BRUNA MARIA FRUTUOSO

SOBRE ALGUNS INVARIANTES EM PROBLEMAS DE SOMA ZERO

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
2019

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

T

F945s
2019

Frutuoso, Bruna Maria, 1997-
Sobre alguns invariantes em problemas de soma zero / Bruna Maria Frutuoso. – Viçosa, MG, 2019.
vii, 78 f. : il. ; 29 cm.

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

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

CDD 22. ed. 512.2

BRUNA MARIA FRUTUOSO

SOBRE ALGUNS INVARIANTES EM PROBLEMAS DE SOMA ZERO

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: 10 de julho de 2019.

Bhavinkumar Kishor Sinh Moriya

Sávio Ribas

Sávio Ribas

Abílio Lemos Cardoso Júnior
(Orientador)

Aos meus pais João e Custódia
e minhas irmãs Paula e Júlia.

"Ninguém pode crescer se não aceitar que é pequeno."
Papa Francisco

Agradecimentos

Agradeço primeiramente a Deus, por me dar forças para seguir sempre em frente e por abençoar meu caminho, através de tantas oportunidades e pessoas incríveis que passaram por minha vida até hoje.

Aos meus pais, João e Custódia, por todo apoio e amor que sempre dedicaram a mim. Por acreditarem em mim e por estarem ao meu lado sempre. Essa conquista é especialmente para vocês.

Agradeço a minha irmã Paula, pelas noites que passou (ou tentou passar) assistindo aos meus ensaios de seminários e por sempre me ajudar a tomar as decisões importantes da vida.

A minha irmã caçula, Júlia, pela ajuda no trabalho duro de elaboração desse trabalho. Obrigada por se dedicar a aprender comandos do LaTex e me ajudar na extensa tarefa de escrever essa dissertação. Sua ajuda foi crucial!

As minhas companheiras de apartamento ao longo desses anos, nos divertimos muito! Aprendi muito sobre a vida com a nossa troca de experiências, vocês me ajudaram tanto! Vocês são minha família de Viçosa.

Aos meus amigos e colegas de curso, por tornarem a vida acadêmica mais leve e agradável, pelas horas de estudo em equipe e pelos conhecimentos que trocamos.

Ao meu orientador, Professor Abílio, por toda a dedicação e por acreditar em mim. Obrigada pela paciência em explicar a mesma coisa várias vezes quando necessário e por todo o aprendizado que me proporcionou.

À todos os professores que tive durante a minha vida acadêmica, pelos ensinamentos acadêmicos e sobre a vida. Vocês contribuíram para que eu me tornasse quem eu sou hoje, por isso sou muito grata a vocês!

À CAPES pelo fundamental auxílio financeiro.

Por fim, muito obrigada a todos que direta ou indiretamente contribuíram com a realização deste trabalho.

Sumário

Resumo

FRUTUOSO, Bruna Maria, M.Sc, Universidade Federal de Viçosa, julho de 2019. **Sobre Alguns Invariantes em Problemas de Soma Zero**. Orientador: Abílio Lemos Cardoso Júnior.

Sejam G um grupo abeliano finito de expoente n e $A \subseteq [1, n-1]$. Neste trabalho estudaremos os invariantes $\eta_A(G)$, $D_A(G)$, $g_A(G)$, $s_A(G)$ e $E_A(G)$ com o intuito de apresentar limitantes e valores exatos para eles.

Abstract

FRUTUOSO, Bruna Maria, M.Sc, Universidade Federal de Viçosa, July, 2019. **About Some Invariants in Zero-Sum Problems**. Adviser: Abílio Lemos Cardoso Júnior.

Let G be a finite abelian group of exponent n and $A \subseteq [1, n-1]$. In this work we will study the invariants $\eta_A(G)$, $D_A(G)$, $g_A(G)$, $s_A(G)$ and $E_A(G)$ in order to present bounds and exact values for them.

Introdução

Em 1961, P. Erdős numa parceria com A. Ginzburg e A. Ziv, demonstraram um importante teorema, conhecido como o Teorema de Erdős-Ginzburg-Ziv, o qual afirma que qualquer sequência de números inteiros de tamanho $2n-1$ possui uma subsequência de tamanho n cuja soma dos seus elementos é congruente a zero módulo n.

Foi a partir deste teorema, que teve incio o estudo dos *problemas de soma zero*, assunto que compõe este trabalho. Problemas desse tipo tratam de sequências de elementos de um grupo G aditivo abeliano finito e estuda em que condições é possível garantir que a soma de todos os elementos de uma sequência tem como resultado o elemento neutro (zero) do grupo em questão. Quando isso é possível, denominamos esta sequência como *sequência de soma zero*.

Alguns anos depois de ser provado o Teorema de Erdős-Ginzburg-Ziv, outros matemáticos mostraram interesse por questões desse tipo, fazendo novas descobertas. Entre eles está H. Davenport, que ao propor uma questão em uma conferência em 1966, introduziu a *constante de Davenport*, hoje denotada por $D(G)$.

Em 1973, H. Harborth introduziu, em [14], as constantes $g(G)$ e $s(G)$, hoje conhecidas como *constante de Harborth* e *constante de Erdős-Ginzburg-Ziv*, respectivamente. Neste mesmo trabalho, H. Harborth apresentou valores exatos de $g(G)$ para grupos específicos, além de formalizar o que havia sido feito no Teorema de Erdős-Ginzburg-Ziv, que até então era simplesmente um resultado em Teoria Aditiva dos Números.

A fim de tornar os problemas de soma zero mais gerais, surgiram perguntas a respeito de resultados envolvendo um *conjunto-peso* $A \subseteq \mathbb{Z}$. O conjunto A recebe esse nome pois seus elementos são usados para criar somas ponderadas dos elementos de uma sequência. Com isso, podemos considerar as constantes sem peso como um caso particular onde $A = \{1\}$.

Havia também o interesse em estudar relações entre as constantes conhecidas e logo apareceram resultados interessantes. Por exemplo, para $G = C_3^r$ com $r \in \mathbb{N}$, H. Harborth mostrou em [14] que

$$s(C_3^r) = 2g(C_3^r) - 1$$

e em 2013, H. Godinho, A. Lemos e D. Marques mostraram em [10] que, para $A = \{-1, 1\}$ e $r \geqslant 3$,

$$s_A(C_3^r) = g_A(C_3^r) = 2\eta_A(C_3^r) - 1.$$

Relações mais gerais também já foram provadas e algumas, conjecturadas. Por exemplo, em 1990, W. D. Gao provou, em [23], que para qualquer grupo abeliano finito,

$$E(G) = D(G) + |G| - 1$$

e, em 2003, W. D. Gao conjecturou, em [8], que para qualquer grupo abeliano finito G com expoente n,

$$s(G) = \eta(G) + n - 1.$$

Até hoje não existem contraexemplos para essa conjectura, bem como não existe uma prova de sua veracidade.

Quando consideramos um conjunto-peso A, alguns resultados obtidos para o caso sem peso continuam válidos e outros, não. Por exemplo, a relação

$$E_A(G) = D_A(G) + |G| - 1 \tag{1}$$

foi provada em [12] para qualquer grupo G e qualquer conjunto-peso A. Abordaremos essa relação no Capítulo 2. Por outro lado, para $A = \{-1, 1\}$, a relação

$$s_A(G) = \eta_A(G) + \exp(G) - 1 \tag{2}$$

não se verifica para certos grupos G, conforme discutiremos no Capítulo 5.

Neste trabalho, estudamos todas as constantes mencionadas acima. Apresentamos resultados a respeito de diversos conjuntos-peso, mas uma atenção especial é dada a casos em que $A = \{-1, 1\}$. Quando esse for o conjunto em questão, denotaremos as constantes por $D_\pm(G), E_\pm(G)$, $s_\pm(G)$, $g_\pm(G)$ e $\eta_\pm(G)$.

Essa dissertação é organizada da seguinte forma: no Capítulo 1, apresentamos todas as definições importantes ao longo do trabalho e alguns resultados básicos. Apresentamos também duas demonstrações do Teorema de Erdős-Ginzburg-Ziv. Uma usando o Teorema de Chevalley-Warning e outra, usando o Teorema de Cauchy-Davenport. No Capítulo 2, exploramos resultados diversos sobre as constantes $E_A(G)$ e $D_A(G)$ com o objetivo de relacionar esses resultados, observando que, em cada caso, a relação (1) se verifica. Apresentamos ao final, a prova da relação (1) quando $G = C_p$ com p primo. O Capítulo 3 é dedicado ao estudo da constante de Davenport com peso $A = \{-1, 1\}$, denotada por $D_\pm(G)$. Apresentamos valores exatos para $D_\pm(G)$ para vários grupos e para outros, encontramos limitantes inferior e superior para $D_\pm(G)$. O trabalho deste capítulo é com base num teorema provado em 2012 por S. D. Adhikari, D. J. Grynkiewicz e Z. W. Sun, em [2], que estabelece limites inferior e superior para $D_\pm(G)$ sob algumas condições. Este capítulo ilustra bem a dificuldade geral que há em obter o valor exato das constantes envolvidas em problemas de soma zero. Em geral, encontram-se apenas intervalos limitantes e isso se deve ao caráter particular que cada grupo e cada conjunto-peso apresenta. No Capítulo 4, estudamos a constante de Harborth. Nosso objetivo é a prova do último teorema do capítulo, que será ferramenta para o capítulo seguinte. Por fim, dedicamos o Capítulo 5 à generalização da conjectura de Gao, que mencionamos em (2), para o caso em que $A = \{-1, 1\}$. Apresentamos exemplos em que a conjectura com peso A é válida e outros exemplos para os quais ela não se verifica.

Capítulo 1

Conceitos Iniciais

Neste capítulo, apresentamos uma série de resultados básicos da Álgebra, bem como da Teoria dos Números, que nos servirão de apoio para os capítulos seguintes.

Para começar, vamos estabelecer algumas convenções.

Ao longo de todo o trabalho, o conjunto dos naturais é $\mathbb{N} = \{1, 2, \dots\}$. Quando incluímos o zero, usamos $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Dados $k, l, m \in \mathbb{Z}$ com $l > k$ e $m > 0$, denotamos

$$[k, l] = \{k, k+1, \dots, l\}$$

e

$$\mathbb{N}_{\geqslant m} = \{m, m+1, \dots\}.$$

Dados $a, b \in \mathbb{N}$, denotamos por (a, b) o *máximo divisor comum de a e b.*

Para x um número real, denotamos por $\lfloor x \rfloor$ o maior inteiro menor ou igual a x, chamado *piso de x.* Analogamente, $\lceil x \rceil$ é o menor inteiro maior ou igual a x, chamado *teto de x.* A *parte não inteira de x* é o número $\{x\} = x - \lfloor x \rfloor$.

A seguinte relação será útil para a obtenção de resultados importantes no Capítulo 3.

Lema 1.1. *Dados $x_1, x_2, \dots, x_t$ números reais quaisquer, tem-se*

$$\left\lfloor \sum_{i=1}^{t} x_i \right\rfloor \leq \sum_{i=1}^{t} \lfloor x_i \rfloor + t - 1.$$

Demonstração: Para cada $i \in [1, t]$ temos $x_i = \lfloor x_i \rfloor + \{x_i\}$. Isso implica que

$$\sum_{i=1}^{t} x_i = \sum_{i=1}^{t} \lfloor x_i \rfloor + \sum_{i=1}^{t} \{x_i\}.$$

Por outro lado,

$$\sum_{i=1}^{t} x_i = \left\lfloor \sum_{i=1}^{t} x_i \right\rfloor + \left\{ \sum_{i=1}^{t} x_i \right\}.$$

Daí,

$$
\begin{aligned}
\sum_{i=1}^{t}\lfloor x_i\rfloor + \sum_{i=1}^{t}\{x_i\} &= \left\lfloor \sum_{i=1}^{t} x_i \right\rfloor + \left\{ \sum_{i=1}^{t} x_i \right\} \\
\Rightarrow \left\lfloor \sum_{i=1}^{t} x_i \right\rfloor &= \sum_{i=1}^{t}\lfloor x_i\rfloor + \sum_{i=1}^{t}\{x_i\} - \left\{ \sum_{i=1}^{t} x_i \right\} \\
&< \sum_{i=1}^{t}\lfloor x_i\rfloor + t \\
\Rightarrow \left\lfloor \sum_{i=1}^{t} x_i \right\rfloor &\leqslant \sum_{i=1}^{t}\lfloor x_i\rfloor + t - 1.
\end{aligned}
$$

■

1.1 Fatos da Teoria de Grupos

Nesta seção vamos falar especificamente sobre grupos aditivos, ou seja, cuja operação é a adição usual. Admitiremos conhecidas as noções de grupo, subgrupo, grupo cíclico, grupo finitamente gerado, classes laterais, subgrupo normal, grupo quociente e isomorfismos. Os resultados aqui apresentados, bem como suas demonstrações, podem ser encontrados em [11] e [24].

Definição 1.2. *Seja G um grupo com elemento neutro e. Dado $a \in G$, se $ma = e \Leftrightarrow m = 0$, dizemos que a tem ordem 0 e que o grupo G é infinito. Agora, se existe $m \neq 0$ tal que $ma = e$, ao menor m que satisfaz isso, chamamos ordem de a e denotamos por $ord(a) = m$.*

Se m é o menor tal que $ma = e$ para todo $a \in G$, dizemos que m é o expoente de G e escrevemos $\exp(G) = m$.

Quando G é finito, o número de elementos (ou a ordem) de G é denotada por $|G|$. Observe que quando G é grupo cíclico finito, digamos, $G = \langle g \rangle$, temos $\operatorname{ord}(g) = |G| = \exp(G)$.

Definição 1.3. *Dado G um grupo abeliano finito, uma família de elementos não nulos $\{e_1, \dots, e_s\}$ de G é dita independente se*

$$\sum_{i-1}^{s} a_i e_i = 0,\ a_i \in \mathbb{Z} \Rightarrow a_i e_i = 0\,\forall i \in [1, s].$$

Se, além disso, $G = \langle \{e_1, \dots, e_s\} \rangle$, então $\{e_1, \dots, e_s\}$ é chamada uma base de G.

A princípio, consideramos $a_i \in \mathbb{Z}$ na definição acima, não estabelecendo, assim, uma condição global sobre o conjunto dos coeficientes, pois isso depende da ocasião em que usaremos a definição e especificaremos isso localmente.

Na Teoria de Grupos, o Teorema de Lagrange relaciona a ordem de um grupo finito G com a ordem de um subgrupo qualquer de G da seguinte forma: Se G é um grupo finito e $H \leq G$, então $|G| = |G/H||H|$. Diversas propriedades interessantes dos grupos finitos podem ser obtidas como corolários do Teorema de Lagrange. Em particular, um resultado que nos será útil adiante e que pode ser obtido como corolário do Teorema de Lagrange é o Teorema de Euler, o qual afirma que $a^{\varphi(n)} \equiv 1 \pmod{n}$ quando $(a, n) = 1$, onde $\varphi(n) = |\mathbb{Z}_n^*|$. φ é conhecida como a função de Euler.

Aqui, temos um interesse especial pelos grupos cíclicos. Isso se dá pelo fato de que, especialmente os grupos que possuem como ordem potência de um primo, são a base para o estudos dos grupos abelianos finitos em geral, objeto sobre o qual nosso trabalho se desenvolve. Como todos os grupos cíclicos de mesma ordem são isomorfos, em geral, um grupo cíclico de ordem n é denotado por C_n. Também podemos escrever $G = \langle a \rangle$ com $\text{ord}(a) = n$. Não há, portanto, perda de generalidade em assumir $C_n = \{0, 1, 2, \ldots, n-1\}$ e isso é importante porque algumas demonstrações são de melhor compreensão quando tratamos um grupo cíclico de ordem n simplesmente como o grupo dos inteiros módulo n, $\mathbb{Z}_n$.

Outra classe de grupos que nos é interessante é a dos chamados p-grupos elementares, que definimos a seguir.

Definição 1.4. *Dado p primo, dizemos que um grupo G é p-grupo se para todo $g \in G$, $ord(x) = p^\alpha$ para algum $\alpha \in \mathbb{N}$. G é denominado um p-grupo abeliano elementar se G for abeliano e $x^p = 1$, para todo $x \in G$.*

Sobre homomorfismos de grupos, alguns serão muito úteis para nós, bem como suas propriedades. Abaixo, citamos os exemplos mais usados em nosso trabalho.

Exemplo 1.5. *(i)* A *projeção canônica* de um grupo G sobre um subgrupo H normal de G é o epimorfismo

$$\begin{aligned} \varphi : G &\longrightarrow G/H \\ x &\longmapsto \varphi(x) = x + H. \end{aligned}$$

(ii) A função

$$\begin{aligned} \varphi : G &\longrightarrow aG \\ x &\longmapsto \varphi(x) = ax \end{aligned}$$

onde G é um grupo abeliano finito e $a \in \mathbb{N}$ é um homomorfismo de grupos. Quando $(a, \exp(G)) = 1$, $aG = G$ e φ é um automorfismo.

Aqui, citamos um resultado básico sobre homomorfismos que usaremos adiante.

Teorema 1.6 (1º Teorema de homomorfismo)**.** *Sejam G e H grupos e $f : G \longrightarrow H$ um homomorfismo. Então*

$$\frac{G}{N(f)} \simeq Im(f).$$

Definição 1.7. *Dada $\{G_i\}_{i=1}^n$ uma família não vazia de grupos aditivos, o produto cartesiano $H = G_1 \times G_2 \times \cdots \times G_n$ com a operação usual da adição é chamado soma direta externa dos grupos $G_1, \ldots, G_n$ e é um grupo com essa operação, que denotamos $H = G_1 \oplus \cdots \oplus G_n$. Quando todos os G_i's são subgrupos normais de um dado grupo G satisfazendo:*

(i) $G = G_1 + G_2 + \cdots + G_n$ *e*

(ii) $G_i \cap G_1 + G_2 + \cdots + G_{i-1} + G_{i+1} + \cdots + G_n = \{0\}$ *para todo* $i \in [1, n]$,

onde $G_1 + G_2 + \cdots + G_n = \{g_1 + g_2 + \cdots + g_n \,|\, g_i \in G_i,\ i \in [1, n]\}$, *dizemos que* G *é a soma direta interna de* $G_1, G_2, \ldots, G_n$ *e, neste caso,* $G \simeq G_1 \oplus \cdots \oplus G_n$.

É natural se perguntar se é possível identificar que tipos de grupos abelianos podem ser vistos como soma direta interna de alguns de seus subgrupos normais. A resposta é sim e é obtida através de um dos mais importantes teoremas da Teoria de Grupos Finitos, o

Teorema 1.8 (Teorema Fundamental dos Grupos Abelianos Finitos)**.** *Todo grupo abeliano finito* $G \neq \{0\}$ *é a soma direta de uma família* $\{G_i\}_{i=1}^r$ *de p-subgrupos cíclicos não triviais. Além disso, o número destes grupos cíclicos e suas ordens são determinados de modo único pelo grupo* G.

Como consequência desse resultado, podemos escrever de maneira única,

$$G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$$

com $n_i | n_{i+1},\ i \in [1, r-1]$ onde C_{n_i} é o grupo cíclico de ordem n_i.

Quando escrito assim, temos $\exp(G) = n_r$ e definimos $r(G) = r$ o *posto de* G e para cada $n \in \mathbb{N}$, $r_n(G) = |\{i\,;\, n|n_i\}|$ o *n-posto de* G.

1.2 Resultados Auxiliares

Dois teoremas particularmente importantes para nosso trabalho serão demonstrados nessa seção. O Teorema de Chevalley-Warning e o Teorema de Cauchy-Davenport. A primeira aplicação deles será apresentada na seção seguinte, nas demonstrações do Teorema de Erdôs-Ginzburg-Ziv. Mas a utilidade deles vai além disso. São bases para vários outros resultados que citaremos nos capítulos seguintes, sendo ferramentas valiosas na solução de problemas de soma zero em geral.

1.2.1 O Teorema de Chevalley-Warning

O Teorema de Chevalley-Warning é resultado de um verdadeiro trabalho em equipe. O resultado foi inicialmente conjecturado por E. Artin em 1935. Logo em seguida, foi demonstrado por C. Chevalley e recebeu um refinamento por E. Warning, então aluno de E. Artin.

Antes de provar o Teorema de Chevalley-Warning, vamos fazer uma breve revisão sobre corpos finitos. Abaixo, seguem algumas das propriedades importantes dos corpos finitos enunciadas, cujas provas podem ser obtidas em [17].

Definição 1.9. *Um corpo é um conjunto* $\mathbb{F}$ *munido de duas operações, "adição"*$(+)$ *e "multiplicação"*$(\cdot)$*, satisfazendo*

(i) $(\mathbb{F}, +)$ *é um grupo abeliano com identidade (aditiva)* 0*;*

(ii) $(\mathbb{F}^*, \cdot)$ *é um grupo abeliano com identidade (multiplicativa)* 1.

Quando o conjunto $\mathbb{F}$ é finito, dizemos que o corpo é finito. Denotamos $\mathbb{F}[x]$ o anel de polinômios com coeficientes de $\mathbb{F}$.

Para todo p primo, $\mathbb{Z}_p$ é um corpo finito com p elementos e é denotado por $\mathbb{F}_p$ na teoria dos corpos finitos. Os corpos $\mathbb{F}_p$ são importantes pois todo corpo finito de característica p possui um subcorpo isomorfo a $\mathbb{F}_p$ e portanto, pode ser visto como uma extensão de $\mathbb{F}_p$. Isso é o que caracteriza os corpos finitos.

Definição 1.10. *Seja $\mathbb{F}$ um corpo. Definimos a característica de $\mathbb{F}$ (char($\mathbb{F}$)) como o menor inteiro positivo n tal que $n \cdot 1 = 0$, caso esse inteiro n exista. Se não existir nenhum n satisfazendo essa condição, dizemos que o corpo tem característica* 0.

Lema 1.11. *Seja $\mathbb{F}$ um corpo finito contendo um subcorpo $\mathbb{K}$ com q elementos. Então $\mathbb{F}$ possui q^m elementos, onde $m = [\mathbb{F} : \mathbb{K}]$, ou seja, m é o grau da extensão $\mathbb{F}$ sobre $\mathbb{K}$.*

Teorema 1.12. *Seja $\mathbb{F}$ um corpo finito. Então $\mathbb{F}$ possui p^n elementos, onde p é a característica de $\mathbb{F}$ e n é o grau de $\mathbb{F}$ sobre $\mathbb{F}_p$.*

O resultado abaixo é o que garante a existência e unicidade de corpos finitos com ordem p^n para todo primo p e para todo natural n.

Teorema 1.13. *Para todo primo p e para todo natural n existe um corpo finito com p^n elementos. Além disso, todo corpo finito $\mathbb{K}$ com $q = p^n$ elementos é o corpo de decomposição de $x^q - x$ sobre $\mathbb{F}_p$, ou seja, $x^q - x$ pode ser escrito em $\mathbb{K}$ como produto de fatores lineares.*

A partir da caracterização dada pelo teorema anterior, vamos denotar o corpo finito de ordem q por $\mathbb{F}_q$. O seguinte resultado é uma característica muito importante dos corpos finitos.

Teorema 1.14. *Para todo corpo finito $\mathbb{F}_q$, o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico.*

A partir de agora, estamos aptos a tratar do teorema de Chevalley-Warning.

Definição 1.15. *Seja $f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$. Definimos o grau de f, denotado por ∂f, como*

$$\partial f = \max \left\{ t_{i_1} + \cdots + t_{i_n} \mid f(x_1, \ldots, x_n) = \sum_i c_i x_1^{t_{i_1}} \cdots x_n^{t_{i_n}} \right\}.$$

Lema 1.16. *Seja $k \in \mathbb{N}$. Então*

$$\sum_{c \in \mathbb{F}_q} c^k = \begin{cases} 0 & se\ k \not\equiv 0 \pmod{q-1} \\ -1 & se\ k \equiv 0 \pmod{q-1} \end{cases}.$$

Demonstração: Seja $b \in \mathbb{F}_q$ tal que $\mathbb{F}_q^* = \langle b \rangle$. Note que,

$$\sum_{c \in \mathbb{F}_q} c^k = \sum_{j=0}^{q-1} (b^j)^k = 1 + \sum_{j=0}^{q-2} (b^j)^k = 1 + \sum_{j=0}^{q-2} (b^k)^j$$

e temos dois casos possíveis:

Caso 1. Se $k \not\equiv 0 \pmod{q-1}$, então

$$\sum_{j=0}^{q-2}(b^k)^j = \frac{((b^k)^{q-1}-1)}{b^k-1} = \frac{1-1}{b^k-1} = 0.$$

Caso 2. Se $k \equiv 0 \pmod{q-1}$, então $k = m(q-1)$ para algum $m \in \mathbb{N}$ e

$$\sum_{j=0}^{q-2}(b^k)^j = \sum_{j=0}^{q-2}(b^j)^{m(q-1)} = \sum_{j=0}^{q-2}((b^k)^{q-1})^m = \sum_{j=0}^{q-2} 1 = q-1 = -1 \text{ em } \mathbb{F}_q.$$

■

Lema 1.17. *Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ com $\partial f < n(q-1)$. Então*

$$\sum_{c_1,\ldots,c_n \in \mathbb{F}_q} f(c_1, \ldots, c_n) = 0.$$

Demonstração: Considere $x_1^{k_1} \cdots x_n^{k_n}$ um monômio qualquer de f. Temos:
Caso 1. Se $k_i = 0$ para algum $i \in [1, n]$, então $c_i^{k_i} = 1$ para todo $c_i \in \mathbb{F}_q$. Rearranjando os termos do monômio, podemos supor $i = 1$. Daí,

$$\sum_{c_1,\ldots,c_n \in \mathbb{F}_q} c_1^{k_1} \cdots c_n^{k_n} = \sum_{c_1 \in \mathbb{F}_q} 1 \left(\sum_{c_2,\ldots,c_n \in \mathbb{F}_q} c_2^{k_2} \cdots c_n^{k_n} \right) = q \left(\sum_{c_2,\ldots,c_n \in \mathbb{F}_q} c_2^{k_2} \cdots c_n^{k_n} \right) = 0$$

em $\mathbb{F}_q$.
Caso 2. Se $k_i > 0$ para todo $i = 1, \ldots, n$, como $\sum_{i=1}^n k_i < n(q-1)$, deve existir $i \in [1, n]$ tal que $k_i < q-1$. Podemos supor, sem perda de generalidade, que $i = 1$ e temos $k_1 \not\equiv 0 \pmod{q-1}$. Logo, pelo Lema 1.16, $\sum_{c_1 \in \mathbb{F}_q} c_1^{k_1} = 0$ e temos

$$\sum_{c_1,\ldots,c_n \in \mathbb{F}_q} c_1^{k_1} \cdots c_n^{k_n} = \sum_{c_1 \in \mathbb{F}_q} c_1^{k_1} \left(\sum_{c_2,\ldots,c_n \in \mathbb{F}_q} c_2^{k_2} \cdots c_n^{k_n} \right) = 0.$$

■

Teorema 1.18 (Warning)**.** *Seja $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ com $\partial f < n$. Então o número N de soluções da equação $f(x_1, \ldots, x_n) = 0$ é tal que $N \equiv 0 \pmod{p}$ onde p é a característica de $\mathbb{F}_q$.*

Demonstração: Considere o polinômio $F = 1 - f^{q-1}$ e observe que

$$F(c_1, \ldots, c_n) = 1 - f(c_1, \ldots, c_n)^{q-1} = \begin{cases} 0 \text{ se } f(c_1, \ldots, c_n) \neq 0 \\ 1 \text{ se } f(c_1, \ldots, c_n) = 0 \end{cases}.$$

Daí,

$$N = \sum_{c_1,\ldots,c_n \in \mathbb{F}_q} F(c_1, \ldots, c_n).$$

Agora, como $\partial f < n$, temos $\partial F = \partial f(q-1) < n(q-1)$ e pelo Lema 1.17,

$$\sum_{c_1,\ldots,c_n \in \mathbb{F}_q} F(c_1,\ldots,c_n) = 0 \text{ em } \mathbb{F}_q,$$

ou seja, $N \equiv 0 \pmod p$. ■

Teorema 1.19 (Chevalley). *Seja $f \in \mathbb{F}_q[x_1,\ldots,x_n]$ com $f(0,\ldots,0) = 0$ e $\partial f < n$. Então existe $(c_1,\ldots,c_n) \in \mathbb{F}_q^n \setminus \{(0,\ldots,0)\}$ tal que $f(c_1,\ldots,c_n) = 0$.*

Demonstração: Como $f(0\ldots,0) = 0$, o número de soluções N é maior ou igual a 1. Mas $p|N$ pelo Teorema 1.18. Logo, $N \geqslant 2$, como queríamos. ■

Teorema 1.20 (Warning). *Sejam $f_1,\ldots,f_r \in \mathbb{F}_q[x_1,\ldots,x_n]$ tais que $\sum_{i=1}^r \partial f_i < n$. Então o número de soluções N do sistema $f_i(x_1,\ldots,x_n) =$ é tal que $N \equiv 0 \pmod p$, onde p é a característica de $\mathbb{F}_q$.*

Demonstração: Considere o polinômio $F = \prod_{i=1}^r (1 - f_i^{q-1})$ e note que

$$F(c_1,\ldots,c_n) = \begin{cases} 1 \text{ se } f_i(c_1,\ldots,c_n) = 0 \ \forall\, i \\ 0 \quad\ \text{cc} \end{cases}.$$

Daí, $N = \sum_{c_1,\ldots,c_n \in \mathbb{F}_q} F(c_1,\ldots,c_n)$. Agora, $\partial F = (q-1)\sum_{i=1}^r \partial f_i < n(q-1)$. Logo, pelo Lema 1.17, $N \equiv 0 \pmod p$, como queríamos. ■

O Teorema 1.20 é ao qual faremos referência quando mencionarmos o Teorema de Chevalley-Warning.

1.2.2 O Teorema de Cauchy-Davenport

O teorema que é o objetivo desta seção, foi provado por H. Davenport em 1935 sem saber que, bem antes dele, o resultado já havia sido demonstrado por A. L. Cauchy, em 1813. Por esse motivo, o teorema recebe o nome dos dois matemáticos. A prova que vamos apresentar aqui é a do trabalho de H. Davenport e pode ser obtida em [1].

Definição 1.21. *Seja G um grupo aditivo abeliano e A, B subconjuntos finitos e não vazios de G. Definimos o conjunto-soma de A e B como sendo*

$$A + B = \{a + b \,|\, a \in A,\, b \in B\} \subseteq G.$$

No mesmo sentido do conjunto-soma, podemos definir os seguintes conjuntos.

(i) Conjunto-soma de n subconjuntos: $A_1 + \cdots + A_n = \{a_1 + \cdots + a_n \,|\, a_i \in A_i\} \subseteq G$;

(ii) Conjunto-soma estrita: $A \hat{+} B = \{a + b \,|\, a \in A,\, b \in B,\, a \neq b\} \subseteq G$;

(iii) Conjunto-diferença: $A - B = \{a - b \,|\, a \in A, b \in B\} \subseteq G$.

Observe que o conjunto-soma generaliza a soma de grupos que aparece na Definição 1.7. É importante destacar a diferença do conjunto-diferença para a diferença de conjuntos. Esta última é dada por:

$$A \setminus B = \{x \mid x \in A \,\text{e}\, x \notin B\}.$$

Se $c \in G$ e $A \subseteq G$, denotamos $\{c\} + A$ simplesmente por $c + A$

Lema 1.22. *Sejam G um grupo abeliano finito com $t = r_2(G)$ e A, B subconjuntos não vazios de G.*

(a) Se $|A| + |B| > |G|$, então $A + B = G$.

(b) Se $|A| + |B| \geqslant |G| + 2^t + 1$, então $A \hat{+} B = G$.

Demonstração: *(a)* Fixe $g \in G$ um elemento qualquer e considere o conjunto $g - B = \{g - b \mid b \in B\}$. Como $|g - B| = |B|$, temos

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

Isso quer dizer que $A \cap (g - B) \neq \emptyset$, pois, caso contrário, $g - B \subseteq G \setminus A$ e $|g - B| \leq |G \setminus A| = |G| - |A|$, ou seja, $|A| + |g - B| \leq |G|$. Assim, existem $a \in A$, $b \in B$ tais que $a = g - b$, ou seja, $g = a + b$ e logo $G \subseteq A + B$. A inclusão contrária é imediata.

(b) Seja $g \in G$. Note que, como $|A| + |B| \geqslant |G| + 2^t + 1$ e $|g - A| = |A|$, temos

$$\begin{aligned} |G| + 2^t + 1 \leqslant |A| + |B| &= |(g - A)| + |B| = |(g - A) \cup B| + |(g - A) \cap B| \\ &\leqslant |G| + |(g - A) \cap B|. \end{aligned}$$

Assim, para cada $i \in [1, 1 + 2^t]$, existem $a_i \in A$ e $b_i \in B$ tais que $g - a_i = b_i$ e com a propriedade $a_i \neq a_j$ e $b_i \neq b_j$ para todo $i \neq j \in [1, 1 + 2^t]$. Se $a_i \neq b_i$ para algum $i \in [1, 1 + 2^t]$, então $g = a_i + b_i \in A \hat{+} B$.

Suponha então que $a_i = b_i$ para todo $i \in [1, 1 + 2^t]$, ou seja, temos $g = 2a_i$ para todo $i \in [1, 1 + 2^t]$. Considere o homomorfismo $\phi : G \longrightarrow G$ definido por $\phi(x) = 2x$ e observe que $\{a_1, \ldots, a_{2^t+1}\} \subseteq \phi^{-1}(g)$. Seja $H = \{y \in G \mid \text{ord}(y) \leqslant 2\} \leq G$. Pela definição de $r_2(G)$, temos $|H| = 2^t$. De fato, escreva $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ e note que para cada $i \in [1, r]$, tem-se

$$2|n_i \Rightarrow n_i = 2k_i \text{ com } k \in \mathbb{N}$$

e em C_{2k_i} há dois elementos de ordem 2: a identidade e $k_i e$ onde e é um gerador de C_{2k_i}. Daí, há 2^t elementos de ordem no máximo 2 em G e esses são os únicos pois se $2 \nmid n_i$ então C_{n_i} não pode conter elementos de ordem 2.

Afirmamos que $\phi^{-1}(g) \subseteq x_0 + H$ para algum $x_0 \in G$. De fato, seja $x_0 \in \phi^{-1}(g)$ e note que para qualquer $x \in \phi^{-1}(g)$, $x \neq x_0$, temos

$$g = 2x_0 = 2x \Rightarrow 2x - 2x_0 = 0 \Rightarrow 2(x - x_0) = 0 \Rightarrow x - x_0 \in H \Rightarrow x \in x_0 + H.$$

É claro que $x_0 \in x_0 + H$ pois $x_0 = x_0 + 0$ e $0 \in H$.

Assim, $\phi^{-1}(g) \subseteq x_0 + H$ e logo $|\phi^{-1}(g)| \leqslant |x_0 + H| = |H| = 2^t$. Mas isso é impossível visto que $|\phi^{-1}(g)| \geqslant |[1, 1 + 2^t]| = 2^t + 1$. Assim, não é possível que $a_i = b_i$ para todo $i \in [1, 1 + 2^t]$.

Concluímos que $G \subseteq A\hat{+}B$. A inclusão contrária é imediata. ■

O item *(a)* do lema acima será útil para a demonstração do Teorema de Cauchy-Davenport, a seguir. O segundo item, por sua vez, será de grande importância para resultados que envolvem a constante de Harborth que estudaremos no Capítulo 4.

Teorema 1.23 (Cauchy-Davenport)**.** *Sejam p primo e A e B subconjuntos não vazios de $\mathbb{Z}_p$. Então*

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

Demonstração: Sejam os conjuntos $A = \{\alpha_1, \ldots, \alpha_m\}$, $B = \{\beta_1, \ldots, \beta_n\}$ e $A+B = \{\gamma_1, \ldots, \gamma_l\}$. Se $|A|+|B|-1 > p$, então $|A|+|B| > p$ e pelo Lema 1.22, $A+B = G$. Daí, $|A+B| = |\mathbb{Z}_p| = p = \min\{p, |A|+|B|-1\}$. Considere agora $|A|+|B|-1 = m+n-1 \leqslant p$. Vamos usar indução sobre n.

Se $n = 1$, então $|A+B| = |A| = m = m+n-1$. Se $n = 2$, escreva $\beta = \beta_1 - \beta_2 \neq 0$ e suponha que $l < m+1 \leq p$. Observe que, dado $\alpha_i \in A$, se $\alpha_i + \beta \notin A$, então $\alpha_i + \beta_1 \neq \alpha_j + \beta_2$ para qualquer $1 \leq j \leq m$ e logo, $l \geqslant m+1$, contrariando o que supomos. Portanto, para todo $\alpha_i \in A$, temos $\alpha_i + \beta \in A$ e logo $\alpha_i + \mu\beta \in A$ para todo inteiro $\mu \geqslant 1$. Como $\mathbb{Z}_p$ pode ser gerado por qualquer um de seus elementos, em particular, pode ser gerado por um elemento de A e logo toda classe de resíduo módulo p pode ser representada da forma $\alpha_i + \mu\beta$, para algum inteiro μ. Daí, segue que $A = \mathbb{Z}_p$ e $|A| = p$. Isso nos conduz a uma contradição ao que assumimos sobre $m+1 \leq p$. Assim, $l \geqslant m+1$ e o teorema está provado para este caso.

Suponha agora que $n > 2$ e que o teorema é válido para todo $n' < n$. Suponha também que $l < p$. Vamos mostrar que $l \geqslant m+n-1$. Considere os conjuntos $A+B = \{\gamma_1, \ldots, \gamma_l\}$ e $\overline{B} = \{\beta_1, \beta_n\}$. Como $l+2-1 = l+1 \leq p$, aplicando a hipótese de indução a $A+B$ e $\overline{B}$, existem pelo menos $l+1$ elementos de $\mathbb{Z}_p$ que são ou da forma $\gamma_i + \beta_1$ ou da forma $\gamma_i + \beta_n$.

Observe que como

$$|(A+B)| + |\overline{B}| \geqslant l+1, \tag{1.1}$$

existe $\delta \in \mathbb{Z}_p$ tal que $\delta - \beta_1 \in A+B$ e $\delta - \beta_n \notin A+B$. De fato, é claro que existe $\delta \in \mathbb{Z}_p$ com $\delta - \beta_1 \in A+B$, já que $(A+B)+\overline{B} \subseteq \mathbb{Z}_p$. Agora, se para todo $\delta \in \mathbb{Z}_p$ tal que $\delta - \beta_1 \in A+B$ tivermos também $\delta - \beta_n \in A+B$ então, para todo $\gamma_i \in A+B$, existe $\gamma_j \in A+B$ tal que $\gamma_i + \beta_1 = \gamma_j + \beta_n$ e neste caso, a cardinalidade de $(A+B)+\overline{B}$ não pode ser maior que l, contradizendo (1.1).

Podemos reordenar os β's e γ's e existe r, com $1 \leq r < n$, tal que

$$\begin{array}{lll} \delta - \beta_s = \gamma_s & \text{para} & 1 \leq s \leq r \\ \delta - \beta_t = \epsilon_t & \text{para} & r < t \leq n \end{array}$$

onde para $r < t \leq n$, $\epsilon_t \neq \gamma_u$ para todo $1 \leq u \leq l$.

Afirmamos que nenhuma das classes de resíduos $\gamma_s - \beta_t$, $r < t \leq n$, $1 \leq s \leq r$ é elemento de A. De fato, se a afirmação não é verdadeira, devemos ter $\alpha + \beta_t = \gamma_s = \delta - \beta_s$ para algum $\alpha \in A$, $\beta_t, \beta_s \in B$, o que implica que $\alpha + \beta_s = \delta - \beta_t$ e, portanto, $\epsilon_t \in A+B$, uma contradição. Isso prova o que afirmamos.

Seja l' o número de elementos de $\mathbb{Z}_p$ da forma $\alpha_i + \beta_t$, com $1 \leq i \leq m$ e $r < t \leq n$. Da afirmação acima, estes elementos formam um subconjunto dos γ's não contendo $\gamma_1, \ldots, \gamma_r$. Portanto, $l' \leq l - r$ e aplicando a hipótese de indução a A e $B' = \{\beta_{r+1}, \ldots, \beta_n\}$, temos

$$l' \geqslant m + (n - r) - 1 \Rightarrow l \geqslant l' + r \geqslant m + n - 1.$$

Isso completa a prova do teorema. ■

Corolário 1.24. *Sejam $n \geqslant 2$, p um primo e $A_1, A_2, \ldots, A_n \subseteq \mathbb{Z}_p$. Então*

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

Demonstração: Vamos usar indução. Para $n = 2$, o resultado é idêntico ao Teorema de Cauchy-Davenport. Suponha então que o Corolário seja válido para $n = k$, ou seja,

$$|A_1 + A_2 + \cdots + A_k| \geqslant \min\left\{p, \sum_{i=1}^{k} |A_i| - k + 1\right\}.$$

Para $n = k + 1$, utilizando mais uma vez o Teorema de Cauchy-Davenport, temos

$$\begin{aligned} |(A_1 + A_2 + \cdots + A_k) + A_{k+1}| &\geqslant \min\{p, |A_1 + \cdots + A_k| + |A_{k+1}| - 1\} \\ &\geqslant \min\left\{p, \sum_{i=1}^{k} |A_i| - k + 1 + |A_{k+1}| - 1\right\} \\ &\geqslant \min\left\{p, \sum_{i=1}^{k+1} |A_i| - k - 1 + 1\right\} \\ &\geqslant \min\left\{p, \sum_{i=1}^{k+1} |A_i| - (k + 1) + 1\right\}. \end{aligned}$$

Assim, concluímos o desejado. ■

Na prática, o Corolário 1.24 é o que aplicamos quando nos referimos ao Teorema de Cauchy-Davenport.

1.3 Estabelecendo Algumas Definições

A partir de agora, vamos estudar os problemas de soma zero propriamente ditos. Para isso, precisamos fixar algumas notações que usaremos ao longo do trabalho. As notações que usamos aqui estão em concordância com os artigos [9, 19] e com a tese [15].

Seja G um grupo abeliano aditivo finito de expoente n. Existem muitas formas de explicitar uma sequência de elementos de G. Vamos fixar a seguinte:

$$S = g_1 \cdots g_l \text{ com } g_i \in G.$$

Em alguns casos, por simplicidade, podemos escrever

$$S = \prod_{g \in G} g^{v_g(S)}$$

onde $v_g(S) \geqslant 0$ é a multiplicidade de g em S, ou seja, o número de vezes em que o elemento g se repete na sequência S. S é dita livre de quadrados se $v_g(S) \leq 1$ para todo $g \in G$.

A multiplicidade máxima de S é dada por $h(S) = \max\{v_g(S) \,|\, g \in G\}$.

Dizemos que uma sequência T é uma subsequência de S se $v_g(T) \leq v_g(S)$ para todo $g \in G$ e escrevemos $T|S$. Neste caso, ST^{-1} ou $T^{-1}S$ denotam a subsequência de S obtida ao remover os elementos de T. Nesse sentido, se R, S são sequências de elementos de G, a sequência RS é a sequência obtida de R ao acrescentar os elementos de S. Podemos resumir isso assim:

$$R = \prod_{g \in G} g^{v_g(R)}, S = \prod_{g \in G} g^{v_g(S)} \Rightarrow RS = \prod_{g \in G} g^{v_g(R)+v_g(S)}.$$

Dadas S, S' sequências de elementos de G, a interseção de S e S' é dada por

$$S \cap S' = \prod_{g \in G} g^{\min\{v_g(S), v_g(S')\}}.$$

Note que $S \cap S'|S$ e $S \cap S'|S'$.

Denotamos por $|S|$ o tamanho (ou o número de elementos) de S. Note que

$$|S| = \sum_{g \in G} v_g(S).$$

Se $|S| = 0$ dizemos que S é a sequência trivial de elementos de G.

O suporte de S é o conjunto

$$\mathrm{supp}(S) = \{g \in G \,|\, v_g(S) > 0\}.$$

Usamos a notação $S \in \mathcal{F}(G)$ para dizer que S é uma sequência de elementos de G. Fica assim entendido que $\mathcal{F}(G)$ é o conjunto de todas as sequências de elementos de G de qualquer tamanho. $\mathcal{F}(G)$ é um monoide abeliano com a multiplicação $*$ de sequências dada por $S * S' = SS'$.

Se $S = g_1 \cdots g_k \in \mathcal{F}(G)$ e $A \subseteq [1, n-1]$, usamos a notação $\sigma_A(S)$ para expressar o conjunto de todas as possíveis somas dos elementos de S considerando os pesos de A, ou ainda, o conjunto de todas as somas A-ponderadas de S, a saber,

$$\sigma_A(S) = \left\{ \sum_{i=1}^{k} a_i g_i \,|\, a_i \in A \right\}.$$

Quando $A = \{1\}$, $\sigma_A(S)$ se reduz a um conjunto unitário. Assim, denotaremos por $\sigma(S) \in G$ a soma dos elementos de S. Um pouco mais geral, $\Sigma_A(S)$ é o conjunto de todas as possíveis somas dos elementos de todas as subsequências de

S considerando os pesos de A, exceto a subsequência trivial, ou seja,

$$\Sigma_A(S) = \left\{ \sum_{i \in I} a_i g_i \,|\, \emptyset \neq I \subseteq [1,k],\, a_i \in A \right\}.$$

Quando incluímos a subsequência trivial, convencionando que, independentemente do conjunto A, a única soma obtida é 0, usamos a notação

$$\Sigma_A^0(S) = \left\{ \sum_{i \in I} a_i g_i \,|\, I \subseteq [1,k],\, a_i \in A \right\}.$$

Em alguns casos, nos será útil conhecer informações a respeito das somas A-ponderadas de subsequências de um tamanho $0 < m < k$ específico. Nesses casos, usaremos a notação

$$\Sigma_{A,m}(S) = \left\{ \sum_{i \in I} a_i g_i \,|\, I \subseteq [1,k], |I| = m,\, a_i \in A \right\}.$$

Se $0 \in \sigma_A(S)$, dizemos que S é uma sequência de A-soma zero e se $0 \in \Sigma_A(S)$, dizemos que S possui uma subsequência não trivial de A-soma zero. Note que sempre é verdade que $\Sigma_A^0(S) = \Sigma_A(S) \cup \{0\}$, porém nem sempre $\Sigma_A^0(S) \setminus \{0\} = \Sigma_A(S)$.

Observação 1.25. Quando $A = \{a\}$ com $(a,n) = 1$ e $S = g_1 \cdots g_k \in \mathcal{F}(G)$, a função

$$\begin{array}{rcl} \varphi : \mathcal{F}(G) & \longrightarrow & \mathcal{F}(G) \\ S & \longmapsto & \varphi(S) = ag_1 \cdots ag_k \end{array}$$

é um isomorfismo. Isso segue do fato de que, quando $(a,n) = 1$, temos

$$\begin{array}{rl} f : G \longrightarrow & G \\ g \longmapsto & f(g) = ag \end{array}$$

um automorfismo de grupos. Além disso, temos

$$\sigma_A(S) = 0 \Leftrightarrow \sum_{i=1}^{k} g_i = 0 \Leftrightarrow a \sum_{i=1}^{k} g_i = \sum_{i=1}^{k} a g_i = 0 \Leftrightarrow \sigma_A(\varphi(S)) = 0.$$

Definição 1.26. *Sejam G um grupo aditivo abeliano finito com $\exp(G) = n$ e $A \subseteq \mathbb{Z} \setminus \{kn \,|\, k \in \mathbb{Z}\}$. Definimos a constante (ou invariante)*

(i) $E_A(G)$ como sendo o menor $t \in \mathbb{N}$ tal que toda sequência $S \in \mathcal{F}(G)$ de tamanho maior ou igual a t possui uma subsequência de A-soma zero de tamanho $|G|$;

(ii) $D_A(G)$ como sendo o menor $t \in \mathbb{N}$ tal que toda sequência $S \in \mathcal{F}(G)$ de tamanho maior ou igual a t possui uma subsequência não trivial de A-soma zero;

(iii) $s_A(G)$ como sendo o menor $t \in \mathbb{N}$ tal que toda sequência $S \in \mathcal{F}(G)$ de

tamanho maior ou igual a t possui uma subsequência de A-soma zero de tamanho n;

(iv) $\eta_A(G)$ *como sendo o menor $t \in \mathbb{N}$ tal que toda sequência $S \in \mathcal{F}(G)$ de tamanho maior ou igual a t possui uma subsequência não trivial de A-soma zero de tamanho no máximo n;*

(v) $g_A(G)$ *como sendo o menor $t \in \mathbb{N}$ tal que toda sequência $S \in \mathcal{F}(G)$ livre de quadrados e de tamanho maior ou igual a t, possui uma subsequência de A-soma zero de tamanho n.*

(vi) $O_A(G)$ *como sendo o menor $t \in \mathbb{N}$ tal que toda sequência $S \in \mathcal{F}(G)$ livre de quadrados e de tamanho maior ou igual a t, possui uma subsequência não trivial de A-soma zero.*

A é chamado *conjunto-peso* e problemas que envolvem a obtenção de valores exatos ou intervalos limitantes para esses invariantes são chamados *problemas de soma zero.*

Observe que não há perda de generalidade em assumir $A \subseteq [1, n-1]$, uma vez que dado $b \neq kn$, $k \in \mathbb{Z}$, tem-se $bg = \overline{b}g$ com $\overline{b} \equiv b \pmod n \in [1, n-1]$.

Por simplicidade, quando $A = \{1\}$, excluímos o conjunto A que aparece como índice de todas as notações acima.

1.4 O Teorema de Erdős-Ginzburg-Ziv

Em 1961, P. Erdős, A. Ginzburg e A. Ziv, demonstraram, em [7], o clássico Teorema de Erdős-Ginzburg-Ziv, no qual 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. Este resultado foi o precursor do estudo dos problemas de soma zero que seria formalizado posteriormente e daí a sua importância.

Teorema 1.27 (Erdős-Ginzburg-Ziv)**.** *Dada uma sequência de números inteiros com $2n-1$ elementos, onde n é um número natural, existe uma subsequência de comprimento n cuja soma de seus elementos é um múltiplo de n.*

Assumindo que o teorema é válido para $n = p$ primo, sua extensão para $n \in \mathbb{N}$ pode ser obtida com um argumento indutivo. De fato, supondo que o resultado seja válido para a e $b \in \mathbb{N}$, podemos mostrar sua validade também para ab, como apresentamos a seguir.

Considere $n = ab$ onde $1 < a \leqslant b < n$. De uma sequência $S = a_0 \cdots a_{2n-2}$ de tamanho $2n-1 > 2b-1$ existe uma subsequência T_1 tal que $\sigma(T_1) \equiv 0 \pmod b$. Tirando esses elementos da sequência original, nos restam $(2ab-1)-b = b(2a-1)-1$ inteiros. Como $2a-1 \geqslant 2$, temos $b(2a-1)-1 \geqslant 2b-1$ e logo existe $T_2 | ST_1^{-1}$, tal que $\sigma(T_2) \equiv 0 \pmod b$. Removendo-a, nos restam agora $b(2a-2)-1$ elementos. Podemos repetir esse processo $2a-1$ vezes obtendo $T_1, \ldots, T_{2a-1}$ subsequências de S e após obter a última subsequência, nos restam $(2ab-1)-(2a-1)b = b-1 < 2b-1$ elementos.

Agora observe que $\sigma(T_1) \cdots \sigma(T_{2a-1})$ é uma sequência de inteiros tal que

$$\sigma(T_j) \equiv 0 \pmod b \text{ com } j \in [1, 2a-1]. \tag{1.2}$$

Como supomos que o teorema é valido para a, a sequência acima possui uma subsequência $\sigma(T_{i_1}) \cdots \sigma(T_{i_a})$ tal que

$$\sum_{j=1}^{a} \sigma(T_{i_j}) \equiv 0 \pmod{a}. \tag{1.3}$$

Como cada $\sigma(T_{i_j})$ é a soma de b elementos de S, a soma em (1.3) pode ser vista como uma soma de ab elementos elementos de S. Assim, $T = T_1 \cdots T_{2a-1}$ é uma subsequência de S de tamanho ab cuja soma é $\sigma(T) = \sum_{j=1}^{a} \sigma(T_{i_j})$ e temos

$$\begin{aligned} \sigma(T) &\equiv 0 \pmod{b} \text{ por } (1.2), \\ \sigma(T) &\equiv 0 \pmod{a} \text{ por } (1.3). \end{aligned}$$

Isso quer dizer que $\sigma(T) \equiv 0 \pmod{ab}$. Daí, T é a subsequência procurada e logo o teorema é válido para $ab = n$. Como todo número natural é produto de primos e assumimos que o teorema é válido para para primos, concluímos que vale para todo $n \in \mathbb{N}$.

Para o caso em que n é primo, existem inúmeras demonstrações e escolhemos duas delas para apresentar aqui. Essas demonstrações são obtidas como aplicação dos teoremas da seção 1.2.

1.4.1 Demonstração via Cauchy-Davenport

Teorema 1.28 (Erdős-Ginzburg-Ziv para p primo)**.** *Dada uma sequência de números inteiros com $2p-1$ elementos, onde p é um número natural primo, existe uma subsequência de comprimento p cuja soma de seus elementos é um múltiplo de p.*

Demonstração: Seja $S = a_0 \cdots a_{2p-2}$ uma sequência de inteiros de tamanho $2p-1$. Vamos mostrar que existe uma subsequência $T = a_{i_1} \cdots a_{i_p}$ tal que

$$a_{i_1} + a_{i_2} + \cdots + a_{i_p} \equiv 0 \pmod{p}.$$

Escrevendo $a_i \equiv a'_i \pmod{p}$ com $a'_i \in [1, p-1]$, vamos reordenar os inteiros a_i de modo que

$$0 \leqslant a'_0 \leqslant \cdots \leqslant a_{2p-2} \leqslant p-1.$$

Temos dois casos:

Caso 1. Existe i, $1 \leqslant i \leqslant p-1$ tal que $a'_i = a'_{i+p-1}$. Desta forma, como organizamos os $a'_i{}'s$ em ordem crescente, temos que $a'_i = \cdots = a'_{i+p-1}$ e como $a'_i \equiv a_i \pmod{p}$, decorre que $a_i \equiv a_{i+1} \equiv \cdots \equiv a_{i+p-1} \pmod{p}$. Fazendo a soma, obtemos

$$a_i + a_{i+1} + \cdots + a_{i+p-1} \equiv pa_i \equiv 0 \pmod{p}$$

e $a_i a_{i+1} \cdots a_{i+p-1}$ é a subsequência procurada.

Caso 2. $a'_i \neq a'_{i+p-1}$ para todo $i \in [1, p-1]$. Definimos em $\mathbb{Z}_p$ os seguintes subconjuntos de dois elementos:

$$A_i = \{a'_i, a'_{i+p-1}\}.$$

Pelo Corolário 1.24, temos

$$|A_1 + A_2 + \cdots + A_{p-1}| \geqslant \min\{p, 2(p-1) - (p-1) + 1\} = p.$$

Agora, como $A_1 + \cdots + A_{p-1} \subseteq \mathbb{Z}_p$, segue que $A_1 + \cdots + A_{p-1} = \mathbb{Z}_p$. Daí, $-a_0' \in A_1 + \cdots + A_{p-1}$, ou seja,

$$-a_0 \equiv a_{j_1} + \cdots + a_{j_{p-1}} \pmod p \Rightarrow a_0 + a_{j_1} + \cdots + a_{j_{p-1}} \equiv 0 \pmod p$$

e $a_0 a_{j_1} \cdots a_{j_{p-1}}$ é a subsequência procurada. ■

1.4.2 Demonstração via Chevalley-Warning

Teorema 1.29 (Erdős-Ginzburg-Ziv para p primo)**.** *Dada uma sequência de números inteiros com $2p-1$ elementos, onde p é um número natural primo, existe uma subsequência de comprimento p cuja soma de seus elementos é um múltiplo de p.*

Demonstração: Seja $S = a_1 \cdots a_{2p-1}$ uma sequência de inteiros. Considere os polinômios:

$$f_1(x_1, \ldots, x_{2p-1}) = \sum_{j=1}^{2p-1} x_j^{p-1}$$
$$f_2(x_1, \ldots, x_{2p-1}) = \sum_{j=1}^{2p-1} a_j' x_j^{p-1}$$

onde $a_j' \equiv a_j \pmod p$ para todo $j \in [1, 2p-1]$. Observe que $\partial f_1 + \partial f_2 = 2(p-1) < 2p-1$. Logo, podemos aplicar o Teorema de Chevalley-Warning que nos garante que existe uma $(2p-1)$-upla $(b_1, \ldots, b_{2p-1}) \neq (0, \ldots, 0)$ tal que

$$f_1(b_1, \ldots, b_{2p-1}) \equiv f_2(b_1, \ldots, b_{2p-1}) \equiv 0 \pmod p.$$

Lembrando que

$$b_j^{p-1} \equiv \begin{cases} 0 \pmod p \iff b_j \equiv 0 \pmod p \\ 1 \pmod p \iff b_j \not\equiv 0 \pmod p \end{cases}$$

temos que, de f_1, $b_j \not\equiv 0 \pmod p$ para exatamente p elementos b_j's, digamos, b_{j_i} com $i \in [1, p]$. Daí, reordenando os monômios de f_2 e aplicando a solução $(b_1, \ldots, b_{2p-1})$, obtemos:

$$\underbrace{a_{j_1} b_{j_1}^{p-1}}_{a_{j_1}} + \cdots + \underbrace{a_{j_p} b_{j_p}^{p-1}}_{a_{j_p}} + \underbrace{a_{j_{p+1}} b_{j_{p+1}}^{p-1}}_{0} + \cdots + \underbrace{a_{j_{2p-1}} b_{j_{2p-1}}^{p-1}}_{0} \equiv 0 \pmod p$$

e logo $a_{j_1} + \cdots + a_{j_p} \equiv 0 \pmod p$ e $a_{j_1} \cdots a_{j_p}$ é a subsequência procurada. ■

1.4.3 Versão Formalizada

Como, pelo que vimos na Seção 1.1, o conjunto dos inteiros módulo n é um grupo aditivo cíclico, o Teorema de Erdős-Ginzburg-Ziv pode ser estendido de maneira geral a um grupo cíclico de ordem n, nos permitindo concluir que $s(C_n) \leqslant 2n-1$.

Por outro lado, observe que a sequência

$$S = 0^{n-1}1^{n-1}$$

tem tamanho $2n-2$ e não possui nenhuma subsequência cuja soma seja um múltiplo de n. Isso quer dizer que $2n-1$ encontrado por P. Erdős, A. Ginzburg e A. Ziv é o menor tamanho que uma sequência pode assumir para que possamos garantir a existência de uma subsequência de tamanho n de soma zero, ou seja, $s(C_n) \geqslant 2n-1$.

Assim, sempre que nos referirmos ao Teorema de Erdős-Ginzburg-Ziv, a referência será a seguinte:

Teorema 1.30. *Dado $n \in \mathbb{N}$, $n \geqslant 2$, temos $s(C_n) = 2n-1$.*

Esta é a versão formalizada apresentada por Harborth, em [14], em 1973. A partir disso, o Teorema de Erdős-Ginzburg-Ziv passou a ser um resultado da teoria dos problemas de soma zero e, posteriormente, a constante s_A recebeu o nome *constante de Erdős-Ginzburg-Ziv*.

Capítulo 2

Relação entre E_A e D_A

Seja G um grupo abeliano finito com $|G| = n$. Não é difícil ver que, para $A \subseteq [1, \exp(G) - 1]$,

$$E_A(G) \geqslant D_A(G) + n - 1. \tag{2.1}$$

De fato, considere $S \in \mathcal{F}(G)$ com $|S| = D_A(G) - 1$ de forma que S não possui subsequência de A-soma zero e observe que a sequência

$$S' = S0^{n-1}$$

não possui subsequência de A-soma zero de tamanho n, uma vez que uma subsequência de A-soma zero de S' de tamanho n implica em uma subsequência de A-soma zero de S de algum tamanho. Assim, da definição de E_A, segue que

$$E_A(G) \geqslant |S'| + 1 = |S| + (n - 1) + 1 = D_A(G) + n - 1.$$

A igualdade

$$E_A(G) = D_A(G) + n - 1 \tag{2.2}$$

foi provada em 1990 por W.D. Gao, [23], no caso em que $A = \{1\}$. O resultado para $A \subseteq [1, \exp(G)-1]$ qualquer foi provado primeiro para o caso em que $G = C_n$ por P. Yuan e X. Zeng em 2010, [29], e em [12] foi provado o caso geral.

Nosso trabalho neste capítulo será estudar as constantes D_A e E_A através de uma coletânea de resultados que nos permitirão conhecer o comportamento de cada constante frente a alguns grupos. Em seguida apresentamos a prova da relação (2.2) para o caso em que $G = C_p$, p primo. Os resultados que compõem este capítulo foram obtidos dos artigos [2, 3, 4, 19, 20, 28].

Nosso objetivo aqui é ilustrar a natureza construtiva dos resultados que solucionam problemas de soma zero. Além disso, conhecer os resultados para grupos mais básicos é de extrema importância para o estudo envolvendo grupos mais gerais. Portanto, muitos do resultados que apresentaremos neste capítulo serão citados nos capítulos seguintes, deixando claro assim o caráter colaborativo que o estudo dos problemas de soma zero apresenta.

2.1 Resultados para D_A

Comecemos com um resultado que será citado várias vezes daqui em diante. Esse é um resultado de Adhikari *et al.*, disponível em [2].

Teorema 2.1. *Sejam G um grupo abeliano finito, $S \in \mathcal{F}(G)$ e $A = \{-1, 1\}$.*

(a) Se $|S| \geqslant \log_2 |G| + 1$ e G não é um 2-grupo elementar, então S possui uma subsequência própria não trivial de A-soma zero.

(b) Se $|S| > \log_2 |G| + 1$ e G não é um 2-grupo elementar de posto par, então S possui uma subsequência própria não trivial de A-soma zero de tamanho par.

Demonstração: *(a)* Seja $S = g_0 g_1 \cdots g_l \in \mathcal{F}(G)$ com $l \geqslant \log_2 |G|$. Note que $|S| = l + 1 > \log_2 |G|$. Defina $S' = g_0^{-1} S$. De acordo com a combinatória elementar, existem 2^l subconjuntos $I \subseteq [1, l]$, a cada um deles correspondendo a uma subsequência S'_I do tipo

$$S'_I = \prod_{i \in I} g_i \in \mathcal{F}(G).$$

Suponha primeiro que existam $I, J \subseteq [1, l]$ com $\sigma(S'_I) = \sigma(S'_J)$. Como $I \setminus J = I \setminus (I \cap J)$ e $J \setminus I = J \setminus (I \cap J)$, removendo os elementos comuns entre I e J, encontramos

$$\sigma(S'_{I \setminus J}) = \sigma(S'_I) - \sigma(S'_{I \cap J}) = \sigma(S'_J) - \sigma(S'_{I \cap J}) = \sigma(S'_{J \setminus I}).$$

Note que, como $I \neq J$, temos $I \setminus J \neq \emptyset$ ou $J \setminus I \neq \emptyset$, além de que $(I \setminus J) \cap (J \setminus I) = \emptyset$. Isso nos dá

$$T = S'_{(I \setminus J) \cup (J \setminus I)} = S'_{I \setminus J} S'_{J \setminus I},$$

uma subsequência de S' (e, portanto, própria de S) tal que

$$\sum_{i \in I \setminus J} (1) g_i + \sum_{i \in J \setminus I} (-1) g_i = 0,$$

ou seja, T é uma subsequência de A-soma zero própria de S.

Suponha agora que $\sigma(S'_I) \neq \sigma(S'_J)$ para todo $I \neq J$. Lembrando que $2^l \geqslant |G|$, observe que nesse caso devemos ter $2^l = |G|$, pois, caso contrário, o Princípio das Casas dos Pombos nos garante a existência de subconjuntos diferentes $I, J \subseteq [1, l]$ satisfazendo $\sigma(S'_I) = \sigma(S'_J)$, contrariando o que supomos. Isso nos dá $|S| = l + 1 = \log_2 |G| + 1 \in \mathbb{Z}$. Além disso, como cada uma das $2^l = |G|$ subsequências S'_I devem fornecer somas A-ponderadas distintas em G, cada elemento de G é obtido com uma subsequência de S', sendo que o 0 é obtido com a sequência trivial correspondente ao conjunto $\emptyset$. Em particular, existem $T_1, T_2 | S'$ tais que $\sigma(T_1) = g_0$ e $\sigma(T_2) = -g_0$. Assim, se T_1 é subsequência própria de S', então $g_0 T_1$ é subsequência própria de S de A-soma zero e o mesmo podemos dizer a respeito de $g_0 T_2$, caso T_2 seja própria. Para finalizar a prova nos resta considerar o caso em que $-g_0 = g_0$ e $T_1 = T_2 = S$.

Como todos os elementos de G podem ser obtidos através se subsequências de S', podemos dizer que $G = \langle \mathrm{supp}(S') \rangle$. Além disso, como G não é 2-grupo elementar, existe $g \in \mathrm{supp}(S')$ tal que $2g \neq 0$, ou seja, $-g \neq g$.

Agora, lembrando que quando o conjunto peso é $A = \{-1, 1\}$ trocar um elemento por seu inverso em S não muda o fato de ser subsequência de A-soma zero ou não, não há problema em considerar tudo o que fizemos acima para a sequência $S_0 = g^{-1}S(-g)$. Note que $\sigma(S_0) = \sigma(S) - 2g$ e $\sigma(S_0') = \sigma(S') - 2g$, onde $S_0' = g^{-1}S'(-g)$. Ao refazer a demonstração acima para S_0, em tudo temos a mesma conclusão, exceto o último caso, em que $\sigma(S_0') = g_0$. Isso porque se $\sigma(S_0') = g_0$, então $2g = \sigma(S') - \sigma(S_0') = g_0 - g_0 = 0$, uma contradição. Deve haver, portanto, uma subsequência própria T de S_0' com $\sigma(T) = g_0$ ou $-g_0$ que em qualquer caso nos fornece uma subsequência própria de S_0 de A-soma zero. Como já mencionamos acima, uma vez que S_0 difere de S apenas por um elemento que trocamos por seu inverso, seque que S possui uma subsequência própria de A-soma zero.

(b) Como no item anterior, considere $S = g_0 \cdots g_l \in \mathcal{F}(G)$ com $l \geqslant \log_2 |G| + 1$ e faça $S' = g_0^{-1}S$. De novo, pela combinatória elementar, existem 2^{l-1} subconjuntos $I \subset [1, l]$ com $|I|$ ímpar e cada I determina uma subsequência de S' da forma

$$S_I' = \prod_{i \in I} g_i.$$

Suponha que existam $I, J \subseteq [1, l]$, $I \neq J$ com $\sigma(S_I') = \sigma(S_J')$. Como antes, ao remover os termos comuns entre I e J, obtemos $\sigma(S'_{I \setminus J}) = \sigma(S'_{J \setminus I})$ e

$$T = S'_{(I \setminus J) \cup (J \setminus I)}$$

é subsequência de A-soma zero de S' (e, portanto, própria de S). Para ver que $|T|$ é par, basta notar que, como $(I \setminus J) \cap (J \setminus I) = \emptyset$ (justificamos isso no item anterior) e $|I|$, $|J|$ são ímpares, temos

$$|(I \setminus J) \cup (J \setminus I)| = |I \setminus J| + |J \setminus I| = |I| + |J| - 2|I \cap J|$$

um número par.

Suponha agora que subconjuntos distintos de $[1, l]$ sempre forneçam somas A-ponderadas distintas para as subsequências determinadas por eles. Como $2^{l-1} \geqslant |G|$, mais uma vez o Princípio das Casas dos Pombos nos leva a concluir que $2^{l-1} = |G|$ e, portanto, cada elemento de G pode ser obtido através da soma A-ponderada de alguma subsequência de S' de tamanho ímpar. Em particular, há $T_1, T_2 | S'$ tais que $\sigma(T_1) = g_0$ e $\sigma(T_2) = -g_0$. Se uma delas é subsequência própria de S', então acrescentando g_0, obtemos uma subsequência própria de tamanho par de A-soma zero.

Para o caso em que nenhuma delas é própria, ou seja, quando $g_0 = -g_0$ e $T_1 = T_2 = S'$, tomamos $g \in \text{supp}(S')$ tal que $2g \neq 0$ (que existe pois, como no item anterior, G não é 2-grupo elementar e $G = \langle \text{supp}(S') \rangle$) e consideramos $S_0 = g^{-1}S(-g)$. O restante da demonstração segue idêntico ao item anterior, sendo importante observar que ao garantir uma subsequência própria de tamanho ímpar de S_0', obtemos uma subsequência própria de tamanho par de S_0, como queríamos. ■

Como consequência direta, apresentamos o corolário abaixo que nos será útil no capítulo seguinte, fornecendo uma forma prática de aplicar o teorema anterior.

Corolário 2.2. *Seja G um grupo abeliano finito, $S \in \mathcal{F}(G)$, $A = \{-1, 1\}$.*

(a) *Se $|S| \geqslant \lfloor \log_2 |G| \rfloor + 1$, então S possui uma subsequência não trivial de A-soma zero e de tamanho no máximo $\lfloor \log_2 |G| \rfloor + 1$.*

(b) *Se $|S| \geqslant \lfloor \log_2 |G| \rfloor + 2$, então S possui uma subsequência não trivial de A-soma zero de tamanho par e no máximo $\lfloor \log_2 |G| \rfloor + 2$.*

Demonstração: Para provar o item *(a)*, basta aplicar o Teorema 2.1 *(a)* a uma subsequência de S de tamanho $\lfloor \log_2 |G| \rfloor + 1$. Para o item *(b)*, aplicamos o Teorema 2.1 *(b)* a uma subsequência de S de tamanho $\lfloor \log_2 |G| \rfloor + 2$. ■

Observe que estamos aplicando o Teorema 2.1 para garantir a existência de uma subsequência de A-soma zero, porém não temos a hipótese de que G não é 2-grupo elementar, logo não podemos garantir que a subsequência encontrada é própria. É o que acontece também quando aplicamos o Teorema 2.1 para obter o corolário abaixo. Este é, essencialmente, o primeiro item do corolário anterior.

Corolário 2.3. *Se G é um grupo abeliano finito, então*

$$D_{\pm}(G) \leqslant \lfloor \log_2 |G| \rfloor + 1.$$

Teorema 2.4. *Se $A = \{a\} \subseteq [1, n-1]$ e $(a, n) = 1$, então $D_A(C_n) = n$.*

Demonstração: Seja $S = x_1 x_2 \cdots x_n \in \mathcal{F}(C_n)$. Primeiramente, observe que

$$\sum_{i=1}^{m} a x_i = a \sum_{i=1}^{m} x_i.$$

Daí, como $(a, n) = 1$, S possui subsequência de soma zero, se e somente se, S possui subsequência de A-soma zero, pela Observação 1.25.

Considere as somas

$$\begin{array}{rcl} S_1 & = & x_1, \\ S_2 & = & x_1 + x_2, \\ & \vdots & \\ S_n & = & x_1 + \cdots + x_n. \end{array}$$

Note que se $S_i \neq S_j$ para todo $i, j \in [1, n], i \neq j$ então $\{S_i\}_{i=1}^{n} = C_n$ e logo existe $k \in [1, n]$ tal que $S_k = 0$, ou seja, $x_1 \cdots x_k | S$ é subsequência de soma zero. Se existem duas somas iguais, digamos $S_i = S_j$, sem perda de generalidade podemos supor $i > j$ e a sequência

$$S_i (S_j)^{-1} = x_{j+1} x_{j+2} \cdots x_i$$

é uma subsequência de S de soma zero. Isso mostra que $D_A(C_n) \leqslant n$.

Por outro lado, a sequência

$$S = 1^{n-1}$$

é tal que para qualquer $k \in [1, n-1]$, $\sum_{i=1}^{k} a \cdot 1 = k \cdot a \neq 0$ pois $(a, n) = 1$. Concluímos, portanto, a igualdade. ■

Teorema 2.5. *Se $A = \{a, n-a\} \subseteq [1, n-1], (a, n) = 1$, então $D_A(C_n) = 1 + \lfloor \log_2 n \rfloor$.*

Demonstração: Como $(a, n) = 1$, temos $D_A(C_n) = D_\pm(C_n)$ pela Observação 1.25.

Para ver que $D_\pm(C_n) \geqslant 1 + \lfloor \log_2 n \rfloor$, considere a sequência $S = \prod_{i=0}^{r} 2^i$ onde $r \in \mathbb{Z}$ é tal que $2^{r+1} < n < 2^{r+2}$ e observe que é impossível obter subsequência de S de A-soma zero de qualquer tamanho. De fato, a maior soma possível considerando os pesos -1 e 1, resulta num número cujo valor absoluto é menor ou igual a $2^{r+1} - 1 < n$ e não pode ser 0 pois isso contraria a unicidade da expansão binária. Daí $D_\pm(C_n) > |S| = r + 1 \geqslant \lfloor \log_2 n \rfloor$ pois

$$2^{r+2} > n \Rightarrow r + 2 > \log_2 n \Rightarrow r + 2 > \lfloor \log_2 n \rfloor \Rightarrow r + 1 \geqslant \lfloor \log_2 n \rfloor.$$

A desigualdade contrária segue do Corolário 2.3. ∎

Quando $A = [1, n-1]$, podemos obter o valor de $D_A(G)$ para todo G com $\exp(G) = n$, conforme o teorema a seguir.

Teorema 2.6. *Sejam $A = [1, n-1]$ e G um grupo abeliano finito com $\exp(G) = n$. Então $D_A(G) = r_n(G) + 1$.*

Demonstração: Como G é abeliano finito, pelo Teorema 1.8, temos

$$G \simeq C_{n_1} \oplus \cdots \oplus C_{n_q} \oplus C_n,$$

com $q, n_i \in \mathbb{N}$ e $i \in [1, q]$. Observe que se $n | n_1$, então $n = n_1$ e existe $g \in C_{n_1}$ tal que $ng = 0 \in C_{n_1}$. Podemos pensar assim para cada $i \in [1, q]$ tal que $n | n_i$ e obtemos $g_i \in C_{n_i}$ com $ng_i = 0$. Isso nos permite obter um subconjunto de G formado pelos elementos $(0, \ldots, 0, g_i, 0, \ldots, 0)$, de cardinalidade $r_n(G)$ e independente (lembre-se da definição de $r_n(G)$, dada no final da Seção 1.1). A sequência formada por esses elementos não pode conter uma subsequência não trivial de A-soma zero pois isso contraria a independência do conjunto. Assim, $D_A(G) \geqslant r_n(G) + 1$.

Por outro lado, seja $S = g_1 \cdots g_{r_n(G)+1} \in \mathcal{F}(G)$. Se S não é livre de quadrados, então S possui uma subsequência de A-soma zero de tamanho 2. Suponha então S livre de quadrados. Se existe $i \in [1, r_n(G)+1]$ tal que $\mathrm{ord}(g_i) = d < n$, então $d \in A$ e $dg_i = 0$, ou seja, g_i é uma subsequência de A-soma zero de S. Se $\mathrm{ord}(g_i) = n$ para todo $i \in [1, r_n(G) + 1]$, então o conjunto $B = \{g_1, \ldots, g_{r_n(G)+1}\}$ não pode ser independente pois, caso contrário, $C_n^{r_n(G)+1} \leq G$ e $|\{i \in \mathbb{N} \,|\, n | n_i\}| \geqslant r_n(G) + 1$, contrariando a definição de $r_n(G)$. Assim, da definição de conjunto independente, existem $a_1, \ldots, a_{r_n(G)+1} \in [0, n-1]$, não todos nulos, tais que

$$\sum_{i=1}^{r_n(G)+1} a_i g_i = 0$$

e os elementos de $\{g_i \,|\, a_i \neq 0\}$ formam uma subsequência de A-soma zero de S. Isso conclui a demonstração. ∎

Como consequência direta, temos o seguinte resultado.

Corolário 2.7. *Dados $n, r \in \mathbb{N}$, sejam $G = C_n^r$ e $A = [1, n-1]$. Então $D_A(G) = r(G) + 1$. Em particular, $D_A(C_n) = 2$.*

Proposição 2.8. *Se $A = [1, r]$ onde $1 < r < n$, então $D_A(C_n) = \lceil \frac{n}{r} \rceil$.*

Demonstração: Seja $S = s_1 \cdots s_{\lceil \frac{n}{r} \rceil} \in \mathcal{F}(C_n)$ de tamanho $\lceil \frac{n}{r} \rceil$ e considere

$$S' = s_1^r s_2^r \cdots s_{\lceil \frac{n}{r} \rceil}^r.$$

Observe que $|S'| \geqslant n$. Daí, pelo Teorema 2.4, S possui uma subsequência de soma zero, digamos, T.

Sejam $\{s_{i_1}, \ldots, s_{i_k}\} = \text{supp}(T)$ e $t_j = v_{s_{i_j}}(T)$. Observe que $1 \leqslant t_j \leqslant r$ para cada $j \in [1, k]$.

Neste caso, T ser uma sequência de soma zero implica em

$$\sum_{j=1}^{k} t_j s_{i_j} = 0,$$

ou seja, $s_{i_1} \cdots s_{i_k}$ é uma subsequência de S de A-soma zero de S. Isso mostra que $D_A(C_n) \leqslant \lceil \frac{n}{r} \rceil$.

Por outro lado, considerando

$$T = 1^{\lceil \frac{n}{r} \rceil - 1},$$

dada qualquer subsequência não vazia de T, digamos $s_{j_1} \cdots s_{j_l}$ temos

$$0 < \sum_{i=1}^{l} a_i s_{j_i} < rl \leqslant r \left(\left\lceil \frac{n}{r} \right\rceil - 1 \right) \leqslant n - r < n - 1$$

qualquer que seja a forma de escolher os elementos $a_i \in A$. Portanto, $D_A(C_n) \geqslant \lceil \frac{n}{r} \rceil$ e a igualdade segue. ■

2.2 Resultados para E_A

O primeiro resultado que podemos destacar a respeito da constante E_A foi provado antes mesmo de o estudo dos problemas de soma zero ser formalizado: O Teorema 1.30 de Erdős-Ginzburg-Ziv que apresentamos no Capítulo 1.

Teorema 2.9. *Se $A = \{1\}$, então $E_A(C_n) = 2n - 1$.*

Lembrando que quando G é cíclico, temos $|G| = \exp(G)$ e logo as definições de E_A e s_A coincidem.

Proposição 2.10. *Se n é par e $A = \{a, n-a\} \subseteq [1, n-1]$, $(a, n) = 1$, então*

$$E_A(C_n) \leqslant n + \lfloor \log_2 n \rfloor.$$

Demonstração: Seja $S = x_1 \cdots x_N$ com $N = n + \lfloor \log_2 n \rfloor$. Vamos reordenar S de forma que $x_i = x_{i+1}$ para todo $i \in [1, 2t-1]$, i ímpar e $x_i \neq x_j$ para todo $i, j \in [2t+1, N]$, $i \neq j$.

Observe que $N - 2t \leqslant n$ pois $\{x_{2t+1}, \ldots, x_N\} \subseteq C_n$ e $|\{x_{2t+1}, \ldots, x_N\}| = N - 2t$. Assim, $2t \geqslant N - n = \lfloor \log_2 n \rfloor$. Considere $B = \{r_1, \ldots, r_l\} \subseteq [2t+1, N]$

de tal forma que $|B|$ seja par e B seja o maior com a propriedade de que existem $\epsilon_1, \ldots, \epsilon_l \in \{-1, 1\}$ com

$$\sum_{j=1}^{l} \epsilon_j x_{r_j} = 0.$$

Temos $l + 2t \geqslant n$. De fato, se $l + 2t < n$, como os números $l + 2t$ e n são ambos pares, teríamos $l + 2t \leqslant n - 2$ e o conjunto $C = [2t + 1, N] \setminus \{r_1, \ldots, r_l\}$ seria tal que

$$|C| = N - 2t - l \geqslant N - n + 2 = \lfloor \log_2 n \rfloor + 2 > \log_2 n + 1.$$

Daí, pelo Corolário 2.2 *(b)*, existem $\emptyset \neq B' \subseteq C$ com $|B'|$ par e $\epsilon_j \in \{-1, 1\}$ para cada $j \in B'$ tal que

$$\sum_{j \in B'} \epsilon_j x_j = 0$$

e $B \cup B'$ contradiz a maximalidade de B. Podemos então escrever $l + 2t = n + r$ com $r \geqslant 0$.

Agora, como l e n são pares, temos que r também é par. Escreva $r = 2r'$ e note que a sequência

$$T = x_{2r'+1} x_{2r'+2} \cdots x_{2t} x_{r_1} \cdots x_{r_l}$$

tem n elementos e

$$\sum_{j=r'+1}^{t} (x_{2j} - x_{2j-1}) + \sum_{j=1}^{l} \epsilon_j x_{r_j} = 0.$$

Assim, T é a subsequência de A-soma zero procurada. ■

Mostraremos a seguir que se n é ímpar, a proposição anterior também é válida. Para isso, precisaremos de alguns resultados auxiliares.

Definição 2.11. *Sejam m um inteiro positivo e $S = x_1 \cdots x_n$ uma sequência de números inteiros. Dizemos que S é completa com respeito a m se, para todo d divisor positivo de m tem-se*

$$|\{j \in [1, n] \,|\, x_j \not\equiv 0 \pmod{d}\}| \geqslant d - 1.$$

Dada S uma sequência completa com respeito a um inteiro positivo m, uma propriedade importante é que podemos obter subsequências de S que também são completas com respeito a m. Isso é o que os lemas abaixo nos fornecem.

Lema 2.12. *Se $S = x_1 \cdots x_n$ é completa com respeito a m e $n \geqslant m$, então existe $j_0 \in [1, n]$ tal que $S x_{j_0}^{-1}$ é completa com respeito a m.*

Demonstração: Sejam $d_1, \ldots, d_s$ os divisores de m que satisfazem

$$|\{j \in [1, n] \,|\, x_j \not\equiv 0 \pmod{d_i}\}| = d_i - 1, \qquad i \in [1, s].$$

Vamos reordenar os d_i's de modo que $m \geqslant d_1 > \cdots > d_s$. Considere

$$D_i = \text{mmc}(d_1, \ldots, d_i)$$
e
$$U_i = \{j \in [1,n] \,|\, x_j \not\equiv 0 \pmod{d_i}\}.$$

Vamos mostrar que $|\bigcup_{i=1}^{s} U_i| < m$. Isso é suficiente para que possamos escolher $j_0 \in [1,n] \setminus \bigcup_{i=1}^{s} U_i$ de modo que a sequência $Sx_{j_0}^{-1}$ obedeça a Definição 2.11.

Agora note que, para cada $i \in [1,s]$, $\bigcup_{k=1}^{i} U_k = \{j \in [1,n] \,|\, x_j \not\equiv 0 \pmod{D_i}\}$ e $\bigcup_{k=1}^{i} U_k = \bigcup_{k=1}^{i-1} U_k$ se $D_{i-1} = D_i$. Isso quer dizer que, na verdade,

$$\bigcup_{k=1}^{s} U_k = U_1 \cup \bigcup_{D_k > D_{k-1}} U_k.$$

Para os k's que aparecem da expressão acima, temos $D_k > d_{k-1}$ e sabemos que $D_k = \text{mmc}(D_{k-1}, d_k)$. Isso implica que, para os k's > 1, $D_k - D_{k-1} \geqslant D_{k-1} \geqslant d_{k-1} > d_k - 1$. Como $D_1 > d_1 - 1$, temos

$$\begin{aligned}
\left|\bigcup_{k=1}^{s} U_k\right| &\leqslant |U_1| + \sum_{D_k > D_{k-1}} |U_k| \\
&= d_1 - 1 + \sum_{D_k > D_{k-1}} (d_k - 1) \\
&< D_1 + \sum_{k=1}^{s} (D_k - D_{k-1}) \\
&= D_s \leqslant m.
\end{aligned}$$

Isso completa a prova do lema. ∎

Lema 2.13. *Se $S = x_1 \cdots x_n$ é uma sequência completa com respeito a m, então existem $j_1, \ldots, j_{m-1} \in [1,n]$ tais que a sequência $x_{j_1} \cdots x_{j_{m-1}}$ é completa com respeito a m.*

Demonstração: Observe que, como m divide a si mesmo, temos $|\{j \in [1,n] \,|\, x_j \not\equiv 0 \pmod{m}\}| \geqslant m - 1$. Em particular, $n \geqslant m - 1$. Se $n = m - 1$, nada temos a fazer. Se $n \geqslant m$, aplicamos recursivamente o Lema 2.12 $n - (m-1)$ vezes e obtemos a sequência desejada. ∎

Teorema 2.14. *Se $S = x_1 \cdots x_n$ é completa com respeito a m, então para todo $b \in \mathbb{Z}$, existem $\epsilon_1, \ldots, \epsilon_n \in \{0,1\}$ tais que*

$$\sum_{j=1}^{n} \epsilon_j x_j \equiv b \pmod{m}.$$

Demonstração: Vamos usar indução sobre m. Se $m = 1$ então $b \equiv 0 \pmod 1$ para todo $b \in \mathbb{Z}$, logo, basta escolher $\epsilon_j = 0$ para todo $j \in [1,n]$.

Suponha então que dado $k \geqslant 2$, o resultado seja válido para todo $m < k$ e seja $S = x_1 \cdots x_n$ sequência completa com respeito a k. Vamos mostrar que o resultado vale também para $m = k$.

Da definição, como k divide a si mesmo, temos

$$|\{j \in [1,n] \,|\, x_j \not\equiv 0 \pmod{k}\}| \geqslant k-1,$$

ou seja, existem pelo menos $k-1$ elementos x_j's tais que $k \nmid x_j$. Sem perda de generalidade, podemos assumir que $k \nmid x_1$. Dado $a \in \mathbb{Z}$, seja $\overline{a}$ a classe de resíduo de a módulo k. Para $A \subseteq \mathbb{Z}$, faça $\overline{A} = \{\overline{a} \,|\, a \in A\}$. Considere $A_1 = \{0, x_1\}$ e vamos fixar uma indexação que inicia em $i_1 = 1$. Temos $|\overline{A_1}| = 2$. Agora, se possível, escolhemos um índice $i_2 \neq i_1$ tal que $\overline{A_1} + \{0, \overline{x_{i_2}}\} \neq \overline{A_1}$. Se tal i_2 existe, então seja $A_2 = A_1 + \{0, x_{i_2}\}$. Continuamos esse procedimento e supomos que ele termine em A_t. Note que

$$A_1 \subseteq A_2 \subseteq \cdots \subseteq A_t.$$

Além disso, temos

$$|\overline{A_t}| \geqslant |\overline{A_{t-1}}| + 1 \geqslant \cdots \geqslant t+1. \tag{2.3}$$

Observe que, por construção, os elementos de A_t são da forma

$$\sum_{j=1}^{t} \epsilon_j x_{i_j},\ \epsilon_j \in \{0,1\}. \tag{2.4}$$

Assim, como $\overline{A_t} \subseteq [1,k]$, basta mostrarmos que $|\overline{A_t}| \geqslant k$ para completar a prova. Por (2.3), temos $t \leqslant k-2$. Assim, podemos reindexar a sequência S, assumindo que $i_j = j \in [1,t]$ e que $k \nmid x_{t+1}$. Agora, como assumimos que o procedimento de obtenção dos A_i's termina em $i = t$, para todo $t+1 \leqslant j \leqslant n$, temos

$$\overline{A_t} + \{0, \overline{x_j}\} = \overline{A_t}. \tag{2.5}$$

Seja $H = \langle \overline{x_{t+1}} \rangle$. Por 2.5, temos $\overline{A_t} + H = \overline{A_t}$. De fato, como $0 \in H$, temos $\overline{A_t} \subseteq \overline{A_t} + H$. Por outro lado, lembrando que os elementos de H são da forma $q\overline{x_{t+1}}$, dado $\alpha \in \overline{A_t} + H$, temos

$$\begin{aligned}
\alpha &= \sum_{j=1}^{t} \epsilon_j \overline{x_j} + q\overline{x_{t+1}} \\
&= \underbrace{\sum_{j=1}^{t} \epsilon_j \overline{x_j} + x_{t+1}}_{\in A_t \text{ por } (2.5)} + (q-1)\overline{x_{t+1}}.
\end{aligned}$$

Fazendo isso $q-1$ vezes, obtemos $\alpha \in \overline{A_t}$. Daí, $\overline{A_t}$ é a união de algumas classes laterais de H. Escreva

$$\overline{A_t} = \bigcup_{i=1}^{s} (b_i + H) \tag{2.6}$$

onde $b_i \in \overline{A_t}$ para todo $i \in [1,s]$ e $b_i - b_j \notin H$ para todo $i \neq j$. Então $|\overline{A_t}| = s|H|$. Seja $k_1 = \mathrm{mdc}(x_{t+1}, k)$. Como $k \nmid x_{t+1}$ temos $k_1 < k$ e, lembrando que a sequência $x_1 \cdots x_n$ é completa com respeito a k_1, pela hipótese de indução, vemos que para todo inteiro b, existem $\epsilon_1, \ldots, \epsilon_n \in \{0,1\}$ tais que

$$\sum_{j=1}^{n} \epsilon_j x_j \equiv b \pmod{k_1}. \tag{2.7}$$

Por (2.4) e (2.5), temos

$$\left\{ \sum_{j=1}^{n} \epsilon_j x_j \pmod{k} \,|\, \epsilon_j \in \{0,1\} \right\} = \overline{A_t}.$$

Assim, como $k_1 = (k, x_{t+1})$ e por (2.6), podemos reescrever a igualdade acima módulo k_1 da seguinte forma:

$$\left\{ \sum_{j=1}^{n} \epsilon_j x_j \pmod{k_1} \,|\, \epsilon_j \in \{0,1\} \right\} = \{b_1 \pmod{k_1}, \ldots, b_s \pmod{k_1}\}.$$

Portanto, por (2.7) temos $s \geqslant k_1$. Notando que $|H|x_{t+1} \equiv 0 \pmod{k}$, segue que $|H| \equiv 0 \pmod{k/k_1}$. Como $|H| \geqslant 1$, temos $|H| \geqslant k/k_1$. Portanto, $|\overline{A_t}| = s|H| \geqslant k$. Isso completa a prova. ∎

Corolário 2.15. *Se m é ímpar e $x_1 \cdots x_n$ é uma sequência completa com respeito a m, então para qualquer inteiro b, existem $\delta_1, \ldots, \delta_n \in \{-1,1\}$ tais que*

$$\sum_{j=1}^{n} \delta_j x_j \equiv b \pmod{m}.$$

Demonstração: Dado $b \in \mathbb{Z}$, pelo teorema anterior existem $\epsilon_1, \ldots, \epsilon_n \in \{0,1\}$ tais que

$$\sum_{j=1}^{n} \epsilon_j x_j \equiv \frac{b}{2} + \frac{x_1 + \cdots + x_n}{2} \pmod{m}$$

e isso é equivalente a

$$b \equiv 2\sum_{j=1}^{n} \epsilon_j x_j - (x_1 + \cdots + x_n) = \sum_{j=1}^{n} (2\epsilon_j - 1)x_j \pmod{m}$$

pois 2 possui inverso multiplicativo módulo m, já que m é ímpar. Considere $\delta_j = 2\epsilon_j - 1 \in \{-1,1\}$ e obtemos o resultado. ∎

Teorema 2.16. *Se n é ímpar e $A = \{a, n-a\} \subseteq [1, n-1]$, $(a,n) = 1$, então*

$$E_A(C_n) \leqslant n + \lfloor \log_2 n \rfloor.$$

Demonstração: Seja $S = x_1 \cdots x_N \in \mathcal{F}(C_n)$ com $N = n + \lfloor \log_2 n \rfloor$. Se S é completa com respeito a n, então pelo Lema 2.13, existem $n-1$ índices $j_1, \ldots, j_{n-1} \in [1, N]$ tais que $x_{j_1} \cdots x_{j_{n-1}}$ é completa com respeito a n. Escolha arbitrariamente $j_n \in [1.N] \backslash \{j_1, \ldots, j_{n-1}\}$. Então é claro que $x_{j_1} \cdots x_{j_n}$ também é completa com respeito a n e o resultado segue do Corolário 2.15. Agora suponha que S não seja completa com respeito a n. Então existe d divisor de n tal que

$$|\{j \in [1,N] \,|\, x_j \not\equiv 0 \pmod{d}\}| < d - 1.$$

Seja D o maior divisor de n com essa propriedade. Note que se $f|n$ é tal que $D|f$, então

$$|\{j \in [1,N] \,|\, x_j \equiv 0 \pmod{D}, x_j \not\equiv 0 \pmod{f}\}| \geqslant \frac{f}{D} - 1. \tag{2.8}$$

De fato, se $f = D$, isso é imediato. Se $f > D$ e (2.8) não se verifica, então

$$\begin{aligned} |\{j \in [1,N] \,|\, x_j \not\equiv 0 \pmod{f}\}| &= |\{j \in [1,N] \,|\, x_j \not\equiv 0 \pmod{D}\}| \\ &+ |\{j \in [1,N] \,|\, x_j \equiv 0 \pmod{D}, x_j \not\equiv 0 \pmod{f}\}| \\ &< D + \tfrac{f}{D} - 2 \leqslant f - 1. \end{aligned} \tag{2.9}$$

Isso contradiz a maximalidade de D. Denote

$$I_1 = \{j \in [1,N] \,|\, x_j \not\equiv 0 \pmod{D}\}$$

$$I_2 = \{j \in [1,N] \,|\, x_j \equiv 0 \pmod{D}\}$$

e tome I_3 o maior subconjunto de I_1 tal que para alguma escolha de coeficientes $\epsilon'_j \in \{-1,1\}$ temos $\sum_{j\in I_3} \epsilon'_j x_j \equiv 0 \pmod{D}$. Pelo Lema 2.1, sabemos que

$$|I_1| - |I_3| \leqslant \lfloor \log_2 D \rfloor \tag{2.10}$$

pois caso contrário, $I_1 \setminus I_3$ possui uma subsequência de $\{-1,1\}$-soma zero e isso contraria a maximalidade de I_3. Temos que $|I_3| \leqslant |I_1| < D - 1 < n - 1$. Seja $k = n - |I_3|$. Por (2.10), temos

$$k = n - |I_3| = N - \lfloor \log_2 n \rfloor - |I_3| \leqslant N - |I_3| - \lfloor \log_2 D \rfloor \leqslant N - |I_1| = |I_2|.$$

Por outro lado, $k = n - |I_3| \geqslant n - |I_1| > n - D + 1 \geqslant n/D$. Portanto,

$$|I_2| \geqslant k \geqslant n/D. \tag{2.11}$$

Agora, fazendo

$$\overline{S} = \prod_{j\in I_2} x_j/D = \prod_{j\in I_2} y_j,$$

por (2.8), $\overline{S}$ é completa com respeito a n/D. O Lema 2.13 implica que existe $I' = \{j_1, \ldots, j_{n/D-1}\} \subseteq I_2$ tal que $y_{j_1} \cdots y_{j_{n/D-1}}$ é completa com respeito a n/D. Por (2.11), podemos escolher um conjunto I'_1 tal que $I' \subseteq I'_1 \subseteq I_2$ e $|I'_1| = k$. Claramente, $\prod_{j\in I'_1} y_j$ também é completa com respeito a n/D. Portanto, o Corolário 2.15 implica que podemos escolher $\epsilon''_j \in \{-1,1\}$, $j \in I'_1$ tais que

$$\sum_{j\in I'_1} \epsilon''_j y_j \equiv -\frac{1}{D} \sum_{j\in I_3} \epsilon'_j x_j \pmod{n/D}. \tag{2.12}$$

Para completar a prova, é suficiente tomar $I_0 = I_3 \cup I_1'$ e escolher

$$\epsilon_j = \begin{cases} \epsilon_j'' \text{ se } j \in I_1' \\ \epsilon_j' \text{ se } j \in I_3 \end{cases}.$$

Isso nos dá

$$|I_0| = |I_3| + |I_1'| = |I_3| + k = |I_3| + n - |I_3| = n.$$

e

$$I_0 = I_3 \cup I_1' \Rightarrow \sum_{j \in I_0} \epsilon_j x_j = \sum_{j \in I_3} \epsilon_j' x_j + \sum_{j \in I_1'} \epsilon_j'' x_j \equiv 0 \pmod{n}$$

pois, de (2.12), existe $p \in \mathbb{N}$ tal que

$$\sum_{j \in I_1'} \epsilon_j'' y_j + \frac{1}{D} \sum_{j \in I_3} \epsilon_j' x_j = p\left(\frac{n}{D}\right) \Rightarrow \sum_{j \in I_1'} \epsilon_j'' x_j + \sum_{j \in I_3} \epsilon_j' x_j = pn$$

■

Podemos resumir a Proposição 2.10 e o teorema anterior no resultado abaixo.

Teorema 2.17. *Se* $A = \{a, n-a\} \subseteq [1, n-1]$, $(a, n) = 1$, *então*

$$E_A(C_n) = n + \lfloor \log_2 n \rfloor.$$

Demonstração: Por (2.1) e pelo Teorema 2.5,

$$E_A(C_n) \geqslant n - 1 + \lfloor \log_2 n \rfloor + 1 = n + \lfloor \log_2 n \rfloor.$$

A desigualdade contrária segue da Proposição 2.10 quando n é par e do Teorema 2.16 quando n é ímpar. ■

Teorema 2.18. *Se* $A = [1, n-1]$, *então* $E_A(C_n) = n + 1$.

Demonstração: Sem perda de generalidade, vamos considerar

$$C_n = \mathbb{Z}_n = \{0, 1, \dots, n-1\}.$$

Se $n = 1$, então $C_n = \{0\}$ e nada temos a fazer. Se $n = 2$, então $A = \{1\}$ e o resultado segue do Teorema 2.9. Assuma $n > 2$. Seja $S = x_1 \cdots x_{n+1} \in \mathcal{F}(C_n)$ ordenada de forma que, para algum $r \geqslant 0$, $(x_j, n) = 1$ para $j \leqslant r$ e $(x_j, n) > 1$ para $j > r$. Temos as seguintes observações.

(i) Para $j \in [1, r]$, existem coeficientes $\alpha_j \in A$ tais que

$$\sum_{j=1}^{r} \alpha_j x_j \equiv 0 \pmod{n}.$$

De fato, da aritmética elementar, se $(x_j, n) = 1$, então existe $a_j \in \mathbb{Z}_n$ tal que $a_j x_j \equiv 1 \pmod{n}$. Assim, se r é par, tome $\alpha_j = (-1)^j a_j$ e temos $\sum_{j=1}^{r} \alpha_j x_j \equiv 0 \pmod{n}$. Se r é ímpar, tome

$$\alpha_j = \begin{cases} (-1)^j a_j & \text{se } \ j \neq 2 \\ 2a_j & \text{se } \ j = 2 \end{cases}$$

e temos

$$\sum_{j=1}^{r} \alpha_j x_j = 2a_2x_2 + \sum_{j=1, j\neq 2}^{r} \alpha_j x_j \equiv 2 - 2 \equiv 0 \pmod{n}.$$

(ii) Para $j > r$, existe $\beta_j \in A$ tal que $\beta_j x_j \equiv 0 \pmod{n}$. De fato, se $(x_j, n) = d > 1$, então $n = dm$ com $1 < m < n$ e pelo Teorema de Bachet-Bezóut, existem $a, b \in \mathbb{Z}$ tais que

$$ax_j + bn = d \Rightarrow amx_j + bmn = dm = n \Rightarrow \overline{am}x_j \equiv 0 \pmod{n}.$$

Assim, basta tomar $\beta_j = \overline{am}$.

Agora, considere a subsequência $T = x_1 \cdots x_n$ e temos:
Se $r = 0$, tome $\epsilon_j = \beta_j$, $j \in [1, n]$ e

$$\sum_{j=1}^{n} \epsilon_j x_j = \sum_{j=1}^{n} \beta_j x_j \equiv 0 \pmod{n}.$$

Se $r = n$, tome $\epsilon_j = \alpha_j$, $j \in [1, n]$ e

$$\sum_{j=1}^{n} \epsilon_j x_j = \sum_{j=1}^{n} \alpha_j x_j \equiv 0 \pmod{n}.$$

Se $0 < r < n$, tome $\epsilon_j = \alpha_j$ para $j \in [1, r]$ e $\epsilon_j = \beta_j$ para $j \in [r+1, n]$ e

$$\sum_{j=1}^{n} \epsilon_j x_j = \sum_{j=1}^{r} \alpha_j x_j + \sum_{j=r+1}^{n} \beta_j x_j \equiv 0 \pmod{n}.$$

Em qualquer caso, provamos que T é subsequência de A-soma zero de S. Isso mostra que $E_A(C_n) \leqslant n + 1$.

Por outro lado, a sequência

$$S = 0^{n-1}1$$

tem tamanho n e não é sequência de A-soma zero. Concluímos, portanto, que $E_A(C_n) \geqslant n + 1$ e a igualdade segue. ∎

Proposição 2.19. *Se $A = [1, r]$ onde $1 < r < p$, então $E_A(C_p) = \lceil \frac{p}{r} \rceil + p - 1$.*

Demonstração: Por (2.1) e pela Proposição 2.8, basta que mostremos a desigualdade $E_A(C_p) \leqslant D_A(C_p) + p - 1 = \left\lceil \frac{p}{r} \right\rceil + p - 1$.

Seja $N = \left\lceil \frac{p}{r} \right\rceil + p - 1$ e considere a sequência $S = s_1 \cdots s_N$ de elementos de C_p. Temos dois casos:

Caso 1. S possui pelo menos p elementos não nulos.

Considere $T = s_{i_1} \cdots s_{i_p}$ uma subsequência de S com $s_{i_j} \neq 0$ para $j \in [1, r]$ e $A_j = \{s_{i_j}, 2s_{i_j}\}$. Como $|A_j| = 2 \forall j$, pelo Teorema 1.24

$$|A_i + \cdots + A_p| \geqslant p.$$

Agora, como $A_1 + \cdots + A_p \subseteq C_p$, segue que $A_1 + \cdots + A_p = C_p$. Daí, $0 \in A_1 + \cdots + A_p$, ou seja, $0 = a_1 s_{i_1} + \cdots + a_p s_{i_p}$ com $a_i \in \{1, 2\} \subseteq A$ e portanto $s_{i_1} \cdots s_{i_p}$ é subsequência de S de A-soma zero.

Caso 2. S possui menos de p elementos não nulos. Neste caso, como $|S| = p - 1 + \lceil \frac{p}{r} \rceil$, há, no mínimo, $\lceil \frac{p}{r} \rceil$ elementos nulos em S. Vamos reordenar S de tal forma que $s_1 = s_2 = \cdots = s_t = 0$ e $s_i \neq 0$ sempre que $i \geqslant t + 1$.

Tome $B = \{r_1, \ldots, r_l\} \subseteq [t + 1, N]$ de tal forma que B seja o maior com a propriedade de que existem $a_1, \ldots, a_l \in [1, r]$ com

$$\sum_{j=1}^{l} a_j s_{r_j} = 0.$$

Temos $l + t \geqslant p$. De fato, se $l + t < p$, então $N - (l + t) > N - p = \lceil p/r \rceil - 1$ e Pela Proposição 2.8 existe $C \subseteq [t + 1, N] \setminus \{r_1, \ldots, r_l\}$ tal que $\sum_{i \in C} a_i s_i = 0$ com $a_i \in [1, r]$ e $B \cup C$ contradiz a maximalidade de B. Assim, anexando a sequência determinada pelos índices de B a $s_1 \cdots s_t$, encontramos a subsequência de A-soma zero procurada.

Em qualquer caso, mostramos que $E_A(C_p) \leqslant \lceil \frac{p}{r} \rceil + p - 1$. ■

Para o próximo resultado, precisaremos da seguinte

Definição 2.20. *Seja $p > 2$ um número primo e $a \in \mathbb{Z}_p^*$. Dizemos que a é um resíduo quadrático módulo p se existe $b \in \mathbb{Z}_p^*$ tal que*

$$a \equiv b^2 \pmod{p}. \tag{2.13}$$

O conjunto $A = \{x^2 \,|\, x \in \mathbb{Z}_p^*\}$ dos resíduos quadráticos módulo p é um subgrupo do grupo multiplicativo $\mathbb{Z}_p^*$.

Proposição 2.21. *Se A é o conjunto dos resíduos quadráticos módulo p temos $E_A(C_p) = p + 2$ e $D_A(C_p) = 3$.*

Demonstração: Seja a sequência $S = s_1 \cdots s_{p+2}$ com elementos de C_p de tamanho $p + 2$. Considere o seguinte sistema de equações em $p + 2$ variáveis:

$$\begin{cases} f_1(x_1, \ldots, x_{p+2}) = \displaystyle\sum_{j=1}^{p+2} s_i x_i^2 = 0 \\ f_2(x_1, \ldots, x_{p+2}) = \displaystyle\sum_{j=1}^{p+2} x_i^{p-1} = 0 \end{cases}.$$

Observe que $p + 1 < p + 2$ e pelo Teorema 1.20, há uma solução não nula para o sistema. Da segunda equação, se $(y_1, \ldots, y_{p+2})$ é solução do sistema, devem haver p elementos $y_i's$ não nulos. Aplicando isso na primeira equação, temos que $\sum_{j=1}^{p} a_j s_j = 0$ onde $a_j = y_j^2 \in A$. Isso nos permite concluir que $E_A(C_p) \leqslant p + 2$. Além disso, pela Desigualdade 2.1, $E_A(C_p) \geqslant D_A(C_p) + p - 1$, ou seja, $D_A(C_p) \leqslant 3$.

Por outro lado, se consideramos a sequência $s_1(-s_2)$ onde s_1 é um quadrado em C_p e s_2 não é, devemos ter $a_1s_1+a_2(-s_2) \neq 0\ \forall a_1, a_2 \in A$. De fato, se existem $a_1, a_2 \in A$ tais que $a_1s_1 = a_2s_2$, então $(a_2)^{-1}a_1s_1 = s_2$ e isso é impossível pois o primeiro membro da última igualdade é um quadrado em C_p e o segundo membro, não. Logo, $D_A(C_p) \geqslant 3$. Daí, $D_A(C_p) = 3$ e, mais uma vez, pela Desigualdade 2.1,

$$E_A(C_p) \geqslant D_A(C_p) + n - 1 = 3 + p - 1 = p + 2$$

e a igualdade segue. ■

2.3 Conclusão

A ordem com que os resultados das seções anteriores foram apresentados não foi escolhida por acaso. A relação (2.2) se verifica quando comparamos cada um deles: no caso em que $A = \{1\}$, podemos associar o Teorema 2.9 com o Teorema 2.4. Quando $A = \{1, -1\}$, temos que $E_A(C_n) = n + \lfloor \log_2\ n \rfloor$ pelo Teorema 2.17 e $D_A(C_n) = \lfloor \log_2 n \rfloor + 1$ pelo Teorema 2.5. O caso em que $A = [1, n-1]$ temos $E_A(C_n) = n+1$ provado no Teorema 2.18 e $D_A(C_n) = 2$ graças ao Corolário 2.7. Quando $A = [1, r]$ com $1 < r < p$ e p primo, temos $E_A(C_p) = \lceil \frac{p}{r} \rceil + p - 1$ pela Proposição 2.19 e $D_A(C_n) = \lceil \frac{p}{r} \rceil$ pela Proposição 2.8. Por fim, na Proposição 2.21 vimos que $E_A(C_p) = p + 2$ e $D_A(C_p) = 3$. Em todos esses casos, (2.2) se verifica.

Como já mencionamos no início, a relação já foi provada para qualquer grupo abeliano finito e para qualquer conjunto-peso. Aqui, vamos apresentar a prova para o caso particular em que $G = C_p$, p primo.

Teorema 2.22. *Dado p um inteiro positivo primo, para todo $A \subseteq [1, p-1]$, tem-se*

$$E_A(C_p) = D_A(C_p) + p - 1.$$

Demonstração: Sejam $S = s_1 \cdots s_N$ sequência de elementos de C_p com $|S| = N = p - 1 + D_A(C_p)$ e $A = \{a_1, \ldots, a_r\} \subseteq [1, p-1]$, $r \geqslant 2$. Temos dois casos:

Caso 1. S tem, no mínimo, p elementos não nulos. Considere $T = s_{i_1} \cdots s_{i_p}$ uma subsequência de S com $s_{i_j} \neq 0$ para todo $j \in [1, p]$ e defina $A_k = \{a_1s_{i_k}, \ldots, a_rs_{i_k}\}$ para cada $k \in [1, p]$. Como $|A_k| \geqslant 2$ para todo k, pelo Corolário 1.24, segue que

$$|A_1 + \cdots + A_p| \geqslant \min\{p, |A_1| + \cdots + |A_p| - p + 1\} = p.$$

Agora, como $A_1+\cdots+A_p \subseteq C_p$, segue que $A_1+\cdots+A_p = C_p$. Daí $0 \in A_1+\cdots+A_p$, ou seja, $0 = a_1s_{i_1} + \cdots + a_ps_{i_p}$ com $a_i \in A$. Portanto, $s_{i_1} \cdots s_{i_p}$ é subsequência de S de tamanho p e de A-soma zero.

Caso 2. S possui menos de p elementos não nulos. Neste caso, como $|S| = p - 1 + D_A(C_p)$, no mínimo $D_A(C_p)$ elementos de S são nulos. Vamos reordenar S de tal forma que $s_1 = \cdots = s_t = 0$ e $s_i \neq 0$ sempre que $i \geqslant t+1$. Tome $B = \{r_1, \ldots, r_l\} \subseteq [t+1, N]$ de tal forma que B seja o maior com a propriedade de que existem $a_1, \ldots, a_l \in [1, r]$ com $\sum_{j=1}^{l} a_js_{i_j} = 0$. Temos $l + t \geqslant p$. De fato, se $l + t < p$, então

$$|S| - (l+t) = p - 1 + D_A(C_p) - (l+t) > D_A(C_p) - 1.$$

Daí, da definição de $D_A(C_p)$, existe $B' \subseteq [t+1, N] \setminus B$ tal que $\prod_{j \in B'} x_j$ é sequência de A-soma zero e $B \cup B'$ contraria a maximalidade de B.

Assim, anexando a sequência determinada pelos índices de B a $s_1 \cdots s_t$, encontramos a subsequência de A-soma zero desejada.

Isso mostra que $E_A(C_p) \leqslant D_A(C_p) + p - 1$. ■

Capítulo 3

A Constante de Davenport com Peso $A = \{-1, 1\}$

Existem diferentes maneiras de generalizar ou modificar problemas de soma zero através de diferentes escolhas de conjunto peso. Problemas particularmente populares são obtidos através da constante de Davenport com $A = \{-1, 1\}$ como conjunto-peso. Neste capítulo trataremos exclusivamente desse caso.

Começamos apresentando um resultado provado por S. D. Adhikari, D. J. Grynkiewicz e Z. W. Sun em [2] em 2012 que estabelece limites inferior e superior para $D_{\pm}(G)$ sob algumas condições. Em seguida, vamos estudar uma forma de melhorar esse resultado, com base num teorema de L. E. Marchan, O. Ordaz e W. A. Schmid, apresentado em [19]. O resultado final do capítulo é o teorema que afirma que $D_{\pm}(G) = 6$ para $G = C_3 \oplus C_3 \oplus C_9$ como exemplo de um caso em que $D_{\pm}(G)$ é menor que o limite superior estabelecido pelo Teorema de L. E. Marchan, O. Ordaz e W. A. Schmid. Nosso trabalho aqui se baseia no artigo [19].

Teorema 3.1 (Adhikari-Grynkiewicz-Sun). *Seja $G \simeq C_{n_1} \oplus \cdots \oplus C_{n_r}$ com $n_i | n_{i+1}$ para $i \in [1, r-1]$, onde C_{n_i} é o grupo cíclico de ordem n_i. Então*

$$\sum_{i=1}^{r} \lfloor \log_2(n_i) \rfloor + 1 \leqslant D_{\pm}(G) \leqslant \lfloor \log_2 |G| \rfloor + 1. \tag{3.1}$$

Além disso,

$$s_{\pm}(G) \geqslant n_r + D_{\pm}(G) - 1 \geqslant \exp(G) + \sum_{i=1}^{r} \lfloor \log_2 n_i \rfloor. \tag{3.2}$$

Demonstração: Seja $A = \{-1, 1\}$. Vamos mostrar (3.1). Para a primeira desigualdade, considere $e_1, \ldots, e_r$ base de G e para $i \in [1, r]$, defina:

$$S_i = (e_i)(2e_i) \cdots (2^{\lfloor \log_2(n_i) \rfloor - 1} e_i) \in \mathcal{F}(\langle e_i \rangle)$$

e então $S = \prod_{i=1}^{r} S_i \in \mathcal{F}(G)$. Note que $|S| = \sum_{i=1}^{r} \lfloor \log_2(n_i) \rfloor$. Para mostrar que S não possui subsequência não trivial de A-soma zero, é suficiente verificar que cada S_i não possui subsequência não trivial de A-soma zero, já que $e_1, \ldots, e_r$ forma uma base de G. Mas isso segue do fato de que, em cada S_i, a maior soma possível, considerando os pesos de A, resulta num número cujo valor absoluto está entre 1 e $n_i - 1$, ou seja, não é possível obter uma subsequência não trivial de A-soma zero. O cota superior segue do Corolário 2.3.

Agora, para mostrar (3.2), seja $S \in \mathcal{F}(G)$ com $|S| = D_{\pm}(G) - 1$ sem subsequência não trivial de A-soma zero. É claro então que a sequência $0^{n_r - 1}S$ não possui subsequência de A-soma zero de tamanho n_r e isso mostra a primeira desigualdade. A segunda desigualdade segue de (3.1), conforme abaixo:

$$\begin{aligned} D_{\pm}(G) \geqslant \sum_{i=1}^{r} \lfloor \log_2 n_i \rfloor + 1 \quad &\Rightarrow n_r + D_{\pm}(G) - 1 \geqslant n_r + \sum_{i=1}^{r} \lfloor \log_2 n_i \rfloor \\ &\Rightarrow n_r + D_{\pm}(G) - 1 \geqslant \exp(G) + \sum_{i=1}^{r} \lfloor \log_2 n_i \rfloor. \end{aligned}$$

■

Em casos particulares onde G é cíclico ou G é um 2-grupo, por exemplo, o Teorema 3.1 nos dá o valor exato de $D_{\pm}(G)$ já que os limites superiores e inferiores coincidem. Nosso trabalho agora é entender como esses limites podem ser melhorados, de forma a nos aproximarmos mais do valor exato de $D_{\pm}(G)$.

Foram L. E. Marchan, O. Ordaz e W. A. Schmid que, em [19], estudaram a constante $D_{\pm}(G)$, fazendo uma pequena mudança nas hipóteses do Teorema 3.1, de forma a tornar mais próximos os limitantes de $D_{\pm}(G)$ em (3.1), como apresentaremos a seguir.

Lema 3.2. *Seja G um grupo abeliano finito com $\exp(G) = n$. Seja $A \subsetneq [1, n-1]$ um subconjunto não vazio e d um divisor de n. Então $D_{dA}(G) = D_A(dG)$.*

Demonstração: Considere a função $\mathrm{m}_d : G \longrightarrow G$ definida por $\mathrm{m}_d(g) = dg$. m_d é um homomorfismo de grupos cuja imagem é dG, conforme o Exemplo 1.5.

Seja $S \in \mathcal{F}(dG)$ com $|S| = D_{dA}(G)$. Vamos mostrar que S possui uma subsequência não trivial de A-soma zero em dG. Considere $S' \in \mathcal{F}(G)$ tal que $\mathrm{m}_d(S') = S$. Como $|S'| = D_{dA}(G)$, existe uma subsequência $g_1' \cdots g_t' | S'$ e coeficientes $a_1', \ldots, a_t' \in dA$ tais que $\sum_{i=1}^{t} a_i' g_i' = 0$. Agora, $a_i' \in dA$ nos diz que $a_i' = da_i$ com $a_i \in A$. Assim,

$$0 = \sum_{i=1}^{t} a_i' g_i' = \sum_{i=1}^{t} da_i g_i' = \sum_{i=1}^{t} a_i \mathrm{m}_d(g_i').$$

Como $\mathrm{m}_d(g_1') \cdots \mathrm{m}_d(g_t')$ é uma subsequência de S, concluímos que $D_{dA}(G) \geqslant D_A(dG)$.

Por outro lado, considere $S' \in \mathcal{F}(G)$ com $|S'| = D_A(dG)$ e note que $\mathrm{m}_d(S') = S$ é uma sequência de elementos de dG de tamanho $D_A(dG)$ e logo existe $g_1 \cdots g_k | S$ e coeficientes $a_1, \ldots, a_k \in A$ tais que $\sum_{i=1}^{k} a_i g_i = 0$. Como cada $g_i \in dG$ temos $g_i = dg_i'$ com $g_i' \in G$ e logo

$$0 = \sum_{i=1}^{k} a_i g_i = \sum_{i=1}^{k} a_i d g_i' = \sum_{i=1}^{k} a_i' g_i'.$$

Assim, $g_i' \cdots g_k'$ é a subsequência de S procurada e, com isso, concluímos que $D_{dA}(G) \leqslant D_A(dG)$ e a igualdade segue. ■

Corolário 3.3. *Seja G um grupo abeliano finito com* $\exp(G) = n$. *Seja* $A \subseteq [1, n-1]$ *e b coprimo com n. Então* $D_{bA}(G) = D_A(G)$.

Demonstração: Basta lembrar que como $(b, n) = 1$, a função $\mathrm{m}_b : G \longrightarrow G$ definida por $\mathrm{m}_b(g) = bg$ é um automorfismo de G. O restante da demonstração segue idêntico ao lema anterior. ■

Proposição 3.4. *Sejam G um grupo abeliano finito com* $\exp(G) = n$, $A \subseteq [1, n-1]$, $b \in \mathbb{Z}$ *e* $d = (b, \exp(G))$. *Então*

$$D_{bA}(G) = D_A(dG).$$

Demonstração: Como $d | \exp(G)$, pelo Lema 3.2

$$D_{bA}(G) = D_{db'A}(G) = D_{b'A}(dG),$$

fazendo $b = db'$. Agora, como b' é coprimo com $\exp(dG)$, temos $D_{b'A}(dG) = D_A(dG)$ pelo Corolário 3.3, como queríamos. ■

Lema 3.5. *Sejam G um grupo abeliano finito, $H \leq G$ e* $A \subseteq [1, \exp(G) - 1]$ *um subconjunto não vazio. Então*

$$D_A(G) \geqslant D_A(G/H) + D_A(H) - 1.$$

Demonstração: Seja $S \in \mathcal{F}(H)$ com $|S| = D_A(H) - 1$, que não possui subsequência não trivial de A-soma zero e seja $T \in \mathcal{F}(G)$ uma sequência de comprimento $D_A(G/H) - 1$ tal que $\phi_H(T)$ não possui subsequência não trivial de A-soma zero em G/H, onde ϕ_H é a projeção canônica de G sobre H. Afirmamos que $ST \in \mathcal{F}(G)$ não possui subsequência não trivial de A-soma zero. De fato, se existe $S'|ST$ tal que $0 \in \sigma_A(S')$, escreva $S' = PQ$ com $P = g_1 \cdots g_{|P|}|S$, $Q = g_{|P|+1} \cdots g_{|S'|}|T$ e existe uma escolha de pesos $a_1, a_2, \ldots, a_{|S'|} \in A$ que nos dá

$$\sum_{i=1}^{|P|} a_i g_i = -\sum_{i=|P|+1}^{|S'|} a_i g_i \Rightarrow \sum_{i=|P|+1}^{|S'|} a_i g_i \in H \Rightarrow \sum_{i=|P|+1}^{|S'|} a_i \phi_H(g_i) = 0 \in G/H$$

e logo $\phi_H(Q)|\phi_H(T)$ é subsequência de A-soma zero em G/H, um absurdo. Com isso, concluímos que $D_A(G) > D_A(G/H) + D_A(H) - 2$. ■

Definição 3.6. *Sejam G, H, K grupos abelianos finitos. Dizemos que G é extensão de H por K quando G tem um subgrupo H' isomorfo a K tal que H é isomorfo a G/H'.*

Lema 3.7. *Sejam H_1, H_2 grupos abelianos finitos tais que* $D_\pm(H_i) = \lfloor \log_2 |H_i| \rfloor + 1$ *com* $i \in \{1, 2\}$ *e* $\{\log_2 |H_1|\} + \{\log_2 |H_2|\} < 1$. *Então, para todo grupo G abeliano finito que é uma extensão de H_1 por H_2, temos* $D_\pm(G) = \lfloor \log_2 |G| \rfloor + 1$.

Demonstração: Seja G extensão de H_1 por H_2. Pelo lema anterior, temos

$$\begin{aligned} D_\pm(G) \geqslant D_\pm(H_1) + D_\pm(H_2) - 1 &= \lfloor \log_2 |H_1| \rfloor + \lfloor \log_2 |H_2| \rfloor + 1 \\ &= \lfloor \log_2 (|H_1||H_2|) \rfloor = \lfloor \log_2 |G| \rfloor. \end{aligned}$$

Podemos fazer isso pois $\lfloor a+b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor$ quando $\{a\}+\{b\} < 1$ e $|H_1||H_2| = |H_1||G/H_1| = |G|$ pelo Teorema de Lagrange. O limite superior segue do Corolário 2.3. ■

Agora estamos prontos para apresentar a prova do Teorema de Marchan-Ordaz-Schmid.

Teorema 3.8 (Marchan-Ordaz-Schmid)**.** *Sejam G um grupo abeliano finito e $m_1, \ldots, m_t$ inteiros positivos tais que $G \simeq C_{m_i} \oplus \cdots \oplus C_{m_t}$. Então*

$$\sum_{i=1}^{t} \lfloor \log_2 m_i \rfloor + 1 \leqslant D_{\pm}(G) \leqslant \left\lfloor \sum_{i=1}^{t} \log_2 m_i \right\rfloor + 1.$$

Demonstração: A segunda desigualdade segue do Corolário 2.3, lembrando que $G = \bigoplus H_i \Rightarrow |G| = \prod |H_i|$.

Para mostrar a primeira desigualdade, vamos usar indução sobre t. Se $t = 1$, nada temos a fazer. Se $t = 2$, $G = C_{m_1} \oplus C_{m_2}$ e $G/C_{m_2} \simeq C_{m_1}$ pelo Teorema 1.6 considerando o homomorfismo $\varphi : G \longrightarrow G$ dado por $\varphi(a, b) = (0, b)$. Assim, pelo Lema 3.5 e pelo Teorema 2.5,

$$D_{\pm}(G) \geqslant D_{\pm}(C_{m_1}) + D_{\pm}(C_{m_2}) = \lfloor \log_2 m_1 \rfloor + \lfloor \log_2 m_2 \rfloor + 2 - 1.$$

Suponha agora que a cota inferior seja válido para $t = k \in \mathbb{N}_{\geqslant 2}$, ou seja,

$$\sum_{i=1}^{k} \lfloor \log_2 m_i \rfloor + 1 \leqslant D_{\pm}(G).$$

Para $t = k + 1$, escreva

$$G \simeq \bigoplus_{i=1}^{k+1} C_{m_i} \simeq \bigoplus_{i=1}^{k} C_{m_i} \oplus C_{m_{k+1}},$$

considere $H_1 = \bigoplus_{i=1}^{k} C_{m_i}$ e note que $G/H_1 = C_{m_{k+1}}$ pelo Teorema 1.6. Aplicando o Lema 3.5 a G e H_1 e lembrando que $D_{\pm}(C_{k+1}) = \lfloor \log_2 m_{k+1} \rfloor + 1$ pelo Teorema 2.5, obtemos

$$\begin{aligned} D_{\pm}(G) &\geqslant D_{\pm}\left(\bigoplus_{i=1}^{k} C_{m_i}\right) + D_{\pm}(C_{m_{k+1}}) - 1 \\ &\geqslant \sum_{i=1}^{k} \lfloor \log_2 m_i \rfloor + 1 + (\lfloor \log_2 m_{k+1} \rfloor + 1) - 1 \\ &= \sum_{i=1}^{k+1} \lfloor \log_2 m_i \rfloor + 1. \end{aligned}$$

Isso conclui a demonstração. ■

Para entender a vantagem desse teorema sobre o Teorema 3.1, vamos investigar como a constante de Davenport com peso $A = \{-1, 1\}$ se comporta diante de diferentes decomposições de alguns grupos nos exemplos abaixo.

Exemplo 3.9.

(i) Temos $C_3 \oplus C_{3\cdot 11\cdot 23} \simeq C_{3\cdot 11} \oplus C_{3\cdot 23}$. Aplicando o Teorema anterior, a primeira decomposição nos fornece $(1+9)+1 = 11$ como limite inferior enquanto com a segunda obtemos $(5+6)+1 = 12$.

(ii) Temos $C_{3\cdot 13\cdot 23}^2 \simeq C_{3\cdot 13} \oplus C_{3\cdot 23} \oplus C_{13\cdot 23}$. As decomposições nos fornecem $(9+9)+1 = 19$ e $(5+6+8)+1 = 20$ como cota interior, respectivamente.

Como o exemplo nos indica, o segredo para obter um maior limite inferior está em escolher uma decomposição conveniente com o qual a perda ao tomar a parte inteira seja minimizada. Para nos ajudar com esta escolha, fazemos a seguinte definição.

Definição 3.10. *Seja G um grupo abeliano finito. Então*

$$D_{\pm}^*(G) = \max\left\{\sum_{i=1}^{t} \lfloor \log_2 m_i \rfloor + 1 \mid G \simeq \bigoplus_{i=1}^{t} C_{m_i},\ m_i, t \in \mathbb{N}\right\}.$$

Essa definição nos permite formular o corolário abaixo:

Corolário 3.11. *Seja G um grupo abeliano finito. Então:*

$$D_{\pm}^*(G) \leqslant D_{\pm}(G) \leqslant D_{\pm}^*(G) + r(G) - 1.$$

Demonstração: A primeira desigualdade segue da definição de $D_{\pm}^*(G)$ e do Teorema 3.8. A segunda segue do Teorema Fundamental dos Grupos Abelianos e do Lema 1.1. ■

Observe que encontrar $D_{\pm}^*(G)$ é o que precisamos para obter o maior limite inferior e assim tornar efetiva a vantagem do teorema anterior sobre o de Adhikari, Grynkiewicz e Sun. Porém, no geral, essa não é uma tarefa simples e pode ser muito trabalhosa do ponto de vista algorítmico (veja [19], Definição 3.3 para detalhes). Mas isso não torna a generalização menos importante. De fato, já podemos melhorar os limites inferiores de $D_{\pm}(G)$ para certos grupos G e, em alguns desses casos, obter até o valor exato, a saber, quando $D_{\pm}^*(G)$ corresponde ao limite superior $\lfloor \log_2 |G| \rfloor + 1$.

Segue abaixo dois exemplos em forma de teorema que seguem diretamente do Teorema 3.8 e nos fornecem o valor exato de $D_{\pm}(G)$.

Teorema 3.12. *Sejam $n, m_1, m_2 \in \mathbb{N}$ coprimos dois a dois, com $\{\log_2 m_i\} + \{\log_2 n\} \geqslant 1$ para cada $i = 1, 2$ e $\{\log_2 m_1\} + \{\log_2 m_2\} + 2\{\log_2 n\} < 3$. Então*

$$D_{\pm}^*(C_n \oplus C_{nm_1m_2}) = D_{\pm}(C_n \oplus C_{nm_1m_2}) = \lfloor \log_2(n^2 m_1 m_2) \rfloor + 1.$$

Demonstração: Note que $C_n \oplus C_{nm_1m_2} \simeq C_{nm_1} \oplus C_{nm_2}$, e $\lfloor \log_2(nm_1) \rfloor + \lfloor \log_2(nm_2) \rfloor = \lfloor \log_2(n^2 m_1 m_2) \rfloor$ pelas condições sobre as partes não inteiras. A afirmação segue do Teorema 3.8. ■

Teorema 3.13. *Sejam $n_1, n_2, n_3 \in \mathbb{N}$ coprimos dois a dois, com $\{\log_2 n_i\} + \{\log_2 n_j\} \geqslant 1$ para cada $i \neq j$ e $\{\log_2 n_1\} + \{\log_2 n_2\} + 2\{\log_2 n_3\} < 3$. Então,*

$$D_{\pm}^*(C_{n_1n_2n_3}^2) = D_{\pm}(C_{n_1n_2n_3}^2) = \lfloor 2\log_2(n_1 n_2 n_3) \rfloor + 1.$$

Demonstração: Note que $C^2_{n_1n_2n_3} \simeq C_{n_1n_2} \oplus C_{n_1n_3} \oplus C_{n_2n_3}$ e $\lfloor \log_2(n_1n_2) \rfloor + \lfloor \log_2(n_1n_3) \rfloor + \lfloor \log_2(n_2n_3) \rfloor = \lfloor 2\log_2(n_1n_2n_3) \rfloor$ pelas condições sobre as partes não inteiras e o resultado segue do Teorema 3.8. ∎

A proposição abaixo é exemplo de um caso onde não se tem necessariamente $D^*_\pm(G) = D_\pm(G)$ mas que conseguimos obter uma cota inferior para $D_\pm(G)$ mediante uma construção diferente de uma sequência sem subsequência não trivial de A-soma zero.

Proposição 3.14. *Sejam m_1, m_2 inteiros com $m_1 \geqslant 4$ e $m_2 \geqslant 3$. Então*

$$D_\pm(C_{m_1} \oplus C_{m_2}) \geqslant \lfloor \log_2(m_1/3) \rfloor + \lfloor \log_2(m_2/3) \rfloor + 4.$$

Demonstração: Seja $A = \{-1, 1\}$. Vamos construir uma sequência de elementos de $G = C_{m_1} \oplus C_{m_2}$ de tamanho $\lfloor \log_2(m_1/3) \rfloor + \lfloor \log_2(m_2/3) \rfloor + 3$ sem subsequência não trivial de A-soma zero. Sejam e_1 e e_2 os geradores de C_{m_1} e C_{m_2} respectivamente. Considere $k = \lfloor \log_2(m_1/3) \rfloor$, $l = \lfloor \log_2(m_2/3) \rfloor$ e $d = m - 2^k$ onde m é o inteiro mais próximo de $m_1/6$ (no caso em que a parte não inteira de $m_1/6$ for $1/2$, m o inteiro maior). Considere as seguintes sequências

$T_1 = \prod_{i=0}^{k-1}(2^i e_1)$,

$T_2 = \prod_{j=0}^{l-1}(2^j 3e_2)$ e

$T_3 = (de_1 + e_2)((d + 2^k)e_1 + e_2)((d + 2^{k+1})e_1 + e_2)$.

Vamos mostrar que $T_1T_2T_3$ cujo tamanho é $k + l + 3 = \lfloor \log_2(m_1/3) \rfloor + \lfloor \log_2(m_2/3) \rfloor + 3$ não possui subsequência não trivial de A-soma zero. É fácil ver que T_1 não possui subsequência não trivial de A-soma zero (essa é a mesma sequência que usamos na demonstração do Teorema 2.5). Com um argumento parecido, o mesmo podemos dizer para T_2. De fato, se há uma subsequência $x_1 \cdots x_r$ de A-soma zero em T_2, $1 \leqslant r \leqslant l - 1$, digamos, $x_i = 2^{j_i} 3e_2$, então existem $\alpha_i \in \{-1, 1\}$, $i \in [1, r]$ tais que

$$\sum_{i=1}^{r} \alpha_i x_i = 0 \Rightarrow 3\sum_{i=1}^{r} \alpha_i 2^{j_i} e_2 = 0 \Rightarrow \sum_{i=1}^{r} \alpha_i 2^{j} e_2 = 0$$

com $j \in [0, l - 1]$ e essa última igualdade é impossível como em T_1. A última implicação segue do fato de

$$\begin{aligned} \left| \sum_{i=1}^{r} \alpha_i 2^{j_i} \right| &\leqslant \sum_{i=1}^{l-1} 2^j = 2^l - 1 = 2^{\lfloor \log_2(m_2/3) \rfloor} - 1 \\ &\leqslant m_2/3 - 1 < \operatorname{ord}(e_2)/3. \end{aligned}$$

De forma mais precisa, podemos escrever

$\Sigma_\pm(T_1) = A_1 = \{-(2^k - 1)e_1, \ldots, -e_1, e_1, \ldots, (2^k - 1)e_1\}$ e

$\Sigma_\pm(T_2) = A_2 = \{-3(2^l - 1)e_2, \ldots, -3e_2, 3e_2, 6e_2, \ldots, 3(2^l - 1)e_2\}$.

Daqui, se existe $S \mid T_1T_2T_3$ subsequência não trivial de A-soma zero então S deve conter elementos de T_3, já que e_1 e e_2 são independentes. Mais que isso, devemos ter ou dois elementos com sinais opostos ou os três com mesmo sinal (essas são as únicas formas de anular a segunda coordenada).

Suponha primeiramente, que há dois elementos de T_3 com pesos opostos em S e chame-os $x_{|S|-1}$ e $x_{|S|}$. Neste caso, a soma $\alpha_{|S|-1}x_{|S|-1} + \alpha_{|S|}x_{|S|} = a$ é igual a $\pm 2^k e_1$ ou $\pm 2^{k+1} e_1$ e em nenhuma dessas opções temos $-a \in A_1$. Como todos os elementos de T_2 possuem primeira coordenada nula, é impossível que S seja de A-soma zero.

Assumindo agora que os três elementos de T_3 estão em S suponha, sem perda de generalidade, que os três assumem peso 1. Neste caso, a primeira coordenada da soma desses três elementos, digamos b, é

$$(3d + 2^k + 2^{k+1})e_1 = (3(m - 2^k) + 2^k + 2^{k+1})e_1 = 3me_1.$$

Lembrando que $m = \lfloor \frac{m_1}{6} \rfloor$, temos (sempre que dissermos abaixo $m_1 \equiv x \pmod 6$, vamos escrever $m_1 = 6p + x$ com $p \in \mathbb{Z}$):

1. Se $m_1 \equiv 0 \pmod 6$ então $\frac{m_1}{6} = p$ e $m = \left\lfloor \frac{m_1}{6} \right\rfloor = \frac{m_1}{6}$.
   Neste caso, $3m = 3\frac{m_1}{6} = \frac{m_1}{2}$ e $-\left(\frac{m_1}{2}\right) e_1 \notin A_1$, pois
   $2^k - 1 = 2^{\left\lfloor \log_2 \frac{m_1}{3} \right\rfloor} - 1 < 2^{\log_2 \frac{m_1}{3}} - 1 = \frac{m_1}{3} - 1 < \frac{m_1}{2}$.

2. Se $m_1 \equiv 1 \pmod 6$ então $\frac{m_1}{6} = \frac{6p+1}{6} = p + \frac{1}{6}$ e $\left\lfloor \frac{m_1}{6} \right\rfloor = p = \frac{m_1}{6} - \frac{1}{6}$.
   Neste caso, $3m = 3\left\lfloor \frac{m_1}{6} \right\rfloor = 3\left(\frac{m_1}{6} - \frac{1}{6}\right) = \frac{3(m_1-1)}{6} = \frac{m_1-1}{2}$ e $-\left(\frac{m_1-1}{2}\right) e_1 \notin A_1$, pois
   $2^k - 1 < \frac{m_1}{3} - 1 = \frac{m_1-3}{3} < \frac{m_1-1}{3} < \frac{m_1-1}{2}$.

3. Se $m_1 \equiv 2 \pmod 6$ então $\left\lfloor \frac{m_1}{6} \right\rfloor = \left\lfloor \frac{6p+2}{6} \right\rfloor = \left\lfloor p + \frac{2}{6} \right\rfloor = p = \frac{m_1}{6} - \frac{2}{6}$.
   Neste caso, $3m = 3\lfloor \frac{m_1}{6} \rfloor = 3\left(\frac{m_1}{6} - \frac{2}{6}\right) = \frac{m_1-2}{2}$ e $-\left(\frac{m_1-2}{2}\right) e_1 \notin A_1$, pois
   $2^k - 1 < \frac{m_1-3}{3} < \frac{m_1-2}{3} < \frac{m_1-2}{2}$.

4. Se $m_1 \equiv 3 \pmod 6$ então $\left\lfloor \frac{m_1}{6} \right\rfloor = \left\lfloor \frac{6p+3}{6} \right\rfloor = p + 1 = \frac{m_1}{6} - \frac{1}{2} + 1 = \frac{m_1}{6} + \frac{1}{2}$.
   Neste caso, $3m = 3\left\lfloor \frac{m_1}{6} \right\rfloor = 3\left(\frac{m_1}{6} + \frac{1}{2}\right) = \frac{m_1}{2} + \frac{1}{2} = \frac{m_1+1}{2}$ e $-\left(\frac{m_1+1}{2}\right) e_1 \notin A_1$, pois
   $2^k - 1 < \frac{m_1-3}{3} < \frac{m_1+1}{3} < \frac{m_1+1}{2}$.

5. Se $m_1 \equiv 4 \pmod 6$ então $\left\lfloor \frac{m_1}{6} \right\rfloor = \left\lfloor \frac{6p+4}{6} \right\rfloor = \left\lfloor p + \frac{4}{6} \right\rfloor = p + 1 = \frac{m_1}{6} - \frac{4}{6} + 1 = \frac{m_1}{6} + \frac{2}{6}$.
   Neste caso, $3m = 3\left\lfloor \frac{m_1}{6} \right\rfloor = 3\left(\frac{m_1}{6} + \frac{2}{6}\right) = \frac{m_1+2}{2}$ e $-\left(\frac{m_1+2}{2}\right) e_1 \notin A_1$, pois
   $2^k - 1 < \frac{m_1-3}{3} < \frac{m_1+2}{3} < \frac{m_1+2}{2}$.

6. Se $m_1 \equiv 5 \pmod 6$ então $\left\lfloor \frac{m_1}{6} \right\rfloor = \left\lfloor \frac{6p+5}{6} \right\rfloor = p + 1 = \frac{m_1}{6} - \frac{5}{6} + 1 = \frac{m_1}{6} + \frac{1}{6}$.
   Neste caso, $3m = 3\left\lfloor \frac{m_1}{6} \right\rfloor = 3\left(\frac{m_1}{6} + \frac{1}{6}\right) = \frac{m_1+1}{2}$ e $\left(-\frac{m_1+1}{2}\right) e_1 \notin A_1$, pois
   $2^k - 1 < \frac{m_1-3}{3} < \frac{m_1+1}{3} < \frac{m_1+1}{2}$.

Resumindo, a soma dos três elementos de T_3 nos dá

$$b = \left(\frac{m_1 + \epsilon}{3}\right) e_1 \text{ com } \epsilon \in [-2, 3]$$

e em nenhum desses casos temos $-b \in A_1$. Assim, novamente é impossível que S seja de A-soma zero. ∎

O caráter geral dessa proposição nos permite obter resultados ainda melhores para o limite inferior de $D_{\pm}(G)$ em alguns casos. De fato, quando m_1 e m_2 nos dá $G = C_{m_1} \oplus C_{m_2}$ como a melhor decomposição em grupos cíclicos no sentido de que produz o maior limite inferior conforme o Teorema 3.8 (quando m_1 e m_2 são potências de primo, por exemplo), obtemos $\lfloor \log_2 m_1 \rfloor + \lfloor \log_2 m_2 \rfloor + 1$ como limite inferior. Já de acordo com a proposição acima, obtemos $\lfloor \log_2(m_1/3) \rfloor + \lfloor \log_2(m_2/3) \rfloor + 4$.

Assim, existem casos em que a construção da proposição é mais vantajosa. Apresentamos agora algumas consequências disso. O resultado abaixo vai nos ajudar a encontrar $D_{\pm}(G)$ para algumas situações mais restritas.

Proposição 3.15. *Sejam $m_1, \ldots, m_r$ inteiros positivos com $\{\log_2 m_i\} \geqslant \{\log_2 3\}$ e $m_i \geqslant 4$ para no mínimo $\lfloor r/2 \rfloor$ deles. Se $\sum_{i=1}^{r} \{\log_2 m_i\} < \lfloor r/2 \rfloor + 1$, então*

$$D_{\pm}(G) = \left\lfloor \sum_{i=1}^{r} \log_2 m_i \right\rfloor + 1$$

onde $G = \bigoplus_{i=1}^{r} C_{m_i}$.

Demonstração: Do Teorema 3.8 segue que $D_{\pm}(G) \leqslant \lfloor \sum_{i=1}^{r} \log_2 m_i \rfloor + 1$. Agora, vamos mostrar que este também é o limite inferior.

Considere $s = \lfloor r/2 \rfloor$ e, sem perda de generalidade, assuma $m_1 \leqslant m_2 \leqslant \cdots \leqslant m_r$. Note que $m_1 \geqslant 3$ pela condição $\{\log_2 m_i\} \geqslant \{\log_2 3\}$. Além disso, como organizamos os m_i's em ordem crescente, temos que para cada $i \in [r - s + 1, r]$, $m_i \geqslant 4$. Daí, para cada i, a Proposição 3.14 nos diz que

$$\begin{aligned} D_{\pm}(C_{m_i} \oplus C_{m_{i-s}}) &\geqslant \lfloor \log_2(m_i/3) \rfloor + \lfloor \log_2(m_{i-s}/3) \rfloor + 4 \\ &= \lfloor \log_2 m_i - \log_2 3 \rfloor + \lfloor \log_2 m_{i-s} - \log_2 3 \rfloor + 4 \\ &\geqslant \lfloor \log_2 m_i \rfloor - \lfloor \log_2 3 \rfloor + \lfloor \log_2 m_{i-s} \rfloor - \lfloor \log_2 3 \rfloor + 4 \\ &= \lfloor \log_2 m_i \rfloor + \lfloor \log_2 m_{i-s} \rfloor + 2. \end{aligned}$$

Por repetição usando o Lema 3.5 e, em caso de r ser ímpar usando o limite inferior de $D_{\pm}(C_{m_i})$, obtemos um limite inferior de $\sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \lfloor r/2 \rfloor + 1$.

Agora, para ver que $D_{\pm}(G) \geqslant \lfloor \sum_{i=1}^{r} \log_2 m_i \rfloor + 1$, note primeiro que como temos $\log_2 m_i = \lfloor \log_2 m_i \rfloor + \{\log_2 m_i\}$ para cada $i \in [1, r]$, então

$$\sum_{i=1}^{r} \log_2 m_i = \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \sum_{i=1}^{r} \{\log_2 m_i\}. \tag{3.3}$$

Assim, de (3.3) e da condição $\sum_{i=1}^{r} \{\log_2 m_i\} < \lfloor r/2 \rfloor + 1$, temos

$$
\begin{aligned}
\left\lfloor \sum_{i=1}^{r} \log_2 m_i \right\rfloor &= \left\lfloor \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \sum_{i=1}^{r} \{\log_2 m_i\} \right\rfloor \\
&= \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \sum_{i=1}^{r} \{\log_2 m_i\} - \left\{ \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \sum_{i=1}^{r} \{\log_2 m_i\} \right\} \\
&= \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \sum_{i=1}^{r} \{\log_2 m_i\} - \left\{ \sum_{i=1}^{r} \{\log_2 m_i\} \right\} \\
&< \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \lfloor r/2 \rfloor + 1 - \left\{ \sum_{i=1}^{r} \{\log_2 m_i\} \right\} \\
&\leqslant \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \lfloor r/2 \rfloor + 1.
\end{aligned}
$$

Daí, concluímos que

$$
\begin{aligned}
\left\lfloor \sum_{i=1}^{r} \log_2 m_i \right\rfloor &< \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \lfloor r/2 \rfloor + 1 \\
&\Rightarrow \left\lfloor \sum_{i=1}^{r} \log_2 m_i \right\rfloor + 1 < \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \lfloor r/2 \rfloor + 2 \\
&\qquad\qquad\qquad\qquad \leqslant \sum_{i=1}^{r} \lfloor \log_2 m_i \rfloor + \lfloor r/2 \rfloor + 1,
\end{aligned}
$$

como queríamos. ∎

É preciso observar que, apesar de o resultado acima ser significativo para $r \leqslant 10$, ele se torna inútil quando r é muito grande já que não existem m_i's suficientes satisfazendo as condições do enunciado. Mas isso não o torna menos importante. Através dele podemos obter o valor exato de $D_{\pm}(G)$ para vários casos adicionais como, por exemplo, os apresentados nos teoremas abaixo.

Teorema 3.16. *Seja $n \geqslant 4$ um inteiro com $\{\log_2 n\} \geqslant \{\log_2 3\}$. Se $r \in \mathbb{Z}$ é tal que $\{\log_2 n\} < \frac{\lfloor r/2 \rfloor + 1}{r}$, então*

$$D_{\pm}(C_n^r) = \lfloor r \log_2 n \rfloor + 1.$$

Demonstração: Essa é uma consequência direta da proposição anterior. De fato, $D_{\pm}(C_n^r) = \lfloor \sum_{i=1}^{r} \log_2 n \rfloor + 1 = \lfloor \log_2 n^r \rfloor + 1 = \lfloor r \log_2 n \rfloor + 1$ e as condições impostas sobre $\{\log_2 n\}$ coincidem com as condições da proposição. ∎

Teorema 3.17. *Seja $n \geqslant 2$ um inteiro tal que $\{\log_2 3n\} < 1 - \{\log_2 3\}$ ou $\{\log_2 3n\} \geqslant \{\log_2 3\}$. Então*

$$D_{\pm}(C_3 \oplus C_{3n}) = \lfloor \log_2 9n \rfloor + 1.$$

Demonstração: Pelo Teorema 3.8, $\lfloor \log_2 9n \rfloor + 1$ é limite superior de $D_{\pm}(C_3 \oplus C_{3n})$ para todo n. Se $\{\log_2 3n\} < 1 - \{\log_2 3\}$, então $\lfloor \log_2 9n \rfloor = \lfloor \log_2 3 \rfloor + \lfloor \log_2 3n \rfloor$ e a afirmação segue obtendo o limite inferior também pelo Teorema 3.8.

Se $\{\log_2 3n\} \geqslant \{\log_2 3\}$, podemos aplicar a proposição acima com $m_1 = 3$, $m_2 = 3n$ para obter o limite inferior de $\lfloor \log_2 3 \rfloor + \lfloor \log_2 3n \rfloor + 2$ que é igual a $\lfloor \log_2 9n \rfloor + 1$. ■

Finalizamos esse capítulo apresentando, com o teorema abaixo, como na prática o limite superior obtido com o Teorema 3.8 também pode ser melhorado.

Teorema 3.18. *Se $G \simeq C_3 \oplus C_3 \oplus C_9$, então $D_\pm(G) = 6$.*

Demonstração: Seja $A = \{-1, 1\}$. Pelo Teorema 3.8 temos $D_\pm(G) \geqslant 6$. Seja S uma sequência de elementos de G de tamanho 6 e suponha que S não possui subsequência não trivial de A-soma zero.

A primeira coisa que observamos é que S possui apenas elementos de ordem 9. De fato, suponha que S possua um elemento h de ordem 3 e considere $H = \langle h \rangle$. Então $G/H \simeq C_3^3$ ou $C_3 \oplus C_9$ e em qualquer caso, pelo Teorema 3.8,

$$D_\pm(C_3 \oplus C_3) \leqslant \lfloor 2\log_2 3 \rfloor + 1 = \lfloor \log_2 9 \rfloor + 1 = 3 + 1 = 4 < 5 \text{ e}$$

$$D_\pm(C_3 \oplus C_9) \leqslant \lfloor 2\log_2 27 \rfloor + 1 = 4 + 1 = 5$$

e temos $D_\pm(G/H) \leqslant 5$. Assim, considerando $\pi : G \longrightarrow G/H$ a projeção canônica, $\pi(h^{-1}S)$ possui uma subsequência não trivial de A-soma zero em G/H, ou seja, $\Sigma_\pm(h^{-1}S) \cap H \neq \emptyset$. Como $H = \{-h, 0, h\}$ (já que é gerado por h que tem ordem 3), qualquer que seja o elemento de H em $\Sigma_\pm(h^{-1}S)$, podemos obter uma subsequência não trivial de A-soma zero de S, uma contradição. Daí, cada elemento de S tem ordem 9.

Escolha então $f \in S$ e considere $G = K \oplus \langle f \rangle$ onde K é um subgrupo de G isomorfo a C_3^2. Chame t o número de elementos de S que estão contidos em $\langle f \rangle$. Como $\langle f \rangle \simeq C_9$, temos $D_\pm(\langle f \rangle) = D_\pm(C_9) = \lfloor \log_2 9 \rfloor + 1 = 4$ pelo Teorema 2.5. Daí, o número t é no máximo 3. Considere os casos abaixo de acordo com o valor de t.

Caso 1: $\mathbf{t = 3}$. Considere T a subsequência de S de elementos em $\langle f \rangle$. Como $D_\pm(C_9) = 4$, T é a sequência de maior comprimento de elementos de $\langle f \rangle$ sem subsequência não trivial de A-soma zero. Afirmamos que $\Sigma_\pm(T) \cup \{0\} = \langle f \rangle$. De fato, escreva $\langle f \rangle = \{f, 2f, 3f, 4f, 5f, 6f, 7f, 8f, 0\}$ e $T = a_1a_2a_3$. Como $0 \notin \Sigma_\pm(T)$, temos $-a_i \neq a_j$ para todo $i, j \in \{1, 2, 3\}$. Daí, $\{a_1, a_2, a_3, -a_1, -a_2, -a_3\} \subset \Sigma_\pm(T)$ e esses são todos os elementos de ordem 9 de $\langle f \rangle$. Sabendo disso, podemos renomear e escrever $a_1 = f$, $a_2 = 2f$, $a_3 = 4f$, obtendo assim $a_1 + a_2 = 3f$ e $a_2 + a_3 = 6f$, ambos pertencentes a $\Sigma_\pm(T)$. Isso mostra que $\langle f \rangle \subset \Sigma_\pm(T) \cup \{0\}$. A inclusão contrária é imediata.

Considere agora o projeção canônica $\pi : K \oplus \langle f \rangle \longrightarrow K$ e observe que $\pi(T^{-1}S)$ possui subsequência não trivial de A-soma zero em K, ou seja, $\Sigma_\pm(T^{-1}S) \cap \langle f \rangle \neq \emptyset$ ($|T^{-1}S| = 3$ e $D_\pm(K) = 3$ pelo Corolário 2.7). Seja $a \in \Sigma_\pm(T^{-1}S) \cap \langle f \rangle$. Como $\Sigma_\pm(T) \cup \{0\} = \langle f \rangle$, existe $-a \in \Sigma_\pm(T)$ e isso nos permite obter uma subsequência não trivial de A-soma zero de S em G, uma contradição.

Caso 2: $\mathbf{t = 2}$. Suponha agora que existem 2 elementos de $\langle f \rangle$ em S. Lembrando que podemos substituir, sem restrição, um elemento por seu inverso, podemos supor que estes elementos são f e $2f$, $2f$ e $4f$ ou f e $4f$.

Observe agora que $\psi : G \longrightarrow G$ definida por $\psi(g) = 2g$ é um isomorfismo pela Observação 1.25 já que $(2, 9) = 1$. Além disso, $\psi(f2f) = 2f4f$. Daí, os casos em que $T = f2f$ e $T = 2f4f$ nos fornecem resultados equivalentes. O mesmo podemos dizer a respeito de $f2f$ e $f4f$ pois $\psi' : G \longrightarrow G$ definida por $\psi'(g) = 5g$ é isomorfismo tal que $\psi'(f2f) = f(-4f)$ e como podemos substituir, sem restrição, um elemento por seu inverso, os casos $T = f2f$ e $T = f4f$ são também equivalentes e podemos assumir que f e $2f$ são os dois elementos de $\langle f \rangle$ em S, ou seja, $T = f2f$.

Note que $\Sigma_\pm(T) \cup \{0\} = \{-3f, -2f, -f, 0, f, 2f, 3f\}$. O conjunto $\Sigma_\pm(T^{-1}S) \cap \langle f \rangle$ é disjunto de $\{-3f, -2f, -f, 0, f, 2f, 3f\}$ pois, caso contrário, S possuiria uma subsequência não trivial de A-soma zero. Daí, $\Sigma_\pm(T^{-1}S) \cap \langle f \rangle \subset \{-4f, 4f\}$.

Defina $R = T^{-1}S$, considere mais uma vez a projeção canônica $\pi : G \simeq K \oplus \langle f \rangle \longrightarrow K$ e vamos analisar como a sequência se comporta através de vários subcasos de acordo com a estrutura de $\pi(R)$:

Subcaso 2.1. $\pi(R)$ possui algum elemento de multiplicidade pelo menos 3. Então R possui uma subsequência do tipo $(e+f_1)(e+f_2)(e+f_3)$ com $e \in K$, $f_i \in \langle f \rangle$, $i \in \{1, 2, 3\}$. Considerando todas as somas do tipo $f_i - f_j$ com $i, j \in \{1, 2, 3\}$ distintos, pelo que dissemos acima, elas são todas elementos de $\{-4f, 4f\}$. Mas note que $f_3 - f_1 = (f_3 - f_2) + (f_2 - f_1)$ e isso é impossível (a soma de dois elementos de $\{-4f, 4f\}$ não pode ser um elemento desse conjunto).

Subcaso 2.2. $\pi(R)$ possui exatamente dois elementos de multiplicidade pelo menos 2.

Então R possui uma subsequência do tipo $(e + f_1)(e + f_2)(e' + f_1')(e' + f_2')$ com $e, e' \in K$ e $f_1, f_2, f_1', f_2' \in \langle f \rangle$. Como anteriormente, $(f_1 - f_2), (f_1' - f_2')$ e $(f_1 - f_2) + (f_1' - f_2')$ são todos elementos de $\{-4f, 4f\}$ e como o último é soma dos dois primeiros, isso é impossível.

Subcaso 2.3. $\pi(R)$ possui exatamente um elemento de multiplicidade 2. Então $\pi(R) = e^2e'e''$, com $e, e', e'' \in K$. Mas, como já vimos que $D_\pm(K) = 3$, vamos assumir e, e' independentes e isso é possível pois existe sequência de dois elementos em K livre de A-soma zero e além disso, os a_i's da definição de independência são unicamente determinados módulo $\mathrm{ord}(e_i)$. No nosso caso, como $\exp(K) = 3$, $a_i \in \{-1, 0, 1\}$. Assim, sendo e, e' independentes, pelas condições impostas por este subcaso, existem $a_1, a_2 \in \{-1, 1\}$ tais que $e'' = a_1e + a_2e'$. Agora, já que quando $A = \{-1, 1\}$, trocar elementos de uma sequência por seus inversos não muda o fato da sequência ser de A-soma zero ou não, podemos assumir $e'' = -e - e'$.

Escrevemos então $R = (e + f_1)(e + f_2)(e' + f')(-e - e' + f'')$ onde os f_i's são elementos de $\langle f \rangle$. De modo análogo ao que já fizemos, temos $f_2 - f_1, f_1 - f' + f''$ e $f_2 + f' + f''$ são todos elementos de $\{-4f, 4f\}$ e o último é a soma dos dois primeiros, impossível.

Subcaso 2.4. $\pi(R)$ é livre de quadrados. Então $\pi(R) = e_1e_2e_3e_4$ com $e_i \in K$, $i \in [1, 4]$. Como no caso anterior, assumimos e_1, e_2 independentes e tomamos $e_3 = -e_1 - e_2$, $e_4 = e_1 - e_2$. Escreva então $R = (e_1+f_1)(e_2+f_2)(-e_1-e_2+f_3)(e_1-e_2+f_4)$ com $f_i \in \langle f \rangle$, $i \in [1, 4]$. Com operações simples, encontramos

$$h_1 = f_1 + f_2 + f_3,\ h_2 = -f_1 + f_2 + f_4,\ h_3 = -f_2 + f_3 + f_4 \text{ e } h_4 = f_1 - f_3 + f_4,$$

todos elementos de $\{-4f, 4f\}$. Sem perda de generalidade, suponha $h_1 = 4f$.

Note que $h_1 + h_2 + 2h_3 = 3(f_3 + f_4)$ é um elemento de $4f + \{-4f, 4f\} + \{f, -f\}$ (se $h_3 \in \{-4f, 4f\}$ então $2h_3 \in \{-8f, 8f\} = \{f, -f\}$).

Se $h_2 = -4f$, então $2h_3 = 3(f_3 + f_4) \in \{f, -f\}$, o que não é possível pois $3(f_3 + f_4)$ tem ordem 3 ou 0 e $f, -f$ são elementos de ordem 9. Então $h_2 = h_1 = 4f$. Agora, $h_1 - h_2 + h_4 = h_4 = 3f_1 \in \{-4f, 4f\}$ o que também é impossível já que $-4f, 4f$ são elementos de ordem 9 e $3f_1$ tem ordem 3 ou 0.

Caso 3: t = 1. Conforme fizemos no caso anterior, vamos estudar o comportamento da sequência $R = f^{-1}S$ de acordo com os subcasos abaixo a respeito da estrutura da imagem de R sobre a projeção canônica $\pi : K \oplus \langle f \rangle \longrightarrow K$.

Subcaso 3.1. $\pi(R)$ possui algum elemento de multiplicidade no mínimo 4. Então $R = (e + f_1)(e + f_2)(e + f_3)(e + f_4)e'$ com $e, e' \in K$, $f_i \in \langle f \rangle$, $i \in [1, 4]$. Mais que isso, devemos ter $f_i \in \{f, 2f, 4f, 5f, 7f, 8f\}$ já que são todos de ordem 9. É fácil ver que dados quaisquer quatro elementos desse conjunto, é possível obter $f_i - f_j = -f$ e isso nos dá uma subsequência não trivial de A-soma zero de S.

Subcaso 3.2. $\pi(R)$ possui algum elemento de multiplicidade 3. Escreva $R = (e + f_1)(e + f_2)(e + f_3)gh$ com $e \in K$, $f_i \in \langle f \rangle$, $g, h \in G$. Suponha primeiro que $\pi(g) = \pm\pi(h)$. Assim, ou $g + h$ ou $g - h$ é um elemento de $\langle f \rangle$. Sem perda de generalidade, suponha que $g + h \in \langle f \rangle$ e observe que a sequência $(g + h)(gh)^{-1}S$ possui dois elementos de $\langle f \rangle$. A princípio, essa sequência não satisfaz as condições do caso anterior já que possui um elemento a menos. Mas o argumento lá usado, utiliza apenas o fato de haver dois elementos em $\langle f \rangle$ e um com multiplicidade 3 em K, então podemos usá-lo aqui também.

Agora, assuma $\pi(g), \pi(h)$ independentes. Então, $\pi(g)$ e $\pi(h)$ geram K e existe uma escolha de pesos $\alpha_1, \alpha_2 \in \{-1, 1\}$ tal que $\alpha_1 g + \alpha_2 h = -e + f'$ para algum $f' \in \langle f \rangle$. Escreva $S' = f(e + f_1)(e + f_2)(e + f_3)(-e + f')$ e como assumimos S livre de subsequência não trivial de A-soma zero, devemos ter $\Sigma_\pm(f^{-1}S) \cap \langle f \rangle \subset \{\pm 2f, \pm 4f\}$, pois $\Sigma_\pm(f) \cup \{0\} = \{-f, 0, f\}$ e $\Sigma_\pm(f^{-1}S) \cap \langle f \rangle$ deve ser disjunto de $\{-f, 0, f\}$.

Note que para cada $i \in \{1, 2, 3\}$, devemos ter

$$f' + f_i \in \Sigma_\pm(f^{-1}S) \cap \langle f \rangle \subset \{\pm 2f, \pm 4f\}$$

e para todo $i, j \in \{1, 2, 3\}$, devemos ter

$$(f' + f_i) - (f' + f_j) = f_i - f_j \in \Sigma_\pm(f^{-1}S) \cap \langle f \rangle.$$

Mas isso é impossível. De fato, cada $f' + f_i$ é distinto e o mesmo vale para as diferenças do tipo $f_i - f_j$ (elementos repetidos fornecem uma subsequência de A-soma zero). Isso gera seis elementos distintos ($f' + f_i$, com $i \in \{1, 2, 3\}$, $f_i - f_j$, com $i \neq j \in \{1, 2, 3\}$) que não podem pertencer todos a $\{\pm 2f, \pm 4f\}$ que possui apenas quatro elementos.

Subcaso 3.3. $\pi(R)$ possui dois elementos distintos com multiplicidade 2. Podemos assumir que esses dois elementos, digamos e_1 e e_2, são independentes (caso contrário, esse seria essencialmente, o Subcaso 3.1). Além disso, o elemento que restou em $\pi(R)$ é independente com e_1 e e_2 pois senão isso se reduziria ao Subcaso 3.2. Tome então esse terceiro elemento como $-e_1 - e_2$ e escreva

$$R = (e_1 + f_1)(e_1 + f_1')(e_2 + f_2)(e_2 + f_2')(-e_1 - e_2 + f').$$

Observe que $(f_1 - f_1')(f_2 - f_2')f$ não possui subsequência não trivial de A-soma zero, pois pode ser obtida de S através de operações de adição e subtração de elementos e S não possui subsequência não trivial de A-soma zero. Podemos então assumir $f_1' - f_1 = 2f$ e $f_2' - f_2 = 4f$ (não há perda de generalidade ao assumir isso, já que podemos substituir, sem restrição, um elemento por seu inverso).

Observe agora que a partir de S podemos obter várias sequências operando de diferentes formas alguns de seus elementos, por exemplo,

$$\begin{aligned} S_2 &= f(e_1 + f_1')(e_2 + f_2')(f_1 + f_2 + f'), \\ S_3 &= f(e_1 + f_1)(e_2 + f_2')(f_1' + f_2 + f'), \\ S_4 &= f(e_1 + f_1')(e_2 + f_2)(f_1 + f_2' + f') \text{ e} \\ S_5 &= f(e_1 + f_1)(e_2 + f_2)(f_1' + f_2' + f'). \end{aligned}$$

Nenhuma dessas sequências possui subsequência não trivial de A-soma zero. Em particular,

$$f_1 + f_2 + f', f_1' + f_2 + f', f_1 + f_2' + f', f_1' + f_2' + f' \notin \{-f, 0, f\}.$$

De acordo com essas informações temos que $f_1 + f_2 + f' + m \notin \{-f, 0, f\}$ para cada $m \in \{0, 2f, 4f, 6f\}$ (para ver isso, basta substituir m por esses valores e lembrar que $2f = f_1' - f_1, 4f = f_2' - f_2$ e $6f = 2f + 4f$). Mas $-\{0, 2f, 4f, 6f, \} + \{-f, 0, f\} = \langle f \rangle$ e isso gera um absurdo. Entenda o porquê:

Chame $f_1 + f_2 + f' = f^* \in \langle f \rangle$. Temos que

$$f^* + m \notin \{-f, 0, f\} \ \forall \ m \in \{0, 2f, 4f, 6f\}.$$

Isso é equivalente a dizer que $f^* \notin \{-f, 0, f\} - \{0, 2f, 4f, 6f\} \Rightarrow f^* \notin \langle f \rangle$, um absurdo.

Subcaso 3.4. $\pi(R)$ possui somente um elemento de multiplicidade 2 (e os outros elementos com multiplicidade 1).

Usando o mesmo argumento dos subcasos anteriores, escreva

$$\pi(R) = e_1(-e_1)e_2(e_1 + e_2)(-e_1 + e_2)$$

e ponha

$$R = (e_1 + f_+)(-e_1 + f_-)(e_1 + e_2 + a_1)(e_2 + a_2)(-e_1 + e_2 + a_3)$$

com os f's e a_i's em $\langle f \rangle$.

Note que $S' = f(f_+ + f_-)(a_1 + a_2 + a_3)$ não possui subsequência não trivial de A-soma zero já que pode ser obtida de S (que é livre de soma zero) ao realizar algumas operações entre seus elementos [para justificar a ausência do termo $3e_2$ no último elemento de S', lembre-se que $3e_2 = 0$ pois $\exp(K) = 3$]. Daí, podemos assumir sem perda de generalidade que

$$\{f_+ + f_-, a_1 + a_2 + a_3\} = \{2f, 4f\} \tag{3.4}$$

Listamos abaixo algumas subsomas de $\pi(R)$ que resultam em zero em $\pi(G) = K$ e as respectivas subsomas resultantes em G quando não consideramos a projeção π.

Subsomas A-ponderadas nulas em $\pi(R)$	Subsomas resultantes em G
$(e_1 + e_2) - (e_2) - (e_1)$	$a_1 - a_2 - f_+$
$(e_1 + e_2) - (e_2) + (-e_1)$	$a_1 - a_2 + f_-$
$(e_1 + e_2) - (e_2) + (e_1) - (-e_1)$	$a_1 - a_2 + f_+ - f_-$
$(e_2) - (-e_1 + e_2) - (e_1)$	$a_2 - a_3 - f_+$
$(e_2) - (-e_1 + e_2) + (-e_1)$	$a_2 - a_3 + f_-$
$(e_2) - (-e_1 + e_2) + (e_1) - (-e_1)$	$a_2 - a_3 + f_+ - f_-$
$(-e_1 + e_2) - (e_1 + e_2) - (e_1)$	$a_3 - a_1 - f_+$
$(-e_1 + e_2) - (e_1 + e_2) + (-e_1)$	$a_3 - a_1 + f_-$
$(-e_1 + e_2) - (e_1 + e_2) + (e_1) - (-e_1)$	$a_3 - a_1 + f_+ - f_-$

Como supomos que S não tem subsequência não trivial de A-soma zero, nenhuma das subsomas de R dadas na segunda coluna da tabela acima pode pertencer a $\{-f, 0, f\}$. Considerando

$$\mathcal{A} = \{a_1 - a_2, a_2 - a_3, a_3 - a_1\}$$
e
$$\mathcal{F} = \{-f_+, f_-, f_+ - f_-\},$$

podemos resumir a tabela tabela acima como $(\mathcal{F} + \mathcal{A}) \cap \{-f, 0, f\} = \emptyset$, ou ainda

$$\mathcal{A} \cap (-\mathcal{F} + \{-f, 0, f\}) = \emptyset.$$

Escreva agora $F = f_+ + f_-$ e $A = a_1 + a_2 + a_3$. Observe que $-\mathcal{F} = \{f_+, -F + f_+, F - 2f_+\}$ e lembre que $F = 2f$ ou $F = 4f$ por (3.4).

Se $F = 2f$, temos as seguintes possibilidades para $-\mathcal{F}$:

$$\{f, -f, 0\}, \{4f, 2f, 3f\} \text{ e } \{-2f, -4f, -3f\}. \tag{3.5}$$

Para $-F + \{-f, 0, f\}$, temos, respectivamente,

$$\{-2f, -f, 0, f, 2f\}, \{-4f, f, 2f, 3f, 4f\} \text{ e } \{-4f, -3f, -2f, -f, -4f\}. \tag{3.6}$$

Encontramos esses conjuntos analisando os valores que f_+ pode assumir, lembrando que f_+ é um elemento de ordem 9 de $\langle f \rangle$ e $f_+ + f_- = F$.

Se $F = 4f$, obtemos as seguintes possibilidades para $-\mathcal{F}$:

$$\{2f, -2f, 0\}, \{-4f, f, 3f\} \text{ e } \{-f, 4f, -3f\}. \tag{3.7}$$

Assim, para $-\mathcal{F} + \{-f, 0, f\}$ temos

$$\begin{gathered} \{-3f, -2f, -f, 0, f, 2f, 3f\}, \{-4f, -3f, 0, f, 2f, 3f, 4f\} \\ \text{e} \\ \{-4f, -3f, -2f, -f, 0, 3f, 4f\} \end{gathered} \tag{3.8}$$

respectivamente. Nosso trabalho agora é verificar se é possível ter

$$\mathcal{A} \cap (-\mathcal{F} + \{-f, 0, f\}) = \emptyset \tag{3.9}$$

para os conjuntos que listamos acima.

Observe que, em $\mathcal{A}$, temos

$$a_3 - a_1 = A - 2a_1 - a_2 \text{ e } a_2 - a_3 = ((a_3 - a_1) + (a_1 - a_2))$$

e podemos escrever $\mathcal{A} = \{a, -(a+b), b\}$ com $a = a_1 - a_2$ e $b = A - 2a_1 - a_2$.

Daqui, vemos que é impossível ter $F = 4f$, já que o complementar de cada um dos três conjuntos listados em (3.8) não contém sequer um conjunto com a mesma quantidade de elementos que $\mathcal{A}$. Vamos estudar então o caso em que $F = 2f$.

Mais uma vez, observando os elementos de $\mathcal{A}$, note que

$$a = a_1 - a_2 \text{ e } b = A - 2a_1 - a_2 \Leftrightarrow a_1 - a_2 = a \text{ e } -3a_2 = 2a + b - A.$$

Assim, devemos ter $2a + b - A$ um elemento de ordem 0 ou 3.

Lembrando que $a, b, A \in \langle f \rangle$, escreva $a = a'f$, $b = b'f$ e $A = A'f$. Pelo que dissemos acima, devemos ter $2a' + b' - A' \equiv 0 \,(\text{mod } 3)$ ou, equivalentemente, $b' \equiv a' + A' \,(\text{mod } 3)$.

Consideramos então cada um dos três conjuntos listados em (3.6) separadamente. Em algum desses conjuntos deverá ser possível encontrar a, b cumprindo $b' \equiv a' + A' (\text{mod } 3)$ tais que $\{a, b, -(a+b)\}$ não intercepta o respectivo conjunto.

Para $\{-2f, -f, 0, f, 2f\}$ temos: se $a = 3f$ então $b = 4f$. Se $a = 4f$ então $b = -4f$. Se $a = -3f$ então $b = 4f$. Se $a = -4f$ então $b = \pm 3f$. Em qualquer caso, $-(a+b)$ está no conjunto.

Para $\{-4f, f, 2f, 3f, 4f\}$ temos: se $a = -3f$ então $b = -2f$. Se $a = -2f, b = -f$ Se $a = -f$ então $b = 0$ ou $3f$. Se $a = 0, b = -2f$. Em qualquer caso, $-(a+b)$ está no conjunto.

Para $\{-4f, -3f, -2f, -f, -4f\}$ temos: se $a = 0$ então $b = f$, se $a = f$ então $b = 2f$, se $a = 2f$ então $b = 3f$ ou $b = 0$ e se $a = 3f$ então $b = f$. Em qualquer caso, $-(a+b)$ está no conjunto.

Assim, não conseguimos obter a e b de forma que $\mathcal{A}$ satisfaça (3.9). Isso estabelece a contradição ao que assumimos no início da demonstração, a saber, que S não possui subsequência não trivial de A-soma zero.

Isso conclui que $D_{\pm}(C_3^2 \oplus C_9) \leqslant 6$ e a igualdade segue. ■

Capítulo 4

A Constante de Harborth

Em 1973, H. Harborth introduziu, em [14], a constante $g(G)$, que hoje leva o seu nome e que é o objeto de estudo deste capítulo. Neste mesmo trabalho, H. Harborth apresentou valores exatos desta constante para grupos específicos, além de formalizar o que havia sido feito no Teorema de Erdős-Ginzburg-Ziv, que até então era apenas um resultado em Teoria Aditiva dos Números.

A versão com peso $\{-1, 1\}$ da constante de Harborth, denotada por $g_{\pm}(G)$, foi estudada, dentre outros, por L. E. Marchan *et al.*, em [21]. Nosso objetivo aqui é a prova de um de seus resultados, a saber, o Teorema 4.10 que será importante para alguns dos resultados que apresentaremos no Capítulo 5.

Vamos apresentar a prova de uma série de resultados sobre $g_{\pm}(G)$ para certos grupos G, que juntos, somarão ferramentas para a demonstração do teorema que é o nosso objetivo. Como já mencionamos, nosso trabalho aqui se baseia no Artigo [21] de Marchan *et al.*

Lema 4.1. *Se G é um 2-grupo elementar, então $g_{\pm}(G) = g(G) = |G| + 1$.*

Demonstração: Seja $A = \{-1, 1\}$. Se G é 2-grupo elementar, então $\text{ord}(g) = 2$, ou seja, $g = -g$ para todo $g \in G$. Isso quer dizer que em uma sequência de elementos de G, a escolha dos sinais é irrelevante quando nosso objetivo é estudar a existência de subsequência de A-soma zero de S. Daí, $g_{\pm}(G) = g(G)$. Para ver que $g(G) = |G|+1$, primeiro observe que não existe $S \in \mathcal{F}(G)$ livre de quadrados com $|S| \geqslant |G| + 1$. Assim, segue imediatamente que $g(G) \leqslant |G| + 1$. Por outro lado, tome $S \in \mathcal{F}(G)$ formada por todos os elementos de G. Temos $|S| = |G|$ e se $T|S$ de tamanho $\exp(G) = 2$, digamos, $T = ab$, então

$$\sigma(T) = a + b = 0 \Rightarrow a = -b = b,$$

o que é impossível, já que T é livre de quadrados. Assim, $g(G) = |G| + 1$, como queríamos. ■

Lema 4.2. *Seja $n \in \mathbb{N}$. Então*

$$g(C_n) = \begin{cases} n+1 & \textit{se } n \textit{ é par} \\ n & \textit{se } n \textit{ é ímpar} \end{cases}.$$

Demonstração: Da definição, $g(C_n) \geqslant n$ para todo $n \in \mathbb{N}$. Suponha n ímpar e escreva $C_n = \langle a \rangle$. Seja $S \in \mathcal{F}(C_n)$ livre de quadrados com $|S| = n$. A única sequência com essa propriedade é $S = 0a \cdots (n-1)a$ e

$$\sigma(S) = 0 + \cdots + (n-1)a = \frac{na(n-1)}{2} = 0$$

pois $\mathrm{ord}(a) = n$ e $2 \mid n-1$. Isso mostra que $g(C_n) = n$ quando n é ímpar. Agora, se n é par, S como indicada no caso n ímpar, é tal que

$$\sigma(S) = \frac{na(n-1)}{2} = -\frac{na}{2} \neq 0$$

já que $\mathrm{ord}(a) = n$. Daí, $g(C_n) > n$.

A igualdade $g(C_n) = n+1$ segue por vacuidade, uma vez que não existe S sequência sobre C_n livre de quadrados com $|S| \geqslant n+1$. ■

Lema 4.3. *Sejam G um grupo abeliano finito e $S \in \mathcal{F}(G)$. Então*

$$\sigma_{\pm}(S) = -\sigma(S) + 2 \cdot \Sigma^0(S),$$

onde $2 \cdot \Sigma^0(S) = \{2a \mid a \in \Sigma^0(S)\}$. Em particular, se $|G|$ é ímpar, então $|\sigma_{\pm}(S)| = |\Sigma^0(S)| \geqslant 1 + |supp(S) \setminus \{0\}|$.

Demonstração: Seja $S = g_1 \cdots g_k \in \mathcal{F}(G)$. Por definição, temos $g \in \sigma_{\pm}(S)$ se, e somente se, $g = \sum_{i=1}^{k} \epsilon_i g_i$ com $\epsilon_i \in \{-1, 1\}$. Isso é equivalente a

$$g = -\sum_{i=1}^{k} g_i + \sum_{i=1}^{k} \delta_i g_i = -\sigma(S) + \sum_{i=1}^{k} \delta_i g_i \text{ com } \delta_i \in \{0, 2\}.$$

Agora note que $h = \sum_{i=1}^{k} \delta_i g_i$ com $\delta_i \in \{0, 2\}$ é equivalente a $h \in 2 \cdot \Sigma^0(S)$. Assim, $\sigma_{\pm}(S) = -\sigma(S) + 2 \cdot \Sigma^0(S)$. Em particular, quando $|G|$ é ímpar temos $|2 \cdot \Sigma^0(S)| = |\Sigma^0(S)|$ e o resultado segue. ■

Lema 4.4. *Sejam G um grupo abeliano finito e $A \subseteq [1, \exp(G)-1]$. Se $G = H \oplus K$ com $\exp(H) | \exp(K)$, então*

$$g_A(G) \geqslant O_A(H) + g_A(K) - 1.$$

Demonstração: Seja $S \in \mathcal{F}(K)$ livre de quadrados com $|S| = g_A(K) - 1$ sem subsequência de A-soma zero de tamanho $\exp(K)$ e $T \in \mathcal{F}(H)$ também livre de quadrados com $|T| = O_A(H) - 1$ sem subsequência não trivial de A-soma zero. Como $\exp(H) | \exp(K)$, temos $\exp(K) = \exp(G)$. Afirmamos que a sequência $ST \in \mathcal{F}(G)$ não possui subsequência de A-soma zero e tamanho $\exp(G)$. De fato, suponha que existe $S' | ST$ com $|S'| = \exp(G)$ e de A-soma zero. S' não pode ser subsequência de S pois isso contraria o fato de S não possuir subsequência de A-soma zero de tamanho $\exp(K)$. Daí, S' deve conter elementos de T, os quais formam uma subsequência de A-soma zero de T, o que é impossível pela forma que tomamos T. Isso mostra que $g_A(G) \geqslant |ST| + 1 = O_A(H) + g_A(K) - 1$. ■

Teorema 4.5. *Seja $n \in \mathbb{N}$. Então*

$$g_{\pm}(C_n) = \begin{cases} n+1 & se\ n \equiv 2 \pmod 4 \\ n & se\ n \not\equiv 2 \pmod 4 \end{cases}.$$

Demonstração: Primeiramente, note que, da definição, $g_{\pm}(C_n) \geqslant n$. Se n é ímpar, segue que $g_{\pm}(C_n) \leqslant g(C_n) = n$ pelo Lema 4.2. Assuma então n par e escreva $T = \prod_{i=0}^{n-1} ia$ onde a é um gerador de C_n. Observe que esta é a única sequência livre de quadrados de C_n de tamanho n. Além disso

$$\begin{aligned}\sum_{i=0}^{n/2} i - \sum_{i=n/2+1}^{n-1} i &= \frac{n}{4}\left(\frac{n}{2}+1\right) - \frac{1}{1}\left((n-1)-\frac{n}{2}\right)\left(\frac{n}{2}+1+(n-1)\right) \\ &= \frac{n}{4}\left(\frac{n}{2}+1\right) - \frac{3n}{4}\left(\frac{n}{2}-1\right) = \frac{-2n^2+8n}{8} = n\left(1-\frac{n}{4}\right).\end{aligned}$$

Assim, para $n \equiv 0 \pmod 4$ a soma acima é um múltiplo de n e logo, $0 \in \sigma_{\pm}(T)$. Agora, vamos mostrar que quando $n \equiv 2 \pmod 4$, $0 \notin \sigma_{\pm}(T)$. Note que

$$-\sigma(T) = -\sum_{i=0}^{n-1} ia = -\frac{n}{2}(n-1)a = \frac{n}{2}a = a + \frac{n-2}{4}2a.$$

Pelo Lema 4.3, temos $\sigma_{\pm}(T) = -\sigma(T) + 2 \cdot \Sigma^0(T)$. Como $n \equiv 2 \pmod 4$, $(n-2)/2$ é par. Assim,

$$-\sigma(T) + 2 \cdot \Sigma^0(T) = \left(a + \frac{n-2}{4}2a\right) + 2 \cdot \Sigma^0(T) \subseteq a + 2\langle a \rangle.$$

Como $2\langle a \rangle = \langle 2a \rangle$ e $-a \notin \langle 2a \rangle$, segue que $0 \notin \sigma_{\pm}(T)$, como queríamos. ■

A seguinte desigualdade é imediata do Lema 4.4 e do Teorema 4.5:

$$g_{\pm}(C_2 \oplus C_{2n}) \geqslant \begin{cases} 2n+2 & \text{se } n \text{ é ímpar} \\ 2n+1 & \text{se } n \text{ é par} \end{cases}. \tag{4.1}$$

Lema 4.6. *Seja $n \in \mathbb{N}_{\geqslant 3}$. Então $g_{\pm}(C_2 \oplus C_{2n}) \geqslant 2n+2$.*

Demonstração: Se n é ímpar, o resultado segue de (4.1). Assuma então n par. Escreva $C_2 \oplus C_{2n} = \langle e_1 \rangle \oplus \langle e_2 \rangle$ com $\mathrm{ord}(e_1) = 2$ e $\mathrm{ord}(e_2) = 2n$. Vamos considerar a sequência $S = TR$ onde $T = \prod_{i=1}^{2n-2} ie_2$ e $R = e_1(e_1+2e_2)(e_1+4e_2)$. T e R (e, portanto, S) são livres de quadrados, pois $\mathrm{ord}(e_2) = 2n$ e como $n \geqslant 3$, temos $2n \geqslant 6$. Vamos mostrar que $0 \notin \sigma_{\pm}(S)$. Observe que

$$\sigma(T) = \frac{(2n-2)(2n-1)}{2}e_2 = (n-1)(-e_2) = (1-n)e_2.$$

Da igualdade acima, do Lema 4.3 e lembrando que assumimos n par, ou seja, $n = 2k$ com $k \in \mathbb{N}$, temos $2ke_2 \in 2\langle e_2 \rangle$ e segue que

$$\begin{aligned}\sigma_{\pm}(T) &= -\sigma(T) + 2 \cdot \Sigma^0(T) = (1-n)e_2 + 2\langle e_2 \rangle \\ &= e_2 - ne_2 + 2\langle e_2 \rangle = e_2 - 2ke_2 + 2\langle e_2 \rangle \subseteq e_2 + 2\langle e_2 \rangle.\end{aligned}$$

Seja $S'|S$ com $|S'| = 2n$. Como $|T| = 2n-2$, S' não é subsequência de T. Isso quer dizer que S' possui elementos de R. Seja $R' = S' \cap R$ e observe que se $0 \in \sigma_{\pm}(S')$, então $|R'| = 2$, uma vez que, como $\mathrm{ord}(e_1) = 2$, essa é a única forma de obter 0 na primeira coordenada. Devemos ter então $S' = R'T$. Note que, quaisquer que sejam os dois elementos de R', temos $\sigma_\pm(R') \subseteq 2\langle e_2\rangle$. Como $\sigma_\pm(T) \subseteq e_2 + 2\langle e_2\rangle$, temos

$$\sigma_\pm(S') = \sigma_\pm(R') + \sigma_\pm(T) \subseteq 2\langle e_2\rangle + e_2 + 2\langle e_2\rangle = e_2 + 2\langle e_2\rangle.$$

Agora note que

$$0 \in e_2 + 2\langle e_2\rangle \Rightarrow 0 = e_2 + 2ke_2 \Rightarrow (1+2k)e_2 = 0 \Rightarrow 2n|(1+2k) \Rightarrow n|(1+2k)$$

para algum $k \in [1, 2n]$ o que é impossível, uma vez que n é par. Assim, temos $0 \notin \sigma_\pm(S')$, como queríamos. ■

Proposição 4.7. *Seja $n \in \mathbb{N}$ um número par. Então $g(C_2 \oplus C_{2n}) \leqslant 2n + 2$.*

Demonstração: Escreva $G = C_2 \oplus C_{2n} = \langle e_1\rangle \oplus \langle e_2\rangle$ com $\mathrm{ord}(e_1) = 2$ e $\mathrm{ord}(e_2) = 2n$. Considere π_1, π_2 as projeções de G em $\langle e_1\rangle$ e $\langle e_2\rangle$, respectivamente.

Seja $S \in \mathcal{F}(G)$ livre de quadrados de tamanho $2n+2$ e escreva $S = S_0S_1$ onde $\pi_1(g) = 0$ para $g|S_0$ e $\pi_1(g) = e_1$ para $g|S_1$. Vamos investigar os dois casos seguintes: $\pi_1(\sigma(S)) \neq 0$ e $\pi_1(\sigma(S)) = 0$.

Assuma primeiro que $\pi_1(\sigma(S)) \neq 0$, isto é $\pi_1(\sigma(S)) = e_1$. Observe que $\pi_2(S_0)$, $\pi_2(S_1)$ devem ser livres de quadrados para garantir que S também o seja, uma vez que $\pi_1(S_0)$, $\pi_1(S_1)$ são sequências constantes e logo, se existem elementos repetidos em $\pi_2(S_i)$, então eles se repetem também em S_i, com $i \in \{1, 2\}$. Com isso, temos

$$|\pi_2(S_0)| + |\pi_2(S_1)| = |S_0| + |S_1| = |S| = 2n + 2 > 2n.$$

Portanto, segue do Lema 1.22 que $\mathrm{supp}(\pi_2(S_0)) + \mathrm{supp}(\pi_2(S_1)) = \langle e_2\rangle$, isto é, cada elemento de $\langle e_2\rangle$ é a soma de um elemento de $\pi_2(S_0)$ e um elemento de $\pi_2(S_1)$. Em particular, existem $g_0|S_0$, $g_1|S_1$ tais que $\pi_2(g_0) + \pi_2(g_1) = \pi_2(\sigma(S))$. Considere $S' = S(g_0g_1)^{-1}$. Então

$$\pi_2(\sigma(S')) = \pi_2(\sigma(S)) - (\pi_2(g_0) + \pi_2(g_1)) = 0.$$

Além disso,

$$\pi_1(\sigma(S')) = \pi_1(\sigma(S) - (\pi_1(g_0) + \pi_1(g_1)) = e_1 - e_1 = 0.$$

Assim, $\sigma(S') = 0$ e como $|S| = (2n+2) - 2 = 2n$, S' é a subsequência de S procurada.

Assumindo agora que $\pi_1(\sigma(S)) = 0$, considere $\{x, y\} = \{0, 1\}$ tal que $|S_x| \geqslant |S_y|$. Temos

$$|S_x| \geqslant \frac{2n+2}{2} = n + 1.$$

Além disso, note que se $|S_x| = n+1$, então também $|S_y| = n+1$ e logo $|S_1| = n+1$. Daí, como $n+1$ é ímpar, $\pi_1(\sigma(S)) = |S_1|e_1 = (n+1)e_1 \neq 0$, contrariando o que assumimos. Devemos ter, portanto, $|S_x| \geqslant n+2$. Com isso, $2|\pi_2(S_x)| = 2|S_x| \geqslant 2n + 4 > |\langle e_2\rangle| + 2^{r_2(\langle e_2\rangle)} + 1$ (lembre-se que $r_2(\langle e_2\rangle) = 1$). Daí, podemos aplicar o Lema 1.22 e temos

$$\mathrm{supp}(\pi_2(S_x)) \hat{+} \mathrm{supp}(\pi_2(S_x)) = \langle e_2\rangle.$$

Em particular, existe $gh|S_x$ tal que $\pi_2(g) + \pi_2(h) = \pi_2(\sigma(S))$. Seja $S' = S(gh)^{-1}$ e observe que $\pi_2(\sigma(S')) = \pi_2(\sigma(S)) - (\pi_2(g) + \pi_2(h)) = 0$. Como $|S'| = (2n+2) - 2 = 2n$, S' é a subsequência de S que procuramos e isso conclui a prova. ■

Proposição 4.8. *Seja $n \in \mathbb{N}$. Dada $S \in \mathcal{F}(C_2^2 \oplus C_n)$ livre de quadrados de tamanho $2n+2$, se $\sigma(\pi_1(S)) \neq 0$, onde π_1 é projeção de $C_2^2 \oplus C_n$ sobre C_2^2, então S possui uma subsequência de soma zero de tamanho $2n$.*

Demonstração: Para $n = 1$, não há o que fazer pois a única sequência livre de quadrados de tamanho 4 de $C_2^2 \oplus C_1$ é

$$S = (0,0,0)(1,0,0)(0,1,0)(1,1,0)$$

e $\sigma(\pi_1(S)) = 0$. Assumiremos, então, $n \neq 1$. Escreva

$$C_2^2 \oplus C_n = \langle f_1 \rangle \oplus \langle f_2 \rangle \oplus \langle e \rangle$$

com $\mathrm{ord}(f_1) = \mathrm{ord}(f_2) = 2$ e $\mathrm{ord}(e) = n$. Denote π_2 a projeção de $C_2^2 \oplus C_n$ sobre $\langle e \rangle$. Por simplicidade, escrevemos $\langle f_1 \rangle \oplus \langle f_2 \rangle = \{0, a, b, c\}$ onde 0 é o elemento neutro. Note que, em qualquer caso, $b + c = a$. Agora, escreva $S = S_0 S_a S_b S_c$ onde $\pi_1(g) = x$ para $g|S_x$. Por hipótese $\sigma(\pi_1(S)) = a \neq 0$.

Seja (B_1, B_2) igual a (S_0, S_a) ou (S_b, S_c) de tal forma que

$$|B_1| + |B_2| = \max(|S_0| + |S_a|, |S_b| + |S_c|).$$

Então $|B_1| + |B_2| \geqslant (2n+2)/2 = n+1$. Note que $\pi_2(B_1)$, $\pi_2(B_2)$ são livres de quadrados e assim, $|\mathrm{supp}(\pi_2(B_i))| = |B_i|$ com $i \in \{1, 2\}$. Assim, pelo Lema 1.22, $\mathrm{supp}(\pi_2(B_1)) + \mathrm{supp}(\pi_2(B_2)) = \langle e \rangle$. Tome $g_1|B_1$, $g_2|B_2$ tais que $\pi_2(g_1) + \pi_2(g_2) = \pi_2(\sigma(S))$. Então $\pi_2(\sigma(S(g_1g_2)^{-1})) = 0$ e também $\pi_1(\sigma(S(g_1g_2)^{-1})) = 0$ já que $(\pi_1(g_1), \pi_1(g_2)) = (0, a)$ ou (b, c) pela forma como escolhemos B_1 e B_2.

Assim, $S(g_1g_2)^{-1}$ é uma subsequência de soma zero de S com $|S| = 2n$, como queríamos. ■

Lema 4.9. *Se $G = C_2 \oplus C_4$, então $g_{\pm}(G) = 5$.*

Demonstração: Seja $A = \{-1, 1\}$. Temos $g_{\pm}(C_2 \oplus C_4) \geqslant 5$ por (4.1). Escreva $C_2 \oplus C_4 = \langle e_1 \rangle \oplus \langle e_2 \rangle$, com $\mathrm{ord}(e_1) = 2$ e $\mathrm{ord}(e_2) = 4$. Tome π_1 e π_2 as projeções de $C_2 \oplus C_4$ em $\langle e_1 \rangle$ e $\langle e_2 \rangle$, respectivamente. Seja $S \in \mathcal{F}(C_2 \oplus C_4)$ livre de quadrados com $|S| = 5$ e escreva $S = S_0 S_1$ onde $\pi_1(g) = 0$ para $g|S_0$ e $\pi_1(g) = e_1$ para $g|S_1$. Seja $\{x, y\} = \{0, 1\}$ tal que $|S_x| \geqslant |S_y|$. Se tivermos $|S_x| \geqslant 4$, então pelo Teorema 4.5 obtemos que $\pi_2(S_x)$, que é uma sequência livre de quadrados sobre C_4, possui uma subsequência de A-soma zero de tamanho 4. Como para cada subsequência T de tamanho 4 de S_x, $\pi_1(\sigma_{\pm}(T)) = \{0\}$, já que a projeção via π_1 fornece as sequências constantes 0^4 ou e_1^4, ambas com soma A-ponderada igual a zero independentemente da escolha de sinais (lembre-se que $\mathrm{ord}(e_1) = 2$), as subsequências de A-soma zero de tamanho 4 de $\pi_2(S_x)$ fornecem, de fato, uma subsequência de A-soma zero de tamanho 4 de S_x e, portanto, de S.

Assim, falta considerar $|S_x| = 3$, $|S_y| = 2$. Note que, neste caso, $\pi_2(\sigma_{\pm}(S_y))$ possui um elemento não nulo de $\langle e_2 \rangle$, uma vez que S (e, portanto, S_y) é livre de quadrados. Digamos, $a \in \pi_2(\sigma_\pm(S_y)) \cap (\langle e_2\rangle \setminus \{0\})$. Além disso, $\pi_2(\Sigma_{\pm,2}(S_x))$ contém $\langle e_2\rangle \setminus \{0\}$. Para ver isso, observe que $\pi_2(S_x)$ é um dos seguintes conjuntos:

$$\{0, e_2, 2e_2\},\ \{0, 2e_2, 3e_2\},\ \{0, e_2, 3e_2\} \text{ ou } \{e_2, 2e_2, 3e_2\}$$

e é fácil ver que para qualquer um dos conjuntos anteriores, $\Sigma_{\pm,2}(\pi_2(S_x))$ contém $\langle e_2\rangle \setminus \{0\}$. Em particular, $a \in \Sigma_{\pm,2}(\pi_2(S_x))$ e assim, obtemos a subsequência de A-soma zero de tamanho 4 desejada. ■

Teorema 4.10. *Dado $n \in \mathbb{N}$, temos*

$$g_\pm(C_2 \oplus C_{2n}) = \begin{cases} 5, & se\ n = 1, 2 \\ 2n+2 & se\ n \geqslant 3 \end{cases}.$$

Demonstração: Para $n = 1$, temos $g_\pm(C_2 \oplus C_2) = 5$ pelo Lema 4.1 e para $n = 2$, o resultado segue do Lema 4.9. Quando $n \geqslant 3$, temos $g_\pm(C_2 \oplus C_{2n}) \geqslant 2n+2$ pelo Lema 4.6 e, se além disso n for par, $g_\pm(C_2 \oplus C_{2n}) \leqslant 2n+2$ pela Proposição 4.7. Assim, basta mostrar que $g_\pm(C_2 \oplus C_{2n}) \leqslant 2n+2$ quando $n \geqslant 3$ e n é ímpar.

Seja $A = \{-1, 1\}$ e assuma $n \geqslant 3$ ímpar. Neste caso, podemos escrever $C_2 \oplus C_{2n} = \langle f_1\rangle \oplus \langle f_2\rangle \oplus \langle e\rangle$ com $\mathrm{o}(f_1) = \mathrm{o}(f_2) = 2$ e $\mathrm{o}(e) = n$. Sejam π_1 e π_2 as projeções de $C_2 \oplus C_{2n}$ sobre $\langle f_1\rangle \oplus \langle f_2\rangle$ e $\langle e\rangle$, respectivamente. Seja $S \in \mathcal{F}(C_2 \oplus C_{2n})$ livre de quadrados de tamanho $2n+2$. Denote $\langle f_1\rangle \oplus \langle f_2\rangle = \{0, a, b, c\}$ e note que $b + c = a$. Agora escreva $S = S_0S_aS_bS_c$ onde $\pi_1(g) = x$ para $g|S_x$. Temos dois casos a considerar, a saber, $\pi_1(\sigma(S)) \neq 0$ e $\pi_1(\sigma(S)) = 0$. Se $\pi_1(\sigma(S)) \neq 0$, a existência de uma subsequência de A-soma zero de S segue diretamente da Proposição 4.8.

Suponha então que $\pi_1(\sigma(S)) = 0$ e seja $x \in \{0, a, b, c\}$ tal que $|S_x|$ é o maior possível. Note que, neste caso,

$$|S_x| \geqslant \frac{2n+2}{4} = \frac{n+1}{2}.$$

Se existe $gh|S_x$ tal que $\pi_2(g)+\pi_2(h) = \pi_2(\sigma(S))$, temos $S(gh)^{-1}$ subsequência de soma zero de tamanho $2n$, uma vez que $\sigma(\pi_2(S(gh)^{-1})) = 0$ por construção e como $\pi_1(g) = \pi_1(h) = x \in \langle f_1\rangle \oplus \langle f_2\rangle$ temos $\mathrm{o}(\pi_1(g)) = \mathrm{o}(\pi_1(h)) = 2$, temos

$$\sigma(\pi_1(S(gh)^{-1})) = \sigma(\pi_1(S)) - \pi_1(g) - \pi_1(h) = 0 - 2\pi_1(g) = 0.$$

Se gh com a propriedade dita acima não existe, pelo Lema 1.22 devemos ter $|S_x| = (n+1)/2$ e assim $|S_y| = (n+1)/2$ para cada $y \in \{0, a, b, c\}$. De fato, se $|S_x| > (n+1)/2$ então $|\pi_2(S_x)| > (n+1)/2$ e logo

$$|\pi_2(S_x)| + |\pi_2(S_x)| > n+1 > n = |\langle e\rangle|.$$

Assim, pelo item *(a)* do Lema 1.22, temos $\pi_2(S_x)+\pi_2(S_x) = \langle e\rangle$ e como $\pi_2(\sigma(S)) \in \langle e\rangle$, devem existir $\pi_2(g), \pi_2(h) \in \pi_2(S_x)$ com $\pi_2(g)+\pi_2(h) = \pi_2(\sigma(S))$, o que estamos assumindo que não acontece (lembre-se que não há problema em considerar S_x um conjunto, já que S é livre de quadrados).

Observe que $\pi_1(\sigma_\pm(S(gh)^{-1})) = \{0\}$ qualquer que seja a sequência de dois elementos $gh|S_0$. Vamos mostrar que $\pi_2(\sigma_\pm(S(gh)^{-1})) = \langle e\rangle$ e isso completa a prova, pois $0 \in \langle e \rangle$ e logo teremos $0 \in \sigma_{\pm}(S(gh)^{-1})$, ou seja, $S(gh)^{-1}$ é subsequência de A-soma zero de S de tamanho $2n$. Observe que, como $S_a S_b | S(gh)^{-1}$, temos

$$|\sigma_{\pm}(\pi_2(S(gh)^{-1}))| \geqslant |\sigma_{\pm}(\pi_2(S_a S_b))| = |\sigma_{\pm}(\pi_2(S_a)) + \sigma_{\pm}(\pi_2(S_b))|.$$

Além disso, pelo Lema 4.3,

$$|\sigma_{\pm}(\pi_2(S_a))| = |\Sigma^0(\pi_2(S_a))| \geqslant |\pi_2(S_a)| = |S_a| = (n+1)/2$$

e

$$|\sigma_{\pm}(\pi_2(S_b))| = |\Sigma^0(\pi_2(S_b))| \geqslant |\pi_2(S_b)| = |S_b| = (n+1)/2.$$

Com isso, podemos aplicar o Lema 1.22 a $\sigma_{\pm}(\pi_2(S_a))$ e $\sigma_{\pm}(\pi_2(S_b))$ e obtemos

$$\sigma_{\pm}(\pi_2(S_a)) + \sigma_{\pm}(\pi_2(S_b)) = \langle e \rangle.$$

Assim $|\sigma_{\pm}(\pi_2(S(gh)^{-1}))| = n$ e isso mostra que $\pi_2(\sigma_{\pm}(S(gh)^{-1})) = \langle e \rangle$. ∎

Capítulo 5

Relação entre s_A e η_A com $A = \{-1, 1\}$

Seja G um grupo abeliano finito com $\exp(G) = n$. Em 2003, W. D. Gao conjecturou, em [8], que

$$s(G) = \eta(G) + n - 1$$

e provou que é verdade para grupos com $n \in \{2, 3, 4\}$. Até hoje não existem contraexemplos que invalidem a conjectura, bem como não existe uma prova de sua veracidade.

Dado $A \subseteq [1, n-1]$, da definição de $\eta_A(G)$, existe uma sequência $S \in \mathcal{F}(G)$ com $|S| = \eta_A(G) - 1$ tal que S não possui subsequência não trivial de A-soma zero e de tamanho no máximo n. Daí,

$$S' = S0^{n-1}$$

é tal que S' não possui subsequência de A-soma zero de tamanho n, uma vez que uma subsequência de A-soma zero de S' de tamanho n implica em uma subsequência de A-soma zero de S de algum tamanho menor ou igual a n. Isso nos diz que

$$s_A(G) \geqslant \eta_A(G) + \exp(G) - 1. \tag{5.1}$$

Neste capítulo, nos dispomos a estudar a generalização

$$s_A(G) = \eta_A(G) + \exp(G) - 1 \tag{5.2}$$

com $A = \{-1, 1\}$. Nosso principal objetivo é verificar a veracidade da generalização para todos os grupos abelianos de ordem 8, 16 e 32, bem como para grupos da forma $G = C_2 \oplus C_{2n}$, com $n \in \mathbb{N}$. Antes disso, apresentamos a prova de que esta generalização não é válida quando $G = C_3^r$ com $r \geqslant 3$ e $G = C_n^2$ para $n > 7$ ímpar. Nosso trabalho aqui se baseia nas referências [5, 10, 20, 22].

5.1 Exemplos para os quais não vale a relação

5.1.1 Caso $G = C_3^r$ com $r \geqslant 3$

Um exemplo para o qual (5.2) não se verifica, foi determinado por H. Godinho, A. Lemos e D. Marques, em [10], quando $G = C_3^r$ onde $r \geqslant 2 = 3$, como veremos a seguir.

Teorema 5.1. *Seja n um inteiro positivo ímpar. Então $s_{\pm}(C_n^2) = 2n - 1$.*

Demonstração: Primeiramente, vamos demonstrar o teorema para o caso $n = p$ primo.

Sejam $m = 2p - 1$ e $S = v_1 v_2 \cdots v_m \in \mathcal{F}(C_p^2)$, ou seja,

$$v_i = (a_i, b_i),\ a_i, b_i \in C_p\ \forall\ i \in [1, m].$$

Considere o sistema abaixo:

$$\begin{cases} \displaystyle\sum_{i=1}^{2p-1} a_i x_i^{\frac{p-1}{2}} = 0 \\ \displaystyle\sum_{i=1}^{2p-1} b_i x_i^{\frac{p-1}{2}} = 0 \\ \displaystyle\sum_{i=1}^{2p-1} x_i^{p-1} = 0 \end{cases}.$$

Observe que $2(p-1) = 2p-2 < 2p-1$. Com isso, o Teorema 1.20 nos garante que existe uma solução não nula para o sistema.

Seja $(c_1, \ldots, c_m)$ a solução não trivial e tome $J \in [1, m]$ o conjunto dos índices das entradas não nulas da solução.

Aplicando essa solução nas duas primeiras equações, obtemos:

$$\sum_{i \in J} q_i v_i \equiv (0, 0) \pmod p \qquad\qquad q_i \in \{1, -1\}$$

pois $\left(x_i^{\frac{p-1}{2}}\right)^2 \equiv x_i^{p-1} \equiv 1 \pmod p$, pelo teorema de Euler-Fermat.

Agora, da terceira equação obtemos que $|J| = p$. Daí, renomeando esses índices, obtemos:

$$\sum_{i=1}^{p} q_i v_i \equiv (0, 0) \pmod p$$

e encontramos a subsequência procurada. Isso mostra que $s_{\pm}(C_p^2) \leqslant 2p - 1$.

Por outro lado, se considerarmos uma sequência com $2p - 2$ elementos de C_p^2 onde cada um dos elementos $(0, 1)$ e $(1, 0)$ é repetido $p - 1$ vezes. É fácil ver que é impossível obter uma subsequência de p elementos cuja soma é $(0, 0)$ módulo p e isso prova o teorema quando p é primo.

Agora, quando $n > 1$ é um inteiro qualquer, usamos o mesmo argumento desenvolvido na demonstração do Teorema 1.27. ■

Lema 5.2. *Seja $G = C_3^r$, onde $r \in \mathbb{N}$. Temos* *(a) Se $r = 1$, então $\eta_{\pm}(G) = 2$, $g_{\pm}(G) = 3$ e $s_{\pm}(G) = 4$;*

(b) $\eta_{\pm}(G) \geqslant r + 1$.

Demonstração: Seja $A = \{-1, 1\}$. Para o item *(a)*, temos $g_{\pm}(C_3) = 3$ pelo Teorema 4.5 e $s_{\pm}(C_3) = 3 + \lfloor \log_2 3 \rfloor = 3 + 1 = 4$ pelo Teorema 2.17. Para ver que $\eta_{\pm}(G) = 2$, escreva $C_3 = \langle f \rangle$ e considere $S = a_1 a_2 \in \mathcal{F}(C_3)$. Se $0 \in \text{supp}(S)$, então S possui uma subsequência de A-soma zero. Se $0 \notin \text{supp}(S)$, então $S = f(2f)$ e $\sigma(S) = 3f = 0$, ou seja, S é uma sequência de A-soma zero e isso mostra que $\eta_{\pm}(C_3) \leqslant 2$. A igualdade é obtida observando-se que a sequência unitária $S = f$ não é de A-soma zero.

O item *(b)* segue do fato de que a sequência $S = e_1 e_2 \cdots e_r$ com $e_j = (0, \ldots, 1, \ldots, 0)$ com o 1 aparecendo na j-ésima coordenada não possui subsequência não trivial de A-soma zero. ∎

Proposição 5.3. *Dado $r \in \mathbb{N}$, temos $g_{\pm}(C_3^r) = 2\eta_{\pm}(C_3^r) - 1$.*

Demonstração: Seja $A = \{-1, 1\}$. Se $r = 1$, então pelo Lema 5.2 $g_{\pm}(C_3) = 3 = 2 \cdot 2 - 1 = 2\eta_{\pm}(C_3) - 1$. Assuma então $r \geqslant 2$ e seja $S = g_1 \cdots g_m \in \mathcal{F}(C_3^r)$ com $m = \eta_{\pm}(C_3^r) - 1$ e tal que S não possua subsequência de A-soma zero de nenhum tamanho. Em particular, S é livre de quadrados e $0 \notin \text{supp}(S)$. Considere

$$S^* = \prod_{i=1}^{m} g_i \prod_{i=1}^{m} (-g_i)$$

e observe que $|S^*| = 2m$, S^* é livre de quadrados e não possui subsequência de A-soma zero de tamanho $\exp(C_3^r) = 3$, uma vez que uma subsequência de A-soma zero em S^* nos fornece uma subsequência de A-soma zero em S ou que $0 \in \text{supp}(S)$, ambas conclusões contrárias ao que supomos. Isso mostra que $g_{\pm}(C_3^r) \geqslant 2m + 1 = 2\eta_{\pm}(C_3^r) - 1$.

Para obter a igualdade, considere $S = g_1 \cdots g_m \in \mathcal{F}(C_3^r)$ livre de quadrados com $m = 2\eta_{\pm}(C_3^r) - 1$ e reordene os elementos de S de forma que

$$S = \prod_{i=1}^{t} g_i \prod_{i=1}^{t} (-g_i) \prod_{i=2t+1}^{m} g_i$$

onde $g_i \neq g_j$ para $2t + 1 \leqslant i < j \leqslant m$. Se $t = 0$, então S não possui subsequência de A-soma zero de tamanho 2. Seja $S^* | S$ formada por todos os elementos diferentes de 0 de S. Como S é livre de quadrados, $|S^*| \geqslant m - 1 = 2\eta_{\pm}(C_3^r) - 2 > \eta_{\pm}(C_3^r)$ quando $r \geqslant 2$ pelo Lema 5.2 *(b)*. Assim, S^* possui uma subsequência de A-soma zero de tamanho 3, já que $0 \notin \text{supp}(S^*)$ e se $T | S^*$ então $T | S$ e S não possui subsequência de A-soma zero de tamanho 2. Isso mostra que S possui uma subsequência de A-soma zero de tamanho 3.

Se $t \geqslant 1$ e $g_j = 0$ para algum $j \in [2t+1, m]$, então $g_t(-g_t)g_j$ é uma subsequência de A-soma zero de S. Vamos assumir então $g_j \neq 0$ para todo $j \in [2t + 1, m]$. Se $t \geqslant \eta_{\pm}(C_3^r)$, então $\prod_{i=1}^{t} g_i$ possui uma subsequência T de A-soma zero e como S é livre de quadrados, $|T| = 3$. Se $t < \eta_{\pm}(C_3^r)$, então $m - t \geqslant \eta_{\pm}(C_3^r)$ e $\prod_{i=1}^{t} (-g_i) \prod_{i=2t+1}^{m} g_i$ possui uma subsequência de A-soma zero de tamanho 3.

Em qualquer caso, obtemos uma subsequência de S de A-soma zero de tamanho 3 e isso mostra que $g_\pm(C_3^r) = 2\eta_\pm(C_3^r) - 1$. ■

Da definição de s_A e g_A, temos

$$s_A(G) \geqslant g_A(G) \tag{5.3}$$

para todo G aditivo abeliano finito e para todo $A \subseteq [1, \exp(G)-1]$. A proposição a seguir nos dá um exemplo de quando a igualdade é satisfeita.

Proposição 5.4. *Se $r \geqslant 2$, então $g_\pm(C_3^r) = s_\pm(C_3^r)$.*

Demonstração: Seja $A = \{-1, 1\}$. Por (5.3), basta mostrar que $g_\pm(C_3^r) \geqslant s_\pm(C_3^r)$. Se $r = 2$, então $s_\pm(C_3^2) = 5$ pelo Teorema 5.1. Por outro lado, a sequência $(1,0)(0,1)(2,0)(0,2) \in \mathcal{F}(C_3^2)$ é livre de quadrados e não possui subsequência de A-soma zero de tamanho 3. Isso mostra que $5 = s_\pm(C_3^r) \geqslant g_\pm(C_3^r) \geqslant 5$.

Suponha então $r \geqslant 3$ e seja $S = g_1 \cdots g_m \in \mathcal{F}(C_3^r)$ com $m = s_\pm(C_3^r) - 1$, tal que S não possui subsequência de A-soma zero de tamanho 3. Em particular, S não pode conter três elementos iguais já que $\exp(C_3^r) = 3$. Se S é livre de quadrados então $g_\pm(C_3^r) > m$, ou seja, $g_\pm(C_3^r) \geqslant s_\pm(C_3^r)$.

Suponha então que S não é livre de quadrados e vamos reindexar a sequência de forma que

$$S = \prod_{i=1}^{t} g_i^2 \prod_{j=2t+1}^{m} g_j$$

onde $g_1, \ldots, g_t, g_{2t+1}, \ldots, g_m$ são todos distintos. Observe que se $g_j = 0$ para algum $j \in [1, m]$, então a subsequência S^* formada por todos os elementos não nulos de S é tal que

$$|S^*| \geqslant s_\pm(C_3^r) - 3 = 2\eta_\pm(C_3^r) - 4 \geqslant \eta_\pm(C_3^r)$$

quando $r \geqslant 3$ pela Proposição 5.3 e pelo Lema 5.2 *(b)*. Isso quer dizer que S^* possui uma subsequência T de A-soma zero de tamanho 2 ou 3. Se $|T| = 2$, então $g_j T$ é subsequência de A-soma zero de S de tamanho 3, contrariando o que assumimos sobre S. Devemos ter, portanto, $g_j \neq 0$ para todo $j \in [1, m]$. Note que, neste caso, se existem $i \in [1, t]$, $j \in [2t+1, m]$ tais que $g_j = -g_i$, então $g_i^2 g_j$ é subsequência de A-soma zero de S ($g_i + g_i - g_j = 3g_i = 0$). Portanto, a sequência

$$R = \prod_{i=1}^{t} g_i \prod_{i=1}^{t} (-g_i) \prod_{i=2t+1}^{m} g_i$$

é livre de quadrados com $|R| = s_\pm(C_3^r) - 1$ e R não possui subsequência de A-soma zero por construção. Isso mostra que $g_\pm(C_3^r) \geqslant s_\pm(C_3^r)$. ■

Pelas Proposições 5.3 e 5.4 e pelo Lema 5.2, quando $r \geqslant 3$

$$\begin{aligned} s_\pm(C_3^r) &= g_\pm(C_3^r) = 2\eta_\pm(C_3^r) - 1 \\ &= \eta_\pm(C_3^r) + \eta_\pm(C_3^r) - 1 \\ &\geqslant \eta_\pm(C_3^r) + r + 1 - 1 \\ &> \eta_\pm(C_3^r) + \exp(C_3^r) - 1 \end{aligned}$$

e a relação (5.2) não se verifica para $G = C_3^r$.

5.1.2 Caso $G = C_n^2$, com $n \geqslant 7$ ímpar

Este exemplo é um dos resultados do trabalho de B. Moriya, em [22].

Teorema 5.5. *Seja n um inteiro positivo ímpar. Então $\eta_{\pm}(C_n^2) \leqslant n$.*

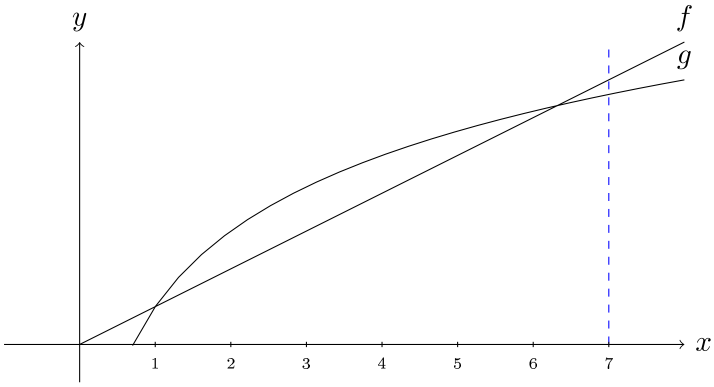
Demonstração: Seja $G = C_n^2$. Suponha $n = p$ primo e seja $S = (a_1, b_1) \cdots (a_p, b_p)$ sequência de elementos de G de tamanho p. Considere o sistema abaixo:

$$\begin{cases} \sum_{i=1}^{p} a_i x_i^{\frac{p-1}{2}} = 0 \\ \sum_{i=1}^{p} b_i x_i^{\frac{p-1}{2}} = 0 \end{cases}.$$

Como as equações do sistema não possuem termo independente, seque que $(0, 0, \ldots, 0) \in C_p^p$ é solução do sistema. Além disso, como $2\left(\frac{p-1}{2}\right) = p - 1 < p$, podemos aplicar o Teorema 1.20 que nos garante que existe uma solução não nula para este sistema. Pelo Teorema de Fermat, essa solução nos fornece uma subsequência de soma zero de tamanho menor ou igual a p de S e o resultado está provado.

Se $n > 1$ é um inteiro ímpar qualquer, usamos um argumento de indução sobre n análogo ao que fizemos na demonstração do Teorema 5.1. ∎

Observação 5.6. Temos $\log_2 n^2 + 1 < n$ para todo $n \in \mathbb{N}_{\geqslant 7}$. Isso pode ser visto simplesmente observando-se a o comportamento das funções $f(x) = x$ e $g(x) = \log_2 x^2 + 1$, conforme o gráfico a seguir:



Agora, seja $A = \{-1, 1\}$ e considere $G = C_n^2$ com n inteiro positivo. Note que $\exp(G) = n$ e pelo Corolário 2.2 *(a)*, toda sequência de elementos de G de tamanho maior ou igual a $\lfloor \log_2 |G| \rfloor + 1 = \lfloor \log_2 n^2 \rfloor + 1$ possui uma subsequência de A-soma zero, não trivial, de tamanho no máximo $\lfloor \log_2 |G| \rfloor + 1$. Quando $n \geqslant 7$, de acordo com o gráfico acima, temos $\lfloor \log_2 n^2 \rfloor + 1 \leqslant n$ e logo

$$n_{\pm}(G) \leqslant \lfloor \log_2 |G| \rfloor + 1 = \lfloor \log_2 n^2 \rfloor + 1 \leqslant \log_2 n^2 + 1 < n.$$

Como, pelo Teorema 5.1, $s_\pm(G) = 2n - 1$ sempre que n é ímpar, temos

$$\eta_\pm(G) + \exp(G) - 1 < 2n - 1 = s_\pm(G)$$

e assim a relação (5.2) não se verifica para $G = C_n^2$ com n ímpar maior ou igual a 7.

No entanto, quando $n = 3, 5$, (5.2) é satisfeita. De fato, quando $G = C_3^2$, o teorema anterior nos diz que $\eta_\pm(G) \leqslant 3$ e a sequência $(1, 0)(0, 1)$ é um exemplo de sequência que não possui subsequência de soma zero, nos permitindo concluir que $\eta_\pm(G) = 3$ e

$$\eta_\pm(G) + \exp(G) - 1 = 6 - 1 = 5 = s_\pm(G)$$

pelo Teorema 5.1. Para $G = C_5^2$, temos $\eta_\pm(G) \leqslant 5$ pelo teorema anterior e a sequência $(1, 0)(2, 0)(0, 1)(0, 2)$ não possui subsequência de soma zero, o que nos leva a concluir que $\eta_\pm(G) = 5$ e $\eta_\pm(G) + \exp(G) - 1 = 9 = s_\pm(G)$. Na próxima seção, vamos conhecer mais exemplos para os quais (5.2) é satisfeita.

5.2 Exemplos para os quais vale a relação

5.2.1 Caso G de ordem 8 e 16

Devido às restrições impostas pela definição de cada constante, é fácil ver que

$$D_\pm(G) \leqslant \eta_\pm(G) \leqslant s_\pm(G). \tag{5.4}$$

O lema abaixo nos dá uma condição para que possamos obter a igualdade $D_\pm(G) = \eta_\pm(G)$.

Lema 5.7. *Se $|G|$ é potência de 2 e $\log_2 |G| \leqslant \exp(G)$, então $D_\pm(G) = \eta_\pm(G)$. Em particular, se $G = C_{2^l}^r$ com $l > 1$ satisfazendo $rl \leqslant 2^l$, temos*

$$D_\pm(G) = \eta_\pm(G) = rl + 1. \tag{5.5}$$

Demonstração: Seja $A = \{-1, 1\}$. Como observamos logo após a demonstração do Teorema 3.1, quando $|G|$ é potência de 2, temos $D_\pm(G) = \log_2 |G| + 1$. Agora, pelo Teorema 2.1, é claro que se S é sequência de G de tamanho $D_\pm(G)$, então S possui uma subsequência de A-soma zero de tamanho estritamente menor que $D_\pm(G) \leqslant \exp(G) + 1$, ou seja, $D_\pm(G) \geqslant \eta_\pm(G)$. A desigualdade contrária segue de (5.4).

Em particular, se $G = C_{2^l}^r$ com $l > 1$ tal que $rl \leqslant 2^l$, temos $|G| = 2^{rl}$ potência de 2 e

$$\log_2 |G| + 1 = \log_2 2^{rl} + 1 = rl + 1 \leqslant 2^l + 1 = \exp(G) + 1.$$

Assim,

$$D_\pm(G) = \eta_\pm(G) = rl + 1.$$

∎

Isso nos será útil na demonstração do teorema que segue.

O lema abaixo contém algumas propriedades dos números naturais que usaremos na demonstração próximo teorema:

Lema 5.8. *Sejam l, n inteiros positivos, $n \geqslant 2$. Então:*

(a) $2l \leqslant 2^l$;

(b) $l + 1 \leqslant 2^{l-1}n$;

(c) $2l + 1 \leqslant 2^{l+1}$;

(d) $2l + 1 \leqslant 2^{l-1}n$ *quando* $n > 2$;

(e) $3l + 1 \leqslant 2^{l+1}$.

Demonstração:

(a) Indução sobre l: Se l, temos $2^l = 2 = 2 \cdot l$.

Suponha que para $l = k \geqslant 1$ seja verdade que $2k \leqslant 2^k$. Para $l = k + 1$, temos $2^{k+1} = 2 \cdot 2^k \geqslant 2 \cdot 2k = 2k + 2k \geqslant 2k + 2 = 2(k + 1)$. Assim, pelo Princípio de Indução Finita, $2l \leqslant 2^l$ para qualquer l inteiro positivo.

(b) Note que $l + 1 \leqslant l + l = 2l$. Pelo item anterior, $l + 1 \leqslant 2l \leqslant 2^l$ e $2^l = 2 \cdot 2^{l-1} \leqslant 2^{l-1}n$ já que $n \geqslant 2$. Isso mostra que $l + 1 \leqslant 2^{l-1}n$.

(c) Temos $2l + 1 \leqslant 2l + 2 = 2(l + 1) \leqslant 2^{l+1}$ pelo item *(a)*.

(d) Fixe $n > 2$. Vamos usar indução sobre l: Se l, temos $2l + 1 = 3$ e $2^{l-1}n = n \geqslant 3$.

Suponha que para $l = k \geqslant 1$ seja verdade que $2k+1 \leqslant 2^{k-1}n$. Para $l = k+1$, temos $2(k+1)+1 = 2k+1+2 \leqslant 2^{k-1}n+2 < 2^{k-1}n+2^{k-1}n = 2^k n$. Assim, pelo Princípio de Indução Finita, $2l + 1 \leqslant 2^{l-1}n$ para qualquer l inteiro positivo e $n > 2$.

(e) Vamos usar indução sobre l: Se l, temos $3l + 1 = 4 = 2^{l+1}$.

Suponha que para $l = k \geqslant 1$ seja verdade que $3k+1 \leqslant 2^{k+1}n$. Para $l = k+1$, temos $3(k+1)+1 = 2k+1+3 \leqslant 2^{k+1}+3 < 2^{k+1}+2^{k+1} = 2^{k+2} = 2^{(k+1)+1}$. Assim, pelo Princípio de Indução Finita, $3l + 1 \leqslant 2^{l+1}$ para qualquer l inteiro positivo.

■

Teorema 5.9. *Dados l, n inteiros positivos, temos os seguintes resultados:*

(a) *Se* $2^l n \geqslant 4$, *então* $\eta_\pm(C_{2^l} \oplus C_{2^l n}) = D_\pm(C_{2^l} \oplus C_{2^l n}) = \lfloor \log_2 2^l n \rfloor + l + 1$;

(b) *Se* $n \geqslant 2$, *então* $\eta_\pm(C_{2^l} \oplus C_{2^l} \oplus C_{2^l n}) = D_\pm(C_{2^l} \oplus C_{2^l} \oplus C_{2^l n}) = \lfloor \log_2 2^l n \rfloor + 2^l + 1$.

Demonstração: *(a)* Seja $G = C_{2^l} \oplus C_{2^l n}$. Se $n = 1$, então $G = C_{2^l} \oplus C_{2^l}$ tem ordem potência de 2 e

$$\lfloor \log_2 |G| \rfloor + 1 = \lfloor \log_2 2^{2l} \rfloor + 1 = 2l + 1 \leqslant 2^l + 1$$

pelo Lema 5.8 *(a)*. Daí, pelo Lema 5.7, $D_\pm(G) = \eta_\pm(G) = 2l+1 = \lfloor \log_2 2^l \rfloor + l + 1$.

Se $n = 2$, então $G = C_{2^l} \oplus C_{2^{l+1}}$. Novamente, G é potência de 2 e $\lfloor \log_2 |G| \rfloor + 1 = \lfloor \log_2 2^{2l+1} \rfloor + 1 = 2l + 2 \leqslant 2^{l+1} + 1$ pelo Lema 5.8 *(c)* e o resultado segue do Lema 5.7.

Suponha agora $n > 2$. Pelo Teorema 3.1, $D_\pm(G) = \lfloor \log_2 2^l n \rfloor + l + 1$. (os limites inferior e superior coincidem nesse caso). Assim, pelo Lema 5.7, basta mostrar que $\lfloor \log_2 |G| \rfloor + 1 \leqslant 2^l n$.

Escreva $k = \lfloor \log_2 2^l n \rfloor$. Novamente, pelo item *(a)* do Lema 5.8, temos $2^l n = 2 \cdot 2^{l-1} n \leqslant 2^{2^{l-1} n}$ (e portanto $k = \lfloor \log_2 2^l n \rfloor \leqslant \log_2 2^l n \leqslant \log_2 2^{2^{l-1} n} = 2^{l-1} n$) e $l + 1 \leqslant 2^{l-1} n$, respectivamente. Assim,

$$\begin{aligned} \lfloor \log_2 |G| \rfloor + 1 &= \lfloor \log_2 2^l n \rfloor + l + 1 \\ &= k + l + 1 \leqslant 2^{l-1} n + 2^{l-1} n \\ &= 2^l n \end{aligned}$$

como queríamos. A última desigualdade segue do Lema 5.8 *(c)*.

(b) Seja $G = C_{2^l} \oplus C_{2^l} \oplus C_{2^l n}$. Se $n = 2$, então G é potência de 2 e $\lfloor \log_2 |G| \rfloor + 1 = \lfloor \log_2 2^l n \rfloor + 2l + 1 = 3l + 2 \leqslant 2^{l+1} + 1$ pelo Lema 5.8 *(e)*. Pelo Lema 5.7,

$$D_\pm(G) = \eta_\pm(G) = \lfloor \log_2 |G| \rfloor + 1 = \lfloor \log_2 2^l n \rfloor + 2l + 1.$$

Suponha então $n > 2$ e escreva $k = \lfloor \log_2 2^l n \rfloor$. Neste caso, o Teorema 3.1 nos garante que $D_\pm(G) = \lfloor \log_2 |G| \rfloor + 1 = \lfloor \log_2 2^l n \rfloor + 2l + 1 = k + 2l + 1$. Assim, basta mostrar que $k + 2l + 1 < 2^l n$ e o resultado seguirá do Lema 5.7. Da demonstração do item anterior, $k \leqslant 2^{l-1} n$ e como $n > 2$, temos $2l + 1 \leqslant 2^{l-1} n$ (item *(d)*, Lema 5.8). Assim, $k + 2l + 1 \leqslant 2^{l-1} n + 2^{l-1} n = 2^l n$, como queríamos. ∎

Lema 5.10. *Se G é 2-grupo elementar, então $s(G) = |G| + 1$ e $\eta(G) = |G|$.*

Demonstração: Para mostrar que $s(G) = |G| + 1$, como $\exp(G) = 2$, dada $S \in \mathcal{F}(G)$, queremos garantir a existência de uma subsequência de soma zero de S de tamanho 2. Observe que a subsequência procurada deve conter, necessariamente, elementos repetidos. O menor tamanho de S para o qual podemos garantir isso é $|G| + 1$.

Agora, dada $S \in \mathcal{F}(G)$, se queremos uma subsequência de tamanho no máximo 2, isso quer dizer que $0 \in S$ ou algum elemento de G aparece em S duas vezes. O menor tamanho de S para o qual podemos garantir isso é $|G|$ e isso mostra que $\eta(G) = |G|$. ∎

Apresentaremos, agora, a prova do principal teorema da seção, que verifica a relação (5.2) para todos os grupos abelianos finitos de ordem 8 e 16.

Teorema 5.11. *As seguintes afirmações são verdadeiras:*

(a) $\eta_\pm(C_2 \oplus C_4) = 4$ *e* $s_\pm(C_2 \oplus C_4) = \eta_\pm(C_2 \oplus C_4) + 4 - 1 = 7$. *Temos* $s_\pm(G) = \eta_\pm(G) + \exp(G) - 1$ *para todo grupo abeliano G de ordem 8.*

(b) Se G é um grupo abeliano de ordem 16 com $\exp(G) \geqslant 4$, *então* $\eta_{\pm}(G) = 5$ *e* $s_{\pm}(G) = 12$ *ou* 8, *dependendo se* $\exp(G) = 8$ *ou* 4. *Concluímos que* $s_{\pm}(G) = \eta_{\pm}(G) + \exp(G) - 1$ *para todo grupo abeliano de ordem* 16.

Demonstração: *(a)* Sejam $A = \{-1, 1\}$ e $G = C_2 \oplus C_4$. Como $\lfloor \log_2 |G| \rfloor + 1 = 4 = \exp(G)$, pelo Teorema 2.1, $\eta_{\pm}(G) \leqslant \lfloor \log_2 |G| \rfloor + 1 = 4$ e $(0,1)(0,2)(1,0)$ é um exemplo de sequência de elementos de G sem subsequência de A-soma zero de tamanho menor ou igual a 4. Isso mostra que $\eta_{\pm}(G) = 4$.

Vamos mostrar que $s_{\pm}(G) = 7$. Seja $S = \prod_{i=1}^{7} x_i$ uma sequência de elementos de G de tamanho 7. Se $h(S) = 1$, não temos o que fazer. De fato, note que como $|G| = 8$, todos os elementos de G aparecem em S, exceto um. Daí, uma dessas duas sequências com certeza é subsequência de S: $(1,3)(1,1)(0,3)(0,1)$ ou $(0,0)(0,2)(1,0)(1,2)$, ambas de A-soma zero.

Se $h(S) \geqslant 2$, existe $x_i \in S$ que aparece mais de uma vez em S e x_i^2 é uma subsequência de soma zero de S de tamanho 2. Reordenando os elementos de S, ponha $i = 1$ e escreva $S = x_1^2 x_2 \cdots x_6$. Como o número de subconjuntos de $\{2,3,4,5,6\}$ de dois elementos é $10 > 8$, devemos ter $x_i + x_j = x_j + x_k$ ou $x_i + x_j = x_k + x_l$ para elementos distintos $i, j, k, l \in \{2,3,4,5,6\}$. No primeiro caso, temos $x_i = x_j$ o que nos dá uma subsequência $x_1^2 x_i x_j$ de A-soma zero de S de tamanho 4 (lembre-se: quando $A = \{-1, 1\}$, elementos que se repetem em S fornecem trivialmente uma subsequência de A-soma zero de tamanho 2). No segundo caso, $x_i x_j x_k x_l$ é uma subsequência de A-soma zero de S de tamanho 4. Assim, em qualquer caso, obtemos uma subsequência de A-soma zero de S de tamanho 4. Isso nos permite concluir que $s_{\pm}(G) \leqslant 7$.

Agora, de (5.1), temos

$$7 \geqslant s_{\pm}(G) \geqslant \eta_{\pm}(G) + \exp(G) - 1 = 4 + 4 - 1 = 7$$

e obtemos a igualdade procurada.

Se $G = C_8$, temos $s_{\pm}(G) = 8 + \lfloor \log_2 8 \rfloor = 8 + 3 = 11$ pelo Teorema 2.17, $n_{\pm}(G) = 4$ pelo Lema 5.7 e logo $s_{\pm}(G) = 11 = 4 + 8 - 1 = \eta_{\pm}(G) + \exp(G) - 1$.

Para $G = C_2^3$, temos $\exp(G) = 2$ e neste caso cada elemento é igual ao seu inverso. Daí, somar ou subtrair elementos de uma sequência não faz diferença e o resultado se resume a $s(G) = \eta(G) + \exp(G) - 1$ que se verifica ao calcularmos $s(G)$ e $\eta(G)$ conforme o Lema 5.10. Isso conclui a prova do item *(a)*.

(b) Sejam $A = \{-1, 1\}$ e G um grupo abeliano finito de ordem 16 e $\exp(G) \geqslant 4$. Então G é isomorfo a um dos seguintes grupos: $C_4^2, C_2 \oplus C_8, C_2^2 \oplus C_4$ ou C_{16}.

Quando $G = C_4^2$ ou $G = C_2 \oplus C_8$, o resultado $\eta_{\pm}(G) = 5$ segue do Teorema 5.9 *(a)* (com $l = 2$, $n = 1$ e $l = 1$, $n = 4$ respectivamente).

Quando $G = C_2^2 \oplus C_4$, o item *(b)* do Teorema 5.9 para $l = 1$, $n = 2$ nos dá $\eta_{\pm}(G) = \lfloor \log_2(2 \cdot 2) \rfloor + 2 + 1 = 5$ e quando $G = C_{16}$, temos $n_{\pm}(G) = 5$ pelo Lema 5.7 Isso prova a primeira parte do item *(b)*.

Vamos mostrar agora que $s_{\pm}(G) = 12$ quando $\exp(G) = 8$ e $s_{\pm}(G) = 8$ se $\exp(G) = 4$. Primeiramente, suponha que $S = \prod_{i=1}^{12} x_i$ é sequência de elementos de G que não admite subsequência de A-soma zero de tamanho 2. Considere o seguinte conjunto

$$B = \left\{ A_I = \sum_{i \in I} x_i \mid I \subset [1, 12], |I| = 2 \right\}.$$

Como o número de subconjuntos de $[1, 12]$ com dois elementos é 66 e $|G| = 16$, pelo Princípio das Casas dos Pombos, existem I_1, I_2, I_3, I_4 distintos tais que $A_{I_1} = A_{I_2} = A_{I_3} = A_{I_4}$ (se todos os A_I's fossem 4 a 4 distintos, deveríamos ter no máximo $3 \times 16 + 15 = 63 < 66$ somas possíveis). Como S não possui subsequência de A-soma zero de tamanho 2, devemos ter $I_i \cap I_j = \emptyset$ sempre que $i \neq j$. De fato, se para algum $i \neq j$ tivéssemos $I_i \cap I_j \neq \emptyset$, digamos, $a \in I_i \cap I_j$, teríamos

$$x_k + x_a = x_l + x_a \Rightarrow x_k = x_l$$

para algum $k, l \in [1, 12]$ e elementos repetidos nos fornecem subsequência de A-soma zero de tamanho 2.

Temos portanto $A_{I_1} + A_{I_2} - A_{I_3} - A_{I_4} = 0$ e como cada A_{I_j} é soma de dois elementos de G, isso nos dá uma subsequência de tamanho 8 de A-soma zero de S.

Suponha que $\exp(G) = 8$. Dada S sequência de elementos de G de tamanho 12, se S não possui subsequência de A-soma zero de comprimento 2, pelo que fizemos acima S possui subsequência de tamanho 8 de A-soma zero e não há mais nada a fazer. Agora, se S possui subsequência de A-soma zero de tamanho 2, digamos $S_1|S$, temos $|SS_1^{-1}| = 10 > \log_2 16 + 1 = 5$. Isso quer dizer que qualquer subsequência de SS_1^{-1} de tamanho $6 > 5$ possui uma subsequência própria de A-soma zero de tamanho par, pelo Teorema 2.1 *(a)*, ou seja, existe $S_2|SS_1^{-1}$ de A-soma zero com $|S_2| = 2$ ou 4. Pelo mesmo argumento, $SS_1^{-1}S_2^{-1}$ possui S_3 subsequência de A-soma zero de tamanho 2 ou 4. Se $|S_2| = 4$ ou $|S_3| = 4$, então obtemos a subsequência de A-soma zero de tamanho 8 que queremos: $|S_1S_2S_3| = 8$ e $S_1S_2S_3$ é de A-soma zero (observe que é impossível ter $|S_2| = |S_3| = 4$). Se ambos S_2 e S_3 tem tamanho de 2 então $SS_1^{-1}S_2^{-1}S_3^{-1}$ tem tamanho 6 e possui subsequência própria de A-soma zero e de tamanho par pelo Teorema 2.1 *(b)*, digamos, S_4. Neste caso, se $|S_4| = 2$, $S_1S_2S_3S_4$ tem tamanho 8 e se $|S_4| = 4$, $S_1S_2S_4$ é tal que $|S_1S_2S_4| = 8$. Isso mostra que $s_\pm(G) \leqslant 12$. Por outro lado, por (5.1),

$$s_\pm(G) \geqslant \eta_\pm(G) + \exp(G) - 1 = 5 + 8 - 1 = 12.$$

Agora assuma que $\exp(G) = 4$. Vamos mostrar que $s_\pm(G) = 8$. Suponha $G = C_4^2$. Pelo Teorema 3.1, temos $s_\pm(G) \geqslant 4 + 2 \cdot 2 = 8$. Seja S uma sequência de elementos de G com $|S| = 8$. Como $\log_2 |G| + 1 = 5$, aplicando o Teorema 2.1 *(b)* a uma subsequência qualquer de S de tamanho 6, existe $T|S$ de A-soma zero com $|T| \in \{2, 4\}$. Se $|T| = 4$, T é a subsequência procurada. Se $|T| = 2$, então $|ST^{-1}| = 6$ e pelo mesmo argumento existe $T'|ST^{-1}$ de A-soma zero com $|T'| \in \{2, 4\}$. Se $|T'| = 4$, T' é a subsequência procurada e se $|T'| = 2$, então TT' é a subsequência procurada. Em qualquer caso, obtemos $s_\pm(G) \leqslant 8$ e a igualdade seque.

Se $G = C_2^2 \oplus C_4$, então por (**??**), $s_\pm(G) \geqslant \eta_\pm(G) + \exp(G) - 1 = 5 + 4 - 1 = 8$. Como $6 > 5 = \log_2 |G| + 1$, pelo Teorema 2.1 *(b)* dada S sequência de elementos de G de tamanho 8, qualquer subsequência de S de tamanho 6 possui uma outra subsequência de tamanho 4 ou 2 de A-soma zero, digamos, S_1. Se $|S_1| = 4$, S_1 é a subsequência procurada. $|S_1| = 2$, então $|SS_1^{-1}| = 6$ e mais uma vez pelo Teorema 2.1 *(b)*, existe $S_2|SS_1^{-1}$ subsequência de A-soma zero com $|S_2| = 4$ ou 2. Se $|S_2| = 4$, S_2 é a subsequência procurada. Se $|S_2| = 2$, então $|S_1S_2| = 4$ e S_1S_2 é a subsequência procurada. Assim, $s_\pm(G) \leqslant 8$ e concluímos que $s_\pm(C_2^2 \oplus C_4) = 8$.

Lembrando que $s_{\pm}(C_{16}) = E_{\pm}(C_{16}) = 16 + \lfloor \log_2 16 \rfloor = 16 + 4 = 20$ pelo Teorema 2.17, concluímos que $s_{\pm}(G) = \eta_{\pm}(G) + \exp(G) - 1$ sempre que $\exp(G) \geqslant 4$ ao calcular explicitamente $s_{\pm}(G)$ e $\eta_{\pm}(G)$. Para $\exp(G) = 2$, temos $G = C_2^4$ e o resultado seque análogo ao que fizemos para $G = C_2^3$ no final da demonstração do item anterior. Temos, portanto, $s_{\pm}(G) = \eta_{\pm}(G) + \exp(G) - 1$ para todo grupo abeliano G com $|G| = 16$. ■

5.2.2 Caso $G = C_2 \oplus C_{2n}$ com $n \in \mathbb{N}$

Usando os resultados da seção anterior e o Teorema 4.10, podemos desenvolver uma estratégia para calcular o valor exato de $s_{\pm}(G)$ para $G = C_2 \oplus C_{2n}$, $n \geqslant 2$. Este resultado é parte do trabalho de L. E. Marchan *et al.*, em [20].

Teorema 5.12. *Seja $G = C_2 \oplus C_{2n}$, $n \geqslant 2$. Então*

$$s_{\pm}(G) = 2n + \lfloor \log_2 2n \rfloor + 1.$$

Demonstração: Pelo Teorema 5.9 *(a)* para $l = 1$, temos $\eta_{\pm}(G) = \lfloor \log_2 2n \rfloor + 2$. Como $\exp(G) = 2n$, temos $\eta_{\pm}(G) + \exp(G) - 1 = \lfloor \log_2 2n \rfloor + 2n + 1$.

Por (5.1), temos $s_{\pm}(G) \geqslant \exp(G) + \eta_{\pm}(G) - 1$. Portanto, basta mostrar que $s_{\pm}(G) \leqslant \exp(G) + \eta_{\pm}(G) - 1$.

Pelos teoremas 5.9 *(a)* e 3.1, $\eta_{\pm}(G) = D_{\pm}(G) = \lfloor \log_2 |G| \rfloor + 1$ (os limites inferior e superior de $D_{\pm}(G)$ dados no Teorema 3.1 coincidem e são iguais a $\lfloor \log_2 |G| \rfloor + 1$).

Sejam $A = \{-1, 1\}$ e S uma sequência de elementos de G com $|S| = \exp(G) + \eta_{\pm}(G) - 1 = \exp(G) + \lfloor \log_2 |G| \rfloor$ e suponha por contradição que S não possua subsequência de A-soma zero de tamanho $\exp(G)$.

Vamos começar introduzindo uma sequência auxiliar. Seja $M|S$ tal que $|M|$ é o maior possível par e M possui subsequência de A-soma zero de tamanho m para cada $m \leqslant |M|$, m par. Note que essa definição certamente faz sentido pois a sequência trivial cumpre essa condição. A demonstração do teorema se resume, portanto, a mostrar que $|M| \geqslant \exp(G)$.

Mostremos primeiro que $|M| > 0$. Note que, pelo Teorema 4.10, $|S| \geqslant g_{\pm}(G) = 2n + 2$. Aqui, devemos assumir que S não é livre de quadrados pois se assim fosse, pela definição de $g_{\pm}(G)$, S teria uma subsequência de A-soma zero de tamanho $\exp(G)$, o que estamos assumindo que não acontece. Assim, existe $g \in G$ com $g^2|S$ e g^2 é uma subsequência de A-soma zero de tamanho 2 mostrando que $|M| \geqslant |g^2| = 2$.

Afirmamos que $M^{-1}S$ não pode ter subsequência de A-soma zero de tamanho par menor ou igual a $|M|+2$. De fato, se existe $N|M^{-1}S$ subsequência de A-soma zero com $|N| = 2k < |M| + 2$, então MN possui subsequência de A-soma zero de tamanho r para cada r par, $r \leqslant |MN|$. Para $n < |M|$ isso é claro pela construção da sequência M e para $n \geqslant |M| + 2$, podemos combinar N com subsequências de M de tamanho $n - |N|$ (note que $|N| \leqslant |M| + 2 \leqslant n \leqslant |M| + |N|$). Mas $|M|$ é o maior que satisfaz isso.

Como sabemos agora que $M^{-1}S$ não possui subsequência de A-soma zero de comprimento 2, temos que $M^{-1}S$ é livre de quadrados e, consequentemente, $|M^{-1}S| < g_{\pm}(G) = 2n + 2$. (se $|M^{-1}S| \geqslant g_{\pm}(G)$, então existe $P|M^{-1}S$ com

$|P| = \exp(G) = 2n$ de A-soma zero. Mas $P|M^{-1}S|S$, contradizendo o que supomos sobre S não possuir subsequência de soma zero de tamanho $\exp(G)$).

Agora note que como $|M^{-1}S| = |S| - |M| < 2n + 2$ e $|S| = 2n + \lfloor \log_2 |G| \rfloor$, temos $|M| \geqslant |S| - 2n - 1 = \lfloor \log_2 |G| \rfloor - 1$. A seguir, vamos mostrar que, mais que isso, $|M| \geqslant \lfloor \log_2 |G| \rfloor$. Suponha que isso não ocorre. Então $|M| = \lfloor \log_2 |G| \rfloor - 1$ e $|M^{-1}S| = |S| - |M| = 2n + 1$. Considere $H \leq G$, $H = C_{2n}$ e seja e o elemento de ordem 2 tal que $G = \langle e \rangle \oplus H$. Escreva $M^{-1}S = T_0(e + T_e)$ onde T_0, T_e são sequências sobre H. Note que ambas são livres de quadrados. Considere T_x a maior das duas e temos $|T_x| \geqslant n + 1$. Como $\lfloor \log_2 2n \rfloor \leqslant n - 1$ para $n \geqslant 3$, temos $|T_x| \geqslant \lfloor \log_2 |H| \rfloor + 2$ e segue do Corolário 2.2 *(b)* que T_x possui uma subsequência de A-soma zero de comprimento par e no máximo $\lfloor \log_2 |H| \rfloor + 2$. Note que isso nos garante a existência de uma subsequência de A-soma zero de mesmo tamanho de $M^{-1}S$. Isso é claro se $x = 0$ e caso $x = e$, isso segue do fato de que o tamanho da tal subsequência é par e $\mathrm{o}(e) = 2$. Agora $\lfloor \log_2 |H| \rfloor + 2 = \lfloor \log_2 |G| \rfloor + 1 = |M| + 2$, contradizendo o que afirmamos sobre $M^{-1}S$ não possuir subsequência de A-soma zero com comprimento par e no máximo $|M| + 2$.

Estabelecemos assim que $|M| \geqslant \lfloor \log_2 |G| \rfloor$. Por fim, assuma $|M| \leqslant \exp(G) - 2$. Então $|M^{-1}S| \geqslant \lfloor \log_2 |G| \rfloor + 2$. De novo, pelo Corolário 2.2, temos uma subsequência de $M^{-1}S$ (e, portanto, subsequência de S) de A-soma zero e tamanho par menor ou igual a $\lfloor \log_2 |G| \rfloor + 2 \leqslant |M| + 2$, uma contradição. Concluímos portanto que $|M| \geqslant \exp(G)$, uma vez que $|M|$ é par e isso finaliza a demonstração do teorema. ∎

Observação 5.13. Seja $G = C_2 \oplus C_{2n}$. Se $n = 1$, temos $s_{\pm}(G) = 5$ e $\eta_{\pm}(G) = 4$ pelo Lema 5.10. Assim, temos

$$s_{\pm}(G) = 5 = 4 + 1 - 1 = \eta_{\pm}(G) + \exp(G) - 1.$$

Se $n \geqslant 2$, pelo Teorema 5.12 temos $s_{\pm}(G) = 2n + \lfloor \log_2 2n \rfloor + 1$ e pelo Teorema 5.9, temos $D_{\pm}(G) = \eta_{\pm}(G) = \lfloor \log_2 2n \rfloor + 2$. Assim, temos

$$s_{\pm}(G) = 2n + \lfloor \log_2 2n \rfloor + 1 = \lfloor \log_2 2n \rfloor + 2 + 2n - 1 = \eta_{\pm}(G) + \exp(G) - 1.$$

Concluímos, portanto, que a relação (5.2) se verifica para $G = C_2 \oplus C_{2n}$ para todo $n \in \mathbb{N}$.

5.2.3 Caso G de ordem 32

Este caso foi estudado em 2016, por S. D. Adhikari, E. Mazumdar e B. K. Moriya, em [5].

Lema 5.14. *Dados $r, n \in \mathbb{N}$, temos*

$$\eta_{\pm}(C_2^r \oplus C_{2n}) \geqslant \max\left\{ \lfloor \log_2 2n \rfloor + r + \left\lfloor \frac{r}{2n-1} \right\rfloor, r + A(r,n) \right\} + 1$$

onde $A(r,n) = \begin{cases} 1 & se\ r \leqslant n \\ \lfloor r/n \rfloor & se\ r > n \end{cases}$.

Demonstração: Se $n = 1$, temos C_2^{r+1} um 2-grupo elementar e logo $\eta_\pm(C_2^{r+1}) = |C_2^{r+1}| = 2^{r+1}$ pelo Lema 5.10. Por outro lado,

$$\lfloor \log_2 2n \rfloor + r + \left\lfloor \frac{r}{2n-1} \right\rfloor = r + 1 + r = 2r + 1 \text{ e}$$

$$r + A(r,n) = \begin{cases} 1 + 1 = 2 & \text{se } r = 1 \\ r + r = 2r & \text{se } r > 1 \end{cases} = 2r.$$

Assim,

$$\max\left\{ \lfloor \log_2 2n \rfloor + r + \left\lfloor \frac{r}{2n-1} \right\rfloor, r + A(r,n) \right\} + 1 = \max\{2r+1, 2r\} + 1 = 2r + 2$$

e pelo item *(a)* do Lema 5.8, $\eta_\pm(C_2^{r+1}) = 2^{r+1} \geqslant (2r+1) + 1 = 2r + 2$. Isso prova o lema quando $n = 1$.

Suponha então $n > 1$. Seja $A = \{-1, 1\}$ e considere a sequência

$$S = \prod_{i=1}^{r} e_i \prod_{t=0}^{s} f_t \prod_{j=1}^{k} g_j,$$

onde $s = \lfloor \log_2 2n \rfloor - 1$, $k = \left\lfloor \frac{r}{2n-1} \right\rfloor$ e e_i, f_t, g_j são definidos como abaixo:

$$e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$$

com 1 na i-ésima posição para $1 \leqslant i \leqslant r$,

$$f_t = (0, 0, \ldots, 0, 2^t), \quad \text{para } 0 \leqslant t \leqslant s,$$

$$g_{j+1} = (0, 0, \ldots, 0, 1, 1, \ldots, 1, 0, \ldots, 0, 1),$$

com 1 na $(r+1)$-ésima posição e nas posições $(2n-1)j+1, (2n-1)j+2, \ldots, (2n-1)j + 2n - 1$, para $0 \leqslant j \leqslant k - 1$.

Vamos mostrar que S não possui subsequência não trivial de A-soma zero. Primeiramente, pela construção de S, é imediato que $\prod_{i=1}^{r} e_i \prod_{t=0}^{s} f_t$ não possui subsequência não trivial de A-soma zero. Assim, uma subsequência de A-soma zero de S deve conter pelo menos um elemento de $\prod_{j=1}^{k} g_j$. Por outro lado, se $T | S$ é de A-soma zero que contém um dos g_j's, então T deve conter, no mínimo, $2n - 1$ elementos entre os e_i's e um entre os f_t's, ou seja, $|T| \geqslant 2n+1 > 2n = \exp(C_2^r \oplus C_{2n})$ e T não satisfaz a condição que a constante $\eta_\pm(C_2^r \oplus C_{2n})$ impõe. Isso mostra que

$$\eta_\pm(C_2^r \oplus C_{2n}) \geqslant |S| = r + (s+1) + k = r + \lfloor \log_2 2n \rfloor + \left\lfloor \frac{r}{2n-1} \right\rfloor.$$

Para ver que $\eta_\pm(C_2^r \oplus C_{2n}) \geqslant r + A(r,n) + 1$, observe que se $r \leqslant n$ então a sequência $S_1 = f_1 \prod_{i=1}^{r} e_i$ é tal que $|S_1| = r + 1 = r + A(r,n)$ e S_1 não possui subsequência não trivial de A-soma zero. Se $r > n$, a sequência $S_2 = \prod_{i=1}^{r} e_i \prod_{j=1}^{u} h_j$ onde $u = \lfloor r/n \rfloor$ e

$$h_{j+1} = (0, 0, \ldots, 0, 1, 1, \ldots, 1, 0, \ldots, 0, 1)$$

com 1 na $(r+1)$-ésima posição e nas posições $nj + 1, nj + 2, \ldots, nj + n$ com $0 \leqslant$

$j \leqslant u-1$ é tal que $|S_2| = r + \lfloor r/n \rfloor = r + A(r, n)$ e S_2 não possui subsequência não trivial de A-soma zero. De fato, da mesma forma como fizemos anteriormente para S, $\prod_{i=1}^{r} e_i$ não possui subsequência de A-soma zero. Assim, uma subsequência de A-soma zero de S_2 deve conter pelo menos um elemento de $\prod_{j=1}^{u} h_j$. Por outro lado, dada T subsequência de A-soma zero de S_2 que contenha um dos h_j's, então T deve conter, no mínimo, dois h_j's para que seja possível obter o zero na $(r+1)$-ésima posição e logo T deve conter, no mínimo, $2n$ elementos de $\prod_{i=1}^{r} e_i$, ou seja, $|T| \geqslant 2n + 2 > 2n = \exp(C_2^r \oplus C_{2n})$ e isso mostra que

$$\eta_{\pm}(C_2^r \oplus C_{2n}) \geqslant |S_2| + 1 = r + A(r, n) + 1.$$

Isso conclui a demonstração do lema. ■

Observação 5.15. Sejam G um grupo aditivo abeliano, $A = \{-1, 1\}$ e $S = g_1, \ldots, g_n \in \mathcal{F}(G)$.

(a) Se S é livre de quadrados e $M = \{g_j + g_j \,|\, 1 \leqslant i < j \leqslant n\}$ é tal que $\binom{n}{2} > |M|$, então pelo menos duas das somas que formam M são iguais, ou seja, $g_i + g_j = g_k + g_l$ para $i, j, k, l \in [1, n]$ com $\{i, j\} \neq \{k, l\}$ e o fato se S ser livre de quadrados garante que $\{i, j\} \cap \{k, l\} = \emptyset$. Daí, S possui uma subsequência de A-soma zero de tamanho 4.

(b) Se $n \geqslant 4$ e $g_1 = g_2$ então $g_1 g_2$ é uma subsequência de A-soma zero de S de tamanho 2. Assim, se $T = (g_1 g_2)^{-1} S$ não é livre de quadrados, existe $T_1 | T$ de A-soma zero de tamanho 2 e logo $g_1 g_2 T_1$ é uma subsequência de A-soma zero de S de tamanho 4.

Lema 5.16. *Temos*

$$s_{\pm}(C_2^3 \oplus C_4) = 10 \text{ e } \eta_{\pm}(C_2^3 \oplus C_4) = 7.$$

Demonstração: Sejam $A = \{-1, 1\}$, $G = C_2^3 \oplus C_4$ e $S = g_1 \cdots g_{10} \in \mathcal{F}(G)$. Se S é livre de quadrados, como $\binom{10}{2} = 45 > 32 = |G|$, então S possui uma subsequência de A-soma zero de tamanho 4 pelo item (a) da Observação 5.15. Suponha então que S não é livre de quadrados e, sem perda de generalidade, considere $g_1 = g_2$. Pela Observação 5.15 (b), se $T = (g_1 g_2)^{-1} S$ não é livre de quadrados, S possui uma subsequência de A-soma zero de tamanho 4. Vamos assumir então T livre de quadrados.

Se T tem no máximo um elemento de ordem 4, então pelo menos sete elementos de T tem ordem ordem no máximo 2. Como a soma de dois elementos distintos em $C_2^3 \oplus C_4$ de ordem no máximo 2 tem ordem 2, G possui 15 elementos de ordem 2 e $\binom{7}{2} = 21 > 15$, pela Observação 5.15 (a), T (e, portanto, S) possui uma subsequência de A-soma zero de tamanho 4.

Se T possui pelo menos dois elementos de ordem 4, considere o conjunto abaixo

$$\begin{aligned} D = &\{g_i \pm g_j, \quad 3 \leqslant i < j \leqslant 10,\, \mathrm{o}(g_i) = \mathrm{o}(g_j) = 4\} \\ &\cup \{g_r + g_s, \quad 3 \leqslant r < s \leqslant 10, \mathrm{o}(g_r) = \mathrm{o}(g_s) = 2\}. \end{aligned}$$

Temos $D \subseteq \{g \in C_2^3 \oplus C_4 \,|\, \mathrm{o}(g) \leqslant 2\}$. De fato, como dissemos acima, a soma de dois elementos distintos de ordem no máximo 2 tem ordem 2 e, lembrando que os elementos de ordem 4 neste grupo são os que tem última coordenada igual a 1 ou 3 e em C_4, $1+1=2$, $3+3=2$ e $1+3=0$, a soma de elementos de ordem 4 em $C_2^3 \oplus C_4$ sempre fornece elementos de ordem no máximo 2.

Seja $N = 2\binom{c}{2} + \binom{d}{2}$ onde c e d são quantos dos g_i's tem ordem 4 e 2, respectivamente e observe que $c+d=8$. Existem 16 elementos de ordem 4 em $C_2^3 \oplus C_4$, mas como $|T| = 8$ e supomos que pelo menos dois deles tem ordem 4, temos $c \in [2, 8]$. Substituindo os valores de c em N vemos que $N \geqslant 16$ para qualquer $c \in [2, 8]$. Mas como $|D| \leqslant |\{g \in C_2^3 \oplus C_4 \,|\, \mathrm{o}(g) \leqslant 2\}| = 15$, segue que duas das somas A-ponderadas de D devem ser iguais. Isso pode acontecer das seguintes maneiras:

Caso 1. Se uma das somas A-ponderadas $g_i \pm g_j$ com $\mathrm{o}(g_i), \mathrm{o}(g_j) = 4$ é igual a uma das somas $g_r + g_s$ com $\mathrm{o}(g_r), \mathrm{o}(g_s) = 2$, então $g_i g_j g_r g_s$ é uma subsequência de T de A-soma zero.

Caso 2. Se $g_r + g_s = g_u + g_v$, então pela observação anterior, $g_r g_s g_u g_v$ forma uma subsequência de T de A-soma zero.

Caso 3. Se duas somas A-ponderadas $g_i \pm g_j$ e $g_p \pm g_q$ com g_i, g_j, g_p, g_q elementos de ordem 4, são iguais e $\{i, j\} \cap \{p, q\} = \emptyset$, então $g_i g_j g_p g_q$ é uma subsequência de T de A-soma zero. Se $\{i, j\} \cap \{p, q\} \neq \emptyset$, então $|\{i, j\} \cap \{p, q\}| = 1$ e observe que como $\mathrm{o}(g_j) = 4$, $g_i + g_j \neq g_i - g_j$. Assim, as possibilidades para a igualdade das somas A-ponderadas são, em resumo,

$$g_i + \epsilon g_j = g_p + \delta g_q,$$

onde $i, j, p, q \in [3, 10]$ com $i < j$, $p < q$, $|\{i, j\} \cap \{p, q\}| = 1$ e $\epsilon, \delta \in \{1, -1\}$. Vamos estudar cada uma delas.

Se $i = p$, então $g_j g_q$ é uma subsequência de A-soma zero de de T de tamanho 2.

Se $i = q$ e $\delta = 1$, então $g_j g_p$ é uma subsequência de A-soma zero de de T de tamanho 2.

Se $j = p$ e $\epsilon = 1$, então $g_i g_q$ é uma subsequência de A-soma zero de de T de tamanho 2.

Se $i = q$ e $\delta = -1$, obtemos uma expressão da forma

$$g_s + \lambda g_t = 2g_u, \text{ onde } \{s, t, u\} = \{i, j\} \cup \{p, q\},\ \lambda \in \{1, -1\}. \tag{5.6}$$

Se $j = q$, então $i \neq p$ e como T é livre de quadrados, $g_i \neq g_p$. Daí, $\delta \neq \epsilon$ e obtemos neste caso uma expressão como (5.6).

Agora, somando $2g_t$ em cada lado de (5.6), temos $g_s + (\lambda+2)g_t = 2(g_u + g_t) = 0$, já que $\mathrm{o}(g_u + g_t) = 2$. Como $\lambda + 2 \in \{1, 3\}$ e $3g_t = -g_t$, temos $g_s g_t$ uma subsequência de A-soma zero de T de tamanho 2.

Mostramos, portanto, que $s_{\pm}(C_2^3 \oplus C_4) \leqslant 10$. Agora, pelo Lema 5.14,

$$\eta_{\pm}\left(C_2^3 \oplus C_4\right) \geqslant \lfloor \log_2 4 \rfloor + 3 + \left\lfloor \frac{3}{4-1} \right\rfloor + 1 = 7$$

e, finalmente, temos

$$10 \geqslant s_{\pm}\left(C_2^3 \oplus C_4\right) \geqslant \eta_{\pm}\left(C_2^3 \oplus C_4\right) + 3 = 10.$$

Isso completa a demonstração do lema. ∎

Lema 5.17. *Para todo $k > 1$ a soma dos elementos de C_2^k é o zero de C_2^k.*

Demonstração: Vamos proceder por indução sobre k. Se $k = 2$, então $C_2^k = \{(0,0), (0,1), (1,0), (1,1)\}$ e

$$(0,0) + (0,1) + (1,0) + (1,1) = (0,0).$$

Suponha que para $k = t \in \mathbb{N}_{\geqslant 2}$ seja verdade que $\sum_{a \in C_2^t} a = 0$. Para $k = t+1$, temos $C_2^{t+1} = C_2^t \oplus C_2$ e

$$\sum_{(a,b) \in C_2^{t+1}} (a,b) = \sum_{a \in C_2^t} (a,0) + \sum_{a \in C_2^t} (a,1) = (0,0) + (0, 2^t \cdot 1) = (0,0).$$

Isso conclui a demonstração. ∎

Lema 5.18. *Temos*

$$s_{\pm}(C_2 \oplus C_4^2) = 9 \text{ e } \eta_{\pm}(C_2 \oplus C_4^2) = 6.$$

Demonstração: Sejam $A = \{-1, 1\}$, $G = C_2 \oplus C_4^2$ e $S = g_1 \cdots g_9 \in \mathcal{F}(G)$. Vamos mostrar que S possui uma subsequência de A-soma zero de tamanho 4.

Se S é livre de quadrados, como $\binom{9}{2} = 36 > 32 = |G|$, pela Observação 5.15 (a), S possui uma subsequência de A-soma zero de tamanho 4. Assuma então, sem perda de generalidade, que $g_1 = g_2$ e pela Observação 5.15(b), podemos supor $T = (g_1 g_2)^{-1} S$ livre de quadrados.

Vamos mostrar que T possui uma subsequência de A-soma zero de tamanho 4 ou 2. Observe que G é formado pelo elemento neutro, sete elementos de ordem 2 e 24 elementos de ordem 4.

Vamos caracterizar os elementos de ordem 4 de G. Dado $g = (x, y, z) \in G$ tem ordem 4, se somente y ou somente z de ordem 4 em C_4, vamos dizer que g é do tipo 1 ou 2, respectivamente. Se ambos y e z tem ordem 4 em C_4, vamos dizer que g é do tipo 3. Uma observação é que a soma de dois elementos de diferentes tipos tem ordem 4, a soma de dois elementos de mesmo tipo tem ordem 2 e a soma de três elementos, um de cada tipo, tem ordem 2. Além disso, com o que acabamos de observar, é fácil ver que se g_i, g_j e g_k são de tipos diferentes, então as quatro somas A-ponderadas $g_i \pm g_j \pm g_k$ são distintas e de ordem no máximo 2.

A seguir, vamos considerar vários casos de acordo com a quantidade de elementos de ordem 4 em T.

Caso 1. Se T tem no máximo dois elementos de ordem 4, então T possui pelo menos cinco elementos de ondem no máximo 2 e como $\binom{5}{2} = 10 > 8$, pela Observação 5.15 (a), T possui uma subsequência de A-soma zero de tamanho 4.

Caso 2. Se T exatamente três elementos de ordem 4, digamos g_7, g_8, g_9, então g_3, g_4, g_5, g_6 tem ordem no máximo 2. O número de subsequências de tamanho 2 de $g_3 g_4 g_5 g_6$ é $\binom{4}{2} = 6$ e para cada subsequência $g_i g_j$, podemos fazer corresponder uma soma $g_i + g_j$.

Suponha que dentre os elementos g_7, g_8, g_9 pelo menos dois deles são do mesmo tipo, digamos g_7 e g_8. Como $\mathrm{o}(g_8) = 4$, temos $g_7 + g_8 \neq g_7 - g_8$. Considere o conjunto

$$B = \{g_i + g_j \,|\, 3 \leqslant i < j \leqslant 6\} \cup \{g_7 + g_8, g_7 - g_8\}$$

e observe que $B \subseteq \{g \in G \,|\, \mathrm{o}(g) \leqslant 2\}$, ou seja, $|B| \leqslant 8$. Se nenhuma das somas A-ponderadas que formam B é nula, então duas das somas $g_i + g_j$ com $3 \leqslant i < j \leqslant 6$ devem ser iguais, ou uma soma $g_i + g_j$ $3 \leqslant i < j \leqslant 6$ deve ser igual a $g_7 + g_8$ ou $g_7 - g_8$ e em qualquer caso, temos uma subsequência de A-soma zero de T de tamanho 4.

Se os três elementos g_7, g_8, g_9 são cada um de um tipo, então pelo que observamos acima, as quatro somas A-ponderadas $g_7 \pm g_8 \pm g_9$ são distintas e são todas de ordem no máximo 2. Se algum dos elementos g_3, g_4, g_5, g_6 é igual a uma das somas A-ponderadas $g_7 \pm g_8 \pm g_9$, então obtemos uma subsequência de A-soma zero de T de tamanho 4. Caso contrário, os elementos g_3, g_4, g_5, g_6 juntamente com as quatro somas $g_7 \pm g_8 \pm g_9$ nos dão todos os elementos de ordem no máximo 2 de G, ou seja, formam o subgrupo de G isomorfo a C_2^3. Agora como para $k > 1$ a soma de todos os elementos de C_2^k é zero pelo Lema 5.17, temos

$$\begin{aligned} 0 &= g_3 + g_4 + g_5 + g_6 + (g_7 + g_8 + g_9) + (g_7 + g_8 - g_9) \\ &\quad + (g_7 - g_8 + g_9) + (g_7 - g_8 - g_9) \\ &= g_3 + g_4 + g_5 + g_6 + 4g_7 \\ &= g_3 + g_4 + g_5 + g_6 \end{aligned}$$

ou seja, $g_3 g_4 g_5 g_6$ é uma subsequência de T de A-soma zero.

Caso 3. Se T possui quatro elementos de ordem 4, digamos g_6, g_7, g_8, g_9, então g_3, g_4, g_5 tem ordem no máximo 2.

Agora, se entre g_6, g_7, g_8, g_9 pelo menos três elementos são do mesmo tipo, digamos g_6, g_7, g_8, lembrando que a soma de elementos de ordem 4 do mesmo tipo tem ordem 2, entre as somas A-ponderadas $g_6 \pm g_7, g_6 \pm g_8, g_7 \pm g_8$ e as três somas $g_i + g_j$, $3 \leqslant i < j \leqslant 5$, devem existir duas iguais e pelo que fizemos na prova do Lema 5.16, isso garante que T possui uma subsequência de A-soma zero de tamanho 4.

Se entre g_6, g_7, g_8, g_9 há dois elementos de um tipo, digamos g_6, g_7 e os outros dois são de um outro tipo, consideramos os elementos $g_6 \pm g_7$, $g_8 \pm g_9$ juntamente com as somas $g_i + g_j$, $3 \leqslant i, j \leqslant 5$. Se duas dessas somas A-ponderadas são iguais, então T possui uma subsequência de A-soma zero de tamanho 4. Se alguma delas é 0, então T possui uma subsequência de A-soma zero de tamanho 2. Se todas elas são distintas e não nulas, então elas são todos os elementos não nulos de ordem 2 de G e como vimos no caso anterior, a soma deles é 0. Porém, ao somar todos os elementos obtemos $2(g_6 + g_8)$ e como $(g_6 + g_8)$ tem ordem 4, é impossível que tenhamos dois elementos de ordem 4 de um tipo e dois de outro tipo.

Finalmente, se dois elementos digamos, g_6, g_7 são do mesmo tipo e os outros dois são cada um de um dos outros tipos, considere as somas A-ponderadas

$$g_5 + g_6 \pm g_8 \pm g_9, g_6 + g_7, g_6 + g_7 + g_3 + g_5, g_6 + g_7 + g_4 + g_5.$$

Como anteriormente, se duas dessas somas são iguais ou uma delas é 0, obtemos uma subsequência de A-soma zero de T de tamanho 4 ou 2, respectivamente.

Caso contrário, a soma deles todos é $3g_6 + 3g_7 + g_3 + g_4 = -g_6 - g_7 + g_3 + g_4 = 0$ e isso nos fornece uma subsequência de A-soma zero de T de tamanho 4.

Caso 4. T possui pelo menos seis elementos de ordem 4, digamos, g_4, g_5, g_6, g_7, g_8 e g_9. Se quatro desses elementos são do mesmo tipo, digamos, g_4, g_5, g_6, g_7, então considere

$$g_4 \pm g_j, \quad j \in \{5, 6, 7\}, \quad \text{e } g_5 \pm g_6.$$

Se todas as somas A-ponderadas acima são distintas, então uma delas é 0 e obtemos uma subsequência de T de A-soma zero de tamanho 2. Se duas delas são iguais, então obtemos uma subsequência de T de A-soma zero de tamanho 4 pelo mesmo argumento feito no Lema 5.16.

Se no máximo três elementos são do mesmo tipo, então temos as seguintes possibilidades: se há três elementos de um mesmo tipo, então pelo menos dois dos elementos restantes são de um outro tipo, digamos g_4, g_5, g_6 de um tipo e g_7, g_8 de outro. Considerando as somas A-ponderadas $g_4 \pm g_5, g_4 \pm g_6, g_5 \pm g_6$ e $g_7 \pm g_8$, obtemos que duas delas devem ser iguais e isso nos dá uma subsequência de A-soma zero de T de tamanho 4.

Se há dois elementos de cada tipo, digamos, $g_4 g_5$ do tipo 1, g_6, g_7 do tipo 2 e g_8, g_9 do tipo 3, como dissemos no começo da demonstração, os elementos $g_4 \pm g_6 \pm g_8$ são todos distintos e, da mesma forma, $g_4 \pm g_7 \pm g_9$ são distintos.

Se algum do primeiro grupo for igual a algum do segundo, obtemos uma subsequência de A-soma zero de T de tamanho 4. Caso contrário, temos uma lista completa dos elementos de ordem 2 de G. Se $\mathrm{o}(g_3) = 2$, então g_3 é igual a um deles e isso nos dá a subsequência procurada. Se $\mathrm{o}(g_3) = 4$, então há três elementos de um tipo e dois de outro e voltamos ao caso anterior.

Caso 5. T possui cinco elementos de ordem 4, digamos g_5, g_6, g_7, g_8, g_9, e dois elementos de ordem 2, digamos g_3, g_4.

Se entre os elementos de ordem 4 há quatro elementos do mesmo tipo ou três elementos de um tipo e dois de outro, recaímos sobre o Caso 4.

Se nada disso acontece, então devemos ter elementos de ordem 4 de todos os três tipos. Neste caso, as duas situações abaixo são possíveis:

Subcaso 5.1. Há um elemento, digamos g_5 de um tipo, dois elementos, digamos g_6, g_7 de outro tipo e g_8, g_9 do último tipo. Nesta situação, se um entre os quatro elementos distintos $g_5 \pm g_7 \pm g_9$ é igual a algum dos elementos $g_5 \pm g_6 \pm g_8$ então temos uma subsequência de A-soma zero de tamanho 4. Se são todos distintos, então algum deles é igual a g_3 e isso nos fornece uma uma subsequência de A-soma zero de T de tamanho 4.

Subcaso 5.2. Há três elementos de um tipo, digamos g_5, g_6, g_7 e os outros dois elementos são um de cada um dos outros dois tipos. Considere os elementos

$$g_5 \pm g_8 \pm g_9, g_5 \pm g_6 + g_3, g_5 \pm g_7 + g_3.$$

Como vimos antes, a igualdade de dois desses elementos nos dá a subsequência procurada. Se todos são distintos, então são todos os elementos de ordem 2 de G e g_4 é igual a algum deles. Com isso, obtemos a subsequência procurada.

Concluímos, portanto, que $s_{\pm}(G) \leqslant 9$.

Como a sequência $(1, 0, 0)(0, 1, 0)(0, 2, 0)(0, 0, 1)(0, 0, 2)$ não possui subsequência não trivial de A-soma zero, temos $\eta_\pm(G) \geqslant 6$ e por fim

$$9 \geqslant s_\pm(G) \geqslant \eta_\pm(G) + \exp(G) - 1 \geqslant 5 + 4 - 1 = 9.$$

Isso completa a prova do lema. ■

Lema 5.19. *Se G é um grupo abeliano com $|G| = 32$ e $\exp(G) = 8$, então*

$$s_\pm(G) = 13 \text{ e } \eta_\pm(G) = 6.$$

Demonstração: Sejam $A = \{-1, 1\}$ e $S = g_1 \cdots g_{13} \in \mathcal{F}(G)$, vamos mostrar que S possui uma subsequência de A-soma zero de tamanho 8.

Se S é livre de quadrados, sabendo que $\binom{13}{2} = 78 > 32 = |G|$, pela Observação 5.15 (a), obtemos $S_1|S$ de A-soma zero e de tamanho 4. Como $\binom{9}{2} = 36 > 32$ então a sequência SS_1^{-1} também possui uma subsequência de A-soma zero de tamanho 4, digamos S_2. Assim $S_1S_2|S$ é de A-soma zero de tamanho 8.

Suponha então que S não é livre de quadrados, digamos $g_1 = g_2$. Então $T = g_1g_2$ é uma subsequência de A-soma zero de S de tamanho 2.

Se ST^{-1} é livre de quadrados, observando que $\binom{11}{2} > 32$, existe $T_1|ST^{-1}$ de A-soma zero de tamanho 4 pela Observação 5.15 (a). Como $|ST^{-1}T_1^{-1}| = 7 = \lfloor \log_2 |G| \rfloor + 2$, pelo Corolário 2.2 *(b)*, existe $T_2|ST^{-1}T_1^{-1}$ de A-soma zero com $|T_2| \in \{2, 4, 6\}$.

Se $|T_2| = 2$, então TT_1T_2 é uma subsequência de A-soma zero de S de tamanho 8. Se $|T_2| = 4$, então T_1T_2 é uma subsequência de A-soma zero de S de tamanho 8 e se $|T_2| = 6$ então TT_2 é uma subsequência de A-soma zero de S de tamanho 8.

Se ST^{-1} não é livre de quadrados, digamos $g_3 = g_4$, então $U_1 = g_3g_4$ é uma subsequência de A-soma zero de S de tamanho 2. Como $|ST^{-1}U_1^{-1}| = 9$, pelo Corolário 2.2 *(b)*, existe $U_2|ST^{-1}U_1^{-1}$ de A-soma zero com $|U_2| \in \{2, 4, 6\}$. Se $|U_2| = 6$, então U_2T é uma subsequência de A-soma zero de S de tamanho 8. Se $|U_2| = 4$, então U_2T_1 é uma subsequência de A-soma zero de S de tamanho 8 e se $|U_2| = 2$, então $|ST^{-1}U_1^{-1}U_2^{-1}| = 7$ e de novo pelo Corolário 2.2 *(b)*, existe $U_3|ST^{-1}U_1^{-1}U_2^{-1}$ com $|U_3| \in \{2, 4, 6\}$ e para cada valor de $|U_3|$, temos uma uma subsequência de A-soma zero de S de tamanho 8: se $|U_3| = 2$, temos $U_2U_3T_1$, se $|U_3| = 4$, temos U_3U_2T e se $|U_3| = 6$ temos U_3T. Em qualquer caso, concluímos que $s_\pm(G) \leqslant 13$.

Agora, $G = C_4 \oplus C_8$ ou $G = C_2^2 \oplus C_8$. Se $G = C_4 \oplus C_8$, então a sequência

$$(0,1)(0,2)(0,4)(1,0)(2,0)$$

não possui subsequência não trivial de A-soma zero e se $G = C_2^2 \oplus C_8$, então a sequência

$$(0,0,1)(0,0,2)(0,0,4)(0,1,0)(1,0,0)$$

não possui subsequência não trivial de A-soma zero. Em qualquer caso, temos $\eta_\pm(G) \geqslant 6$.

De acordo com as informações obtidas acima, temos

$$13 \geqslant s_\pm(G) \geqslant \eta_\pm(G) + \exp(G) - 1 \geqslant 6 + 8 - 1 = 13$$

e isso conclui a prova do lema. ■

Teorema 5.20. *Se G é um grupo abeliano com $|G| = 32$, então $s_\pm(G) = \eta_\pm(G) + \exp(G) - 1$.*

Demonstração: Se G é um 2-grupo elementar, então $s_\pm(G) = 33$ e $\eta_\pm(G) = 32$ pelo Lema 5.10 e temos

$$\eta_\pm(G) + \exp(G) - 1 = 32 + 2 - 1 = 33 = s_\pm(G).$$

Se $\exp(G) = 4$, então $G = C_2^3 \oplus C_4$ ou $G = C_2 \oplus C_4^2$. Para o primeiro caso, pelo Lema 5.16 temos

$$\eta_\pm(G) + \exp(G) - 1 = 7 + 4 - 1 = 10 = s_\pm(G)$$

e para o segundo caso, o Lema 5.18 nos dá que

$$\eta_\pm(G) + \exp(G) - 1 = 6 + 4 - 1 = 9 = s_\pm(G).$$

Se $\exp(G) = 8$, então pelo Lema 5.19,

$$\eta_\pm(G) + \exp(G) - 1 = 6 + 8 - 1 = 13 = s_\pm(G).$$

Se $\exp(G) = 16$, então $G = C_2 \oplus C_{16}$ e o resultado segue da Observação 5.13.

Por fim, se $G = C_{32}$, temos $s_\pm(G) = 32 + \lfloor \log_2 32 \rfloor = 32 + 5 = 37$ pelo Teorema 2.17 e $D_\pm(G) = \eta_\pm(G) = 1 \cdot 5 + 1 = 6$ pelo Lema 5.7. Daí,

$$\eta_\pm(G) + \exp(G) - 1 = 6 + 32 - 1 = 37 = s_\pm(G).$$

■

Referências Bibliográficas

[1] S. D. Adhikari, M. N. Chintamani, H. Geeta and B. K. Moriya. *Cauchy-Davenport theorem: various proofs and some early generalizations*. The Mathematics Student, v. 79, p. 109-116, 2010.

[2] S. D. Adhikari, D. J. Grynkiewicz and Z. W. Sun. *On weighted zero-sum sequences*. Adv. Appl. Math., 48, p. 506-527, 2012.

[3] S. D. Adhikari, Y. G. Chen, J. B. Friedlander, S. V. Konyagin and F. Pappalardi. *Contributions to zero-sum problems*. Discrete Math, 306, p. 1-10, 2006.

[4] S. D. Adhikari and P. Rath. *Davenport constant with weights and some related questions*. Integers, v. 6, p. A30, 2006.

[5] S. D. Adhikari, E. Mazumdar and B. K. Moriya. *Relation between two weighted zero-sum constants*. Integers, v. 16, p. 1-13, 2016.

[6] P. L. Clark. *The Chevalley-Warning Theorem (featuring... the Erdos-Ginzburg-Ziv Theorem)*. Disponível em `https://bit.ly/2QKjLLT`.

[7] P. Erdös, A. Ginzburg and A. Ziv. *Theorem in the additive number theory*. Bulletiv Research Council Israel 10F, p. 41-43, 1961.

[8] W. D. Gao. *On zero-sum subsequences of restricted size II*. Discrete Mathematics, 271.1-3, p. 51-59, 2003.

[9] W. Gao and A. Geroldinger. *Zero-sum problems in finite abelian groups: a survey*. Expositiones Mathematicae, v. 24, n. 4, p. 337-369, 2006.

[10] H. Godinho, A. Lemos and D. Marques. *Weighted zero-sum problems over C_3^r*. Algebra and Discrete Mathematics, v. 15, n. 2, p. 201–212, 2013.

[11] A. Gonçalves. *Introdução à Álgebra*. 5.ed, Rio de Janeiro: IMPA, 2015.

[12] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz. *A weighted generalization of two theorems of Gao*. Ramanujan J, 28, p. 323–340, 2012.

[13] F. Halter-Koch. *Arithmetical interpretation of weighted Davenport constants*. Archiv der Mathematik, v. 103, n. 2, p. 125-131, 2014.

[14] H. Harbort. *Ein Extremalproblem für Gitterpunkte*. J. Reine Angew. Math., 262/263, p. 356–360, 1973.

[15] A. Lemos. *Problemas de soma zero com peso sobre grupos abelianos finitos.* 56 f. Tese (Doutorado em Matemática)- Universidade de Brasília, Brasília, 2010.

[16] V. F. Lev and R. Yuster. *On the size of dissociated bases.* The Electronic Journal of Combinatorics, v. 18, n. 1, p. 117, 2011.

[17] R. Lidi and H. Niederreiter. *Finite Fields.* Cambridge University Press, Cambridge, 2008.

[18] F. Luca. *A generalization of a classical zero sum problem.* Discrete mathematics, v. 307, n. 13, p. 1672-1678, 2007.

[19] L. E. Marchan, O. Ordaz and W. A. Schmid. *Remarks on the plus-minus weighted Davenport constant.* International Journal of Number Theory, v. 10, n. 05, p. 1219-1239, 2014.

[20] L. E. Marchan, O. Ordaz, D. Ramos and W. A. Schmid. *Inverse results for weighted Harborth constants.* International Journal of Number Theory, v. 12, n. 07, p. 1845-1861, 2016.

[21] L. E. Marchan, O. Ordaz, D. Ramos and W. A. Schmid. *Some exact values of the Harborth constant and its plus-minus weighted analogue.* Archiv der Mathematik, v. 101, n. 6, p. 501-512, 2013.

[22] B. K. Moriya. *On weighted zero sum subsequences of short length.* Integers, v. 14, p. A21, 2014.

[23] W. D. Gao. *A combinatorial problem on finite abelian groups.* Jornal of Number Theory, 58, p. 100-103, 1996.

[24] C. Polcino Milies. it Grupos Nilpotentes: Uma Introdução. Matemática Universitária, 34, p. 55-100, Jun., 2003.

[25] J. P. de O. Santos. *Introdução à teoria dos números*, 3. ed. Rio de Janeiro: IMPA, 2014.

[26] S. Shokranian, M. Soares and H. Godinho. *Teoria dos Números*, 2 ed. Brasília: UnB, 1999.

[27] T. Tao and V. H. Vu. *Additive combinatorics.* Cambridge University Press, 2006.

[28] X. Xia and Z. Li. *Some Davenport constants ith weights and Adhikari and Rath's conjecture.* Ars Combin., 88, p. 83–95, 2008.

[29] P. Yuan and X. Zeng. *Davenport constant with weights.* European Journal of Combinatorics, 31, p. 677-680, 2010.