_i com sua classe em $\mathbb{Z}_p$), para todo $i \in \{1, 2, \ldots, N\}$, e usando o Corolário 1.10, temos

$$|A_1 + A_2 + \ldots + A_N| \geq \min \left\{ p, \sum_{i=1}^{N} |A_i| - N + 1 \right\} = \min\{p, N+1\} = p,$$

ou seja,

$$|\{x_1, -x_1\} + \{x_2, -x_2\} + \ldots + \{x_N, -x_N\}| \geq p,$$

o que implica imediatamente $\sum_{i=1}^{N} A_i = \mathbb{Z}_p$, concluindo a demonstração deste lema. □

As afirmações do Teorema 2.5 e do Lema 2.6 implicam o resultado do Teorema 2.1 quando $n = p$ é um primo ímpar, sendo a primeira afirmação relacionada ao caso em que nenhum dos elementos da sequência é *zero* módulo p e a segunda afirmação relacionada ao caso em que a sequência contém pelo menos um elemento que é *zero* módulo p.

2.2.3 Sequências Completas de Inteiros

Não temos conhecimento se a definição a seguir já apareceu anteriormente na literatura. No entanto, no contexto do artigo [1], nos parece natural.

Definição 2.7. *Seja a sequência $\underline{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$. Dizemos que a sequência $\underline{x}$ é completa com respeito a um inteiro positivo m se, para cada positivo $d|m$, temos*

$$|\{j \in [N] | x_j \not\equiv 0 (mod\ d)\}| \geq d - 1.$$

Uma sequência completa de inteiros com respeito a um primo p é uma sequência que contém $p-1$ elementos não divisíveis por p.

Vamos enunciar algumas propriedades de sequências completas:

Lema 2.8. *Se $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ é completa com respeito a m e $N \geq m$ então existe $j_0 \in \mathbb{N}$, $1 \leq j_0 \leq N$, tal que $(x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_N) \in \mathbb{Z}^{N-1}$ é completa com respeito a m.*

Demonstração. Sejam d_1, d_2, ..., d_s os divisores positivos de m que satisfazem

$$|\{j \in [N] | x_j \not\equiv 0 (mod\ d_i)\}| = d_i - 1.$$

Vamos assumir $m \geq d_1 > d_2 > \ldots > d_s$, também que $D_k = mmc(d_1, d_2, \ldots, d_k)$ e o conjunto $U_k = \{j \in [N] | x_j \not\equiv 0 (mod\ d_k)\}$.

Vamos mostrar que $|U_1 \cup U_2 \cup \ldots \cup U_s| < m$ e que podemos escolher $j_0 \in [N] \setminus U_1 \cup U_2 \cup \ldots \cup U_s$ tal que a sequência $(x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_N)$ ainda é completa.

Notemos a igualdade

$$U_1 \cup U_2 \cup \ldots \cup U_k = \{j \in [N] | x_j \not\equiv 0 (mod\ D_k)\}.$$

Para justificar a afirmação acima observemos que, dado $j \in U_1 \cup U_2 \cup \ldots \cup U_k$, se $x_j \equiv 0 (mod\ D_k)$, como $D_k = mmc(d_1, d_2, \ldots, d_k)$, então $x_j \equiv 0 (mod\ d_i)$, para todo $i = 1, 2, \ldots, k$, contradizendo a hipótese de $j \in U_1 \cup U_2 \cup \ldots \cup U_k$. Portanto, $U_1 \cup U_2 \cup \ldots \cup U_k \subseteq \{j \in [N] | x_j \not\equiv 0 (mod\ D_k)\}$.

Por outro lado, seja $j \in \{j \in [N] | x_j \not\equiv 0 (mod\ D_k)\}$. Se tivermos $x_j \equiv 0 (mod\ d_i)$, para todo $i = 1, 2, \ldots, k$, então, como $D_k = mmc(d_1, d_2, \ldots, d_k)$, temos $x_j \equiv 0 (mod\ D_k)$, contrariando a hipótese de $j \in \{j \in [N] | x_j \not\equiv 0 (mod\ D_k)\}$. Portanto, existe $i \in \{1, 2, \ldots, k\}$ tal que $x_j \not\equiv 0 (mod\ d_i)$, ou seja, $j \in U_i \subseteq U_1 \cup U_2 \cup \ldots \cup U_k$. Assim, concluímos a inclusão $\{j \in [N] | x_j \not\equiv 0 (mod\ D_k)\} \subseteq U_1 \cup U_2 \cup \ldots \cup U_k$.

Se $D_k = D_{k-1}$, então $U_1 \cup U_2 \cup \ldots \cup U_k = U_1 \cup U_2 \cup \ldots \cup U_{k-1}$. Assim

$$U_1 \cup U_2 \cup \ldots \cup U_s = U_1 \cup \bigcup_{D_k > D_{k-1}} U_k.$$

Agora, para k participando da fórmula acima, temos $D_k > D_{k-1}$ e $D_k = mmc(D_{k-1}, d_k) \geq 2D_{k-1}$, pois $D_{k-1} | D_k$.

Para $k > 1$, temos $D_k - D_{k-1} \geq D_k - 1 \geq d_{k-1} > d_k - 1$, pois $D_k \geq 2D_{k-1}$.

Como $D_1 = d_1 > d_1 - 1$, deduzimos o seguinte:

$$\begin{aligned}
|U_1 \cup U_2 \cup \ldots \cup U_s| &\leq |U_1| + \sum_{D_k > D_{k-1}} |U_k| \\
&= d_1 - 1 + \sum_{D_k > D_{k-1}} |U_k| \\
&< D_1 + \sum_{D_k > D_{k-1}} (D_k - D_{k-1}) \\
&= D_1 + \sum_{k=2}^{s} (D_k - D_{k-1}) \\
&= D_s \\
&\leq m
\end{aligned}$$

Como $|U_1 \cup U_2 \cup \ldots \cup U_s| < m$, então basta escolher um índice

$$j_0 \in [N] \setminus (U_1 \cup U_2 \cup \ldots \cup U_s).$$

□

Lema 2.9. *Se $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ é completa com respeito a m e $N \geq m$, então existem índices $\{j_1, j_2, \ldots, j_{m-1}\} \subseteq [N]$ tais que a sequência $(x_{j_1}, x_{j_2}, \ldots, x_{j_{m-1}}) \in \mathbb{Z}^{m-1}$ é completa com respeito a m.*

Demonstração. Da definição de sequência completa temos $N \geq m-1$, pois devem existir ao menos $m-1$ elementos que não são congruentes a *zero* módulo m. Tomando $r = N - (m-1)$, basta aplicar o Lema 2.8 r vezes para obtermos uma sequência com $m-1$ elementos que continua completa com respeito a m. □

Como consequência destes lemas obtemos o próximo teorema.

Teorema 2.10. *Se $(x_1, \ldots, x_N) \in \mathbb{Z}^N$ é completa com respeito a m, então para cada $b \in \mathbb{Z}$ existe uma escolha de coeficientes $\xi_1, \xi_2, \ldots, \xi_N \in \{0, 1\}$ tal que*

$$\sum_{j=1}^{N} \xi_j x_j \equiv b (mod\ m).$$

Demonstração. Vamos proceder por indução sobre m.

Para $m = 1$, para quaisquer que sejam os valores ξ_j, x_j e b, temos,

$$\sum_{j=1}^{N} \xi_j x_j \equiv b (mod\ 1).$$

Agora, dado $k \geq 2$, suponha o teorema válido para $m < k$, ou seja, existem $\xi_j \in \{0, 1\}$ tais que

$$\sum_{j=1}^{N} \xi_j x_j \equiv b(mod\ m).$$

para quaisquer $b \in \mathbb{Z}$ e $m < k$.

Suponhamos que a sequência $(x_1, x_2, \ldots, x_N)$ seja completa com respeito a k. Sem perda de generalidade, vamos assumir $k \nmid x_1$. Para qualquer $a \in \mathbb{Z}$, tomemos $\bar{a}$ como a classe de a módulo k e dado um conjunto A de inteiros, consideremos $\overline{A} = \{\bar{a}\ ;\ a \in A\}$.

Seja $A_1 = \{0, x_1\}$ e $i_1 = 1$. Então $|\overline{A}_1| = 2$.

Agora, se possível, vamos escolher $i_2 \neq i_1$ tal que $\overline{A}_1 + \{0, \bar{x}_{i_2}\} \neq \overline{A}_1$. Se existe tal i_2, tomemos $A_2 = A_1 + \{0, x_{i_2}\}$. Então existe um inteiro positivo t tal que este procedimento para em A_t. Notemos que

$$A_1 \subset A_2 \subset \ldots \subset A_t$$

e que $|\overline{A}_t| \geq |\overline{A}_{t-1}| + 1 \geq \ldots \geq t + 1$.

Para completar nossa demonstração é suficiente mostrar que $|\overline{A}_t| \geq k$, pois neste caso, é fácil ver que $\overline{A}_t = \mathbb{Z}_k$ e assim, para todo $b \in \mathbb{Z}$, existe $x \in A_t$ tal que $\bar{x} = \bar{b}$, ou seja, $x \equiv b(mod\ k)$. Como $x \in A_t$, então

$$x = \xi_1 x_{i_1} + \xi_2 x_{i_2} + \ldots + \xi_t x_{i_t},$$

onde $\xi_j \in \{0, 1\}$ para $j \in \{i_1, i_2, \ldots, i_t\}$. Assim, tomando $\xi_j = 0$, para $j \in [N] \setminus \{i_1, i_2, \ldots, i_t\}$, podemos concluir a congruência

$$\sum_{j=1}^{N} \xi_j x_j \equiv b(mod\ k).$$

Como $k = |\mathbb{Z}_k| \geq |\overline{A}_t| \geq |\overline{A}_{t-1}| + 1 \geq |\overline{A}_{t-2}| + 2 \geq \ldots \geq |\overline{A}_1| + t - 1 = t + 1$, então $t \leq k - 2$.

Sem perda de generalidade, tomemos $i_j = j$ para $j \in \{1, 2, \ldots, t\}$. Como $|\{j \in [N]/x_j \not\equiv 0(mod\ k)\}| \geq k - 1$, temos $N \geq k - 1 > k - 2 \geq t$. Além disso, rearranjando (se necessário) os elementos restantes, podemos assumir $k \nmid x_{t+1}$, pois $t < k - 1$, logo existe tal x_{t+1}.

Agora, para todo $j \in \mathbb{N}$ tal que $t + 1 \leq j \leq N$ temos $\overline{A}_t + \{0, \bar{x}_j\} = \overline{A}_t$. Seja H o subgrupo de $\mathbb{Z}_k$ gerado por $\bar{x}_{t+1}$. Temos $\overline{A}_t + H = \overline{A}_t$. Assim, $\overline{A}_t$ é a união de alguns subconjuntos de H. Logo

$$\overline{A}_t = \bigcup_{i=1}^{s} (b_i + H),$$

onde $b_i - b_j \notin H$, para todos $i \neq j$. Então $|\overline{A}_t| = s|H|$.

Seja $k_1 = mdc(x_{t+1}, k)$. Como $k \nmid x_{t+1}$, temos $k_1 < k$ e a sequência $(x_1, x_2, \ldots, x_N)$ é completa com respeito a k_1. Pela hipótese de indução, para cada $b \in \mathbb{Z}$, existem $\xi_i \in \{0, 1\}$ tais que

$$\sum_{i=1}^{N} \xi_i x_i \equiv b(mod\ k_1).$$

Além disso, observamos a igualdade

$$\left\{ \sum_{i=1}^{N} \xi_i x_i (mod\ k_1) / \xi_j = 0, 1\ ;\ j = 1, 2, \ldots, N \right\} = \overline{A}_t.$$

Assim, como $k_1 \mid k$, $k_1 \mid x_{t+1}$, temos

$$\left\{ \sum_{i=1}^{N} \xi_i x_i (mod\ k_1) / \xi_j = 0, 1 \right\} = \{b_1(mod\ k_1), b_2(mod\ k_1), \ldots, b_s(mod\ k_1)\}.$$

O primeiro tem k_1 elementos, pois existem $\xi_i \in \{0, 1\}$ tais que $\sum_{i=1}^{N} \xi_i x_i \equiv b(mod\ k_1)$, para todo $b \in \mathbb{Z}$. O segundo tem k_1 elementos, pois cada b_j, $j = 1, 2, \ldots, s$ é representante uma classe diferente de $\mathbb{Z}_k/H$. Assim $k_1 \leq s$.

Temos $|H| \cdot x_{t+1} \equiv 0(mod\ k)$ e $< x_{t+1} >= H \leq \mathbb{Z}_k$. Logo, como $k_1 = mdc(k, x_{t+1})$, então

$$|H| \equiv 0 \left(mod\ \frac{k}{k_1} \right).$$

Como $|H| \geq 1$, temos $|H| \geq \dfrac{k}{k_1}$. Portanto, $|\overline{A}_t| = s.|H| \geq k_1|H| \geq k_1.\dfrac{k}{k_1} = k.$ □

Corolário 2.11. *Sejam $m \in \mathbb{N}$ ímpar e a sequência $(x_1, x_2, \ldots, x_N) \in \mathbb{Z}^N$ completa com respeito a m. Então, para cada $b \in \mathbb{Z}$, existe uma escolha de coeficientes $\xi_1, \xi_2, \ldots, \xi_N \in \{1, -1\}$ tais que*

$$\sum_{j=1}^{N} \xi_j x_j \equiv b(mod\ m).$$

Demonstração. Dado $b \in \mathbb{Z}$, consideremos $C = b + x_1 + x_2 + \ldots + x_N$. Como m é ímpar, então existe $r \in \mathbb{Z}$ tal que $m = 2r - 1$. Assim, temos

$$\begin{aligned} 1 &\equiv 2r(mod\ m) \\ C &\equiv 2rC(mod\ m) \end{aligned}$$

Aplicando o Teorema 2.10 para o número inteiro rC, existem α_1, α_2, ..., $\alpha_N \in \{0, 1\}$

tais que

$$\begin{aligned} rC &\equiv \sum_{j=1}^{N} \alpha_j x_j (mod\ m) \Rightarrow \\ 2rC &\equiv 2\sum_{j=1}^{N} \alpha_j x_j (mod\ m) \Rightarrow \\ C &\equiv 2\sum_{j=1}^{N} \alpha_j x_j (mod\ m) \Rightarrow \\ b + x_1 + x_2 + \ldots + x_N &\equiv 2\sum_{j=1}^{N} \alpha_j x_j (mod\ m) \Rightarrow \\ b &\equiv \sum_{j=1}^{N} (2\alpha_j - 1) x_j (mod\ m). \end{aligned}$$

Tomando $\xi_j = 2\alpha_j - 1$, então temos

$$b \equiv \sum_{j=1}^{N} \xi_j x_j (mod\ m),$$

onde $\xi_j \in \{1, -1\}$ para $j = 1, 2, \ldots, N$. □

Este corolário nem sempre é válido para o caso em que m é par. De fato, basta tomarmos $m = 4$ e a sequência $(1, 2, 2, 2)$ que é completa com respeito a 4. Qualquer soma, com peso $\{1, -1\}$, desta sequência gera um número ímpar que, portanto, não é um múltiplo de 4, contrariando o Corolário 2.11.

Este corolário é o resultado principal desta seção, pois podemos usá-lo para demonstrar o Teorema 2.1 para o caso em que n é ímpar, que será o nosso próximo objetivo.

2.2.4 O Caso em que n é Ímpar

Teorema 2.12. *Seja $m \in \mathbb{N}$ ímpar. Se $N \geq m + \lfloor log\ m \rfloor$ e $\underline{x} = (x_1, x_2, \ldots, x_N) \in \mathbb{Z}^N$, então existem $I_0 = \{j_1, j_2, \ldots, j_t\} \subseteq [N]$ com $|I_0| = t = N - \lfloor log\ m \rfloor$ e uma escolha de sinais $\xi_1, \xi_2, \ldots, \xi_t \in \{1, -1\}$ tais que*

$$\sum_{i=1}^{t} \xi_i x_{j_i} \equiv 0 (mod\ m).$$

Demonstração. • Se $\underline{x}$ é completa com respeito a m, pelo Lema 2.9, existem $m-1$ índices $j_1, j_2, \ldots, j_{m-1} \in [N]$ tais que a sequência $(x_{j_1}, x_{j_2}, \ldots, x_{j_{m-1}})$ também é completa com respeito a m.

Escolhendo arbitrariamente $j_m, j_{m+1}, \ldots, j_t \in [N] \setminus \{j_1, j_2, \ldots, j_{m-1}\}$ vemos que a sequência $(x_{j_1}, x_{j_2}, \ldots, x_{j_t})$ continua completa com respeito a m. Assim, o Teorema 2.1 segue do Corolário 2.11.

• Supondo que $\underline{x}$ não seja completa com respeito a m, então existe $d|m$ tal que

$$|\{j \in [N]/x_j \not\equiv 0(mod\ d)\}| < d - 1.$$

Tomemos D como o máximo dos divisores de m que satisfazem esta propriedade. Afirmamos que se $f|m$ é tal que $D|f$, então

$$|\{j \in [N]/x_j \equiv 0(mod\ D), x_j \not\equiv 0(mod\ f)\}| \geq \frac{f}{D} - 1.$$

De fato, vamos primeiro fazer algumas considerações sobre os conjuntos $A = \{j \in [N]/x_j \not\equiv 0(mod\ f)\}$ e $B = \{j \in [N]/x_j \not\equiv 0(mod\ D)\}$.

$$B \subseteq A \quad , \quad |A| \geq f - 1 \quad \text{e} \quad |B| < D - 1$$

$$\begin{aligned} |A \setminus B| &= |A| - |A \cap B| \\ &= |A| - |B| \\ &\geq (f-1) - (D-1) \\ &= f - D \\ &= \frac{f}{D}.D - D \\ &= \left(\frac{f}{D} - 1\right).D \\ &\geq \frac{f}{D} - 1 \end{aligned}$$

Além disso, $D \geq 2$ e $\dfrac{f}{D} \geq 2$. Portanto, temos

$$f \geq 2\frac{f}{D} \quad \text{e} \quad f \geq 2D \quad \Rightarrow \quad f > D + \frac{f}{D} - 1.$$

Agora, para justificarmos a afirmação, vemos que se $f = D$ este resultado é trivial. Caso $f > D$ e a afirmação fosse falsa teríamos,

$$|\{j \in [N]/x_j \equiv 0(mod\ D), x_j \not\equiv 0(mod\ f)\}| < \frac{f}{D} - 1.$$

e

$$\begin{aligned} |\{j \in [N]/x_j \not\equiv 0(mod\ f)\}| &= |B| + |\{j \in [N]/x_j \equiv 0(mod\ D), x_j \not\equiv 0(mod\ f)\}| \\ &< (D-1) + \left(\frac{f}{D} - 1\right) \\ &= \left(D + \frac{f}{D} - 1\right) - 1 \\ &< f - 1 \end{aligned}$$

Daí, teríamos $|\{j \in [N]/x_j \not\equiv 0(mod\ f)\}| < f - 1$, contrariando a maximalidade de D. Assim, concluimos a justificativa da afirmação.

Tomemos, agora, os conjuntos $I_1 = B$ e $I_2 = \{j \in [N]/x_j \equiv 0(mod\ D)\}$. Seja $I_3 \subset I_1$ o subconjunto maximal de I_1 de forma que existam $\alpha_i' \in \{1, -1\}$, com $i \in I_3$ tais que

$$\sum_{i \in I_3} \alpha_i' x_i \equiv 0(mod\ D).$$

Observe que o caso em que $I_3 = \emptyset$ não nos impedirá de seguir o reciocínio abaixo.

Pelo Lema 2.4, $|I_1 \setminus I_3| \leq \lfloor log\ D \rfloor$.

Assim, temos $|I_1| - |I_3| \leq \lfloor log\ D \rfloor$ e, por hipótese, $t = N - \lfloor log\ m \rfloor$, onde $N \geq m + \lfloor log\ m \rfloor$. Tomando $k = t - |I_3|$, temos

$$\begin{aligned} k = t - |I_3| &= N - \lfloor log\ m \rfloor - |I_3| \\ &\leq N - \lfloor log\ m \rfloor + \lfloor log\ D \rfloor - |I_1| \\ &\leq N - |I_1| \\ &= |I_2|. \end{aligned}$$

Assim, $k \leq |I_2|$. Por outro lado, temos

$$\begin{aligned} k &= t - |I_3| \\ &\geq m - |I_3| \\ &\geq m - |I_1| \\ &> m - (D-1) \\ &= m - D + 1 \\ &> \frac{m}{D}. \end{aligned}$$

Esta última desigualdade se deve a fato de $D \geq 2$, $\frac{m}{D} \geq 2$ e, assim, temos

$$m \geq 2\frac{m}{D} \quad \text{e} \quad m \geq 2D \quad \Rightarrow \quad m > D + \frac{m}{D} - 1.$$

Portanto, $\frac{m}{D} < k \leq |I_2|$.

Tomemos agora $\tilde{x} = \left(\frac{x_j}{D}\right)_{j \in I_2}$.

Os divisores de $\frac{m}{D}$ são todos os elementos da forma $\frac{f}{D}$ tais que $f|m$ e $D|f$. Assim,

$$\begin{aligned} \left|\left\{j \in [N]/x_j \not\equiv 0 \left(mod\ \frac{f}{D}\right)\right\}\right| &= |\{j \in [N]/x_j \equiv 0(mod\ D), x_j \not\equiv 0(mod\ f)\}| \\ &\geq \frac{f}{D} - 1. \end{aligned}$$

Portanto, $\tilde{x}$ é uma sequência completa com respeito a $\frac{m}{D}$.

Pelo Lema 2.9, existe o conjunto $I' = \{j_1, j_2, \ldots, j_{\frac{m}{D}-1}\} \subseteq I_2$ tal que a sequência

$$\left(\frac{x_j}{D}\right)_{j \in I'} = \left(\frac{x_{j_1}}{D}, \frac{x_{j_2}}{D}, \ldots, \frac{x_{j_{\frac{m}{D}-1}}}{D}\right)$$

também é completa com respeito a $\frac{m}{D}$.

Como $\frac{m}{D} < k \leq |I_2|$, então podemos escolher I_1' tal que $I' \subseteq I_1' \subseteq I_2$ e $|I_1'| = k$ e, claramente, a sequência $\left(\frac{x_j}{D}\right)_{j \in I_1'}$ continua completa com respeito a $\frac{m}{D}$.

Tomando $b = -\frac{1}{D}\sum_{j \in I_3} \alpha_j' x_j$, pelo Corolário 2.11, existem $\alpha_j'' \in \{1, -1\}$ para $j \in I_1'$ tais que

$$\sum_{j \in I_1'} \alpha_j'' \frac{x_j}{D} \equiv -\frac{1}{D}\sum_{j \in I_3} \alpha_j' x_j \left(mod\ \frac{m}{D}\right).$$

Considerando $I_0 = I_3 \cup I_1'$ e $\begin{cases} \alpha_j = \alpha_j' \text{ , se } j \in I_3 \\ \alpha_j = \alpha_j'' \text{ , se } j \in I_1' \end{cases}$, temos

$$\sum_{j \in I_0} \alpha_j \frac{x_j}{D} \equiv 0 \left(mod\ \frac{m}{D}\right)$$

e $|I_0| = |I_1'| + |I_3| = k + |I_3| = t - |I_3| + |I_3| = t = N - \lfloor log\ m \rfloor$.

Assim, concluimos a demonstração do Teorema 2.12. □

De posse dos Teoremas 2.3 e 2.12, observamos que o Teorema 2.1 está demonstrado.

Capítulo 3

Teorema de Erdös-Ginzburg-Ziv com Peso Qualquer

Antes de enunciarmos os objetivos deste capítulo, vamos dar alguma definições que serão imprescindíveis para a compreensão de nossos estudos.

Seja $(G, +, 0)$ um grupo abeliano. Vamos considerar o grupo abeliano G como um $\mathbb{Z}$-módulo. O *expoente de* G, para G finito, é o menor inteiro k tal que $kg = 0$, para todo $g \in G$. Denotamos o expoente do grupo G por $exp(G)$.

Definição 3.1. *Sejam S uma sequência finita de elementos de um grupo abeliano G e $n \leq |S|$ um número natural. Dizemos que uma n-***partição** *de S é uma coleção de n subsequências de S não-vazias, disjuntas duas a duas, tais que cada termo de S pertence a exatamente uma das subsequências e os termos em cada subsequência são todos distintos de modo que podem ser consideradas como conjuntos.*

Uma *subsequência rearranjada de S* é uma sequência que, sob algumas permutações de termos, é uma subsequência de S.

Observamos facilmente que uma sequência S tem uma n-partição se, e somente se, o seu comprimento $|S|$ é no mínimo igual a n e cada termo de S tem multiplicidade no máximo n, ou seja, cada elemento de G que aparece em S pode figurar em, no máximo, n posições distintas da sequência S.

Dado um subgrupo H de G, durante nosso estudo usaremos $\phi_H : G \longrightarrow G/H$ para denotar o homomorfismo natural,

$$\begin{array}{rccl} \phi_H : & G & \longrightarrow & G/H \\ & g & \longmapsto & \phi_H(g) = g + H. \end{array}$$

Esta definição poderia nos levar a crer que, dado um subconjunto A de G, teríamos $\phi_H(A) = A + H$, mas, apesar de o conjunto $A + H$ conter todos os elementos das classes

em $\phi_H(A)$, o conjunto $A+H$ é um subconjunto do grupo G e o conjunto $\phi_H(A)$ é um subconjunto do grupo G/H. Tendo esclarecido isso, podemos citar algumas propriedades que são facilmente deduzidas das propriedades do grupo quociente. Sejam A e B subconjuntos de um grupo G abeliano e finito e H um subgrupo de G, temos:

(i) $\phi_H(A+B) = \phi_H(A) + \phi_H(B)$;

(ii) $|A+H| = |\phi_H(A)| \cdot |H|$.

Para $w \in \mathbb{Z}$ e $A \subseteq G$, definimos $wA = \{wa \,/\, a \in A\}$. Esta definição difere da definição de hA dada na Introdução (Pág. 1). É fácil observarmos que $|wA| \leq |A|$, para qualquer que seja $A \subseteq G$.

Neste capítulo, iremos mostrar que se S é uma sequência de $m+n-1$ elementos de um grupo abeliano finito G de ordem m e expoente k e se $W = (w_i)_{i=1}^n$ é uma sequência de números inteiros cuja soma é zero módulo k, então existe uma subsequência rearranjada $(b_i)_{i=1}^n$ de S tal que $\sum_{i=1}^n w_i b_i = 0$. Este resultado estende o Teorema de Erdös-Ginzburg-Ziv para o caso em que os elementos da sequência pertencem a um grupo abeliano qualquer, onde $m = n$ e $w_i = 1$ para todo i. Além disso, vamos mostrar que se S tem uma *n-partição* $A = A_1, ..., A_n$ tal que $|w_i A_i| = |A_i|$ para todo i, então existe um subgrupo H não trivial de G e uma *n-partição* $A' = A'_1, ..., A'_n$ de S tal que

$$H \subseteq \sum_{i=1}^{n} w_i.A'_i = \{w_1a_1 + w_2a_2 + \ldots + w_na_n \;/\; a_i \in A'_i \;,\; i = 1, 2, \ldots, n\}$$

e $|w_i A'_i| = |A'_i|$, para todo i.

Começamos por enunciar a versão estendida do Teorema de Erdös-Ginzburg-Ziv, hoje conhecido como o Teorema EGZ.

Teorema 3.2. **(a)** *Seja G um grupo abeliano de ordem n. Seja I um conjunto de índices e seja $\{a_i\}_{i\in I}$ um conjunto indexado de elementos de G. Se $|I| = 2n-1$, então existe um subconjunto $J \subseteq I$, com $|J| = n$, tal que*

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

(b) *Se $|I| = 2n-2$ e não existe um subconjunto $J \subseteq I$, com $|J| = n$, tal que $\sum_{j\in J} a_j = 0$, então concluímos que:*

- **(i)** *O grupo G é cíclico.*
- **(ii)** *Metade dos $a'_i s$ são iguais a $x \in G$, a outra metade do $a'_i s$ são iguais a $y \in G$, onde $x - y$ é um gerador de G.*

Demonstração. Para a parte (a), podemos observar em [17] que, para grupos cíclicos e finitos, a demonstração deste ítem é consequência do Teorema de Erdös-Ginzburg-Ziv para inteiros.

Agora, afirmamos que, se o teorema vale para os grupos G e K abelianos e finitos, então vale para o grupo $G \oplus K$. De fato, sejam os grupos G e K abelianos e finitos tais que $|G| = m$ e $|K| = n$. Então $|G \oplus K| = m \cdot n$. Agora tomemos a sequência

$$(a_1, a_2, \ldots, a_{2mn-1})$$

de elementos de $G \oplus K$. Pela hipótese de que o teorema é válido para o grupo K temos que, para cada subconjunto A de índices em $\{1, 2, \ldots, 2mn-1\}$ com $2n-1$ índices, existe um subconjunto $B \subseteq A$ com n índices tal que a segunda coordenada do elemento $\sum_{i \in B} a_i$ é igual ao 0_K (elemento neutro do grupo K). Assim, construímos os conjuntos B_j, indutivamente, para $1 \leq j \leq 2m-1$, seguindo os seguintes passos

- Escolhemos um subconjunto A_j de $\{1, 2, \ldots, 2mn-1\} \setminus \bigcup_{k<j} B_k$ com $2n-1$ índices.
- De A_j escolhemos um subconjunto B_j com n índices tal que a segunda coordenada do elemento $\sum_{i \in B_j} a_i$ seja igual ao 0_K.

Observemos que, se $j \leq 2m-1$, então

$$\begin{aligned} \left| \{1, 2, \ldots, 2mn-1\} \setminus \bigcup_{k<j} B_j \right| &= 2mn - 1 - (j-1)n \\ &\geq 2mn - 1 - (2m-2)n \\ &= 2n - 1. \end{aligned}$$

o que garante a construção até $j = 2m-1$. Assim, a segunda coordenada dos elementos $\sum_{i \in B_j} x_i$ são iguais ao 0_K, para $1 \leq j \leq 2m-1$ e, pela hipótese de que o teorema vale para o grupo G, existe um subconjunto de índices $C \in \{1, 2, \ldots, 2m-1\}$ com m índices tal que

$$\sum_{j \in C} \sum_{i \in B_j} a_i = (0_G, 0_K),$$

onde 0_G é o elemento neutro do grupo G. Esta soma é formada por $|C| \cdot |B_j| = mn$ elementos de $G \oplus K$. Assim mostramos que existe um conjunto de índices $I = \bigcup_{j \in C} B_j \subseteq \{1, 2, \ldots, 2mn-1\}$ tal que $\sum_{i \in I} a_i = 0_{G \oplus K}$ que é o neutro de $G \oplus K$, completando a demonstração da afirmação.

Agora, vamos proceder a demonstração do ítem (a) para um grupo G abeliano e finito qualquer. Pelo *Teorema Fundamental dos Grupos Abelianos Finitos*, podemos decompor G da seguinte forma

$$G \cong C_{e_1} \oplus C_{e_2} \oplus \ldots \oplus C_{e_n}.$$

Sabemos que o teorema vale para os grupos C_{e_1} e C_{e_2}, pois eles são cíclicos e finitos. Portanto, tendo em vista a afirmação que demonstramos, concluímos que o teorema vale para o grupo $C_{e_1} \oplus C_{e_2}$.

Suponha agora que o teorema seja válido para o grupo $C_{e_1} \oplus C_{e_2} \oplus \ldots \oplus C_{e_{k-1}}$. Por nossa afirmação demonstrada e sabendo que C_{e_k} é cíclico e finito, vemos que o teorema também vale para o grupo

$$(C_{e_1} \oplus C_{e_2} \oplus \ldots \oplus C_{e_{k-1}}) \oplus C_{e_k}.$$

Logo, pelo processo de indução finita, fica claro que o teorema é valido para o grupo G.

A parte (b) é entendida como a solução de um problema inverso. A demonstração das partes (b)(i) e (b)(ii) não será feita devido a sua extensão, mas elas podem ser deduzidas das referências [8] e [10], respectivamente. □

Este teorema estimulou o crescimento do atual campo de desenvolvimento da *Teoria de Ramsey de soma-zero* e tem sido objeto de numerosas e variadas generalizações.

No início de 1990, N. Alon demonstrou a seguinte conjectura de Y. Caro, para o caso de $n = m$, com m primo.

Conjectura 3.3 (Y. Caro)**.** *Dados os inteiros n e m, com $n \geq 2$ e $S = (b_i)_{i=1}^{m+n-1}$ uma sequência qualquer de números inteiros. Se $W = (w_i)_{i=1}^{n}$ é uma sequência de números inteiros tais que $\sum_{i=1}^{n} w_i \equiv 0(mod\ m)$. Então existe uma subsequência rearranjada $(b_{j_i})_{i=1}^{n}$ de S tal que*

$$\sum_{i=1}^{n} w_i b_{j_i} \equiv 0(mod\ m).$$

N. Alon comunicou-se com A. Bialostocki e Y. Caro e logo depois a demonstração desta conjectura foi estendida para n arbitrário e m primo. Entretanto o caso geral do problema não foi resolvido. Alguns anos mais tarde esta conjectura foi incluída em uma pesquisa de Y. Caro em problemas combinatórios de soma zero [11], onde uma referência foi feita para a prova do caso em que n é arbitrário e m é primo [7], a qual não foi publicada.

Pouco tempo depois, Y. Hamidoune publicou dois artigos onde, no primeiro ele provou uma forma equivalente à Conjectura de Y. Caro (em uma definição mais geral do grupo abeliano) sob a condição de que cada w_i, para $i \in \{1, ..., n-1\}$, fosse coprimo com m [27], e na segunda ele introduziu a seguinte conjectura que ele verificou para $n = m$ [28].

Conjectura 3.4 (Y. Hamidoune)**.** *Sejam $n \geq 2$, m inteiros, uma sequência S de $m+n-1$ elementos de um grupo abeliano finito G de ordem m e $W = (w_i)_{i=1}^{n}$ uma sequência de números inteiros cuja soma é zero modulo m. Se a multiplicidade de cada elemento de*

S é no máximo n e se cada w_i, para $i \leq n-1$, é relativamente primo a m, então existe um subgrupo H não trivial de G tal que, para cada $h \in H$, existe uma subsequência rearranjada $(b_{h_i})_{i=1}^n$ de S com

$$\sum_{i=1}^{n} w_i b_{h_i} = h.$$

Nenhum progresso foi feito em qualquer uma das conjecturas até 2003, quando W. Gao e X. Jin estabeleceram a Conjectura de Y. Caro (3.3) no caso de $m = p^2$, para p primo [19].

Em 2006, D. J. Grynkiewicz demonstrou, em [23], o seguinte teorema, que é o principal resultado deste capítulo.

Teorema 3.5. *Sejam m, k e $n \geq 2$ inteiros positivos. Se S é uma sequência de $m+n-1$ elementos de um grupo abeliano não trivial G de ordem m e expoente k e $W = (w_i)_{i=1}^n$ é uma sequência de números inteiros cuja soma é zero módulo k, então:*

(i) existe uma subsequência rearranjada $(b_i)_{i=1}^n$ de S tal que $\sum_{i=1}^n w_i b_i = 0$ e

(ii) se S tem uma n-partição $A = A_1, ..., A_n$ tal que $|w_i A_i| = |A_i|$, para todo i, então existe um subgrupo H não trivial de G e uma n-partição $A' = A'_1, ..., A'_n$ de S com $|w_i A'_i| = |A'_i|$, para todo i, tal que $H \subseteq \sum_{i=1}^n w_i.A'_i$.

Notemos que o exemplo onde $m = k = n$,

$$W = (\overbrace{1, \ldots, 1}^{m-2}, 0, 2) \text{ e } S = (-1, \overbrace{0, \ldots, 0}^{m-1}, \overbrace{1, \ldots, 1}^{m-1}),$$

com $G = \mathbb{Z}_m$ cíclico, mostra que no teorema acima, não podemos exigir que a subsequência $(b_i)_{i=1}^m$ de S seja uma subsequência verdadeira (incluindo os índices dos elementos) de S. Vamos ilustrar este argumento com alguns exemplos:

(i) $W = (\overbrace{1, \ldots, 1}^{m-2}, 0, 2)$ e $(b_i)_{i=1}^m = (-1, \overbrace{0, \ldots, 0}^{m-1})$, implicam $\sum_{i=1}^{m} w_i b_i = -1$

(ii) $W = (\overbrace{1, \ldots, 1}^{m-2}, 0, 2)$ e $(b_i)_{i=1}^m = (\overbrace{0, \ldots, 0}^{m-1}, 1)$, implicam $\sum_{i=1}^{m} w_i b_i = 2$

(iii) $W = (\overbrace{1, \ldots, 1}^{m-2}, 0, 2)$ e $(b_i)_{i=1}^m = (-1, \overbrace{1, \ldots, 1}^{m-1})$, implicam $\sum_{i=1}^{m} w_i b_i = m-2$

(iv) $W = (\overbrace{1, \ldots, 1}^{m-2}, 0, 2)$ e $(b_i)_{i=1}^m = (\overbrace{0, \ldots, 0}^{m-2}, 1, 0)$, implicam $\sum_{i=1}^{m} w_i b_i = 0$

Observe que no exemplo (iv) a ordem dos elementos de S foi alterada na construção da subsequência $(b_i)_{i=1}^m$ para que fosse possível escrever a soma cujo resultado é nulo.

É fácil ver que o Teorema 3.5 confirma completamente a Conjectura 3.3. Sabemos também que, se w_i for coprimo com m, então $|w_i A_i| = |A_i|$.

Corolário 3.6. *O Teorema 3.5 implica a Conjectura 3.4, desde que pelo menos uma das seguintes condições seja válida:*

(a) *w_n é coprimo com m, ou*

(b) *$n \geq m$, ou*

(c) *cada termo de S tem multiplicidade no máximo $n-1$.*

Observação: Vamos mostrar que ambas as condições (b) e (c) implicam que existe uma n-partição de S com pelo menos um conjunto A_i de cardinalidade *um*.

Demonstração. **(a)** Por hipótese da Conjectura 3.4, w_i é coprimo com m para todo $i \in \{1, 2, \ldots, n-1\}$. Se w_n é também coprimo com m, então, para qualquer n-partição A de S, obtemos $|w_i A_i| = |A_i|$ para todo $i \in \{1, 2, \ldots, n\}$. Com esta afirmação podemos aplicar o Teorema 3.5 e, assim, concluir a Conjectura 3.4.

Neste momento, vamos mostrar que as condições (b) e (c) implicam que existe uma n-partição de S com pelo menos um conjunto A_i de cardinalidade *um*.

(b) Vamos supor que, para qualquer n-partição $A = A_1, A_2, \ldots, A_n$ de S, $|A_i| \geq 2$. Como $n \geq m$, obtemos

$$2n \leq \sum_{i=1}^{n} |A_i| = |S| = m + n - 1 \leq n + n - 1 = 2n - 1,$$

o que é um absurdo. Portanto, existe uma n-partição A de S com pelo menos um conjunto A_i de cardinalidade *um*.

(c) Consideremos a sequência S escrita da seguinte forma

$$S = (a_1, a_2, \ldots, a_{m+n-2}, a_{m+n-1}).$$

Consideremos também a subsequência $S^* = (a_1, a_2, \ldots, a_{m+n-2})$.

Se cada termo de S tem multiplicidade no máximo $n-1$, então o mesmo acontece em S^*. Além disso, como $|S^*| = m + n - 2 = m + (n-1) - 1$ e $m \geq 1$ então existe uma $(n-1)$-partição $A^* = A_1, A_2, \ldots, A_{n-1}$ de S^*. Tomando $A_n = \{a_{m+n-1}\}$, temos que a coleção $A = A_1, A_2, \ldots, A_{n-1}, A_n$ é uma n-partição de S com $|A_n| = 1$.

Dada uma das condições (b) ou (c), existe uma n-partição $A = A_1, A_2, \ldots, A_n$ de S com pelo menos um conjunto A_i de cardinalidade um. Reindexando a n-partição A, podemos considerar que o conjunto de cardinalidade igual a um seja o conjunto A_n. Dada a hipótese da Conjectura 3.4 de w_i ser coprimo com m, para todo $i \in \{1, 2, \ldots, n-1\}$, temos

$$|w_i A_i| = |A_i| \text{ para } i \in \{1, 2, \ldots, n-1\} \text{ e, além disso, } |w_n A_n| = 1 = |A_n|.$$

Unsando esta n-partição, podemos aplicar o Teorema 3.5 e, novamente, concluir a Conjectura 3.4. □

Para finalizar esta seção, citamos o artigo [25], onde D. J. Grynkiewicz *et al* enunciam dois exemplos que mostram que a Conjectura 3.4 não se verifica para o caso geral. São eles:

EXEMPLO 1: Seja $G = C_p$ o grupo cíclico de ordem p, onde $p \equiv -1(mod\ 4)$ é um primo e $n = \dfrac{p-1}{2}$. Agora, considere

$$W = (\overbrace{1, 1, \ldots, 1}^{(n-1)/2 \text{ vezes}}, \overbrace{-1, -1, \ldots, -1}^{(n-1)/2 \text{ vezes}}, 0)$$

uma sequência de inteiros e tome

$$S = (\overbrace{0, 0, \ldots, 0}^{n \text{ vezes}}, \overbrace{g, g, \ldots, g}^{n \text{ vezes}}, \overbrace{2g, 2g, \ldots, 2g}^{n \text{ vezes}}),$$

onde $g \in G \setminus \{0\}$. Assim, $|W| = n$, $|S| = 3n = |G| + |W| - 1$, $\sum_{w \in W} w = 0$ e, ainda,

$$\Sigma_{|W|}(W, S) = \sum_{i=1}^{(n-1)/2} \{0, g, 2g\} - \sum_{i=1}^{(n-1)/2} \{0, g, 2g\} = G \setminus \{\frac{p-1}{2}g, \frac{p+1}{2}g\},$$

onde $\Sigma_{|W|}(W, S)$ representa o conjunto de todas as somas de $|W| = n$ elementos de S com peso em W e $\sum_{i=1}^{(n-1)/2}\{0, g, 2g\}$ é o conjunto de todas as somas possíveis de $(n-1)/2$ elementos do conjunto $\{0, g, 2g\}$.

Como G não está contido em $\Sigma_{|W|}(W, S)$ e $|G| = p$ é primo, então G não possui subgrupo diferente do trivial e, assim, $\Sigma_{|W|}(W, S)$ não contém um subgrupo não trivial de G.

EXEMPLO 2: Seja $G = C_m$ o grupo cíclico de ordem m, onde $m = 2^r$, para algum natural r, e $n = m - 1$. Agora, considere

$$W = (\overbrace{1, 1, \ldots, 1}^{(n-1)/2 \text{ vezes}}, \overbrace{-1, -1, \ldots, -1}^{(n-1)/2 \text{ vezes}}, 0)$$

uma sequência de inteiros e tome

$$S = (\overbrace{0, 0, \ldots, 0}^{n \text{ vezes}}, \overbrace{g, g, \ldots, g}^{n \text{ vezes}}),$$

onde $g \in G$ é um elemento de ordem m. Assim, $|W| = n$, $|S| = 2n = |G| + |W| - 1$, $\sum_{w \in W} w = 0$ e, ainda,

$$\Sigma_{|W|}(W, S) = \sum_{i=1}^{(n-1)/2} \{0, g\} - \sum_{i=1}^{(n-1)/2} \{0, g\} = G \setminus \{\frac{m}{2} g\}.$$

Como todo subgrupo não trivial de $G \cong \mathbb{Z}/2^r\mathbb{Z}$ contém o único elemento de ordem 2, denotado por $\frac{m}{2}g$, segue que $\Sigma_{|W|}(W, S)$ não contém um subgrupo não trivial de G.

Perceba que, nestes dois exemplos, as hipóteses do Corolário 3.6 não se verificam.

3.1 Teorema de EGZ com Peso

Definiremos, agora, algumas propriedades parecidas com as que vimos no primeiro capítulo, mas que serão de muita importância para a demonstração dos resultados deste capítulo.

Definição 3.7. *Dado um grupo abeliano G, um conjunto $A \subseteq G$ é dito H-periódico se ele é a união de classes em G/H, para algum subgrupo H de G.*

Note que essa definição de periódico difere ligeiramente da definição usual dada no primeiro capítulo, permitindo que H seja o subgrupo trivial.

Consequentemente, temos

Definição 3.8. *Dado um grupo abeliano G, diz-se que $A \subseteq G$ é maximalmente H-periódico se A é H-periódico e H é o subgrupo maximal em que A é periódico.*

Um conjunto que é *maximalmente H-periódico*, com $H = \{0\}$ o grupo trivial, é dito *não-periódico* e, caso contrário, nos referimos a A como *não-trivialmente periódico.*

Neste caso, podemos demonstrar algumas propriedades bem interessantes:

Proposição 3.9. *Seja G um grupo abeliano e H um subgrupo não trivial de G. Dados A e B subconjuntos de G:*

(a) *O conjunto $A \subseteq G$ é maximalmente H-periódico se, e somente se, $H = \{x \in G\,;\, x + A = A\}$, ou seja, $H = H(A)$, o estabilizador de A.*

(b) *Se A é H'-periódico, para algum subgrupo H' de G, então $A+B$ é também H'-periódico e, além disso, H' é também um subgrupo do grupo H em que $A+B$ é maximalmente H-periódico.*

(c) *Se A é maximalmente H-periódico, então $\phi_H(A)$ é não-periódico.*

Demonstração. **(a)** Como o grupo G é abeliano e H é um subgrupo de G, então existe um conjunto K de índices tal que

$$G/H = \bigcup_{i\in K}(x_i + H),$$

onde cada x_i é um elemento do grupo G.

($\Rightarrow$) Sendo o conjunto A maximalmente H-periódico, então A é H-periódico e podemos escrever

$$A = \bigcup_{i\in J}(x_i + H),$$

para algum $J \subseteq K$.

Primeiramente, temos

$$A + H = \bigcup_{i\in J}(x_i + H) + H = \bigcup_{i\in J}(x_i + H + H) = \bigcup_{i\in J}(x_i + H) = A.$$

Agora, suponha que exista $g \in G$ tal que $g + A = A$ e $g \notin H$. Considere, então, o subgrupo H' de G definido por $H' = \langle H, g\rangle$ (subgrupo gerado pelos elememtos do conjunto $H \cup \{g\}$). Fica claro que $H \leq H'$, $g \in H'$ e, ainda, $A = A + H'$, ou seja, existe um conjunto L de índices tais que

$$A = \bigcup_{i\in L}(x_i + H'),$$

onde cada x_i é um elemento do grupo G. Portanto, A é H'-periódico e chegamos a um absurdo, pois H' contraria a maximalidade de H. Logo, não existe tal g e, assim, $H = \{x \in G \ ; \ x + A = A\}$.

($\Leftarrow$) Se $H = \{x \in G \ ; \ x + A = A\}$, então $A = A + H$, ou seja, existe um conjunto de índices $J \subseteq K$ tal que

$$A = \bigcup_{i\in J}(x_i + H).$$

Com isso, vemos que A é H-periódico.

Agora, suponha que exista um subgrupo H^* de G tal que A é H^*-periódico e $|H| < |H^*|$. Assim, existe um conjunto L de índices tais que

$$A = \bigcup_{i\in L}(x_i + H^*),$$

onde cada x_i é um elemento do grupo G. Além disso,

$$A + H^* = \bigcup_{i \in L}(x_i + H^*) + H^* = \bigcup_{i \in L}(x_i + H^* + H^*) = \bigcup_{i \in L}(x_i + H^*) = A.$$

Com isso, concluímos que $H^* \subseteq H$, o que é um absurdo. Portanto, não existe tal H^* e, assim, A é maximalmente H-periódico.

(b) Para o grupo G abeliano e H' um subgrupo de G, então existe um conjunto K de índices tal que

$$G/H' = \bigcup_{i \in K}(x_i + H'),$$

onde cada x_i é um elemento do grupo G.

Como o conjunto A é H'-periódico, então podemos escrever

$$A = \bigcup_{i \in J}(x_i + H'),$$

para algum $J \subseteq K$. Agora, temos

$$\begin{aligned} A + B &= \bigcup_{i \in J}(x_i + H') + B \\ &= \bigcup_{i \in J}(x_i + H' + B) \\ &= \bigcup_{i \in J}[(x_i + B) + H'] \end{aligned}$$

É evidente que, para cada $i \in J$, o conjunto $(x_i + B) + H'$ é uma coleção de classes de G/H'. Portanto, existe um conjunto de índices $L \subseteq K$ tal que

$$A + B = \bigcup_{i \in L}(x_i + H'),$$

ou seja, $A + B$ é H'-periódico.

Além disso, como $A + B$ é maximalmente H-periódico, pelo ítem **(a)**, temos

$$H = \{x \in G \ ; \ x + (A + B) = (A + B)\}.$$

Tomemos $h' \in H'$. Assim, temos

$$\begin{aligned} h' + A + B &= h' + \bigcup_{i \in L}(x_i + H') \\ &= \bigcup_{i \in L}(x_i + H' + h') \\ &= \bigcup_{i \in L}(x_i + H') \\ &= A + B \end{aligned}$$

Com isso, vemos que $h' \in H$. Portanto, como h' é arbitrário, então $H' \subseteq H$.

(c) Como A é maximalmente H-periódico, então, pelo ítem **(a)**, temos que $H = \{x \in G \ ; \ x + A = A\}$.

Consideremos o grupo G/H. Assim, $0_{G/H} = H$ e $\phi_H(A) \subseteq G/H$. Vamos considerar que, no grupo G/H, temos $\phi_H(A) = A + H$.

Vamos, agora, encontrar as classes $x + H \in G/H$ tais que $x + H + \phi_H(A) = \phi_H(A)$.

Temos

$$\begin{aligned} (x + H) + \phi_H(A) &= \phi_H(A) \Rightarrow \\ (x + H) + (A + H) &= (A + H) \Rightarrow \\ x + A + (H + H) &= A + H \Rightarrow \\ x + A + H &= A + H \Rightarrow \\ x + A &= A \end{aligned}$$

Com esta última igualdade, temos $x \in H$, ou seja, a classe $x + H = H = 0_{G/H}$. Com isso, vemos que $\phi_H(A)$ é maximalmente K-periódico, onde $K = \{H\} = \{0_{G/H}\} \subseteq G/H$, ou seja, $\phi_H(A)$ é não-periódico.

□

Uma outra ferramenta importante será definida a seguir.

Definição 3.10. *Dados um grupo abeliano G, um conjunto $A \subseteq G$ e um subgrupo H de G, um H-hole de A é um elemento $\alpha \in (A + H) \setminus A$.*

Começamos por afirmar um resultado obtido a partir do Corolário 1.20, que, por sua vez, é uma consequência do clássico *Teorema de Kneser* para somas de subconjuntos de um grupo abeliano finito que foi demonstrado no primeiro capítulo.

Teorema 3.11 (Kneser)**.** *Sejam G um grupo abeliano de ordem m e $A_1, A_2, \ldots, A_n$ uma coleção de subconjuntos finitos e não vazios de G. Se $\sum_{i=1}^{n} A_i$ é maximalmente*

H-periódico, então

$$\left|\sum_{i=1}^{n}\phi_H(A_i)\right| \geq \sum_{i=1}^{n}|\phi_H(A_i)| - n + 1.$$

Demonstração. Observemos que os conjuntos

$$\phi_H\left(\sum_{i=1}^{n}A_i\right) = \sum_{i=1}^{n}\phi_H(A_i) \quad \text{e} \quad \phi_H(A_i), \text{ para } i = 1, 2, \ldots, n,$$

são subconjuntos do grupo G/H.

Pelo ítem **(c)** da Proposição 3.9, o conjunto $\sum_{i=1}^{n}\phi_H(A_i)$ é não-periódico em G/H, ou seja, $\sum_{i=1}^{n}\phi_H(A_i)$ é maximalmente K-periódico, onde $K = \{0_{G/H}\} \subseteq G/H$.

Aplicando o Corolário 1.20 aos subconjuntos de G/H, temos

$$\left|\sum_{i=1}^{n}\phi_H(A_i)\right| \geq \sum_{i=1}^{n}|\phi_H(A_i)| - (n-1).|K|.$$

Como $|K| = 1$, concluímos

$$\left|\sum_{i=1}^{n}\phi_H(A_i)\right| \geq \sum_{i=1}^{n}|\phi_H(A_i)| - n + 1.$$

□

O caso em que m é primo é conhecido como o Teorema de Cauchy-Davenport, que também consta no primeiro capítulo, e foi o instrumento original utilizado na prova da Conjectura 3.3 para m primo.

Corolário 3.12. *Se $A+B$ é maximalmente H-periódico e $\rho = |A+H|-|A|+|B+H|-|B|$ é o número de H-holes em A e B, então o Teorema de Kneser implica:*

(a) $|A + B| \geq |A| + |B| - |H| + \rho$.

(b) *Se A ou B contém um elemento que é o único de sua H-classe, então $|A + B| \geq |A| + |B| - 1$.*

(c) *Se $\sum_{i=1}^{n} A_i$ é maximalmente H-periódico e $\sum_{i=1}^{n}(|A_i + H| - |A_i|)$ é o número total de H-holes nos conjuntos A_i, onde $i \in \{1, 2, \ldots, n\}$, então $|\sum_{i=1}^{n} A_i| \geq \sum_{i=1}^{n}|A_i| - (n-1)|H| + \rho$.*

Demonstração. **(a)**

$$\begin{aligned} |A|+|B|-|H|+\rho &= |A|+|B|-|H|+(|A+H|-|A|+|B+H|-|B|) \\ &= |A+H|+|B+H|-|H| \\ &\overset{(*)}{\leq} |A+B| \end{aligned}$$

$(*)$ Pelo Teorema 1.19 que é consequência do Teorema de Kneser.

(b) Suponha, sem perda de generalidade, que o conjunto A contenha um elemento que é o único de sua H-classe. Afirmamos que existem pelo menos $|H|-1$ H-holes em A, ou seja,

$$|A+H|-|A| \geq |H|-1.$$

Para justificarmos esta afirmação, considere que o elemento $a \in A$ é o único de sua H-classe em G/H, temos

$$\begin{aligned} |A+H| &= |[(A\setminus\{a\})+H]\cup(a+H)| \\ &= |(A\setminus\{a\})+H|+|a+H| \\ &\geq |(A\setminus\{a\})|+|a+H| \\ &= |A|-1+|a+H| \\ &= |A|-1+|H| \\ &= |A|+|H|-1 \end{aligned}$$

Agora, temos $\rho \geq |H|-1$ e, pelo ítem **(a)**, temos também

$$|A+B| \geq |A|+|B|-|H|+\rho \geq |A|+|B|-|H|+(|H|-1) = |A|+|B|-1,$$

concluindo a demonstração.

(c)

$$\begin{aligned} \sum_{i=1}^{n}|A_i|-(n-1)|H|+\rho &= \sum_{i=1}^{n}|A_i|-(n-1)|H|+\sum_{i=1}^{n}(|A_i+H|-|A_i|) \\ &= \sum_{i=1}^{n}|A_i+H|-(n-1)|H| \\ &\leq \sum_{i=1}^{n}|A_i|-(n-1)|H| \\ &\overset{(*)}{\leq} \left|\sum_{i=1}^{n}A_i\right| \end{aligned}$$

(∗) Pelo Corolário 1.20 que é consequência do Teorema de Kneser.

□

Lembrando que, no início da Seção 1.2, definimos $r_{A,B}(g)$, onde A e B são subconjuntos de um grupo abeliano e g é um elemento deste grupo, como

$$r_{A,B}(g) = |\{(a,b) \ / \ g = a+b\,,\ a \in A \text{ e } b \in B\}|,$$

então podemos enunciar o seguinte resultado que foi citado em [38].

Teorema 3.13 (Kemperman-Scherk)**.** *Sejam A e B dois subconjuntos finitos e não vazios de um grupo abeliano G. Então $r_{A,B}(c) \geq |A| + |B| - |A+B|$, para qualquer $c \in A+B$.*

Demonstração. Se $|A+B| \geq |A|+|B|-1$, a afirmação é trivial. Sendo assim, suponhamos $|A+B| = |A|+|B|-k$, para algum $k \geq 2$. Vamos mostrar que $r_{A,B}(c) \geq k$, para qualquer $c \in A+B$.

Tomemos $H = H(A+B)$ e, além disso, fixemos uma representação $c = a_0 + b_0$, onde $a_0 \in A$ e $b_0 \in B$. O Teorema de Kneser (Teorema 1.18) nos diz que se $|A+B| < |A|+|B|$, então

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

Portanto,

$$\begin{aligned}
|(A-a_0)\cap H| + |(b_0-B)\cap H| &= |A\cap(a_0+H)| + |B\cap(b_0+H)| \\
&= |H| - |(a_0+H)\setminus A| + |H| - |(b_0+H)\setminus B| \\
&\geq 2|H| - |(A+H)\setminus A| - |(B+H)\setminus B| \\
&= 2|H| - (|A+H| - |A|) - (|B+H| - |B|) \\
&= 2|H| - |A+H| + |A| - |B+H| + |B| \\
&= |H| + |A| + |B| - (|A+H| + |B+H| - |H|) \\
&= |H| + |A| + |B| - |A+B| \\
&= |H| + k
\end{aligned}$$

Assim, pelo Princípio da Casa dos Pombos, $(A-a_0)\cap H$ e $(b_0-B)\cap H$ possuem pelo menos k elementos em comum. Portanto, cada par (a,b) tal que $a \in A$, $b \in B$ e $a - a_0 = b_0 - b$ nos fornece uma para $a+b=c$. Logo $r_{A,B}(c) \geq k$ como queríamos demonstrar. □

Demonstramos o Teorema 3.13 usando o Teorema de Kneser. Entretanto, este teorema é datado de 1951, quando Moser propôs na American Mathematical Monthly um problema que pode ser formulado da seguinte maneira:

Para A e B subconjuntos finitos do grupo Toro, $\mathbb{R}/\mathbb{Z}$, tal que $0 \in A \cap B$ e $r_{A,B}(0) = 1$, prove que $|A + B| \geq |A| + |B| - 1$.

Em 1955 (veja [46]) Scherk publicou uma solução que assume A e B subconjuntos de um grupo abeliano arbitrário (não necessariamente o grupo toroidal). O argumento de Scherk requer pequenas modificações para produzir a demonstração do Teorema 3.13, mas estas modificações só foram estabelecidas após a publicação de dois artigos de Kemperman [[32], [33]] que estabelecem a versão completa do Teorema 3.13. Com efeito, no segundo dos dois artigos, Kemperman atribui o teorema a Scherk. Por outro lado, na sua solução do problema de Moser, Scherk indica que o argumento segue as idéias de seu trabalho anterior que foi desenvolvido em conjunto com Kemperman. Com isto em mente, acreditamos que o teorema deve levar os dois nomes.

Como consequência deste teorema, temos o

Corolário 3.14. *Sejam A e B subconjuntos finitos e não-vazios de um grupo abeliano G com $|B| \geq 2$. Se existe $b \in B$ tal que $A+B \neq A+(B \setminus \{b\})$, então $|A+B| \geq |A|+|B|-1$.*

Demonstração. Por hipótese, existe um elemento $g \in A + B$ cuja expressão como soma $g = a + b$, para algum $a \in A$, é única, ou seja, $r_{A,B}(g) = 1$. Assim, pelo Teorema 3.13, temos $r_{A,B}(g) \geq |A| + |B| - |A + B|$, ou seja,

$$|A + B| \geq |A| + |B| - 1.$$

□

Podemos, agora, começar a prova do Teorema 3.5. Na prova vamos considerar essencialmente uma n-partição de conjuntos $A = A_1, \ldots, A_n$ de S que maximiza iterativamente $\sum_{i=1}^{n} |w_i A_i|$, $|\sum_{i=1}^{n} w_i A_i|$ e $\sum_{i=1}^{n} |\phi_H(w_i A_i)|$, onde $\sum_{i=1}^{n} w_i A_i$ é maximalmente H-periódico. Com o uso do Teorema de Kneser, seremos capazes de mostrar que podemos remover algum termo $b \in S$ a partir da partição de conjuntos A deixando a terceira quantidade maximizada inalterada. Se a segunda quantidade maximizada também é preservada, então isto nos permitirá colocar o termo b de volta para a n-partição de conjuntos, de tal modo a preservar a primeira quantidade e aumentar uma das duas quantidades posteriores, uma contradição, a menos que o termo $\phi_H(b)$ esteja contido em cada conjunto $w_i A_i$, caso em que $H = \sum_{i=i}^{n} w_i b + H \subseteq \sum_{i=1}^{n} w_i A_i$ seguirá do Teorema de Kneser, completando a prova. Por outro lado, se remover o termo b a partir do seu conjunto $w_j A_j$ destruir a segunda quantidade maximizada, então usaremos Corolário 3.14 para mostrar que o conjunto $w_j A_j$ adiciona localmente muitos elementos para o conjunto soma $\sum_{i=1}^{n} w_i A_i$. Um argumento extremo será então usado para mostrar que em ambos os casos deve haver um termo de S que pode ser removido de A preservando as duas quantidades posteriores maximizadas, ou então haverá muitos conjuntos $w_i A_i$ que adicionam localmente muitos elementos em $\sum_{i=1}^{n} w_i A_i$, o suficiente para que possamos concluir que o conjunto soma $\sum_{i=1}^{n} w_i A_i$ tem cardinalidade grande o suficiente para representar cada elemento de G.

Para demonstrarmos o Teorema 3.5 vamos enunciar alguns resultados particulares. Para todos estes resultados vamos considerar m, k e $n \geq 2$ inteiros positivos, uma sequência S de $m+n-1$ elementos de um grupo abeliano não trivial G que possui ordem m e expoente k e $W = (w_i)_{i=1}^n$ é uma sequência de números inteiros cuja soma é zero módulo k.

Lema 3.15. *Se existe $x \in S$ cuja multiplicidade seja maior ou igual a $n+1$, então podemos concluir as teses do Teorema 3.5.*

Demonstração. Se existe $x \in S$ cuja multiplicidade seja no mínimo $n+1$, então S não possui uma n-partição, pois, caso contrário, existiria um índice $j \in \{1, 2, \ldots, n\}$ tal que a multiplicidade de x em A_j seria maior ou igual a 2, o que é um absurdo dada a definição de n-partição de uma sequência.

Além disso, dada a sequência $W = (w_i)_{i=1}^n$, com $w_i \in \mathbb{Z}$, para todo $i = 1, 2, \ldots, n$, e $\sum_{i=1}^n w_i \equiv 0 (mod\ k)$, basta tomarmos $(b_i)_{i=1}^n$ onde $b_i = x$, para todo $i = 1, 2, \ldots, n$, e assim teremos

$$\sum_{i=1}^{n} w_i.b_i = \sum_{i=1}^{n} w_i.x = x.\sum_{i=1}^{n} w_i = x.(t.k) = t.(k.x) = 0$$

donde podemos concluir a demonstração do Teorema 3.5. □

Lema 3.16. *Se existe uma n-partição $A = A_1, A_2, \ldots, A_n$ de S de tal maneira que $\sum_{i=1}^n |w_i A_i|$ seja maximal e, além disso, $|w_i A_i| < |A_i|$ para todo i, então podemos concluir as teses do Teorema 3.5.*

Demonstração. Em primeiro lugar, observamos que a segunda parte do Teorema 3.5 se verifica, pois não existe uma n-partição $A^* = A_1^*, A_2^*, \ldots, A_n^*$ tal que $|w_i A_i^*| = |A_i^*|$. De fato, se existisse tal n-partição teríamos $\sum_{i=1}^n |w_i A_i^*| > \sum_{i=1}^n |w_i A_i|$, o que seria uma contradição à maximalidade de $\sum_{i=1}^n |w_i A_i|$.

Dado um índice $j \in \{1, 2, \ldots, n\}$, como $|w_j A_j| < |A_j|$, tomemos $b, b' \in A_j$ tais que $w_j b = w_j b'$ e $b \neq b'$.

Se existisse um índice r tal que $w_r b \notin w_r A_r$, então a n-partição $A' = A_1', A_2', \ldots, A_n'$ dada por $A_j' = A_j \setminus \{b\}$, $A_r' = A_r \cup \{b\}$ e $A_i' = A_i$ para $i \neq j, r$ nos forneceria $|w_j A_j'| = |w_j A_j|$, $|w_r A_r'| = |w_r A_r| + 1$ e $|w_i A_i'| < |w_i A_i|$ para $i \neq j, r$ contradizendo a maximalidade de $\sum_{i=1}^n |w_i A_i|$.

Assim, podemos assumir $w_i b \in w_i A_i$, para todo $i \in \{1, 2, \ldots, n\}$ e podemos escolher $(b_i)_{i=1}^n$ de forma que $w_i b_i = w_i b$, para todo $i \in \{1, 2, \ldots, n\}$, de onde temos

$$0 = \sum_{i=1}^{n} w_i = \left(\sum_{i=1}^{n} w_i\right).b = \sum_{i=1}^{n} w_i b = \sum_{i=1}^{n} w_i b_i \in \sum_{i=1}^{n} w_i A_i,$$

completando a demonstração do Teorema 3.5. □

Lema 3.17. *Se existe uma n-partição $A = A_1, A_2, \ldots, A_n$ de S de tal maneira que $|w_i A_i| = |A_i|$, para todo $i \in \{1, 2, \ldots, n\}$, e, além disso, $|\sum_{i=1}^{n} w_i A_i| \geq m$, então podemos concluir as teses do Teorema 3.5.*

Demonstração. Como $|\sum_{i=1}^{n} w_i A_i| \geq m$, então $\sum_{i=1}^{n} w_i A_i = G$ e assim

$$0 \in G = \sum_{i=1}^{n} w_i A_i,$$

ou seja, existe uma subsequência $(b_i)_{i=1}^{n}$ de S, onde cada $b_i \in A_i$, tal que $\sum_{i=1}^{n} w_i b_i = 0$ e assim completamos a demonstração da primeira parte do Teorema 3.5.

Para demonstrarmos a segunda parte, basta escolhermos $H = G \subseteq \sum_{i=1}^{n} w_i A_i$ e, assim, teminamos a demonstração. □

Lema 3.18. *Se existe uma n-partição $A = A_1, A_2, \ldots, A_n$ de S de tal maneira que $|w_i A_i| = |A_i|$, para todo $i \in \{1, 2, \ldots, n\}$, e, além disso, $|\sum_{i=1}^{n} w_i A_i| < m$, então podemos concluir a desigualdade*

$$\left|\sum_{i=1}^{n} w_i A_i\right| < \sum_{i=1}^{n} |w_i A_i| - n + 1. \tag{3.1}$$

Demonstração. Como $|\sum_{i=1}^{n} w_i A_i| < m$ e ainda temos as hipóteses $|S| = m + n - 1$ e $|w_i A_i| = |A_i|$, para todo $i = 1, 2, \ldots, n$, então $\sum_{i=1}^{n} |w_i A_i| = \sum_{i=1}^{n} |A_i| = |S|$ e, portanto,

$$\begin{aligned}
\left|\sum_{i=1}^{n} w_i A_i\right| &< m \\
&= |S| - n + 1 \\
&= \sum_{i=1}^{n} |A_i| - n + 1 \\
&= \sum_{i=1}^{n} |w_i A_i| - n + 1
\end{aligned}$$

e assim temos

$$\left|\sum_{i=1}^{n} w_i A_i\right| < \sum_{i=1}^{n} |w_i A_i| - n + 1.$$

□

Lema 3.19. *Suponha que exista uma n-partição $A = A_1, A_2, \ldots, A_n$ de S, com $|w_iA_i| = |A_i|$, para todo $i \in \{1, 2, \ldots, n\}$, e $|\sum_{i=1}^n w_iA_i| < m$, então $\sum_{i=1}^n w_iA_i$ é maximalmente H-periódico para algum subgrupo H próprio e não trivial de G.*

Demonstração. Tome o subgrupo $H = H(\sum_{i=1}^n w_iA_i)$ de G, que é o estabilizador de $\sum_{i=1}^n w_iA_i$. Assim, $\sum_{i=1}^n w_iA_i$ é maximalmente H-periódico. Vamos mostrar que H é próprio e não trivial em G.

Pelo Lema 3.18, temos

$$\left|\sum_{i=1}^n w_iA_i\right| < \sum_{i=1}^n |w_iA_i| - n + 1.$$

Por outro lado, aplicando o Teorema de Kneser (Teorema 3.11), temos

$$\left|\sum_{i=1}^n \phi_H(w_iA_i)\right| \geq \sum_{i=1}^n |\phi_H(w_iA_i)| - n + 1.$$

Portanto, temos

$$\begin{aligned}
\sum_{i=1}^n |\phi_H(w_iA_i)| - n + 1 &\leq \left|\sum_{i=1}^n \phi_H(w_iA_i)\right| \\
&= \left|\phi_H\left(\sum_{i=1}^n w_iA_i\right)\right| \\
&= \left|\left(\sum_{i=1}^n w_iA_i\right) + H\right| : |H| \\
&= \left|\sum_{i=1}^n w_iA_i\right| : |H| \\
&< \left(\sum_{i=1}^n |w_iA_i| - n + 1\right) : |H| \\
&< \sum_{i=1}^n |w_iA_i| - n + 1
\end{aligned}$$

Desta desigualdade, temos $\sum_{i=1}^n |\phi_H(w_iA_i)| < \sum_{i=1}^n |w_iA_i|$. Se, de fato, $H = \{0\}$, então teríamos a igualdade. Portanto H é não trivial em G.

Por outro lado, se $H = G$, pelo ítem **(ii)** da Proposição 1.13, temos

$$|\sum_{i=1}^{n} w_i A_i + H| = |\sum_{i=1}^{n} w_i A_i|$$

um múltiplo de $|H| = |G| = m$, contrariando a hipótese $|\sum_{i=1}^{n} w_i A_i| < m$. Portanto, H é um subgrupo próprio de G.

□

Lema 3.20. *Se existe uma n-partição $A = A_1, A_2, \ldots, A_n$ de S tal que $|w_i A_i| = |A_i|$, para todo $i \in \{1, 2, \ldots, n\}$, $|\sum_{i=1}^{n} w_i A_i| < m$ e ainda $\sum_{i=1}^{n} w_i A_i$ é maximalmente H-periódico para algum subgrupo H próprio e não trivial de G, então existe algum índice $j \geq 2$ tal que $w_j A_j$ não contém um elemento que é o único de sua H-classe em $w_j A_j$.*

Demonstração. Suponha que todo $w_i A_i$, com $i \geq 2$, contém um elemento que é o único de sua classe em G/H, então afirmamos que existem ao menos $(n-1).(|H|-1)$ *H-holes* entre todos os conjuntos $w_i A_i$. Para justificarmos esta afirmação, observemos que o ítem **(b)** do Corolário 3.12 nos garante que o número de *H-holes* em cada $w_i A_i$, para $i = 2, 3, \ldots, n$, é dado por

$$\rho_i = |w_i A_i + H| - |w_i A_i| \geq |H| - 1.$$

Como este resultado vale para todos os conjuntos $w_i A_i$ para $2 \leq i \leq n$ então o número total de *H-holes* entre os conjuntos $w_i A_i$, $i = 2, 3, \ldots, n$, é dado por

$$\sum_{i=2}^{n} \rho_i \geq (n-1).(|H|-1).$$

Tomando $\rho = \sum_{i=1}^{n} \rho_i$ o número total de *H-holes* entre os conjuntos $w_i A_i$, $i = 1, 2, \ldots, n$ e usando ítem **(c)** do Corolário 3.12, temos

$$\begin{aligned}\left|\sum_{i=1}^{n} w_iA_i\right| &\geq \sum_{i=1}^{n}|w_iA_i| - (n-1)|H| + \rho \\ &\geq \sum_{i=1}^{n}|w_iA_i| - (n-1)|H| + \sum_{i=2}^{n}\rho_i \\ &\geq \sum_{i=1}^{n}|w_iA_i| - (n-1)|H| + (n-1)(|H|-1) \\ &= \sum_{i=1}^{n}|w_iA_i| - (n-1)|H| + (n-1)|H| - n + 1 \\ &= \sum_{i=1}^{n}|w_iA_i| - n + 1,\end{aligned}$$

o que contradiz a inequação (3.1) no Lema 3.18. □

Lema 3.21. *Se a sequência S possui uma n-partição $A = A_1, A_2, \ldots, A_n$ de S de tal maneira que $|w_iA_i| = |A_i|$, para todo $i \in \{1, 2, \ldots, n\}$, $|\sum_{i=1}^{n} w_iA_i| < m$, $\sum_{i=1}^{n} w_iA_i = X \subseteq G$ é maximalmente H-periódico, para algum subgrupo H de G próprio e não trivial e, além disso, A foi escolhida dentre todas as n-partições de S com estas propriedades tal que $\sum_{i=1}^{n}|\phi_H(w_iA_i)|$ é maximal, então a equação*

$$\sum_{i=1}^{j} w_iA_i = \sum_{i=1}^{j-1} w_iA_i + w_j.(A_j \setminus \{b\}), \tag{3.2}$$

para algum $b \in A_j$ tal que $\phi_H(w_jA_j) = \phi_H(w_j(A_j \setminus \{b\}))$, é válida.

Demonstração. Pelo Lema 3.20, existe um índice $j \geq 2$ tal que w_jA_j não contém um elemento que é o único de sua H-classe em w_jA_j.

Agora, vamos supor que a equação (3.2) não seja válida. Pelo Corolário 3.14, temos

$$\left|\sum_{i=1}^{j} w_iA_i\right| \geq \left|\sum_{i=1}^{j-1} w_iA_i\right| + |w_jA_j| - 1. \tag{3.3}$$

Seja l, onde $2 \leq l \leq n$, o menor inteiro tal que podemos reindexar w_iA_i de que forma que

$$\left|\sum_{i=1}^{k} w_iA_i\right| \geq \left|\sum_{i=1}^{k-1} w_iA_i\right| + |w_kA_k| - 1 \quad , \quad \text{para todo } k \geq l. \tag{3.4}$$

Pelas conclusões dos dois últimos parágrafos e usando a reindexação, se necessário, podemos assumir $j = n$ no parágrafo anterior e, assim, segue que l existe. Além disso,

$$\left|\sum_{i=1}^{l-1} w_i A_i\right| < \sum_{i=1}^{l-1} |w_i A_i| - (l-1) + 1 \tag{3.5}$$

pois, caso contrário, poderíamos aplicar (3.4) iterativamente e teríamos

$$\left|\sum_{i=1}^{n} w_i A_i\right| \geq \sum_{i=1}^{n} |w_i A_i| - (n-1)$$

que contradiz a inequação (3.1) do Lema 3.18.

Se $\sum_{i=1}^{l-1} w_i A_i$ fosse não periódico, ou seja, o estabilizador $H\left(\sum_{i=1}^{l-1} w_i A_i\right) = \{0\}$, então o Corolário 1.20 nos daria

$$\left|\sum_{i=1}^{l-1} w_i A_i\right| \geq \sum_{i=1}^{l-1} |w_i A_i| - (l-2),$$

contrariando a inequação (3.5). Assim, pela maximalidade de H, segue que $\sum_{i=1}^{l-1} w_i A_i$ é maximalmente H^*-periódico para algum subgrupo não-trivial $H^* \leq H$.

Note que (3.5) só pode fornecer $l - 1 \geq 2$. Agora, suponha que cada conjunto $w_i A_i$ com $2 \leq i \leq l-1$ contém um elemento que é único de sua H^*-classe em $w_i A_i$, então haverá, no mínimo, $(l-2).(|H^*|-1)$ H^*-*holes* entre os conjuntos $w_i A_i$ com $i \leq l-1$, daí o ítem **(c)** do Corolário 3.12 implica

$$\begin{aligned}\left|\sum_{i=1}^{l-1} w_i A_i\right| &\geq \sum_{i=1}^{l-1} |w_i A_i| - (l-2)|H^*| + (l-2).(|H^*|-1) \\ &= \sum_{i=1}^{l-1} |A_i| - (l-1) + 1\end{aligned}$$

e isto contradiz (3.5). Portanto, deve existir A_j com $2 \leq j \leq l-1$, tal que $w_j A_j$ não contém um elemento que é o único elemento de sua H^*-classe em A_j.

Assim, como $H^* \leq H$, então $|\phi_H(w_j A_j)| < |w_j A_j|$ para algum índice j, com $2 \leq j \leq l-1$. Assim, usando a reindexação podemos assumir $j = l-1$ e daí (3.3) vale com $j = l-1$. Portanto, em vista de (3.4), temos uma contradição quanto a minimalidade de l. □

Lema 3.22. *Se existe uma n-partição $A = A_1, A_2, \ldots, A_n$ de S de tal maneira que $|w_i A_i| = |A_i|$, para todo $i \in \{1, 2, \ldots, n\}$, $|\sum_{i=1}^{n} w_i A_i| < m$, $\sum_{i=1}^{n} w_i A_i = X \subseteq G$ é*

maximalmente H-periódico para algum subgrupo H de G próprio e não trivial e, além disso, A foi escolhida dentre todas as n-partições de S que satisfazem estas propriedades tal que $\sum_{i=1}^{n} |\phi_H(w_iA_i)|$ é maximal, então podemos concluir as teses do Teorema 3.5.

Demonstração. Pelo Lema 3.20, existe um índice $j \geq 2$ tal que w_jA_j não contém um elemento que é o único de sua $|H|$-classe em w_jA_j. Além disso, o Lema 3.21 nos garante que é válida a equação (3.2),

$$\sum_{i=1}^{j} w_iA_i = \sum_{i=1}^{j-1} w_iA_i + w_j.(A_j \setminus \{b\}),$$

para algum $b \in A_j$ tal que $\phi_H(w_jA_j) = \phi_H(w_j(A_j \setminus \{b\}))$.

Agora, se existe um índice r tal que $\phi_H(w_rb) \notin \phi_H(w_rA_r)$, então tomamos a n-partição de conjuntos $A^* = A_1^*, A_2^*, \ldots, A_n^*$ definida por

$$A_j^* = A_j \setminus \{b\} \quad , \quad A_r^* = A_r \cup \{b\} \quad \text{e} \quad A_i^* = A_i, \text{ para } i \neq j, r.$$

A partição A^* claramente contradiz a maximalidade de $\sum_{i=1}^{n} |\phi_H(w_iA_i)|$.

Podemos supor então que $\phi_H(w_ib) \in \phi_H(w_iA_i)$ para todo i. Assim, como $\sum_{i=1}^{n} w_i \equiv 0(mod\ k)$, então $0_{G/H} = \sum_{i=1}^{n} \phi_H(w_ib) \in \sum_{i=1}^{n} \phi_H(w_iA_i)$. Assim, como $\sum_{i=1}^{n} w_iA_i$ é maximalmente H-periódico, segue $H \subseteq \sum_{i=1}^{n} w_iA_i$, pois

$$H \subseteq \left(\sum_{i=1}^{n} w_iA_i\right) + H = \sum_{i=1}^{n} w_iA_i$$

e, assim, completamos a demonstração do Teorema 3.5. □

3.1.1 Demonstração do Teorema de EGZ com Peso

Vamos agora, usar todas as ferramentas que definimos até agora, para demonstrar o Teorema 3.5 (Teorema de EGZ com Peso).

Pelo Lema 3.15, basta considerarmos o caso em que todo elemento de S possui multiplicidade no máximo n. Assim, existe uma n-partição $A = A_1, A_2, \ldots, A_n$ de S. Vamos escolher A de tal maneira que $\sum_{i=1}^{n} |w_iA_i|$ seja maximal.

Sendo $|w_iA_i| \leq |A_i|$ para todo i, podemos usar o Lema 3.16 e verificar apenas o caso em que $|w_iA_i| = |A_i|$, para todo $i \in \{1, 2, \ldots, n\}$.

Além disso, vamos escolher a n-partição A de tal forma que $|w_iA_i| = |A_i|$, para todo i, e $|\sum_{i=1}^{n} w_iA_i|$ seja maximal. Pelo Lema 3.17, podemos nos ater somente ao caso em que $|\sum_{i=1}^{n} w_iA_i| < m$.

Assumindo $|\sum_{i=1}^{n} w_i A_i| < m$, temos a equação (3.1) dada no Lema 3.18,

$$\left|\sum_{i=1}^{n} w_i A_i\right| < \sum_{i=1}^{n} |w_i A_i| - n + 1.$$

Pelo Lema 3.19, segue que $\sum_{i=1}^{n} w_i A_i = X \subseteq G$ é maximalmente H-periódico para algum subgrupo H de G próprio e não trivial. Suponhamos, agora, que A foi escolhida entre todas as n-partições de conjuntos $A' = A'_1, A'_2, \ldots, A'_n$ de S que satisfazem $|w_i A'_i| = |A'_i|$, para todo $i = 1, 2, \ldots, n$, e $\sum_{i=1}^{n} w_i A'_i = X$ tal que $\sum_{i=1}^{n} |\phi_H(w_i A'_i)|$ é maximal.

Pelo Lema 3.20, podemos considerar que, para algum índice $j \geq 2$, $w_j A_j$ não contém um elemento que é o único de sua H-classe em $w_j A_j$, pois, caso contrário, haveria uma contradição com a inequação (3.1).

Agora, pelo Lema 3.21, a equação (3.2),

$$\sum_{i=1}^{j} w_i A_i = \sum_{i=1}^{j-1} w_i A_i + w_j.(A_j \setminus \{b\}),$$

para algum $b \in A_j$ tal que $\phi_H(w_j A_j) = \phi_H(w_j(A_j \setminus \{b\}))$, é válida.

Por fim, aplicando o Lema 3.22, verificamos que o Teorema 3.5 está completamente demonstrado.

3.2 Considerações Finais

Dentro da teoria de soma-zero ainda existem inúmeros problemas em aberto, onde os principais problemas tratam do cálculo dos invariantes, definidos na Introdução deste trabalho, para grupos abelianos finitos específicos e, também, das relações entre estes invariantes.

Harborth provou, em [26], os seguintes resultados:

(1) $2^r(n-1)+1 \leq s(C_n^r) \leq n^r(n-1)+1$, onde $C_n^r = C_n \oplus \ldots \oplus C_n$, r vezes;

(2) $2^{r-1}(n-1)+1 \leq g(C_n^r) \leq n^{r-1}(n-1)+1$;

(3) $s(C_3^r) = 2g(C_3^r) - 1$;

(4) Se n é par então $g(C_n^r) \geq 2^{r-1}n + 1$ e se n é ímpar então $g(C_n) = n$;

(5) $s(C_{mn}^r) \leq \min\{(s(C_m^r)-1)n + s(C_n^r), (s(C_n^r)-1)m + s(C_m^r)\}$;

(6) Além de valores exatos destes invariantes para grupos específicos.

Em 1983, A. Kemnitz em [31] provou que $g(C_p^2) = 2p - 1$, para $p \in \{3, 5, 7\}$, e conjecturou que $s(C_n^2) = 4n - 3$. O que nos diz que o limite inferior dado em (1) acima é atingido. Ele também provou que basta considerarmos n primo para a demonstração desta conjectura. Alguns resultados para o invariante $g(C_3^r)$ foram obtidos para r fixo e consequentemente para $s(C_3^r)$ por (3) acima. Os valores de $g(C_3^3) = 10$ e $g(C_3^4) = 21$ estão em vários trabalhos na internet; aqui mencionamos apenas o programa de computador de Knuth (ver [35]). O valor de $g(C_3^5) = 46$ pode ser encontrado em [14]. Para $r = 6$, não temos o valor exato, mas temos o seguinte resultado $112 \leq g(C_3^6) \leq 114$, sendo que o limite inferior pode ser encontrado aplicando a elementar duplicação devido à Mukhopadhyay [40] ao 56 pontos do cap de Hill em $PG(5, 3)$ [29] e [30] e o limite superior pode ser encontrado em [9]. Para um limite geral, com $r \in \mathbb{N}$, temos o resultado de R. Menshulam que pode ser encontrado em [39].

Em 2004, no trabalho de Gao e Thangadurai em [21] está provado que $g(C_p^2) = 2p-1$, para todo $p \geq 67$, e dai temos a seguinte conjectura:

$$g(C_n^2) = \begin{cases} 2n - 1, & \text{se n é ímpar} \\ 2n + 1, & \text{se n é par} \end{cases}$$

A conjectura para o caso n par é motivada pelo limite inferior dado pela sequência $S = ((0, 0), (0, 1), \ldots, (0, n - 1), (1, 0), (1, 1), \ldots, (1, n - 1))$ que não possui subsequência de comprimento n cuja soma é o zero de C_n^2. Para o caso n ímpar a sequência para o limite inferior é $S = ((0, 0), (0, 1), \ldots, (0, n - 2), (1, 1), (1, 2), \ldots, (1, n - 1))$.

Em 2003, C. Reiher provou a veracidade da conjectura de Kemnitz, em artigo que só foi publicado em 2007 (ver [45]).

Após o resultado de Reiher iniciou-se o estudo para grupos de posto 3 e em 2007 Gao et al provaram em [22] que

$$\begin{array}{ll} \eta(C_n^3) + n - 1 = s(C_n^3) = 9n - 8, & \text{se } n = 3^a \cdot 5^b, \text{ onde } a, b \in \mathbb{N} \cup \{0\} \\ \eta(C_n^3) + n - 1 = s(C_n^3) = 8n - 7, & \text{se } n = 2^a \cdot 3, \text{ onde } a \in \mathbb{N} \end{array}$$

A partir deste resultado surgiu a seguinte conjectura

$$s(C_n^3) = \begin{cases} 9n - 8, & \text{se n é ímpar} \\ 8n - 7, & \text{se n é par} \end{cases}$$

Neste mesmo artigo, Gao *et al* provaram que $s(G) = \eta(G) + n - 1$, onde n é o expoente de G, para grupos G específicos, com algumas hipóteses adicionais sobre o grupo G e sobre o invariante $s(G)$. A relação $s(G) = \eta(G) + n - 1$, onde n é o expoente de G, é uma conjectura de outro artigo de Gao que pode ser encontrada em [20].

Outro resultado obtido, ainda em 2007, por Edel *et al* em [13] é $s(C_n^4) \geq 20n - 19$,

para n ímpar, e a igualdade se verifica para $n = 3^a$, com $a \in \mathbb{N}$. Neste artigo também é feito um longo estudo de caps maximais em geometria finita (um cap maximal é o maior subconjunto de $AG(r, q)$ que não possui três pontos colineares, $AG(r, q)$ é a parte afim do espaço projetivo $PG(r, q)$ sobre $\mathbb{F}_q$), além de ter uma demonstração mais simples para o seguinte resultado sobre C_n^3: se n é ímpar, então existe uma subsequência T de S, de comprimento 9, tal que T^{n-1} não tem subsequência de comprimento n cuja a soma de seus elementos seja o zero de C_n^3; em particular, $\eta(C_n^3) \geq 8n - 7$ e $s(C_n^3) \geq 9n - 8$. Este resultado já havia sido provado por C. Elsholtz em [16], mas de uma forma mais complicada.

Em 2008, Edel provou, em [15], que $s(C_n^5) \geq 42n - 41$, $s(C_n^6) \geq 96n - 95$ e $s(C_n^7) \geq 196n - 195$ usando, ainda, a teoria de caps maximais em geometria finita.

Caso o leitor tenha interesse em conhecer outros resultados dentro da teoria de soma zero para grupos abelianos finitos, indicamos os estudos [3], [4], [5], [6], [48], [49] e, principalmente, o artigo (survey) de Weidong Gao e Alfred Geroldinger [18], no qual são apresentadas varias relações e propriedades de vários invariantes para grupos abelianos finitos e seus problemas inversos relacionados.

Referências Bibliográficas

[1] S.D. Adhikari, Y.G. Chen, J.B. Friedlander, S.V. Konyagin, F. Pappalardi, Contributions to zero-sum problems, *Discrete Math.*, 306 (2006) 1-10.

[2] S.D. Adhikari, "Aspects of Combinatorics and Combinatorial Number Theory", Narosa, New Delhi, 2002.

[3] S. D. Adhikari, R. Balasubramanian, F. Pappalardi, P. Rath, Some zero-sum constants with weights, *Proc. Indian Acad. Sci. (Math. Sci.)*, 118(2) (2008) 183-188.

[4] S. D. Adhikari, R. Balasubramanian, P. Rath, Some combinatorial group invariants and their generalizations with weights. *Additive combinatorics, (Eds. Granville, Nathanson, Solymosi)*, 327-335, CRM, *Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI,* 2007.

[5] S. D. Adhikari, Y. G. Chen, Davenport constant with weights and some related questions II. *J. Combin. Theory, Ser.*, A115(1) (2008) 178-184.

[6] S. D. Adhikari, C. David, J. J. Urroz, Generalizations of some zero-sum theorems, *Integers Electron Comb. Number Theory*, 8 (2008) A52.

[7] N. Alon, A. Bialostocki and Y. Caro: The Extremal cases in the Erdös-Ginzburg-Ziv theorem, unpublished.

[8] A. Bialostocki, P. Dierker, On the Erdös-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings. *Discrete Math.* 110 (1992), no. 1-3, 1-8.

[9] J. Bierbrauer, Y. Edel. Bounds on affine caps. *J. Comb. Des.*, 10 (2002) 111-115.

[10] Y. Caro, Zero-sum subsequences in abelian non-cyclic groups, *Israel J. Math.* 92 (1995), no. 1-3, 221-233.

[11] Y. Caro, Zero-sum problems - a survey, *Discrete Math.* 152(1-3) (1996) 93-113.

[12] H. Davenport, On the addition of residue classes, *J. London Math. Soc.*, 22 (1947) 100-101.

[13] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, L.Rackham, Zero-sum problems in finite abelian groups and affine caps. *Quart. J. Math.*, 58 (2007) 159-186.

[14] Y. Edel, S. Ferret, I. Landjev, L. Storme, The classification of the largest caps in $AG(5,3)$. *J. Comb. Theory*, 99 (2002) 95-110.

[15] Y. Edel, Sequences in abelian groups G of odd order without zero-sum subsequences of length $exp(G)$. *Des. Codes Cryptogr.*, 47 (2008) 125-134.

[16] C. Elsholtz. Lower bounds for multidimensional zero sums. *Combinatorica*, 24 (2004) 351-358.

[17] P. Erdös, A. Ginzburg, A. Ziv, Theorem in additive number theory, *Bull. Res. Council Israel*, 10F (1961) 41-43.

[18] W. D. Gao, A. Geroldinger, Zero-sum problem in finite abelian groups: A survey. *Expositiones Mathematicae*, 24(6) (2006) 337-369.

[19] W. Gao e X. Jin, Weighted sums in finite cyclic groups, *Discrete Math.* 283(1-3) (2004) 243-247.

[20] W. D. Gao. On zero-sum subsequence of restricted size. II. *Discrete Math.*, 271(1-3) (2003) 51-59.

[21] W. D. Gao, R. Thangadurai. A variant of Kemnitz conjecture. *J. Comb. Theory*, Ser. A107 (2004) 69-86.

[22] W. D. Gao, Q. H. Hou, W. A. Schmid, R. Thangadurai. On short zero-sum subsequences II. *Integers Electron Comb. Number Theory*, 7 (2007) A21.

[23] D. J. Grynkiewicz, A weighted Erdös-Ginzburg-Ziv Theorem, *Combinatorica* 26 (4) (2006) 445-453.

[24] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, A Weighted Generalization of Two Theorems of Gao, *Ramanujan J.* 28 (2012) 323-340.

[25] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, Representation of finite abelian group elements by subsequence sums, *Journal de Théorie des Nombres de Bordeaux* 21 (2009) 559-587.

[26] H. Harborth, Ein Extremalproblem für Gitterpunkte, *J. Reine Angew. Math.* 262 (1973) 356-360.

[27] Y. O. Hamidoune, On weighted sums in abelian groups, *Discrete Math.* 162 (1996) 127-132.

[28] Y. O. Hamidoune, On weighted sequence sums, *Comb. Prob. Comput.* 4 (1995) 363-367.

[29] R. Hill. On the largest size of a cap in $S_{5,3}$. *Atti Accad. Naz. Lincei Rend.*, 54 (1973) 378-384.

[30] R. Hill. Caps and Codes. *Discrete Math.*, 22 (1978) 111-137.

[31] A. Kemnitz, On a lattice point problem. *Ars Combinatoria* 16 (1983) 151-160.

[32] J. H. B. Kemperman, On complexes in a semigroup. *Indag. Math.* 18 (1956) 247-254.

[33] J. H. B. Kemperman, On small sumsets in an abelian group. *Acta Math.* 103 (1960) 63-88.

[34] M. Kneser, Abschätzungen der asymptotischen Dichte von Summenmengen. *Math. Zeitschr. (in German)* 58 (1953) 459-484.

[35] D. E. Knuth, *Computerprogramme.* http://www-cs-faculty.stanford.edu/knuth/programs/setset-all.w.

[36] A. Lemos, Problemas de Soma Zero com Peso sobre Grupos Abelianos Finitos. *Tese de Doutorado,* UnB, 2010.

[37] A. Lemos, H. Godinho, D. Marques, Weighted zero-sum problems over C_3^r, *Algebra and Discrete Mathematics*, 15 (2013) 201-212.

[38] V. F. Lev, Restricted set addition in Abelian groups: results and conjectures. *Journal de Théorie des Nombres de Bordeaux* 17 (2005) 181-193.

[39] R. Meshulam. On subsets of finite abelian groups with no 3-term arithmetic progressions. *J. Comb. Theory*, A71 (1995) 168-172.

[40] A. C. Mukhopadhyay. Lower bounds on $m_t(r, s)$. *J. Comb. Theory*, Ser. A25 (1978) 1-13.

[41] M. B. Nathanson, "Additive Number Theory. Inverse Problems and the Geometry of Sumsets", Graduate Texts in Mathematics, 165, Springer-Verlag, New York, 1996.

[42] T. C. S. Neto, Problemas de Soma Zero e o Número Crítico. *Dissertação de Mestrado,* UnB, 2007.

[43] J. E. Olson, A combinatorial problem on finite abelian groups I, *Jornal of Number Theory* 1 (1969) 8-10.

[44] J. E. Olson, A combinatorial problem on finite abelian groups II. *Jornal of Number Theory* 1 (1969) 195-199.

[45] C. Reiher. On Kemnitz'conjecture concerning lattice points in the plane. *Ramanujan J.*, 13 (2007) 333-337.

[46] P. Scherk, Distinct elements in a set of sums (solution to Problem 4466). *American Math. Monthly* 62 (1) (1955) 46-47.

[47] R. Thangadurai, A variant of Davenport's constant. *Proc. Indian Acad. Sci. (Math. Sci.)* 117 (2007) 147-158.

[48] X. Xia, Two generalized constants related to zero-sum problems for two special sets. *Integers Electron Comb. Number Theory* 7 (2007) A52.

[49] X. Xia, Z. Li, Some Davenport constants with weights and Adhikari and Rath's conjecture. *Ars Combin.* 88 (2008) 83-95.

[50] P. Yuan, X. Zeng. Davenport constant with weights. *European J. Combin.* 31 (2010) 677-680.