LUANA SOUZA MARQUES

MÉTODO ISOPERIMÉTRICO EM TEORIA ADITIVA DOS NÚMEROS

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
2018

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

T
M357m
2018

Marques, Luana Souza, 1990-
Método isoperimétrico em teoria aditiva dos números / Luana Souza Marques. – Viçosa, MG, 2018.
vii, 35 f. ; 29 cm.

Orientador: Bhavinkumar Kishor Sinh Moriya.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f. 34-35.

1. Teoria aditiva dos números. 2. Cauchy-Davenport, Teorema de. 3. Vosper, Teorema de. 4. Desigualdades isoperimétricas. I. Universidade Federal de Viçosa. Departamento de Matemática. Programa de Pós-Graduação em Matemática. II. Título.

CDD 22. ed. 512.7

LUANA SOUZA MARQUES

MÉTODO ISOPERIMÉTRICO EM TEORIA ADITIVA DOS NÚMEROS

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

APROVADA: 04 de julho de 2018.

Sávio Ribas

Sávio Ribas

Sônia Maria Fernandes

Abílio Lemos Cardoso Júnior
(Coorientador)

Bhavinkumar Kishor Sinh Moriya
(Orientador)

Dedico este trabalho à minha família, em especial à minha mãe Seilde, pelo exemplo de força e determinação. E ao meu noivo Rondinei, pelo apoio incondicional.

RESILIÊNCIA: Capacidade de superar, de recuperar-se de adversidades.

Dicionário Aurélio

Agradecimentos

Agradeço à minha mãe Seilde, que sempre me incentivou a estudar, e me apoiou em todos os momentos. Todas as conquistas na minha vida são graças à ela. Agradeço também as minhas irmãs, Rafaela e Daniele, por todas as alegrias proporcionadas, e a minha sobrinha Larinha, pelo lindo sorriso.

Ao meu noivo, Rondinei, por todo apoio ao longo desses oito anos juntos, todos os ensinamentos, todo amor e carinho que tem dedicado a mim, muito do que sou hoje devo à ele.

Aos professores do DMA-UFV, que foram fundamentais em meu processo de formação.

Aos amigos de curso, que tornaram essa minha caminhada mais agradável e alegre, em especial a Vanessa, minha companheira em todos os momentos, Javier minha agenda cultural, Vângellis por várias parcerias, Verônica por ser uma excelente parceira de apartamento, e a todos da minha turma por todas as conversas, almoços e boas risadas que me proporcionaram.

Ao João Marcos Viana, secretário da pós-graduação durante boa parte do meu curso, por toda a disponibilidade, vontade de ajudar, chocolates salvadores e por ser essa pessoa maravilhosa que sempre me lembrarei como muito carinho.

Ao Professor Sávio Ribas, que participou da minha banca e contribuiu de forma significativamente para o meu trabalho, sempre muito prestativo, um exemplo de profissional.

Por fim, agradeço à CAPES pelo apoio financeiro fundamental para a realização deste trabalho.

Resumo

MARQUES, Luana Souza, M.Sc., Universidade Federal de Viçosa, julho de 2018. **Método Isoperimétrico em Teoria Aditiva dos Números**. Orientador: Bhavinkumar Kishor Sinh Moriya. Coorientador: Abílio Lemos Cardoso Júnior.

Neste trabalho, estudamos o Método Isoperimétrico e sua aplicação na Teoria Aditiva dos Números. O Método Isoperimétrico foi desenvolvido por Y. Hamidoune e é um dos métodos mais importantes na Teoria Aditiva dos Números. Um dos problemas mais estudados na Teoria Aditiva dos Números é a soma $A + B$, para subconjuntos dados A, B (de um grupo G) de forma que $|A + B| \geq |A| + |B| - 1$. Vamos apresentar a k-separabilidade e o número k-isoperimétrico do par (G, B), a fim de estudar os problemas relacionados a soma $A + B$. Como consequência do Método Isoperimétrico foram obtidos pelo Hamidoune muitos resultados poderosos, alguns dos quais são os seguintes: Generalização do Teorema de Cauchy-Davenport [2, 3], Teorema de Vosper [20], Brailovski-Freiman [8] e Zemor [21].

Abstract

MARQUES, Luana Souza, M.Sc., Universidade Federal de Viçosa, July, 2018 **Isoperimetric Method in Addition Number Theory**. Adviser: Bhavinkumar Kishor Sinh Moriya. Co-adviser: Abílio Lemos Cardoso Júnior.

In this work, we study the Isoperimetric Method and its application in the Additive Number Theory. The Isoperimetric Method was developed by Y. Hamidoune; is one of the most important methods in Additive Number Theory. One of the most studied problems in the Additive Number Theory is studying sumsets $A+B$, for a given subsets A, B (of a group G) such that $|AB| \geq |A|+|B|-1$. We will be introducing k-separability and k-isoperimetric number of the pair (G, B), in order to study the problems related to sum $A + B$. As consequence of the Isoperimetric Method were obtained by Hamidoune powerful results, some of which are as follows: generalization of Cauchy-Davenport Theorem [2, 3], Vosper's Theorem [20], Brailovski-Freiman [8] and Zemor [21].

Sumário

Introdução **1**

1 Introdução à Teoria Aditiva dos Números **3**

1.1 Adição de Subconjuntos de um Grupo 3

1.2 e-transformada 4

1.3 Teorema de Cauchy-Davenport 5

1.4 Teorema de Erdös-Ginzburg-Ziv 7

1.5 Demonstração de Matt DeVos para o Teorema de Kneser 10

1.6 Teorema de Vosper 14

2 Número Isoperimétrico **19**

2.1 Notações e Terminologias 19

2.2 Resultados Principais 20

3 Aplicações do Método Isoperimétrico **26**

3.1 Generalização do Teorema de Cauchy-Davenport 26

3.2 Problemas Críticos 29

Considerações Finais **33**

Referências Bibliográficas **34**

Introdução

Em Teoria dos Números, a Teoria Aditiva dos Números estuda o comportamento de subconjuntos de um grupo sob a operação de soma, como por exemplo saber qual a quantidade de elementos que possui a soma de dois ou mais subconjuntos ou ainda estudar a quantidade de formas possíveis de expressar um inteiro positivo como a soma de elementos de um certo conjunto.

Os problemas em Teoria Aditiva dos Números são classificados em duas classes, problemas diretos e problemas inversos. Os problemas diretos são problemas em que temos informações sobre os subconjuntos $A_1, A_2, ..., A_n$ e assim obtemos informações sobre a soma $A_1 + A_2 + ... + A_n$. E os problemas inversos, onde sabemos informações sobre o conjunto soma $A_1 + A_2 + ... + A_n$ e assim obtemos informações sobre os A_i's.

Os dois problemas mais famosos nesta área são a Conjectura de Goldbach e o Problema de Waring. A Conjectura de Goldbach [7], proposta pelo matemático Christian Goldbach, é um dos problemas mais antigos não resolvidos da matemática, mais especificamente da Teoria dos Números. Ela diz que todo número par maior que 2 pode ser representado pela soma de dois números primos. Verificações por computador já confirmaram a Conjectura de Goldbach para vários números. No entanto, a demonstração matemática ainda não ocorreu.

Em 1970 Edward Waring propôs a seguinte questão: para cada número natural k, existe associado a ele um número inteiro positivo s, de tal forma que qualquer número natural n possa ser representado pela soma de, no máximo, s potências de ordem k. E este ficou conhecido como "Problema de Waring"que pode ser encontrado no capítulo 4 do livro [16]. Esses problemas clássicos fascinam e inspiram estudos na área.

Assim, o ponto de partida para vários estudos, é a estimativa da cardinalidade da soma $A+B$ e a desigualdade $|A+B| \geq \min(|G|, |A|+|B|-1)$, onde A e B são subconjuntos não vazios de um grupo G de ordem prima, provado por Cauchy [2] em 1813, e redescoberto por Davenport [3] em 1935. E a generalização desse teorema é um dos principais resultados estudados nesse trabalho.

Uma outra ferramenta importante em Teoria Aditiva dos Números, é o Teorema de Kneser [4], que possui o seguinte enunciado: Sejam G um grupo abeliano, $A, B \subseteq G$ finitos e não vazios, com $|A| + |B| \leq |G|$ e $H = H(A + B)$, onde H é o estabilizador de $A + B$. Então $|A + B| \geq |A + H| + |B + H| - |H|$. Um belo resultado sobre soma de subconjuntos finitos de um grupo abeliano, que possui numerosas aplicações, dentre elas mencionamos o Problema de Frobenius [6].

Várias tentativas foram feitas para generalizar o Teorema de Kneser para grupos não-abelianos. O primeiro resultado nessa direção é o Teorema de Diderrich [5], que estabelece que, dado G um grupo multiplicativo e subconjuntos $A, B \subset G$ finito tal que $A + B$ não é a união das classes laterais à esquerda. Suponha além disso que os elementos de B comutam, então $|A + B| \geq |A| + |B| - 1$. Foi observado em [10] que isto é equivalente a generalização do Teorema de Kneser. Porém, mais investigações e alguns exemplos, mostram que a extensão natural ao caso não abeliano falha e podem ser encontrados em [19].

Outro teorema importante é o Teorema de Vosper [20], este é o principal exemplo dos problemas inversos, esse teorema foi demonstrado em 1956, quando Vosper caracterizou os pares de conjuntos críticos, ou seja, os conjuntos tais que a cardinalidade do conjunto soma é menor do que a soma de suas cardinalidades, isto é, $|A + B| < |A| + |B|$.

Neste trabalho tivemos como principal referência o artigo [9] de Yahya Ould Hamidoune (1947-2011). Este matemático forneceu várias contribuições para a matemática. Seu interesse inicial era em Teoria dos Grafos e evoluiu para o desenvolvimento do Método Isoperimétrico e a aplicação do Método Isoperimétrico aos problemas em combinações aditivas. Hamidoune percebeu que muitos resultados clássicos na Teoria Aditiva dos Números poderiam ser reformulados em termos de conectividade dos grafos de Cayley [11]. Inspirado por essa conexão, ele começou a desenvolver o chamado Método Isoperimétrico em Teoria Aditiva e provou vários resultados usando o Método Isoperimétrico [11].

Assim, neste trabalho apresentaremos no primeiro capítulo as demonstrações dos resultados clássicos da Teoria Aditiva dos Números, acima citados, considerando G um grupo aditivo. No segundo desenvolvemos o Método Isoperimétrico, apresentando as definições e propriedades da k-separabilidade e do número k-isoperimétrico do par (G, B), onde B é um subconjunto de um grupo G multiplicativo com a unidade em B.

Por fim, no terceiro apresentamos os resultados obtidos por Hamidoune no artigo [9] que são: a generalização do Teorema de Cauchy-Davenport [2, 3], que ao invés de tomarmos $A, B \subset \mathbb{Z}_p$, tomamos agora em um grupo qualquer e com algumas condições sobre a cardinalidade de B e obtemos assim uma generalização do resultado. Tem-se também o resultado principal provado por Brailovski e Freiman em [8] e uma prova do teorema de adição em característica 2, provada por Zemor em [21].

Além disso, o principal resultado estudado é o seguinte corolário: Seja G um grupo contendo dois subconjuntos finitos A e B tal que $2 \leq \min(|A|, |B|)$. Assuma que cada elemento de $G \setminus \{1\}$ tenha ordem maior ou igual que o $\max(|A|, |B|)$ e $|A + B| = |A| + |B| - 1 < |G| - 1$. Suponha que $1 \in B$ e que G é gerado por B, então existem $x, y, r \in G$ tal que $A = \{xr^i : 0 \leq i \leq |A| - 1\}$ e $B = \{r^i y : 0 \leq i \leq |B| - 1\}$. Aplicando esse resultado à ordem de G prima, obtemos o Teorema de Vosper [20].

Capítulo 1

Introdução à Teoria Aditiva dos Números

Neste capítulo faremos uma introdução à Teoria Aditiva dos Números e apresentaremos os seus teoremas mais clássicos. Inicialmente falaremos da Adição de Subconjuntos de um Grupo, estabelecendo suas principais propriedades, dentre elas a e-trnasformada, que é uma importante ferramenta a ser utilizada nas demonstrações seguintes. Além disso, apresentaremos o Teorema de Couchy-Davenport, que estuda a estimativa da cardinalidade da soma $A+B$ e a desigualdade $|A+B| \geq \min(|G|, |A|+|B|-1)$, onde A e B são subconjuntos não vazios de um grupo G de ordem prima. Exibiremos o Teorema de Erdös-Ginzburg-Ziv, resultado esse que foi um dos pontos de partida para as pesquisas sobre problemas de soma zero. Apresentaremos também o Teorema de Kneser que é um resultado sobre soma de subconjuntos finitos de um grupo abeliano. Por fim, concluiremos este capítulo com o Teorema de Vosper, este é um importante exemplo dos problemas inversos em Teoria Aditiva dos Números. As demonstrações feitas neste capítulo podem ser encontradas nas referências [17] e [18].

1.1 Adição de Subconjuntos de um Grupo

Definição 1.1. *Seja $G = (G, +)$ um grupo aditivo e sejam A e B subconjuntos não vazios de G. O **conjunto soma** é dado por $A+B = \{x+y : x \in A \text{ e } y \in B\}$.*

Definição 1.2. *Para todo elemento $g \in G$, definimos o número de representações de g como soma de elementos de A e B, por $r_{A,B}(g) = |\{g = a+b : (a,b) \in A \times B\}|$, ou seja, $r_{A,B}(g)$ é o número de pares ordenados $(a,b) \in A \times B$ tais que $g = a+b$.*

Exemplo 1.3. *Sejam $G = \mathbb{Z}_6 = \{0,1,2,3,4,5\}$, $A = \{0,1,2\}$ e $B = \{0,1,3\}$ subconjuntos de $\mathbb{Z}_6$. Note que, se $g = 5$ então $r_{A,B}(5) = 1$.*

Lema 1.4. *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 $r_{A,B}(g) \geq t, \quad \forall g \in G$.*

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

Agora, podemos obter o seguinte fato importante, pois para estudar o conjunto $A + B$ devemos nos ocupar apenas com os conjuntos não vazios A e B de G, tais que $|A| + |B| \leq |G|$.

Lema 1.5. *Seja G um grupo abeliano finito e seja A, B subconjuntos não vazios de G, tais que $|A| + |B| > |G|$. Então, $A + B = G$.*

Demonstração. Por hipótese $|A| + |B| - |G| > 0$, segue do lema anterior que $r_{A,B}(g) > 0$. Logo dado $g \in G$, existem $a \in A$ e $b \in B$ tal que $g = a + b$. Assim, $G \subset A + B$. Como a desigualdade contrária é válida, temos $A + B = G$. □

1.2 e-transformada

A e-transformada é de grande utilidade nas demonstrações de muitos resultados na Teoria Aditiva dos Números. Assim, vamos definir e estabelecer algumas propriedades dessa ferramenta.

Definição 1.6. *Seja (A, B) um par ordenado de subconjuntos não vazios de um grupo abeliano G. Para cada $e \in G$, definimos a e-transformada de (A, B) como sendo o par $(A(e), B(e))$ de subconjuntos de G, tais que*

$$A(e) = A \cup (B + e) \text{ e } B(e) = B \cap (A - e).$$

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

Exemplo 1.7. *Considere $e = 2$, $A = \{1, 3, 5\}$ e $B = \{1, 5, 7\}$ em $\mathbb{Z}_9$. Assim, a 2-transformada do par (A, B) é o par $(A(2), B(2))$, tais que $A(2) = \{0, 1, 3, 5, 7\}$ e $B(2) = \{1\}$.*

Lema 1.8. *Sejam A e B subconjuntos não vazios de um grupo finito abeliano G. Para cada $e \in G$, a e-transformada de (A, B) satisfaz as seguintes condições:*

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

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

(iii) $|A(e)| + |B(e)| = |A| + |B|$;

(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 $a' \in (B + e)$.

1. Se $a' \in A$, como $b' \in B(e) \subseteq B \Rightarrow a' + b' \in A + B$.
2. Se $a' \in (B + e)$, logo existe $b \in B$, tal que $a' = b + e$. Como $b' \in B(e) \subseteq (A - e)$, ou seja, $b' \in B(e) \subseteq (A - e)$ o que implica que existe $a \in A$, tal que $b' = a - e$.

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

(ii) Temos, $A(e) \setminus A = (B + e) \setminus A = \{b + e : b \in B \text{ e } b + e \notin A\} = e + \{b \in B : b \notin A - e\} = e + \{b \in B : b \notin B(e)\} = e + (B \setminus B(e))$.

(iii) Como A e B são finitos, usando (ii), temos $|A(e)| - |A| = |A(e) \setminus A| = |e + (B \setminus B(e))| = |B \setminus B(e)| = |B| - |B(e)|$. Portanto, $|A(e)| + |B(e)| = |A| + |B|$.

(iv) Se $e \in A$, então $0 \in A - e$. Por hipótese, $0 \in B$, logo $0 \in B \cap (A - e)$, ou seja, $e \in A(e)$ e $0 \in B(e)$.

□

1.3 Teorema de Cauchy-Davenport

Nesta seção iremos apresentar o Teorema de Cauchy-Davenport [2], que foi demonstrado por Cauchy em 1813, e posteriormente por Davenport [3] em 1935, sem o conhecimento da demonstração de Cauchy. Este Teorema estabelece um limite inferior para a cardinalidade do conjunto soma. Para demonstrar tal Teorema utilizaremos o seguinte resultado.

Teorema 1.9 (**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. Observe que pelo lema 1.5, precisamos mostrar apenas o caso em que $|A| + |B| \leq m$. Assim, $\min(m, |A| + |B| - 1) = |A| + |B| - 1 \leq m - 1$.

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

$$|A + B| = |A| = |A| + 1 - 1 = |A| + |B| - 1 \geq \min(m, |A| + |B| - 1).$$

Agora, suponhamos por contradição, que existam $A, B \subset \mathbb{Z}_m$, tais que

$$\min(|A|, |B|) \geq 2 \text{ e } |A + B| < |A| + |B| - 1.$$

Note que, esta última desigualdade nos diz que $A \neq \mathbb{Z}_m$, pois caso contrário, teríamos $|A| = m$ e $|B| \geq 2$, o que é absurdo, considerando a hipótese de $|A| + |B| \leq m$.

Dessa maneira, escolha o par (A, B) tal que a cardinalidade de B é mínima. Desde que $|B| \geq 2$, existe $b' \in B, b' \neq 0$. Consideremos então dois casos:

Caso 1. Se $a + b' \in A, \forall a \in A$, então recursivamente $a + jb' \in A$, para todo $j = 0, 1, 2, ...$, como por hipótese $(b', m) = 1$, temos $\{a+jb' : j = 0, 1, ..., m-1\} = \mathbb{Z}_m$, ou seja $A = \mathbb{Z}_m$, uma contradição.

Caso 2. Caso contrário, existe $e \in A$ tal que $e + b' \notin A$. Aplicando a e-transformada no par (A, B) e usando o lema 1.8, obtemos um novo par $(A(e), B(e))$ de subconjuntos não vazios de $\mathbb{Z}_m$, tais que

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

Além disso, como $e \in A$ e $0 \in B$, pelo item (iv) do lema 1.8 temos $0 \in B(e)$, temos ainda, $(b, m) = 1$, para todo $b \in B(e) \setminus \{0\}$, pois $B(e) \subset B$. Note que, $|B(e)| = 1$, implica que $|A(e) + B(e)| = |A(e)| + |B(e)| - 1$, uma contradição. Então, $|B(e)| \geq 2$. Como $b' \notin (A - e)$, logo $|B| > |B(e)|$, contradizendo a minimalidade de $|B|$. E isso conclui a demonstração. □

Tomando $m = p$, onde p é número primo, obtemos o importante Teorema de Cauchy-Davenport.

Teorema 1.10 (**Cauchy-Davenport**). *Sejam p um número primo, A e B subconjuntos não vazios de $\mathbb{Z}_p$. Então, $|A + B| \geq \min(p, |A| + |B| - 1)$.*

Demonstração. Seja $b' \in B$. Temos $0 \in B - b'$ e $(b, p) = 1$, para todo $b \neq 0$ em $B - b'$. Usando o Teorema de Chowla 1.9, temos

$$|A + B| = |A + (B - b')| \geq \min(p, |A| + |B - b'| - 1) = \min(p, |A| + |B| - 1).$$

Como desejado. □

Obsevação 1.11. *As condições do Teorema de Chowla são essenciais, pois caso contrário não há garantias do limite inferior. Basta tomarmos o seguinte exemplo, $A = \{0, 2, 4, 6\}$ e $B = \{0, 2, 4\}$ em $\mathbb{Z}_8$, note que não temos a condição $(b, m) = 1, \forall b \in B \setminus \{0\}$.*

Temos $A + B = \{0, 2, 4, 6\}$. Assim, $|A + B| = 4 < \min(8, |A| + |B| - 1) = \min(8, 6) = 6$.

Corolário 1.12. *Sejam $n \geq 2$, p primo, $A_1, A_2, ..., A_n$ subconjuntos não vazios de $\mathbb{Z}_p$. Então,*

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

Demonstração. A demonstração será feita por indução sobre n. O caso $n = 2$ é o Teorema de Cauchy-Davenport, assim suponhamos o resultado válido n

subconjuntos de $\mathbb{Z}_p$. Usando novamente o Teorema de Cauchy-Davenport, temos

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

Isto conclui a demonstração. □

1.4 Teorema de Erdös-Ginzburg-Ziv

Agora, exibiremos a demonstração do clássico Teorema de Erdös-Ginzburg-Ziv (1961) como em [17], de duas formas, usando o Teorema de Cauchy-Davenport e a outra usando o Teorema de Chevalley-Warning. Esse resultado foi um dos pontos de partida para as pesquisas sobre problemas de soma zero.

Teorema 1.13 (**Erdös-Ginzburg-Ziv**). *Seja $n \geq 1$. Se $a_0, a_1, ..., a_{2n-2}$ é uma sequência de $2n-1$ inteiros, não necessariamente todos distintos, então existe uma sequência $a_{j_1}, a_{j_2}, ..., a_{j_n}$, tal que $a_{j_1} + a_{j_2} + ... + a_{j_n} \equiv 0 \pmod{n}$.*

Demonstração. Primeiramente suponha que $n = p$, onde p é um número primo. Escolha $a_i' \in \mathbb{Z}_p$, tal que $a_i' \equiv a_i \pmod{p}$ e $0 \leq a_i' < p$. Renumere os inteiros a_i, tais que

$$0 \leq a_0' \leq a_1' \leq ... \leq a_{2p-2}' \leq p - 1. \tag{1.1}$$

Desta forma, vamos os seguintes casos:

Caso 1. Existe $i \in \{1, ..., p-1\}$ tal que $a_i' = a_{i+p-1}'$. Assim, da desigualdade (1.1) temos, $a_i' = ... = a_{i+p-1}'$ e como $a_i' \equiv a_i$, logo, $a_i \equiv a_{i+1} \equiv ... \equiv a_{i+p-1} \pmod{p}$ e $a_i + a_{i+1} + ... + a_{i+p-1} \equiv pa_i \equiv 0 \pmod{p}$.

Caso 2. Para todo $i \in \{1, ..., p-1,\ a_i' \neq a_{i+p-1}'\}$, definimos em $\mathbb{Z}_p$ os subconjuntos de dois elementos $A_i = \{a_i + p\mathbb{Z}, a_{i+p-1} + p\mathbb{Z}\}$.

Aplicando o corolário 1.12, temos $|A_1 + A_2 + ... + A_{p-1}| \geq \min(p, 2(p-1) - (p-1)+1) = p$, assim, $A_1 + A_2 + ... + A_{p-1} = \mathbb{Z}_p$. Logo, $-a_0 \equiv a_{j_1} + a_{j_2} + ... + a_{j_{p-1}} \pmod{p}$, tal que $a_{j_i} \in A_i$ com $i \in \{1, ..., p-1\}$.

Isto é, $a_0 + a_{j_1} + a_{j_2} + ... + a_{j_{p-1}} \equiv 0 \pmod{p}$. Ou seja, o teorema é válido quando $n = p$.

Agora, provaremos o teorema por indução sobre n. Se $n = 1$, nada temos a fazer. Suponha que $n > 1$ e que o teorema é válido para todo inteiro menor do que n. Se n é primo já provamos que o teorema é verdadeiro. Assim, considere n um número composto, logo $n = uv$, onde $1 < u \leq v < n$. Então, o resultado vale para u e v. Da sequência $a_0, ..., a_{2n-2}$ de comprimento $2n - 1 = 2uv - 1$ existe uma subsequência $a_{1,i_1}, ..., a_{1,i_v}$, tal que $a_{1,i_1} + ... + a_{1,i_v} \equiv 0 \pmod{v}$.

Existem $2n-1-v=(2u-1)v-1$ inteiros na sequência original que não estão nessa subsequência. Como $2u-1 \geq 2$, podemos encontrar uma subsequência disjunta $a_{2,i_1},...,a_{2,i_v}$ de comprimento v, tal que $a_{2,i_1}+...+a_{2,i_v} \equiv 0 \pmod{v}$.

Existem $2n-1-2v=(2u-2)v-1$ termos que não pertencem a nenhuma das duas subsequências já relacionadas. De maneira indutiva para $j=1,...,2u-1$, obtemos $2u-1$ subsequências distintas $a_{j,i_1},...,a_{j,i_v}$ de comprimento v, tal que $a_{j,i_1}+...+a_{j,i_v} \equiv 0 \pmod{v}$.

Então, $a_{j,i_1}+...+a_{j,i_v}=b_jv$, onde $b_j \in \mathbb{Z}$. Desde que o teorema é válido para u, existe uma subsequência $b_{j_1}+...+b_{j_u}$ da sequência $b_1,...,b_{2u-1}$, tal que $b_{j_1}+...+b_{j_u} \equiv 0 \pmod{u}$.

Isto é, $b_{j_1}+...+b_{j_u}=cu$ para algum $c \in \mathbb{Z}$. Então

$$\sum_{r=1}^{u}\sum_{s=1}^{v} a_{j_r,i_s} = \sum_{r=1}^{u} b_{j_r}v = cuv = cn \equiv 0 \pmod{n}.$$

E isto completa a demonstração. □

Apresentaremos o Teorema de Chevalley-Warning, que é uma ferramenta utilizada em muitas demonstrações da Teoria Aditiva dos Números, e em seguida, provaremos o Teorema de Erdös-Ginzburg-Ziv usando o Teorema de Chevalley-Warning, assim como feito em [17]. Iremos também convencionar que $0^0=1$.

Lema 1.14. *Sejam $\mathbb{F}_q$ um corpo com q elementos e $0 \leq r < q-1$. Temos $\sum_{x\in\mathbb{F}_q} x^r = 0$.*

Demonstração. Para $r=0$, o resultado é óbvio. Suponha que $0<r<q-1$ e considere α um gerador do grupo multiplicativo $\mathbb{F}_q^*$. Logo,

$$\sum_{x\in\mathbb{F}_q} x^r = 0^r + \sum_{x\in\mathbb{F}_q^*} x^r = 0^0 + \alpha^r + ... + \alpha^{(q-1)r}.$$

Observemos que $(\alpha^r, \alpha^{2r}, \alpha^{3r}, ..., \alpha^{(q-1)r})$ é uma progressão geométrica de razão $\alpha^r \neq 1$ e como $x^{(q-1)}=1$ para todo $x \in \mathbb{F}_q^*$, temos

$$\sum_{x\in\mathbb{F}_q} x^r \;=\; 0 + \frac{\alpha^r((\alpha^r)^{q-1}-1)}{\alpha^r-1} = \frac{\alpha^r(1-1)}{\alpha^r-1} = 0.$$

□

Teorema 1.15 (Chevalley-Warning). *Seja p um número primo e $\mathbb{F}_q$ o corpo finito com $q=p^t$ elementos. Para $i=1,...,m$, seja $f_i(x_1,x_2,...,x_n)$ um polinômio de grau d_i n variáveis com coeficientes em $\mathbb{F}_q$. Denote por N o número de n-uplas $(x_1,x_2,...,x_n)$ de elementos de $\mathbb{F}_q$, tais que $f_i(x_1,x_2,...,x_n)=0$ para todo $i=1,...,m$. Se*

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

então, $N \equiv 0 \pmod{p}$.

Demonstração. Pelo lema 1.14

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

Sejam $x_1, x_2, ..., x_n \in \mathbb{F}_q$. Note que,

$$\prod_{i=1}^{m}(1 - f_i(x_1, x_2, ..., x_n)^{q-1}) = \begin{cases} 1 & \text{se } f_i(x_1, x_2, ..., x_n) = 0 \quad \forall i \in \{1, ..., m\} \\ 0 & \text{caso contrário} \end{cases}$$

e assim,

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

Como o grau de $f_i(x_1, x_2, ..., x_n)$ é d_i, temos

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

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

$$\begin{aligned} N &\equiv \sum_{x_1,...,x_n\in\mathbb{F}_q} \prod_{i=1}^{m}(1 - f_i(x_1, x_2, ..., x_n)^{q-1}) \pmod p \\ &\equiv \sum_{x_1,...,x_n\in\mathbb{F}_q} \sum_{r_1,...,r_n} a_{r_1,...,r_n} x_1^{r_1}...x_n^{r_n} \pmod p \\ &\equiv \sum_{r_1,...,r_n} a_{r_1,...,r_n} \sum_{x_1,...,x_n\in\mathbb{F}_q} x_1^{r_1}...x_n^{r_n} \pmod p \\ &\equiv \sum_{r_1,...,r_n} a_{r_1,...,r_n} \prod_{j=1}^{n} \sum_{x_j\in\mathbb{F}_q} x_j^{r_j} \pmod p, \end{aligned} \tag{1.3}$$

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

$$\sum_{j=1}^{n} r_j \leq (q-1)\sum_{j=1}^{n} d_j < n(q-1). \tag{1.4}$$

Isso implica que para algum $0 \leq r_j < q-1$ na equação (1.4) a última desigualdade decorre da hipótese. Pelo lema 1.14 temos, $\sum_{x_j\in\mathbb{F}_q} x_j^{r_j} = 0$. E voltando a equação (1.3) obtemos $N = 0$. □

Observemos que no caso $n = p$, onde p é um número primo, o Teorema de Erdös-Ginzburg-Ziv é um corolário do Teorema de Chevalley-Warning. Assim, temos a segunda demonstração do teorema 1.13.

Corolário 1.16 (**Erdös-Ginzburg-Ziv**). *Seja $n \geq 1$. Se $a_0, a_1, ..., a_{2n-2}$ é uma sequência de $2n-1$ inteiros, não necessariamente todos distintos, então existe uma sequência $a_{j_1}, a_{j_2}, ..., a_{j_n}$, tal que*

$$a_{j_1} + a_{j_2} + ... + a_{j_n} \equiv 0 \pmod{n}.$$

Demonstração. Dados $a_1, ..., a_{2p-1}$ uma sequência de elementos no corpo finito $\mathbb{F}_p \cong \mathbb{Z}_p$. Considere os polinômios $f_1, f_2 \in \mathbb{F}_p[x_1, ..., x_{2p-1}]$ definidos por

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

e

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

Seja d_i o grau do polinômio f_i. Então, $d_1 = d_2 = p-1$. Denotamos por N o número de soluções simultâneas desses polinômios. Como $d_1 + d_2 = 2p-2 < 2p-1$, temos do Teorema de Chevalley-Warning que $N \equiv 0 \pmod{p}$. Como $f_1(0, ..., 0) = f_2(0, ..., 0) = 0$, temos $N \geq 1$ e assim, $N \geq p \geq 2$. Portanto, os polinômios f_1 e f_2 têm uma solução não trivial, ou seja, existem $x_1, ..., x_{2p-1} \in \mathbb{Z}_p$ não todos nulos, tais que $f_1(x_1, ..., x_{p-1}) = f_2(x_1, ..., x_{p-1}) = 0$.

Como $x^{p-1} = 1$ se, e somente se, $x \neq 0$, segue da definição do polinômio f_1 que $x_j \neq 0$ para exatamente p elementos $x_{j_1}, ..., x_{j_p} \in \mathbb{Z}_p$. Assim, $a_{j_1} + ... + a_{j_p} \equiv 0 \pmod{p}$. □

1.5 Demonstração de Matt DeVos para o Teorema de Kneser

Nesta seção iremos apresentar um Teorema de Kneser [18], 1953, um resultado sobre soma de subconjuntos finitos de um grupo abeliano. Faremos a demonstração do Teorema de Kneser, baseada no artigo de Matt DeVos [4]. A ideia dessa demonstração é fornecer uma prova pequena com base em um argumento de uniões e interseções simples.

Definição 1.17. *Seja A um subconjunto não vazio de um grupo abeliano G. O estabilizador de A é o conjunto $H(A) = \{g \in G : g + A = A\}$.*

Definição 1.18. *Se um elemento $g \in H(A)$ é chamado de período de A e A é chamado conjunto periódico, então $H(A) \neq \{0\}$.*

Proposição 1.19. *Seja G um grupo abeliano finito. Dados A e B subconjuntos não vazios de G, tome $H = H(A+B)$. Então:*

(i) $H(A) \subseteq H$;

(ii) $|A+H|$, $|B+H|$ *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) Seja H um subgrupo de G, consideremos $A = \{x_1, x_2, ..., x_l\}$. Assim, $A + H = \bigcup_{i=1}^{l}(x_i + H)$. Logo, existem no máximo l classes laterais à esquerda geradas por elementos de A, ou seja, existem k índices, $1 \leq i_1 < i_2 < ... < i_k \leq l$, onde $1 \leq k \leq l$, tais que

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

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

(iii) ($\Rightarrow$) Imediata.

($\Leftarrow$) Se $A = G$, então para qualquer que seja $g \in G$, temos $g+A = g+G = G = A$. Logo, $g \in H(A)$ e $H(A) = G$.

□

Teorema 1.20 (Kneser). *Sejam G um grupo abeliano, $A, B \subseteq G$ finitos e não vazios, com $|A| + |B| \leq |G|$ e $H = H(A+B)$, então*

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

Demonstração. Faremos a demonstração por indução sobre $|A+B|$. Suponha que $H \neq \{0\}$ e seja $\varphi : G \longrightarrow G/H$ o homomorfismo canônico. Então, $H(\varphi(A+B))$ é trivial. Aplicando indução para $\varphi(A), \varphi(B)$, temos

$$\begin{aligned} |A+B| = |A+B+H| = (|H|(|\varphi(A) + \varphi(B)|) &\geq |H|(|\varphi(A)| + |\varphi(B)| - 1) \\ &= |A+H| + |H+B| - |H|. \end{aligned}$$

Assim, podemos assumir $H = \{0\}$. Se $|A| = 1$, então o resultado é trivial, então podemos assumir $|A| > 1$ e escolher $a, a' \in A$. Desde de que $a' - a \notin H(B) \subseteq H(A+B) = \{0\}$, podemos escolher $b \in B$, tal que $b + a' - a \notin B$. Agora, substituindo B por $B - b + a$ podemos assumir $\emptyset \neq A \cap B \neq A$.

Seja $C \subseteq A + B$ e $K = H(C)$. Chamamos de C um convergente se

$$|C| + |K| \geq |A \cap B| + |(A \cup B) + K|.$$

Seja $C_0 = (A \cap B) + (A \cup B)$ e observe que $C_0 \subseteq A + B$. Desde que $0 < |A \cap B| < |A|$, podemos aplicar indução em $A \cap B$ e $A \cup B$ para concluir que C_0 é convergente. Assim, existe um convergente e agora podemos escolher um C convergente com $K = H(C)$ mínimo. Se $K = \{0\}$, então

$$|A + B| \geq |C| \geq |A \cap B| + |A \cup B| - |\{0\}| = |A| + |B| - 1$$

e segue o resultado.

Então, vamos supor $K \neq \{0\}$ e dessa forma iremos obter uma contradição. Desde que $H(A + B) = \{0\}$ e $H(C) = K$, podemos escolher $a \in A$ e $b \in B$, tal que $a + b + K \nsubseteq A + B$. Sejam $A_1 = A \cap (a + K)$, $A_2 = A \cap (b + K)$, $B_1 = B \cap (b + K)$ e $B_2 = B \cap (a + K)$. Agora, observe que $A_1, B_1 \neq \emptyset$. Para $i = 1, 2$ sejam $C_i = C \cup (A_i + B_i)$ e $K_i = H(A_i + B_i)$. Note que se $A_i, B_i \neq \emptyset$, então $K_i = H(C_i) < K$.

Agora, a seguinte equação é válida para $i = 1$ e também para $i = 2$ se $A_2, B_2 \neq \emptyset$, e podemos ver que C_i não é convergente, de fato pela minimalidade de K, e indução aplicada a A_i, B_i,

$$\begin{aligned} |(A \cup B) + K| - |(A \cup B) + K_i| &< (|C| + |K| - |A \cap B|) - (|C_i| + |K_i| \\ &- |A \cap B|) \\ &= |K| - |A_i + B_i| - |K_i| \\ &\leq |K| - |A_i + K_i| - |B_i + K_i|. \end{aligned} \tag{1.5}$$

Se $B_2 = \emptyset$, então

$$\begin{aligned} |(A \cup B) + K| - |(A \cup B) + K_1| &\geq |(a + K) \setminus (A_1 + K_1)| \\ &= |K| - |A_1 + K_1| \end{aligned}$$

contradizendo a equação (1.5) para $i = 1$. De forma análoga, obtemos uma contradição semelhante supondo $A_2 = \emptyset$. Assim, temos que $A_2, B_2 \neq \emptyset$ e a equação (1.5) é válida para $i = 1, 2$. Se $a + K = b + K$, então $A_1 = A_2$ e $B_1 = B_2$, temos

$$\begin{aligned} |(A \cup B) + K| - |(A \cup B) + K_1| &\geq |(a + K) \setminus ((A_1 \cup B_1) + K_1)| \\ &\geq |K| - |A_1 + K_1| - |B_1 + K_1| \end{aligned}$$

o que novamente contradiz a equação (1.5). Portanto, $a + K \neq b + K$. Assim, obtemos a próxima equação, observando que do lado esquerdo da equação (1.5) é não negativo, e todos os termos do lado direito são múltiplos de K_i. Logo,

$$|K| \geq |A_i| + |B_i| + |K_i|. \tag{1.6}$$

Agora, sejam $S = (a + K) \setminus (A_1 \cup B_2)$ e $T = (b + K) \setminus (A_2 \cup B_1)$ e note que S e T são disjuntos. A próxima equação segue do fato de $A + B$ não ser convergente, pela minimalidade de K, e a indução aplicada a A_i, B_i,

$$\begin{aligned} |K| &\geq |(A \cup B) + K| + |A \cap B| - |C| \\ &\geq |S| + |T| + |A \cup B| + |A \cap B| - |A + B| + |A_i + B_i| \\ &> |S| + |T| + |A_i| + |B_i| + |K_i|. \end{aligned} \tag{1.7}$$

Das equações (1.6) e (1.7) para $i = 1, 2$, obtemos $2|K| > |A_1| + |B_2| + |S| + |A_2| + |B_1| + |T|$. No entanto, $a + K = S \cup A_1 \cup B_2$ e $b + K = T \cup A_2 \cup B_1$, e essa contradição completa a demonstração. □

Corolário 1.21. *Sejam $n \geq 2$ e $A_1, A_2, ..., A_n$ subconjuntos finitos e não vazios de um grupo abeliano G e $H = H(A_1 + A_2 + ... + A_n)$. Então,*

$$|A_1 + A_2 + ... + A_n| \geq |A_1| + |A_2| + ... + |A_n| - (n-1)|H|.$$

Demonstração. A demonstração será feita por indução sobre n. O caso $n = 2$ segue do teorema anterior. Seja $n \geq 3$ e suponhamos que o teorema é válido para $n - 1$. Seja $H' = H(A_1 + A_2 + ... + A_{n-1})$. Claramente $H' \subset H$ e temos ainda

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

□

Agora, temos o seguinte caso particular do corolário anterior.

Corolário 1.22. *Sejam G um grupo abeliano e A um subconjunto finito e não vazio de G. Seja nA a n-soma do subconjunto A, ou seja,*

$$nA = \underbrace{A + A + ... + A}_{n-vezes}.$$

Seja $H_n = H(nA) = \{g \in G : g + nA = nA\}$ o estabilizador de nA. Então, $|nA| \geq n|A + H_n| - (n-1)|A_n|$ para todo $n \geq 1$.

Demonstração. Pelo corolário anterior, para qualquer subconjunto finito e não vazio de G, temos $|nB| \geq n|B| - (n-1)|H(nB)|$ para todo $n \geq 2$. Seja $B = A + H_n$. Então, $nB = n(A + H_n) = nA$ e assim, $H(nB) = H(nA) = H_n$. Portanto, $|nA| = |nB| \geq n|A + H_n| - (n-1)|H_n|$. □

No caso particular em que G é um grupo cíclico finito cuja ordem é um número primo, o Teorema de Kneser implica o teorema 1.10.

Corolário 1.23 (**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 $A + B = \mathbb{Z}_p$, isto é, $|A + B| = p$ e segue o resultado. Por outro lado, se $H = \{\overline{0}\}$, o teorema 1.20 implica que

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

□

1.6 Teorema de Vosper

Apresentaremos agora alguns lemas necessários para demonstrar o Teorema de Vosper, que fornece condições para a igualdade no Teorema de Cauchy-Davenport.

Definição 1.24. *Dados A e B subconjuntos finitos em G, dizemos que o par (A, B) é crítico quando $A + B \neq G$ e $|A + B| < |A| + |B|$.*

Definição 1.25. *Fixados A e B subconjuntos em G e $d \neq 0$, com $d \in G$, dizemos que A e B são progressões aritméticas com mesma razão d, quando $A = \{a + id : i = 0, 1, ..., s-1\}$ e $B = \{b+id : i = 0, 1, ..., t-1\}$ onde s e t são os comprimentos das progressões A e B, respectivamente.*

Lema 1.26. *Seja (A, B) um par crítico em $\mathbb{Z}_p$, tal que $\min(|A|, |B|) \geq 2$ e $|A+B| = |A|+|B|-1 < p-1$. Seja $D = \overline{A + B}$, então $(D, -A)$ é um par crítico, onde $\overline{A + B}$ é o complementar de $A + B$.*

Demonstração. Denote $s = |A|$ e $t = |B|$. Segue das hipóteses que $s+t-1 \leq p-2$, temos $|D| = |\overline{A+B}| = p - (s + t - 1) \geq 2$. Afirmamos que: $|D - A| = |D| + | - A| - 1 = p - t$. De fato, pelo Teorema de Cauchy-Davenport 1.10,

$$|D - A| \geq \min(p, |D| + | - A| - 1) = \min(p, p - t) = p - t. \tag{1.8}$$

Por outro lado, como $(A + B) \cap D = \emptyset$, segue que $B \cap (D - A) = \emptyset$ e assim, $D-A \subseteq \overline{B}$, ou seja, $|D-A| \leq p-t$. Como da equação (1.8) temos, $|D-A| \geq p-t$, portanto $|D-A| \leq |\overline{B}| = p-t = |D|-|-A|+1$. Como queríamos demonstrar. □

Lema 1.27. *Seja (A, B) um par crítico de $\mathbb{Z}_p$, tal que $|A| = s \geq 2$, $|B| = t \geq 3$, $0 \in B$ e $|A+B| = |A|+|B|-1 < p-1$. Então, existe uma classe de congruência $e \in A$, tal que a e-transformada $(A(e), B(e))$ é um par crítico, $A(e)+B(e) = A+B$ e $2 \leq |B(e)| < |B|$.*

Demonstração. Considere $A(e) + B(e)$ e e-transformada do par crítico (A, B), segue do lema 1.8 e do Teorema de Cauchy-Davenport 1.10

$$\begin{aligned} |A| + |B| - 1 = |A(e)| + |B(e)| - 1 &\leq |A(e) + B(e)| \\ &\leq |A + B| \leq |A| + |B| - 1. \end{aligned}$$

Portanto, $|A(e) + B(e)| = |A(e)| + |B(e)| - 1$, ou seja, $A(e), B(e)$ é também um par crítico. Como $A(e) + B(e) \subseteq A + B$, segue $A(e) + B(e) = A + B$. Defina $X = \{e \in A : B(e) \neq B\}$. Como $B(e) \subseteq B$ para todo $e \in G$, segue $|B(e)| < |B|$. Afirmamos que $|X| \geq 2$. De fato, considere $Y = A \setminus X = \{e \in A : B(e) = B\}$.

Analisemos as condições sobre o conjunto Y. Se $Y = \emptyset$, então $X = A$ e $|X| = |A| \geq 2$. Se $Y \neq \emptyset$, selecione $e \in Y$, assim $B = B(e) = B \cap (A - e)$ e logo, $B \subseteq A - e$. Temos, $e + B \subseteq A$ para todo $e \in Y$, então $Y + B \subseteq A$. Pelo Teorema de Cauchy-Davenport, temos

$$\begin{aligned} s = |A| \geq |Y + B| &\geq \min(p, |Y| + t - 1) \\ &= |Y| + t - 1 = s - |X| + t - 1, \end{aligned}$$

consequentemente $|X| \geq t-1 \geq 2$.

Agora, mostraremos que $|B(e)| \geq 2$ para algum $e \in X$. Visto que $e \in X$ e $0 \in B$, temos $0 \in B(e)$. Suponhamos que $B(e) = B \cap (A-e) = \{0\}$ para todo $e \in X$. Seja $B' = B \setminus \{0\}$, portanto, $B' \cap (A-e) = \emptyset$ implica $(e + B' \cap A) = \emptyset$, para todo $e \in X$. Como $X + B' \subset A + B$, segue que $X + B' \subseteq (A+B) \setminus A$ e usando novamente o Teorema de Cauchy-Davenport, temos

$$\begin{aligned} |X| + t - 2 = |X| + (t-1) - 1 &\leq |X + B'| \\ &\leq |A+B| - |A| = t - 1. \end{aligned}$$

Então, $|X| \leq 1$, o que é uma contradição. Logo, $2 \leq |B(e)| < |B|$. Completando a demonstração. □

Apresentamos até agora condições para que casos especiais de pares de conjuntos sejam críticos. A seguir apresentaremos condições para que o par (A, B) seja formado por progressões aritméticas com mesma razão.

Lema 1.28. *Seja A e B subconjuntos de $\mathbb{Z}_p$ tais que $\min(|A|, |B|) \geq 2$ e $|A+B| = |A|+|B|-1 < p-1$. Se A é uma progressão aritmética, então B é uma progressão aritmética com mesma razão de A.*

Demonstração. Denote $s = |A|$ e $t = |B|$. Como A é uma progressão aritmética, existem $a_0 \in A$ e $d \in \mathbb{Z}_p$, com $d \neq 0$, tal que $\{a_0 + id : i = 0, 1, ..., s-1\}$. Tomando $b_0 \in B$ considere os subconjuntos $A' = \{(a - a_0)d^{-1} : a \in A\} = \{i + p\mathbb{Z} : i = 0, 1, ..., s-1\}$ e $B' = \{(b - b_0)d^{-1} : b \in B\}$, segue das definições de A' e B' que $A', B' \subseteq \mathbb{Z}_p$. Assim $0 \in B', |A'| = |A| = s, |B'| = |B| = t$ com $t \geq 2$ e $A' + B' = \{(c - a_0) - b_0)d^{-1} : c \in A + B\}$. Por hipótese, temos

$$|A' + B'| = |A + B| = |A| + |B| - 1 < p - 1.$$

Assim, podemos assumir sem perda de generalidade que $B' = B$. Mostraremos portanto que $B = \{b, b+1, b+2, ..., b+t-1\}$ para algum $b \in B$.

Seja $B = \{b_0, b_1, ..., b_{t-1}\}$. Para $j = 0, 1, ..., t-1$, escolha $r_j = 0, ..., p-1$, tal que $b_j = r_j + p\mathbb{Z}$. Reenumerando as classes de congruência b_j de maneira adequada, podemos assumir que $0 = r_0 < r_1 < ... < r_{t-1} < p$ e supor que $r_t = p$. Como todo elemento de $A + B$ é da forma $b_j + i = r_j + i + p\mathbb{Z}$, para algum $i = 0, ..., t-1$, segue

$$A + B = \bigcup_{j=0}^{t-1} [r_j, r_j + \min(s-1, r_{j+1} - r_j - 1)] + p\mathbb{Z}.$$

Desse modo os t conjuntos nessa união são dois a dois disjuntos. De fato, dados $0 \leq i < j \leq t-1$ observe que

$$[r_i, r_i + \min(s-1, r_{i+1} - r_i - 1)] \subset [r_i, r_i + r_{i+1} - r_i - 1] = [r_i, r_{i+1} - 1].$$

Desta forma,

$$[r_j, r_j + \min(s-1, r_{j+1} - r_j - 1)] \subset [r_j, r_{j+1} - 1].$$

Assim, $[r_i, r_{i+1} - 1] \cap [r_j, r_{j+1} - 1] = \emptyset$. Logo,

$$\begin{aligned} s + t - 1 = |A + B| &= \sum_{j=0}^{t-1} (1 + \min(s-1, r_{j+1} - r_j - 1)) \\ &= t + \sum_{j=0}^{t-1} \min(s-1, r_{j+1} - r_j - 1). \end{aligned}$$

Agora, vamos analisar a minimalidade entre $s-1$ e $r_{j+1} - r_j - 1$. Primeiramente se $r_{j+1} - r_j - 1 \leq s - 1$, para todo $j = 0, 1, ..., t-1$ temos,

$$s + t - 1 = t + \sum_{j=0}^{t-1} (r_{j+1} - r_j - 1) = r_t - r_0 = p,$$

mas isso contradiz o fato de que $|A| + |B| - 1 < p - 1$. Assim, existe $j_0 \in [0, t-1]$, tal que $r_{j_0+1} - r_{j_0} - 1 > s - 1$ e assim,

$$s + t - 1 = |A + B| = s + t - 1 + \sum_{j=0, j \neq j_0}^{t-1} \min(s-1, r_{j+1} - r_j - 1).$$

Temos $r_{j+1} - r_j = 1$, para todo $j = 0, ..., t-1, j \neq j_0$ e portanto, B corresponde a progressão aritmética da forma $[r_{j_0+1}, r_{j_0+1} + t - 1] + p\mathbb{Z}$. □

Corolário 1.29. *Sejam A e B subconjuntos de $\mathbb{Z}_p$, tais que $\min(|A|, |B|) = 2$, além disso, $|A + B| = |A| + |B| - 1 < p - 1$. Então, A e B são progressões aritméticas com a mesma razão.*

Demonstração. Segue diretamente do lema 1.28, observando que um conjunto com dois elementos é uma progressão aritmética. □

Lema 1.30. *Seja (A, B) um par crítico em $\mathbb{Z}_p$, tal que $\min(|A|, |B|) \geq 2$, além disso $|A + B| = |A| + |B| - 1 < p - 1$. Se $A + B$ é uma progressão aritmética, então A e B são progressões aritméticas com mesma razão.*

Demonstração. Sendo $A + B$ uma progressão aritmética, então $D = \overline{A + B}$ também é uma progressão aritmética. Pelo lema 1.26, o par $(D, -A)$ é crítico, assim pelo lema 1.28, o conjunto $-A$ é uma progressão aritmética. Desse fato, temos A é uma progressão aritmética, como o par (A, B) é crítico, os conjuntos A e B são progressões aritméticas com mesma razão. □

Agora, munido desses resultados podemos demonstrar o Teorema de Vosper.

Teorema 1.31 (**Vosper**). *Seja p um número primo. Sejam A e B conjuntos não vazios de $\mathbb{Z}_p$, tais que $A+B \neq \mathbb{Z}_p$. Então, $|A+B| = |A|+|B|-1$ se, e somente se, uma das seguintes condições é satisfeita:*

(i) $\min(|A|,|B|) = 1$;

(ii) $|A+B| = p-1$ *e* $B = \overline{c-A}$, *onde* $\{c\} = \mathbb{Z}_p \setminus (A+B)$;

(iii) A *e* B *são progressões aritméticas com mesma razão.*

Demonstração. Pelo lema 1.5, se $A+B \neq \mathbb{Z}_p$, então $|A|+|B| \leq p$. Suponhamos sem perda de generalidade que (i) é válida, isto é, $\min(|A|,|B|) = |B| = 1$, então $|A+B| = |A| = |A|+|B|-1$ e assim, (A,B) é um par crítico.

Se (ii) é válida, temos $c \in \mathbb{Z}_p$ e A um subconjunto de $\mathbb{Z}_p$, tal que $1 \leq |A| \leq p-1$. Definimos $B = \overline{c-A}$. Como $c \notin A+B$ por hipótese, temos $|A|+|B|-1 = p-1 \Rightarrow |A+B| \leq p-1$. Então,

$$|B| = |\overline{c-A}| = p - |c-A| = p - |A|,$$

e do Teorema de Cauchy Davenport 1.10 segue

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

ou seja, $p-1 = |A|+|B|-1 \leq |A+B| \leq p-1$, e assim, $|A+B| = |A|+|B|-1$, isto é, (A,B) é crítico.

Agora, se A e B são progressões aritméticas em $\mathbb{Z}_p$ com mesma razão e r,t inteiros positivos, com $r+t \leq p$, tais que $A = \{a+id : i = 0,1,...,r-1\}$ e $B = \{b+id : i = 0,1,...,s-1\}$.

Como $d \in \mathbb{Z}_p \setminus \{0\}$ e $o(d)$ é um divisor de p, resulta que $o(d) = p$. Então, $A+B = \{a+b+id : i = 0,1,...,r+t-2\}$, e assim $|A+B| = r+t-1 = |A|+|B|-1$. Portanto se (i), (ii) ou (iii) são válidos, então o par (A,B) é crítico.

Reciprocamente, é suficiente provar que uma das três condições ocorre. Seja (A,B) um par crítico, isto é, $|A+B| = |A|+|B|-1$. Se $|A| = 1$ ou $|B| = 1$, o par é da forma (i).

Como $|A+B| = p-1$, pois (ii) é válida, então $\overline{A+B} = \{c\}$ para algum $c \in \mathbb{Z}_p$. Vamos provar que $B = \overline{c-A}$. De fato, como $c \notin A+B$, segue que $B \cap (c-A) = \emptyset$ e assim, $B \subseteq \overline{c-A}$. Então,

$$|B| \leq |\overline{c-A}| = p - |c-A| = p - |A|.$$

Assim, $|B| < p-|A| \Rightarrow |A|+|B| < p \Rightarrow |A|+|B| \leq p-1 \Rightarrow |A|+|B|-1 \leq p-2$, absurdo, pois $|A+B| = |A|+|B|-1$. Segue

$$|B| = p - |A| = \overline{c-A}$$

e assim, $B = \overline{c - A}$. Logo o par (A, B) é da forma (ii).

Para finalizarmos a demonstração, assumiremos que (A, B) é um par crítico tal que, $\min(|A|, |B|) \geq 2$ e $|A + B| < p - 1$. Pois caso contrário estaremos nas condições (i) e (ii).

Seja (A, B) um par crítico com $|B| = t \geq 2$. Faremos a conclusão da demonstração por indução sobre t. Se $t = 2$ o resultado segue do lema 1.30. Suponha $t \geq 3$ e assuma que o teorema é válido para todo para crítico (A, B) com $|B| \geq 3$.

Pelo lema 1.27, existe $e \in A$, tal que $(A(e), B(e))$ é um par crítico com $A(e) + B(e) = A + B$ e $2 \leq |B(e)| < t$.

Pela hipótese de indução, $A(e)$ e $B(e)$ são progressões aritméticas com mesma razão e como $A(e) + B(e) = A + B$, temos portanto do lema 1.30, que A e B são progressões aritméticas com a mesma razão, completando a demonstração. □

Finalizaremos este capítulo com o seguinte lema, cuja demonstração encontra-se em [12]. Esse lema será utilizado na demonstração do resultado principal estudado neste trabalho, observando que esse resultado quando aplicado à ordem de G prima, obtemos o teorema anterior.

Lema 1.32. *Seja G um grupo contendo dois subconjuntos A e B, tal que $1 \in A \cap B$ e $2 \leq |B|$. Seja $r \in G \setminus \{1\}$, tal que $|\langle r \rangle| \geq \max(|A|, |B|)$. Então, as seguintes afirmações valem:*

(i) Se $|\{1, r\}B| = |B| + 1$, então existe $j \in \mathbb{Z}$ tal que $B = \{r^i : j \leq i \leq j + |B| - 1\}$;

(ii) Se $B = \{r^i : j \leq i \leq j + |B| - 1\}$ e $|AB| = |A| + |B| - 1$ então existe $s \in \mathbb{Z}$ tal que $A = \{r^i : s \leq i \leq s + |A| - 1\}$.

Capítulo 2

Número Isoperimétrico

Neste capítulo iremos desenvolver o Método Isoperimétrico, apresentando as definições e propriedades da k-separabilidade e do número k-isoperimétrico do par (G, B), onde B é um subconjunto de um grupo G multiplicativo com a unidade em B. Tais propriedades permitiram mostrar a generalização do Teorema de Cauchy-Davenport e um resultado equivalente ao Teorema de Vosper, quando aplicado a ordem de G prima, que apresentaremos no capítulo três.

2.1 Notações e Terminologias

Inicialmente iremos estabelecer algumas notações:

- k denota um número natural maior ou igual que 1;
- Seja G um grupo multiplicativo contendo um elemento r e um subconjunto B. O subgrupo gerado por B será denotado $\langle B\rangle$. Escrevemos também $\langle r\rangle$ para $\langle\{r\}\rangle$.

Definição 2.1. *Seja G um grupo multiplicativo contendo dois subconjuntos A e B não vazios, então o* ***produto de Minkowski*** *é dado por $AB = \{xy : x \in A \text{ e } y \in B\}$.*

Definição 2.2. *Seja B um subconjunto de um grupo G multiplicativo tal que $1 \in B$. Dizemos que o par (G, B) é k-**separável** se existe $X \subset G$, tal que $|X| \geq k$ e $|G \setminus XB| \geq k$.*

Definição 2.3. *Se (G, B) é k-separável, definimos o* ***número k-isoperimétrico*** *de (G, B) da seguinte forma*

$$\kappa_k(G, B) = \min\{|XB \setminus X| : |X| \geq k \text{ e } |G \setminus XB| \geq k\}.$$

- Observe que $|XB \setminus X| = |XB| - |X|$, pois $X \subseteq XB$, já que $1 \in B$;
- Vamos escrever κ_k em vez de $\kappa_k(G, B)$, quando o contexto for claro;

- O conjunto de $X \subseteq G$ será chamado de conjunto k-**crítico** se

$$|X| \geq k, \quad |G \setminus XB| \geq k \quad \text{e} \quad |XB \setminus X| = \kappa_k(G, B);$$

- Um conjunto k-crítico com cardinalidade mínima será chamado de k-**átomo** de (G, B) e sua cardinalidade será denotada por $\alpha_k(G, B)$.

2.2 Resultados Principais

De posse de tais definições, apresentaremos alguns resultados que irão nos permitir dizer em que condições $\kappa_k(G, B) = \kappa_k(G, B^{-1})$, onde B^{-1} são os inversos de B ou ainda estabelecer relações entre as cardinalidades de dois k-átomos de (G, B).

Lema 2.4. *Seja B um subconjunto finito de um grupo G, tal que $1 \in B$. Suponha que (G, B) é k-separável. Sejam A um k-átomo de (G, B) e $x \in G$. Então, xA é um k-átomo de (G, B).*

Demonstração. Como $|xA| = |A|$, a demonstração segue de forma imediata. □

Note que, o lema 2.4 nos diz que satisfeita a definição de k-separável, existe um k-átomo de (G, B).

Lema 2.5. *Seja B um subconjunto finito de um grupo G, tal que $1 \in B$. Suponha que (G, B) é k-separável. Então, para todo $|X| \geq k$,*

$$|XB| \geq \min\{|G| - k + 1, |X| + \kappa_k(G, B)\}. \tag{2.1}$$

Além disso, $\kappa_k(\langle B\rangle, B) \geq 1$.

Demonstração. Se $|XB| \geq |G| - k + 1$, segue o resultado. Agora, suponha que $|XB| \leq |G| - k$. Então, por definição, temos

$$\kappa_k(G, B) \leq |XB \setminus X| = |XB| - |X| \Rightarrow |XB| \geq |X| + \kappa_k(G, B). \tag{2.2}$$

Da desigualdade (2.2) segue a relação (2.1).

Agora, suponha que $\kappa_k(\langle B\rangle, B) = 0$. Existe um subconjunto finito não vazio $X \subset \langle B\rangle$, tal que $XB = X$ e $X \neq \langle B\rangle$. Então, segue que $XB^i = X$, para $i \geq 1$, onde B^i são potências de B, e portanto $B^i \subset X^{-1}X$, e segue que todo elemento de B tem ordem finita e assim, $\langle B\rangle = \bigcup_{i\geq 1} B^i$.

Logo, $X = \bigcup_{i\geq 1} XB^i = X\langle B\rangle = \langle B\rangle$. Uma contradição, pois $X \neq \langle B\rangle$. Portanto, $\kappa_k(\langle B\rangle, B) \geq 1$. □

Lema 2.6. *Seja B um subconjunto finito de um grupo G tal que $1 \in B$. Suponha que (G, B) é k-separável. Seja A um k-átomo de (G, B), tal que $|A| \geq k + 1$ e $x \in A$. Então, $|A \cap xB^{-1}| \geq 2$, onde $B^{-1} = \{b^{-1} : b \in B\}$.*

Em particular, existe uma função $\psi : A \longrightarrow A$, tal que para cada $a \in A$ temos $(\psi(a)^{-1})a \in B \setminus \{1\}$.

Demonstração. Suponha que $|A \cap xB^{-1}| \leq 1$. Tome $F = A \setminus \{x\}$, note que $|F| \geq k$ e $|G \setminus FB| \geq k$, pois

$$|G \setminus FB| = |G| - |FB| \geq |G| - |AB| = |G \setminus AB| \geq k.$$

Portanto,

$$\kappa_k(G, B) \leq |FB \setminus F| = |FB| - |F| \quad \Rightarrow |FB| \geq |F| + \kappa_k(G, B). \tag{2.3}$$

Por outro lado, note que $FB \subset AB \setminus \{x\}$, pois caso contrário, existiria $x \in FB \subset AB$ tal que, $x = fb$ com $f \in F \Rightarrow f = xb^{-1} \Rightarrow f \in xB^{-1}$, ou seja, $f \in A \cap xB^{-1}$, e assim $|A \cap xB^{-1}| \geq 2$, pois $x \in A \cap xB^{-1}$, o que contraria a hipótese de $|A \cap xB^{-1}| \leq 1$, isto é, $FB \subset AB \setminus \{x\}$. Logo,

$$|FB| \leq |AB| - 1 = |A| + \kappa_k(G, B) - 1 = |F| + \kappa_k(G, B). \tag{2.4}$$

De (2.3) e (2.4) segue $\kappa_k(G, B) = |FB \setminus F|$, portanto F é um conjunto k-crítico, o que é absurdo pois $|F| < |A|$ e A é um k-átomo. Portanto $|A \cap xB^{-1}| \geq 2$.

Agora, tome $a \in A$, escolha $y \in A \cap a(B^{-1} \setminus \{1\})$, então podemos definir $\psi(a) = y$, e assim segue o resultado. □

Lema 2.7. *Seja B um subconjunto finito de um grupo G tal que $1 \in B$. Suponha que (G, B) é k-separável. Se F é um conjunto k-crítico de (G, B), então (G, B^{-1}) é k-separável e $\kappa_k(G, B) = \kappa_k(G, B^{-1})$. Além disso, $G \setminus FB$ é um conjunto k-crítico de (G, B^{-1}).*

Demonstração. Defina $R = G \setminus FB$. Note que, $RB^{-1} \subset G \setminus F$, pois caso contrário existiria $f \in F$, tal que $f = rb^{-1}$, com $r \in R, b \in B \Rightarrow r = fb \notin R$. Portanto, temos $|G \setminus RB^{-1}| \geq |F| \geq k$.

Assim, temos $|R| \geq k$, pois $|G \setminus FB| \geq k$ e $|G \setminus RB^{-1}| \geq |F| \geq k$, ou seja, (G, B^{-1}) é k-separável. Temos $|RB^{-1}| \leq |G \setminus F| = |G| - |F|$. Como F é k-crítico, então

$$|RB^{-1}| \leq |G \setminus F| = |G| - |F| = |G| - |FB| + \kappa_k(G, B) = |R| + \kappa_k(G, B),$$

ou seja $\kappa_k(G, B^{-1}) \leq |RB^{-1}| - |R| \leq \kappa_k(G, B) \Rightarrow |RB^{-1} \setminus R| \leq \kappa_k(G, B)$.

Assim, por dualidade temos $\kappa_k(G, B) = \kappa_k(G, B^{-1})$. □

Proposição 2.8. *Seja B um subconjunto finito de um grupo G tal que $1 \in B$. Suponha que (G, B) é k-separável. Seja F um conjunto k-crítico de (G, B) e seja A um k-átomo de (G, B) tal que $|A| \leq |G \setminus FB|$. Então $A \subset F$ ou $|A \cap F| \leq k-1$.*

Demonstração. Defina

$$R_{11} = A \cap F, \quad R_{12} = A \cap (FB \setminus F), \quad R_{13} = A \cap (G \setminus FB),$$

$$R_{21} = (AB \setminus A) \cap F,\ R_{22} = (AB \setminus A) \cap (FB \setminus F),\ R_{23} = (AB \setminus A) \cap (G \setminus FB),$$

$$R_{31} = F \cap (G \setminus AB),\ R_{32} = (FB \setminus F) \cap (G \setminus AB),\ R_{33} = (G \setminus AB) \cap (G \setminus FB).$$

Assim segue,

$$|R_{21}| + |R_{22}| + |R_{23}| = |R_{12}| + |R_{22}| + |R_{32}| = \kappa_k(G, B). \tag{2.5}$$

De fato, observemos as seguintes relações

$$|R_{21}| = |(AB \setminus A) \cap F| = |(AB \cap F) \setminus (A \cap F)| = |AB \cap F| - |A \cap F|.$$

$$\begin{aligned} |R_{22}| &= |(AB \setminus A) \cap (FB \setminus F)| = |((AB \setminus A) \cap FB) \setminus ((AB \setminus A) \cap F)| \\ &= |(AB \setminus A) \cap FB| - |AB \setminus A) \cap F| = |(AB \cap FB) \setminus (A \cap FB)| \\ &= |AB \cap FB| - |A \cap FB| - |AB \cap F| + |A \cap F|. \end{aligned}$$

$$\begin{aligned} |R_{23}| &= |(AB \setminus A) \cap (G \setminus FB)| = |((AB \setminus A) \cap G) \setminus ((AB \setminus A) \cap FB)| \\ &= |(AB \setminus A) \cap G| - |AB \setminus A) \cap FB| \\ &= |AB \setminus A| - |AB \cap FB| + |A \cap FB|. \end{aligned}$$

Segue que,

$$|R_{21}| + |R_{22}| + |R_{23}| = |AB \setminus A| = \kappa_k(G, B).$$

Note que,

$$|R_{12}| = |A \cap (FB \setminus F)| = |(A \cap FB) \setminus (A \cap F)| = |A \cap FB| - |A \cap F|.$$

Agora, temos

$$\begin{aligned} |R_{32}| &= |(FB \setminus F) \cap (G \setminus AB)| = |((FB \setminus F) \cap G) \setminus ((FB \setminus F) \cap AB)| \\ &= |FB \setminus F| - |FB \cap AB| + |F \cap AB|. \end{aligned}$$

Assim,

$$|R_{12}| + |R_{22}| + |R_{32}| = |FB \setminus F| = \kappa_k(G, B).$$

Logo, obtemos a relação (2.5). Verifiquemos agora a seguinte relação

$$(A \cap F)B \setminus (A \cap F) \subset R_{12} \cup R_{22} \cup R_{21}. \tag{2.6}$$

De fato, suponha $x \in (A \cap F)B \setminus (A \cap F)$, ou seja, $x = yb$, com $b \in B$ e $y \in A \cap F$, e note que $x \notin A \cap F$, isto é, $x \notin A$ ou $x \notin F$, temos:

Caso 1. Se $x \notin A \Rightarrow x \in AB \setminus A$. Assim se $x \in FB \setminus F$, segue o resultado, ou seja, $x \in R_{22}$. Caso contrário $x \in F$, e neste caso $x \in R_{21} = (AB \setminus A) \cap F$.

Caso 2. Se $x \in A \Rightarrow x \notin F$, ou seja, $x \in FB \setminus F$, e desta forma $x \in R_{12} = A \cap (FB \setminus F)$, logo, segue o resultado. Temos, também a relação

$$(A \cup F)B \setminus (A \cup F) \subset R_{32} \cup R_{22} \cup R_{23}. \tag{2.7}$$

De fato, suponha $x \in (A \cup F)B \setminus (A \cup F)$, ou seja, $x = yb$, com $b \in B$ e $y \in A \cup F$, e note que $x \notin A \cup F$, isto é, $x \notin A$ e $x \notin F$, temos:

Caso 3. $x \in FB \setminus AB \Rightarrow x \in (FB \setminus F) \cap (G \setminus AB) = R_{32}$.

Caso 4. $x \in AB \setminus FB \Rightarrow x \in (AB \setminus A) \cap (G \setminus FB) = R_{23}$.

Caso 5. $x \in (FB \setminus F) \cap (AB \setminus A) - R_{22}$.

Suponha que $|A \cap F| \geq k$. Como $|G \setminus (A \cap F)B| \geq |G \setminus (AB)| \geq k$, temos, $\kappa_k(G, B) \leq |(A \cap F)B \setminus (A \cap F)|$, pois $|A \cap F| \geq k$ e $|G \setminus (A \cap F)B| \geq k$ e assim, $A \cap F$ satisfaz a definição de número isoperimétrico.

Agora, usando as relações (2.5) e (2.6), temos

$$|R_{12}| + |R_{22}| + |R_{32}| = \kappa_k(G, B) \leq |(A \cap F)B \setminus (A \cap F)| \leq |R_{12}| + |R_{22}| + |R_{21}|$$

assim, $|R_{12}| + |R_{22}| + |R_{32}| \leq |R_{12}| + |R_{22}| + |R_{21}|$, mas usando a relação (2.5), temos $|R_{21}| + |R_{22}| + |R_{23}| \leq |R_{12}| + |R_{22}| + |R_{21}|$, portanto,

$$|R_{12}| \geq |R_{23}|. \tag{2.8}$$

Agora note que, $|R_{33}| + |R_{23}| + |R_{13}| = |G \setminus FB|$. De fato,

$$\begin{aligned} |R_{33}| = |(G \setminus AB) \cap (G \setminus FB)| &= |((G \cap G \setminus FB) \setminus ((AB \cap G \setminus FB)| \\ &= |(G \setminus FB)| - |(AB \cap G) \setminus (AB \cap FB)| \\ &= |G \setminus FB| - |AB| + |AB \cap FB|. \end{aligned}$$

$$\begin{aligned} |R_{23}| = |(AB \setminus A) \cap (G \setminus FB)| &= |((AB \setminus A) \cap G) \setminus ((AB \setminus A) \cap FB)| \\ &= |(AB \setminus A) \cap G| - |AB \setminus A) \cap FB| \\ &= |AB \setminus A| - |(AB \cap FB) \setminus (A \cap FB)| \\ &= |AB \setminus A| - |AB \cap FB| + |A \cap FB| \\ &= |AB| - |A| - |AB \cap FB| + |A \cap FB|. \end{aligned}$$

$$\begin{aligned} |R_{13}| = |A \cap (G \setminus FB)| &= |(A \cap G) \setminus (A \cap FB)| \\ &= |A \cap G| - |A \cap FB| \\ &= |A| - |A \cap FB|. \end{aligned}$$

Portanto, $|R_{33}| + |R_{23}| + |R_{13}| = |G \setminus FB|$. Usando a relação (2.8), temos

$$|R_{33}| = |G \setminus FB| - |R_{23}| - |R_{13}| \geq |A| - |R_{12}| + |R_{13}|.$$

Observe que

$$\begin{aligned} |A| - |R_{12}| + |R_{13}| &= |A| - |A \cap (FB \setminus F)| - |A \cap (G \setminus FB)| \\ &= |A| - |(A \cap FB) \setminus (A \cap F)| - |(A \cap G) \setminus (A \cap FB)| \\ &= |A| - |A \cap FB| + |A \cap F| - |A| + |A \cap FB| \\ &= |A \cap F|. \end{aligned}$$

Assim, $|R_{33}| \geq |A \cap F| \geq k$. Como $R_{33} \subset G \setminus (A \cup F)B$. Temos, $|G \setminus (A \cup F)B| \geq k$, por definição de número k-isoperimétrico, temos $|(A \cup F)B \setminus (A \cup F)| \geq \kappa_k(G, B)$. Usando (2.5) e (2.7), temos

$$|R_{12}| + |R_{22}| + |R_{32}| = \kappa_k(G, B) \leq |(A \cup F)B \setminus (A \cup F)| \leq |R_{32}| + |R_{22}| + |R_{23}|.$$

Assim, $|R_{12}| + |R_{22}| + |R_{32}| \leq |R_{32}| + |R_{22}| + |R_{23}|$. Portanto, $|R_{12}| \leq |R_{23}|$. Logo, da relação (2.8), temos

$$|R_{12}| = |R_{23}|. \tag{2.9}$$

Segue agora, usando a relação (2.6) e a equação (2.9), que

$$|(A \cap F)B \setminus (A \cap F)| \leq |R_{23}| + |R_{22}| + |R_{21}|.$$

Pela equação (2.5), temos $|(A \cap F)B \setminus (A \cap F)| \leq \kappa_k(G, B)$, a desigualdade contrária decorre da definição. Assim, $A \cap F$ é um conjunto k-crítico, então $|A| = |A \cap F|$. Logo, $A = A \cap F$, portanto $A \subset F$. □

Proposição 2.9. *Seja B um subconjunto finito de um grupo G, tal que $1 \in B$. Suponha que (G, B) é k-separável e que $2\alpha_k(G, B) + \kappa_k(G, B) \leq |G|$. Sejam K e M k-átomos distintos de (G, B). Então, $|K \cap M| \leq k - 1$.*

Demonstração. Suponha $|K \cap M| \geq 1$. Temos,

$$|K| + |MB| = |K| + |M| + \kappa_k(G, B) = 2\alpha_k(G, B) + \kappa_k(G, B) \leq |G|. \tag{2.10}$$

Na primeira igualdade usamos que M é k-crítico e na segunda que K e M são k-átomos. Segue da equação (2.10) que $|K| + |MB| \leq |G| \Rightarrow |K| \leq |G \setminus MB|$, como K e M são conjuntos distintos, segue pela proposição 2.8 que $|K \cap M| \leq k - 1$. □

Lema 2.10. *Seja B um subconjunto finito de um grupo G, tal que $1 \in B$. Assuma que (G, B) é k-separável e que $2\alpha_k(G, B) + \kappa_k(G, B) > |G|$. Então, G é finito e (G, B^{-1}) é k-separável. Além disso, $2\alpha_k(G, B^{-1}) + \kappa_k(G, B^{-1}) \leq |G|$.*

Demonstração. Claramente G é finito, pois $\alpha_k(G,B)$ e $\kappa_k(G,B)$ são finitos. Pelo lema 2.7 (G,B^{-1}) é k-separável. Agora, seja K um k-átomo de (G,B). Usando o lema 2.7 novamente, $G \setminus KB$ é um conjunto k-crítico de (G,B^{-1}), logo

$$\begin{aligned} \alpha_k(G,B^{-1}) \leq |G \setminus KB| = |G| - |KB| = |G| - |K| - \kappa_k(G,B) \\ \Rightarrow \alpha_k(G,B^{-1}) + \alpha_k(G,B) + \kappa_k(G,B) \leq |G|. \end{aligned} \tag{2.11}$$

Aplicando em (G,B^{-1}), temos

$$\alpha_k(G,B) + \alpha_k(G,B^{-1}) + \kappa_k(G,B^{-1}) \leq |G|. \tag{2.12}$$

Somando (2.11) e (2.12), temos

$$2\alpha_k(G,B) + \kappa_k(G,B) + 2\alpha_k(G,B^{-1}) + \kappa_k(G,B^{-1}) \leq 2|G|. \tag{2.13}$$

Agora suponha,

$$2\alpha_k(G,B^{-1}) + \kappa_k(G,B^{-1}) > |G|. \tag{2.14}$$

Usando a hipótese $2\alpha_k(G,B) + \kappa_k(G,B) > |G|$ e somando com (2.14) temos

$$2\alpha_k(G,B) + \kappa_k(G,B) + 2\alpha_k(G,B^{-1}) + \kappa_k(G,B^{-1}) > 2|G|,$$

o que é uma contradição à (2.13). Portanto, $2\alpha_k(G,B^{-1}) + \kappa_k(G,B^{-1}) \leq |G|$. $\square$

Capítulo 3

Aplicações do Método Isoperimétrico

3.1 Generalização do Teorema de Cauchy-Davenport

Agora munido dos resultados do capítulo dois, apresentaremos os resultados obtidos por Hamidoune no artigo [9] que são: a generalização do Teorema de Cauchy-Davenport [2, 3] que ao invés de tomarmos $A, B \subset \mathbb{Z}_p$ tomamos agora em um grupo qualquer e com algumas condições sobre a cardinalidade de B obtemos assim uma generalização do resultado. Tem-se também o resultado principal provado por Brailovski e Freiman em [8] e uma prova do teorema de adição em característica 2, provada por Zemor em [21]. Além disso, temos o corolário que aplicado à ordem de G prima, obtemos o Teorema de Vosper [20].

Proposição 3.1. *Seja G um grupo gerado por um subconjunto B finito, tal que $1 \in B$ e $|B| \leq |G| - 1$. Suponha que cada elemento de $G \setminus \{1\}$ tenha ordem maior ou igual à $|B|$. Então, $\kappa_1(G, B) \geq |B| - 1$.*

Demonstração. Por hipótese $|B| = |G| - 1$, logo $|G \setminus B| \geq 1$. Assim, (G, B) é 1-separável, pois podemos tomar $X = \{1\}$, temos $|X| \geq 1$ e $|G \setminus B| \geq 1$. Agora, considere os seguintes casos:

Caso 1. $2\alpha_1(G, B) + \kappa_1(G, B) \leq |G|$.

Pelo lema 2.4, existe K, 1-átomo de (G, B), tal que $1 \in K$. Suponha $|K| \geq 2$ e que $\kappa_1(G, B) < |B| - 1$. Pelo lema 2.6, existe $a \in (K \setminus \{1\}) \cap B^{-1}$, e assim $a \in K \cap aK$.

Pelo lema 2.4, aK é um 1-átomo de (G, B) e pela proposição 2.9, $aK = K$, pois se aK e K são distintos, então $|aK \cap K| \leq k - 1 = 1 - 1 = 0 \neq 1 \Rightarrow aK = K$. Segue que $\langle a \rangle K = K$, e assim

$$\kappa_1(G, B) = |\langle a \rangle KB| - |\langle a \rangle K| \Rightarrow \kappa_1(G, B) \equiv 0 \pmod{|\langle a \rangle|}.$$

Pelo lema 2.5, $\kappa_1(G,B) \geq 1$. Portanto,

$$\kappa_1(G,B) \geq |\langle a \rangle| = |\langle a^{-1} \rangle| \geq |B|,$$

uma contradição, pois supomos $\kappa_1(G,B) < |B| - 1$. Consequentemente $|K| = 1$. E por definição temos $\kappa_1(G,B) = |KB| - |K| = |B| - 1$.

Caso 2. $2\alpha_1(G,B) + \kappa_1(G,B) > |G|$.

Pelo lema 2.10, G é finito, (G, B^1) é 1-separável e $2\alpha_1(G,B^{-1}) + \kappa_1(G,B^{-1}) < |G|$. Pelo caso 1, aplicado a (G,B^{-1}), temos $\kappa_1(G,B^{-1}) = |B| - 1$, mas pelo lema 2.7, $\kappa_1(G,B) = \kappa_1(G,B^{-1})$, logo segue o resultado. □

Este resultado generaliza de certa forma o Teorema de Cauchy-Davenport, no sentido de que existem subconjuntos A e B que satisfazem a desigualdade $|AB| \geq |A| + |B| - 1$ em outros conjuntos diferentes de $\mathbb{Z}_p$. De fato, como (G,B) é 1-separável, pelo lema 2.4 existe um k-átomo A em G tal que $\kappa_1(G,B) = |AB \setminus A|$, segue que

$$|B| - 1 \leq \kappa_1(G,B) = |AB \setminus A|,$$

e isto implica que :

$$|AB \setminus A| = |AB| - |A| \geq |B| - 1 \Rightarrow |AB| \geq |A| + |B| - 1.$$

Corolário 3.2. *Seja G um grupo contendo dois subconjuntos finitos A e B tal que $1 \in A \cap B$, $2 \leq \min(|A|,|B|)$ e $|AB| \leq |A| + |B| - 1$. Suponha que cada elemento de $G \setminus \{1\}$ tenha ordem maior ou igual que o $\max\{|A|,|B|\}$. Então $\langle A \rangle = \langle B \rangle$.*

Demonstração. Suponha que $\langle A \rangle \not\subset \langle B \rangle$. Tome uma partição de $A = A_1 \cup A_2 \cup \cdots \cup A_t$, onde A_i é uma interseção não vazia de A com uma $\langle B \rangle$-classe lateral à esquerda. Como $1 \in A$, temos que $t \geq 2$, pois quando $t < 2$, $\langle A \rangle \subset \langle B \rangle$ é uma contradição à afirmação $\langle A \rangle \not\subset \langle B \rangle$. Assim, escolha $a_i \in A_i$, para cada $1 \leq i \leq t$, onde $b \in B$, temos $o(b) \geq |B|$ e por hipótese $|B| \geq 2$, logo $|B| \leq |\langle B \rangle| - 1$. Portanto, pela proposição 3.1

$$\kappa_1(G,B) = |B| - 1.$$

Seja $J = \{i \in [1,t] : |A_iB| < |\langle B \rangle|\}$. Pelo lema 2.5, temos

$$|a_i^{-1}A_iB| \geq |a_i^{-1}A_i| + |B| - 1, \quad i \in J.$$

Agora, observe que $A_iB \cap A_jB = \emptyset$, para todo $i \neq j$, pois são classes laterais à esquerda. Assim, $|AB| = \sum_{i \in J} |A_iB| + \sum_{i \notin J} |A_iB|$.

Como $|A_iB| \geq |A_i| + |B| - 1$ e $|A_iB| \geq |\langle B \rangle|$, para todo $i \notin J$, temos

$$|AB| \geq \sum_{i \in J} (|A_i| + |B| - 1) + \sum_{i \notin J} |\langle B \rangle|. \tag{3.1}$$

Observe que a primeira parcela da desigualdade (3.1), tem exatamente $|J|$ parcelas e na segunda parcela $t - |J|$, e note ainda que $|A_i| + |B| - 1 \geq |B|$, portanto

$$|AB| \geq |J||B| + (t - |J|)|\langle B\rangle|. \tag{3.2}$$

Usando a relação $t \geq 2$, $|\langle B\rangle| \geq \max(|A|, |B|)$ e $|J| \leq t$, vamos mostrar que $|J| = t$. Suponha então $|J| < t$. Como $|\langle B\rangle| \geq \max(|A|, |B|)$, temos

$$|A| + |B| - 1 \geq |AB| \geq |J||B| + (t - |J|)|\langle B\rangle| \geq |J||B| + (t - |J|)|A|,$$

ou seja, $|A|(1+|J|-t)+|B|(1-|J|)-1 \geq 0$. Logo $|J| = 0$ e assim, $|A|+|B|-1 \geq t|B|$. Por outro lado,

$$|A| + |B| - 1 \geq |AB| \geq t|\langle B\rangle| \geq 2\max(|A|, |B|) \geq |A| + |B|,$$

o que é absurdo, logo $|J| = t$. Agora, por (3.1) e (3.2), temos $|A| + |B| - 1 \geq |AB| \geq |A| + |J|(|B| - 1)$. Logo,

$$\begin{aligned} |A| + |B| - 1 \geq |A| + |J|(|B| - 1) \Rightarrow |B| - 1 &\geq |J|(|B| - 1) \\ &\Rightarrow |J| \leq 1, \end{aligned}$$

ou seja, $|J| = 1$ o que é uma contradição, pois $t = |J|$ e $t \geq 2$. Portanto, $\langle A\rangle \subset \langle B\rangle$. Similarmente prova-se a inclusão contrária. □

Agora, apresentaremos o resultado provado por Zemor [21].

Corolário 3.3. *Seja s um número natural. Seja B um subconjunto finito não vazio de um corpo finito F com característica 2. Então as seguintes condições são equivalentes:*

(i) Para todo $2 \leq |A|$, com $A \subset F$, temos $|A+B| \geq \min(|F|-1, |A|+|B|+s)$;

(ii) Para cada subgrupo aditivo não nulo H, $|H+B| \geq \min(|F|-1, |H|+|B|+s)$.

Demonstração. Claramente $(i) \Rightarrow (ii)$. Agora suponha que (i) não é válido e escolha $b \in B$. Daí segue que $(F, B+b)$ é 2-separável, pois como (i) não é válido, então existe um A, com $|A| \geq 2$, tal que $|A + B| < \min(|F| - 1, |A| + |B| + s)$, ou seja, $|A + B| < |F| - 1 \Rightarrow |A + B| \leq |F| - 2 \Rightarrow |F| - |A + B| \geq 2$.

Como $|B| = |b+B|$, temos que $(F, B+b)$ é 2-separável. Observe também que $\kappa_2(F, B + b) \leq |B| + s - 1$, pois

$$|A+B| < |A|+|B|+s \Rightarrow |A+B| \leq |A|+|B|+s-1 \Rightarrow |A+B|-|A| \leq |B|+s-1.$$

Como $\kappa_2(F, B + b) \leq |A + B| - |A|$, temos $\kappa_2(F, B + b) \leq |B| + s - 1$. Pelo lema 2.4, existe um 2-átomo H contendo o 0. Como $B + b = -(B + b)$, pois a característica de F é 2, então temos pelo lema 2.10

$$2\alpha_2(F, B + b) + \kappa_2(F, B + b) \leq |F|,$$

assim, note que

$$\begin{aligned} 2\alpha_2(F, B+b) + \kappa_2(F, B+b) &\leq |F| \\ 2|H| + |H+B| - |H| &\leq |F| \\ |H+B| &\leq |F| - |H| \\ |H+B| &\leq |F| - 2 \\ |H+B| &< |F| - 1. \end{aligned}$$

Agora, pelo lema 2.9 e pelo lema 2.4, para cada x, temos $|(H+x) \cap H| \leq k-1 = 1$ ou $H + x = H$. Desta forma, tome $x \in H \setminus \{0\}$, assim temos $\{0, x\} \subset H \cap (H+x)$, portanto $H + x = H$. Assim, segue que H é um subgrupo aditivo de F, então como H é 2-átomo, temos

$$|H+B| - |H| = \kappa_2 \leq |B| + s - 1 \Rightarrow |H+B| \leq |H| + |B| + s - 1,$$

como queríamos. Portanto, $(ii) \Rightarrow (i)$, segue o resultado. □

Assim, concluímos esta seção apresentando a prova desse teorema de adição em característica 2, provada em [21]. O corolário 3.3 é um pouco mais preciso do que o teorema 1.4 provado no artigo [21], já que evita a restrição $|A| \leq s^2 - 2$.

3.2 Problemas Críticos

Agora, apresentaremos o principal resultado deste trabalho, que constrói um resultado equivalente ao Teorema de Vosper [20], ou seja, obtemos um resultado através do Método Isoperimétrico que caracteriza os pares de conjuntos críticos.

Teorema 3.4. *Seja G um grupo gerado por um subconjunto finito B, tal que $1 \in B$. Suponha que cada elemento de $G \setminus \{1\}$ tenha ordem maior ou igual que $|B|$. Então, uma das seguintes condições é válida:*

(i) Para todo $2 \leq |X| < \infty, |XB| \geq \min(|G| - 1, |X| + |B|)$;

(ii) Existem $r \neq 1$ e $j \in \mathbb{Z}$ tal que $B = \{r^i : j \leq i \leq j + |B| - 1\}$.

Demonstração. A demonstração será por indução sobre a cardinalidade de B. Note que quando $|B| \leq 2$, a condição (ii) é válida.

Suponha que o resultado é válido para todo B', com $|B'| < |B|$. Suponha que a condição (i) não é válida, então existe $X \subset G$, com $2 \leq |X| < \infty$, tal que $|XB| < \min(|G| - 1, |X| + |B|)$, isto é

- $|XB| < |G| - 1 \Rightarrow |G \setminus XB| > 1 \Rightarrow |G \setminus XB| \geq 2$, ou seja, (G, B) é 2-separável.

- Temos também,

$$\begin{aligned} |XB| < |X| + |B| &\Rightarrow |XB \setminus X| < |B| \\ &\Rightarrow \kappa_2(G,B) < |B| \\ &\Rightarrow \kappa_2(G,B) \leq |B| - 1. \end{aligned} \tag{3.3}$$

Assim considere os seguintes casos:

Caso 1. $2\alpha_2(G,B) + \kappa_2(G,B) \leq |G|$.

Pelo lema 2.4, existe um 2-átomo K de (G,B) tal que $1 \in K$. Considere inicialmente o caso em que $|K| = 2$, ou seja, $K = \{1, r\}$, temos por (3.3)

$$\begin{aligned} |KB| - |K| &\leq |B| - 1 \\ |KB| &\leq |B| + |K| - 1 \\ |KB| &\leq |B| + 1 \Rightarrow |KB| = |B| + 1. \end{aligned} \tag{3.4}$$

Para obtermos a igualdade (3.4), observe que, $|KB| < |B| + 1 \Rightarrow |KB| \leq |B| \Rightarrow KB = B$. Temos

$$\begin{aligned} KB &= \{1, r\}B \Rightarrow r^i \in B, \forall i, \text{ pois} \\ 1 \in B &\Rightarrow r^1 1 \in KB = B \Rightarrow r \in B \\ r \in B &\Rightarrow r^2 \in B \\ &\vdots \\ &\Rightarrow r^i \in B, \forall i. \end{aligned}$$

Como $r \in G \setminus \{1\}, |r| \geq |B|$, se $|B| = k$, então $\{1, r, r^2, r^3, ..., r^{k-1}\} = B$.

Assim, pelo item (i) do lema 1.32 existe $j \in \mathbb{Z}$, tal que $B = \{r^i : j \leq i \leq j + |B| - 1\}$.

Suponha $|K| \geq 3$. Pelo lema 2.6 existe uma função $\psi : K \longrightarrow K$, tal que para cada $a \in K, \psi(a)^{-1}a \in B \setminus \{1\}$. Assuma agora que $|K| > |B| - 1$. Claramente, existem $a, b \in K$ tal que $a \neq b$ e

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

Tome agora, $u = ba^{-1}$, temos

$$\begin{aligned} \psi(a)^{-1}a &= \psi(b)^{-1}b \\ \psi(b)\psi(a)^{-1}a &= b \\ \psi(b)\psi(a)^{-1} &= ba^{-1} = u. \end{aligned} \tag{3.5}$$

Agora por (3.5), temos $b = ua \Rightarrow b \in uK$ e da mesma forma tem-se, $u\psi(a) = \psi(b) \Rightarrow \psi(b) \in uK$, portanto $\{b, \psi(b)\} \subset uK \cap K$. Observe que $b \neq \psi(b)$, pois $\psi(b)^{-1}b \neq 1 \Rightarrow b \neq \psi(b)$. Além disso, temos $u \neq 1$, pois caso contrário temos $ba^{-1} = 1 \Rightarrow b = a$, uma contradição pois $a \neq b$.

Logo, pela proposição 2.9, $uK = K$, assim segue que $\langle u\rangle K = K$. Temos

$$\kappa_2(G, B) = |\langle u\rangle KB| - |\langle u\rangle K| \Rightarrow \kappa_2(G, B) \equiv 0 \pmod{|\langle u\rangle|}.$$

Pelo lema 2.5, $\kappa_2(G, B) \geq 1$. Consequentemente, $\kappa_2(G, B) \geq |\langle u\rangle| \geq |B|$, uma contradição por (3.4). Então,

$$|K| \leq |B| - 1. \tag{3.6}$$

Assim, pelo corolário 3.2 e (3.6) temos $G = \langle B\rangle = \langle K\rangle$. Sabemos que

$$\begin{aligned} 2\alpha_2(G, B) + \kappa_2(G, B) &\leq |G| \\ 2|K| + |KB| - |K| &\leq |G| \\ |B| + |K| \leq |KB| + |K| &\leq |G| \\ |B| + |K| - 1 &< |G| - 1. \end{aligned}$$

Segue que,

$$|B^{-1}K^{-1}| = |K^{-1}| + |B^{-1}| - 1 < |G| - 1,$$

isto é,

$$|B^{-1}K^{-1}| = |K^{-1}| + |B^{-1}| - 1 \leq |G| - 2.$$

Por (3.5) e hipótese de indução, aplicado à (G, K^{-1}), existem $r \neq 1$ e $q \in \mathbb{Z}$, tal que $K^{-1} = \{r^i : j \leq i \leq j + |K| - 1\}$, portanto pelo o item (ii) do lema 1.32 existe $s \in \mathbb{Z}$, tal que

$$B^{-1} = \{r^i : s \leq i \leq s + |B| - 1\}.$$

Portanto,

$$B = \{r^{-i} : s \leq i \leq s + |B| - 1\}.$$

Caso 2. $2\alpha_2(G, B) + \kappa_2(G, B) > |G|$.

Pelo lema 2.10, G é finito e (G, B^{-1}) é 2-separável e $2\alpha_2(G, B^{-1}) + \kappa_2(G, B^{-1}) \leq |G|$. Pelo lema 2.7, temos $\kappa_2(G, B^{-1}) = \kappa_2(G, B)$. Assim, com os mesmos argumentos usados no Caso 1 aplicado a (G, B^{-1}), mostra-se que

$$B = \{r^i : s \leq i \leq s + |B| - 1\},$$

para algum $s \in \mathbb{Z}$. □

Corolário 3.5. *Seja G um grupo contendo dois subconjuntos finitos A e B tal que $2 \leq \min(|A|, |B|)$. Suponha que cada elemento de $G \setminus \{1\}$ tenha ordem maior ou igual que $\max(|A|, |B|)$ e $|AB| = |A| + |B| - 1 < |G|$. Assuma que $1 \in B$ e que G é gerado por B. Então uma das seguintes condições é válida:*

(i) Existe y tal que $A = G \setminus (yB^{-1})$;

(ii) Existem $x, y, r \in G$ *tal que* $A = \{xr^i : 0 \leq i \leq |A| - 1\}$ *e* $B = \{r^i y : 0 \leq i \leq |B| - 1\}$.

Demonstração. Considere primeiro o caso $|A| + |B| - 1 = |G| - 1$. Seja y o único elemento $G \setminus AB$. Assim, $A \subset G \setminus (yB^{-1})$, pois note que, $A \subset G$, então suponha que exista $a \in A$, tal que $a = yb^{-1} \Rightarrow y = ab$, uma contradição pois $y \in G \setminus AB$. Por outro lado, temos

$$\begin{aligned} |A| + |B| - 1 &= |G| - 1 \\ |A| + |B| &= |G| \\ |A| &= |G| - |B| \\ |A| &= |G| - |yB^{-1}| \\ |A| &= |G \setminus yB^{-1}|, \end{aligned}$$

o que mostra que $A = G \setminus yB^{-1}$, o que prova (i).

Considere agora o caso em que $|A| + |B| - 1 \leq |G| - 2$. Seja $a \in A^{-1}$ e $b \in B^{-1}$. Pelo corolário 3.2, $aA \subset \langle Bb \rangle$. Pelo teorema 3.4, existe $r \neq 1$ e $m \in \mathbb{Z}$ tal que $Bb = \{r^i : m \leq i \leq m + |B| - 1\}$. Pelo lema 1.32, existe $n \in \mathbb{Z}$ tal que $aA = \{r^i : n \leq i \leq n + |A| - 1\}$. □

O corolário 3.5 quando aplicado a ordem de G prima obtem-se o Teorema de Vosper [20]. Note que, da condição $|A| + |B| - 1 = |G| - 1$ da primeira parte da demonstração do corolário 3.5, temos $|A+B| = |A|+|B|-1 = |G|-1 \Rightarrow |A+B| = |G| - 1$, tomando a ordem de G um número primo p, tem-se $|A + B| = p - 1$. Além disso, do fato $y \in G \setminus AB \Rightarrow A = \overline{y - B}$, o que equivale a condição (ii) do teorema 1.31. Temos ainda da condição (ii) do corolário 3.5 que A e B são progressões aritméticas de mesma razão.

Além disso, no caso em que G é sem torsão, a condição (i) não é válida, pois G é infinito, o corolário 3.5 equivale ao resultado principal provado por Brailovski e Freiman em [8].

Considerações Finais

Com esse trabalho conseguimos estudar os resultados clássicos da Teoria Aditiva dos Números. Utilizando o Método Isoperimétrico estudamos uma outra forma de obter esses resultados, e no caso do Teorema de Cauchy-Davenport, um resultado generalizado.

O Método Isoperimétrico também pode ser aplicado à Teoria de Grafos. Observa-se que a estimativa da cardinalidade mínima da soma $A + B$ pode ser interpretada como a conectividade, que é intuitivamente o número mínimo de elementos (vértices ou arestas) que precisam ser removidos para desconectar os vértices restantes uns dos outros.

Desta forma os teoremas da Teoria Aditiva dos Números são usados para responder perguntas sobre conectividades de grafos. No artigo [11] o autor apresenta essa aplicação, de forma detalhada, exibindo vários resultados importantes sobre o tema.

Referências Bibliográficas

[1] BRAILOVSKI, L. V; FREIMAN, G. A. *On a product of finite subsets in a torsion free group*. J. Algebra **130** (1990), 462-476.

[2] CAUCHY, A. L. *Recherches sur les nombres*. J. Ecole Polytech. **9** (1813), 99-116.

[3] DAVENPORT, H. *On the addition of residue classes*. J. London Math. Soc. **10** (1935), 30-32.

[4] DEVOS, M. *A short proof of Kneser's addition theorem for abelian groups*. Combinatorial abd additive number theory-CANT 2011 and 2012, 39-41, Springer Proc. Math. Stat., 101, Springer, New York, 2014.

[5] DIDERRICH, G.T. *On Kneser's addition theorem in groups*. Proc. Amer. Math. Soc. (1973), 443-451.

[6] DIXMIER, J. *Proof of a conjecture by Erdös, Graham concerning the problem of Frobenius*. J. number Theory **34** (1990), 198-209.

[7] DOXIADIS, Apostolos. *Tio Petros e a Conjectura de Goldbach*. São Paulo: Editora 34, 2001.

[8] FREIMAN, G. *Structure theory of set addition*. in "Proceedings Conf. Structure Theory of Set Addition, Marseille, Luminy, June 1993," pp. 7-11.

[9] HAMIDOUNE, Y.O. *An isoperimetric method in additive theory*. J. Algebra **179** (1996), no.2, 622-630.

[10] HAMIDOUNE, Y.O. *On a subgroup contained in words with a bounded length*. Discrete Math. **103** (1992), 171-176.

[11] HAMIDOUNE, Y.O. *Some additive applications of the isoperimetric approach*. Annales de L'institut Fourier (2008): 2007-2036.

[12] HAMIDOUNE, Y.O. *Subsets with a small product in groups*. preprint, April 1994.

[13] HAMIDOUNE, Y. O. *Sur les atomes d'un graphe orienté*. C. R. Acad. Sci. Paris **284** (1977), 1253-1256.

[14] KEMPERMANN, J. H. B. *On small sumsets in abelian groups.*Acta Math. **103** (1960), 66-88.

[15] MANN, H. B. *"Addition Theorems: The Addition Theorems of Group Theory and Number Theory", Interscience.* New York, 1965.

[16] MARTINEZ, Fabio E. Brochero; MOREIRA, Carlos Gustavo T. de A; SALDANHA, Nicolau C; TENGAN. Eduardo. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro.* Coleção Projeto Euclides - 3ª ed. IMPA 2013.

[17] NATHANSON, M. B. *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[18] OLIVEIRA, F. A. Alves. *Teorema de Erdos-Ginzburg-Ziv com peso.* Dissertação (Mestrado em Matemática) - Universidade Federal de Viçosa, Minas Gerais, 2014.

[19] OLSON, J.E. *On the symmetric difference of two sets in a group.* Europ. J. Combinatorics, (1986), 43?54.

[20] VOSPER, G. *The critical pairs of subsets of a group of prime order.* J. London Math. Soc. **31** (1956), 200-205.

[21] ZEMOR,G. *Subset sums in binary spaces*, European J. Combin. **13** (1992), 221-230.